1 Background

1.1 Arithmetic function

Definition. An **arithmetic function** is a complex-valued function whose domain is the positive integers.

1.2 Bernoulli numbers

Definition. The **Bernoulli numbers** are the rational numbers B_n that appear as coefficients of the formal power series

$$\frac{T}{e^T - 1} = \sum_{n \geq 0} B_n \frac{T^n}{n!},$$

which has radius of convergence 2π.

1.3 Divisor function

Definition. A **divisor function** is a multiplicative arithmetic function of the form

$$\sigma_\tau(n) = \sum_{d|n} d^\tau,$$

for some fixed $\tau \in \mathbb{C}$.

1.4 Multiplicative arithmetic function

Definition. An arithmetic function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ is **multiplicative** if $f(mn) = f(m)f(n)$ for all coprime integers $m, n > 0$, and is not the zero-function (in particular, $f(1) = 1$).

1.5 Abelian variety

Definition. An **abelian variety** defined over the field K is a smooth connected projective variety equipped with the structure of an algebraic group. The group law is automatically commutative.

An abelian variety of dimension 1 is the same as an elliptic curve.

1.6 Affine space

Definition. **Affine space** $\mathbb{A}^n(K)$ of dimension n over a field K is the set K^n.

If $P = (x_1, \ldots, x_n)$ is a point in $\mathbb{A}^n(K)$, the x_i are called the *affine coordinates* of P. Thus

$$\mathbb{A}^n(K) = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in K\}.$$

1.7 Base change

Definition. Let V be an algebraic variety defined over a field K. If L/K is a field extension, then any set of equations that define V over K can be used to define an algebraic variety over L, the **base change** of V from K to L (typically denoted V_L).

An algebraic variety over a field L is said to be a **base change** if it is the base change of an algebraic variety defined over a proper subfield of L, equivalently, if its base field is not a minimal field of definition.

1.8 Base field

Definition. The **base field**, of an algebraic variety is the field over which it is defined; it necessarily contains the coefficients of a set of defining equations for the variety, but it is not necessarily a minimal field of definition.

1.9 Complex multiplication

Definition. A simple abelian variety of dimension g is said to have **complex multiplication** (CM) if its endomorphism algebra is a CM field of degree $2g$, or equivalently, if its endomorphism ring is an order in a CM field of degree $2g$.

1.10 Algebraic curve

Definition. An **algebraic curve** is an algebraic variety of dimension 1.

1.11 Genus of a smooth curve

Definition. The **genus** of a smooth projective geometrically integral curve C defined over a field k is the dimension of the k-vector space of regular differentials $H^0(C, \omega_C)$. When $k = \mathbb{C}$ this coincides with the topological genus of the corresponding Riemann surface.

The quantity defined above is sometimes also called the **algebraic genus** or the **geometric genus** of C. Because of our assumption on the smoothness of C, it coincides with the **arithmetic genus** $H^1(C, \mathcal{O}_C)$.

1.12 Smoothness of an algebraic curve

Definition. Let C be an algebraic curve over a perfect field k. Then C is called **smooth** if the extension of C to the algebraic closure of k is non-singular at all of its points.

1.13 Dimension of an algebraic variety

Definition. The **dimension** of an algebraic variety V is the maximal length d of a chain

$$V_0 \subset V_1 \subset \cdots \subset V_d$$

of distinct irreducible subvarieties of V.

1.14 Endomorphism algebra

Definition. The **endomorphism algebra** of an abelian variety A is the $\mathbb{Q}$-algebra $\mathrm{End}(A) \otimes \mathbb{Q}$, where $\mathrm{End}(A)$ is the endomorphism ring of A.

1.15 Endomorphism ring

Definition. An **endomorphism** of an abelian variety A over a field k is a homomorphism $\varphi\colon A \to A$ defined over k. The set of endomorphisms of an abelian variety A can be given the structure of a ring in which addition is defined pointwise (using the group operation of A) and multiplication is composition; this ring is called the **endomorphism ring** of A, denoted $\mathrm{End}(A)$.

For endomorphisms defined over an extension of k, we instead speak about the geometric endomorphism ring.

1.16 Geometric endomorphism ring

Definition. For an abelian variety A over a field F, the **geometric endomorphism ring** of A is $\mathrm{End}(A_{\overline{F}})$, the endomorphism ring of the base change of A to an algebraic closure $\overline{F}$ of F.

1.17 Geometrically simple

Definition. An abelian variety over a field k is **geometrically (or absolutely) simple** if it is simple when viewed as a variety over $\bar{k}$.

1.18 Hyperelliptic curve

Definition. A **hyperelliptic curve** X over a field k is a smooth projective algebraic curve of genus $g \geq 2$ that admits a 2-to-1 map $X \to \mathbb{P}^1$ defined over

the algebraic closure $\bar{k}$.

If X is a hyperelliptic curve over k, then the canonical map $X \to \mathbb{P}^{g-1}$ is a 2-to-1 map onto a smooth genus 0 curve Y. The curve Y is isomorphic to $\mathbb{P}^1$ if and only if Y has a k-rational point.

If X admits a 2-to-1 map to $\mathbb{P}^1$ that is defined over k, then X has a **Weierstrass model** of the form $y^2 + h(x)y = f(x)$; when the characteristic of k is not 2 one can complete the square to put this model in the form $y^2 = f(x)$.

In general, there is always a model for X in $\mathbb{P}^3$ of the form

$$h(x, y, z) = 0 \qquad w^2 = f(x, y, z)$$

where $h(x, y, z)$ is a homogeneous polynomial of degree 2 (a **conic**) and $f(x, y, z)$ is a homogeneous polynomial of degree $g + 1$.

1.19 Irreducible variety

Definition. A variety defined over a field F is **irreducible** if it is nonempty and cannot be decomposed as the union of two strictly smaller varieties over F. It is **geometrically irreducible** if it remains irreducible when seen as a variety over the algebraic closure of F.

1.20 Jacobian of a curve

Definition. The **Jacobian** of a (smooth, projective, geometrically integral) curve X of genus g over a field k is a g-dimensional principally polarized abelian variety J that is canonically associated to X.

If X has a k-rational point, then $J(k)$ is isomorphic to the group of degree zero divisors on X modulo linear equivalence. A choice of rational point on X determines a morphism $X \to J$ called an Abel-Jacobi map; it is an embedding

if and only if $g \geq 1$, and an isomorphism if and only if $g = 1$.

The Torelli theorem states that if X and Y are curves whose Jacobians are isomorphic as *principally polarized* abelian varieties, then X and Y are isomorphic. It is possible, however, for non-isomorphic curves to have Jacobians that are isomorphic as unpolarized abelian varieties.

1.21 Minimal field of definition

Definition. Let V/k be an algebraic variety defined over a field k and let S be the set of subfields $k_0 \subseteq k$ for which there exists an algebraic variety V_0/k_0 whose base change to k is isomorphic to V.

Any field $k_0 \in S$ that contains no other elements of S is a **minimal field of definition** for V.

In general, an algebraic variety may have more than one minimal field of definition; this does not occur for elliptic curves but it does occur for curves of genus 2.

1.22 Mordell-Weil group of an abelian variety

Definition. The **Mordell-Weil group** of an abelian variety A over a number field K is its group of K-rational points $A(K)$.

Weil, building on Mordell's theorem for elliptic curves over $\mathbb{Q}$, proved that the abelian group $A(K)$ is finitely generated. Thus

$$A(K) \simeq \mathbb{Z}^r \oplus T,$$

where r is a nonnegative integer called the **Mordell-Weil rank** of A, and T is a finite abelian group called the **torsion subgroup**.

The torsion subgroup T is the product of at most $2g$ cyclic groups, where g is the dimension of A.

1.23 Projective space

Definition. Projective space $\mathbb{P}^n(K)$ of dimension n over a field K is the set $(K^{n+1} \setminus \{0\})/\sim$, where

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n) \iff x_0 = \lambda y_0, \ldots, x_n = \lambda y_n \quad \text{for some } \lambda \in K^*.$$

The equivalence class of $(x_0, x_1, \ldots, x_n)$ in $\mathbb{P}^n(K)$ is denoted by $(x_0 : x_1 : \cdots : x_n)$, and the x_i are called **homogeneous coordinates**. Thus

$$\mathbb{P}^n(K) = \{(x_0 : \cdots : x_n) \mid x_0, \ldots, x_n \in K, \text{ not all zero}\}.$$

1.24 Quotient curve

Definition. Let X be an algebraic curve and let H be a finite subgroup of its automorphism group.

The **quotient curve** X/H is the algebraic curve obtained by identifying points of X that lie in the same H-orbit (equations defining X/H as an algebraic variety of dimension one can be constructed from the equations defining X and the automorphisms in H).

The natural projection $X \to X/H$ that sends each point on X to its H-orbit is a surjective morphism

1.25 Riemann surface

Definition. A **Riemann surface** is a connected complex manifold of dimension one. Compact Riemann surfaces can be identified with smooth projective

curves over $\mathbb{C}$.

1.26 Simple

Definition. An abelian variety is **simple** if it is nonzero and not isogenous to a product of abelian varieties of lower dimension.

1.27 Non-singular point (definition)

Definition. Let V be a variety over a perfect field F. A point P of V is **non-singular** if the module of differentials of V is locally free at P. According to the Jacobian criterion, if V is defined in a neighborhood of P by affine polynomial equations $f_1(X_1, \ldots, X_n) = \ldots = f_r(X_1, \ldots, X_n) = 0$, then V is non-singular at P if the Jacobian matrix $\left(\frac{\partial f_i}{\partial X_j}\right)_{ij}$ has the same rank as the codimension of V in $\mathbb{A}^n$.

1.28 Algebraic variety

Definition. There are two main kinds of **algebraic varieties**, *affine varieties* and *projective varieties*. Both are defined as the set of common zeros of a collection of polynomials. Let K be a field with algebraic closure $\overline{K}$.

An **affine algebraic set** is a subset of affine space $\mathbb{A}^n(\overline{K})$ of the form

$$V(I) = \{P \in \mathbb{A}^n(\overline{K}) : f(P) = 0 \text{ for all } f \in I\}$$

where $I \subseteq \overline{K}[x_1, \ldots, x_n]$ is an ideal. Given an affine algebraic set V, its **defining ideal** is

$$I(V) = \{f \in \overline{K}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V\}.$$

An **affine variety** over $\overline{K}$ is an affine algebraic set whose defining ideal $I \subseteq \overline{K}[x_1, \ldots, x_n]$ is a prime ideal. An **affine variety** over K is an affine variety

over $\overline{K}$ whose defining ideal can be generated by polynomials in $K[x_1, \ldots, x_n]$.

We define projective notions similarly. A **projective algebraic set** is a subset of projective space $\mathbb{P}^n(\overline{K})$ defined by a *homogeneous* ideal $I \subseteq \overline{K}[x_1, \ldots, x_n]$. A **projective variety** over $\overline{K}$ is a projective algebraic set whose defining ideal is a homogeneous prime ideal. A **projective variety** over K is a projective variety over $\overline{K}$ whose defining ideal can be generated by homogeneous polynomials in $K[x_1, \ldots, x_n]$.

1.29 Binary operation

Definition. A **binary operation** on a set S is a function $S \times S \to S$.

If the operation is denoted by $*$, then the output of this function applied to (s_1, s_2) is typically denoted $s_1 * s_2$.

1.30 Associative binary operation

Definition. If $*$ is a binary operation on a set A, then $*$ is **associative** on A if for all $a, b, c \in A$,

$$a * (b * c) = (a * b) * c.$$

/div>

1.31 Commutative binary operation

Definition. If $*$ is a binary operation on a set A, then $*$ is **commutative** on A if for all $a, b \in A$,

$$a * b = b * a.$$

1.32 Identity for a binary operation

Definition. If $*$ is a binary operation on a set A, then A has an **identity** element with respect to $*$ if there exists $e \in A$ such that for all $a \in A$,

$$a * e = e * a = a.$$

Such an identity element e, if it exists, is unique and is thus called **the identity element** of A with respect to $*$.

1.33 Inverse for a binary operation

Definition. If $*$ is a binary operation on a set A having identity element $e \in A$, then an element $a \in A$ has an **inverse** in A with respect to $*$ if there exists $a' \in A$ such that

$$a * a' = a' * a = e.$$

1.34 Symplectic isomorphism

Definition. Let $N \geq 1$. Let μ_N be the group of Nth roots of unity in some algebraically closed field of characteristic not dividing N. Let M be a free rank 2 $\mathbb{Z}/N\mathbb{Z}$-module together with an isomorphism $\alpha\colon \bigwedge^2 M \xrightarrow{\sim} \mu_N$, or equivalently with a nondegenerate alternating pairing $M \times M \to \mu_N$. For example, M could be $E[N]$ for an elliptic curve E, together with the Weil pairing. Or M could be $\mathbb{Z}/N\mathbb{Z} \times \mu_N$ with the "determinant" pairing $(a, \gamma), (b, \delta) \mapsto \delta^a/\gamma^b$.

A **symplectic isomorphism** from M to another such structure M' is a $\mathbb{Z}/N\mathbb{Z}$-module isomorphism $M \to M'$ such that the induced isomorphism $\bigwedge^2 M \to \bigwedge^2 M'$ gets identified via α and α' with the *identity* $\mu_N \to \mu_N$.

The same definition makes sense in a context in which each free rank 2 $\mathbb{Z}/N\mathbb{Z}$-module is enriched with a Galois action to make a Galois module, or replaced

by a finite étale group scheme that is $(\mathbb{Z}/N\mathbb{Z})^2$ étale locally.

1.35 Artin representation (definition)

Definition. An **Artin representation** is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ from the absolute Galois group of $\mathbb{Q}$ to the automorphism group of a finite-dimensional $\mathbb{C}$-vector space V. Here continuity means that ρ factors through the Galois group of some finite extension $K/\mathbb{Q}$. The smallest such K is called the Artin field of ρ.

1.36 Conductor of an Artin representation

Definition. The **conductor** of an Artin representation is a positive integer that measures its ramification. It can be expressed as a product of local conductors.

Let $K/\mathbb{Q}$ be a Galois extension and $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}(V)$ an Artin representation. Then the conductor of ρ is $\prod_p p^{f(\rho,p)}$ for non-negative integers $f(\rho, p)$, where the product is taken over prime numbers p.

To define the exponents $f(\rho, p)$, fix a prime $\mathfrak{p}$ of K above p and consider the corresponding extension of local fields $K_\mathfrak{p}/\mathbb{Q}_p$ with Galois group G. Then G has a filtration of higher ramification groups in lower numbering G_i, as defined in Chapter IV of Serre's *Local Fields* [**?**, **?**]. In particular, $G_{-1} = G$, G_0 is the inertia group of $K_\mathfrak{p}/\mathbb{Q}_p$, and G_1 is the wild inertia group, which is a finite p-group.

Let $g_i = |G_i|$. Then

$$f(\rho, p) = \sum_{i \geq 0} \frac{g_i}{g_0} (\dim(V) - \dim(V^{G_i}))$$

where V^{G_i} is the subspace of V fixed by G_i.

Note that if p is unramified in K, then $f(\rho, p) = 0$ and conversely, if ρ is faithful

and p is ramified in K, then $f(\rho, p) > 0$.

1.37 Number field associated to an Artin representation

Definition. The **Artin field** is a number field associated to an Artin representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ by being the smallest Galois extension $K/\mathbb{Q}$ such that ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$.

1.38 Parity of a representation

Definition. An Artin representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ is **even** or **odd** if $\det(\rho(c))$ equals 1 or -1, respectively, where c is a complex conjugation.

1.39 Ramified prime of an Artin representation

Definition. If $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ is an Artin representation with Artin field K, then a prime p is **ramified** if it is ramified in $K/\mathbb{Q}$.

Equivalently, a prime is ramified if the inertia subgroup for a prime above p is not contained in the kernel of ρ.

1.40 Unramified prime of an Artin representation

Definition. If $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ is an Artin representation, a prime p is **unramified** if it is not ramified.

Equivalently, a prime is unramified if the inertia subgroup for a prime above p in the Artin field of ρ is contained in the kernel of ρ.

1.41 Isogeny of abelian varieties

Definition. An **isogeny** of abelian varieties is a surjective algebraic group homomorphism with finite kernel.

Two abelian varieties are **isogenous** if there is an isogeny between them. This defines an equivalence relation on the set of isomorphism classes. Equivalence classes are called isogeny classes.

1.42 Simple abelian variety

Definition. An abelian variety is **simple** if it is nonzero and not isogenous to a product of abelian varieties of lower dimension.

1.43 Tate module of an abelian variety

Definition. Let $p \in \mathbb{Z}_{\geq 0}$ be a prime and A an abelian variety of dimension g defined over a field K. The **p-adic Tate module** of A is the inverse limit

$$T_p(A) = \varprojlim_{n \in \mathbb{N}} A[p^n].$$

Here for $m \in \mathbb{Z}_{>0}$, $A[m]$ denotes the m-torsion subgroup of A, which is the kernel of the multiplication-by-m isogeny of A.

If K has characteristic not equal to p, then $T_p(A)$ is a free $\mathbb{Z}_p$-module of rank $2g$. It carries an action of the absolute Galois group of K, and thus has an associated Galois representation.

1.44 Twist of an abelian variety

Definition. A **twist** of an abelian variety A is an abelian variety A' over the same field that becomes isomorphic to A upon base change to an algebraic closure.

1.45 Dirichlet character

Definition. A **Dirichlet character** is a function $\chi : \mathbb{Z} \to \mathbb{C}$ together with a positive integer q called the **modulus** such that χ is completely multiplicative,

i.e. $\chi(mn) = \chi(m)\chi(n)$ for all integers m and n, and χ is periodic modulo q, i.e. $\chi(n+q) = \chi(n)$ for all n. If $(n,q) > 1$ then $\chi(n) = 0$, whereas if $(n,q) = 1$, then $\chi(n)$ is a root of unity. The character χ is primitive if its conductor is equal to its modulus.

1.46 Conductor of a Dirichlet character

Definition. The **conductor** of a Dirichlet character χ modulo q is the least positive integer q_1 dividing q for which $\chi(n + kq_1) = \chi(n)$ for all n and $n + kq_1$ coprime to q.

1.47 Galois orbit of a Dirichlet character

Definition. The **Galois orbit** of a Dirichlet character χ of modulus q and order n is the set $[\chi] := \{\sigma(\chi) : \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\}$, where $\sigma(\chi)$ denotes the Dirichlet character of modulus q defined by $k \mapsto \sigma(\chi(k))$. The map $\chi \to \sigma(\chi)$ defines a faithful action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ on the set of Dirichlet characters of modulus q and order n, each of which has $\mathbb{Q}(\zeta_n)$ as its field of values.

1.48 Orbit index of a Dirichlet character

Definition. The Galois orbits of Dirichlet characters of modulus q are ordered as follows. Let χ be any character in the Galois orbit $[\chi]$ and define the N-tuple of integers

$$t([\chi]) := (n, t_1, t_2, \ldots, t_{q-1}) \in \mathbb{Z}^q,$$

where n is the order of χ and $t_i := \mathrm{tr}_{\mathbb{Q}(\chi)/\mathbb{Q}}(\chi(i))$ is the trace of $\chi(i)$ from the field of values of χ to $\mathbb{Q}$. The q-tuple $t([\chi])$ is independent of the choice of representative χ and uniquely identifies the Galois orbit $[\chi]$.

The **orbit index** of χ is the index of $t([\chi])$ in the lexicographic ordering of all such tuples arising for Dirichlet characters of modulus q; indexing begins at

1, which is always the index of the Galois orbit of the principal character of modulus 1.

1.49 Label of a Galois orbit of a Dirichlet character

Definition. The **label** of a Galois orbit of a Dirichlet character χ of modulus N takes the form $N.a$, where a is a letter or string of letters representing the index of the Galois orbit. The index 1 is written as a, the index 2 is written as b, the index 27 is written as ba, and so on.

1.50 Induced Dirichlet character

Definition. A Dirichlet character χ_1 of modulus q_1 is said to be **induced** by a Dirichlet character χ_2 of modulus q_2 dividing q_1 if $\chi_1(m) = \chi_2(m)$ for all m coprime to q_1.

A Dirichlet character is primitive if it is not induced by any character other than itself; every Dirichlet character is induced by a uniquely determined primitive Dirichlet character.

1.51 Minimal Dirichlet character

Definition. A Dirichlet character χ of prime power modulus N is **minimal** if the following conditions both hold:

1. The conductor of χ does not lie in the open interval $(\sqrt{N}, N)$, and if N is a square divisible by 16 then $\mathrm{cond}(\chi) \in \{\sqrt{N}, N\}$.

2. Both the order and conductor of χ are minimal among the set of all Dirichlet character $\chi\psi^2$ for which $\mathrm{cond}(\psi)\mathrm{cond}(\chi\psi)|N$.

This includes all primitive Dirichlet characters of prime power modulus, but not every minimal Dirichlet character of prime power modulus is primitive.

For a composite modulus N with prime power factorization $N = p_1^{e_1} \cdots p_n^{e_n}$, a Dirichlet character χ of modulus N is **minimal** if and only if every character in its unique factorization into Dirichlet characters of modulus $p_1^{e_1}, \cdots, p_n^{e_n}$ is minimal. The trivial Dirichlet character is minimal.

1.52 Modulus of a Dirichlet character

Definition. A **Dirichlet character** is a function $\chi : \mathbb{Z} \to \mathbb{C}$ together with a positive integer q, called the **modulus** of the character, such that χ is completely multiplicative, i.e. $\chi(mn) = \chi(m)\chi(n)$ for all integers m and n, and χ is periodic modulo q, i.e. $\chi(n + q) = \chi(n)$ for all n. If $(n, q) > 1$ then $\chi(n) = 0$, whereas if $(n, q) = 1$, then $\chi(n)$ is a root of unity.

1.53 Order of a Dirichlet character

Definition. The **order** of a Dirichlet character χ is the least positive integer n such that χ^n is the trivial character of the same modulus as χ. Equivalently, it is the order n of the image of χ in $\mathbb{C}^\times$, the group of nth roots of unity.

1.54 Primitive Dirichlet character

Definition. A Dirichlet character χ is **primitive** if its conductor is equal to its modulus; equivalently, χ is not induced by a Dirichlet character of smaller modulus.

1.55 Principal Dirichlet character

Definition. A Dirichlet character is **principal** (or **trivial**) if it has order 1, equivalently, if it is induced by the unique Dirichlet character of modulus 1.

The value of the principal Dirichlet character of modulus q at an integer n is 1 if n is coprime to q and 0 otherwise.

1.56 Field of values of a Dirichlet character

Definition. The **field of values** of a Dirichlet character $\chi\colon \mathbb{Z} \to \mathbb{C}$ is the field $\mathbb{Q}(\chi(\mathbb{Z}))$ generated by its values; it is equal to the cyclotomic field $\mathbb{Q}(\zeta_n)$, where n is the order of χ.

1.57 Automorphism group of an algebraic curve

Definition. An **automorphism** of an algebraic curve is an isomorphism from the curve to itself. The set of automorphisms of a curve X form a group $\mathrm{Aut}(X)$ under composition; this is the **automorphism group** of the curve.

The automorphism group of a genus 2 curve necessarily includes the **hyperelliptic involution** $(x, y) \mapsto (x, -y)$, which is an automorphism of order 2; this means that the automorphism group of a genus 2 curve is never trivial.

The geometric automorphism group of a curve X/k is the automorphism group of $X_{\bar{k}}$.

1.58 Discriminant of a genus 2 curve

Definition. The discriminant Δ of a Weierstrass equation $y^2 + h(x)y = f(x)$ can be computed as

$$\Delta := \begin{cases} 2^8 \mathrm{lc}(f)^2 \mathrm{disc}(f + h^2/4) & \text{if } f + h^2/4 \text{ has odd degree,} \\ 2^8 \mathrm{disc}(f + h^2/4) & \text{if } f + h^2/4 \text{ has even degree,} \end{cases}$$

where $\mathrm{lc}(f)$ denotes the leading coefficient of f and $\mathrm{disc}(f)$ its discriminant.

The **discriminant** of a genus 2 curve over $\mathbb{Q}$ is the discriminant of a minimal equation for the curve; it is an invariant of the curve that does not depend on the choice of minimal equation.

1.59 Genus 2 curve

Definition. Every (smooth, projective, geometrically integral) curve of genus 2 can be defined by a **Weierstrass equation** of the form

$$y^2 + h(x)y = f(x)$$

with nonzero discriminant and $\deg h \leq 3$ and $\deg f \leq 6$; in order to have genus 2 we must have $\deg h = 3$ or $\deg f = 5, 6$. Over a field whose characteristic is not 2 one can complete the square to make $h(x)$ zero, but this will yield a model with bad reduction at 2 that is typically not a minimal equation for the curve.

This equation can be viewed as defining the function field of the curve, or as a smooth model of the curve in the weighted projective plane. Every curve of genus 2 admits a degree 2 cover of the projective line (consider the function x) and is therefore a hyperelliptic curve.

1.60 Primes of good reduction

Definition. A variety X over $\mathbb{Q}$ is said to have **good reduction** at a prime p if it has an integral model whose reduction modulo p defines a smooth variety of the same dimension; otherwise, p is said to be a prime of **bad reduction**.

When X is a curve, any prime of good reduction for X is also a prime of good reduction for its Jacobian, but the converse need not hold when X has genus $g > 1$.

For all of the genus 2 curves currently in the LMFDB, every prime of good reduction for the curve is also a prime of good reduction for the Jacobian of the curve.

1.61 Minimal equation of a hyperelliptic curve

Definition. Every (smooth, projective, geometrically integral) hyperelliptic curve X over $\mathbb{Q}$ of genus g can be defined by an integral Weierstrass equation

$$y^2 + h(x)y = f(x),$$

where $h(x)$ and $f(x)$ are integral polynomials of degree at most $g+1$ and $2g+2$, respectively. Each such equation has a discriminant Δ. A **minimal equation** is one for which $|\Delta|$ is minimal among all integral Weierstrass equations for the same curve. Over $\mathbb{Q}$, every hyperelliptic curve has a minimal equation. The prime divisors of Δ are the primes of bad reduction for X.

The equation $y^2 + h(x)y = f(x)$ uniquely determines a homogeneous equation of weighted degree 6 in variables x, y, z, where y has weight $g + 1$, while x and z both have weight 1: one homogenizes $h(x)$ to obtain a homogeneous polynomial $h(x, z)$ of degree $g+1$ and homogenizes $f(x)$ to obtain a homogeneous polynomial $f(x, z)$ of degree $2g + 2$. This yields a smooth projective model $y^2 + h(x, z)y = f(x, z)$ for the curve X.

One can always transform the minimal equation into a simplified equation $y^2 = g(x) = 4f(x)+h(x)^2$, but this equation need not have minimal discriminant and may have bad reduction at primes that do not divide the minimal discriminant (it will always have bad reduction at the prime 2).

1.62 Galois group

Definition. The **Galois group** of an irreducible separable polynomial of degree n can be embedded in S_n through its action on the roots of the polynomial, with the image being well-defined up to labeling of the roots. Different labelings lead to conjugate subgroups. The subgroup acts transitively on $\{1, \ldots, n\}$. Conversely, for every transitive subgroup G of S_n with $n \in \mathbb{Z}^+$, there is a field

K such that G is the Galois group of some polynomial over K.

1.63 Borel subgroup

Definition. A **Borel subgroup** of a general linear group is a subgroup that is conjugate to the group of upper triangular matrices.

The Borel subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ are maximal subgroups that fix a one-dimensional subspace of $\mathbb{F}_p^2$; every such subgroup is conjugate to the subgroup of upper triangular matrices.

Subgroup labels containing the letter **B** identify a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that lies in the Borel subgroup of upper triangular matrices but is not contained in the subgroup of diagonal matrices; these are precisely the subgroups of a Borel subgroup that contain an element of order p.

The label **B** is used for the full Borel subgroup of upper triangular matrices

The label **B.a.b** denotes the proper subgroup of **B** generated by the matrices

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & r/b \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

where a and b are minimally chosen positive integers and r is the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$, as defined in [**?**, **?**, **?**].

1.64 Cartan subgroup

Definition. Let R be a commutative ring. Given a free rank 2 étale R-algebra A equipped with a basis, any $a \in A^\times$ defines an R-linear multiplication-by-a map $A \to A$, so we get an injective homomorphism $A^\times \to \mathrm{Aut}_{R\text{-module}}(A) \simeq \mathrm{GL}_2(R)$, and the image is called a **Cartan subgroup** of $\mathrm{GL}_2(R)$. The canonical involution of the R-algebra A gives another element of $\mathrm{Aut}_{R\text{-module}}(A)$; we call

the group generated by it and the Cartan subgroup $A^\times$ the **extended Cartan subgroup**. The Cartan subgroup has index 2 in the extended Cartan subgroup.

If $R = \mathbb{F}_p$, there are two possibilities for A: the split algebra $\mathbb{F}_p \times \mathbb{F}_p$ and the nonsplit algebra $\mathbb{F}_{p^2}$; the resulting Cartan subgroups are called split and nonsplit. The extended Cartan subgroup equals the normalizer of the Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$ except when $p = 2$ and A is split. In the split case, if we use the standard basis of $\mathbb{F}_p \times \mathbb{F}_p$, the Cartan subgroup is the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$, and the extended Cartan subgroup is this together with the coset of antidiagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$.

If $R = \mathbb{Z}/p^e\mathbb{Z}$, again there are two possibilities for A: the split algebra $R \times R$, or the nonsplit algebra. The nonsplit algebra can be described as $\mathcal{O}/p^e\mathcal{O}$ where $\mathcal{O}$ is either the degree 2 unramified extension of $\mathbb{Z}_p$ or a quadratic order in which p is inert. The nonsplit algebra can also be described as the ring of length e Witt vectors $W_e(\mathbb{F}_{p^2})$.

If $R = \mathbb{Z}/N\mathbb{Z}$ for some $N \geq 1$, then A can be split or nonsplit independently at each prime dividing N.

1.65 Exceptional subgroup

Definition. An **exceptional subgroup** of $\mathrm{GL}_2(\mathbb{F}_p)$ does not contain $\mathrm{SL}_2(\mathbb{F}_p)$ and is not contained in a Borel subgroup or in the normalizer of a Cartan subgroup.

Exceptional subgroups are classified according to their image in $\mathrm{PGL}_2(\mathbb{F}_p)$, which must be isomorphic to one of the alternating groups A_4 or A_5, or to the symmetric group S_4. These groups are labelled using identifiers containing one of the strings **A4**, **A5**, **S4**, as described in [**?**, **?**].

1.66 Index of an open subgroup

Definition. The **index** of an open subgroup H of a profinite group G is the positive integer $[G : H]$.

When G is a matrix group over $\widehat{\mathbb{Z}}$ or $\mathbb{Z}_\ell$ and H is a subgroup of level N, this is the same as the index of H in the reduction of G modulo N.

1.67 Level of an open subgroup

Definition. The **level** of an open subgroup H of a matrix group G over $\widehat{\mathbb{Z}}$ is the least positive integer N for which H is equal to the inverse image of its projection to the reduction of G modulo N.

This also applies to open subgroups of matrix groups over $\mathbb{Z}_\ell$, in which case the level is necessarily a power of ℓ.

1.68 Non-split Cartan subgroup

Definition. A **non-split Cartan subgroup** of $\mathrm{GL}_2(\mathbb{F}_p)$ is a Cartan subgroup that is not diagonalizable over $\mathbb{F}_p$. Every non-split Cartan subgroup is a cyclic group isomorphic to $\mathbb{F}_{p^2}^\times$.

For $p = 2$ the label **Cn** identifies the unique index 2 subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$. For $p > 2$ the label **Cn** identifies the nonsplit Cartan subgroup consisting of matrices of the form

$$\begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix},$$

with $x, y \in \mathbb{F}_p$ not both zero and ε the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$, corresponding to $x + y\sqrt{\varepsilon} \in \mathbb{F}_{p^2}^\times$. Every non-split Cartan subgroup is conjugate to the group **Cn**.

Labels of the form **Cn.a.b** identify the proper subgroup of **Cn** generated by

the matrix

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix},$$

where a and b are minimally chosen positive integers and ε is the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$, as defined in [**?**, **?**, **?**].

1.69 Normalizer of a Cartan subgroup

Definition. For $p > 2$ the **normalizer of a Cartan subgroup** of $\mathrm{GL}_2(\mathbb{F}_p)$ is a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that contains a Cartan subgroup with index 2. It is the normalizer in $\mathrm{GL}_2(\mathbb{F}_p)$ of the Cartan subgroup it contains.

For $p = 2$ the Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_2)$ are already normal and we instead define the normalizer of a Cartan subgroup to be a group that contains a Cartan subgroup with index 2. This means that the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ has order 2 (which makes it conjugate to the Borel subgroup), while the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ has order 6 (which makes it all of $\mathrm{GL}_2(\mathbb{F}_2)$).

1.70 Normalizer of a non-split Cartan subgroup

Definition. For $p > 2$ the **normalizer of a non-split Cartan subgroup** of $\mathrm{GL}_2(\mathbb{F}_p)$ is a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that contains a non-split Cartan subgroup with index 2, and it is the normalizer in $\mathrm{GL}_2(\mathbb{F}_p)$ of the non-split Cartan subgroup it contains. For $p = 2$ the normalizer of a non-split Cartan subgroup is defined to be all of $\mathrm{GL}_2(\mathbb{F}_2)$, which contains its (already normal) non-split Cartan subgroup with index 2.

For $p > 2$ the label **Nn** identifies the normalizer of the nonsplit Cartan subgroup

generated by the non-split Cartan subgroup **Cn** and the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and every normalizer of a non-split Cartan subgroup is conjugate to the group **Nn**.

The label **Nn.a.b** denotes the proper subgroup of the normalizer of the nonsplit Cartan subgroup **Nn** generated by the matrices

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

where a and b are minimally chosen positive integers and ε is the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$, as defined in [**?**, **?**, **?**].

1.71 Normalizer of a split Cartan subgroup

Definition. The **normalizer of a split Cartan subgroup** of $\mathrm{GL}_2(\mathbb{F}_p)$ is a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that contains a split Cartan subgroup with index 2. For $p > 2$ such a group is in fact the normalizer in $\mathrm{GL}_2(\mathbb{F}_p)$ of the split Cartan subgroup it contains, but for $p = 2$ this is not the case (the split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ is already normal).

The label **Ns** identifies the subgroup generated by the split Cartan subgroup **Cs** of diagonal matrices and the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Every normalizer of a split Cartan subgroup is conjugate to the group **Ns**.

The label **Ns.a.b** identifies the proper subgroup of **Ns** generated by the matrices

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \begin{pmatrix} 0 & b \\ -r/b & 0 \end{pmatrix},$$

where a and b are minimally chosen positive integers and r is the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$.

The label **Ns.a.b.c** identifies the proper subgroup of the normalizer of the split Cartan subgroup generated by the matrices

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \begin{pmatrix} 0 & b \\ -1/b & 0 \end{pmatrix}, \begin{pmatrix} 0 & c \\ -r/c & 0 \end{pmatrix}$$

where a and b are minimally chosen positive integers and r is the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$, as defined in [**?**, **?**, **?**].

1.72 Open subgroup

Definition. An **open subgroup** H of a profinite group G is a subgroup that is open in the topology of G, which implies that it is equal to the inverse image of its projection to a a finite quotient of G.

Open subgroups of G necessarily have finite index (since G is compact), but not every finite index subgroup of G is necessarily open.

When the profinite group G is a matrix group over a ring R that is equipped with canonical projections to finite rings of the form $\mathbb{Z}/n\mathbb{Z}$ (take $R = \mathbb{Z}_\ell$ or $R = \widehat{\mathbb{Z}}$, for example), we use $G(n)$ to denote the image of G under the group homomorphism induced by the projection $R \to \mathbb{Z}/n\mathbb{Z}$. In this situation we may identify H with its projection to $G(N)$, where N is the least positive integer for which H is the inverse image of its projection to $G(N)$ (this N is the level of H).

1.73 Profinite group

Definition. A **profinite group** is a compact totally disconnected topological group. Equivalently, it is the inverse limit of a system of finite groups equipped with the discrete topology.

For example, if we take the finite groups $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ as n varies over positive integers, order them by divisibility of n and consider the inverse system equipped with reduction maps $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ for all positive integers $m|n$, then the inverse limit

$$\varprojlim_n \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

is a profinite group which is isomorphic to the group of invertible 2×2 matrices over the topological ring $\widehat{\mathbb{Z}}$, which is the inverse limit of the finite rings $\mathbb{Z}/n\mathbb{Z}$ equipped with the discrete topology.

1.74 Split Cartan subgroup

Definition. A **split Cartan subgroup** of $\mathrm{GL}_2(\mathbb{F}_p)$ is a Cartan subgroup that is diagonalizable over $\mathbb{F}_p$. Every split Cartan subgroup is conjugate to the subgroup of diagonal matrices, which is isomorphic to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$.

The label **Cs** identifies the split Cartan subgroup of diagonal matrices.

The label **Cs.a.b** identifies the proper subgroup of **Cs** generated by

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & r/b \end{pmatrix},$$

where a and b are minimally chosen positive integers and r is the least positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times$, as defined in [**?**, **?**, **?**].

1.75 Definition of group

Definition. A **group** $\langle G, * \rangle$ is a set G with a binary operation $*$ such that

1. $*$ is associative 2. $*$ has an identity element 3. every element $g \in G$ has an inverse.

1.76 Abelian group

Definition. A group is **abelian** if its operation is commutative.

1.77 Automorphisms of a group

Definition. If G is a group, an **automorphism** of G is a group isomorphism $f : G \to G$.

The set of automorphisms of G, $\mathrm{Aut}(G)$, is a group under composition.

1.78 Characteristic subgroup

Definition. A subgroup H of a group G is a **characteristic subgroup** if $\phi(H) = H$ for all automorphisms $\phi \in \mathrm{Aut}(G)$.

1.79 Coset of a subgroup

Definition. If G is a group and H is a subgroup of G, then a left **coset** of H is a set

$$gH = \{gh \mid h \in H\}$$

and similarly, a right coset of H is a set

$$Hg = \{hg \mid h \in H\}.$$

The left cosets partition G, as do the right cosets.

1.80 Frattini subgroup of a group

Definition. If G is a group, then the **Frattini subgroup** of G, denoted $\Phi(G)$, is the intersection of all maximal subgroups of G. If there are no maximal subgroups of G, then $\Phi(G) = G$.

The Frattini subgroup is always a characteristic subgroup, hence a normal subgroup, of G.

1.81 Cusps of a subgroup of the modular group

Definition. The **cusps** of a subgroup Γ of the modular group are equivalence classes of points in $\mathbb{Q} \cup \infty$ under the action of Γ by linear fractional transformation, where for

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

we define $\gamma\infty = \frac{a}{c}$ when $c \neq 0$, and $\gamma\infty = \infty$ when $c = 0$.

1.82 Width of a cusp

Definition. The **width** of the cusp ∞ for the group Γ is the smallest number w such that $T^w = \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} \in \Gamma$. Furthermore, for a general $x \in \mathbb{P}^1(\mathbb{Q})$ and $\gamma \in \Gamma$ such that $\gamma\infty = x$, we define the **width** of x for Γ to be the width of ∞ for $\gamma^{-1}\Gamma\gamma$.

Note that $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is one of the **generators** of the modular group $\mathrm{SL}_2(\mathbb{Z})$.

1.83 Fundamental domain

Definition. If $G \subseteq \Gamma$ is a subgroup of the modular group, then a closed set $F \in \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ is said to be a **fundamental domain** for G if: <ol> For any point $z \in \mathcal{H}$ there is a $g \in G$ such that $gz \in F$. If $z \neq z' \in F$ are equivalent with respect to the action of G, that is, if $z' = gz$ for some $g \in G$, then z and z' belong to ∂F, the boundary of F.

1.84 Absolute Galois group

Definition. The **absolute Galois group** of a field K is the group of all automorphisms of the algebraic closure of K that fix the field K.

1.85 Generators of a group

Definition. If G is a group and S is a subset of G, then S is a set of **generators** if the smallest subgroup of G containing S equals G.

Equivalently, S generates G if

$$G = \bigcap_{S \subseteq H \leq G} H\,.$$

The automorphism group of G acts on such S, and we say S and S' are equivalent if they are related by this action.

1.86 Haar measure of a topological group

Definition. For G a locally compact topological group, a **Haar measure** on G is a nonnegative, countably additive, real-valued measure on G which is invariant under left translation on G. Any such measure is also invariant under right translation on G.

A Haar measure always exists and is unique up to multiplication by a positive scalar. If G is compact, then the **normalized Haar measure** on G is the unique Haar measure on G under which G has total measure 1.

As a special case, if G is finite of order n, then the normalized Haar measure is the uniform measure that assigns to each element the measure $1/n$.

1.87 Group homomorphism

Definition. If G and H are groups, then a **group homomorphism** from G to H is a function

$$f : G \to H$$

such that for all $a, b \in G$, $f(a * b) = f(a) * f(b)$.

1.88 Group isomorphism

Definition. A **group isomorphism** is a group homomorphism $f : G \to H$ which is bijective.

1.89 Maximal subgroup of a group

Definition. If G is a group, a subgroup M is a **maximal subgroup** if for every subgroup H such that $M \subseteq H \subseteq G$, either $H = M$ or $H = G$.

1.90 Normal series of a group

Definition. If G is a group, a **subnormal series** for G is a chain of subgroups

$$\langle e \rangle = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$$

where each subgroup H_i is normal in H_{i+1} for all i.

A subnormal series where H_i is normal in G for all i is a **normal series**.

1.91 Order of a group

Definition. The **order** of a group is its cardinality as a set.

1.92 Presentation of a finite group

Definition. A **presentation** of a group G is a description of G as the quotient F/R of a free group F generated by a specified set of generators, modulo the normal subgroup R generated by a set of words in those generators. When G is abelian we instead express G as a quotient of a free abelian group F so that we can omit commutator relations.

In what follows, we denote by g^h the conjugate $h^{-1}gh$ and by $[g,h]$ the commutator $ghg^{-1}h^{-1}$.

We only give presentations for finite solvable groups, where they can take a special form. A **polycyclic series** is a subnormal series $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n \trianglerighteq G_{n+1} = \{1\}$ so that G_i/G_{i+1} is cyclic for each i. A **polycyclic sequence** is a sequence of elements $(g_1, \ldots, g_n)$ of G so that $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$. The **relative orders** of a polycyclic series are the orders r_i of the cyclic quotients G_i/G_{i+1}. The **polycyclic presentation** associated to a polycyclic sequence has generators $g_1, \ldots, g_n$ and relations of the following shape.

- $g_i^{r_i} = \prod_{k=i+1}^{n} g_k^{a_{i,k}}$ for all i;
- $g_i^{g_j} = \prod_{k=j+1}^{n} g_k^{b_{i,j,k}}$ for $j < i$.

Any finite solvable group has a polycyclic presentation. When the size of G is not too large, we choose a presentation with the following properties:

- it has a minimal number of generators;
- among such, it has a maximal number of i so that all $a_{i,k} = 0$;

- among such, it has a maximal number of commuting g_i;
- among such, aim for an increasing sequence of relative orders;
- among such, minimize the sum of the $b_{i,j,k}$ for noncommuting generators g_i and g_j.

1.93 Rank

Definition. The **rank** of a finite group G is the minimal number of elements required to generate it, which is often smaller than the number of generators in a polycyclic presentation. For p-groups, the rank can be computed by taking the $\mathbb{F}_p$-dimension of the quotient by the Frattini subgroup.

1.94 Modular group $\mathrm{SL}(2,\mathbb{Z})$

Definition. The **modular group** is the group of 2×2 matrices with integer coefficients and determinant 1; it is denoted by $\mathrm{SL}(2,\mathbb{Z})$ or $\mathrm{SL}_2(\mathbb{Z})$.

A standard set of generators for the modular group are the matrices:

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

1.95 Subgroup of a group

Definition. If G is a group, a subset $H \subseteq G$ is a **subgroup** of G if the binary operation of G restricts to a binary operation on H, and H is a group for this induced operation.

Equivalently, the subset H must satisfy the following conditions:

1. for all $a, b \in H$, $a * b \in H$ 2. the identity of G is an element of H 3. for every

$a \in H$, the inverse of a in G is also in H.

1.96 Index of a subgroup

Definition. The **index** of a subgroup G' of a group G, denoted $[G : G']$, is the order of the set of left cosets of G' in G.

1.97 Normal subgroup of a group

Definition. If H is a subgroup of a group G, then H is **normal** if any of the following equivalent conditions hold:

1. $gHg^{-1} = H$ for all $g \in G$ 2. $gHg^{-1} \subseteq H$ for all $g \in G$ 3. $gH = Hg$ for all $g \in G$ 4. $(aH) * (bH) = (ab)H$ is a well-defined binary operation on the set of left cosets of H

If H is a normal subgroup, we write $H \lhd G$, and the set of left cosets G/H form a group under the operation given in (4) above.

1.98 Sylow subgroup

Definition. If p is a prime and G is a finite group of order $p^n m$ where $p \nmid m$, then a **p-Sylow subgroup** of G is any subgroup of order p^n.

Sylow subgroups exist for every finite group and prime p.

1.99 Torsion group

Definition. A **torsion group** is a group in which every element has finite order.

The elements of finite order in an abelian group A form a torsion group called the **torsion subgroup** of A.

1.100 Automorphism group of a field extension

Definition. If K/F is an extension of fields, its **automorphism group** is

$$\mathrm{Aut}(K/F) = \{\sigma : K \to K \mid \forall a \in F, \sigma(a) = a, \text{ and } \sigma \text{ is an isomorphism}\}.$$

Note, a finite extension is Galois if and only if $|\mathrm{Aut}(K/F)| = [K : F]$.

1.101 Inertia group

Definition. Let

- K be a p-adic field.
- L a finite Galois extension of K.
- $\mathcal{O}_K$, $\mathcal{O}_L$ the rings of integers for K, L,
- P_K, P_L the unique maximal ideals of $\mathcal{O}_K$, $\mathcal{O}_L$, and
- $\kappa = \mathcal{O}_K/P_K$, $\lambda = \mathcal{O}_L/P_L$ the

residue fields of K, L.

Then each $\sigma \in \mathrm{Gal}(L/K)$ induces a element of $\mathrm{Gal}(\lambda/\kappa)$. The kernel of the resulting homomorphism

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(\lambda/\kappa)$$

is the **inertia group** of L/K.

1.102 Local field

Definition. A **local field** is a field K with a non-trivial absolute value $|\ |$ that is locally compact in the topology induced by the distance metric $d(x, y) := |x-y|$.

An **archimedean local field** is a local field whose absolute value is archimedean; such a field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

A **nonarchimedean local field** is a local field whose absolute value is nonarchimedean. Such a field is either isomorphic to a finite extension of $\mathbb{Q}_p$ when K has characteristic zero (in which case it is a p-adic field), or to a finite extension of $\mathbb{F}_p((t))$ when K has characteristic p. In both cases p is the characteristic of the residue field of K..

1.103 Maximal ideal of a local field

Definition. The **maximal ideal** of a nonarchimedean local field K is the unique maximal ideal of its ring of integers $\mathcal{O}_K$.

It consists of all elements of $\mathcal{O}_K$ that are not units, equivalently, all elements of K whose absolute value is strictly less than 1.

1.104 p-adic field

Definition. A **p-adic field** (or **local number field**) is a finite extension of $\mathbb{Q}_p$, equivalently, a nonarchimedean local field of characteristic zero.

1.105 Residue field

Definition. The **residue field** of a nonarchimedean local field is the quotient of its ring of integers by its unique maximal ideal.

The residue field is finite and its characteristic p is the **residue field characteristic**. Finite extensions of $\mathbb{Q}_p$ have residue field characteristic p.

1.106 Ring of integers of a local field

Definition. The **ring of integers** of a local field K with absolute value $|\ |$ is the subring $\mathcal{O}_K := \{x \in K : |x| \leq 1\}$; it is a discrete valuation ring.

1.107 Wild inertia group

Definition. The **wild inertia group** of a Galois extension $K/\mathbb{Q}_p$ is the unique p-Sylow subgroup of its inertia group.

1.108 L-function

Definition. An (analytic) **L-function** is a Dirichlet series that has an Euler product and satisfies a certain type of functional equation.

It is expected that all L-functions satisfy the Riemann Hypothesis, that all of the zeros in the critical strip are on the critical line. Selberg has defined a class $\mathcal{S}$ of Dirichlet series that satisfy the Selberg axioms. It is conjectured (but far from proven) that $\mathcal{S}$ is precisely the set of all L-functions. Selberg's axioms have not been verified for all of the L-functions in this database but are known to hold for many of them.

It is also conjectured that a precise form of the functional equation holds for every element of $\mathcal{S}$. Under this assumption the functional equation is determined by a quadruple known as the Selberg data, consisting of the degree, conductor, spectral parameters, and sign.

1.109 Analytic rank

Definition. The **analytic rank** of an L-function $L(s)$ is its order of vanishing at its central point.

When the analytic rank r is positive, the value listed in the LMFDB is typically

an upper bound that is believed to be tight (in the sense that there are known to be r zeroes located very near to the central point).

1.110 Arithmetic L-function

Definition. An L-function $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is called **arithmetic** if its Dirichlet coefficients a_n are algebraic numbers.

1.111 Central point of an L-function

Definition. The **central point** of an L-function is the point on the real axis of the critical line. Equivalently, it is the fixed point of the functional equation.

In the analytic normalization, the central point is $s = 1/2$, in the arithmetic normalization, it is $s = \frac{w+1}{2}$, where w is the weight of the L-function.

1.112 Critical line of an L-function

Definition. The **critical line** of an L-function is the line of symmetry of its functional equation.

In the analytic normalization, the functional equation relates s to $1-s$ and the critical line is the line $\Re(s) = \frac{1}{2}$.

In the arithmetic normalization, the functional equation relates s to $1 + w - s$, where w is the motivic weight. In that normalization the critical line is $\Re(s) = \frac{1+w}{2}$.

1.113 Dirichlet series

Definition. A **Dirichlet series** is a formal series of the form $F(s) = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where $a_n \in \mathbb{C}$.

1.114 Dual of an L-function

Definition. The **dual** of an L-function $L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is the complex conjugate $\bar{L}(s) = \sum_{n=1}^{\infty} \frac{\bar{a_n}}{n^s}$.

1.115 Euler product of an L-function

Definition. It is expected that the **Euler product** of an L-function of degree d and conductor N can be written as

$$L(s) = \prod_p L_p(s)$$

where for $p \nmid N$

$$L_p(s) = \prod_{n=1}^{d} \left(1 - \frac{\alpha_n(p)}{p^s}\right)^{-1} \text{ with } |\alpha_n(p)| = 1$$

and for $p \mid N$,

$$L_p(s) = \prod_{n=1}^{d_p} \left(1 - \frac{\beta_n(p)}{p^s}\right)^{-1} \text{ where } d_p < d \text{ and } |\beta_n(p)| \leq 1.$$

The functions $L_p(s)$ are called **Euler factors** (or **local factors**).

1.116 Functional equation of an L-function

Definition. All known analytic L-functions have a **functional equation** that can be written in the form

$$\Lambda(s) := N^{s/2} \prod_{j=1}^{J} \Gamma_{\mathbb{R}}(s + \mu_j) \prod_{k=1}^{K} \Gamma_{\mathbb{C}}(s + \nu_k) \cdot L(s) = \varepsilon \overline{\Lambda}(1 - s),$$

where N is an integer, $\Gamma_{\mathbb{R}}$ and $\Gamma_{\mathbb{C}}$ are defined in terms of the Γ-function, $\mathrm{Re}(\mu_j) = 0$ or 1 (assuming Selberg's eigenvalue conjecture), and $\mathrm{Re}(\nu_k)$ is a

positive integer or half-integer,

$$\sum \mu_j + 2\sum \nu_k \quad \text{is real,}$$

and ε is the sign of the functional equation. With those restrictions on the spectral parameters, the data in the functional equation is specified uniquely. The integer $d = J + 2K$ is the degree of the L-function. The integer N is the conductor (or level) of the L-function. The pair $[J, K]$ is the signature of the L-function. The parameters in the functional equation can be used to make up the 4-tuple called the Selberg data.

The axioms of the Selberg class are less restrictive than given above.

Note that the functional equation above has the central point at $s = 1/2$, and relates $s \leftrightarrow 1 - s$.

For many L-functions there is another normalization which is natural. The corresponding functional equation relates $s \leftrightarrow w+1-s$ for some positive integer w, called the motivic weight of the L-function. The central point is at $s = (w + 1)/2$, and the arithmetically normalized Dirichlet coefficients $a_n n^{w/2}$ are algebraic integers.

1.117 Gamma factors

Definition. The complex functions

$$\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2) \qquad \text{and} \qquad \Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s}\Gamma(s)$$

that appear in the functional equation of an L-function are known as **gamma factors**. Here $\Gamma(s) := \int_0^\infty e^{-t}t^{s-1}dt$ is Euler's gamma function.

The gamma factors satisfy $\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s + 1)$ and can also be viewed as "missing" factors of the Euler product of an L-function corresponding to (real

or complex) archimedean places.

1.118 Leading coefficient

Definition. The **leading coefficient** of an arithmetic L-function is the first nonzero coefficient of its Laurent series expansion at the central point.

1.119 Normalization of an L-function

Definition. In its **arithmetic normalization**, an L-function $L(s)$ of weight w has its central value at $s = \frac{w+1}{2}$ and the functional equation relates s to $1 + w - s$. For L-functions defined by an Euler product $\prod_p L_p(s)^{-1}$ where the coefficients of L_p are algebraic integers, this is the usual normalization implied by the definition.

The **analytic normalization** of an L-function is defined by $L_{an}(s) := L(s + w/2)$, where $L(s)$ is the L-function in its arithmetic normalization. This moves the central value to $s = 1/2$, and the functional equation of $L_{an}(s)$ relates s to $1 - s$.

1.120 Generalized Riemann hypothesis

Definition. The **Riemann hypothesis** is the assertion that if ρ is a zero of an analytic L-function then $\mathrm{Re}(\rho) > 0$ implies that $\mathrm{Re}(\rho) = 1/2$.

1.121 Self-dual L-function

Definition. An L-function $L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is called **self-dual** if its Dirichlet coefficients a_n are real.

1.122 Sign of the functional equation

Definition. The **sign** of the functional equation of an analytic L-function, also called the **root number**, is the complex number ε that appears in the functional equation of $\Lambda(s) = \varepsilon\overline{\Lambda}(1-s)$. The sign appears as the 4th entry in the quadruple known as the Selberg data.

1.123 Dedekind eta function

Definition. We define the **Dedekind eta function** $\eta(z)$ by the formula

$$\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n),$$

where $q = e^{2\pi iz}$.

It is related to the Discriminant modular form via the formula

$$\Delta(z) = \eta^{24}(z).$$

1.124 Upper half-plane

Definition. The **upper half-plane** $\mathcal{H}$ is the set of complex numbers whose imaginary part is positive, endowed with the topology induced from $\mathbb{C}$.

The **completed upper** half-plane $\mathcal{H}^*$ is

$$\mathcal{H}\cup\mathbb{Q}\cup\{\infty\},$$

endowed with the topology such that the disks tangent to the real line at $r\in\mathbb{Q}$ form a fundamental system of neighbourhoods of r, and strips $\{z\in\mathcal{H} \mid \operatorname{Im} z > y\}\cup\{\infty\}$, $y>0$, form a fundamental system of neighbourhoods of ∞, which should therefore be thought of as $i\infty$.

The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts properly discontinuously on $\mathcal{H}$ and $\mathcal{H}^*$ by the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d},$$

with the obvious conventions regarding ∞.

1.125 Modular curve

Definition. For each open subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, there is a **modular curve** X_H, defined as a quotient of the full modular curve $X_{\mathrm{full}}(N)$, where N is the level of H. More precisely, H is the inverse image of a subgroup $H_N \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, which acts on $X_{\mathrm{full}}(N)$ over $\mathbb{Q}$, and X_H is the quotient curve $H_N \backslash X_{\mathrm{full}}(N)$, also defined over $\mathbb{Q}$.

Like $X_{\mathrm{full}}(N)$, the curve X_H is smooth, projective, and integral, and when $\det(H) = \widehat{\mathbb{Z}}$ it is also geometrically integral, but in general it may have several geometric components, as is the case for $X_{\mathrm{full}}(N)$ when $N > 2$.

Rational points: When $-1 \in H$ the rational points of X_H consist of cusps and $\mathrm{Gal}_{\mathbb{Q}}$-stable isomorphism classes of pairs $(E, [\iota]_H)$, where E is an elliptic curve over $\mathbb{Q}$, and $[\iota]_H$ is an H-level structure on E. Such points exist precisely when the image of the adelic Galois representation $\rho_E \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is conjugate to a subgroup of H.

Complex points: The congruence subgroup $\Gamma_H := H \cap \mathrm{SL}_2(\mathbb{Z})$ acts on the completed upper half-plane $\overline{\mathfrak{h}}$; one connected component of $X_H(\mathbb{C})$ is biholomorphic to the quotient $\Gamma_H \backslash \overline{\mathfrak{h}}$.

The curve X_H can alternatively be constructed as the coarse moduli space of the stack $\mathcal{X}_H$ over $\mathbb{Q}$ defined in Deligne-Rapoport [**?**, **?**]. Both constructions of X_H can be carried out over any field of characteristic not dividing N, or even over $\mathbb{Z}[1/N]$.

1.126 Cusps of a modular curve

Definition. The **cusps** on X_H are the points whose image under the canonical morphism $j\colon X_H \to X(1) \simeq \mathbb{P}^1$ is ∞. It is only the noncuspidal points that parametrize elliptic curves (with level structure).

The **cusps** of a modular curve X_H correspond to the complement of Y_H in X_H, where Y_H is the coarse moduli stack $\mathcal{M}_H^0$ defined in [**?**, **?**].

The **rational cusps** (also called $\mathbb{Q}$**-cusps**) are the cusps fixed by $\mathrm{Gal}_{\mathbb{Q}}$.

1.127 Level structure of a modular curve

Definition. Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N, let $\pi_N\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the natural projection, and let E be an elliptic curve over a number field K.

An H**-level structure** on E is the H-orbit $[\iota]_H := \{h \circ \iota\colon h \in \pi_N(H)\}$ of an isomorphism $\iota\colon E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$.

An H-level structure on E is **rational** if it lies in a Gal_K-stable isomorphism class of pairs $(E, [\iota]_H)$, where $\sigma \in \mathrm{Gal}_K$ acts via $(E, [\iota]_H) \mapsto (E^\sigma, [\iota \circ \sigma^{-1}]_H)$. Two pairs $(E, [\iota]_H)$ and $(E', [\iota']_H)$ are isomorphic if there is an isomorphism $\phi\colon E \to E'$ that induces an isomorphism $\phi_N\colon E[N] \to E'[N]$ for which $\phi_N^*([\iota']_H) = [\iota]_H$.

If E admits a rational H-level structure $[\iota]_H$ then image of its adelic Galois representation $\rho_E\colon \mathrm{Gal}_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is conjugate to a subgroup of H and the isomorphism class of $(E, [\iota]_H)$ is a non-cuspidal K-rational point on the modular curve X_H.

When $-1 \in H$ every non-cuspidal K-rational point on X_H arises in this way. When $-1 \notin H$ this is almost true, but there may be exceptions at points with

$j(E) = 0, 1728$.

Invariants of a rational H-level structure include:

- **Cyclic N-isogeny field degree**: the minimal degree of an extension L/K over which the base change E_L admits a rational cyclic isogeny of degree N; equivalently, the index of the largest subgroup of H fixing a subgroup of $(\mathbb{Z}/N\mathbb{Z})^2$ isomorphic to $\mathbb{Z}/N\mathbb{Z}$.

- **Cyclic N-torsion field degree**: the minimal degree of an extension L/K for which E_L has a rational point of order N; equivalently, the index of the largest subgroup of H that fixes a point of order N in $(\mathbb{Z}/N\mathbb{Z})^2$.

- **N-torsion field degree** the minimal degree of an extension L/K for which $E[N] \subseteq E(L)$; this is simply the cardinality of the reduction of H to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

1.128 Modular curve $X(N)$

Definition. There are three variants of the modular curve $Y(N)$:

1. There is a functor sending each $\mathbb{Z}[1/N]$-algebra R to the set of (isomorphism classes of) pairs (E, α) such that E is an elliptic curve over R and $\alpha\colon E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ is an isomorphism of group schemes. Suppose that $N \geq 3$; then this functor is represented by a smooth affine $\mathbb{Z}[1/N]$-scheme $Y_{\mathrm{full}}(N)$, called the **full modular curve of level** N. (If $N < 3$, it is representable only by an algebraic stack, and one must take the coarse moduli space to get a scheme.) For any field k with $\operatorname{char} k \nmid N$, the set $Y_{\mathrm{full}}(N)(k)$ is the set of isomorphism classes of triples (E, P, Q) , where E is an elliptic curve over k and $P, Q \in E(k)$ form a $(\mathbb{Z}/N\mathbb{Z})$-basis of $E[N]$. The curve $Y_{\mathrm{full}}(N)_{\mathbb{Q}}$ is integral but typically has several geometric components.

2. Let $\zeta_N \in \overline{\mathbb{Q}}$ be a primitive Nth root of unity. There is a functor sending each

$\mathbb{Z}[1/N, \zeta_N]$-algebra R to the set of pairs (E, α) such that E is an elliptic curve over R and $\alpha\colon E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ is an isomorphism of group schemes such that the resulting elements $P, Q \in E[N](R)$ satisfy $e_N(P, Q) = \zeta_N$. For $N \geq 3$, this functor is represented by a smooth affine $\mathbb{Z}[1/N, \zeta_N]$-scheme $Y(N)$, called the **classical modular curve of level** N. Over any $\mathbb{Z}[1/N, \zeta_N]$-field k, the curve $Y(N)_k$ is geometrically integral.

3. There is a functor sending each $\mathbb{Z}[1/N]$-algebra R to the set of pairs (E, α) consisting of an elliptic curve E over R and a symplectic isomorphism $\alpha\colon E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mu_N$. For $N \geq 3$, this functor is represented by a smooth affine $\mathbb{Z}[1/N]$-scheme $Y_{\mathrm{arith}}(N)$. Over any field k with $\operatorname{char} k \nmid N$, the curve $Y_{\mathrm{arith}}(N)_k$ is geometrically integral.

- Relationships*: Over any $\mathbb{Z}[1/N, \zeta]$-field k, the curve $Y_{\mathrm{arith}}(N)_k$ is isomorphic to $Y(N)_k$ and to a connected component of $Y_{\mathrm{full}}(N)_k$.
- Complex points*: The group $\Gamma(N)$ acts on the upper half-plane $\mathfrak{h}$, and the quotient $\Gamma(N)\backslash\mathfrak{h}$ is biholomorphic to $Y(N)(\mathbb{C}) \simeq Y_{\mathrm{arith}}(\mathbb{C})$ (choosing $\zeta_N \in \mathbb{C}$).
- Compactifications*: For each variant, there is a corresponding smooth projective model, denoted $X_{\mathrm{full}}(N)$, $X(N)$, or $X_{\mathrm{arith}}(N)$.
- Quotients*: For each open subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, there is a quotient X_H of $X_{\mathrm{full}}(N)$.

1.129 Definition of ring

Definition. A **ring** is a set R with two binary operations $+$ and $\cdot$ such that

1. R is an abelian group with respect to $+$ 2. $\cdot$ is associative on R 3. the

distributive laws hold, i.e., for all $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{and} \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

4. there is an identity element with respect to the operation $\cdot$, typically denoted by 1_R or, more simply, by 1.

The identity element of R as a group with respect to $+$ is typically denoted by 0_R or, more simply, by 0.

The ring R is a **commutative ring** if R is a ring such that the operation $\cdot$ is commutative on R.

We say that R is a **rng** (also called **ring without identity**) if conditions 1-3 (but not necessarily 4) are satisfied.

1.130 A-field

Definition. Let A be a commutative ring. An **A-field** is an A-algebra that is a field.

1.131 Characteristic of a ring

Definition. The **characteristic** of a ring is the least positive integer n for which

$$\underbrace{1 + \cdots + 1}_{n} = 0,$$

if such an n exists, and 0 otherwise. Equivalently, it is the exponent of the additive group of the ring.

The characteristic of a field k is either 0 or a prime number p, depending on whether the prime field of k is isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$.

1.132 Dedekind domain

Definition. A **Dedekind domain** D is a integral domain which is not a field such that

1. D is Noetherian; 2. every non-zero prime ideal is maximal; 3. D is integrally closed.

The ring of integers of a number field is always a Dedekind domain, as is every discrete valuation ring.

In a Dedekind domain, every non-zero ideal I can be written as a product of non-zero prime ideals,

$$I = P_1 P_2 \cdots P_k,$$

and the product is unique up to the order of the factors. Repeated factors are often grouped, so we write $I = Q_1^{e_1} \cdots Q_g^{e_g}$ where the Q_i are non-zero prime ideals of D.

In addition, every fractional ideal I is invertible in the sense that there exists a fractional ideal J such that $IJ = D$.

1.133 Field

Definition. A **field** is a commutative ring R such that $0_R \neq 1_R$ and every nonzero element of R has an inverse in R with respect to multiplication.

1.134 Field of fractions of an integral domain

Definition. If R is an integral domain, then its **field of fractions** F is the smallest field containing R.

It can be constructed by mimicking the set of fractions a/b where $a, b \in R$ with $b \neq 0$ following the usual rules for fraction arithmetic. It is unique, up to unique

isomorphism.

1.135 Fractional ideal

Definition. If R is an integral domain with field of fractions K, then a **fractional ideal** I of R is an R-submodule of K such that there exists $d \in R - \{0\}$ with

$$dI = \{da \mid a \in I\} \subseteq R\,.$$

1.136 Ideal of a ring

Definition. If R is a ring, a subset $I \subseteq R$ is an **ideal** of R if I is a subgroup of R for $+$ and for all $a \in I$ and all $r \in R$,

$$r \cdot a \in I \qquad \text{and} \qquad a \cdot r \in I.$$

In a polynomial ring $R[X_1, \ldots, X_n]$, an ideal is **homogeneous** if it can be generated by homogeneous polynomials.

1.137 Integral element of a ring

Definition. If $R \subseteq S$ are commutative rings, an element $s \in S$ is **integral** over R if there exists $n \in \mathbb{Z}^+$ and $a_i \in R$ such that

$$s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0\,.$$

The **integral closure** of R in S is $\{s \in S \mid s \text{ is integral over } R\}$.

1.138 Integral domain

Definition. An **integral domain** is a commutative ring R such that $1_R \neq 0_R$ and R contains no zero divisors.

1.139 Integrally closed

Definition. Let R be an integral domain and F its field of fractions. Then R is **integrally closed** if R equals the integral closure of R in F.

1.140 Irreducible element

Definition. An element $x \neq 0$ of a commutative ring R is **irreducible** if it is not a unit and has the property that whenever $x = yz$ for some $y, z \in R$, either y or z is a unit.

1.141 Maximal ideal

Definition. In a ring R, an ideal M is **maximal** if $M \neq R$ and for all ideals I of R,

$$M \subseteq I \subseteq R \implies M = I \quad \text{or} \quad I = R.$$

1.142 Noetherian ring

Definition. A commutative ring R is **Noetherian** if for every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

there exists N such that for all $n \geq N$, $I_n = I_N$.

1.143 Prime ideal

Definition. If R is a commutative ring R, an ideal I is **prime** if for all $a, b \in R$,

$$ab \in I \implies a \in I \quad \text{or} \quad b \in I.$$

1.144 Principal fractional ideal

Definition. Let R be an integral domain with field of fractions K. If $a \in K^\times$, then the **principal fractional ideal** generated by a is the set

$$\{ar \mid r \in R\}.$$

1.145 Unit in a ring

Definition. A **unit** in a commutative ring R is an element $x \in R$ so that there exists $y \in R$ with $xy = 1$. The set of units in R is denoted R^* or $R^\times$ and forms a group under multiplication.

1.146 Zero divisor

Definition. An element a in a ring R is a **zero divisor** if $a \neq 0_R$ and there exists an element $b \in R - \{0_R\}$ such that

$$a \cdot b = 0_R \qquad \text{or} \qquad b \cdot a = 0_R.$$

1.147 Euler gamma function

Definition. The **(Euler) gamma function** $\Gamma(z)$ is defined by the integral

$$\Gamma(z) = \int_0^\infty e^{-t} t^z \frac{dt}{t}$$

for $\mathrm{Re}(z) > 0$. It satisfies the functional equation

$$\Gamma(z+1) = z\Gamma(z),$$

and can thus be continued into a meromorphic function on the complex plane, whose poles are at the non-positive integers $\{0, -1, -2, \ldots\}$.

1.148 Sato-Tate group

Definition. The **Sato-Tate group** of a motive X is a compact Lie group G containing (as a dense subset) the image of a representation that maps Frobenius elements to conjugacy classes. When X is an Artin motive, G corresponds to the image of the Artin representation; when X is an abelian variety over a number field, one can define G in terms of an ℓ-adic Galois representation attached to X.

For motives of even weight w and degree d, the Sato-Tate group is a compact subgroup of the orthogonal group $\mathrm{O}(d)$. For motives of odd weight w and even degree d, the Sato-Tate group is a compact subgroup of the unitary symplectic group $\mathrm{USp}(d)$. For motives X arising as abelian varieties, the weight is always $w = 1$ and the the degree is $d = 2g$, where g is the dimension of the variety.

The simplest case is when X is an elliptic curve $E/\mathbb{Q}$, in which case G is either $\mathrm{SU}(2) = \mathrm{USp}(2)$ (the generic case), or G is $N(\mathrm{U}(1))$, the normalizer of the subgroup $\mathrm{U}(1)$ of diagonal matrices in $\mathrm{SU}(2)$, which contains $\mathrm{U}(1)$ with index 2.

The generalized Sato-Tate conjecture states that when ordered by norm, the sequence of images of Frobenius elements under this representation is equidistributed with respect to the pushforward of the Haar measure of G onto its set of conjugacy classes. This is known for all elliptic curves over totally real number fields (including $\mathbb{Q}$) or CM fields.

1.149 Symplectic form

Definition. A **symplectic form** on a vector space V over a field k is a non-degenerate alternating bilinear form $\omega\colon V \times V \to k$. This means that

- if $\omega(u, v) = 0$ for all $v \in V$ then $u = 0$ (non-degenerate);
- $\omega(v, v) = 0$ for all $v \in V$ (alternating);
- $\omega(\lambda u + v, w) = \lambda\omega(u, v) + \omega(v, w)$ and $\omega(u, \lambda v + w) = \omega(u) + \lambda\omega(v, w)$ for all $\lambda \in k$, $u, v, w \in V$ (bilinear).

A finite dimensional vector space admitting a symplectic form ω necessarily has even dimension $2n$, and in this case ω can be represented by a matrix $\Omega \in k^{2n\times 2n}$ that satisfies $u^\intercal \Omega v = \omega(u, w)$ for all $u, v \in V$. One can always choose a basis for V so that

$$\Omega = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix},$$

where I_n denotes the $n \times n$ identity matrix.

1.150 Unitary symplectic group

Definition. For a positive even integer d the **unitary symplectic group** $\mathrm{USp}(d)$ is the group of unitary transformations of a d-dimensional $\mathbb{C}$-vector space equipped with a symplectic form Ω. In other words, the subgroup of $\mathrm{GL}_d(\mathbb{C})$ whose elements A satisfy:

- $A^{-1} = \bar{A}^\intercal$ (unitary);
- $A^\intercal \Omega A = \Omega$ (symplectic).

It is a compact real Lie group that can also be viewed as the intersection of $\mathrm{U}(d)$ and $\mathrm{Sp}(d, \mathbb{C})$ in $\mathrm{GL}_d(\mathbb{C})$.

2 Number fields

2.1 Number field

Definition. A **number field** is a finite degree field extension of the field $\mathbb{Q}$ of rational numbers. In LMFDB, number fields are identified by a label.

2.2 Abelian number field

Definition. A number field K is **abelian** if it is Galois over $\mathbb{Q}$ and its Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian.

2.3 Absolute discriminant of a number field

Definition. The **absolute discriminant** of a number field is the absolute value of its discriminant.

2.4 Absolute value of a field

Definition. An **absolute value** of a field k is a function $|\ | : k \to \mathbb{R}_{\geq 0}$ that satisfies:

- $|x| = 0$ if and only if $x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$.

Absolute values that satisfy the stronger condition $|x + y| \leq \max(|x|, |y|)$ are **nonarchimedean**, while those that do not are **archimedean**; the latter arise only in fields of characteristic zero. The **trivial absolute value** assigns 1 to every nonzero element of k; it is a nonarchimedean absolute value.

Absolute values $|\ |_1$ and $|\ |_2$ are **equivalent** if there exists a positive real number

c such that $|x|_1 = |x|_2^c$ for all $x \in k$; this defines an equivalence relation on the set of absolute values of k.

2.5 Arithmetically equivalent fields

Definition. Two number fields are **arithmetically equivalent** if they have the same Dedekind ζ-functions. Arithmetically equivalent fields share many invariants, such as their degrees, signatures, discriminants, and Galois groups. For a given field, the existence of an arithmetically equivalent sibling depends only on the Galois group.

2.6 Class number of a number field

Definition. The **class number** of a number field K is the order of the ideal class group of K.

2.7 Analytic class number formula

Definition. If K is a number field with signature (r_1, r_2), discriminant D, regulator R, class number h, containing w roots of unity, and Dedekind ζ-function ζ_K, then ζ_K has a meromorphic continuation to the whole complex plane with a single pole at $s = 1$, which is of order 1. The **analytic class number formula** gives the residue at this pole:

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot R \cdot h}{w \cdot \sqrt{|D|}}.$$

2.8 CM number field

Definition. A **CM field** is a totally complex quadratic extension of a totally real number field.

2.9 Complex embedding

Definition. A **complex embedding** of a number field K is a nonzero field homomorphism $K \to \mathbb{C}$ whose image is not contained in $\mathbb{R}$.

A single number field may have several distinct complex embeddings.

For $K = \mathbb{Q}(a)$ where a is an algebraic number with minimal polynomial $f(X)$, the embeddings $\iota : K \to \mathbb{C}$ are determined by the value $z = \iota(a)$ which is one of the complex roots of $f(X)$, and the embedding is complex when $z \notin \mathbb{R}$. The complex embeddings come in conjugate pairs.

2.10 Conductor of an abelian number field

Definition. If a number field K is abelian, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some positive integer n. The minimum such n is the **conductor** of K.

2.11 Defining Polynomial of a Number Field

Definition. A **defining polynomial** of a number field K is an irreducible polynomial $f \in \mathbb{Q}[x]$ such that $K \cong \mathbb{Q}(a)$, where a is a root of $f(x)$. Equivalently, it is a polynomial $f \in \mathbb{Q}[x]$ such that $K \cong \mathbb{Q}[x]/(f)$.

A root $a \in K$ of the defining polynomial is a generator of K.

2.12 Degree of a number field

Definition. The **degree** of a number field K is its degree as an extension of the rational field $\mathbb{Q}$, i.e., the dimension of K as a $\mathbb{Q}$-vector space. The degree of $K/\mathbb{Q}$ is written $[K : \mathbb{Q}]$.

2.13 Dirichlet group of an Abelian number field

Definition. If K is an abelian number field, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some positive integer n. Take the minimal such n, i.e., the conductor of K.

The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is canonically isomorphic to $\mathbb{Z}_n^\times$. The Dirichlet characters modulo n form the dual group of homomorphisms $\chi : \mathbb{Z}_n^\times \to \mathbb{C}^\times$. Since $\mathrm{Gal}(K/\mathbb{Q})$ is a quotient group of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, its dual group is a subgroup of the group of Dirichlet characters modulo n, called the **Dirichlet character group** of K.

2.14 Discriminant of a number field

Definition. The **discriminant** of a number field K is the square of the determinant of the matrix

$$\begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix}$$

where $\sigma_1, ..., \sigma_n$ are the embeddings of K into the complex numbers $\mathbb{C}$, and $\{\beta_1, \ldots, \beta_n\}$ is an integral basis for the ring of integers of K.

The discriminant of K is a non-zero integer divisible exactly by the primes which ramify in K.

2.15 Discriminant root field

Definition. If K/F is a finite algebraic extension, it can be defined by a polynomial $f(x) \in F[x]$. The polynomial discriminant, $\mathrm{disc}(f)$, is well-defined up a factor of a non-zero square. The **discriminant root field** of the extension is $F(\sqrt{\mathrm{disc}(f)})$, which is well-defined.

If $n = [K : F]$, then the Galois group G for K/F is a subgroup of S_n, well-defined up to conjugation. The discriminant root field can alternatively be described as

the fixed field of $G \cap A_n$.

2.16 Embedding of a number field

Definition. An **embedding** of a number field K is a field homomorphism $K \to \mathbb{C}$. A number field of degree n has n distinct embeddings, which may be distinguished as real or complex depending on whether the image of the embedding is contained in $\mathbb{R}$ or not.

Complex embeddings necessarily come in conjugate pairs. The signature of a number field is determined by the number of real embeddings and the number of pairs of conjugate complex embeddings.

For $K = \mathbb{Q}(a)$, where a is an algebraic number with minimal polynomial $f(X)$, each embedding ι is uniquely determined by the value $z = \iota(a)$, which is one of the complex roots of $f(X)$. The embedding is real if $z \in \mathbb{R}$ and complex if $z \notin \mathbb{R}$.

2.17 Frobenius cycle types

Definition. If K is a degree n extension of $\mathbb{Q}$, $\hat{K}$ its normal closure and $G = \mathrm{Gal}(\hat{K}/\mathbb{Q})$, then G acts on the set of n embeddings of $K \to \hat{K}$ giving an embedding $G \to S_n$. Let $\mathcal{O}_K$ be the ring of integers of K and p a prime number. Then

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_g^{e_g}$$

where the P_i are distinct prime ideals of $\mathcal{O}_K$. The prime p is **unramified** if $e_i = 1$ for all i.

Suppose hereafter that p is unramified. For each P_i, there is a unique element of G that fixes P_i and acts on the quotient $\mathcal{O}_K/P_i$ via the Frobenius automorphism $x \mapsto x^p$; this element is the **Frobenius element** associated to P_i. The Frobenius elements associated to the different P_i are conjugate to each other,

so their images in S_n all have the same lengths of cycles in their disjoint cycle decompositions. This is the **Frobenius cycle type** of p.

Alternatively, for each prime P_i, its **residue degree** f_i is defined by $|\mathcal{O}_K/P_i| = p^{f_i}$. The list of f_i is the same partition of n as the cycle decomposition described above.

2.18 Fundamental units of a number field

Definition. A minimal set of generators of a maximal torsion-free subgroup of the unit group of a number field K is called a set of **fundamental units** for K.

2.19 Galois closure of an extension

Definition. If K is a separable algebraic extension of a field F, then its **Galois closure** is the smallest extension field, in terms of inclusion, which contains K and is Galois over F. If $K = F(\alpha)$ where α has irreducible polynomial f over F, then the Galois closure of K is the splitting field of f over F.

2.20 Galois group

Definition. Let K be a finite degree n separable extension of a field F, and K^{gal} be its Galois (or normal) closure. The **Galois group** for K/F is the automorphism group $\mathrm{Aut}(K^{gal}/F)$.

This automorphism group acts on the n embeddings $K \hookrightarrow K^{gal}$ via composition. As a result, we get an injection $\mathrm{Aut}(K^{gal}/F) \hookrightarrow S_n$, which is well-defined up to the labelling of the n embeddings, which corresponds to being well-defined up to conjugation in S_n.

We use the notation $\mathrm{Gal}(K/F)$ for $\mathrm{Aut}(K/F)$ when $K = K^{gal}$.

There is a naming convention for Galois groups up to degree 47.

2.21 Galois root discriminant

Definition. The **Galois root discriminant** of a number field is the root discriminant of its Galois closure.

2.22 Generator of a number field

Definition. A **generator** of a number field K is an element $a \in K$ such that $K = \mathbb{Q}(a)$. The minimal polynomial of a generator is a defining polynomial for K.

2.23 Ideal class group of a number field

Definition. The **ideal class group** of a number field K with ring of integers O_K is the group of equivalence classes of ideals, given by the quotient of the multiplicative group of all fractional ideals of O_K by the subgroup of principal fractional ideals.

Since K is a number field, the ideal class group of K is a finite abelian group, and so has the structure of a product of cyclic groups encoded by a finite list $[a_1, \ldots, a_n]$, where the a_i are positive integers with $a_i \mid a_{i+1}$ for $1 \leq i < n$.

2.24 Ideal labels

Definition. In the LMFDB ideals in rings of integers of number fields are identified using the labeling system developed by John Cremona, Aurel Page and Andrew Sutherland [**?**].

In a number field K, each nonzero ideal I of its ring of integers $\mathcal{O}_K$ is assigned an **ideal label** of the form `N.i`, where N and i are positive integers, in which $N := [\mathcal{O}_K : I]$ is the norm of the ideal and i is the index of the ideal in a sorted

list of all ideals of norm N. Once an integral primitive element α for the field K is fixed, the ordering of ideals of the same norm is defined in a deterministic fashion (involving no arbitrary choices).

In the LMFDB we always represent number fields as $K = \mathbb{Q}[X]/(g(X))$ where g is the unique monic integral polynomial which satisfies the polredabs condition. In this representation the image of X under the quotient map $\mathbb{Q}[X] \to \mathbb{Q}[X]/(g(X))$ is a canonical integral primitive element α for K. Fixing this element determines a unique ordering of all $\mathcal{O}_K$-ideals of the same norm.

2.25 Inessential prime

Definition. An **inessential prime** of a number field is a prime divisor of its index.

2.26 Integral elements

Definition. An element of a number field K is **integral** if it is integral over $\mathbb{Z}$.

2.27 Integral basis of a number field

Definition. An **integral basis** of a number field K is a $\mathbb{Z}$-basis for the ring of integers of K. This is also a $\mathbb{Q}$-basis for K.

2.28 Intermediate fields

Definition. For a number field K, **intermediate fields** F are fields with $\mathbb{Q} \subsetneqq F \subsetneqq K$.

2.29 Is a Galois extension

Definition. Let F be a subfield of K,

$$\mathrm{Aut}(K/F) = \{\sigma : K \to K \mid \sigma(a) = a \text{ for all } a \in F \text{ and } \sigma \text{ is a ring homomorphism}\},$$

and

$$K^{\mathrm{Aut}(K/F)} = \{a \in K \mid \sigma(a) = a\}.$$

Then K is **Galois** over F if $K^{\mathrm{Aut}(K/F)} = F$.

2.30 Local algebra

Definition. Given a global number field K and a prime p, the **local algebra** for K is $K \otimes \mathbb{Q}_p$. This is a finite separable algebra over $\mathbb{Q}_p$ which is isomorphic to a finite direct product of finite extension fields of $\mathbb{Q}_p$.

2.31 Maximal CM subfield

Definition. The **maximal CM subfield** of a number field is the largest subfield by degree which is a CM field.

2.32 Minimal polynomial

Definition. The **minimal polynomial** of an element a in a number field K is the unique monic polynomial $f(X) \in \mathbb{Q}[X]$ of minimal degree such that $f(a) = 0$. It is necessarily irreducible over $\mathbb{Q}$.

2.33 Minimal sibling

Definition. The **minimal sibling** of a number field is a sibling that is minimal with respect to the following quantities considered in order:

- its degree

- the T-number of its Galois group
- the absolute value of its discriminant
- the vector $(a_0, a_1, \ldots, a_{n-1})$ of coefficients of its normalized defining polynomial

$x^n + a_{n-1}x^{n-1} + \cdots + a_0$

2.34 Monogenic field

Definition. A number field K is **monogenic** if its ring of integers $\mathcal{O}_K$ equals $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$.

2.35 Monomial order

Definition. A **monomial order** in a number field K is an order of the form $\mathbb{Z}[\alpha]$, where α is an element of K. The element α is necessarily both an algebraic integer and a primitive element for K.

2.36 Narrow class group

Definition. The **narrow class group** (also called the **strict class group**) of a number field K is the group of equivalence classes of ideals, given by the quotient of the multiplicative group of all fractional ideals of K by the subgroup of principal fractional ideals which have a totally positive generator. It is a finite abelian group whose order is the narrow class number.

2.37 Narrow class number

Definition. The **narrow class number** (also called the **strict class number**) of an algebraic number field is the order of its narrow class group. Since the ordinary ideal class group is a quotient of the narrow class group, the narrow

class number is a multiple of the class number. Moreover, the ratio is a power of 2. The two class numbers are the same in many cases, for example when the number field is totally complex.

2.38 Number field nicknames

Definition. The LMFDB supports **nicknames**, short human-readable names for various fields. Examples include:

- Q, for the rationals $\mathbb{Q}$
- Qi, for $\mathbb{Q}(i)$
- QsqrtN, for $\mathbb{Q}(\sqrt{N})$, as in Qsqrt-5 for $\mathbb{Q}(\sqrt{-5})$
- QzetaN, for $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive Nth root of unity.

2.39 Order

Definition. An **order** in a number field K is a subring of K which is also a lattice in K. Every order in K is contained in the ring of integers of K, which is itself an order in K; for this reason, the ring of integers is sometimes called the *maximal order*.

Example: $\mathbb{Z}[\sqrt{5}]$ is an order in $K = \mathbb{Q}(\sqrt{5})$. However, it is not maximal, since the maximal order (i.e. ring of integers) of K is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

2.40 p-adic completion of a number field

Definition. Let K be a number field, $\mathcal{O}_K$ its ring of integers, $\mathfrak{P}$ a non-zero prime ideal of $\mathcal{O}_K$, and $p \in \mathbb{Z} \cap \mathfrak{P}$. There are a couple of ways to construct $K_{\mathfrak{P}}$, the **p-adic completion of K at $\mathfrak{P}$**.

First, we can take the inverse limit

$$\lim_{\leftarrow} \mathcal{O}_K/\mathfrak{P}^n$$

which is an integral domain. Its field of fractions is $K_{\mathfrak{P}}$.

Second, since $\mathcal{O}_K$ is a Dedekind domain, if $\alpha \in K^*$ the fractional ideal

$$\langle \alpha \rangle = \prod_{\mathfrak{Q}} \mathfrak{Q}^{e_{\mathfrak{Q}}}$$

where the product is over all non-zero prime ideals $\mathfrak{Q}$, all $e_{\mathfrak{Q}} \in \mathbb{Z}$, and all but finitely many $e_{\mathfrak{Q}} = 0$. Then we define $v_{\mathfrak{P}}(\alpha) = e_{\mathfrak{P}}$, and then the metric d on K by $d(\alpha, \beta) = p^{-v_{\mathfrak{P}}(\alpha-\beta)}$ if $\alpha \neq \beta$ and $d(\alpha, \alpha) = 0$. Then the completion of K with respect to this metric is $K_{\mathfrak{P}}$.

If $K = \mathbb{Q}(a)$, and $f \in \mathbb{Q}[x]$ is the monic irreducible polynomial for a over $\mathbb{Q}$, then adjoining the roots of f to $\mathbb{Q}_p$ provide another means of constructing the completions.

Finally, the local algebra of K, $\prod_{j=1}^{g} K_j$ is a product of the p-adic completions of K. The p-adic completions of K correspond to the nonarchimedian places of K.

2.41 Place of a number field

Definition. A **place** v of a field K is an equivalence class of non-trivial absolute values on K. As with absolute values, places may be classified as archimedean or nonarchimedean, since these properties are preserved under equivalence.

Each place induces a distance metric that gives K a metric topology. The **completion** K_v of K at v is the completion of this metric space, which is also a topological field.

When K is a number field each nonarchimedean place arises from the valuation associated to each prime ideal in the ring of integers of K, while archimedean places arise from embeddings of K into the complex numbers: each real embedding determines a **real place**, and each conjugate pair of complex embeddings determines a **complex place**. The archimedean places of a number field are also called **infinite places**.

2.42 Canonical defining polynomial for number fields

Definition. Every number field K can be represented as $K = \mathbb{Q}[X]/P(x)$ for some monic $P \in \mathbb{Z}[X]$, called a **defining polynomial** for K. Among all such defining polynomials, we define the **reduced defining polynomial** as follows.

Recall that for a monic polynomial $P(x) = \prod_i (x - \alpha_i)$, the T_2 norm of P is $T_2(P) = \sum_i |\alpha_i|^2$.

- Let L_0 be the list of (monic integral) defining polynomials for K that are minimal with respect to the T_2 norm.
- Let L_1 be the sublist of L_0 of polynomials whose discriminant has minimal absolute value.
- For a polynomial $P = x^n + a_1 x^{n-1} + \cdots + a_n$, let $S(P) = (|a_1|, a_1, \ldots, |a_n|, a_n)$, and order the polynomials in L_1 by the lexicographic order of the vectors $S(P)$.

Then the reduced defining polynomial of K is the first polynomial in L_1 with respect to this order.

The pari/gp function <code>polredabs()</code> computes reduced defining polynomials, which are also commonly called <code>polredabs</code> polynomials.

2.43 Discriminant of polynomial

Definition. The **discriminant** of a monic polynomial $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ is the quantity

$$\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

If f has integral coefficients, K is the number field defined by f and α is a root of f in K, then the discriminant D of K divides Δ and the ratio Δ/D is the square of the index of $\mathbb{Z}[\alpha]$ in the ring of integers of K.

2.44 Prime of a number field

Definition. A **prime** $\mathfrak{p}$ of a number field K is a nonzero prime ideal of its ring of integers $\mathcal{O}_K$.

The ideal $\mathfrak{p} \cap \mathcal{O}_K$ is a nonzero prime ideal of $\mathbb{Z}$ (a prime of $\mathbb{Q}$), which is necessarily a principal ideal (p) for some prime number p. The prime $\mathfrak{p}$ is then said to be a **prime above** p.

2.45 Ramified (rational) prime of a number field

Definition. A prime integer p is a **ramified prime** of a number field K if, when the ideal generated by p is factored into prime ideals in the ring of integers $\mathcal{O}_K$ of K,

$$p\mathcal{O}_K = {\mathcal{P}_\infty}^{e_1} \cdots {\mathcal{P}_\parallel}^{e_k},$$

there is an i such that $e_i \geq 2$.

The ramified primes of K are the primes dividing the discriminant of K.

2.46 Rank of a number field

Definition. The **rank** of a number field K is the size of any set of fundamental units of K. It is equal to $r = r_1 + r_2 - 1$ where r_1 is the number of real

embeddings of K into $\mathbb{C}$ and $2r_2$ is the number of complex embeddings of K into $\mathbb{C}$.

2.47 Real embedding

Definition. A **real embedding** of a number field K is a field homomorphism $K \to \mathbb{R}$. A single number field may have several distinct real embeddings.

2.48 Reflex field

Definition. Let K be a CM number field and let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. A subset $\Phi \subset \mathrm{Hom}(K, \overline{\mathbb{Q}})$ is called a **CM type** if for every embedding $\iota \in \mathrm{Hom}(K, \overline{\mathbb{Q}})$ either $\iota \in \Phi$ or $\bar{\iota} \in \Phi$, but not both, where $\bar{\iota}$ is the complex conjugate of ι.

Given a CM field K and a CM type Φ, the **reflex field** is the fixed field inside $\overline{\mathbb{Q}}$ corresponding to the subgroup $\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \rho\Phi = \Phi\}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A CM type Φ and its complement $\overline{\Phi}$, which is the same as the set of complex conjugate embeddings, have the same reflex field. The number of complex conjugate pairs of CM types is 2^{g-1}, where $2g = [K : \mathbb{Q}]$, the degree of K over $\mathbb{Q}$.

To specify a CM type Φ for the CM field $K = \mathbb{Q}(a)$: <ol> fix an order $(\iota_1, \overline{\iota_1}), \ldots, (\iota_g, \overline{\iota_g})$ of the pairs of complex embeddings of K; then $\Phi = (\varphi_1, \ldots, \varphi_g)$ where $\varphi_j \in \{\iota_j, \overline{\iota_j}\}$ for $1 \le j \le g$; now Φ can be encoded by the list $(\mathrm{sign}(\mathrm{im}(\varphi_1(a))), \ldots, \mathrm{sign}(\mathrm{im}(\varphi_g(a))))$.

The CM types in the LMFDB are grouped in Galois orbits under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ described above.

<!— (commented out by John Cremona: this information should be in the completeness knowl for number fields) In the LMFDB, there is a potentially incomplete list of reflex fields for each CM field K of degree at most 12. For each reflex field, it is indicated for how many of the $2^{[K:\mathbb{Q}]/2-1}$ pairs of complementary

CM types this particular field is the reflex field. The only reflex fields listed are those of degree at most 36.

- –>

2.49 Reflex field of the reflex field

Definition. Let K be a CM number field and let N a normal closure of K, let $\Phi \subset \mathrm{Hom}(K, \overline{\mathbb{Q}})$ be a CM type and L its associated reflex field. Then Φ induces a CM type $\Phi_N \subset \mathrm{Hom}(N, \mathbb{C})$ by taking the maps that restrict to a map inside Φ on K. The maps in Φ_N are isomorphisms on the image F of N inside $\overline{\mathbb{Q}}$ and by inverting them, we obtain a CM type on F with values in N. The **reflex field of the reflex field** is the reflex field of this CM type.

It can also be computed as follows. Consider the right action of $\mathrm{Gal}(N/K)$ on the set of CM types on K. Then the reflex field of the reflex field is the subfield corresponding to the subgroup stabilising Φ.

The reflex field of the reflex field is also the smallest field of definition of the CM type Φ, i.e. it is the largest subfield M of K such that Φ is induced from a CM type on M.

2.50 Regulator of a number field

Definition. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of a number field K into the complex numbers $\mathbb{C}$, and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ be complex embeddings of K into $\mathbb{C}$ such that no two are complex conjugate. Let $u_1, \ldots, u_r$ be a set of fundamental units of K. Then $r = r_1 + r_2 - 1$.

Let M be the $(r_1 + r_2 - 1) \times (r_1 + r_2)$ matrix $(d_j \log \sigma_j(u_i))$, where $d_j = 1$ if $j \leq r_1$, i.e, if σ_j is a real embedding, and $d_j = 2$ otherwise, i.e., if σ_j is a complex embedding. The sum of the columns of M is the zero vector.

The **regulator** of K is the absolute value of the determinant of the sub-matrix of M where one column is removed. Its value is independent of the choice of column which is removed.

2.51 Relative class number of a CM field

Definition. If K is a number field with CM with class number h, and K^+ is its maximal totally real subfield with class number h^+, then h^+ divides h and the **relative class number** is h/h^+.

2.52 Ring of integers of a number field

Definition. The **ring of integers** of a number field K is the integral closure of $\mathbb{Z}$ in K.

2.53 Root discriminant of a number field

Definition. If K is a number field of degree n and discriminant D, then the **root discriminant** of K is

$$\mathrm{rd}(K) = |D|^{1/n}.$$

It gives a measure of the discriminant of a number field which is normalized for the degree. For example, if $K \subseteq L$ are number fields and L/K is unramified, then $\mathrm{rd}(K) = \mathrm{rd}(L)$.

2.54 Separable extension

Definition. If K/F is a finite degree field extension, $\alpha \in K$ is **separable** over F if its monic irreducible polynomial has distinct roots in the algebraic closure $\overline{F}$.

The extension K/F is **separable** if every $\alpha \in K$ is separable over F.

All algebraic extensions of local and global number fields are separable.

2.55 Separable algebra

Definition. A (finite) **separable algebra** A over a field F, also called an **étale F-algebra**, is an F-algebra of finite dimension that is isomorphic to a product of separable field extensions of F.

If L/K is a field extension and A is a separable K-algebra then $A \otimes_K L$ is a separable L-algebra (which is typically not a field, even when A is).

2.56 Serre Odlyzko bound

Definition. For each positive integer n, let C_n for the minimum root discriminant for all number fields of degree n. Assuming the Generalized Riemann Hypothesis, $\limsup C_n \geq \Omega$ where

$$\Omega = 8\pi e^{\gamma} \approx 44.7632\ldots$$

and γ is the Euler–Mascheroni constant. Lower bounds for the C_n were deduced by analytic methods through the work of Odlyzko and others. In particular, Serre introduced the constant Ω which we refer to as the **Serre Odlyzko bound**,

Consequently, any number field whose root discriminant lies below Ω can be considered to have small discriminant.

2.57 Sibling fields and algebras

Definition. Two finite separable extension fields K_1 and K_2 of a ground field F are called **siblings** if they are not isomorphic, but have isomorphic Galois closures.

A finite dimensional separable $\mathbb{Q}$-algebra is isomorphic to a product of number fields. By its Galois closure, we mean the compositum of the Galois closures of the constituent fields. Then two algebras are **siblings** if they have isomorphic Galois closures, but are not isomorphic as $\mathbb{Q}$-algebras.

2.58 Signature of a number field

Definition. The **signature** of a number field K is the pair $[r_1, r_2]$ where r_1 is the number of real embeddings of K and r_2 is the number of conjugate pairs of complex embeddings.

The degree of K is $r_1 + 2r_2$.

2.59 Stem field for a Galois extension

Definition. If K/F is a Galois extension of fields, a **stem field** for K/F is a field E such that $F \subseteq E \subseteq K$ and K is the Galois closure of E/F.

This is connected to the notion of the stem field of a polynomial. If $f \in F[x]$ is a separable irreducible polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ (in some extension field), then the fields $F(\alpha_i)$ are the **stem fields of the polynomial** f. The splitting field of f is $K = F(\alpha_1, \ldots, \alpha_n)$, which is a Galois extension of F, and the fields $F(\alpha_i)$ are stem fields for K/F as defined above.

2.60 Unit group torsion

Definition. A **torsion generator** of a number field is a primitive root of unity that generates the torsion subgroup of the unit group (which is necessarily cyclic).

2.61 Totally imaginary

Definition. A number field K is **totally imaginary** (or **totally complex**) if it cannot be embedded in the real numbers $\mathbb{R}$; equivalently, $\mathbb{R}$ does not contain the image of any of the homomorphisms from K to $\mathbb{C}$.

2.62 Totally positive

Definition. An element α in a number field K is **totally positive** if $\sigma(\alpha) > 0$ for all real embeddings σ of K into $\mathbb{R}$.

2.63 Totally real

Definition. A global number field K is always of the form $K = \mathbb{Q}(\alpha)$ where α has monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$. The field is **totally real** if all of the roots of $f(x)$ in $\mathbb{C}$ lie in the real numbers $\mathbb{R}$.

Equivalently, K is totally real if all the embeddings of K into $\mathbb{C}$ have image contained in $\mathbb{R}$.

2.64 Unit group of a number field

Definition. The **unit group** of a number field K is the group of units of the ring of integers of K. It is a finitely generated abelian group with cyclic torsion subgroup. A set of generators of a maximal torsion-free subgroup is called a set of fundamental units for K.

The unit group of K has as invariants the rank and the regulator of K.

2.65 Unramified (rational) prime of a number field

Definition. A **unramified (rational) prime** of a number field K is a prime integer p such that the ideal generated by p is factored into distinct prime ideals

in the ring of integers $\mathcal{O}_K$ of K

$$p\mathcal{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_k.$$

The unramified primes of K are the primes which do not divide the discriminant of K.

2.66 Weil height

Definition. The (**logarithmic**) **Weil height** of a nonzero rational number $a/b \in \mathbb{Q}$ in lowest terms is the quantity

$$h(a/b) = \log \max\bigl\{|a|, |b|\bigr\}.$$

The height of 0 is taken to be 0.

The (**absolute logarithmic**) **Weil height** of an element α in a number field K is the quantity

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\bigl\{\|\alpha\|_v, 1\bigr\},$$

where M_K is an appropriately normalized set of inequivalent absolute values on K. More generally, the height of a point $P = [\alpha_0, \alpha_1, \ldots, \alpha_n]$ in projective space $\mathbb{P}^n(K)$ is given by

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max_{0 \le i \le n} \bigl\{\|\alpha_i\|_v\bigr\}.$$

If $\mathcal{L}$ is a very amply line bundle on a projective variety V inducing an embedding $\iota \colon V \hookrightarrow \mathbb{P}^n$, then the Weil height associated on X associated to $\mathcal{L}$ is given by

$$h_{\mathcal{L}}(P) = h(\iota(P)).$$

This definition can be extended to all line bundles by using the following linearity:

$$h_{\mathcal{L}_1 \otimes \mathcal{L}_2}(P) = h_{\mathcal{L}_1}(P) + h_{\mathcal{L}_2}(P).$$

2.67 Weil polynomial

Definition. For a prime power q, a **Weil q-polynomial** is a monic polynomial with integer coefficients whose complex roots are of absolute value $\sqrt{q}$.

Given q and a nonnegative integer d, there are only finitely many Weil q-polynomials of degree d.

The characteristic polynomial of an abelian variety over $\mathbb{F}_q$ is a Weil q-polynomial, but it is not quite true that every Weil q-polynomial arises in this way. Every irreducible Weil q-polynomial has a unique power that is the characteristic polynomial of a simple abelian variety over $\mathbb{F}_q$; it is the products of these powers that arise from abelian varieties.

2.68 Index of a number field

Definition. If K is a number field with ring of integers $\mathcal{O}_K$, then for all $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$, the index of α, $i(\alpha)$ is the index of the order $\mathbb{Z}[\alpha]$.

The **index of the number field** is the greatest common divisor of all $i(\alpha)$ with α as above.

3 Elliptic curves

3.1 Elliptic curve over a field

Definition. An **elliptic curve** E over a field k is a smooth projective curve of genus 1 together with a distinguished k-rational point O.

The most commonly used model for elliptic curves is a Weierstrass model: a smooth plane cubic with the point O as the unique point at infinity.

3.2 Additive reduction

Definition. An elliptic curve E defined over a number field K is said to have **additive reduction** at a prime $\mathfrak{p}$ of K if the reduction of E modulo $\mathfrak{p}$ has a cuspidal singularity.

3.3 Analytic order of Ш

Definition. The **Tate-Shafarevich group** Ш of an elliptic curve E defined over a number field K is a torsion abelian group, which can be defined in terms of Galois cohomology as

$$Ш(E) := \ker\left(H^1(G_K, E) \to \prod_v H^1(G_{K_v}, E_{K_v})\right),$$

where v runs over all places of K (finite and infinite), K_v is the completion of K at v, E_{K_v} is the base change of E to K_v, and G_K and G_{K_v} denote absolute Galois groups.

The group Ш is conjectured to be finite, and its order appears in the strong form of the Birch-Swinnerton-Dyer Conjecture for E. The order implied by the conjecture is called the **analytic order of Sha** and can be defined as the real number

$$Ш_{\mathrm{an}} := |D_K|^{1/2} \cdot \frac{L^{(r)}(E,1)}{r!} \cdot \frac{\#E(K)_{\mathrm{tor}}^2}{\mathrm{Reg}_{\mathrm{NT}}(E/K)} \cdot \frac{1}{\Omega(E/K) \cdot \prod_{\mathfrak{p}} c_{\mathfrak{p}}}.$$

Here D_K is the discriminant of K, $L(E,s)$ is the L-function of E/K, r is the analytic rank of E/K, $\mathrm{Reg}_{\mathrm{NT}}(E/K)$ is the Néron-Tate (un-normalised) regulator of E/K, $E(K)_{\mathrm{tor}}$ is the torsion subgroup of the Mordell-Weil group $E(K)$, $\Omega(E/K)$ is the global period of E/K, and $c_{\mathfrak{p}}$ is the Tamagawa number of E at

the prime $\mathfrak{p}$ of K.

It is known that if Ш is finite then its order is a square, so one expects the real number $Ш_{an}$ to always be a square integer.

For elliptic curves defined over $\mathbb{Q}$ of rank 0 or 1, it is a theorem that Ш_{an} is a positive rational number, and this rational number can in principle be computed exactly. This exact computation has only been carried out for the curves in the database with rank 0. For curves of rank 2 and above, there is no such theorem, and the values computed are floating point approximate values which are very close to integers. In the LMFDB we store and display the rounded values in this case.

3.4 Bad reduction of an elliptic curve at a prime

Definition. An elliptic curve E defined over a number field K is said to have **bad reduction** at a prime $\mathfrak{p}$ of K if the reduction of E modulo $\mathfrak{p}$ is singular. There are three types of bad reduction:

- split multiplicative,
- non-split multiplicative,
- additive.

A curve has bad reduction at $\mathfrak{p}$ if and only if $\mathfrak{p}$ divides its discriminant.

3.5 Base change

Definition. If E is an elliptic curve defined over a field K, and L is an extension field of K, then the same equation defining E as an elliptic curve over K also defines a curve over L called the **base change** of E from K to L. Any curve defined over L which is isomorphic to E over L is called a base-change curve

from K to L. A sufficient but not necessary condition for a curve to be a base change is that the coefficients of its Weierstrass equation lie in K.

When $K = \mathbb{Q}$ and L is a number field, elliptic curves over L which are base-changes of curves over $\mathbb{Q}$ may simply be called base-change curves. A necessary, but not sufficient, condition for this is that the j-invariant of E should be in $\mathbb{Q}$.

3.6 Birch Swinnerton-Dyer conjecture

Definition. The **Birch and Swinnerton-Dyer** conjecture (**BSD**) is one of the Millennium Prize Problems listed by the Clay Mathematics Institute. It relates the order of vanishing (or analytic rank) and the leading coefficient of the L-function associated to an elliptic curve E defined over a number field K at the central point $s = 1$ to certain arithmetic data, the **BSD invariants** of E.

- The *weak form* of the BSD conjecture states just that the analytic rank r_{an} (that is, the order of vanishing of vanishing of $L(E, s)$ at $s = 1$), is equal to the rank r of E/K.
- The *strong form* of the conjecture states that $r = r_{an}$ and also that the leading coefficient of the L-function is given by the formula

$$\frac{1}{r!}L^{(r)}(E,1) = \frac{1}{|d_K|^{1/2}} \cdot \frac{\#Ш(E/K) \cdot \Omega(E/K) \cdot \mathrm{Reg}_{\mathrm{NT}}(E/K) \cdot \prod_{\mathfrak{p}} c_{\mathfrak{p}}}{\#E(K)^2_{\mathrm{tor}}}.$$

The quantities appearing in this formula are as follows:

- d_K is the discriminant of K;
- r is the rank of $E(K)$;
- $Ш(E/K)$ is the Tate-Shafarevich group

of E/K;

- $\mathrm{Reg}(E/K)$ is the regulator of E/K;
- $\Omega(E/K)$ is the global period of E/K;
- $c_{\mathfrak{p}}$ is the Tamagawa number of E at each prime $\mathfrak{p}$ of K;
- $E(K)_{\mathrm{tor}}$ is the torsion subgroup of $E(K)$.

Implicit in the strong form of the conjecture is that the Tate-Sharafevich group $Ш(E/K)$ is finite.

There is a similar conjecture for abelian varieties over number fields.

3.7 Canonical height on an elliptic curve

Definition. Let E be an elliptic curve defined over a number field K. The **canonical height** on E is a function

$$\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$$

defined on the Mordell-Weil group $E(K)$ which induces a positive definite quadratic form on $E(K) \otimes \mathbb{R}$.

One definition of $\hat{h}(P)$ is

$$\hat{h}(P) = \lim_{n \to \infty} n^{-2} h\big(x(nP)\big),$$

where $h(x)$ is the Weil height of $x \in K$. This definition gives the non-normalised height. A normalised height which is invariant under base-change is given by

$$\frac{1}{[K : \mathbb{Q}]} \hat{h}(P).$$

Related to the canonical height is the **height pairing**

$$\langle -, - \rangle : E(K) \times E(K) \to \mathbb{R}$$

defined by $\langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$, which is a positive definite quadratic form on $E(K) \otimes \mathbb{R}$, used in defining the regulator of E/K.

3.8 Complex multiplication

Definition. An elliptic curve whose endomorphism ring is larger than $\mathbb{Z}$ is said to have **complex multiplication** (often abbreviated to CM). In this case, for curves defined over fields of characteristic zero, the endomorphism ring is isomorphic to an order in an imaginary quadratic field. The discriminant of this order is the **CM discriminant**.

An elliptic curve whose geometric endomorphism ring is larger than $\mathbb{Z}$ is said to have **potential complex multiplication** (potential CM). In the literature, these too are often called CM elliptic curves.

The property of having potential CM depends only on the j-invariant of the curve. In characteristic 0, CM j-invariants are algebraic integers, and there are only finitely many in any given number field. There are precisely 13 CM j-invariants in $\mathbb{Q}$ (all integers), associated to the 13 imaginary quadratic orders of class number 1:

j	-12288000	54000	0	287496	1728	16581375	-3375	8000	-32768	-884736
CM discriminant	-27	-12	-3	-16	-4	-28	-7	-8	-11	-19

CM elliptic curves are examples of CM abelian varieties.

3.9 Conductor of an elliptic curve

Definition. The **conductor** of an elliptic curve E defined over a number field K is an ideal of the ring of integers of K that is divisible by the prime ideals of bad reduction and no others. It is defined as

$$\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$$

where the exponent $e_{\mathfrak{p}}$ is as follows:

- $e_{\mathfrak{p}} = 0$ if E has good reduction at $\mathfrak{p}$;
- $e_{\mathfrak{p}} = 1$ if E has multiplicative reduction at $\mathfrak{p}$;
- $e_{\mathfrak{p}} = 2$ if E has additive reduction at $\mathfrak{p}$ and $\mathfrak{p}$ does not lie above either 2 or 3; and
- $2 \leq e_{\mathfrak{p}} \leq 2 + 6v_{\mathfrak{p}}(2) + 3v_{\mathfrak{p}}(3)$, where $v_{\mathfrak{p}}$ is the valuation at $\mathfrak{p}$, if E has additive reduction and $\mathfrak{p}$ lies above 2 or 3.

For $\mathfrak{p} = 2$ and 3, there is an algorithm of Tate that simultaneously creates a minimal Weierstrass equation and computes the exponent of the conductor. See:

<UL> <LI> J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 33-52. <EM>Lecture Notes in Math.</EM>, Vol. <B>476</B>, Springer, Berlin, 1975.

<LI> J.H. Silverman, <EM>Advanced topics in the arithmetic of elliptic curves</EM>, GTM <B>151</B>, Springer-Verlag, New York, 1994.

</UL>

The **conductor norm** is the norm $[\mathcal{O}_K : \mathfrak{n}]$ of the ideal $\mathfrak{n}$.

3.10 Discriminant of a Weierstrass equation

Definition. The **discriminant** Δ of a Weierstrass equation over a field K is an element of K defined in terms of the Weierstrass coefficients. If the Weierstrass equation is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then Δ is given by a polynomial expression in $a_1, \ldots, a_6$, namely,

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where

$$b_2 = a_1^2 + 4a_2$$
$$b_4 = 2a_4 + a_1a_3$$
$$b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Then $\Delta \neq 0$ if and only if the equation defines a smooth curve, in which case its projective closure gives an elliptic curve.

3.11 Endomorphism of an elliptic curve

Definition. An **endomorphism** of an elliptic curve defined over a field K is a homomorphism $\varphi\colon E \to E$ defined over K. The set of all endomorphisms of E forms a ring called the endomorphism ring of E, denoted $\mathrm{End}(E)$, a special case of the endomorphism ring of an abelian variety.

3.12 Endomorphism ring of an elliptic curve

Definition. The **endomorphism ring** $\mathrm{End}(E)$ of an elliptic curve E over a field K is the ring of all endomorphisms of E defined over K. For endomorphisms defined over extensions, we speak of the geometric endomorphism ring of E.

For elliptic curves defined over fields of characteristic zero, this ring is isomorphic to $\mathbb{Z}$, unless the curve has complex multiplication (CM) defined over the ground field, in which case the endomorphism ring is an order in an imaginary quadratic field; for curves defined over $\mathbb{Q}$, this order is one of the 13 orders of class number one.

$\mathrm{End}(E)$ always contains a subring isomorphic to $\mathbb{Z}$, since for $m \in \mathbb{Z}$ there is the multiplication-by-m map $[m]\colon E \to E$.

This is a special case of the endomorphism ring of an abelian variety.

3.13 Galois representations attached to an elliptic curve

Definition. If E is an elliptic curve defined over a field K and m is a positive integer, then the **mod-m Galois representation** attached to E is the continuous homomorphism

$$\overline{\rho}_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m])$$

describing the action of the absolute Galois group of K on the m-torsion subgroup $E[m]$.

When the characteristic of K does not divide $m > 1$, we may identify the finite abelian group $E[m]$ with $(\mathbb{Z}/m\mathbb{Z})^2$ and hence view the representation as a map

$$\overline{\rho}_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Z}/m\mathbb{Z})$$

defined up to conjugation. In particular, when $m = \ell$ is a prime different from the characteristic of K, we have the **mod-ℓ Galois representation**

$$\overline{\rho}_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Z}/\ell\mathbb{Z}).$$

Taking the inverse limit over prime powers $m = \ell^n$ yields the **ℓ-adic Galois representation** attached to E,

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}(2, \mathbb{Z}_\ell),$$

which describes the action of the absolute Galois group of K on $T_\ell(E)$, the ℓ-adic Tate module of E.

When K has characteristic zero one can take the inverse limit over all positive integers m (ordered by divisibility) to obtain the **adelic Galois representation**

$$\rho_E : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \hat{\mathbb{Z}}).$$

If E is an elliptic curve without complex multiplication that is defined over a number field, then the image of ρ_E is an open subgroup of $\mathrm{GL}(2, \hat{\mathbb{Z}})$ that has an associated level, index, and genus.

3.14 Image of the adelic Galois representation

Definition. The image of the adelic Galois representation associate to an elliptic curve E over a number field K that does not have potential complex multiplication is an open subgroup H of $\mathrm{GL}(2, \widehat{\mathbb{Z}})$. The subgroup H has the following invariants:

- The **level** of H is the least positive integer N such that H is the full inverse image of its projection to $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.
- The **index** of H is the positive integer $[\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) : H]$.

- The **genus** of H is the genus of the corresponding modular curve X_H.

3.15 Image of mod-ℓ Galois representation

Definition. Let ℓ be a prime and let E be an elliptic curve defined over a number field K.

Subgroups G of $\mathrm{GL}(2,\mathbb{F}_\ell)$ that can arise as the image of the mod-ℓ Galois representation

$$\bar{\rho}_{E,\ell}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{F}_\ell)$$

attached to E that do not contain $\mathrm{SL}(2,\mathbb{F}_\ell)$ are identified using the labels introduced by Sutherland in [**?**, **?**]. For groups with surjective determinant map (necessarily the case when $K=\mathbb{Q}$), these labels have the form

`LS.a.b.c`,

where `L` is the prime ℓ, `S` is one of **G**, **B**, **Cs**, **Cn**, **Ns**, **Nn**, **A4**, **S4**, **A5**, and `a`, `b`, `c` are optional positive integers. When the determinant map is not surjective the label has `"[d]"`, where d is the index of the determinant image in $\mathbb{F}_\ell^\times$.

When $\bar{\rho}_{E,\ell}$ does not contain $\mathrm{SL}(2,\mathbb{F}_\ell)$ the possibilities for `S` are: Borel **B**, split Cartan **Cs**, normalizer of the split Cartan **Ns**, nonsplit Cartan **Cn**, normalizer of the nonsplit Cartan **Nn**, exceptional **A4**, **S4**, **A5**. The cases **A4** and **A5** cannot occur when $K=\mathbb{Q}$.

3.16 Geometric endomorphism ring

Definition. The **geometric endomorphism ring** of an elliptic curve E over a field K is $\mathrm{End}(E_{\overline{K}})$, the endomorphism ring of the base change of E to an algebraic closure $\overline{K}$ of K.

This is a special case of the geometric endomorphism ring of an abelian variety.

3.17 Global minimal model

Definition. A **global minimal model** for an elliptic curve E defined over a number field K is a Weierstrass equation for E which is integral and is a local minimal model at all primes of K.

When K has class number 1 all elliptic curves over K have global minimal models. In general, there is an obstruction to the existence of a global minimal model for each elliptic curve E defined over K, which is an ideal class of K. In case this class is nontrivial for E, there is a semi-global minimal model for E, which is minimal at all primes except one, the ideal class of that one prime being the obstruction class.

3.18 Good ordinary reduction

Definition. An elliptic curve E defined over a number field K is said to have **ordinary reduction** at a prime $\mathfrak{p}$ of K if the reduction $E_\mathfrak{p}$ of E modulo $\mathfrak{p}$ is smooth, and $E_\mathfrak{p}$ is ordinary.

An elliptic curve $E_\mathfrak{p}$ defined over a finite field of characteristic p is **ordinary** if $E_\mathfrak{p}(\overline{\mathbb{F}_p})$ has nontrivial p-torsion.

3.19 Good reduction

Definition. An elliptic curve E defined over a number field K is said to have **good reduction** at a prime $\mathfrak{p}$ of K if the reduction of E modulo $\mathfrak{p}$ is smooth.

If E has good reduction at every prime of K then E is said to have **everywhere good reduction**.

3.20 Good supersingular reduction

Definition. An elliptic curve E defined over a number field K is said to have **supersingular reduction** at a prime $\mathfrak{p}$ of K if the reduction $E_{\mathfrak{p}}$ of E modulo $\mathfrak{p}$ is smooth, and $E_{\mathfrak{p}}$ is supersingular.

An elliptic curve $E_{\mathfrak{p}}$ defined over a finite field of characteristic p is **supersingular** if $E_{\mathfrak{p}}(\overline{\mathbb{F}_p})$ has no p-torsion.

3.21 Integral model

Definition. An **integral model** for an elliptic curve E defined over a number field K is a Weierstrass equation for E all of whose coefficients are in the ring of integers of K.

3.22 Elliptic curve invariants

Definition. The invariants of an elliptic curve E over a number field K are its

- conductor, $\mathfrak{N}$, which is an integral ideal of K whose norm is the **conductor norm** $N(\mathfrak{N})$
- minimal discriminant, $\mathfrak{D}$, also an integral ideal of K, whose norm is the **minimal discriminant norm** $N(\mathfrak{D})$
- j-invariant, j
- endomorphism ring, $\mathrm{End}(E)$
- Sato-Tate group, $\mathrm{ST}(E)$

Each Weierstrass model for E also has a discriminant, Δ, and discriminant norm, $N(\Delta)$, which are not strictly invariants of E since different models have, in general, different discriminants.

3.23 Isogeny between elliptic curves

Definition. Let E_1 and E_2 be two elliptic curves defined over a field K. An **isogeny** (over K) between E_1 and E_2 is a non-constant morphism $f\colon E_1 \to E_2$ defined over K, i.e., a morphism of curves given by rational functions with coefficients in K, such that $f(O_{E_1}) = O_{E_2}$. Elliptic curves E_1 and E_2 are called **isogenous** if there exists an isogeny $f\colon E_1 \to E_2$.

An isogeny respects the group laws on E_1 and E_2, and hence determines a group homomorphism $E_1(L) \to E_2(L)$ for any extension L of K. The kernel is a finite group, defined over K; in general the points in the kernel are not individually defined over K but over a finite Galois extension of K and are permuted by the Galois action.

The **degree** of an isogeny is its degree as a morphism of algebraic curves. For a separable isogeny this is equal to the cardinality of the kernel. Over a field of characteristic 0 such as a number field, all isogenies are separable. In finite characteristic p, isogenies of degree coprime to p are all separable.

An isogeny is **cyclic** if its kernel is a cyclic group. Every isogeny is the composition of a cyclic isogeny with the multiplication-by-m map for some $m \geq 1$.

Isogeny is an equivalence relation, and the equivalence classes are called **isogeny classes**. Over a number field, it is a consequence of a theorem of Shafarevich that isogeny classes are finite. Between any two curves in an isogeny class there is a unique degree of cyclic isogeny between them, except when the curves have additional endomorphisms defined over the base field of the curves; in that case there are cyclic isogenies of infinitely many different degrees between any two isogenous curves.

Isogenies from an elliptic curve E to itself are called **endomorphisms**. The set of all endomrpshisms of E forms a ring under pointwise addition and composition, the endomorphism ring of E.

An isogeny of elliptic curves is a special case of an isogeny of abelian varieties.

3.24 Isogeny class of an elliptic curve

Definition. The **isogeny class (over a field K)** of an elliptic curve E defined over K is the set of all isomorphism classes of elliptic curves defined over K that are isogenous to E over K. Over a number field K this is always a finite set; over $\mathbb{Q}$, it has at most 8 elements by a theorem of Kenku [**?**, **?**].

3.25 Isogeny class degree

Definition. The **isogeny class degree** of an isogeny class of elliptic curves is the least common multiple of the degrees of all rational cyclic isogenies between elliptic curves in the isogeny class.

3.26 Isogeny graph of an isogeny class of elliptic curves

Definition. The **isogeny graph** of an isogeny class of elliptic curves is the graph whose vertices are the isomorphism classes (over the base field) of elliptic curves in the isogeny class and whose edges are the isogenies of prime degree between the curves representing the vertices.

The vertices of the isogeny graphs in the LMFDB are labeled by the final entry of the LMFDB label of the corresponding (isomorphism classes of) elliptic curves. Their edges, of which there may be several between any two given vertices, are labeled by the prime that is the degree of the corresponding isogeny.

3.27 Isogeny matrix of an isogeny class of elliptic curves

Definition. The **isogeny matrix** of an isogeny class of elliptic curves is a symmetric matrix with integral entries that records the minimum among the degrees of the cyclic isogenies between the elliptic curves in the isogeny class.

In the LMFDB, the rows and columns of the matrices are ordered by the final entry of the label of the elliptic curves in the isogeny class in question, so that the (i, j)-th entry is the smallest possible degree of a cyclic isogeny between the i-th and j-th curve in the isogeny class.

3.28 Isomorphism of elliptic curves

Definition. An **isomorphism** between two elliptic curves E, E' defined over a field K is an isogeny $f : E \to E'$ such that there exist an isogeny $g : E' \to E$ with the compositions $g \circ f$ and $f \circ g$ being the identity maps. Equivalently, an isomorphism $E \to E'$ is an isogeny of degree 1.

Isomorphism is an equivalence relation, the equivalnce classes being called **isomorphism classes**.

When E and E' are defined by Weierstrass models, such an isomorphism is uniquely represented as a Weierstrass isomorphism between these models.

3.29 j-invariant of an elliptic curve

Definition. The **j-invariant** of an elliptic curve E defined over a field K is an invariant of the isomorphism class of E over $\overline{K}$. If the Weierstrass equation of E is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then its j-invariant is given by

$$j = \frac{c_4^3}{\Delta}$$

where

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = 2a_4 + a_1 a_3$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

$$c_4 = b_2^2 - 24 b_4$$

and

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9 b_2 b_4 b_6$$

is the discriminant of E.

3.30 Kodaira symbol

Definition. The **Kodaira symbol** of an elliptic curve E defined over a number field encodes the reduction type of E at a prime $\mathfrak{p}$ of K. It describes the combinatorics of the special fiber of the Né;ron model of the elliptic curve. The Né;ron model is obtained from the local minimal model for E at $\mathfrak{p}$ using Tate's algorithm. For an exact definition and properties, consult a text on elliptic curves.

3.31 Local data of an elliptic curve

Definition. The **local data** of an elliptic curve E defined over a number field K at a prime $\mathfrak{p}$ of K consists of

- the Tamagawa number $c_{\mathfrak{p}}$
- the Kodaira symbol
- the reduction type
- the local root number

- the conductor valuation $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{N})$
- the discriminant_valuation $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{D})$
- the j-invariant denominator valuation $\mathrm{ord}_{\mathfrak{p}}(j)_-$

3.32 Local minimal discriminant of an elliptic curve

Definition. Let E be an elliptic curve defined over a number field K, and $\mathfrak{p}$ a prime of K. The **local minimal discriminant** of E is the ideal $\mathfrak{p}^e$ where e is is the valuation of the discriminant of a local minimal model for E at $\mathfrak{p}$.

3.33 Local minimal model

Definition. A **local minimal model** for an elliptic curve E defined over a number field K at a prime $\mathfrak{p}$ of K is a Weierstrass equation for E all of whose coefficients are integral at $\mathfrak{p}$, and whose discriminant has minimal valuation at $\mathfrak{p}$ among all such equations.

3.34 Maximal ℓ-adic Galois representation

Definition. Let E be an elliptic curve over a number field K, let ℓ be prime, and let

$$\rho_{E,\ell}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[\ell^\infty]) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$$

be the ℓ-adic Galois representation associated to E.

If E does not have potential complex multiplication, then $\rho_{E,\ell}$ is **maximal** if its image contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

In general, let $\mathcal{O}$ be the geometric endomorphism ring of E. Then $E[\ell^\infty]$ is an $\mathcal{O}$-module, and we view $\mathrm{Aut}_{\mathcal{O}}(E[\ell^\infty])$ as a subgroup of $\mathrm{Aut}(E[\ell^\infty]) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$ that contains the image of $\rho_{E,\ell}$ whenever K contains $\mathcal{O}$. We say that $\rho_{E,\ell}$ is **maximal** if its image contains $\mathrm{SL}_2(\mathbb{Z}_\ell) \cap \mathrm{Aut}_{\mathcal{O}}(E[\ell^\infty])$, in which case we call ℓ

a **maximal prime** for E.

3.35 Maximal Galois representation

Definition. Let E be an elliptic curve over a number field K, let ℓ be prime, and let

$$\bar{\rho}_{E,\ell}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

be the mod-ℓ Galois representation associated to E.

If E does not have potential complex multiplication, then $\bar{\rho}_{E,\ell}$ is **maximal** if its image contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.

In general, let $\mathcal{O}$ be the geometric endomorphism ring. Then $E[\ell]$ is an $\mathcal{O}$-module and we view $\mathrm{Aut}_{\mathcal{O}}(E[\ell]) \leq \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$. We say that $\bar{\rho}_{E,\ell}$ is **maximal** if its image contains $\mathrm{SL}_2(\mathbb{F}_\ell) \cap \mathrm{Aut}_{\mathcal{O}}(E[\ell])$.

For $K = \mathbb{Q}$, the image of a maximal $\bar{\rho}_{E,\ell}$ is $\mathrm{GL}_2(\mathbb{F}_\ell)$, a Borel subgroup, the normalizer of a split Cartan subgroup, or the normalizer of a non-split Cartan subgroup, depending on whether $\mathcal{O} = \mathbb{Z}$ or $\mathcal{O} \neq \mathbb{Z}$ and ℓ is ramified, split, or inert in $\mathcal{O}$, respectively.

3.36 Minimal discriminant

Definition. The **minimal discriminant** (or minimal discriminant ideal) of an elliptic curve E over a number field K is the ideal $\mathfrak{D}_{min}$ of the ring of integers of K given by

$$\mathfrak{D}_{\mathrm{min}} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}},$$

where the product is over all primes $\mathfrak{p}$ of K, and $\mathfrak{p}^{e_{\mathfrak{p}}}$ is the local minimal discriminant of E at $\mathfrak{p}$.

If E has a Weierstrass model which is a global minimal model then $\mathfrak{D}_{\mathrm{min}} = (\Delta)$, the principal ideal generated by the discriminant Δ of this model. In general,

$\mathfrak{D}_{\mathrm{min}}$ differs from the ideal generated by the discriminant of any Weierstrass model by the 12th power of an ideal.

3.37 Mordell-Weil group

Definition. For an elliptic curve E defined over a field K, the **Mordell-Weil group** of E/K is the group $E(K)$ of K-rational points of E. It is a finitely-generated Abelian group.

This is a special case of the Mordell-Weil group of an abelian variety.

The Mordell-Weil Theorem, first proved by Mordell for elliptic curves defined over $\mathbb{Q}$ and later generalized by Weil to abelian varieties A over general number fields K, states that, if K is a number field, then $A(K)$ is a finitely generated abelian group. Its rank is called the **Mordell-Weil rank** of A over K.

The Mordell-Weil theorem implies in particular that the torsion subgroup $E(K)_{\mathrm{tor}}$ of $E(K)$ is finite, and thus that the torsion order of E, one of the BSD invariants, is finite.

3.38 Mordell-Weil theorem

Definition. For an elliptic curve E defined over a number field F, the **Mordell-Weil theorem** states that the set $E(F)$ of F-rational points on E is a finitely generated Abelian group.

This group is called the Mordell-Weil group of E/K.

3.39 Multiplicative reduction

Definition. An elliptic curve E defined over a number field K is said to have **multiplicative reduction** at a prime $\mathfrak{p}$ of K if the reduction of E modulo $\mathfrak{p}$ has a nodal singularity.

The case of multiplicative reduction is further subdivided into split multiplicative reduction and nonsplit multiplicative reduction.

3.40 Mordell-Weil generators

Definition. The **Mordell-Weil group** $E(K)$ of an elliptic curve E over a number field K is a finitely generated abelian group, explicitly described by giving a $\mathbb{Z}$-basis for the group, equivalently, a (minimal) set of **Mordell-Weil generators**, each of which is a rational point on the curve.

The generators consist of r **non-torsion generators**, where r is the rank of $E(K)$, and up to two **torsion generators**, which generate the torsion subgroup $E(K)_{\mathrm{tor}}$.

3.41 Non-split multiplicative reduction

Definition. An elliptic curve E defined over a number field K is said to have **non-split multiplicative reduction** at a prime $\mathfrak{p}$ of K if the reduction of E modulo $\mathfrak{p}$ has a nodal singularity with tangent slopes *not* defined over the residue field at $\mathfrak{p}$.

3.42 Obstruction class of an elliptic curve

Definition. Let E be an elliptic curve defined over a number field K. The **obstruction class** of E is an ideal class of K which is trivial if and only if E has a global minimal model.

3.43 Tate module of an elliptic curve

Definition. Let $p \in \mathbb{Z}_{\geq 0}$ be a prime and E an elliptic curve defined over a field K. The **p-adic Tate module** of E is the inverse limit

$$T_p(E) = \varprojlim_{n \in \mathbb{N}} E[p^n].$$

Here for $m \in \mathbb{Z}_{\geq 0}$, $E[m]$ denotes the m-torsion subgroup of E, which is the kernel of the multiplication-by-m endomorphism of E.

If K has characteristic not equal to p, then $T_p(E)$ is a free $\mathbb{Z}_p$-module of rank 2. It carries an action of the absolute Galois group of K, and thus has an associated Galois representation.

This is a special case of the Tate module of an abelian variety.

3.44 Global period of an elliptic curve

Definition. The **global period** $\Omega(E/K)$ of an elliptic curve defined over a number field K is a product of local factors $\Omega_v(E_v/K_v)$, one for each infinite place v of K. Here, K_v denotes the completion of K at v (so $K_v = \mathbb{R}$ for a real place and $K_v = \mathbb{C}$ for a complex place), and E_v denotes the base change of E to K_v.

Fixing a Weierstrass model for E with coefficients $a_i \in K$, a model for E_v is given by the Weierstrass equation with coefficients $a_{i,v}$, the images of a_i under v in K_v. Associated to this model we have a discriminant $\Delta(E_v)$ and an invariant differential $\omega_v = dx/(2y + a_{1,v}x + a_{3,v})$.

For a real place given by an embedding $v : K \to \mathbb{R}$, we define

$$\Omega_v(E_v) = \left| \int_{E_v(\mathbb{R})} \omega_E \right|.$$

In terms of a basis of the period lattice of E_v of the form $[x, yi]$ (when $\Delta(E_v) > 0$) or $[2x, x + yi]$ (when $\Delta(E_v) < 0$), where x and y are positive real numbers, we have $\Omega_v(E_v) = 2x$.

For a complex place given by an embedding $v : K \to \mathbb{C}$, we define

$$\Omega_v(E_v) = \left| \int_{E_v(\mathbb{C})} \omega_E \wedge \overline{\omega_E} \right|.$$

In terms of a basis $[w_1, w_2]$ of the period lattice of E_v, where $\Im(w_2/w_1) > 0$, we have $\Omega_v(E_v) = 2\Im(\overline{w_1} w_2)$, which is double the covolume of the period lattice.

When E has a global minimal model, we have

$$\Omega(E/K) = \prod_v \Omega_v(E_v).$$

In general, given an arbitrary model for E with discriminant $\Delta(E)$, we have

$$\Omega(E/K) = \left| \frac{N(\Delta(E))}{N(\mathfrak{d}(E))} \right|^{1/12} \prod_v \Omega_v(E_v),$$

where $\mathfrak{d}$ is the minimal discriminant ideal of E and $N(\mathfrak{d})$ denotes its norm. This quantity is independent of the model of E.

3.45 Potential good reduction

Definition. An elliptic curve E defined over a number field K is said to have **potential good reduction** if E has everywhere good reduction over a finite extension of K.

This is equivalent to the j-invariant of E being integral.

3.46 Elliptic curve over $\mathbb{Q}$

Definition. An **elliptic curve** E **over** $\mathbb{Q}$ has a Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ such that its discriminant

$$\Delta := -16(4a^3 + 27b^2) \neq 0.$$

Note that such an equation is not unique and E has a unique minimal Weierstrass equation.

3.47 *abc* quality

Definition. Given a triple a, b, c of nonzero coprime integers, the **quality** of the triple is defined as

$$Q = \frac{\log \max(|a|, |b|, |c|)}{\log \operatorname{rad}(abc)},$$

where $\operatorname{rad}(abc)$ is the product of the primes dividing abc. The abc conjecture stipulates that for any $\epsilon > 0$ there are only finitely many relatively prime triples a, b, c with quality larger than $1 + \epsilon$.

The abc **quality** of an elliptic curve E is the quality of an a, b, c triple determined by its j-invariant, namely the one defined by writing $\frac{j}{1728} = \frac{a}{c}$ in lowest terms and setting $b = c - a$. Note that the abc quality is undefined for $j = 0$ and $j = 1728$.

The reason for defining the quality of E in this way comes from the equivalence of the abc conjecture with the modified Szpiro conjecture. For elliptic curves with small conductor, j-invariants often have unusually large quality.

3.48 Analytic rank of an elliptic curve over $\mathbb{Q}$

Definition. The **analytic rank** of an elliptic curve E is the analytic rank of its L-function $L(E,s)$. The weak form of the BSD conjecture implies that the analytic rank is equal to the rank of the Mordell-Weil group of E.

For elliptic curves E over $\mathbb{Q}$, it is known that $L(E,s)$ satisfies the Hasse-Weil conjecture, and hence that the parity of the analytic rank is always compatible with the sign of the functional equation.

In general, analytic ranks stored in the LMFDB are only upper bounds on the true analytic rank (they could be incorrect if $L(E,s)$ had a zero very close to but not on the central point). For elliptic curves over $\mathbb{Q}$ of analytic rank less than 2 this upper bound is necessarily tight, due to parity; for analytic ranks 2 and 3 is also tight due to results of Kolyvagin; Murty and Murty; Bump, Friedberg and Hoffstein; Coates and Wiles; Gross and Zagier which together say that when the analytic rank is 0 or 1 then it equals the Mordell-Weil rank.

3.49 Analytic order of Ш

Definition. The **Tate-Shafarevic group** Ш of an elliptic curve E defined over $\mathbb{Q}$ is a torsion group defined in terms of Galois cohomology, which is conjectured to be finite. Its order #Ш appears in the strong form of the Birch-Swinnerton-Dyer Conjecture for E. The value of the order which is predicted by the conjecture is called the **Analytic Order of Sha**, $Ш_{an}$. <!–Note that the value of Ш_{an} predicted by the conjecture is always a square.–>

For elliptic curves of rank 0 or 1 it is a theorem that Ш_{an} is a positive rational number, and this rational number can be computed exactly; this exact computation has only been carried out for the curves in the database with rank 0 and conductor $N \leq 500000$. These values are always in fact integer squares in all cases computed to date. For curves of rank 2 and above, there is no

such theorem, and the values computed are simply floating point approximate values which happen to be very close to integers. In the LMFDB we store and display the rounded values in this case.

3.50 Birch and Swinnerton-Dyer conjecture

Definition. The **Birch and Swinnerton-Dyer** conjecture is one of the Millennium Prize Problems listed by the Clay Mathematics Institute. It relates the order of vanishing and the first non-zero Taylor series coefficient of the L-function associated to an elliptic curve E defined over $\mathbb{Q}$ at the central point $s = 1$ to certain arithmetic data, the BSD invariants of E.

Specifically, the BSD conjecture states that the order r of vanishing of $L(E, s)$ at $s = 1$ is equal to the rank of the Mordell-Weil group $E(\mathbb{Q})$, and that

<!– comment: if you make the following display into a normal one using

..

or

..

then something about the html code for Sha stops it displaying properly–>

 $\frac{1}{r!}L^{(r)}(E,1) = \frac{\#Ш(E/\mathbb{Q}) \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}.$

The quantities appearing in this formula are the BSD invariants of E:

- r is the rank of $E(\mathbb{Q})$ (a non-negative integer);
- $\#Ш(E/\mathbb{Q})$ is the order of the Tate-Shafarevich group

of E (which is conjectured to always be finite, a positive integer);

- $\mathrm{Reg}(E/\mathbb{Q})$ is the regulator of $E/\mathbb{Q}$;

- Ω_E is the real period of $E/\mathbb{Q}$ (a positive real number);
- c_p is the Tamagawa number of E at each prime p (a positive integer which is 1 for all but at most finitely many primes);
- $E(\mathbb{Q})_{\mathrm{tor}}$ is the torsion order of $E(\mathbb{Q})$ (a positive integer).

There is a similar conjecture for abelian varieties, in which the real period is replaced by the covolume of the period lattice.

3.51 Canonical height

Definition. Let E be an elliptic curve defined over $\mathbb{Q}$. The **canonical height** of a rational point $P \in E(\mathbb{Q})$ is computed by writing the x-coordinate $x(nP) = A_n(P)/D_n(P)$ as a fraction in lowest terms and setting

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{n^2} \log \max\bigl\{|A_n(P)|, |D_n(P)|\bigr\}.$$

(<EM>Note</EM>. Some sources define $\hat{h}$ to be $\frac{1}{2}$ of this quantity.)

Properties of $\hat{h}$: <UL> <LI> $\hat{h}(P) = \log\max\bigl\{|A_1(P)|, |D_1(P)|\bigr\} + O(1)$ as P ranges over $E(\mathbb{Q})$. <LI> $\hat{h}(P) \geq 0$; and $\hat{h}(P) = 0$ if and only if P is a torsion point. <LI> $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ extends to a positive definite quadratic form on $E(\mathbb{Q}) \otimes \mathbb{R}$. </UL> The **height pairing** on E is the associated bilinear form $\langle P, Q\rangle = \frac{1}{2}\bigl(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\bigr)$, which is used to compute the elliptic regulator of E. It is a symmetric positive definite bilinear form on $E(\mathbb{Q}) \otimes \mathbb{R}$.

For a number field K, the **canonical height** of $P \in E(K)$ is given by $\hat{h}(P) = \lim_{n\to\infty} n^{-2} h\bigl(x(nP)\bigr)$, where h is the Weil height.

3.52 Conductor of an elliptic curve over $\mathbb{Q}$

Definition. The **conductor** N of an elliptic curve E defined over $\mathbb{Q}$ is a positive integer divisible by the primes of bad reduction and no others. It has the form $N = \prod p^{e_p}$, where the exponent e_p is

- $e_p = 1$ if E has multiplicative reduction at p,
- $e_p = 2$ if E has additive reduction at p and $p \geq 5$,
- $2 \leq e_p \leq 5$ if E has additive reduction and $p = 3$, and
- $2 \leq e_p \leq 8$ if E has additive reduction and $p = 2$.

For all primes p, there is an algorithm of Tate that simultaneously creates a local minimal Weierstrass equation and computes the exponent of the conductor. See:

<UL> <LI> J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 33-52. <EM>Lecture Notes in Math.</EM>, Vol. <B>476</B>, Springer, Berlin, 1975. [?]

<LI> J.H. Silverman, <EM>Advanced topics in the arithmetic of elliptic curves</EM>, GTM <B>151</B>, Springer-Verlag, New York, 1994.[?]

</UL>

3.53 Cremona label

Definition. The **Cremona label** of an elliptic curve over $\mathbb{Q}$ is a way of indexing the elliptic curves over $\mathbb{Q}$. It has the form $11a1$ or $10050bf2$. The first number represents the conductor, the letter or letters represent the isogeny class and the last number represents the isomorphism class within the isogeny class as it appears in [Cremona's tables.](http://johncremona.github.io/ecdata/) In each

isogeny class the curve with number 1 is the $\Gamma_0(N)$-optimal curve.
 For more details, see "The elliptic curve database for conductors to 130000" by John Cremona in ANTS-VII proceedings, Lecture Notes in Computer Science, vol. 4076, 2006, 11-29.

In the Cremona labeling, it is somewhat difficult to describe the mechanisms for ordering isogeny classes or curves within a class, since these depend on the order in which the curves were computed (though for conductors over 230,000 the isogeny class labels coincide). Cremona labels are only available for conductors up to 500,000. For these reasons, within this site we also use the LMFDB label, whose definition is somewhat simpler. Note that the lack of internal punctuation distinguishes Cremona labels from LMFDB labels.

3.54 Discriminant of an elliptic curve over $\mathbb{Q}$

Definition. The **discriminant** Δ of an elliptic curve E defined over $\mathbb{Q}$ is a nonzero integer divisible exactly by the primes of bad reduction. It is the discriminant of the minimal Weierstrass equation of the curve.

3.55 Endomorphism ring of an elliptic curve

Definition. The **endomorphism ring** $\mathrm{End}(E)$ of an elliptic curve E is the ring of all endomorphisms of E defined over K. For endomorphisms defined over extensions, we speak of the geometric endomorphism ring of E.

For elliptic curves defined over $\mathbb{Q}$, this ring is always isomorphic to $\mathbb{Z}$ consisting of the multiplication-by-m maps $[m]\colon E \to E$ for $m \in \mathbb{Z}$.

This is a special case of the endomorphism ring of an abelian variety.

3.56 Faltings height of an elliptic curve

Definition. The **Faltings height** of an elliptic curve E defined over $\mathbb{Q}$ is the quantity

$$h_{\text{Faltings}}(E) = -\frac{1}{2}\log(A),$$

where A is the covolume (that is, the area of a fundamental period parallelogram) of the KNOWL('ec.q.period_lattice', 'Né;ron lattice') of E.

The **stable Faltings height** of E is

$$h_{\text{stable}}(E) = \frac{1}{12}(\log \text{denom}(j) - \log(|\Delta|)) - \frac{1}{2}\log(A),$$

where j is the j-invariant of E, Δ the discriminant of any model of E and A the covolume of the period lattice of that model. The stable height is independent of the model of E, and the unstable and stable heights are equal for semistable curves, for which $\text{denom}(j) = |\Delta|$.

3.57 Faltings ratio

Definition. In each isogeny class of elliptic curves defined over $\mathbb{Q}$, there is a unique curve E_{min} whose KNOWL('ec.q.period_lattice', 'Né;ron lattice') is a sublattice of the Né;ron lattices of all the curves in the class (G. Stevens, [**?**]); it is the unique curve of minimal Faltings height among the curves in the isogeny class.

The **Faltings ratio** of each curve E is the index of the Né;ron lattice of E_{min} in that of E.

3.58 Frey curve

Definition. Given a triple of integers A, B, C with $A + B = C$, the [**Frey curve**](https://en.wikipedia.org/wiki/Frey_curve) (or **Frey-Hellegouarch curve**)

associated to this triple is the elliptic curve

$$y^2 = x(x - A)(x + B).$$

3.59 Integral points

Definition. The **integral points** on a given model of an elliptic curve E defined over $\mathbb{Q}$ are the points $P = (x, y)$ on the model that have integral coordinates x and y.

The number of integral points is finite, by a theorem of Siegel.

3.60 j-invariant of a rational elliptic curve

Definition. The j**-invariant** of an elliptic curve E defined over $\mathbb{Q}$ is an invariant of the isomorphism class of E over $\overline{\mathbb{Q}}$. If the Weierstrass equation of E is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then its j-invariant is given by

$$j = \frac{c_4^3}{\Delta}$$

where

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

and

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

is the discriminant of E.

3.61 Kodaira symbol

Definition. The **Kodaira symbol** encodes the reduction type of an elliptic curve at a prime p. It describes the combinatorics of the special fiber of the Né;ron model of the elliptic curve. The Né;ron model is obtained from the minimal Weierstrass equation using Tate's algorithm. For an exact definition and properties, consult a text on elliptic curves.

3.62 Label for an elliptic curve over $\mathbb{Q}$

Definition. The **LMFDB label** of an elliptic curve E over $\mathbb{Q}$ is a way of indexing the elliptic curves over $\mathbb{Q}$. It has the form "11.a1" or "10050.bf2".

The label has three components: the **conductor**, the **isogeny class label**, and the **isomorphism class index**.

1. The first component is the decimal representation of the conductor (a positive integer).

2. The second component is the isogeny class label, a string which represents the **isogeny class index**, a non-negative integer encoded as in base 26 using the 26 symbols a,b,.., z. The isogeny classes of elliptic curves with the same conductor are sorted lexicographically by the q-expansions of the associated modular forms, and the isogeny class index of each isogeny class of fixed conductor is the index (starting at 0) of the class in this ordering.

3. The third component is the decimal representation of the isomorphism class index, a positive integer giving the index of the coefficient vector $[a_1, a_2, a_3, a_4, a_6]$ of the reduced minimal Weierstrass equation of E in a lexicographically sorted list of all the elliptic curves in the isogeny class.

The complete label is obtained by concatenating [conductor, ".", isogeny class label, isomorphism class index].

Note that this is not the same as the Cremona label, even though for certain curves they only differ in the insertion of the dot "." (for example, "37a1" and "37.a1" are the same curve). The presence of the punctuation "." distinguishes an LMFDB label from a Cremona label. Cremona labels are only defined for curves of conductor up to 500000.

3.63 Manin constant for elliptic curves over $\mathbb{Q}$

Definition. Let E be an optimal elliptic curves of conductor N, let f be the modular form associated to E, and let $\varphi : X_0(N) \to E$ be the associated modular parametrization. Let ω_E be the Né;ron differential on E. Then the pull-back $\varphi^*\omega_E$ of ω_E to $X_0(N)$ satisfies

$$\varphi^*\omega_E = c \cdot 2\pi i f(z)dz$$

for some non-zero rational number c called the **Manin constant** of E. In fact $c \in \mathbb{Z}$, by a theorem of Edixhoven.

It is conjectured that $c = 1$ for all optimal curves, and there are several results stating that $c = 1$ if certain conditions hold: see Amod Agashe, Ken Ribet and William Stein: The Manin Constant, Pure and Applied Mathematics Quarterly, Vol. 2 no.2 (2006), pp. 617–636. In an appendix to that paper, John Cremona gives an algorithm for verifying that $c = 1$ in individual cases, and proves that $c = 1$ for all optimal elliptic curves over $\mathbb{Q}$ in the database. Kęstutis Česnavičius proves $c = 1$ for semistable elliptic curves over $\mathbb{Q}$, and more generally that $v_p(c) = 0$ if $p^2 \nmid N$ in *The Manin constant in the semistable case*, Compositio Math. **154** (2018), 1889–1920.

For non-optimal elliptic curves E' over $\mathbb{Q}$, the **Manin constant** is defined, in

terms of the Manin constant of the unique optimal curve isogenous to E'. Let $\varphi : X_0(N) \to E$ and f be as above, and $\psi : E \to E'$ an isogeny of least degree from E to E'. Then we obtain a parametrization $\psi \circ \varphi : X_0(N) \to E'$ and define the Manin constant c' of E' to be the non-zero rational number such that

$$(\psi \circ \varphi)^* \omega_{E'} = c' \cdot 2\pi i f(z) dz.$$

This is an integer multiple of the Manin constant of E, since $\psi^* \omega_{E'}$ is an integer multiple of ω_E; the multiplier divides the degree of ψ but may be strictly less: it may equal 1.

3.64 Minimal twists of elliptic curves over $\mathbb{Q}$

Definition. The **minimal quadratic twist** of an elliptic curve E defined over $\mathbb{Q}$ is defined as follows.

- First consider the finite set of all quadratic twists of E which have minimal conductor. If this set contains just one curve, it is the minimal quadratic twist.

- Otherwise, sort the curves with minimal conductor into isogeny classes, and restrict attention to the curves whose class comes first in the LMFDB labelling; equivalently, sort the curves by the sequence of coefficients (a_n) of their L-function and restrict to the curve or curves with the first such sequence.

- If E does not have Complex Multiplication (CM), then the minimal isogeny class contains a *unique* curve with the same j-invariant as E, and this curve is the minimal quadratic twist of E.

- If E does have CM, then the minimal isogeny class contains exactly *two* curves with j-invariant $j(E)$. In all but one case these two curves have distinct minimal discriminants, with the same sign, and we define the

minimal quadratic twist to be the curve whose minimal discriminant has smallest absolute value.

- The exception is for elliptic curves with $j = 66^3$, which have CM by the imaginary quadratic order with discriminant -16. The minimal conductor is 32, and curves [32.a1](https://www.lmfdb.org/EllipticCurve/Q/32/a/1) and [32.a2](https://www.lmfdb.org/EllipticCurve/Q/32/a/2) (which are quadratic twists of each other by -1) both have minimal discriminant 2^9. The minimal quadratic twist for $j = 66^3$ is defined to be [32.a1](https://www.lmfdb.org/EllipticCurve/Q/

All elliptic curves E over $\mathbb{Q}$ with j-invariant 1728 are quartic twists of each other. The smallest conductor of such a curve is 32. Both the curves [32.a3](https://www.lmfdb.org/EllipticCurve/Q/3 and [32.a4](https://www.lmfdb.org/EllipticCurve/Q/32/a/4) have j-invariant 1728, and they have minimal discriminants -2^{12} and 2^6 respectively. We define the **minimal quartic twist** (or just **minimal twist**) of every elliptic curve with $j = 1728$ to be the curve [32.a3](https://www.lmfdb.org/EllipticCurve/Q/32/a/3), which has smaller discriminant, and equation $Y^2 = X^3 - X$.

All elliptic curves E over $\mathbb{Q}$ with j-invariant 0 are sextic twists of each other. The smallest conductor of such a curve is 27. Both the curves [27.a3](https://www.lmfdb.org/EllipticCurve/Q/27/a/ and [27.a4](https://www.lmfdb.org/EllipticCurve/Q/27/a/4) have j-invariant 0, and they have minimal discriminants -3^9 and -3^3 respectively. We define the **minimal sextic twist** (or just **minimal twist**) of every elliptic curve with $j = 0$ to be the curve [27.a4](https://www.lmfdb.org/EllipticCurve/Q/27/a/4), which has smaller discriminant, and equation $Y^2 + Y = X^3$.

The **minimal twist** of an elliptic curve E is its minimal quadratic twist, unless $j(E) = 0$ or 1728, in which cases the minimal twist is its minimal sextic or quartic twist respectively. The minimal quadratic twist depends only on the j-invariant unless $j = 0$ or 1728; in each of these cases, there are infinitely many different minimal quadratic twists, though only one minimal twist.

3.65 Minimal Weierstrass equation over $\mathbb{Q}$

Definition. Every elliptic curve over $\mathbb{Q}$ has an integral Weierstrass model (or equation) of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where a_1, a_2, a_3, a_4, a_6 are integers. Each such equation has a discriminant Δ. A **minimal Weierstrass equation** is one for which $|\Delta|$ is minimal among all Weierstrass models for the same curve. For elliptic curves over $\mathbb{Q}$, minimal models exist, and there is a unique **reduced minimal model** which satisfies the additional constraints $a_1, a_3 \in \{0, 1\}$, $a_2 \in \{-1, 0, 1\}$.

3.66 Modular degree of an elliptic curve over $\mathbb{Q}$

Definition. The **modular degree** of an elliptic curve over $\mathbb{Q}$ is the minimum degree of a modular parametrization of the curve.

3.67 Modular parametrization of an elliptic curve over $\mathbb{Q}$

Definition. A **modular parametrization** of an elliptic curve E over $\mathbb{Q}$ is a non-constant map $X_0(N) \to E$, where N is the conductor of E.

3.68 Naive height

Definition. The **naive height** of an elliptic curve in short Weierstrass form

$$y^2 = x^3 + a_4x + a_6$$

is the quantity $\max(4|a_4|^3, 27|a_6|^2)$.

3.69 Optimal elliptic curve over $\mathbb{Q}$

Definition. An elliptic curve over $\mathbb{Q}$ is **optimal** if it is an optimal quotient of the corresponding modular curve. Every isogeny class contains a unique optimal curve. For more information, see [William Stein's page on optimal quotients.](http://wstein.org/papers/ars-manin/html/node2.html)

Optimal curves have a Cremona label whose last component is the number 1, with the exception of class 990h where the optimal curve is 990h3 (number 3). This is a historical accident and has no mathematical significance.

NB It has not yet been proved in all cases that the first curve in each class is optimal; however this is true for all isogeny classes of conductor ≤ 400000, and for many others (for example whenever the isogeny class consists of only one curve). The current optimality status of each curve is shown on its home page.

3.70 Period lattice of an elliptic curve

Definition. For E an elliptic curve defined over $\mathbb{C}$ by a Weierstrass equation with coefficients a_1, a_2, a_3, a_4, a_6, the **period lattice** of E is the set Λ of periods of the invariant differential $dx/(2y+a_1x+a_3)$, which is a discrete lattice of rank 2 in $\mathbb{C}$. There is an isomorphism (of complex Lie groups) $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ defined in terms of the Weierstrass $\wp$-function.

For elliptic curves defined over $\mathbb{R}$ (and in particular, for those defined over $\mathbb{Q}$), the period lattice has one of two possible types dependng on the sign of the discriminant Δ of E:

- If $\Delta > 0$, then Λ is *rectangular*, with a $\mathbb{Z}$-basis of the form $\langle x, yi\rangle$, where x and y are positive real numbers; in this case, $E(\mathbb{R})$ has two connected components.

- If $\Delta < 0$, then Λ has a $\mathbb{Z}$-basis of the form $\langle 2x, x+yi\rangle$, where x and y are

positive real numbers; in this case, $E(\mathbb{R})$ has one connected component.

The **real period** of E is defined to be $2x$ in each case, so is equal to the smallest positive real period multiplied by the number of real components.

Note that the period lattice depends on the choice of Weierstrass model of E; different models have homothetic lattices. For elliptic curves defined over $\mathbb{Q}$, the period lattice associated to a global minimal model of E is called the **Né;ron lattice** of E. The real period of the Né;ron lattice is denoted Ω_E, and appears in the Birch Swinnerton-Dyer conjecture for E.

3.71 Real period

Definition. For an elliptic curve E defined over $\mathbb{R}$ with period lattice Λ, the **real period** Ω is the least positive element of $\Lambda \cap \mathbb{R}$ multiplied by the number of components of $E(\mathbb{R})$.

When an elliptic curve is defined by means of a Weierstrass equation, the period lattice Λ is the lattice of periods of the invariant differential $dx/(2y + a_1x + a_3)$. Different Weierstrass models defining isomorphic curves have period lattices which are **homothetic**, meaning that they differ by a nonzero multiplicative constant. When we speak of **the** period lattice or **the** real period for an elliptic curve defined over $\mathbb{Q}$, we always mean the lattice and period associated with a minimal equation.

3.72 Reduction type of an elliptic curve over $\mathbb{Q}$

Definition. The **reduction type** of an elliptic curve E defined over $\mathbb{Q}$ at a prime p depends on the reduction $\tilde{E}$ of E modulo p. This reduction is constructed by taking a minimal Weierstrass equation for E and reducing its coefficients modulo p to obtain a curves over $\mathbb{F}_p$. The reduced curve is either smooth (non-singular) or has a unique singular point.

E has **good reduction** at p if $\tilde{E}$ is non-singular over $\mathbb{F}_p$. The reduction type is **ordinary** (ord) if $\tilde{E}$ is ordinary (equivalently, if $\tilde{E}(\overline{\mathbb{F}_p})$ has non-trivial p-torsion) and **supersingular** (ss) otherwise. The coefficient $a(p)$ of the L-function $L(E,s)$ is divisible by p if the reduction is supersingular and not if it is ordinary.

E has **bad reduction** at p if $\tilde{E}$ is singular over $\mathbb{F}_p$. In this case the reduction type is further classified according to the nature of the singularity. In all cases the singularity is a double point.

E has **multiplicative reduction** at p if $\tilde{E}$ has a **nodal** singularity: the singular point is a node, with distinct tangents. It is called **split** if the two tangents are defined over $\mathbb{F}_p$ and **non-split** otherwise. The coefficient $a(p)$ of $L(E,s)$ is 1 if the reduction is split and -1 if it is non-split.

E has **additive reduction** at p if $\tilde{E}$ has a **cuspidal** singularity: the singular point is a cusp, with only one tangent. In this case $a(p) = 0$.

3.73 Regulator of elliptic curve

Definition. The **regulator** of an elliptic curve E defined over a number field K, denoted $\mathrm{Reg}(E/K)$, is the volume of $E(K)/E(K)_{tor}$ with respect to the **height pairing** $\langle -,- \rangle$ associated to the canonical height $\hat{h}$, i.e. $\langle P,Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$.

If the Mordell-Weil group $E(K)$ has rank r and $P_1, \ldots, P_r \in E(K)$ generate $E(K)/E(K)_{tor}$, then

$$\mathrm{Reg}(E/K) = |\det(\langle P_i, P_j \rangle)_{1 \le i,j \le r}|\,,$$

which is independent of the choice of generators.

Special cases are when $E(K)$ has rank 0, in which case $E(K)/E(K)_{tor} = 0$ and $\mathrm{Reg}(E/K) = 1$, and when $E(K)$ has rank 1, in which case $\mathrm{Reg}(E/K)$ is equal

to the canonical height $\hat{h}(P)$ of a generator P.

3.74 Semistable elliptic curve

Definition. An elliptic curve is **semistable** if it has multiplicative reduction at every bad prime.

3.75 Serre invariants

Definition. Let $\bar{\rho}_{E,\ell}$ be the mod-ℓ Galois representation of an elliptic curve $E/\mathbb{Q}$.

The **Serre invariants** (k, M) of $\bar{\rho}_{E,\ell}$ consist of the **Serre weight** k and the **Serre conductor** M giving the weight and minimal level of a newform $f \in S_k^{new}(\Gamma_1(M))$ whose associated mod-ℓ Galois representation is isomorphic to $\bar{\rho}_{E,\ell}$.

This means that $a_p(E)$ and $a_p(f)$ reduce to the same element of the residue field of a prime above ℓ in the coefficient field of f (this residue field need not have degree one, but every $a_p(f)$ must reduce to an element of $\mathbb{F}_\ell$ in order for this condition to hold).

The modular form f is not uniquely determined, but the minimal level M arising among all such f is uniquely determined, and among those with level M, the weight is uniquely determined.

For all but finitely many primes ℓ, including all $\ell > 7$ of good reduction for E, the Serre invariants are $(2, N)$, where N is the conductor of the elliptic curve. The primes ℓ for which this does not hold are **exceptional**.

In general, the Serre weight k is divisible by 2 and the Serre conductor M divides N.

3.76 Special value of an elliptic curve L-function

Definition. The **special value** of an elliptic curve $E/\mathbb{Q}$ is the first nonzero value of $L^{(r)}(E,1)/r!$ for $r \in \mathbb{Z}_{\geq 0}$, where $L(E,s)$ is the L-function of E in its arithmetic normalization.

The special value appears on the LHS of the formula in the Birch and Swinnerton-Dyer conjecture.

3.77 Szpiro ratio

Definition. The (modified) **Szpiro ratio** of an elliptic curve E is defined as

$$\sigma_m(E) = \frac{\log \max(|c_4|^3, |c_6|^2)}{\log N},$$

where N is the conductor of E and c_4 and c_6 are defined as for the j-invariant. The (modified) Szpiro conjecture is that, for any $\epsilon > 0$, there are only finitely many elliptic curves with Szpiro ratio larger than $6 + \epsilon$. In [**?**], Oesterlé proves that this conjecture is equivalent to the *abc* conjecture.

In Oesterlé's paper cited above, there is another conjecture, that the ratio

$$\frac{\log \Delta}{\log N},$$

also has the property of only taking values larger than $6 + \epsilon$ finitely many times (here Δ is the minimal discriminant of E). This conjecture is implied by the modified Szpiro conjecture (and thus the *abc* conjecture), but it is not currently known to be equivalent. All of the Szpiro ratios in the LMFDB are computed in terms of c_4 and c_6 rather than Δ for this reason.

3.78 Torsion growth in number fields

Definition. Let E be an elliptic curve defined over $\mathbb{Q}$ and let K be a number field. We say that there is **torsion growth** from $\mathbb{Q}$ to K if the torsion subgroup $E(K)_{\mathrm{tor}}$ of $E(K)$ is strictly larger than $E(\mathbb{Q})_{\mathrm{tor}}$.

If there is torsion growth in a field K then obviously the torsion also grows in every extension of K. We say that the torsion growth in K is **primitive** if $E(K)_{\mathrm{tor}}$ is strictly larger than $E(K')_{\mathrm{tor}}$ for all proper subfields $K' \subsetneq K$.

For every elliptic curve E there is torsion growth in at least one field of degree 2, 3, or 4, and torsion can only grow in fields whose degree is divisible by 2, 3, 5 or 7: see Theorem 7.2 of [**?**]. Additionally, there is no primitive torsion growth in fields of degrees 22 or 26: see Lemma 2.11 of [**?**]. Hence the only degrees less than 24 in which primitive torsion growth occurs are $2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21$.

3.79 Torsion subgroup of an elliptic curve over $\mathbb{Q}$

Definition. If E is an elliptic curve defined over $\mathbb{Q}$, its **torsion subgroup** is the subgroup of the Mordell-Weil group $E(\mathbb{Q})$ consisting of all the rational points of finite order. It is a finite abelian group of order at most 16 (by a theorem of Mazur), which is a product of at most 2 cyclic factors. The "torsion structure" is the list of invariants of the group:

- [] for the trivial group;
- $[n]$ for a cyclic group of order n (only $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$ or 12 occur for elliptic curves over $\mathbb{Q}$);
- $[n_1, n_2]$ with $n_1 \mid n_2$ for a product of cyclic groups of orders n_1 and n_2 (only $[2, 2m]$ for $m = 2, 4, 6$ or 8 occur over $\mathbb{Q}$).

3.80 $\mathbb{Q}$-curves

Definition. An elliptic curve E defined over a number field K is a **$\mathbb{Q}$-curve** if it is isogenous over $\overline{K}$ to each of its Galois conjugates. Note that the isogenies need not be defined over K itself.

An elliptic curve which is the base change of a curve defined over $\mathbb{Q}$ is a $\mathbb{Q}$-curve, but not all $\mathbb{Q}$-curves are base-change curves.

Elliptic curves with CM are all $\mathbb{Q}$-curves, as are all those whose j-invariant is in $\mathbb{Q}$.

3.81 Rank of an elliptic curve over a number field

Definition. The **rank** of an elliptic curve E defined over a number field K is the rank of its Mordell-Weil group $E(K)$.

The Mordell-Weil Theorem says that $E(K)$ is a finitely-generated abelian group, hence

$$E(K) \cong E(K)_{\mathrm{tor}} \times \mathbb{Z}^r$$

where $E(K)_{\mathrm{tor}}$ is the finite torsion subgroup of $E(K)$, and $r \geq 0$ is the **rank**.

Rank is an isogeny invariant: all curves in an isogeny class have the same rank.

3.82 Reduction of an elliptic curve

Definition. An elliptic curve E over a number field K is **semistable** if it has multiplicative reduction at every bad prime, and has **potential good reduction** if its j-invariant is integral.

If E has potential good reduction then it cannot be semistable unless it has everywhere good reduction.

3.83 Reduction type

Definition. The **reduction type** of an elliptic curve E defined over a number field K at a prime $\mathfrak{p}$ of K depends on the reduction $\tilde{E}$ of E modulo $\mathfrak{p}$. Let $\mathbb{F}_q$ be the ring of integers of K modulo $\mathfrak{p}$, a finite field of characteristic p.

E has good reduction at $\mathfrak{p}$ if $\tilde{E}$ is non-singular over $\mathbb{F}_q$. The reduction type is **ordinary** if $\tilde{E}$ is ordinary (equivalently, $\tilde{E}(\overline{\mathbb{F}_q})$ has p-torsion) and **supersingular** otherwise.

On the other hand, if the reduction of E modulo $\mathfrak{p}$ is singular, then E has bad reduction. There are two types of bad reduction are as follows.

E has **multiplicative reduction** at $\mathfrak{p}$ if $\tilde{E}$ has a nodal singularity. It is called **split multiplicative reduction** if the two tangents at the node are defined over $\mathbb{F}_q$ and **non-split multiplicative reduction** otherwise.

E has **additive reduction** at $\mathfrak{p}$ if $\tilde{E}$ has a cuspidal singularity.

3.84 Regulator of an elliptic curve

Definition. The **regulator** of an elliptic curve E defined over a number field K, denoted $\mathrm{Reg}(E/K)$, is the volume of $E(K)/E(K)_{tor}$ with respect to the **height pairing** $\langle -,- \rangle$ associated to the canonical height $\hat{h}$, i.e. $\langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$.

If the Mordell-Weil group $E(K)$ has rank r and $P_1, \ldots, P_r \in E(K)$ generate $E(K)/E(K)_{\mathrm{tor}}$, then

$$\mathrm{Reg}(E/K) = |\det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}|\,,$$

which is independent of the choice of generators.

Special cases are when $E(K)$ has rank 0, in which case $E(K)/E(K)_{\mathrm{tor}} = 0$ and

$\mathrm{Reg}(E/K) = 1$, and when $E(K)$ has rank 1, in which case $\mathrm{Reg}(E/K)$ is equal to the canonical height $\hat{h}(P)$ of a generator P.

The canonical height used to define the regulator is usually *normalised* so that it is invariant under base change. Note that the regulator which appears in the Birch Swinnerton-Dyer conjecture is with respect to the non-normalised height; this is sometimes called the Néron-Tate regulator, and denoted $\mathrm{Reg}_{\mathrm{NT}}(E/K)$. These are related by

$$\mathrm{Reg}_{\mathrm{NT}}(E/K) = d^r \,\mathrm{Reg}(E/K),$$

where d is the degree $[K : \mathbb{Q}]$.

3.85 Elliptic curve over a ring

Definition. An **elliptic curve** over a commutative ring R is an elliptic scheme $E \to \operatorname{Spec} R$.

For example, an elliptic curve over $\mathbb{Z}[1/N]$ is the same as an elliptic curve over $\mathbb{Q}$ with good reduction at all primes not dividing N. (More precisely, the latter is the generic fiber of the former.)

3.86 Elliptic scheme

Definition. An **elliptic scheme** over a scheme S is a smooth proper morphism $E \to S$ whose fibers are elliptic curves.

3.87 Semi-global minimal model

Definition. An elliptic curve E defined over a number field K of class number $h(K)$ greater than 1 may not have a global minimal model. In this case there still exist **semi-global minimal models** for E which are local minimal models at all except one prime. At this prime, the discriminant valuation exceeds that

of the minimal discriminant ideal by 12.

3.88 Semistable elliptic curve

Definition. An elliptic curve is **semistable** if it has multiplicative reduction at every bad prime.

3.89 Simplified equation

Definition. Every elliptic curve over a field k whose characteristic is not 2 or 3 has a **simplified equation** (or **short Weierstrass model**) of the form $y^2 = x^3 + Ax + B$. When $k = \mathbb{Q}$ is the field of rational numbers, one can choose A and B to be integers.

For elliptic curves over $\mathbb{Q}$ this model will necessarily have bad reduction at 2, even when E has good reduction at 2; it may also bad reduction at 3 even when the minimal model of E does not.

3.90 Special value of an elliptic curve L-function

Definition. The **special value** of an elliptic curve E defined over a number field K is the first nonzero value of $L^{(r)}(E, 1)/r!$ for $r \in \mathbb{Z}_{\geq 0}$, where $L(E/K, s)$ is the L-function of E in its arithmetic normalization. It is also known as the **leading coefficient** of the L-function.

The special value appears in the Birch and Swinnerton-Dyer conjecture.

3.91 Split multiplicative reduction

Definition. An elliptic curve E defined over a number field K is said to have **split multiplicative reduction** at a prime $\mathfrak{p}$ of K if the reduction of E modulo $\mathfrak{p}$ has a nodal singularity with both tangent slopes defined over the residue field at $\mathfrak{p}$.

3.92 Tamagawa number

Definition. The **Tamagawa number** of an elliptic curve E defined over a number field at a prime $\mathfrak{p}$ of K is the index $[E(K_\mathfrak{p}) : E^0(K_\mathfrak{p})]$, where $K_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$ and $E^0(K_\mathfrak{p})$ is the subgroup of $E(K_\mathfrak{p})$ consisting of all points whose reduction modulo $\mathfrak{p}$ is smooth.

The Tamagawa number of E at $\mathfrak{p}$ is usually denoted $c_\mathfrak{p}(E)$. It is a positive integer, and equal to 1 if E has good reduction at $\mathfrak{p}$ and may be computed in general using Tate's algorithm.

The product of the Tamagawa numbers over all primes is a positive integer known as the **Tamagawa product**.

3.93 Torsion order of an elliptic curve

Definition. The **torsion order** of an elliptic curve E over a field K is the order of the torsion subgroup $E(K)_{\mathrm{tor}}$ of its Mordell-Weil group E(K).

The torsion subgroup $E(K)_{\mathrm{tor}}$ is the set of all points on E with coordinates in K having finite order in the group $E(K)$. When K is a number field (for example, when $K = \mathbb{Q}$) it is a finite set, since by the Mordell-Weil Theorem, $E(K)$ is finitely generated.

When $K = \mathbb{Q}$ the torsion order n satisfies $n \leq 16$, by a theorem of Mazur.

3.94 Torsion subgroup of an elliptic curve

Definition. For an elliptic curve E over a field K, the **torsion subgroup** of E over K is the subgroup $E(K)_{\mathrm{tor}}$ of the Mordell-Weil group $E(K)$ consisting of points of finite order. For a number field K this is always a finite group, since by the Mordell-Weil Theorem $E(K)$ is finitely generated.

The torsion subgroup is always either cyclic or a product of two cyclic groups. The **torsion structure** is the list of invariants of the group:

- [] for the trivial group;
- $[n]$ for a cyclic group of order $n > 1$;
- $[n_1, n_2]$ with $n_1 \mid n_2$ for a product of non-trivial cyclic groups of orders n_1 and n_2.

For $K = \mathbb{Q}$ the possible torsion structures are $[n]$ for $n \leq 10$ and $n = 12$, and $[2, 2n]$ for $n = 1, 2, 3, 4$.

3.95 Twists of elliptic curves

Definition. A **twist** of an elliptic curve E defined over a field K is another elliptic curve E', also defined over K, which is isomorphic to E over the algebraic closure of K.

Two elliptic curves are twists if an only if they have the same j-invariant.

For elliptic curves E with $j(E) \neq 0, 1728$, the only twists of E are its **quadratic twists** $E^{(d)}$. Provided that the characteristic of K is not 2, the nontrivial quadratic twists of E are in bijection with the nontrivial elements d of $K^*/(K^*)^2$, and $E^{(d)}$ is isomorphic to E over the quadratic extension $K(\sqrt{d})$.

Over fields of characteristic not 2 or 3, elliptic curves with j-invariant 1728 also admit **quartic twists**, parametrised by $K^*/(K^*)^4$, and elliptic curves with j-invariant 0 also admit **sextic twists**, parametrised by $K^*/(K^*)^6$. Elliptic curves E over fields K of characteristic 2 and 3 with $j(E) = 0 = 1728$ have nonabelian automorphism groups, and their twists are more complicated to describe, being in all cases parametrised by $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}(E))$.

Elliptic curve twists are a special case of twists of abelian varieties.

3.96 Weierstrass equation or model

Definition. A **Weierstrass equation** or **Weierstrass model** over a field k is a plane curve E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, a_2, a_3, a_4, a_6 \in k$.

The **Weierstrass coefficients** of this model E are the five coefficients a_i. These are often displayed as a list $[a_1, a_2, a_3, a_4, a_6]$.

It is common not to distinguish between the *affine* curve defined by a Weierstrass equation and its *projective closure*, which contains exactly one additional *point at infinity*, $[0 : 1 : 0]$.

A Weierstrass model is smooth if and only if its discriminant Δ is nonzero. In this case, the plane curve E together with the point at infinity as base point, define an elliptic curve defined over k.

Two smooth Weierstrass models define isomorphic elliptic curves if and only if they are isomorphic as Weierstrass models.

3.97 Isomorphism between Weierstrass models

Definition. Two Weierstrass models E, E' over a field K with Weierstrass coefficients $[a_1, a_2, a_3, a_4, a_6]$ and $[a'_1, a'_2, a'_3, a'_4, a'_6]$ are **isomorphic over** K if

there exist $u \in K^*$ and $r, s, t \in K$ such that

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2 a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3 a_3' &= a_3 + ra_1 + 2t, \\ u^4 a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6 a_6' &= a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned}$$

The set of transformations with parameters $[u, r, s, t] \in K^* \times K^3$ form the group of **Weierstrass isomorphisms**, which acts on both the set of all Weierstrass models over K and also on the subset of smooth models, preserving the point at infinity. The discriminants Δ, Δ' of the two models are related by

$$u^{12}\Delta' = \Delta.$$

In the smooth case such a Weierstrass isomorphism $[u, r, s, t]$ induces an isomorphism between the two elliptic curves E, E' they define. In terms of affine coordinates this is given by

$$(x, y) \mapsto (x', y')$$

where

$$\begin{aligned} x &= u^2 x' + r \\ y &= u^3 y' + su^2 x' + t \end{aligned}$$

4 Modular forms

4.1 Classical modular form

Definition. Let k be a positive integer and let Γ be a finite index subgroup of the modular group $\mathrm{SL}(2, \mathbb{Z})$.

A (classical) **modular form** f of weight k on Γ, is a holomorphic function defined on the upper half plane $\mathcal{H}$, which satisfies the transformation property

$$f(\gamma z) = (cz + d)^k f(z)$$

for all $z \in \mathcal{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and is holomorphic at all the cusps of Γ.

If Γ contains the principal congruence subgroup $\Gamma(N)$ then f is said to be a modular form of level N.

For each fixed choice of k and Γ the set of modular forms of weight k on G form a finite-dimensional $\mathbb{C}$-vector space denoted $M_k(\Gamma)$.

For the congruence subgroup $\Gamma_1(N)$ the space $M_k(\Gamma_1(N))$ decomposes as a direct sum of subspaces $M_k(N, \chi)$ over the group of Dirichlet characters χ of modulus N, where $M_k(N, \chi)$ is the subspace of forms $f \in M_k(N)$ that satisfy

$$f(\gamma z) = \chi(d)(cz + d)^k f(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(N)$.

Elements of $M_k(N, \chi)$ are said to be modular forms of weight k, level N, and character χ.

For trivial character χ of modulus N we have $M_k(N, \chi) = M_k(\Gamma_0(N))$.

4.2 Analytic conductor of a classical newform

Definition. The **analytic conductor** of a newform $f \in S_k^{\text{new}}(N, \chi)$ is the positive real number

$$N \left(\frac{\exp(\psi(k/2))}{2\pi} \right)^2,$$

where $\psi(x) := \Gamma'(x)/\Gamma(x)$ is the logarithmic derivative of the Gamma function.

4.3 Analytic rank

Definition. The **analytic rank** of a cuspidal modular form f is the analytic rank of the L-function

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s}$$

where the a_n are the complex coefficients that appear in the q-expansion of the modular form: $f(z) = \sum_{n\geq 1} a_n q^n$, where $q = e^{2\pi i z}$.

The complex coefficients a_n depend on a choice of embedding of the coefficient field of f into the complex numbers. It is conjectured that the analytic rank does not depend on this choice, and this conjecture has been verified for all classical modular forms stored in the LMFDB.

In general, analytic ranks of L-functions listed in the LMFDB are upper bounds that are believed (but not proven) to be tight.

For modular forms, the analytic ranks listed in the LMFDB are provably correct whenever the listed analytic rank is 0, or the listed analytic rank is 1 and the modular form is self dual (in the self dual case the sign of the functional equation determines the parity of the analytic rank).

4.4 Artin field

Definition. The **Artin field** of a weight one newform is the number field fixed by the kernel of its associated Galois representation $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$.

This number field is typically identified as the Galois closure of a sibling subfield with minimal degree and absolute discriminant.

4.5 Artin image

Definition. The **Artin image** of a weight one newform is the image of its associated Galois representation $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$.

The Artin image is a finite subgroup of $\mathrm{GL}_2(\mathbb{C})$ whose cardinality is equal to the degree of the Artin field.

4.6 Atkin-Lehner involution w_Q

Definition. Let N be a positive integer, and let Q be a positive divisor of N satisfying $\gcd(Q, N/Q) = 1$. Then there exist $x, y, z, t \in \mathbb{Z}$ for which the matrix

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qt \end{pmatrix}$$

has determinant Q. The matrix W_Q normalizes the group $\Gamma_0(N)$, and for any weight k it induces a linear operator w_Q on the space of cusp forms $S_k(\Gamma_0(N))$ that commutes with the Hecke operators T_p for all $p \nmid Q$ and acts as its own inverse.

The linear operator w_Q does not depend on the choice of x, y, z, t and is called the **Atkin-Lehner involution** of $S_k(\Gamma_0(N))$. Any cusp form f in $S_k(\Gamma_0(N))$ which is an eigenform for all T_p with $p \nmid N$ is also an eigenform for w_Q, with eigenvalue ± 1.

The matrix W_Q induces an automorphism of the modular curve $X_0(N)$ that is also denoted w_Q.

In the case $Q = N$, the Atkin-Lehner involution w_N is also called the Fricke involution.

4.7 Bad prime

Definition. A **bad prime** for a modular form f is a prime dividing the level of f.

A **good prime** is a prime that is not a bad prime. In other words, a prime that does not divide the level.

4.8 Character of a modular form

Definition. The **character** of an elliptic modular form f of weight k for the group Γ is the Dirichlet character χ that appears in its transformation under the action of the defining group Γ. Namely,

$$f(\gamma z) = \chi(d)(cz + d)^k f(z)$$

for any $z \in \mathcal{H}$ and $\gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma$. Here Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing the principal congruence subgroup $\Gamma(N)$, and χ is a character mod N.

4.9 CM form

Definition. A classical modular form is said to have **complex multiplication** if it admits a self twist by the Kronecker character of an imaginary quadratic field.

4.10 Coefficient field for newforms

Definition. The **coefficient field** of a modular form is the subfield of $\mathbb{C}$ generated by the coefficients a_n of its q-expansion $\sum a_n q^n$. The space of cusp forms $S_k^{\mathrm{new}}(N, \chi)$ has a basis of modular forms that are simultaneous eigenforms for all Hecke operators and with algebraic Fourier coefficients. For such eigenforms the coefficient field will be a number field, and Galois conjugate eigenforms will

share the same coefficient field. Moreover, if m is the smallest positive integer such that the values of the character χ are contained in the cyclotomic field $\mathbb{Q}(\zeta_m)$, the coefficient field will contain $\mathbb{Q}(\zeta_m)$ For eigenforms, the coefficient field is also known as the **Hecke field**.

4.11 Coefficient ring

Definition. The **coefficient ring** of a modular form is the subring $\mathbb{Z}[a_1, a_2, a_3, \ldots]$ of $\mathbb{C}$ generated by the coefficients a_n of its q-expansion $\sum a_n q^n$. In the case of a newform the coefficients a_n are algebraic integers and the coefficient ring is a finite index subring of the ring of integers of the coefficient field of the newform. It is also known as the **Hecke ring**, since the a_n are eigenvalues of Hecke operators.

4.12 Congruence subgroup

Definition. A **congruence subgroup** Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup that contains a **principal congruence subgroup** $\Gamma(N) := \ker\left(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right)$ for some $N \geq 1$. The least such N is the **level** of Γ.

4.13 Cuspidal modular form

Definition. Let k be a positive integer and let Γ be a finite index subgroup of the modular group $\mathrm{SL}(2, \mathbb{Z})$.

A **cusp form** of weight k on Γ is a modular form $f \in M_k(\Gamma)$ that vanishes at all cusps of Γ. In particular, the constant term in the Fourier expansion of f about any cusp is zero.

The cusp forms in $M_k(\Gamma)$ form a subspace $S_k(\Gamma)$. For each Dirichlet character χ of modulus N the cusp forms in $M_k(N, \chi)$ form a subspace $S_k(N, \chi)$; these are the cusp forms of weight k, level N, and character χ.

4.14 Decomposition into newforms

Definition. The Hecke algebra acts on $S_k^{\mathrm{new}}(N,\chi)$, breaking it up into irreducible pieces. Each piece is spanned by a set of conjugate eigenforms with Fourier coefficients in a number field of degree equal to the dimension of the subspace. We refer to an irreducible orbit as a **newform**.

4.15 Defining polynomial

Definition. The coefficient field of a modular form is a number field. A **defining polynomial** for this number field is explicitly recorded, because some of the data associated to the modular form will be expressed in terms of roots of this polynomial.

4.16 Dimension

Definition. The **dimension** of a space of modular forms is its dimension as a complex vector space; for spaces of newforms $S_k^{\mathrm{new}}(N,\chi)$ this is the same as the dimension of the $\mathbb{Q}$-vector space spanned by its eigenforms.

The **dimension** of a newform refers to the dimension of its newform subspace, equivalently, the cardinality of its newform orbit. This is equal to the degree of its coefficient field (as an extension of $\mathbb{Q}$).

The **relative dimension** of $S_k^{\mathrm{new}}(N,\chi)$ is its dimension as a $\mathbb{Q}(\chi)$-vector space, where $\mathbb{Q}(\chi)$ is the field generated by the values of χ, and similarly for newform subspaces.

4.17 Distinguishing Hecke operators

Definition. For a newspace $S_k^{\mathrm{new}}(N,\chi)$ we say that a set of Hecke operators $\mathcal{T} := \{T_{p_1},\dots,T_{p_r}\}$ **distinguishes** the newforms in the space if the sets $X_f(\mathcal{T})$ of characteristic polynomials of the $T_p \in \mathcal{T}$ acting on the subspace V_f spanned by

the Galois orbit of f in $S_k^{\mathrm{new}}(N,\chi)$ are distinct as f ranges over (non-conjugate) newforms in $S_k^{\mathrm{new}}(N,\chi)$.

The set $\mathcal{T}$ can be identified by a list of primes p. For convenience we restrict to primes p that do not divide the level N and list the unique ordered sequence of primes $p_1,\ldots,p_n$ for which the sequence of integers $c_1,\ldots,c_n$ defined by

$$c_m := \#\big\{X_f(\{T_{p_i} : i < m\}) : \text{newforms } f \in S_k^{\mathrm{new}}(N,\chi)\big\}$$

is strictly increasing. The length of the sequence $p_1,\ldots p_n$ is always less then the number of newforms in $S_k^{\mathrm{new}}(N,\chi)$ and we obtain the empty sequence when $S_k^{\mathrm{new}}(N,\chi)$ contains just one newform.

4.18 Dual cuspform

Definition. The **dual** of a cuspidal modular form f is the form whose coefficients a_n in its q-expansion are the complex conjugates of those of f. The L-function of the dual form is the dual of the L-function of f.

The coefficient field of a non-self-dual newform is a CM field.

4.19 Holomorphic Eisenstein series of level 1

Definition. For an even integer $k \geq 4$, we define the (normalized) holomorphic **Eisenstein series** of level 1

$$E_k(z) = \frac{1}{2\zeta(k)} \sum_{(c,d)\neq(0,0)} (cz+d)^{-k} = \sum_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in\, \Gamma_\infty\backslash \mathrm{SL}(2,\mathbb{Z})} (cz+d)^{-k},$$

where $\Gamma_z = \{\gamma \in \Gamma : \gamma z = z\}$ is the **isotropy group** of the cusp z.

The Eisenstein series E_k are modular forms of weight k and level 1 on the

modular group.

They have the following q-expansion:

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n,$$

where the B_k are the Bernoulli numbers, $\sigma_{k-1}(n)$ is a divisor function, and $q = e^{2\pi i z}$.

4.20 Embedding of a modular form

Definition. The coefficients in the q-expansion $\sum a_n q^n$ of a newform f are algebraic integers that generate the coefficient field $\mathbb{Q}(f)$ of f.

Each embedding $\iota\colon \mathbb{Q}(f) \to \mathbb{C}$ gives rise to a modular form $\iota(f)$ with q-expansion $\sum \iota(a_n) q^n$; the modular form $\iota(f)$ is an **embedding** of the newform f.

Distinct embeddings give rise to modular forms that lie in the same galois orbit but have distinct L-functions $L(s) := \sum \iota(a_n) n^{-s}$.

If f is a newform of character χ, each embedding $\mathbb{Q}(f) \to \mathbb{C}$ induces an embedding $\mathbb{Q}(\chi) \to \mathbb{C}$ of the value field of χ. The embeddings of f may be grouped into blocks with the same Dirichlet character; distinct blocks correspond to modular forms with distinct (but Galois conjugate) Dirichlet characters.

4.21 Complex embedding label

Definition. The **label** complex embedded holomorphic cusp form f is $N.k.a.x.c.j$ (sometimes shortened as $a.j$), where

- N is the level,
- k is the weight,

- $N.a$ is the label of the Galois orbit of the Dirichlet character,
- x is the Hecke Galois orbit label,
- $N.c$ is the Conrey label for the character corresponding to the embedding, and
- j is the index for the embedding within those with the same Dirichlet character, these are ordered by the vector $\iota(a_n)$, where we order the complex numbers first by their real part and then by their imaginary part.

4.22 Eta quotient

Definition. An **eta quotient** is any function f of the form

$$f(z) = \prod_{1 \le i \le s} \eta^{r_i}(m_i z),$$

where $m_i \in \mathbb{N}$ and $r_i \in \mathbb{Z}$ and $\eta(z)$ is the Dedekind eta function.

An **eta product** is an eta quotient in which all the r_i are non-negative.

4.23 Fourier coefficients of a modular form

Definition. Let f be a modular form on a finite index subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, and suppose Γ contains the matrix $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then f is periodic with period 1, so it has a Fourier expansion of the form

$$f(z) = \sum_{n \ge 0} a_n q^n,$$

where $q = e^{2\pi i z}$. That is the **Fourier expansion** of f around the cusp ∞, with **Fourier coefficients** a_n. If one says "the Fourier expansion of f", is it understood to refer to the expansion at ∞.

For other cusps of Γ, suppose w is the width of the cusp $\gamma\infty$, for some cusp representative γ. Then we can write f as $f(z) = g_\gamma(e^{2\pi iz/w})$ for some holomorphic function g_γ on the punctured unit disk. We can expand g as a Laurent series:

$$g_\gamma(q^{1/w}) = \sum_{n\geq 0} a_\gamma(n) q^{n/w} \quad \text{for} \quad 0 < |q| < 1.$$

We then define the **Fourier expansion** of f around the cusp $\gamma\infty$ to be

$$f(z) = \sum_{n\geq 0} a_\gamma(n) q^{n/w},$$

where $q = e^{2\pi iz}$.

The $a_\gamma(n)$ are called the **Fourier coefficients** of f with respect to the cusp $\gamma\infty$.

4.24 Fricke involution

Definition. The **Fricke involution** is the Atkin-Lehner involution w_N on the space $S_k(\Gamma_0(N))$ (induced by the corresponding involution on the modular curve $X_0(N)$).

For a newform $f \in S_k^{\text{new}}(\Gamma_0(N))$, the sign of the functional equation satisfied by the L-function attached to f is i^{-k} times the eigenvalue of ω_N on f. So, for example when $k = 2$, the signs swap, and the analytic rank of f is even when $w_N f = -f$ and odd when $w_N f = +f$.

4.25 Galois conjugate newforms

Definition. Two newforms $f = \sum a_n q^n$ and $g = \sum b_n q^n$ are **Galois conjugate** if there is an automorphism $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $b_n = \sigma(a_n)$ for all $n \geq 1$, in which case we write $g = \sigma(f)$.

The set $\{\sigma(f) : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}$ of all Galois conjugates of f is the Galois orbit of f; it has cardinality equal to the dimension of f, equivalently, the degree of its coefficient field

4.26 Galois orbit of a newform

Definition. The **Galois orbit** of a newform $f \in S_k^{\mathrm{new}}(N, \chi)$ is the finite set

$$[f] := \{\sigma(f) : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}$$

of its Galois conjugates, which forms a canonical $\mathbb{Q}$-basis for the corresponding newform subspace.

Galois orbits of newforms are also called **newform orbits**.

4.27 Galois representation

Definition. As shown by Deligne and Serre [**?**], every newform of weight one has an associated **Galois representation** $\rho\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$.

This representation corresponds to an Artin representation of dimension two whose conductor is the level N of the modular form.

Conversely, every odd irreducible two-dimensional Artin representation of conductor N gives rise to a modular form of weight one and level N.

Composing the representation ρ with the natural map $\mathrm{GL}_2(\mathbb{C}) \to \mathrm{PGL}_2(\mathbb{C})$ yields the **projective Galois representation** $\bar{\rho}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{C})$.

4.28 Hecke operator

Definition. Let f be a modular form of weight k, level N, and character χ.

For each positive integer n the **Hecke operator** T_n is a linear operator on the

vector space $M_k(N,\chi)$ whose action on $f \in M_k(N,\chi)$ can be defined as follows. If $f(z) = \sum a_n(f)q^n$ is the q-expansion of $f \in M_k(N,\chi)$, where $q = e^{2\pi iz}$, then the q-expansion of $T_n f \in M_k(N,\chi)$ has coefficients

$$a_m(T_n f) := \sum_{d \mid \gcd(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f).$$

The Hecke operators pairwise commute, and when restricted to the subspace $S_k(N,\chi)$ of cusp forms, they commute with their adjoints with respect to the Petersson scalar product. This implies that $S_k(N,\chi)$ has a canonical basis whose elements are eigenforms for all the Hecke operators. If we normalize such an eigenform $f(z) = \sum a_n q^n$ so that $a_1 = 1$, then for all $n \geq 1$ we have

$$T_n f = a_n f.$$

The newspace $S_k^{\text{new}}(N,\chi) \subseteq S_k(N,\chi)$ is invariant under the action of the Hecke operators, so the canonical basis of normalized eigenforms for $S_k(N,\chi)$ includes a basis of newforms for $S_k^{\text{new}}(N,\chi)$.

4.29 Hecke orbit

Definition. The **Hecke orbit** of a cusp form f in $S_k(N,\chi)$ is defined as the space generated by $T_p(f)$ for all Hecke operators T_p for p coprime to the level.

4.30 Coefficient ring generator bound

Definition. The **coefficient ring generator bound** of a newform with q-expansion $\sum a_n q^n$ is the least positive integer n such that $\mathbb{Z}[a_1, \ldots, a_n]$ is the entire coefficient ring $\mathbb{Z}[a_1, a_2, a_3, \ldots]$.

4.31 Hecke characteristic polynomial

Definition. The **Hecke characteristic polynomial** of a newform f at a prime p is the characteristic polynomial of the Hecke operator T_p acting on the newform subspace V_f.

4.32 Inner twist

Definition. Galois conjugate newforms f and g are **inner twists** if there is a Dirichlet character χ such that

$$a_p(g) = \chi(p)a_p(f)$$

for all but finitely many primes p. Without loss of generality, we may assume that χ is a primitive Dirichlet character, and by a theorem of Ribet [**?**, **?**], the newform g is conjugate to f via a $\mathbb{Q}$-automorphism σ of the coefficient field of f. The set of pairs (χ, σ) form the group of inner twists of f.

Each pair (χ, σ) corresponding to an inner twist of f is uniquely determined by the the primitive character χ, and we say that f admits an inner twist by χ. When $\sigma = 1$ is is the trivial automorphism, we have $g = f$ and say that f admits a self twist by χ; in this case χ is either the trivial character or the Kronecker character of a quadratic field.

The number of inner twists of f is an invariant of its Galois orbit, as is the number of inner twists by characters in any particular Galois orbit of Dirichlet characters.

The home page of each newform in the LMFDB includes a list of inner twists, in which non-trivial self twists are distinguished by listing the associated quadratic field (the CM or RM field), while inner twists that are not self twists are simply marked as "inner".

4.33 Inner twist count

Definition. The **inner twist count** of a newform f is the number of distinct inner twists of f.

Associated to each inner twist is a pair (χ, σ), where χ is a primitive Dirichlet character and σ is a $\mathbb{Q}$-automorphism of the coefficient field of f.

Pairs with $\sigma = 1$ are self twists $(\chi, 1)$, including the pair $(1, 1)$ corresponding to the twist of f by the trivial character; self twists are included in the count of inner twists.

The set of pairs (χ, σ) forms the group of inner twists; the inner twist count is the cardinality of this group.

Not all of the inner twists included in the inner twist count have necessarily been proved; those that have are explicitly identified in the table of inner twists on the newforms home page. In cases where not every inner twist has been proved the inner twist should be viewed as a rigorous upper bound that is believed to be tight.

Inner twist data is available only for newforms for which exact eigenvalue data has been computed; this includes all newforms of dimension up to 20 and all newforms of weight 1; when the inner twist count is specified in a search the results include only newforms for which inner twists have been computed.

4.34 Inner twist multiplicity

Definition. It is possible for a newform f to admit an inner twist by more than one Dirichlet character φ in the same Galois orbit. Different embeddings of f into $\mathbb{C}$ will yield different φ, but the number of such φ is the same for every embedding; this number is the **multiplicity**.

4.35 Label of a classical modular form

Definition. The **label** of a newform $f \in S_k^{\mathrm{new}}(N, \chi)$ has the format $N.k.a.x$, where

- N is the level;
- k is the weight;
- $N.a$ is the label of the Galois orbit of the Dirichlet character χ;
- x is the label of the Galois orbit of the newform f.

For each embedding of the coefficient field of f into the complex numbers, the corresponding modular form over $\mathbb{C}$ has a label of the form $N.k.a.x.n.i$, where

- n determines the Conrey label $N.n$ of the Dirichlet character χ;
- i is an integer ranging from 1 to the relative dimension of the newform that distinguishes embeddings with the same character χ.

4.36 Level of a modular form

Definition. A **level** of a modular form f is a positive integer N such that f is a modular form on a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ that contains the principal congruence subgroup $\Gamma(N)$.

The **level** of a newform is the least such integer N.

4.37 Maximal newform

Definition. A newform is **maximal** if its Galois orbit spans the ambient subspace that contains it (its Atkin-Lehner subspace when the character is trivial, the entire newspace otherwise).

A newform is the **largest** newform in its ambient subspace if its dimension is strictly larger than that of any other newform in the same subspace (this includes newforms that are maximal).

4.38 Minimal modular form

Definition. A modular form is **minimal** if it is not a twist of a form of lower level.

4.39 Minimal twist

Definition. The **minimal twist** of a newform f is the twist g of f whose label is lexicographically minimal among all twists of f that are both twist minimal and have minimal character χ.

A key feature of the minimal twist g (and more generally, of any twist minimal g of level N and minimal character χ) is that for any character ψ, the level M of the twist $g \otimes \psi$ can be computed as $M = \mathrm{lcm}(N, \mathrm{cond}(\psi)\mathrm{cond}(\chi\psi))$.

4.40 Minus space

Definition. The **minus subspace** of $S_k(\Gamma_0(N))$ is the eigenspace of the Fricke involution w_N with eigenvalue -1.

4.41 Newform

Definition. A **newform** is a cusp form $f \in S_k^{\mathrm{new}}(N, \chi)$ in the new subspace that is also an eigenform of all Hecke operators, normalized so that the q-expansion $f(z) = \sum a_n q^n$, where $q = e^{2\pi i z}$, begins with the coefficient $a_1 = 1$. The newforms are a basis for the new subspace.

4.42 Newform subspace

Definition. The **newform subspace** of a newform f in $S_k^{\text{new}}(N, \chi)$ is the subspace generated by $T_p(f)$ for all Hecke operators T_p for p coprime to the level, equivalently, the subspace generated by the Galois conjugates of f.

Every newspace has a canonical decomposition into newform subspaces.

4.43 New subspace

Definition. The space $S_k(N, \chi)$ of cuspidal modular forms of level N, weight k, and character χ can be decomposed

$$S_k(N, \chi) = S_k^{\text{old}}(N, \chi) \oplus S_k^{\text{new}}(N, \chi)$$

into old and new subspaces, defined as follows.

If M is a proper divisor of N and χ_M is a Dirichlet character of modulus M that induces χ, then for all $d \mid (N/M)$, there is a map from $S_k(M, \chi_M) \to S_k(N, \chi)$ via $f(z) \mapsto f(dz)$. The span of the images of all of these maps is the **old subspace** $S_k^{\text{old}}(N, \chi) \subseteq S_k(N, \chi)$.

The **new subspace** $S_k^{\text{new}}(N, \chi)$ is the orthogonal complement of $S_k^{\text{old}}(N, \chi)$ with respect to the Petersson inner product.

A basis for the new subspace is given by newforms.

4.44 Nontrivial inner twist

Definition. An inner twist is **nontrivial** if it is not the self twist by the trivial character.

4.45 Old subspace of modular forms

Definition. Each space of $S_k(N,\chi)$ of cuspidal modular forms of weight k, level N, and character χ contains an **old** subspace $S_k^{\text{old}}(N,\chi)$ that can be expressed as a direct sum of spaces of newforms $S_k^{\text{new}}(N_i,\chi_i)$, where each N_i is a proper divisor of N divisible by the conductor of χ, and each χ_i is the unique character of modulus N_i induced by the primitive character that induces χ.

This decomposition arises from the injective maps

$$\begin{aligned} \iota_d \colon S_k(N_i,\chi_i) &\to S_k(N,\chi) \\ f &\mapsto f(d\tau) \end{aligned}$$

that exist for each divisor d of N/N_i. The image of each ι_d is isomorphic to $S_k(N_i,\chi_i)$, and we have the decomposition

$$S_k(N,\chi) \simeq \bigoplus_{\text{cond}(\chi)\mid N_i \mid N} S_k^{\text{new}}(N_i,\chi_i)^{\oplus m_i},$$

where m_i is the number of divisors of N/N_i. Restricting the direct sum to proper divisors N_i of N yields a decomposition for $S_k^{\text{old}}(N,\chi)$.

4.46 Petersson scalar product

Definition. Let f and g be two modular forms with respect to a finite index subgroup G of Γ. When it exists, we define the **Petersson scalar product** of f and g with respect to the group G by

$$\langle f,g\rangle_G = \frac{1}{[\Gamma : G]} \int_{\mathfrak{F}} f(z)\overline{g(z)} y^k d\mu,$$

where $\mathfrak{F}$ is a fundamental domain for G and $d\mu = dxdy/y^2$ is the measure associated to the hyperbolic metric.

Note that the Petersson scalar product exists if at least one of f, g is a cusp

form.

4.47 Plus space

Definition. The **plus subspace** of $S_k(\Gamma_0(N)$ is the eigenspace of the Fricke involution ω_N with eigenvalue 1.

4.48 Projective field

Definition. The **projective field** of a weight one newform is the number field fixed by the kernel of its associated projective Galois representation $\bar{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{C})$.

This number field is typically identified as the Galois closure of a sibling subfield with minimal degree and absolute discriminant.

4.49 Projective image

Definition. The **projective image** of a weight one newform is the image of its associated projective Galois representation $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{C})$. It is a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ that can be classified as one of four **types**: It is either isomorphic to a dihedral group D_n for some integer $n \geq 2$ (where $D_2 := C_2 \times C_2$ is the Klein group), or to one of A_4, S_4, A_5, where A_n and S_n respectively denote the alternating and symmetric groups on n letters.

4.50 q-expansion of a modular form

Definition. The **q-expansion** of a modular form $f(z)$ is its Fourier expansion at the cusp $z = i\infty$, expressed as a power series $\sum_{n=0}^{\infty} a_n q^n$ in the variable $q = e^{2\pi i z}$.

For cusp forms, the constant coefficient a_0 of the q-expansion is zero.

For newforms, we have $a_1 = 1$ and the coefficients a_n are algebraic integers in a number field $K \subseteq \mathbb{C}$.

Accordingly, we define the **q-expansion** of a newform orbit $[f]$ to be the q-expansion of any newform f in the orbit, but with coefficients $a_n \in K$ (without an embedding into $\mathbb{C}$). Each embedding $K \hookrightarrow \mathbb{C}$ then gives rise to an embedded newform whose q-expansion has $a_n \in \mathbb{C}$, as above.

4.51 Relative dimension

Definition. The **relative dimension** of a newform in a space of modular forms $S_k^{\mathrm{new}}(\Gamma_0(N), \chi)$ is the dimension of its coefficient field as an extension of the character field $\mathbb{Q}(\chi)$ (the number field generated by the values of χ).

4.52 Real multiplication

Definition. A modular form is said to have **real multiplication** if it admits a self twist by the Kronecker character of a real quadratic field.

Only modular forms of weight one can have real multiplication.

4.53 Satake Angles

Definition. The **Satake angles** $\theta_p = \arg \alpha_p \in [-\pi, \pi]$ are the arguments of a complex embedding of the Satake parameters α_p.

4.54 Satake parameters

Definition. Let f be newform of level N, weight k and character χ. Let p be a good prime, i.e., $p \nmid N$.

The **Satake parameters** α_p are the reciprocal roots of $L_p\left(p^{-(k-1)/2}t\right)$, where

$$L_p(t) = 1 - a_p t + \chi(p)p^{k-1}t^2 = \det(1 - t\,T_p) = (1 - \alpha_p p^{\frac{k-1}{2}}t)(1 - \alpha_p^{-1}\chi(p)p^{\frac{k-1}{2}}t),$$

T_p is Hecke operator, and a_p its trace.

4.55 Sato-Tate group of a modular form

Definition. The **Sato-Tate group** of a newform is a compact Lie group that one can attach to the Galois representation associated to the newform.

For newforms of weight $k = 1$, the Sato-Tate group is simply the image of the corresponding 2-dimensional Artin representation, a finite subgroup of $\mathrm{SL}_2(\mathbb{C})$.

For newforms of weight $k > 1$ the Sato-Tate group is a subgroup of $\mathrm{U}(2)$ whose identity component is either $\mathrm{SU}(2)$ (for newforms without CM) or $\mathrm{U}(1)$ (for CM newforms) diagonally embedded in $\mathrm{U}(2)$.

The Sato-Tate conjecture implies that as $p \to \infty$ the limiting distribution of normalized Hecke eigenvalues $a_p/p^{(k-1)/2}$ converges to the trace distribution induced by the Haar measure of the Sato-Tate group.

The Sato-Tate conjecture for classical modular forms has been proved [**?**, **?**].

4.56 Self-twist

Definition. A newform f admits a **self-twist** by a primitive Dirichlet character χ if the equality

$$a_p(f) = \chi(p)a_p(f)$$

holds for all but finitely many primes p.

For non-trivial χ this can hold only when χ has order 2 and $a_p = 0$ for all primes p not dividing the level of f for which $\chi(p) = -1$. The character χ is

then the Kronecker character of a quadratic field K and may be identified by the discriminant D of K.

If D is negative, the modular form f is said to have complex multiplication (CM) by K, and if D is positive, f is said to have real multiplication (RM) by K. The latter can occur only when f is a modular form of weight 1 whose projective image is dihedral.

It is possible for a modular form to have multiple non-trivial self twists; this occurs precisely when f is a modular form of weight one whose projective image is isomorphic to $D_2 := C_2 \times C_2$; in this case f admits three non-trivial self twists, two of which are CM and one of which is RM.

4.57 Self dual modular form

Definition. A cuspidal modular form f is said to be **self dual** if the coefficients a_n that appear in its q-expansion are real numbers; equivalently, the L-function of the modular form is self dual.

The coefficient field of a newform is either a totally real number field or a CM field, depending on whether the newform is self dual or not.

4.58 Shimura correspondence

Definition. Let k be an odd integer, and let N a positive integer divisible by 4. Let χ be a character modulo N. Let t be a square-free integer. The **Shimura correspondence** is the linear map $Sh_t : S_{k/2}(N, \chi) \to S_{k-1}(N/2, \chi^2)$ defined by the equation

$$L(s, Sh_t(g)) = L(\chi_t, s + 1 - \lambda) \cdot \sum_{n \geq 1} a_{tn^2} n^{-s},$$

where

- $\lambda = (k-1)/2$.
- χ_t is the character given by $\chi_t(m) = \chi(m)\left(\frac{-1}{m}\right)\left(\frac{t}{m}\right)$.
- $g(z) = \sum_{n\geq 1} a_n q^n$ is the q-expansion of g.

This map is Hecke linear. If $k \geq 5$, it takes cusp forms to cusp forms.

4.59 Spaces of modular forms

Definition. The **space** of modular forms of level N, weight k, and character χ is denoted $M_k(N, \chi)$.

The space $M_k(N, \chi)$ is a finite-dimensional complex vector space which further decmoposes into subspaces. In particular, we have a subspace of cusp forms $S_k(N, \chi) \subseteq M_k(N, \chi)$.

4.60 Trace form

Definition. The **trace form** of a newspace $S_k(N, \chi)$ is the modular form obtained by summing its canonical basis of newforms.

4.61 Stark unit of a newform of weight one

Definition. Stark's conjecture applied to the associated Galois representation of a newform $f(z) = \sum a_n q^n$ of weight one [**?**] states the following. Let $E = \mathbb{Q}((a_n)_{n\in\mathbb{N}})$, $\Delta = \mathrm{Gal}(E/\mathbb{Q})$ and $f^\alpha(z) = \sum \alpha(a_n)q^n$ for $\alpha \in \Delta$. Let $L(s, f)$ be the L-function of f. Then, for all $b \in E^*$ there exists an integer $m \geq 1$ and a unit ε in the Artin field of f, called the **Stark unit**, such that

$$e^{m\sum_{\alpha\in\Delta}\alpha(b)L'(0,f^\alpha)} = \varepsilon$$

In the case where the coefficients of $\mathrm{Tr}(bf)$ are in $\mathbb{Z}$, Chinburg further conjectured that there exists a Stark unit for $m = 1$ [**?**]. Notice that if we choose $b = 1$, the preceding condition always holds. Here, we compute the Stark unit of the newform for $b = 1$ and $m = 1$.

4.62 Sturm bound

Definition. The **Sturm bound** is an upper bound on the least index where the coefficients of the Fourier expansions of distinct modular forms in the same space $M_k(N, \chi)$ must differ.

More precisely, for any space $M_k(N, \chi)$ of modular forms of weight k, level N, and character χ, the Sturm bound is the integer

$$B(M_k(N, \chi)) := \left\lfloor \frac{km}{12} \right\rfloor,$$

where

$$m := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

If $f = \sum_{n\geq 0} a_n q^n$ and $g = \sum_{n\geq 0} b_n q^n$ are elements of $M_k(N, \chi)$ with $a_n = b_n$ for all $n \leq B(M_k(N, \chi))$ then $f = g$; see Corollary 9.20 in [**?**, **?**] for $k > 1$ and Lemma 5 in [**?**] for $k = 1$.

The Sturm bound applies, in particular, to newforms of the same level, weight, and character. Better bounds for newforms are known in certain cases (see Corollary 9.19 and Theorem 9.21 in [**?**, **?**], for example), but for consistency we always take the Sturm bound to be the integer $B(M_k(N, \chi))$ defined above.

Note that the Sturm bound for $S_k^{\mathrm{new}}(N, \chi)$ does not apply (in general) to the space

$$S_k^{\mathrm{new}}(N, [\chi]) := \bigoplus_{\chi' \in [\chi]} S_k^{\mathrm{new}}(N, \chi')$$

associated to the Galois orbit $[\chi]$; rather, it applies to each direct summand

$S_k^{\mathrm{new}}(N,\chi')$.

4.63 Sturm bound for $\Gamma_1(N)$

Definition. The **Sturm bound** is an upper bound on the least index where the coefficients of the Fourier expansions of distinct modular forms in the same space must differ.

More precisely, for any space $M_k(\Gamma_1(N))$ of modular forms of weight k and level N, the Sturm bound is the integer

$$B(M_k(\Gamma_1(N))) := \left\lfloor \frac{km}{12} \right\rfloor,$$

where

$$m := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right).$$

If $f = \sum_{n\geq 0} a_n q^n$ and $g = \sum_{n\geq 0} b_n q^n$ are elements of $M_k(\Gamma_1(N))$ with $a_n = b_n$ for all $n \leq B(M_k(\Gamma_1(N)))$ then $f = g$; see Corollary 9.19 in [**?**, **?**] for $k > 1$.

The Sturm bound applies, in particular, to newforms of the same level and weight. Better bounds for newforms are known in certain cases (see Corollary 9.19 and Theorem 9.21 in [**?**, **?**], for example), but for consistency we always take the Sturm bound to be the integer $B(M_k(\Gamma_1(N)))$ defined above.

4.64 Subspaces of modular forms

Definition. The space $M_k(N,\chi)$ of modular forms of level N, weight k, and character χ can be decomposed as

$$M_k(N,\chi) = E_k(N,\chi) \oplus S_k(N,\chi)$$

where $E_k(N,\chi)$ is the Eisenstein subspace (the span of Eisenstein series) and $S_k(N,\chi)$ the subspace of cusp forms.

These spaces further decompose into old and new subspaces as follows. If M is a proper divisor of N and χ_M is a Dirichlet character of modulus M that induces χ, then for every divisor $d \mid (N/M)$, there is a map from $M_k(M, \chi_M) \to M_k(N, \chi)$ via $f(z) \mapsto f(dz)$. The span of the images of all of these maps is the **old subspace** $M_k^{\mathrm{old}}(N, \chi) \subseteq M_k(N, \chi)$.

The cuspidal subspace decomposes as

$$S_k(N, \chi) = S_k^{\mathrm{new}}(N, \chi) \oplus S_k^{\mathrm{old}}(N, \chi)$$

where the **new subspace** $S_k^{\mathrm{new}}(N, \chi)$ is the orthogonal complement of $S_k^{\mathrm{old}}(N, \chi)$ with respect to the Petersson inner product.

The Eisenstein subspace similarly decomposes as

$$E_k(N, \chi) = E_k^{\mathrm{new}}(N, \chi) \oplus E_k^{\mathrm{old}}(N, \chi)$$

where $E_k^{\mathrm{new}}(N, \chi)$ is the span of those Eisenstein series attached to a pair (χ_1, χ_2) of (primitive) characters of conductor N.

4.65 Trace bound

Definition. The **trace bound** for a space of newforms $S_k^{new}(N, \chi)$ is the least positive integer m such that taking traces down to $\mathbb{Q}$ of the coefficients a_n for $n \leq m$ suffices to distinguish all the Galois orbits of newforms in the space; here a_n denotes the nth coefficient of the q-expansion $\sum a_n q^n$ of a newform.

If the newforms in the space all have distinct dimensions then the trace bound is 1, because the trace of $a_1 = 1$ from the coefficient field of the newform down to $\mathbb{Q}$ is equal to the dimension of its Galois orbit.

4.66 Trace form

Definition. For a newform $f \in S_k^{\mathrm{new}}(\Gamma_1(N))$, its **trace form** $\mathrm{Tr}(f)$ is the sum of its distinct conjugates under $\mathrm{Aut}(\mathbb{C})$ (equivalently, the sum under all embeddings of the coefficient field into $\mathbb{C}$). The trace form is a modular form $\mathrm{Tr}(f) \in S_k^{\mathrm{new}}(\Gamma_1(N))$ whose q-expansion has integral coefficients $a_n(\mathrm{Tr}(f)) \in \mathbb{Z}$.

The coefficient a_1 is equal to the dimension of the newform.

For p prime, the coefficient a_p is the trace of Frobenius in the direct sum of the ℓ-adic Galois representations attached to the conjugates of f (for any prime ℓ). When f has weight $k = 2$, the coefficient $a_p(f)$ is the trace of Frobenius acting on the modular abelian variety associated to f.

For a newspace $S_k^{\mathrm{new}}(N, \chi)$, its trace form is the sum of the trace forms $\mathrm{Tr}(f)$ over all newforms $f \in S_k^{\mathrm{new}}(N, k)$; it is also a modular form in $S_k^{\mathrm{new}}(\Gamma_1(N))$.

The graphical plot displayed in the properties box on the home page of each newform or newspace is computed using the trace form.

4.67 Twist

Definition. Associated to each newform f and primitive Dirichlet character ψ, there is a unique newform $g := f \otimes \psi$, the **twist** of f by ψ, that satisfies

$$a_n(g) = \psi(n) a_n(f)$$

for all integers $n \geq 1$ coprime to N and the conductor of ψ. The newforms f and g are then **twist equivalent**. When g is a Galois conjugate of f, it is said to be an inner twist.

The newform orbit $[g]$ is a **twist** of the newform orbit $[f]$ by the character orbit $[\psi]$ if some $g \in [g]$ is a twist of f by some ψ in $[\psi]$. This may occur with

multiplicity.

Twist equivalence is an equivalence relation. The **twist class** of a newform or newform orbit is its equivalence class under this relation.

In the LMFDB each twist class is identified by the label of its minimal twist.

4.68 Twist minimal

Definition. A newform f is **twist minimal** if its level achieves the minimum within its twist class.

A twist minimal newform f need not have minimal character, but if this is not the case there will be a twist of f that is both twist minimal and has minimal character.

In the LMFDB, the designated representative of each twist class is the twist minimal newform g of minimal character whose label is lexicographically minimal among all such newforms. This newform g is called the **minimal twist** of the newforms in its twist equivalence class and is identified by a checkmark (✓) in tables of twists.

These conventions also apply to newform orbits.

4.69 Twist multiplicity

Definition. The **multiplicity** of a newform orbit $[g]$ as a twist of a newform orbit $[f]$ by a primitive character orbit $[\psi]$ is the number of distinct $\psi \in [\psi]$ for which $f \otimes \psi \in [g]$. This number is the same for every $f \in [f]$ and depends only on the Galois orbits $[g]$, $[f]$, and $[\psi]$.

When g is an inner twist of f, this multiplicity is equal to the inner twist count of f.

4.70 Weight of an elliptic modular form

Definition. The **weight** of an elliptic modular form f is the integer or half-integer power of $(cz+d)$ that occurs in the modular transformation property of f under the action of $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on the upper half plane. That is, the weight is the number k in the transformation law

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z).$$