# Algebraic Geometry

Tim Dokchitser
(Thanks to Céline Maistret for copying notes in my absence)

Prerequisites**: Seen varieties; algebraic curves up to Riemann-Roch**
**Topics**:

- Review of varieties
- Algebraic graph and abelian varieties
- Families
- Moduli spaces
- Models of curves

## Part I
# Reviews of Varieties

## 1 Affine Varieties

The base field will be $k = \overline{k}$. Let $\mathbb{A}^k = k^n$ be the affine space, $f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \Rightarrow V = \{x \in \mathbb{A}^n | \text{all} f_i(x) = 0\}$, this is called a (Zariski) *closed set* (or closed affine algebraic set).

- $V_1 \cup V_2 = \{f_i = 0\} \cup \{g_j = 0\} = \{f_i g_j = 0\}$ also closed
- $\cap V_i$ closed (since $k(x_1, \ldots, x_n)$ is Noetherian)

Hence we have a (Zariski) topology.

**Definition 1.1.** An *(affine) variety* is an irreducible, non-empty, closed set. (Where irreducible means, if $V = V_1 \cup V_2$ closed, then $V = V_1$ or $V = V_2$)

Any closed sets is $\cup_{\text{finite}}$varieties

**Example.** Let $f \in k[x_1, \ldots, x_n]$ and non-constant. Then $V = \{f = 0\}$ called hypersurface. This is irreducible if and only if $f$ is irreducible.
Let $V \subseteq \mathbb{A}^1$ be closed, then $V = \emptyset, \mathbb{A}^1$or a finite set. This is a variety if and only if $V = \mathbb{A}^1$ or $V = \{\text{pt}\}$
Let $V \subseteq \mathbb{A}^2$ variety if and only if $V =\mathbb{A}^2$, irreducible curve $f(x, y) = 0$ or $\{\text{pt}\}$

*Note.* Very coarse: e.g., $\mathbb{A}^1$ homeomorphic to any other curve $f(x, y) = 0$.

## 1.1 Morphisms

**Definition 1.2.** A map $\mathbb{A}^n \supseteq V \to W \subseteq \mathbb{A}^m$ is a *morphism* (or *regular map*) if it is given by $x \mapsto (f_i(x))$ where $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$.

An *Isomorphism*: $\begin{tikzcd} V \arrow[r, shift left, "f"] & W \arrow[l, shift left, "g"] \end{tikzcd}$ and $f \cdot g = \mathrm{id} = g \cdot f$

A *regular function* is a morphism $f : V \to \mathbb{A}^1 = k$
$k[V] = \{\text{regular functions on } V\} = k[x_1, \ldots, x_n]/I$, where $I = \{f | f|_V \equiv 0\}$. This is a ring

$V$ is a variety if and only if $I$ is prime if and only if $k[V]$ is an integral domain

**Theorem 1.3.** *Let $V$ be closed sets consider the map to finitely generated $k$-algebras with no nilpotents (defined by $V \mapsto k[V]$ and inverse $f \mapsto f^*$), is an (anti) equivalence of categories. This maps refines to Varieties map to finitely generated integral $k$-algebras.*
*The other map is $A \to \operatorname{Spec} A$*

**Definition 1.4.** Let $V$ be a variety, the field of fractions of $k[v]$ is denoted by $k(v)$, and is called *field of rational functions.*
$\phi : V \rightsquigarrow W$ is a *rational map* if given by rational functions (defined on a dense open subset of $V$)

$V$ and $W$ are *birational* (equivalently $k(V) \cong k(W)$) if there exists $\begin{tikzcd} V \arrow[r, squiggly, shift left, "f"] & W \arrow[l, squiggly, shift left, "g"] \end{tikzcd}$ such that $f \cdot g = \mathrm{id} = g \cdot f$

**Example.** Let $V = \mathbb{A}^n$, then $k[V] = k[x_1, \ldots, x_n]$ and $k(V) = k(x_1, \ldots, x_n)$
Let $V : y^2 = x^3 + 1 \subset \mathbb{A}^2_{x,y}$ . Then $k[V] = k[x, y]/({}^2 - x^3 - 1)$, $k(V) = k(x)(\sqrt{x^3 + 1})$ $([k(V) : k(x)] = 2)$

**Note**: The image of a Variety is not a Variety in general.

**Example.** Take $\mathbb{A}^2 \to \mathbb{A}^1$ defined by $x, y \mapsto x$ then the variety $V : xy = 1$ maps to $\mathbb{A}^1 \setminus \{0\}$
Take $\mathbb{A}^2 \to \mathbb{A}^2$ defined by $(x, y) \mapsto (xy, x)$. Then $V = \mathbb{A}^2$ is $\mathbb{A}^2 \backslash \{x - \text{axis}\} \cup \{(0, 0)\}$.

The first of these example actually makes $\mathbb{A}^1 \setminus \{0\}$ into an affine variety. Indeed consider the map $\mathbb{A}^1 \setminus \{0\} \to \mathbb{A}^2$ defined by $(t, t^{-1})$. These are two rational maps, defined everywhere and whose compositions with $(x, y) \mapsto x$ is the identity. On the level of functions $k[t, t^{-1}] \cong k[x, y]/(xy - 1)$.
Generally,

**Example.** $V : f(x_1, \ldots, x_n) = 0$ is a hypersurface, then $U = \mathbb{A}^n \setminus V$ has a structure of an affine variety ($k[U] = k[x_1, \ldots, x_n, 1/f]$)

## 1.2 Invariants

**Definition 1.5.** The *dimension* $d = \dim V$ of $V \subset \mathbb{A}^n$ is defined as the length of a longest chain $\emptyset \subseteq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_d \subseteq V$ (where each $V_i$ is a variety)
This is also equal to the longest chain of prime ideals $k[V] \supsetneq P_0 \supsetneq \cdots \supsetneq P_d \supseteq \{0\}$, $P_i$ prime.
This is also equal to the transcendence degreed of $k(V)$ for varieties.

**Example.** $\dim \mathbb{A}^n = n$, $V \subset \mathbb{A}^n$ is a hypersurface, it has dimension $n - 1$. A point has dimension 0.

**Definition 1.6.** Let $V \subseteq \mathbb{A}^n$ of dimension $d$, $x \in V$ be a point. Recall that $k[V] = \{\text{regular functions } V \to k\}$. For $x$, we have the *evaluation map* $f \mapsto f(x) \in k$. This has a kernel which is a maximal ideal and denoted by $\mathfrak{m}_x$ (In fact all maxima ideals of $k[V]$ are of this form).
The *local ring* $\mathcal{O}_x = \left\{ \frac{f}{g} \in k(V) | g(x) \neq 0 \right\}$.
*Completion* $\widehat{\mathcal{O}_x} = \varprojlim_j \mathcal{O}_x/\mathfrak{m}_x^j = \{\text{compatible sequences in } (\mathcal{O}_x/\mathfrak{m}_x^n)_n\}$
$x$ is a *non-singular point* if, equivalently

1. $\dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 = d$

2. $\widehat{\mathcal{O}_x} \cong k[[t_1, \dots, t_d]]$

3. if $V$ is given by $f_1 = \cdots = f_m = 0$, then $\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}$ has rank $n-d$.

$V$ is *regular* (or *non-singular*) if every point is non-singular.

**Fact.** $V_{\text{ns}} = \{\text{non-singular points on } V\} \subseteq V$ *is dense open.*

**Example.**

- $y = x^2$. This is regular.
- $y^2 + x^1 = 1$. This is regular.
- $y^2 = x^3$. This is singular at $(0,0)$.
- $y^2 = x^3 + x^2$. This is singular at $(0,0)$.

Finally, there are products of varieties. If $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ are closed (respectively varieties) then $V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m$ is closed (respectively a variety; $k[V \times W] \cong k[V] \otimes_k k[W]$)

# 2 Affine algebraic groups

Many categories have groups like topological groups, Lie groups,.... In our case if we have affine varieties which are also groups, then we can call them affine algebraic group

**Definition 2.1.** *Affine algebraic groups* is a closed set $G \subseteq \mathbb{A}^n$, and there are morphisms $m : G \times G \to G$ (multiplication), $i : G \to G$ (inverse) and a point $e \in G$ (unit) satisfying the usual group axioms:

1. Associativity
$$\begin{tikzcd} G \times G \times G \arrow[r, "\mathrm{id} \times m"] \arrow[d, "m \times \mathrm{id}"'] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

2. Units (Exercise) $m(\mathrm{id} \times m) = m(m \times \mathrm{id})$

3. Inverse (Exercise)

**Example.** Additive group $\mathbb{G}_a = \mathbb{A}^1$, $m : (x, y) \mapsto x + y$, $i : x \mapsto -x$, $e = 0$.
Multiplicative group $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$, $m : (x, y) \mapsto xy$, $i : x \mapsto x^{-1}$, $e = 1$.

Generally, $\mathrm{GL}_n = \{A \in M_{n \times n}(k) | \det A \neq 0\} = \mathbb{A}^{n^2} \setminus$ hypersurfaces $\det = 0$. Again affine algebraic groups (note that $n = 1$ gives $\mathbb{G}_m$)

**Definition 2.2.** (Algebraic) *subgroups* is a closed subgroup.
(Algebraic group) *homomorphism* are group homomorphism which is a homomorphism (of closed sets)
*An action of* $G$ *on a variety* $V$ is a group action $G \times V \to V$ given by a morphism.
*Representations of* $G$ is a homomorphism $G \to \mathrm{GL}_n$. [equivalently it is a linear actions of $G$ on $\mathbb{A}^n$]

**Fact.** *Kernels and images of homomorphisms are algebraic groups. (Exercise for kernel, images is not so trivial)*

**Example.** $\det \mathrm{GL}_n \to \mathbb{G}_m$, the kernel is $\mathrm{SL}_n$.
$\mathrm{SL}_n \hookrightarrow \mathrm{GL}_n$ is a subgroup.
$\mathbb{G}_m \hookrightarrow \mathrm{SL}_2$ by $t \mapsto \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$.
Other classical groups: $O_n = \{A \in M_{n \times n}(k) | A^t A = I\}$, $\mathrm{Sp}_{2n} = \{A \times M_{n \times n}(k) | A^t \Omega A = \Omega\}$ where $\Omega = \begin{pmatrix} 0 & \mathrm{id}_n \\ -\mathrm{id}_n & 0 \end{pmatrix}$, are also algebraic groups.

Observe: (left) translations maps $l_h : G \to G$ defined by $g \mapsto hg$, are isomorphisms of algebraic sets. So "every points of $G$ looks the same"

Hence $G$ is non-singular (as $G_{\mathrm{ns}} \subseteq G$ is non-empty)

Connected components are irreducible components.

Connected components of $e$, denoted $G^0$, is a closed normal subgroup, $G^0 \lhd G$, $G/G^0$ is finite.

We usual study connected algebraic groups ($\mathbb{G}_m, \mathbb{G}_a, \mathrm{GL}_n, \mathrm{SL}_n, O_n, \mathrm{Sp}_n, \dots$ are all connected)

**Example.** Let $G$ be a finite group, then it is a algebraic group

*Proof.* $G \hookrightarrow \mathrm{Aut}(k[G])$ regular representation $= \mathrm{GL}_n$ for $n = |G|$. So this is a closed subgroup. □

**Theorem 2.3.** *Every affine algebraic group is a closed subgroup of* $\mathrm{GL}_n$ *for some* $n$

A consequence of this is affine algebraic groups are also called linear algebraic groups.)

*Proof.* Let $G$ be an affine algebraic group, $m : G \times G \to G$, $i : G \to G$, $e : \{\mathrm{pt}\} \to G$. Let $A := k[G]$ and consider $m^* : A \otimes A \leftarrow A, i^* : A \to A, e^* : k \leftarrow A$. Structure map, $A = k[G]$ Hopf algebra. We want to prove: $\Sigma : G \to \mathrm{GL}(V)$ closed, equivalently find $\Sigma^* : A \twoheadleftarrow k[\mathrm{GL}(V)] = k[x_{11}, \dots, x_{nn}, 1/\det]$. This equivalent $\sigma : V \to V \otimes A$ $k$-linear such that $\sigma$ is an action, $(\mathrm{id} \otimes e^*)\sigma = \mathrm{id}$, $(\mathrm{id} \otimes m^*)\sigma = (\sigma \otimes \mathrm{id})m$. We want $\sigma : v_i \mapsto \sum v_j \otimes a_{ij}$. We say that $V$ is an *A-comodule.* One (and only one) obvious comodule, $V = A = k[G]$ and $\sigma = m^*$. There is only one problem: this is infinite-dimensional (unless $G$ is finite). So we need the following:

**Lemma 2.4.** *Every finite dimensional k-subspace $W \subseteq A$ is contained in a finite dimensional co-module $V \subseteq A$ (i.e., $m^*(V) \subseteq V \otimes A$)*

*Proof.* Enough to take $W = \langle W \rangle$ is one dimensional. $m^*(W) = \sum_{i=1}^m v_i \otimes G_i$, check that $\langle w, v_!, \dots, v_n \rangle$ is a comodule. □

To finish proving the theorem: take $A = k[G] = k[x_1, \dots, x_n]/I$, $W := \langle x_1, \dots, x_n \rangle$ and take $V$ as in the lemma. Then check that $k[\mathrm{GL}_n] \twoheadrightarrow A$ □

**Example.** Let $G = \mathbb{G}_a = (\mathbb{A}^1, +)$. Then $A = k[G] = k[t]$ and take $W = \langle t \rangle$ (1-dimensional). Look at $m^*(t) = t \otimes 1 + 1 \otimes t$. Take $V = \langle 1, t \rangle$, as in the lemma. $t \mapsto t \otimes 1 + 1 \otimes t$, $1 \mapsto 1 \otimes 1$, all in $W \otimes A$, so $V$ is a comodule, corresponding embedding $\mathbb{G}_a \to \mathrm{GL}(V) = \mathrm{GL}_2$, $t \mapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

# 3 General Varieties and completeness

In topology: Manifold is a topological space $X$, covered by opens $U_i$ such that

1. $U_i$ open balls in $\mathbb{R}^n$ ($\mathbb{C}^n$)
2. Transitions functions $U_i \supset U_i \cap U_j \to U_j \cap U_i \subset U_j$ are continuous (or $C^\infty$, or analytic, ...)
3. $X$ Hausdorff, second countable

We now copy this definition

**Definition 3.1.** An *algebraic set* $V$ is a topological space, covered by finitely many open $V_i$, $V = V_1 \cup \cdots \cup V_n$, such that

1. Each $V_i$ is an affine variety
2. Transition maps $V_i \supset V_i \cap V_j \to V_j \cap V_i \subset V_j$ are regular isomorphisms
3. $V$ is closed in $V \times V$ (Note $V \times V$ is covered by affines $V_i \times V_j$ hence have a topology)

The third condition in topology is equivalent to Hausdorff.

An *algebraic variety* is an irreducible algebraic variety.

A *curve* is a one dimensional variety

A *surface* is a two dimensional variety

**Example.** If $X$ is a variety, then every open $U \subset X$ is also a variety. As are irreducible closed subspaces

The *projective space* $\mathbb{P}^n = \mathbb{P}^n_k$. $\mathbb{P}^n = \{[x_0 : \cdots : x_n] | x_i \in k, \text{not all } 0\} / \sim$ where $[x_0 : \cdots : x_n] \sim [\alpha x_0 : \cdots : \alpha x_n]$ for any $\alpha \in k^*$. Subset $V \subset \mathbb{P}^n$ is *closed* if it is the zero set of homogeneous polynomials $f_1, \ldots, f_m \in k[x_0, \ldots, x_n]$

To give $\mathbb{P}^n$ the structure of a variety, cover $\mathbb{P}^n = \mathbb{A}^n_{(0)} \cup \cdots \cup \mathbb{A}^n_{(n)}$ where $\mathbb{A}^n_j = \{[x_0 : x_1 : \cdots : \underset{j-\text{place}}{1} : \cdots : x_n]\}$. The transition maps $\mathbb{A}^n_k \setminus \{x_i = 0\} \to \mathbb{A}_k \setminus \{x_j = 0)$ defined by $(x_m) \mapsto (x_m \frac{x_j}{x_i})$ is an isomorphism. So $\mathbb{P}^n$is a variety.

Closed subsets of $\mathbb{P}^n$ are called projective varieties.

**Example.** $C : xy = 1 \subset \mathbb{A}^2_{x,y} \subset \mathbb{P}^2_{x,y,z}$. The closure $\overline{C} \subset \mathbb{P}^2$ is a curve $\overline{C} : xy = z^2$.

**Definition 3.2.** A *morphism* $X \to Y$ of algebraic sets is a continuous map given locally by morphism on affine charts.

A *rational* map is a morphism from a dense open

*Regular functions* is a morphism $f : X \to \mathbb{A}^1 = k$

*Rational function* is a rational map $f : X \rightsquigarrow \mathbb{A}^1$

**Example.** On $\mathbb{P}^n$ the only regular functions are constants $k[\mathbb{P}^n] = k$ (ring of regular functions)

Rational functions $\{f/g | f, g \text{homogenous of same degree}\}$. $k(\mathbb{P}^n) \cong k(t_1, \ldots, t_n)$ (field of rational functions)

**Definition 3.3.** A variety $X$ is *complete* if it satisfies the following equivalent conditions:

1. (Universally closed) For every variety $Y$, the projection $p_2 : X \times Y \to Y$ takes closed sets to closed sets.
2. (Maximality) If $X \subset Y$ open with $Y$ a variety, then $X = Y$
3. (Valuative criterion) For every curve $C$ and a non-singular point $P \in C$, then every morphism $C \setminus \{p\} \to Y$ extends to (a unique) morphism $C \to X$.

**Example.** $\mathbb{A}^1$ is not complete.

1. fails, because $p_2 : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ takes $xy = 1$ to $\mathbb{A}^1 \setminus \{0\}$ which is not closed.
2. fails because $\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$
3. fails because $\mathbb{A}^1 \setminus \{0\} \to \mathbb{A}^1$ defined by $x \mapsto x^{-1}$ does not extend to a morphism $\mathbb{A}^1 \to \mathbb{A}^1$.

**Corollary 3.4.** *Every variety can be embedded in a complete variety as a dense open*

(This is proved first, first for affine charts and then mat the completion together using blowing ups and blowing downs)

Consequence of completeness:

**Lemma 3.5.** *Suppose $X$ is a complete variety*

1. *If $Z \subseteq X$ closed, then $Z$ is complete*
2. *If $f : X \to Y$ is a morphism, then $f(X)$ is closed and complete*
3. *$k[X] = k$ ($X$ has no non-constant regular functions)*
4. *If $X$ is affine, then $X$ is a point*

*Proof.*

1. Immediate from definition condition 1)

2. $f(X)$ is the $p_2$ of the graph $(X, f(X)) \subseteq X \times Y$
3. Image of $X$ under $f : X \to \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ is closed, connected, misses $\infty$, therefore must be a point.
4. Affine varieties are characterised by their regular functions

□

Main example of a complete variety is:

**Theorem 3.6.** *$\mathbb{P}^n$ is complete*

**Corollary 3.7.** *Projective varieties are complete (and have $k[X] = k$)*

Complete non-projective varieties exists in dimension $\geq 3$ (Hironaka), but we'll never see them

**Theorem 3.8** (Chow's Lemma). *If $X$ is complete, there exists $X'$ projective and a morphism $X' \to X$ which is birational.*

Finally, for complete varieties over $\mathbb{C}$ we have:

**Theorem 3.9** (Chow). *Let $X$ be a complete variety over $\mathbb{C}$.*

1. *Ever analytic subvariety of $X$ is closed in Zariski topology*
2. *Every holomorphic map $f : X \to Y$ between complete varieties is a morphism.*

*(In particular, the only meromorphic functions on $X$ are rational functions)*

One application:

**Theorem** (Weak Bezout). *Every two curves $C, D \subset \mathbb{P}^2$ intersect:*

*Proof.* $C : f(x, y, z) = 0$, $D : g(x, y, z) = 0$. If $C \cap D = \emptyset$, then $[f(x, y, z) : x^{\deg f}] : D \to \mathbb{P}^1$ is a regular map $D \to \mathbb{P}^1$ that misses $[0 : 1]$, hence constant, which is a contradiction. □

# 4 Curves

Power of completeness:

**Lemma 4.1.** *$C_1, C_2$ non-singular complete curves.*

1. *Every rational map $f : C_1 \to C_2$ extends to a unique morphism*
2. *Every non-constant map $f : C_1 \to C_2$ is onto*

*Proof.*

1. $f$ is a morphism $C_n\{P_1, \ldots, P_n\} \to C_2$ and extends to $C_1 \to C_2$ by definition 3. of completeness
2. $\operatorname{im} f$ is irreducible and closed, hence either $C_2$ or a point.

□

It is not hard to deduce that $C \to k(C)$ defines an anti-equivalence of categories between {complete non-singular curves over $k$} and {finitely generated field extensions of $k$ of transcendence degree 1}

In higher dimension, this is not true: e.g., $\mathbb{P}^1 \times \mathbb{P}^1 \ncong \mathbb{P}^2$ (though they have the same field of rational functions)

From now on we look at non-singular complete curves (which is equivalent to look at non-singular projective)

A non-constant map $f : C_1 \to C_2$ gives a field inclusion $f^* : k(C_2) \hookrightarrow k(C_1)$ of finite index, called the *degree of $f$*. $\deg f = [k(C_1) : f^* k(C_2)]$. In particular, $\deg f = 1$ if and only if $f : C_1 \cong C_2$.

**Example.** Consider $x^2 + y^2 = 1$ (meaning the unique complete curve $\overline{C}$ which contains $C$ as Zariski open), maps this to $x$. This corresponds to $k(x) \hookrightarrow k(x)\left(\sqrt{1-x^2}\right)$, so the map is of degree 2.

Not hard to see: if $f : C \to D$ is non-constant, then every point of $D$ has $d$ preimages, counted with multiplicities (exactly $d$ distinct points for all but finitely many $p \in D$), where $d = \deg f$ if characteristic $k = 0$, otherwise $d$ is the separable degree of $k(C)/f^*k(D)$.

Every non-constant rational functions $f \in k(C)$ is a morphism $f : C \to \mathbb{P}^1$, so $f(P) \subset k \cup \{\infty\}$ is always defined.

**Definition 4.2.** We say that $f$ has a *zero* at $P$ if $f(P) = 0$, and a *pole* at $P$ if $f(P) = \infty$

From the above discussion, we see that every functions on $C$ has the same number of zeros as poles, if counted with multiplicities.

### Local behaviours of functions on curves

Let $P \in C$ be a point. We define $\mathcal{O} = \mathcal{O}_{C,P}$ a local ring of functions defined at $P$. This is a local domain of dimension 1, $\dim_K m/m^2 = 1$, hence $\mathcal{O}$ is a DVR (Discrete Valuation Ring). In other words, there is a valuation, $\operatorname{ord}_P : k(C)^* \twoheadrightarrow \mathbb{Z}$ (called *order of vanishing* at $P$). This is a discrete valuation, so it satisfies:

1. $\operatorname{ord}_P(fg) = \operatorname{ord}_P f + \operatorname{ord}_P g$
2. $\operatorname{ord}_P(f + g) \geq \min(\operatorname{ord}_P f, \operatorname{ord}_P g)$
3. $\operatorname{ord}_P c = 0$ for $c \in k^*$

In fact, $\{\text{discrete valuations on } k(C) \text{ trivial on } k\} \overset{1:1}{\leftrightarrow} \{\text{pts } P \text{ on } C\}$ via ord. If $\operatorname{ord}_P t = 1$, then $t$ is called a *uniformiser*. If we pick a uniformiser, say $t$, at $P$, then every $f \in k(C)$ can be written uniquely as $f = u \cdot t^n$ where $n = \operatorname{ord}_P f$ and $u$ has neither a zero or a pole at $p$.

**Exercise.** Take $C : x^2 + y^2 = 1$, $P = (1, 0)$, prove that $\operatorname{ord}_P y = 1$ and $\operatorname{ord}_P(x - 1) = 2$. Show that $x - 1 = \frac{1}{x+1}y^2$.

**Definition 4.3.** A *divisor* on a (non-singular complete) curve $C$ is a finite formal linear combination of points, $D = \sum_{i=1}^{r} n_i(P_i)$, $n_i \in \mathbb{Z}, P_i \in C$.

The *degree* of $D$ is $\sum n_i$, $D$ is *effective* if all $n_i \geq 0$.

If $f \in k(C)^*$, then the divisor of $f$ is defined as $(f) = \sum_{P \in C} \operatorname{ord}_P(f) \cdot (P)$ (finite). Divisors of this forms are called *principal*. They have degree 0, so principal divisors are a subset of degree 0 divisors, which are a subset of all divisors, i.e., $\text{Principal Divisors} < \operatorname{Div}^0(C) < \operatorname{Div}(C)$

**Definition 4.4.** $\operatorname{Pic}(C) = \operatorname{Div}(C)/\text{principal divisors}$ is called the *Picard group*. We define $\operatorname{Pic}^0(C) = \operatorname{Div}^0(C)/\text{principal divisors}$. Elements in Pic and $\operatorname{Pic}^0$ are called equivalent classes of divisors.

We have an exact sequence $0 \to \operatorname{Pic}^0(C) \to \operatorname{Pic}(C) \overset{\deg}{\to} \mathbb{Z} \to 0$

We say that $D, D' \in \operatorname{Div}(C)$ are linearly *equivalent* if they have the same class, i.e, $D = D' + (f)$ for some $f$.

# 5 Differentials and genus

Over $\mathbb{C}$ curves are Riemann surfaces. We define *genus* for a general curves using differentials.

Let $X$ be a variety over $k$.

**Definition 5.1.** *Rational $k$-differentials* on $X$ are formal finite sums $\omega = \sum_i f_i dg_i$ where $f_i, h_i \in k(X)$, modulo the relations $d(f + g) = df + dg$, $d(fg) = fdg + gdf$ and $da = 0$ for $a \in k$.

If $k(X)$ is written as finite separable extension of $k(x_1, \ldots, x_n)$ then every $\omega$ has a unique expression $g_1 dx_1 + \cdots + g_n dx_n$ (note $n = \dim X$). So their space is isomorphic to $k(x)^n$.

**Example.** $X = \mathbb{A}^n$ (or $\mathbb{P}^n$) has differentials $f_1 dx_1 + \cdots + f_n dx_n$ with $f_i \in k(x_1, \dots, x_n)$ and $f_1 dx_1$ is on $\mathbb{A}^1$ (or $\mathbb{P}^1$)

$C : y^2 = x^3 + 1$ (char$k \neq 2, 3$). Every $\omega$ can be written as $f(x,y)dx$ and also as $h(x,y)dy$. Use $0 = d(y^2 - x^3 - 1) = 2ydy - 3x^2dx$, hence $dy = \frac{3x^2}{2y}dx$

**Definition 5.2.** A differential $\omega$ is regular at $P \in X$ if it has a representation $\omega = \sum_i f_i dg_i$ where $f_i, g_i$ are regular at $P$.

$\omega$ is *regular* if $\omega$ is regular at every point.

*Notation.* $\Omega_X = \{\text{regular differentiations}\}$ (a $k$-vector space)

(For complete varieties $X$, $\dim \Omega_X < \infty$; also if $X$ is projective and $k = \mathbb{C}$, regular differentials are the same as holomorphic differentials.)

If $X = C$ a curve, $P \in C$ a non-singular point and $\omega$ a differential, write $\omega = fdt$ where $t$ is a uniformiser at $P$. Then $\omega$ is regular at $P$ if and only if $f$ is regular at $P$ if and only if $\operatorname{ord}_P f \geq 0$.

We define $\operatorname{ord}_P \omega = \operatorname{ord}_p f$ (well-defined). So $\omega$ is regular if and only if $\operatorname{ord}_p \omega \geq 0$.

**Definition 5.3.** For $C$ a complete non-singular curve, the *genus of* $C$ if $g(C) := \dim_k \Omega_C$.

If $C$ is any curve, the *geometric genus* of $C$ is the genus of the unique complete non-singular curve birational to $C$.

**Example.** Let $C = \mathbb{P}^1 = \mathbb{A}^1_x \times \mathbb{A}^1_y$ with $xy = 1$. Then $x - a$ are uniformisers at $a \in \mathbb{A}^1_x$, so $d(x-a) = dx$ has no zeroes or poles on $\mathbb{A}^1_x$ (and similarly $dy$ on $\mathbb{A}^1_y$). If $\omega = f(x)dx \neq 0$ then $xy = 1$ implies $xdy + ydx = 0$, hence $f(x)dx = -\frac{1}{y^2} f(\frac{1}{y})dy$. For $\omega$ to be regular:

1. $f(x)$ must be a polynomial in $x$
2. $\frac{1}{y^2} f(\frac{1}{y})$ must be a polynomial in $y$.

But those two conditions can be not be satisfied at the same time. So $\Omega_{\mathbb{P}^1} = \{0\}$ and hence has genus 0.

**Example.** $C : y^2 = x^3 + 1 \subseteq \mathbb{P}^2$ (char$k \neq 2, 3$). Can check that $\frac{dx}{y}$ is regular everywhere.

Generally, $C : f(x,y) = 0$ a non-singular affine curve embedded in $\mathbb{A}^2$. How to find the corresponding complete curve $\overline{C}$ and find $g(\overline{C})$ and $\Omega_{\overline{C}}$?

Take $P = (a, b) \in C$, so $\mathcal{O}_P$ is a local ring, $\mathfrak{m} = (x - a, y - b)$ (one of these is a uniformiser). Expand $f(x,y)$ at $P$, $f(x,y) = 0 + f'_x(x-a) + f'_y(y-b)+$terms in $\mathfrak{m}^2$. Either $f'_x(P) \neq 0$ if $y - b$ is a uniformiser, or $f'_y(P) \neq 0$ if $x - a$ uniformiser; so either $\operatorname{ord}_P \left(\frac{dy}{f'_x}\right) = 0$ or $\operatorname{ord}_P \left(\frac{dx}{f'_y}\right) = 0$. But $0 = df = f'_x dx + f'_y dy$, hence $\frac{dx}{f'_y} = -\frac{dy}{f'_x}$. So this differential has no zeroes or poles on $C \subseteq \mathbb{A}^2$. Therefore $x^i y^j \frac{dx}{f'_y}$ have no poles on $C$ and hence form a basis.

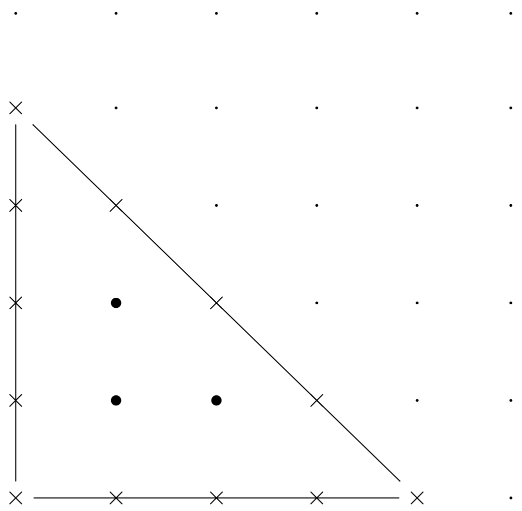
If we embed $\mathbb{A}^2$ as an open of some complete variety $X$ (e.g., $\mathbb{P}^2, \mathbb{P}^1 \times \mathbb{P}^1, \dots$) and if $\overline{C}$ ( the closure of $C$ in $X$) happens to be non-singular, then we just need to inspect $x^i y^j \frac{dx}{f'_y}$ at $\overline{C} \backslash C$ (a finite set) to find $\Omega_{\overline{C}}$ and $g(\overline{C})$.

**Theorem 5.4** (Baker). *Let $C : \sum_{i,j} c_{ij} x^i y^j = 0$ be a curve in $\mathbb{A}^2$, $\overline{C}$ be a unique non-singular complete curve birationals to $C$. Define $\Delta$ (subset of $\mathbb{R}^2$) to be the convex hull of $(i,j)$ for which $c_{ij} \neq 0$. Let $I := \Delta \setminus \partial\Delta \cap \mathbb{Z}^2$ (interior lattice points).*

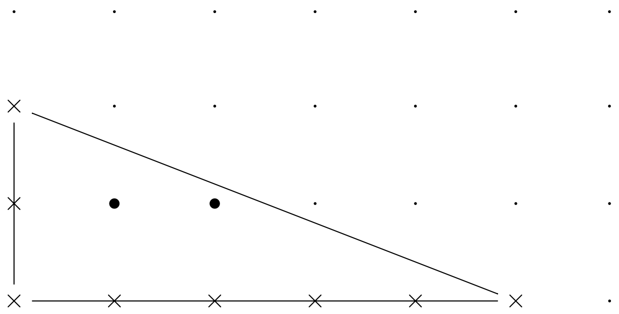
1. *$\Omega_{\overline{C}} \subseteq$ span of $x^{i-1} y^{j-1} \frac{dx}{d'_y}$ for $(i,j) \in I$.*
2. *The equality $g(\overline{C}) = |I|$ holds if e.g. $C \subseteq \mathbb{A}^2$ non-singular, and for all segments $\sigma \subseteq \partial\Delta$ that do no have both end points on the coordinate axe have that the polynomial $f_\sigma = \sum_{(i,j) \in \sigma} c_{ij} x^i y^j$ is square-free.*

(Basically this embeds $\mathbb{A}^2 \subseteq X :=$toric variety with the corresponding Newton polygon, and compute arithmetic genus of $\overline{C}$ in $X$)

**Example.** (char$k > 5$)
$x^4 + y^4 = 1$



Hence $g = 3$
$y^2 = x^5 + 1$



Hence $g = 2$

Both example generalise:

**Example.** (Plane curves) Let $C : f = 0 \subseteq \mathbb{P}^2$ non-singular, $f$ homogeneous of degree $d \geq 1$. Then $g \leq \frac{(d-1)(d-2)}{2}$ by the Theorem,, and it gives differential $x^{i-1}y^{j-1}\frac{dx}{f'_y}$. It is not difficult to check that these are regular everywhere, so $g = \frac{(d-1)(d-2)}{2}$

**Example.** (Hyperelliptic curves) Let $y^2 = f(x)$, $f$ square-free, $\deg(f) = 2g + 1$ or $2g + 2$ has genus $g$. $\Omega_{\overline{C}} = \left\langle \frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y} \right\rangle$.

## 6 Riemann - Roch

*Notation.* For a divisor $D \in \text{Div}(C)$, where $C$ is a complete non-singular curve, we write $\mathscr{L}(D) = \{D' \geq 0 | D' \sim D\}$ or equivalently $\mathscr{L}(D) = \{0\} \cup \{f \in k(C)^* | (f) \geq -D\}$. This is called "the space of functions with poles at most at $D$"

[E.g., $D = 4(P)$, then $\mathscr{L}(D) = \{f$ with no poles outside $P$ and at most pole of order 4 at $P\}$]

Write $K_C = [(\omega)] \in \text{Pic}(C)$ for (any) differential form on $C$, this is the *canonical class*.

*Note.* $\dim_{\mathscr{L}}(K_C) = \dim \Omega_C = g(C)$

**Theorem 6.1** (Riemann - Roch)**.** *Let $C$ be a complete non-singular curve. Then for every $D \in \mathrm{Div}(C)$,*

$$\dim \mathscr{L}(D) - \dim \mathscr{L}(K_C - D) = \deg D - g + 1$$

**Corollary 6.2.**

1. $\deg K_C = 2g - 2$
2. *If* $\deg D > 2g - 2$, *then* $\dim \mathscr{L}(D) = \deg D - g(C) + 1$.

*Note.* If $D = 0$, then $\mathscr{L}(D) = k$ and hence $\dim \mathscr{L}(D) = 1$. If $\deg D < 0$ then $\dim \mathscr{L}(D) = 0$.

*Proof of Corollary.*

1. $D = K_C$, $g - 1 = \deg K_C - g + 1$
2. $\deg D > 2g - 2$ then $K_C - D$ will have negative degree and $\mathscr{L}(K_C - D) = 0$.

□

**Example.** (genus 0). Suppose $C$ has genus 0. Pick $P \in C$, $D = (P)$. Then using Riemann - Roch, we have $\dim \mathscr{L}(0) = 1$, $\mathscr{L}(0) = k = \langle 1 \rangle$, $\dim \mathscr{L}((P)) = 1 - 0 + 1 = 2$, hence $\mathscr{L}((P)) = \langle 1, f \rangle$ where $f$ has exactly one simple pole at $P$ and no other poles. Then $f : C \to \mathbb{P}^1$ has degree 1, hence it is an isomorphic and so $C \cong \mathbb{P}^1$.

*Remark.* If $g(C) > 0$ and $P \in C$, then $\mathscr{L}((P)) = \mathscr{L}(0) = k$ 1-dimensional. (Otherwise pick $f \in \mathscr{L}((P)) - \mathscr{L}(0)$ implies $f : C \overset{\sim}{\to} \mathbb{P}^1$)

**Example.** (Genus 1)

**Definition 6.3.** A genus 1 curve $C$ with a chosen point ("origin") $\mathcal{O}$, is called an *elliptic curve*.

Suppose $(C, \mathcal{O})$ is elliptic. $\mathscr{L}(0) = \mathscr{L}(1 \cdot (\mathcal{O})) = k$ 1-dimensional
$\mathscr{L}(n \cdot (\mathcal{O}))$ has dimension $n$ (for $n \geq 1$). In particular:

- $\mathscr{L}(2 \cdot (\mathcal{O})) = \langle 1, x \rangle$ (where $x$ is a function with exactly a double pole at $\mathcal{O}$ and no other poles).
- $\mathscr{L}(3 \cdot (\mathcal{O})) = \langle 1, x, y \rangle$ (where $y$ is a function with a triple pole...)
- $\mathscr{L}(4 \cdot (\mathcal{O})) = \langle 1, x, y, x^2 \rangle$
- $\mathscr{L}(5 \cdot (\mathcal{O})) = \langle 1, x, y, x^2, xy \rangle$
- $\mathscr{L}(6 \cdot (\mathcal{O})) = \langle 1, x, y, x^2, xy, x^3, y^2 \rangle$. But this is 6-dimensional by Riemann - Roch, so there must exists a liner relation (rescaling $x, y$, if necessary): $y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6$ (Weierstrass equations).

First note: fields

$$\begin{tikzcd}
 & k(C) \arrow[d, equal] \arrow[ddl, dash, "2"'] \arrow[ddr, dash, "3"] & \\
 & k(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
k(x) & & k(y)
\end{tikzcd}$$

so $k(C) = k(x,y)$, and so $C$ is birational to $y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6 \subseteq \mathbb{A}^2$. Finally, this curve is non-singular, otherwise has geometric genus 0 by Baker's theorem and $C \cong \mathbb{P}^1$ which is a contradiction. This defines a non-singular curve in $\mathbb{P}^1$ (with a unique point $\mathcal{O} = (0:1:0)$ outside $\mathbb{A}^2$) which must therefore be isomorphic to $C$.

Conclusion: Every elliptic curve is isomorphic to one in Weierstrass form. If char$k \neq 2, 3$, complete the square and cube, get $y^2 = x^3 + Ax + B$, $A, B \in k$, $x^3 + Ax + B$ square-free.

The only functions with a double pole at $\mathcal{O}$ are $ax + b$ ($a \neq 0$) and triple pole $cy + dx + e$ ($c \neq 0$). So the only isomorphism between Weierstrass equations are $x \mapsto u^2x + r, y \to u^3y + sx + t$, and between simplified Weierstrass equations, $x \mapsto u^2x, y \mapsto u^3y$. So $y^2 = x^3 + Ax + B \cong y^2 = x^3 + u^4Ax + u^6B$.

**Corollary 6.4.** Aut$(E, \mathcal{O})$ *is finite. In* char$k \neq 2, 3$*:*

- *if* $A, B \neq 0$ *then* Aut $\cong C_2$ *(*$u = \pm 1$*)*
- $A \neq 0$ *then* $C_6$
- $B \neq 0$ *then* $C_4$

*Similarly if* char$K = 2, 3$ *then* Aut$(E, \mathcal{O})$ *is finite of order at most* 24.

**Theorem 6.5** (Hurwitz)**.** *If* $C$ *has genus greater than* 1*, then* Aut$(C)$ *is finite.*

Embedding of curves in $\mathbb{P}^n$:

If $D \in \text{Div}C$, say $\mathscr{L}(D) = \langle f_1, \ldots, f_n \rangle \neq 0$, then get $\phi : C \rightsquigarrow \mathbb{P}^{n-1}$ defined by $P \mapsto [f_1(P) : \cdots : f_n(P)]$ extends to a morphism. Different basis gives the same map up to linear transformation of $\mathbb{P}^{n-1}$ (in $\text{PGL}_n(K)$). Also $\phi$ clearly depends only on $[D] \in \text{Pic}(C)$. Finally, there are conditions to ensure that $\phi$ is an isomorphism $C \to \phi(C)$ ["closed inversion"]. Thence $\phi(C)$ is a curve in $\mathbb{P}^{n-1}$ of degree $\deg D$ (recall that degree is number of $\phi(C) \cap$generic hyperplane)

**Example.** Let $(C, \mathcal{O})$ be an elliptic curve, given by $y^2 = x^3 + Ax^2 + B$, take $D = n \cdot (\mathcal{O})$ with $n \geq 1$. Then

- $\mathscr{L}(1 \cdot (\mathcal{O})) = \langle 1 \rangle$, this gives $E \to \{\text{pt}\} = \mathbb{P}^0$
- $\mathscr{L}(2 \cdot (\mathcal{O})) = \langle 1, x \rangle$, this gives $E \overset{x,2:1}{\to} \mathbb{P}^1$
- $\mathscr{L}(3 \cdot (\mathcal{O})) = \langle 1, x, y \rangle$, this gives $E \hookrightarrow \mathbb{P}^2$ (degree 3)
- $\mathscr{L}(4 \cdot (\mathcal{O})) = \langle 1, x, y, x^2 \rangle$, this gives $E \hookrightarrow \mathbb{P}^3$ (degree 4). Here $\phi(E) = \begin{cases} x_1^2 = x_0x_3 \\ x_2^2 = x_1x_3 + Ax_0x_1 + Bx_0^2 \end{cases}$. This is the intersection of two quadrics.

When $\deg D$ is large (greater than $2g - 2$), then $\dim \mathscr{L}(D)$ does not depend on the curve (only genus), or $D$. But for $\deg D$ small it does. Existence of these linear systems can be used to classify curves (complete classification is unknown).

**Example.** The *canonical map*, given by $D = K_C$, $\phi : C \to \mathbb{P}^{g-1}$ and $\phi(C)$ is a curve of degree $2g - 2$ (for $g \geq 3$). For non-hyperelliptic curves, this is a closed immersion. [Conversely, if $C \subseteq \mathbb{P}^{g-1}$ of degree $2g - 2$, then $C \cap$generic hyperplane is a divisor in the canonical class]

For hyperelliptic curves $y^2 = f(x)$, $\phi : C \overset{2:1}{\to} \mathbb{P}^1 \hookrightarrow \mathbb{P}^{g-1}$ and the 2: 1 map to $\mathbb{P}^1$ is unique when $g \geq 3$.

**Example.** A *genus 3* curve is either hyperelliptic $y^2 = f(x)$ with $f(x)$ having degree 7 or 8, or its canonical embedding gives $C \hookrightarrow \mathbb{P}^2$ plane quartic (and not both)

A *genus 4* curve is either hyperelliptic (deg 9, 10) or canonical $C \hookrightarrow \mathbb{P}^3$ with $\phi(C) = \deg 2 \cap \deg 3$.

A *genus 5* curve is either hyperelliptic (deg 11, 12) or canonical $C \hookrightarrow \mathbb{P}^4$ with $\phi(C) = \deg 2 \cap \deg 2 \cap \deg 2$.

A *genus* 6 does not have complete intersections in $\mathbb{P}^{g-1}$.

## Picard Groups of curves

**Example.** ($g = 0$) $C \cong \mathbb{P}^1$. On $C$ every $D \in \mathrm{Div}^0(C)$ is $\sim 0$ (hence $\mathrm{Pic}^0(C) = 0$, $\mathrm{Pic}(C) = \mathbb{Z}$). Let $D = \sum_{a \in \mathbb{P}^1} n_a(a) = \mathrm{div}(f)$, where $f = \prod_{a \neq \infty}(x-a)^{n_a}$.

**Example.** ($g = 1$). On an elliptic curve $(E, \mathcal{O})$ every $D \in \mathrm{Div}^0(C)$ is $\sim (P) - (\mathcal{O})$ for a unique point $P \in E$. To see this, take $D \in \mathrm{Div}^0(C)$, $\mathscr{L}(D + (\mathcal{O}))$ is 1-dimensional by Riemann - Roch, hence there exists $f \in k(E)^*$ such that $(f) \geq -D - (\mathcal{O})$, so $(f) = -D - (\mathcal{O}) + (P)$ for some $P \in E$. As $f$ in unique up to constant multiple, $P$ is unique.

This shows that $E \overset{1:1}{\to} \mathrm{Pic}^0(E)$ defined by $P \mapsto (P) - (\mathcal{O})$. In particular, this gives $E$ the structure of an abelian group, with $\mathcal{O}$ as the identity element. Geometrically, if $E$ is in Weierstrass form $y^2$ =cubic in $X$, $\mathcal{O} = [0:1:0]$, then $P + Q + R = \mathcal{O}$ if and only if $P, Q, R$ lie on a line. Indeed, if $L$ is the line through $P, Q$ (tangent if $P = Q$), $L : \alpha x + \beta y + \gamma = 0$, then the function $\alpha x + \beta y + \gamma$ has divisor $(P) + (Q) + (R) - 3(\mathcal{O})$ and so $(P) - (\mathcal{O}) + (Q) - (\mathcal{O}) + (R) - (\mathcal{O}) \sim 0$, hence $P + Q + R = 0$. To add $P, Q$, draw the line through $P, Q$, find 3rd point of intersection, say $R'$, and let $P + Q = R$, where $R$ is $R'$ reflected in the $x$-axis.

From here not hard to see that addition $E \times E \to E$ defined by $P, Q \mapsto P + Q$ is a morphism of varieties.

**Example.** ($g = 2$) Let $C : y^2 = x^5 + a_4x^4 + \cdots + a_0$ (characteristic not 2, then every genus 2 curve has this form). This model has a unique point $\infty$ at infinity. $C$ is hyperelliptic, write $\iota : (x, y) \mapsto (x, -y)$, the *hyperelliptic involution*. Let $\Omega_C = \left\langle \frac{dx}{y}, \frac{xdx}{y} \right\rangle$, $\left\langle \frac{dx}{y} \right\rangle = 2 \cdot (\infty)$ (no zeroes, poles on $C \cap \mathbb{A}^2$ and degree 2), $\left( \frac{(x-a)dx}{y} \right) = (P) + (\iota(P))$. So, effective divisors in the canonical class $K$, are fibres of $C \xrightarrow{x} \mathbb{P}^1$.

If $D \in \mathrm{Div}^2(C)$, (i.e. a degree 2 divisor) and $D \notin [K_C]$ then, by Riemann - Roch, $\dim \mathscr{L}(D) - \dim \mathscr{L}(K - D) = \deg D - g + 1 = 1$, but $K - D$ had degree 0 and is not principal, hence $\mathscr{L}(K - D)$ has dimension 0. Therefore $[D]$ has a unique effective divisors $(P_1) + (P_2)$.

Hence every $D \in \mathrm{Div}^2(C)$ is equivalent to $(P_1) + (P_2)$ for a unique $\{P_1, P_2\}$, except that all $\{P, \iota(P)\}$ are equivalent. Adding $-2(\infty)$ we get a description of $\mathrm{Pic}^0(C)$.

unordered pairs of points $\{P_1, P_2\}$, except all $\{P, \iota(P)\}$ give the same class $\overset{1:1}{\leftrightarrow}$ $\mathrm{Pic}^0(C)$ defined by $P_1, P_2 \mapsto (P_1) + (P_2) - 2(\infty)$. The group law on $\mathrm{Pic}^0(C)$:

Unit Element: any pair $\{P, \iota(P)\}$.

Inverse: $\{P_1, P_2\} \mapsto \{\iota(P_1), \iota(P_2)\}$

Addition: to add $\{P_1, P_2\}$ and $\{Q_1, Q_2\}$, find a unique curve $y = a_3x^3 + \cdots + a_0$ that intersect $C$ at those points plus two other points $\{R_1, R_2\}$ and let $\{P_1, P_2\} + \{Q_1, Q_2\} := \{\iota(R_1), \iota(R_2)\}$

*Remark.* Let $C$ be any curve of genus $g > 0$

- Every divisors $D \geq 0$ of degree $g$ is equivalent to one of the form $(P_1) + (P_2) + \cdots + (P_g)$, "usually" uniquely ($\mathrm{Pic}^5(C)$ is birational to $\mathrm{Sym}^8 C = C^9/S_9$)

**Example.** (Cantor) Let $C : y^2 = f(x)$ an hyperelliptic curve (any genus $g > 0$) with $f(x)$ having degree $2g + 1$ square free. Every class in $\mathrm{Pic}^0(C)$ is represented by a unique divisor $(P_1) + \cdots + (P_r) - r(\infty)$, $0 \leq r \leq g$, where $P_i$ are affine points and $P_j \neq \iota(P_i)$ for $j \neq i$.

*Remark.* In general $\mathrm{Pic}^0(C)$ has a structure of an algebraic group, specifically of an abelian variety of dimension $g$.

## General Algebraic Groups

**Definition 6.6.** A group $G$ is *an algebraic group* over $k$ if it has a structure of an algebraic set, and multiplication $G \times G \to G$, inverse $G \to G$ are morphisms.

**Example.** Affine algebraic groups, $\mathbb{G}_a, \mathbb{G}_m, \mathrm{GL}_n, \ldots$

**Example.** Elliptic curves and their products $E_1 \times E_2 \times \ldots$

**Example.** Multiplication by $[m]$ map, $[m] : G \to G$, $P \mapsto P + \cdots + P$ ($m$ times) is a homomorphism, if $G$ is commutative.

As before, connected component $G^0$ is a variety, $G = G^0 \rtimes$ finite group. Kernels and images exist, as before

**Example.** Algebra groups often occur as automorphism groups of varieties. For example, if $C$ is a non-singular complete curve

($g = 0$) $C \cong \mathbb{P}^1$, $\text{Aut}\mathbb{P}^1 = \left\{ \frac{ax+b}{cx+d} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Gl}_2 \right\} / k^* \cong \text{PGL}_2(k)$. Möbius group.

($g = 1$) Choose $\mathcal{O} \in C$, hence $C$ is an elliptic curve, then $\text{Aut}(C) \cong C \rtimes \text{Aut}(C, \mathcal{O})$ (translation, using the group law, and automorphism that fixes $\mathcal{O}$). We know $\text{Aut}(C, \mathcal{O})$ is finite of order $\leq 24$.

($g \geq 2$) Theorem: $\text{Aut}(C)$ is finite.

**Proposition 6.7.** *The only* 1*-dimensional connected algebraic groups are* $\mathbb{G}_a, \mathbb{G}_m$ *and elliptic curves.*

*Proof.* Suppose $G$ is such an algebraic group. So $G = C \setminus \{P_1, \ldots, P_n\}$ for some complete non-singular curve $C$, and points $P_i \in C$. The left translation map $l_x : G \to G$ defined by $y \mapsto xy$, extends to $C \to C$, so $C$ has $\infty$-many automorphism that are

1. fixed points free on $G$
2. preserve $\{P_1, \ldots, P_n\}$

Let $g =$genus $(C)$ and $e \in G$.

If $g \geq 2$ $\quad$ $\text{Aut}(C)$ finite (contradiction)

$g = 1$ $\quad$ If $n \geq 1$, then $\text{Aut}(C, \{P_i\})$ finite (size $\leq 24$) , contradiction. So $n = 0$. There exists a unique fixed point free map taking $e$ to a given $x \in G$, so the group law must be the standard one.

$g = 0$ $\quad$ Now $C = \mathbb{P}^1$, $G = C \setminus \{P_1, \ldots, P_n\}$.

$n = 0$ $\quad$ $l_x : \mathbb{P}^1 \to \mathbb{P}^1$ have no fixed points (impossible)

$n \geq 3$ $\quad$ $\text{Aut}(\mathbb{P}^1, \{P_1, \ldots, P_n\})$ is finite.

$n = 1$ $\quad$ Move $P_1$ to $\infty$, $G = \mathbb{A}^1$, fixed point free transformation of $\mathbb{A}^1$ are of the form $x \mapsto x + a$. Hence $G \cong \mathbb{G}_a$

$n = 2$ $\quad$ Move $P_1, P_2$ to 0 and $\infty$, $G = \mathbb{A}^1 \setminus \{0\}$, fixed point free transformation of $G$ are of the form $x \mapsto bx$, hence $G \cong \mathbb{G}_m$.

□

## An Abelian Variety is a Complete Connected Algebraic Group

**Example.** Elliptic curves and product of elliptic curves

**Theorem 6.8** (Barsotti - Chevalley)**.** *Every connected algebraic group* $G$ *fits in an exact sequence* $1 \to H \to G \to A \to 1$ *with* $H \lhd G$ *is the largest linear connected normal subgroup and* $A$ *an Abelian variety.*

Recall that linear are closed subgroups of $\text{GL}_n$ and are well understood.

In view of this, every algebraic groups $G$ has a (unique) filtration

$$G \underset{\lhd}{\overset{\text{finite}}{-}} G_0\text{connected} \underset{\lhd}{\overset{\text{ab variety}}{-}} G_1\text{linear} \underset{\lhd}{\overset{\text{semi}-\text{simple}}{-}} G_2\text{solvable} \underset{\lhd}{\overset{\text{torus}}{-}} G_3\text{unipotent}\underset{\lhd}{-}1$$

with $G_i$ connected.

**Example.** A torus is isomorphic to $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$.

- unipotent = subgroups of $\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (which is build up from $\mathbb{G}_a$) .
- Solvable = admits a filtration $1 \lhd H_0 \lhd \cdots \lhd H_k = G$ with $H_i/H_{i-1}$ commutative
- Semi-simple group is one that admits a finite cover $G_1 \times \cdots \times G_k \to G$ with $G_i$ almost simple [centre $C$ is finite, and $G/C$ is simple], where simple of is of type $A_n, B_n, \ldots, G_n$ [$\mathrm{PSL}, \mathrm{SO}, \ldots$]

Let $A$ be an Abelian variety over $k$ (i.e., complete algebraic group). We will show that $A$ is commutative (whence "abelian")

**Lemma 6.9** (Mumford's Rigidity)**.** *Suppose $f : V \times W \to U$ is a morphism, where $V, W, U$ are varieties and $V$ is complete. If $f(\{v_0\} \times W) = f(V \times \{w_0\}) = \{u_0\}$ for some point $u_0, v_0, w_0$ then $f$ is constant, i.e., $f(V \times W) = \{u_0\}$.*

Aside: Over $\mathbb{C}$, if $w$ is close to $w_0$, then compactness of $V$ and continuity of $f$ implies $f(V \times \{w\}) \subseteq$ some open ball around $u_0$. But Liouville Theorem implies that no non-constant maps from a compact complex manifold to an open disc. So $f(W \times \{w\}) = \mathrm{pt} = u_0$. Hence the set of points $w \in W$ such that $f(V \times \{w\}) = \{u_0\}$ is open. It is closed as well, $W$ is connected so $f$ is constant.

*Proof of Lemma.* Let $U_0$ be an open affine neigbourhood of $u_0$ and $Z = f^{-1}(U \setminus U_0)$ which is closed subset of $V \times W$. Since $V$ is complete the projection $p_2(Z)$ under $V \times W \to W$ is closed. As $w_0 \notin p_2(Z)$, complement $W_0 = W \setminus p_2(Z)$ is open and hence dense in $W$. But for all $w \in W_0$, the image $f(V \times \{w\}) \subseteq U_0$ must be a point, as $V \times \{w\}$ is complete and $U_0$ is open affine. So $f(V \times \{w\}) = u_0$. In other words $f$ is constant on a dense open set hence constant everywhere. □

**Corollary 6.10.** *If $U, V, W$ are varieties, $V$ is complete and $U$ is an Algebraic group then if $f_1, f_2 : V \times W \to U$ are two morphisms which agree on $\{v_0\} \times W$ and on $V \times \{w_0\}$, then $f_1 = f_2$.*

*Proof.* The map $p \mapsto f_1(p)f_2(p)^{-1}$ is constant by the Rigidity lemma. □

**Corollary 6.11.** *Every Abelian variety over $k$ is Commutative.*

*Proof.* The map $xy, yx : A \times A \to A$ agree on $\{e\} \times A$ and $A \times \{e\}$, hence everywhere. □

**Corollary 6.12.** *Let $f : A \to B$ be a morphism of varieties, $A$ an abelian variety and $B$ an algebraic group. Then*

1. *If $f(e_A) = e_B$ then $f$ is a homomorphism of Algebraic groups*
2. *In general $f$ is a composition of a translation on $B$ and a homomorphism $A \to B$.*

*Proof.* We proof the first part. The morphism $f(x)f(y)$ and $f(xy)$ are morphisms on $A \times A \to B$ and agree on $A \times \{e\}$ and $\{e\} \times A$.Hence they agree everywhere. □

Another consequence: In defining an abelian variety, we could drop the associativity conditions (it's automatic from rigidity). This gives an easy proof that the chord-tangent addition on Elliptic curves defines an associative addition.

The last corollary can be extended: Any rational map $G \rightsquigarrow A$ from an connected algebraic group to an abelian variety is a morphism and is an in the corollary.

# Part II
# Families and Moduli Spaces

## The most powerful technique in modern algebraic geometry:

Viewing a morphism $f : X \to Y$ as a family of varieties (fibres) parametrised by $Y$.

**Example.** Let $E : y^2 = x^3 + t^3 \subseteq \mathbb{A}^3_{x,y,t}$. This can be viewed either as a surface in $\mathbb{A}^3$ or as a family of (elliptic) curves parameterised by $t \in \mathbb{A}^1$. This is line an "Elliptic curve over $k[t]$" and embedding $k[t] \subseteq k(t) \subseteq \overline{k(t)}$. This does become an Elliptic curve as we know them.

This allows us to pass between geometry of surfaces and curves over another field. Some of the main results in Algebraic geometry are proved by reducing questions about general varieties to questions about curves (over some general bases)

**Example.** Deligne's proof of Weil Conjecture
de Jong's alteration.

# 7 Varieties over a general field

Let $K$ be any field, $k = \overline{K}$ its algebraic closure. If $V$ is an affine variety over $\overline{K}$, we say that $V$ is defined over $K$ if $V$ can be defined with polynomials with $K$-coefficients. For such $V$and $V'$ a ($K$-)morphism $f : V \to V'$ is a morphism given by polynomial with coefficients in $K$. As before $K[V]$ are morphism $V \to \mathbb{A}^1$ and $K(V)$ is the field of fractions of $K[V]$. We say that $V$ is complete, regular (usually geometrically regular) if $V$ over $\overline{K}$ is.

General variety - Covered by affine Varieties defined over $K$ with transition maps defined over $K$. Products exists: $K[V \times W] = K[V] \otimes K[W]$.

**Example.**

- $\mathbb{A}^n, \mathbb{P}^n$ are varieties over any field.
- The line $\sqrt{2}x + \sqrt{3}y = 0$ in $\mathbb{A}^2_{\overline{\mathbb{Q}}}$, it is not defined over $\mathbb{Q}$ but it is over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that it is also defined over $\mathbb{Q}(\sqrt{6})$ since $x + \frac{\sqrt{6}}{2}y$ defines the same line.
- $f : x^2 + y^2 = 0$ is an algebraic set over $\mathbb{R}$, but not a variety over $\mathbb{R}$ though $x^2 + y^2$ is irreducible.

*Note.* The old definition "variety = Zariski closed irreducible subset of $K^n$" does not work. For example over $\mathbb{F}_p$ only varieties could be points.

Let $V$ be an affine variety over $K$, i.e., $V \subset \mathbb{A}^n_{\overline{K}}$. Define its set of $K$-rational point as $V(K) = V \cap K^n$ and similarly for non affine varieties ($V(K) = \cup V_i(K)$). Note that this may be small or empty.

Assume that $K$ is perfect (i.e., every $f$ extension of $K$ is separable that is $K = \mathbb{F}_q$ or it has characteristic 0)

Let $C$ be a curve over $K$. We say that $D \in \operatorname{Div}(C)$ is defined over $K$ if it is invariant under all automorphism $\sigma \in \operatorname{Gal}(\overline{K}/K)$

**Example.** Consider $\mathbb{P}^1_{\mathbb{Q}}$. The divisors $(0), (1/2), (\infty)$ are $\mathbb{Q}$-rational, and the divisors $(\sqrt{2}) + \left(\sqrt{-2}\right)$, $4(i) + 4(-i)$ are defined over $\mathbb{Q}$.

There are two main complications when $K \neq \overline{K}$

- Varieties might not have any $K$-rational points
- There are varieties over $K$ which are not isomorphic over $K$ but are isomorphic over $\overline{K}$

**Example** (Selmer)**.** Let $C$ be a curve of genus 1 over $\mathbb{Q}$. $C : 3X^3 + 4Y^3 = 5Z^3 \subseteq \mathbb{P}^2_{\overline{\mathbb{Q}}}$, it is isomorphic over $\overline{\mathbb{Q}}$ to the elliptic curve $E : y^2 = x^3 - 100/3$. However, $C(\mathbb{Q}) = \emptyset$ hence $C \ncong E$ or any other elliptic curve over $\mathbb{Q}$ (as they are genus 1 curves with a $\mathbb{Q}$-rational point $\mathcal{O}$). In fact, all $\mathbb{Q}$-rational divisors on $C$ have degree multiple of 3. So $C$ does not even admit a degree 2 map to $\mathbb{P}^1$. Fortunately, if $C$ has a $K$-rational divisor $D$, then $\mathscr{L}(D)$ has basis of rational functions defined over $K$.

**Lemma 7.1.** *Let $V$ be a $\overline{K}$-vector space such that* $\operatorname{Gal}(\overline{K}/K)$ *acts on $V$ (compatibly with its action on $\overline{K}$) then* ˇ *has a basis of* $\operatorname{Gal}(\overline{K}/K)$*invariant vectors.*

**Example.** If $C/K$ has genus 1 and $D \in \mathrm{Div}^1(C)$ is $K$-rational then we can apply the lemma to $\mathscr{L}(n \cdot D)$, $n \geq 1$ and as before prove that $C \cong$ Elliptic curve in Weierstrass form, $P \rightsquigarrow \mathcal{O} = (0:1:0)$.

**Example.** Genus 0. Let $C/K$ be genus 0, the divisor $D = (\omega)$ of any $K$-rational differential form $\omega \neq 0$ has degree $-2$ and is $K$-rational by Riemann - Roch, $\mathscr{L}(-D)$ is 3-dimensional, has a basis of $K$-rational functions $f_1, f_2, f_3$ and $(f_1, f_2, f_3) : C \to \mathbb{P}^2$ has image of degree 2 (possibly singular). Hence every curve of genus 0 is isomorphic to $\mathbb{P}^1_K$ or a nonsingular conic in $\mathbb{P}^2_K$.

**Example.** Over $\mathbb{R}$. Every genus 0 curve over $\mathbb{R}$ is isomorphic to $\mathbb{P}^1_{\mathbb{R}}$ or $x^2 + y^2 - z^2 = 0 \subseteq \mathbb{P}^2_{\mathbb{R}}$.

**Example.** Genus 2. Let $C/K$ with $K$ a field of characteristic not 2. The canonical divisor class has degree 2, has $K$-rational divisors in it, hence use this to get a model $y^2 = g(x)$ where $\deg f \in \{5, 6\}$ and $f$ is square free.

Can have varieties $V, V'$ over $K$ (or algebraic groups over $K$) that are non-isomorphic over $K$ but are isomorphic over $\overline{K}$. In either setting, we say that $V$ and $V''$ are *forms* or *twists* of each other. If $V$ and $V'$ are twists, pick an isomorphism over $\overline{K}$, $i : V \to V'$. Any automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$ defines another such isomorphism, $i^\sigma$, and the composition $\xi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V/\overline{K})$ defined by $\sigma \mapsto (i^\sigma)^{-1} i$ satisfies $\xi(\sigma\tau) = \xi(\sigma)^\tau \xi(\tau)$. This makes $\xi$ into a 1-cocycle.

**Theorem 7.2.** *If either*

- *$V$ is an algebraic group, or*
- *$V$ is a quasi-projective (open subset of a projective variety) and* $\mathrm{Aut}(V/\overline{K})$ *is an algebraic group*

*then the above map $\xi$ gives a bijection between* $\{\text{twists of } V \text{ over } K\} \leftrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}(V/\overline{K}))$.

*[Moreover, if $L/K$ is Galois, then twists of $K$ that become isomorphic over $L$ are in bijection with* $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(V/L))$.*]*

**Example.** (Elliptic Curves). Suppose that the field $K$ does not have characteristic 2 or 3. Every $E/K$ has a model $E : y^2 = x^3 + Ax + B$ with $A, B \in K$, and we call $E_d : dy^2 = x^3 + Ax + B$ (which is isomorphic to $y^2 = x^3 + d^2Ax + d^3B$) is the quadratic twist of $E$ by $d \in K^*/K^{*2}$.

If $AB \neq 0$, then $\mathrm{Aut}_{\overline{K}}(E) = \mathrm{Aut}_K(E) = \{\pm 1\}$. This acts with trivial Galois actions. Hence $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}_{\overline{K}}(E)) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \{\pm 1\})$. A non-trivial element of this group is characterised by its kernel, which is $\mathrm{Gal}\left(\overline{K}/K\left(\sqrt{d}\right)\right)$, for some $d \in K^*/K^{*2}$. It corresponds to the quadratic twist of $E/K$ by $d$:

Choose $i : E \to E_d$ to be defined by $P = (x, y) \mapsto i(P) = (x, \frac{y}{\sqrt{d}})$. Then $(i^\sigma)^{-1} i : P = (x, y) \mapsto (x, \frac{y}{\sqrt{d}}) \mapsto (x, \underbrace{\frac{\left(\sqrt{d}\right)^\sigma}{\sqrt{d}}}_{=\pm 1} y) = \begin{cases} P & \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ -P & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \end{cases}$ which is indeed the corresponding element of $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}_{\overline{K}} E)$.

Finally, there are 2 exceptional curves:

- $E : y^2 = x^3 + x$. Then $\mathrm{Aut}(E/\overline{K}) = \langle \zeta_4 \rangle$ (as $[i] : (x, y) \mapsto (-x, iy)$ is an automorphism)
- $E : y^2 = x^3 + 1$. Then $\mathrm{Aut}(E/\overline{K}) = \langle \zeta_6 \rangle$.

and in these cases the corresponding twists are $y^2 = x^3 + dx$ where $d \in K^*/K^{*4}$ (quartic twists) and $y^2 = x^3 + d$ where $d \in K^*/K^{*6}$ (sextic twist)

**Exercise.** What happens when $\mathrm{char} K = 2, 3$ and $\mathrm{Aut}(E/\overline{K}) \cong \mathrm{SL}_2(\mathbb{F}_3)$ (of order 24).

# 8 Moduli problems

There exists many classification problems in which objects that we want to classify are "naturally" parametrised by points on a variety. As before we work $k = \overline{k}$

**Example.** Lines through the origin in $\mathbb{A}^2$. They are parameterised by points of $\mathbb{P}^1$. To see this, $ax+by=0 \overset{1:1}{\leftrightarrow} [a:b] \in \mathbb{P}^1$.

Similarly, all lines in $\mathbb{A}^2$: $ax+by+c=0 \overset{1:1}{\leftrightarrow} \mathbb{P}^2 \setminus \{[0:0:1]\}$.

All lines in $\mathbb{P}^2 \overset{1:1}{\leftrightarrow} \mathbb{P}^2$.

**Example.** Generally, $d$-dimensional linear subspaces in $\mathbb{A}^n$ are again parameterised by points on a variety, called the *Grassmanian*, denoted by $\mathrm{Gr}(d, \mathbb{A}^n)$

**Example.** Curves of degree 2 in $\mathbb{P}^2$ (*conics*) have an equation $a_0x^2+a_1xy+a_2xz+a_3y^2+a_4yz+a_5z^2$ and again $(a_i)$ and $\lambda(a_i)$ defines the same conic. So conics $\overset{1:1}{\leftrightarrow} \{\text{pts in}\, \mathbb{P}^5\} \setminus \{\text{pts that correspond to reducible conics}\}$. If $a_0x^2+\cdots+a_5z^2=(b_0x+b_1y+b_2z)(c_0x+c_1y+c_2z)$ then $(a_i)\in\mathbb{P}^5$ is in the image of the map $\mathbb{P}^2\times\mathbb{P}^2\to\mathbb{P}^5$ defined by $[b_0,b_1,b_2],[c_1,c_2,c_3]\mapsto[b_0c_0, b_0c_1+b_1c_1, b_0c_2+b_2c_0, b_1c_1, b_1c_2+b_2c_1, b_2c_2]$. This image, say $Z$, is closed (image of a complete variety under morphism) and $\mathbb{P}^5\setminus Z$ is open [we say that "being irreducible is an open condition"] and parameterised conics in $\mathbb{P}^2$.

Another type of problems: classifying e.g. varieties up to isomorphism. Usually there are discrete invariants (e.g. dimension, genus) that breaks the problem naturally into "connected components" and fixing these may lead to a set that has a structure of variety.

**Example.** Genus 0 curves over $k$ are all isomorphic to $\mathbb{P}^1$, so the variety parametrising them is $\{\text{pt}\}$.

**Example.** Genus 1 curves or elliptic curves. Again we assume the characteristic of $k$ is not 2 or 3. Every $E$ can be given by $y^2=x^3+Ax+B$. Define the $j$invariant by $j(E)=1728\frac{4A^3}{4A^3+27B^2}\in k$, this is unchanged under isomorphism of Weierstrass equations. Conversely, every $j\in k$ is the $j$invariant of some curve, $E_j: y^2+xy=x^3-\frac{36}{j-1728}x-\frac{1}{j-1728}$ $(j\neq 0,1728)$, $E_0: y^2=x^3+1$ and $E_{1728}: y^2=x^3+x$. In over words, genus 1 curves over $k$ up to isomorphism are in one to one correspondence to points $j\in\mathbb{A}^1$ (the $j$-line)

**Exercise.** Show that $E\cong E' \iff j(E)=j(E')$

Generally, consider the set $M_{g,n}=\{$isomorphism classes of (non-singular projective) curves $C$ of genus $g$, with $n$ distinct ordered marked points $P_1,\ldots,P_n\in C\}/\cong$, where we define the isomorphism as $(C,(P_i))\cong(C',(P_i)')$ if there exists isomorphism $\phi: C\to C'$ such that $\phi(P_i)=P_i'$. If we make points unordered, get $M_{g,n}^{\text{sym}}=M_{g,n}/S_n$ (acts by permuting the marked points)

**Example.** (Genus 0) Every $C\cong\mathbb{P}^1$, Aut($\mathbb{P}^1$)= Möbius group, acts triply transitive, so $M_{0,0}=M_{0,1}=M_{0,2}=M_{0,3}=\{\text{pt}\}$. For higher $n$, every $(C,(P_i))\in M_{0,n}$ is represented by a unique curve $(\mathbb{P}^1,(0,1,\infty,P_4,\ldots,P_n))$. So we have natural identification $M_{0,n}=\left(\mathbb{P}^1\setminus\{0,1,\infty\}\right)^{n-3}\setminus\{\text{diagonal}\, x_i=x_j\}$

**Example.** (Genus 1) As we have seen, $M_{1,0}=M_{1,1}=\mathbb{A}^1$ ($j$-line)

**Example.** (Hyperelliptic Curves of fields with characteristic not 2) $C$ hyperelliptic genus $g\geq 2$, $C$ has admits a $2:1$ map to $\mathbb{P}^1$, unique up to an automorphism of $\mathbb{P}^1$. In other words, $C$ has a model $y^2=f(x)$ where $f$ is square free, $\deg f\in\{2g+1,2g+2\}$. The set of $2g+2$ roots of $f$ (including $\infty$ if $\deg f=2g+1$) is an element of $M_{g,2g+2}^{\text{sym}}$, so this is the set that classifies hyperelliptic curves of genus $g$, up to isomorphism.

# 9 Functorial approach

What does it mean for a variety $X$ to classify something? [i.e., for $X$ to be the moduli space for that classification problem]. How does the variety structure on $X$ come in? So far, $\{$our objects over $K\}/\cong\overset{1:1}{\leftrightarrow}$set of points $X(k)$ only specifies $X$ as a set. Over $\mathbb{R},\mathbb{C}$ can appeal to continuity, and insists that "close points" correspond to "close objects". In other words, if we have a continuous family of objects parameterised by some $Y$, we get a map $Y\to X$ defined by (objects above $Y$) $\mapsto X(k)$ which is continuous. This works in our setting, if we replace "continuous" by "morphisms"

**Example.** Lines through origin in $\mathbb{A}^2$, $ax+by=0 \overset{[1:1]}{\leftrightarrow}$points $[a:b] \in \mathbb{P}^1$. A family of such lines over a variety $Y$ is a closed subvariety $L \subseteq Y \times \mathbb{A}^2$ such that every fibre $L_y$ is a line through 0 in $\mathbb{A}^2$.

Such a family gives a map $Y \to \mathbb{P}^1$ defined by $L_y : ax+by=0 \mapsto [a:b]$ which is a morphism. Indeed, intersecting $L \cap Y \times \{(1,t)\}, Y \times \{(t,1)\}$ and projecting onto the $t$-line gives rational functions $f, g$ on $Y$, $fg=1$ and at least one of them regular at every $y \in Y$. So we get a morphism $Y \to \mathbb{P}^1$, $y \mapsto [f(y):1] = [1:g(y)]$.

Moreover, the families over different varieties are related under morphisms $f: X \to Y$. The morphism $f$ takes $(\pi : L \to Y) \mapsto (f^*\pi : L \times_Y X \to X)$ where $L \times_Y X = \{(l,x) \in L \times X | \pi(l) = f(x)\}$ (puts the line above $f(x)$ over $x$). Under the correspondence: families over $Y$ correspond to maps $Y \to \mathbb{P}^1$. This pullback $f^*\pi$ corresponds to composition with $f$, $f^* : \mathrm{Hom}(Y, \mathbb{P}^1) \to \mathrm{Hom}(X, \mathbb{P}^1)$ defined by $\phi \mapsto f \circ \phi$.

**Definition 9.1.** A contravariant functor $\mathcal{F}$ : Varieties/$k \to$ Sets is *representable* (by a variety $Y$) if $\mathcal{F} \cong \mathrm{Hom}(-, Y)$.

Same in any category; similarly a covariant functor is representable if $\mathcal{F} \cong \mathrm{Hom}(Y, -)$

What we showed is that the functor "families of lines through 0 is $\mathbb{A}^2$" is representable by $\mathbb{P}^1$.

**Example.** Say we have a family of lines parametrised by $C \setminus \{P\}$. Does it extend uniquely to a family over $C$? This is equivalent to the question whether a map $C \setminus \{P\} \to \mathbb{P}^1$ extends to $C \to \mathbb{P}^1$? Yes if $P$ is non-singular (because $\mathbb{P}^1$ is complete) (No in general)

Generally, geometry of the representing variety (connected, irreducible, complete, dimension,...)

A few more examples for affine varieties corresponding to covariant functors on $\mathrm{Alg}_k$ (finitely generated $k$-algebras with no nilpotents)

First, take $\mathcal{F} : \mathrm{Alg}_k \to$ Sets defined by $A \mapsto A$ (often called the *forgetful functor*). Is $\mathcal{F}$ representable? I.e., does there exists a ring $R$ such that $\mathrm{Hom}_{\mathrm{Alg}_k}(R, A) \to A$ is one to one and natural? Yes, take $R = k[t]$, then elements of $\mathrm{Hom}(k[t], A)$ determined by image of $t \in A$.

Similarly

- $\mathcal{F}(A) = A$, $R = k[t]$ (the above)
- $\mathcal{F}(A) = A \times A$, $R = k[t_1, t_2]$
- $\mathcal{F}(A) = A^*$ units, $R = k[s,t]/(st-1)$
- $\mathcal{F}(A) = \{$4th root of unity in $A\}$, $R = k[x]/(x^4-1)$. ($\mathrm{char} k \neq 2$)

So a representable functor $\mathcal{F}$ on $\mathrm{Alg}_k$ is one for which has a structure of solutions in $A$ to *a* fixed system of poly equations.

Similar, but not representable: reuse lines through 0 in $\mathbb{A}^2$, reformulated in terms of $k$-algebras. $\mathcal{F}(A) = \{f, g \in A | fA + gA = A\}/A^*$.

It has two subfunctors $\mathcal{F}_1(A) = \{f, g \in A | fA + fA = A, f\,\text{units}\}/A^* = \{g \in A\}$ represented by $k[t]$. $\mathcal{F}_2(A)$ is similar, $g$ unit. So $\mathcal{F}$ corresponds to $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{A}^1$.

Back to $\mathcal{F}_1(A) = \{\text{units in}\, A\} = \mathrm{Hom}(k[x,y]/(xy-1), A)$ and $\mathcal{F}_2(A) = \{\text{elements in}\, A\} = \mathrm{Hom}(k[x], A)$. There is a natural inclusion $\mathcal{F}_1(A) = A^* \hookrightarrow A = \mathcal{F}_2(A)$ (natural means commutes with $A \to B$), corresponds to a homomorphism $k[x] \to k[x,y]/(xy-1)$ defined by $x \mapsto x$.

**Yoneda's Lemma.** *For any category $\mathcal{C}$, $A \to \mathrm{Hom}(A, -)$ is a full embedding of $\mathcal{C}$ into the category of covariant functors $\mathcal{C} \to$* Sets.

Full embedding means: every natural transformation of functors $\mathrm{Hom}(A,-) \to \mathrm{Hom}(B,-)$ is induced by a unique morphism $B \to A$. In particular, $\mathrm{Hom}(A,-) \cong \mathrm{Hom}(B,-)$ if and only if $A \cong B$.

So every moduli problem has at most one representation variety.

*Note.* We don't need $k$ to be algebraically closed. Can talk about moduli problems over any field $K$. E.g., the functor "families of lines in $\mathbb{A}^2$ through $(0,0)$" is representable on the category of algebraic sets over $\mathbb{Q}$. In particular, for every field $K \supseteq \mathbb{Q}$,

$$\{\text{lines in}\, \mathbb{A}^2\, \text{through}\, (0,0)\, \text{defined over}\, K\} \overset{1:1}{\leftrightarrow} \mathrm{Hom}(\mathrm{Spec} L, \mathbb{P}^1_{\mathbb{Q}}) = \mathbb{P}^1(K)$$

This suggest to define the set of *$\mathcal{S}$-rational points* on a variety $X$ for any algebraic sets $\mathcal{S}$ to be $X(S) := \mathrm{Hom}(\mathcal{S}, X)$. In this language the $\mathrm{Hom}(-X)$ is simply "functor of points", $\mathcal{S} \to X(S)$.

Now Yoneda implies that $X$ is determined uniquely by its functor of points. If $S = \operatorname{Spec} A$ we write $X(A) = X(S)$ "solutions in $A$ to a system of polynomial equations"

**Example.** (Product of varieties). Let $V, V'$ be varieties. Naively $V \times V'$ is, as a set, the set of pair $(\mathrm{pt\,in}\,V, \mathrm{pt\,in}\,V')$. This only describe $V \times V'$ as a set, not as a variety.

Construction approach: pass to $\overline{k}$, suppose $V, V'$ affine so $V \subseteq \mathbb{A}^m$ and $V' \subseteq \mathbb{A}^n$. Then $V \times V' \subseteq \mathbb{A}^{m+n}$ irreducible, then glue affine charts in general and deduce its properties (e.g., $(V \times V') \times V'' = V \times (V' \times V'')$, existence of projections $V \times V' \to V$) from the construction.

Functorial approach: Use the "naive" pairs of points description, but for all $\mathcal{S}$. Thus $V \times V'$ is defined as a variety that represents the functor $\mathcal{S} \mapsto V(S) \times V'(S)$. If such a $V \times V'$ exists, it is unique, and all the properties follow from Yoneda. (e.g., the projections $V(S) \times V'(S) \to V(S)$ gives a natural transformation of functors that correspond to a morphism $V \times V' \to V$.)

Important (and unsolved) problem: Characterise representable functors on varieties in an intrinsic way.

# 10 Hilbert Scheme and Standard Moduli Spaces

We started with lines, conics in $\mathbb{P}^2$, Grassmanians. These are special cases of the *Hilbert Scheme*, that classifies closed subsets of $\mathbb{P}^n$ with given discrete invariants specified by *Hilbert polynomial*: Closed $Z \subseteq \mathbb{P}^n$ is a zero set of homogeneous ideal $I \subseteq k[x_0, \dots, x_n]$. Its homogeneous coordinate ring splits into graded pieces, $S = k[x_0, \dots, x_n]/I = \oplus_{d \geq 0} S_d$ (homogeneous of degree $d$). Consider the dimension counting function (the *Hilbert function*) $d \mapsto \dim_k S_d$

**Example.** (Point) Let $Z = \{[1 : 0 : \cdots : 0]\} \subseteq \mathbb{P}^n$ then $I = (x_1, \dots, x_n)$ and $S = k[x_0]$, $\dim_k S_d = (1, 1, 1, \dots)$.

(Linear subspaces) Let $Z = \mathbb{P}^m \subseteq \mathbb{P}^n$, then $S = k[x_0, \dots, x_m]$ and $\dim_k S_d = \binom{d+m}{m} = \frac{1}{m!} d(d-1) \dots (d-m+1)$.

(3 points in $\mathbb{P}^2$) Let $Z = \{P_0, P_1, P_2\}$ be three distinct points. Let $I = \{\mathrm{all}\, f \in k[x_0, x_1, x_2] | f(P_i) = 0 \forall i\}$. The coordinate ring $S = k[x_0, x_1, x_2]/I = \oplus S_d$ depends on whether the $P_i$ are collinear or not. Fixing a choice of coordinates on $P_i$, it is clear that $k[x_0, x_1, x_2]_1 \to k^3$ (linear functions $ax_0 + bx_1 + cx_2$) defined by $f \mapsto (f(P_0), f(P_1), f(P_2))$ is onto if $P_i$ are not collinear, and has 2-dimensional image if the $P_i$ are collinear. So $\dim I_1 = 0$, $\dim S_1 = 3$ if $P_i$ are not collinear, but $\dim I_1 = 1$ and $\dim S_1 = 2$ is $P_i$ are collinear. For $d \geq 2$, it is easy to check that $k[x_0, x_1, x_2]_d \to k^3$ defined by $f \mapsto (f(P_0), f(P_1), f(P_2))$ is onto. So $\dim S_d = 3$. Hence $\dim_k S_d = \begin{cases} (2, 3, 3, \dots) & P_i \text{ collinear} \\ (3, 3, 3, \dots) & \text{else} \end{cases}$.

Hilbert-Serre Theorem implies that for every $Z \subseteq \mathbb{P}^n$ closed, $I = \{f | f(Z) = 0\}$, $S = k[x_0, \dots, x_n]/I$, the sequence $\dim S_d$ stabilises for $d \gg 0$ to coincide with values of a unique polynomial $H_Z(d)$, whose degree is the dimension of $Z$.

**Definition 10.1.** $H_Z(d)$ *is the* Hilbert polynomial *of* $Z$. *Its leading coefficients times* $(\dim Z)!$ *is the* degree *of* $Z$ *in* $\mathbb{P}^n$.

**Example.** (Points) $Z = \{\mathrm{pt}\}$, then $H_Z(d) = 1$ $(\deg Z = 1)$

(Linear subspaces) $\mathbb{P}^m \subseteq \mathbb{P}^n$, then $H_Z(d) = \frac{1}{m!} d(d-1) \dots (d-m+1)$ and $\deg Z = 1$.

(3 points in $\mathbb{P}^2$) $Z = \{P_1, P_2, P_3\}$, $H_Z(d) = 3$ $(\deg Z = 3)$.

$H \subseteq \mathbb{P}^n$ hypersurface, given by $f = 0$, $\deg H = \deg f$ as before.

This polynomial captures the discrete invariants of $Z$.

**Theorem 10.2.** *For every polynomial* $H(d)$*, the functor* $\mathcal{S} \to$families $Y \subseteq S \times \mathbb{P}^n$ of closed subsets with Hilbert polynomial $H(d)$ over $\mathcal{S}$ *is representable by a projective scheme* $\mathrm{Hilb}_H$.

Other closely related functors:

- $\mathrm{Hil}(\mathbb{P}^n) = \coprod_H \mathrm{Hilb}_H$ all closed subsets of $\mathbb{P}^n$ (or rather, flat families of them)

- $\mathrm{Hilb}(X)$ closed subsets of an arbitrary projective variety
- $\underline{\mathrm{Hom}}(X, Y) : S \mapsto \mathrm{Hom}_S(X \times S, Y \times S)$ (sits inside $\mathrm{Hilb}(X \times Y)$ open, $X, Y$ projective)
- $\underline{\mathrm{Isom}}(X, Y) : S \mapsto \mathrm{Isom}_S(X \times S, Y \times S)$ (sits inside $\underline{\mathrm{Hom}}$ open)
- $\underline{\mathrm{Aut}}(X) : T \mapsto \mathrm{Aut}_T(X \times T)$ (Take $X = Y$)

These are all representable (by schemes) if $X, Y$ are projective.

- $\underline{\mathrm{Pic}}(X) : S \mapsto \frac{\mathrm{Pic}_S(X \times S)}{\mathrm{Pic}(S)}$ is also representable if $X$ is complete [and in fact, representable over any field $K$, if $X/K$ has a $K$-rational point]

**Example.** Let $C/K$ be a complete nonsingular curve, $C(K) \neq \emptyset$. Then $\mathrm{Pic}C$ has a structure of a projective scheme, which is a group and $\mathrm{Pic}^0(C)$ is an abelian variety of dimension equal to the genus of $C$. It is called the *Jacobian* variety of $C$, also denote $\mathrm{Pic}^0(C)$ or $\mathrm{Jac}(C)$.