The Formalization of Algebraic Curves

Pan Lin

Supervised by Dr. Yu Fu

Oct 2024

Abstract

The Riemann-Roch theorem plays a crucial role in algebraic geometry. This paper aims to use Lean 4, an efficient proof assistant, to formalize the background definitions and theorems necessary for sketching the Riemann-Roch theorem. I will provide formal definitions of affine and projective algebraic varieties, as well as Zariski cotangent spaces, smooth curves, Weil divisors, Kähler differential forms, and related lemmas. Through this formalization, I hope to establish a rigorous, verified framework that will facilitate the formalization of the Riemann-Roch theorem and explore Lean 4's ability to describe traditional point-set mathematics.

Contents

1 Terminology

The terminology of this paper is mostly consistent to GTM 106 by Silverman.

- We let $\mathbb{N}$ denote the set of natural numbers **including** 0, i.e., $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- For a field $\mathbb{K}$, we let $\mathbb{K}^*$ denote the **multiplicative group** of $\mathbb{K}$, i.e., $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$, the set of all nonzero elements of $\mathbb{K}$ under multiplication.
- We only regard $\mathbb{K}$ as a perfect field.
- We denote by $A \to B$ the set (type) of functions which have domain A and codomain B.
- We denote by $\langle a_0, a_1, \dots, a_n \rangle$ the ideal generated by $a_0, a_1, \dots, a_n \in R$.
- Let M be a module. We denote by $\langle S \rangle$ the submodule (ideal) generated by $S \subseteq M$, and particularly denote by $\langle a_i : i \in I \rangle$ the ideal generated by $\{a_i : i \in I\} \subseteq M$.
- We denote by $\mathrm{Free}_R(S)$ the free R-module generated by the set of symbols S.
- ```
  scoped[MvPolynomial] notation:9000 R "[X,..]" n => MvPolynomial (Fin n) R
  scoped[MvPolynomial] notation:9000 R "[X,..]" n "homo"
      => (homogeneousSubmodule (Fin n) R)
  ```

2 Introduction

Definition 2.1. For any set A and additive abelian group B, the **support** of a function $f : A \to B$ is the set $\mathrm{supp}(f) := \{x \in A : f(x) \neq 0\}$

Definition 2.2. A **function with finite support**, denoted by $f : A \to_0 B$, is a function $f : A \to B$ whose support is finite.

Definition 2.3. For $f : A \to_0 B$, the summation of $f(x)$ over all $x \in A$ is defined as

$$\sum_{x \in A} f(x) := \sum_{x \in \mathrm{supp}(f)} f(x)$$
  ```

3 Affine Varieties

Intuitively, the affine n-space over the field $\mathbb{K}$ can be regard as the n-dimensional space of points, where each point can be represented by an n-tuple of elememts from $\mathbb{K}$, or functionally, a map from a finite index set to $\mathbb{K}$ as shown below.

Definition 3.1. The **affine n-space** over $\mathbb{K}$ is the set of $\mathbb{K}$-valued functions defined on the finite index set

$$\mathbb{A}^n_{\mathbb{K}} := \{0 \mathinner{..} n-1\} \to \mathbb{K}$$

In this section, we defaultly suppose $\mathbb{K}$ is a field, and $n \in \mathbb{N}$ is the dimension of the space we are mentioning.

```
variable {n : ℕ}
variable {K : Type ℓ} [Field K]
```

In Lean4, we define the affine space as below:

```
abbrev 𝔸 (R : Type ℓ) [Ring R] (n : ℕ) : Type ℓ := Fin n → R
```

Definition 3.2. For any ideal I of $\mathbb{K}[X_1, .., X_n]$, the **zero locus** of I is in $\mathbb{A}^n_{\mathbb{K}}$ is the set

$$\mathbb{V}(I) := \{P \in \mathbb{A}^n_{\mathbb{K}} : \forall f \in I, f(P) = 0\}$$

```
abbrev 𝕍 (I : Ideal K[X,..]n) : Set (𝔸 K n) := { P : 𝔸 K n | ∀ f ∈ I, eval P f = 0}
```

For convinience, we directly use the Nullstellensatz package from Mathlib

```
abbrev 𝕍 : Ideal (K[X,..]n) → Set (𝔸 K n) := zeroLocus
```

Definition 3.3. Any subset of $\mathbb{A}^n_{\mathbb{K}}$ is called an **(affine) algebraic set** if it is a zero locus of some ideal of $\mathbb{K}[X_0, .., X_{n-1}]$.

```
structure AlgSet (K : Type ℓ) [Field K] (n : ℕ) : Type ℓ where
  carrier : Set (𝔸 K n)
  gen_by_ideal : ∃ I : Ideal K[X,..]n, 𝕍 I = carrier
```

Definition 3.4. For any algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$, the **vanishing ideal** of V is the set

$$\mathbb{I}(V) := \{f \in \mathbb{K}[X_0, .., X_{n-1}] : \forall P \in V, f(P) = 0\}$$

proposition 3.1. *The vanishing ideal $I(V)$ is an ideal of $\mathbb{K}[X_0, .., X_{n-1}]$*

The vanishing ideal can be defined as below

```
def 𝕀 (V : AlgSet K n) : Ideal K[X,..]n where
  carrier := {f : K[X,..]n | ∀ P ∈ V.1, eval P f = 0}
  add_mem' := by
    intro f g fh gh
    simp at fh gh ⊢
    intro P Ph
    rw [fh P Ph, gh P Ph]
    simp
  zero_mem' := by
    simp
  smul_mem' := by
    intro c f fh
    simp at fh ⊢
    intro P Ph
    right
    exact fh P Ph
```

For convinience, we directly use the Nullstellensatz package from Mathlib

```
abbrev 𝕀 : Set (𝔸 K n) → Ideal K[X,..]n := vanishingIdeal
```

Definition 3.5. For any algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$, the **coordinate ring** of V is the quotient ring

$$\mathbb{K}[V] := \mathbb{K}[X_0, .., X_{n-1}]/\mathbb{I}(V)$$

and the **function field** of V is $\mathbb{K}(V)$ the fraction field of $\mathbb{K}[V]$. A **regular function** is an element of $\mathbb{K}(V)$.

```
def AlgSet.coordRing (V : AlgSet K n) : Type ℓ := (K[X,..]n) / (𝕀 V.1)
instance AlgSet.coordRing.commRing (V : AlgSet K n) : CommRing V.coordRing :=
  Ideal.Quotient.commRing (𝕀 V.1)
```

Definition 3.6. Any subset of $\mathbb{A}^n_{\mathbb{K}}$ is called an **(affine) variety** if it is a zero locus of some prime ideal of $\mathbb{K}[X_0, .., X_{n-1}]$.

```
structure Variety (K : Type ℓ) [Field K] (n : ℕ) : Type ℓ where
  carrier : Set (𝔸 K n)
  gen_by_prime : ∃ I : Ideal K[X,..]n, I.IsPrime ∧ 𝕍 I = carrier
```

proposition 3.2. *An affine variety is an affine algebraic set.*

```
def Variety.toAlgSet (A : Variety K n) : AlgSet K n := {
  carrier := A.carrier
  gen_by_ideal := Exists.elim A.gen_by_prime $ by
    rintro I₀ ⟨_, h⟩
    exists I₀
}
```

Definition 3.7. The **maximal ideal corresponding to the point** $P = (x_0, .., x_{n-1}) \in \mathbb{A}^n_{\mathbb{K}}$ is the vanishing ideal $\mathfrak{m}_P := \mathbb{I}(\{P\})$. If there is an affine variety $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ s.t.$P \in V$, the **maximal ideal at the point** P **of the affine variety** V is defined as the maximal ideal $\mathfrak{m}_{V,P} := \mathfrak{m}_P/\mathbb{I}(V) \subseteq \mathbb{K}[V]$.

```
def AlgSet.𝔪 (V : AlgSet K n) {P : 𝔸 K n} (_ : P ∈ V) : Ideal V.coordRing where
  carrier := {f : V.coordRing | ∃ f₀ ∈ 𝕀 {P}, Ideal.Quotient.mk (𝕀 V.1) f₀ = f}
  add_mem' := by
    simp
    intro f g f₀ fh0 fh g₀ gh0 gh
    exists f₀ + g₀
    constructor
    . simp [eval_add, fh0, gh0]
```

```
  . show Ideal.Quotient.mk _ f₀ + Ideal.Quotient.mk _ g₀ = f + g
    rw [fh, gh]
zero_mem' := by exists 0; simp
smul_mem' := by
  simp
  apply Quotient.ind
  intro k f fh0
  exists k * f
  simp [fh0]
  congr
```

Theorem 3.3. *For $P \in \mathbb{A}^n_{\mathbb{K}}$, the ideal $\mathfrak{m}_P$ is maximal in $\mathbb{K}[X_0, .., X_{n-1}]$.*

Theorem 3.4. *For $P = (x_0, .., x_{n-1}) \in \mathbb{A}^n_{\mathbb{K}}$, we have $\mathfrak{m}_P = \langle X_0 - x_0, .., X_{n-1} - x_{n-1} \rangle$*

Theorem 3.5. *For algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $P \in V$, the ideal $\mathfrak{m}_{V,P}$ is maximal in $\mathbb{K}[V]$.*

Definition 3.8. For any variety $V \subseteq \mathbb{P}^n_{\mathbb{K}}$, the **(Krull) dimension** of V, denoted by $\dim V$, is the maximal n of strict chains $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ where $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ are prime ideals of $\mathbb{K}[V]$.

In this paper, since we only need to talk about one-dimensional varieties, I did not formalize this definition.

Definition 3.9. For any affine variety $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $P \in V$, the **(Zariski) cotangent space** at $P \in V$ is the structure $T^*_P V := \mathfrak{m}_{V,P}/\mathfrak{m}^2_{V,P}$.

```
abbrev AlgSet.cotKer (V : AlgSet K n) {P : 𝔸 K n} (_ : P ∈ V)
    : Submodule V.coordRing (V.m P) :=
  V.m P • ⊤
abbrev AlgSet.cotSpace (V : AlgSet K n) {P : 𝔸 K n} (PinV : P ∈ V) : Type ℓ :=
  V.m P / V.cotKer PinV
```

proposition 3.6. *For any affine variety $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $P \in V$, $T^*_P V$ is a finite-dimensional linear space over the residue field $\mathbb{K}[X_0, .., X_{n-1}]/\mathfrak{m}_P$.*

proposition 3.7. $\dim V \leq \dim T_P^* V \leq n$

Proof. Suppose $(f + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2 \in T_P^* V$ and $k + \mathfrak{m}_P \in \mathbb{K}[X_0, .., X_{n-1}]/\mathfrak{m}_P$. Define the scalar multiplication $(k + \mathfrak{m}_P) \bullet ((f + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2) := ((kf + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2)$.

We arbitrarily pick $p \in \mathfrak{m}_P$ and $q \in \mathbb{I}(V)$, then

$$\begin{aligned}
&(k + p + \mathfrak{m}_P) \bullet ((f + q + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2) \\
&= ((k + p) \cdot (f + q) + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2 \\
&= (k \cdot f + k \cdot q + p \cdot (f + q) + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2 \\
&= (k \cdot f + p \cdot (f + q) + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2 && (k \cdot q \in \mathbb{I}(V)) \\
&= ((k \cdot f + \mathbb{I}(V)) + (p \cdot (f + q) + \mathbb{I}(V))) + \mathfrak{m}_{V,P}^2 \\
&= (k \cdot f + \mathbb{I}(V)) + \mathfrak{m}_{V,P}^2 && (p \cdot (f + q) + \mathbb{I}(V) \in \mathfrak{m}_{V,P}^2)
\end{aligned}$$

implying the scalar multiplication is well-defined. The abelian group properties of $T_P^* V$ is given by the quotient ring, and it is easy to prove the other four properties. □

```
instance AlgSet.maximalIdeal {V : AlgSet K n} {P : 𝔸 K n} (PinV : P ∈ V)
    : IsMaximal (𝔪 PinV)

instance AlgSet.cotSpace.addCommGroup {V : AlgSet K n} {P : 𝔸 K n} {PinV : P ∈ V}
    : AddCommGroup (cotSpace PinV) :=
  Submodule.Quotient.addCommGroup (cotKer PinV)

instance AlgSet.cotSpace.module {V : AlgSet K n} {P : 𝔸 K n} {PinV : P ∈ V}
    : Module (V.coordRing/𝔪 PinV) (cotSpace PinV) :=
  Module.instQuotientIdealSubmoduleHSMulTop (𝔪 PinV) (𝔪 PinV)

instance AlgSet.residueField {V : AlgSet K n} {P : 𝔸 K n} {PinV : P ∈ V}
    : Field (V.coordRing / 𝔪 PinV) := Ideal.Quotient.field (𝔪 PinV)

instance AlgSet.cotSpace.finiteDimensional {V : AlgSet K n} {P : 𝔸 K n} {PinV : P ∈ V}
```

```
  : FiniteDimensional (V.coordRing/𝕞 PinV) (cotSpace PinV)
```

4 Projective Varieties

Definition 4.1. The **projective** n**-space** is the quotient set

$$\mathbb{P}^n_{\mathbb{K}} := (\mathbb{A}^n_{\mathbb{K}} \backslash \{(0,..,0)\})/\sim$$

where for $P, Q \in \mathbb{A}^n_{\mathbb{K}} \backslash \{(0,..,0)\}$, let $P \sim Q$ if and only if $\exists k \in \mathbb{K}, P = kQ$ where $(kQ)(i) := k \cdot Q(i)$.

```
abbrev no0 (A : Type ℓ) [Zero A] : Type ℓ := {x : A // x ≠ 0}

variable {K : Type ℓ} [Field K]
variable {n : ℕ}

namespace 𝔸

instance : NoZeroSMulDivisors K (𝔸 K n) where
  eq_zero_or_eq_zero_of_smul_eq_zero := by
    intros k P kPh
    simp [𝔸] at P
    have kPh' := congrFun kPh
    simp [forall_or_left] at kPh'
    cases kPh'
    case inl h => left; assumption
    case inr h => right; exact funext h

namespace no0

def mul' (a b : no0 K) : no0 K := ⟨a.1 * b.1, by simp [a.2, b.2]⟩

theorem mul_assoc' : ∀ (a b c : no0 K), mul' (mul' a b) c = mul' a (mul' b c) := by
```

```
  intros a b c
  simp only [mul', mul_assoc]

def one' : no0 K := ⟨1, by simp⟩

theorem one_mul' : ∀ (a : no0 K), mul' one' a = a := by
  intro ⟨a1, ah⟩
  simp [mul', one']

theorem mul_one' : ∀ (a : no0 K), mul' a one' = a := by
  intro ⟨a, ah⟩
  simp [mul', one']

def inv' (a : no0 K) : no0 K := ⟨a.1⁻¹, by simp [a.2]⟩

theorem mul_left_inv' : ∀ (a : no0 K), mul' (inv' a) a = one' := by
  intro ⟨a, ah⟩
  simp [mul', inv', one']
  rw [←mul_inv_cancel ah]
  apply mul_comm

theorem mul_comm' : ∀ (a b : no0 K), mul' a b = mul' b a := by
  intro a b
  simp only [mul', mul_comm]

instance : CommGroup (no0 K) where
  mul := mul'
  mul_assoc := mul_assoc'
  one := one'
  one_mul := one_mul'
```

```
  mul_one := mul_one'
  inv := inv'
  mul_left_inv := mul_left_inv'
  mul_comm := mul_comm'

@[simp]
def smul' (k : no0 K) (P: no0 (𝔸 K n)) : no0 (𝔸 K n) := ⟨ k.1 • P.1, by
  intro kPh
  rw [smul_eq_zero] at kPh
  cases kPh
  case inl h => exact absurd h k.2
  case inr h => exact absurd h P.2
⟩

theorem one_smul' : ∀ (b : no0 (𝔸 K n)), smul' one' b = b := by
  intro b
  simp [smul', one']

theorem mul_smul' : ∀ (x y : no0 K) (b : no0 (𝔸 K n))
, smul' (mul' x y) b = smul' x (smul' y b) := by
  intro ⟨x, xh⟩ ⟨y, yh⟩ ⟨b, bh⟩
  simp only [smul', mul', mul_smul]

instance : MulAction (no0 K) (no0 (𝔸 K n)) where
  smul := smul'
  one_smul := one_smul'
  mul_smul := mul_smul'

@[simp]
abbrev collinear : no0 (𝔸 K n) → no0 (𝔸 K n) → Prop
```

```
| xs, ys => ∃ k : no0 K, xs = k • ys

namespace collinear

theorem refl' (xs : no0 (𝔸 K n))
: collinear xs xs := by
  dsimp [collinear]
  exists 1
  simp

theorem symm' {xs ys : no0 (𝔸 K n)}
: collinear xs ys → collinear ys xs := by
  rintro ⟨k, h⟩
  exists k⁻¹
  symm
  simp [h]

theorem trans' {xs ys zs : no0 (𝔸 K n)}
: collinear xs ys → collinear ys zs → collinear xs zs := by
  rintro ⟨k1, h1⟩ ⟨k2, h2⟩
  exists k1 * k2
  rw [mul_smul, ←h2]
  exact h1

instance eqv {n : ℕ} : Setoid (no0 (𝔸 K n)) where
  r := collinear
  iseqv := {
    refl := refl',
    symm := symm',
    trans := trans'
```

```
}

theorem smul_closed (P₀ : no0 (𝔸 K n))
: ∀ k : no0 K, Quotient.mk eqv (k • P₀) = Quotient.mk eqv (P₀) := by
  intro k
  simp [collinear]
  exists k

end collinear
end no0
end 𝔸

def ℙ (K : Type ℓ) [Field K] (n : ℕ) : Type ℓ :=
  Quotient (𝔸.no0.collinear.eqv : Setoid (no0 (𝔸 K n.succ)))

namespace ℙ

notation "𝔸≃" => 𝔸.no0.collinear.eqv

abbrev mk : no0 (𝔸 K n.succ) → ℙ K n :=
  Quotient.mk (𝔸≃ : Setoid (no0 (𝔸 K n.succ)))
```

Definition 4.2. For any homogeneous ideal I of graded ring $\mathbb{K}[X_1, .., X_n]$, the **zero locus** of I in $\mathbb{P}^n_{\mathbb{K}}$ is the set

$$\mathbb{V}(I) := \{[P] \in \mathbb{P}^n : \forall P_0 \in [P], \forall f \in I, f(P_0) = 0\}$$

```
abbrev HomogeneousIdeal.zero_locus (I : HomogeneousIdeal K[X,..] n+1 homo)
    : Set (ℙ K n) :=
  { P : ℙ K n | ∀ f ∈ I, P.vanish f}
```

Definition 4.3. Any subset of $\mathbb{P}^n_{\mathbb{K}}$ is called an **(projective) algebraic set** if it is a zero locus of some homogeneous ideal of $\mathbb{K}[X_0, .., X_n]$.

```
def 𝕍 (I : HomogeneousIdeal (K[X,..] n+1 homo)) : AlgSet K n := ⟨I.zero_locus, by exists I⟩
```

Definition 4.4. Let $\mathbb{P}^n_{\mathbb{K}}\backslash j := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n_{\mathbb{K}} : x_j \neq 0\}$. For $j = 0..n$, the j-th **affine chart** of $\mathbb{P}^n_{\mathbb{K}}$ is the bijection

$$\psi_j : \mathbb{A}^n_{\mathbb{K}} \leftrightarrow \mathbb{P}^n_{\mathbb{K}}\backslash j$$

$$\psi_j(x_0, \ldots, x_n) := [x_0, \ldots, x_{j-1}, 1, x_j, \ldots, x_{n-1}]$$

$$\psi_j^{-1}[x_0 : \cdots : x_n] := \left(\frac{x_0}{x_j}, \ldots, \frac{x_{j-1}}{x_j}, \ldots, \frac{x_{n-1}}{x_j}\right)$$

```
def ℙ.ne0_at (j : Fin n.succ) (P : ℙ K n) : Prop :=
  ∀ P₀ : no0 (𝔸 K n.succ), ℙ.mk P₀ = P → P₀.1 j ≠ 0

abbrev ℙ.Part (K : Type ℓ) [Field K] (n : ℕ) (j : Fin n.succ) : Type ℓ :=
  {P : ℙ K n // P.ne0_at j}

abbrev 𝔸.no0.Part (K : Type ℓ) [Field K] (n : ℕ) (j : Fin n.succ) : Type ℓ
:= {P : no0 (𝔸 K n.succ) // P.1 j ≠ 0}

instance 𝔸.no0.Part.collinear.eqv {j : Fin n.succ}
    : Setoid (𝔸.no0.Part K n j)
:= Subtype.instSetoid_mathlib (λ P : no0 (𝔸 K n.succ) ↦ P.1 j ≠ 0)

def 𝔸.no0.Part.toℙPart (P : 𝔸.no0.Part K n j)
    : ℙ.Part K n ⟨j.1, by linarith [j.2]⟩ := ⟨ℙ.mk P.1, (by
  simp [𝔸.no0.Part] at P
  simp [ℙ.ne0_at]
  intro _ _ P₀h
  rw [ℙ.eq_iff] at P₀h
  rcases P₀h with ⟨k, k_no0, kh⟩
```

```
  simp [k.2, P.2]
)⟩

def 𝔸.no0.Part.Equivℙpart (j : Fin n.succ)
    : Quotient (@𝔸.no0.Part.collinear.eqv K _ n j) ≃ ℙ.Part K n j  := by
  symm
  apply Equiv.subtypeQuotientEquivQuotientSubtype
  intro ⟨P, P_ne0⟩
  simp [ℙ.ne0_at, ℙ.mk]
  constructor
  . intro Pj_ne0 Q  Q_ne0 Q_eqv_P
    rw [Quotient.eq] at Q_eqv_P
    rcases Q_eqv_P with ⟨⟨k, k_ne0⟩, Q_eq_kP⟩
    simp [.•., SMul.smul] at Q_eq_kP
    simp [Q_eq_kP]
    exact ⟨k_ne0, Pj_ne0⟩
  . intro h
    exact h P P_ne0 rfl
  simp [Setoid.r, .•., SMul.smul, .≈.]

def 𝔸.toℙ (j : Fin n.succ) (P : 𝔸 K n) : ℙ K n := ℙ.mk ⟨
  (λ i ↦
    if oh : i < j then P ⟨i, by
      have jh := j.2
      simp [LT.lt, Nat.lt] at oh jh
      exact Nat.le_trans oh jh
    ⟩
    else if ohh : i = j then 1
    else match i with
      | ⟨.zero, _⟩ => by
```

```
        simp at oh ohh
        have := ohh oh.symm
        contradiction
      | ⟨.succ i₀, i₀h⟩ => P ⟨i₀, Nat.le_of_succ_le_succ i₀h⟩
  ), by
    intro F
    have := congrFun F j
    simp at this
⟩

def 𝔸.toℙPart (j : Fin n.succ) (P : 𝔸 K n) : ℙ.Part K n j
:= ⟨P.toℙ j, by
    simp [ℙ.ne0_at, 𝔸.toℙ]
    intro P₀ P₀_ne0 P₀h
    rw [Quotient.eq] at P₀h
    simp [HasEquiv.Equiv, Setoid.r] at P₀h
    rcases P₀h with ⟨k, k_ne0, kh⟩
    simp [.•., SMul.smul, 𝔸.no0.smul'] at kh
    have := congrFun kh j
    simp at this
    rw [this]
    exact k_ne0
  ⟩

def 𝔸.no0.Part.to𝔸 (j : Fin n.succ) (P : 𝔸.no0.Part K n j) : 𝔸 K n
:= λ i ↦
  if i.1 < j.1 then
    P.1.1 ⟨i.1, by apply lt_trans i.2; simp⟩ / P.1.1 j
  else
    P.1.1 ⟨i.1.succ, by rw [Nat.succ_lt_succ_iff]; exact i.2⟩ / P.1.1 j
```

```
instance 𝔸.instSetoidEq : Setoid (𝔸 K n) := ⟨Eq, Eq.refl, Eq.symm, Eq.trans⟩

def ℙ.Part.to𝔸 {j : Fin n.succ} (P : Part K n j) : 𝔸 K n
:= ((𝔸.no0.Part.EquivℙPart j).invFun P).lift (𝔸.no0.Part.to𝔸 j) $ by
  simp
  intro P P_ne0 Pj_ne0 Q Q_ne0 Qj_ne0 P_eqv_Q
  rcases P_eqv_Q with ⟨⟨k, k_ne0⟩, P_eq_kQ⟩
  simp [.•.,SMul.smul] at P_eq_kQ
  ext i
  simp [𝔸.no0.Part.to𝔸]
  simp [P_eq_kQ, mul_div_mul_left _ _ k_ne0]

def AffineChart (K : Type ℓ) [Field K] (n : ℕ) (j : Fin n.succ)
    : 𝔸 K n ≃ ℙ.Part K n j := {
  toFun := 𝔸.toℙPart j
  invFun := ℙ.Part.to𝔸
  left_inv := by
    simp [Function.LeftInverse, 𝔸.toℙPart,
      ℙ.Part.to𝔸, 𝔸.toℙ, ℙ.mk, 𝔸.no0.Part.EquivℙPart,
      Equiv.subtypeQuotientEquivQuotientSubtype, Quotient.hrecOn,
      Quot.hrecOn, Quot.recOn, Quot.rec]
    intro P
    funext i
    simp [𝔸.no0.Part.to𝔸]
    if oh : i.1 < j.1 then
    . simp [oh]
      intro j_le_i
      have : i.1 ≥ j.1 := by apply j_le_i
      have : False := by linarith
```

```
    contradiction
  else
  . simp [oh]
    simp at oh
    if ohh : i.1.succ < j.1 then
      have : False := by linarith
      contradiction
    else
      simp at ohh
      simp [show ¬(⟨i.1 + 1, by linarith [i.2]⟩ < j) by
        simp
        rcases j with ⟨j₁, j₁h⟩
        apply Fin.mk_le_mk.mpr
        apply ohh.ge
      ]
      intro ohhh
      rw [←ohhh, Fin.val_mk] at oh
      have : False := by linarith
      contradiction

right_inv := by
  simp [Function.RightInverse, Function.LeftInverse, 𝔸.toℙPart,
    ℙ.Part.to𝔸, 𝔸.toℙ, 𝔸.no0.Part.EquivℙPart,
    Equiv.subtypeQuotientEquivQuotientSubtype, Quotient.hrecOn,
    Quot.hrecOn, Quot.recOn, Quot.rec]
  intro P Pj_ne0
  rcases P with ⟨Pₐ⟩
  show _ = ⟦Pₐ⟧
  rw [Quotient.eq]
  simp [.≈., Setoid.r]
```

```
exists (Pₐ.1 j)⁻¹
have Pₐj_inv_ne0 : (Pₐ.1 j)⁻¹ ≠ 0 := by
  simp [ℙ.ne0_at, ℙ.mk] at Pj_ne0
  apply inv_ne_zero (Pj_ne0 Pₐ Pₐ.2 $ by dsimp [Quotient.mk])
exists Pₐj_inv_ne0
apply Subtype.eq
simp [𝔸.no0.Part.to𝔸, .•., SMul.smul]
ext i
if oh : i < j then
  simp [oh, 𝔸.no0.Part.to𝔸]
  rw [Fin.lt_def] at oh
  simp [oh]
  rw [div_eq_mul_inv, mul_comm]
else if ohh : i = j then
  simp [oh, ohh]
  rw [←GroupWithZero.mul_inv_cancel _ Pₐj_inv_ne0, inv_inv]
else
  simp [oh, ohh]
  rcases i with ⟨i₀, i₀h⟩
  cases i₀ with
  | zero =>
    simp at oh ohh
    exact (ohh oh.symm).elim
  | succ i' =>
    rcases j with ⟨j', j'h⟩
    simp [] at oh ohh ⊢
    if ohhh : i' < j' then
      simp [ohhh]
      rw [div_eq_mul_inv, mul_comm]
      have : i' + 1 = j' := by linarith
```

```
        contradiction
      else
        simp [ohhh]
        rw [div_eq_mul_inv, mul_comm]
}
```

Definition 4.5. The **homogenization** of a polynomial $f \in \mathbb{K}[X_0, .., X_{n-1}]$ with respect to X_j is a homogeneous polynomial

$$f_{\bar{j}}(X_0, \ldots, X_n) := X_j^{\deg(f)} \cdot f(\frac{X_0}{X_j}, \ldots, \frac{X_{j-1}}{X_j}, \frac{X_{j+1}}{X_j}, \ldots, \frac{X_n}{X_j})$$

```
def homogenization (j : Fin n.succ) (p : K[X,..]n) : (K[X,..]n.succ) :=
   m ∈ p.support,
   aeval (embX j) (monomial m (coeff m p)) * (X j)^(p.totalDegree + 1 - degree m)
```

Definition 4.6. The **dehomogenization** of a homogeneous polynomial $f \in \mathbb{K}[X_0, .., X_{n-1}]_d$ with respect to X_j is a polynomial

$$f_{[j]} := f(X_0, \ldots, X_{j-1}, 1, X_{j+1}, \ldots, X_n)$$

```
def dehomogenization (j : Fin n.succ) : (K[X,..]n.succ) →ₐ[K] K[X,..]n :=
  aeval (dehX j)
```

Definition 4.7. The j**-th projective closure** of an affine algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ is the projective algebraic set

$$V_{\bar{j}} := \mathbb{V}(\langle f_{\bar{j}} : f \in \mathbb{I}(V) \rangle)$$

```
def 𝔸.AlgSet.projClosure (V : 𝔸.AlgSet K n) (j : Fin n.succ) : ℙ.AlgSet K n :=
  ℙ.𝕍 ⟨Ideal.span (MvPolynomial.homogenization j '' (𝔸.𝕀 V.1)), (by
    apply Ideal.homogeneous_span
    intro f ⟨f', _, homo_f'_eq_f⟩
    simp [SetLike.Homogeneous, ←homo_f'_eq_f]
```

```
  exists f'.totalDegree
  apply isHomogeneous_homogenization
))
```

Definition 4.8. The **j-th affine part** of an projective algebraic set $V \subseteq \mathbb{P}^n_{\mathbb{K}}$ is the set

$$V_{[j]} := \psi_j^{-1}(V \cap \mathbb{P}^n_{\mathbb{K}} \backslash j)$$

proposition 4.1. *$V_{[j]}$ is an affine variety for any projective space V and index j.*

Definition 4.9. Any subset of $\mathbb{P}^n_{\mathbb{K}}$ is called an **(projective) variety** if it is a zero locus of some prime homogeneous ideal of $\mathbb{K}[X_1, .., X_n]$.

Definition 4.10. For any projective variety $V \subseteq \mathbb{P}^n_{\mathbb{K}}$, the **(Zariski) cotangent space** of $P \in V$ is the cotangent space $T^*_P V := T^*_{\psi_j^{-1}(P)} V_{[j]}$ for some j.

```
def AlgSet.cotSpace {V : AlgSet K n} {j : Fin n.succ} {P : ℙ.Part K n j}
    (PinV : P.to𝔸 ∈ V.affinePart j) : Type ℓ :=
  (V.affinePart j).cotSpace PinV
```

proposition 4.2. *The definition above is valid for each $P \in V$ and does not depend on the choice of j.*

Definition 4.11. For any projective variety $V \subseteq \mathbb{P}^n_{\mathbb{K}}$, a point $P \in V$ is **smooth (nonsingular)** if $\dim T^*_P V = \dim V$.

5 Smooth Curves

Definition 5.1. A projective/affine variety V is **smooth (nonsingular)** if all points in V are smooth.

Definition 5.2. An **(algebraic) curve** is a 1-dimensional projective variety.

6 Divisors

Definition 6.1. The order of $f \in \mathbb{K}[C]_P$ at $P \in C$ is

$$\mathrm{ord}_P(f) := \sup\{d \in \mathbb{Z} : f \in \mathfrak{m}^d_{C,P}\}$$

Definition 6.2. The order of $f \in \mathbb{K}(C)^*$ at $P \in C$ is

$$\mathrm{ord}_P\left(\frac{f}{g}\right) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$$

Definition 6.3. A function $t \in \mathbb{K}(C)$ is said to be a **uniformizer** for the curve C at $P \in C$ if $\mathrm{ord}_P(t) = 1$, i.e. t is a generator for the maximal ideal $\mathfrak{m}_{C,P}$.

Definition 6.4. A function f is said to be **regular** at $P \in C$ if $\mathrm{ord}_P(f) \geq 0$, and is said to be **nonvanishing** at $P \in C$ if $\mathrm{ord}_P(f) \leq 0$.

Let C be a curve over an algebraically closed field $\mathbb{K}$. If $f \in \mathbb{K}(C)$ is regular at P, then we can evaluate $f(P) \in \mathbb{K}$; otherwise, we denote $f(P) = \infty$.

Definition 6.5. The **divisor group** of a curve C is the free abelian group

$$\mathrm{Div}(C) := \mathrm{Free}_{\mathbb{Z}}C$$

A **divisor** is an element $D \in \mathrm{Div}(C)$, which can be written as a formal sum

$$D = \sum_{P \in C} n_P\,[P]$$

where $n_P = 0$ for all but finitely many $P \in C$.

The order of the divisor D at $P \in C$ is defined by $\mathrm{ord}_P(D) := n_P$.

Definition 6.6. The degree of a divisor $D \in \mathrm{Div}(C)$ is

$$\deg D := \sum_{P \in C} \mathrm{ord}_P(D) \cdot \dim(\mathbb{K}[X_0, .., X_n]/\mathfrak{m}_P)$$

Particularly, if C is over an algebraically closed field $\mathbb{K}$, then

$$\deg D = \sum_{P \in C} \mathrm{ord}_P(D)$$

proposition 6.1. $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ *is a homomorphism of abelian groups.*

Definition 6.7. The **degree-0 divisor group** of a curve C is

$$\mathrm{Div}^0(C) := \ker(\deg) = \{D \in \mathrm{Div}(C) : \deg D = 0\}$$

Definition 6.8. The **principal divisor** associate to a function $f \in \mathbb{K}(C)^*$ is

$$\operatorname{div}(f) := \sum_{P \in C} \operatorname{ord}_P(f)\,[P]$$

Definition 6.9. $\operatorname{div} : \mathbb{K}(C)^* \to \operatorname{Div}^0(C)$ is defined as a homomorphism of abelian groups.

Definition 6.10. The **principal divisor group** of a curve C is $\operatorname{div}(C) := \operatorname{im}(\operatorname{div})$.

Definition 6.11. The **Picard group (divisor class group)** of a curve C is the quotient group $\operatorname{Pic}(C) := \operatorname{Div}(C)/\operatorname{div}(C)$, and we define the **degree-**0 **part of Picard group** as the quotient $\operatorname{Pic}^0(C) := \operatorname{Div}^0(C)/\operatorname{div}(C)$

proposition 6.2. *For $f \in \mathbb{K}(C)^*$, $\operatorname{div}(f) = 0$ iff f is a nonzero constant.*

proposition 6.3. *For $f \in \mathbb{K}(C)^*$, $\deg(\operatorname{div}(f)) = 0$*

Definition 6.12. A divisor $D \in \operatorname{Div}(C)$ is **effective**, denoted by $D \geq 0$, if $\operatorname{ord}_P(D) \geq 0$ for $P \in C$. We say $D_1 \leq D_2$ if $D_2 - D_1$ is effective.

7 Differentials

In the remainder of this note, we assume that $\mathbb{K}$ is an algebraically closed field and C is an algebraic curve over $\mathbb{K}$.

Definition 7.1. The **space of (Kähler) differential forms** on C over $\mathbb{K}$ is the $\mathbb{K}$-linear space generated by the form $\mathrm{d}f$ for each $f \in \mathbb{K}(C)$ s.t. for $f, g \in \mathbb{K}(C), c \in \mathbb{K}$,

$$\mathrm{d}(f+g) = \mathrm{d}f + \mathrm{d}g \tag{linearity}$$

$$\mathrm{d}(fg) = g\mathrm{d}f + f\mathrm{d}g \tag{Leibniz law}$$

$$\mathrm{d}c = 0 \tag{vanishing constants}$$

It can be defined by the quotient $\mathbb{K}$-linear space

$\Omega_C := \operatorname{Free}_{\mathbb{K}}\{\mathrm{d}f : f \in \mathbb{K}(C)\} \;/\; \langle \mathrm{d}(f+g) - \mathrm{d}f - \mathrm{d}g,\ \mathrm{d}(fg) - g\mathrm{d}f - f\mathrm{d}g,\ \mathrm{d}c :\ f, g \in \mathbb{K}(C),\ c \in \mathbb{K} \rangle$

proposition 7.1. $\dim_{\mathbb{K}(C)} \Omega_C = 1$

proposition 7.2. *For all $\omega \in \Omega_C$, there exists a unique function $g \in \mathbb{K}(C)$ s.t. $\omega = g\mathrm{d}t$.*

Definition 7.2. We denote by $\frac{\omega}{\mathrm{d}t}$ the unique g, which only depends on $\omega \in \Omega_C$ and t, given by 7.2

proposition 7.3. *If $f \in \mathbb{K}(C)$ is regular at P, then $\frac{\mathrm{d}f}{\mathrm{d}t}$ is regular at P.*

proposition 7.4. *For all $\omega \in \Omega_C$ with $\omega = 0$, $\mathrm{ord}_P(\frac{\omega}{\mathrm{d}t})$ does not depend on the choice of uniformizer t.*

Definition 7.3. By 7.4, we can define the **order of the differential form** $\omega \in \Omega_C$ at P as

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P\left(\frac{\omega}{\mathrm{d}t}\right)$$

proposition 7.5. $(P \mapsto \mathrm{ord}_P(f)) : C \to_0 \mathbb{Z}$

Definition 7.4. The **divisor associated to the differential form** $\omega \in \Omega_C$ is defined as

$$\mathrm{div}(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega)\,[P]$$

Definition 7.5. The differential form $\omega \in \Omega_C$ is said to be **regular (or holomorphic)**

proposition 7.6. $\mathrm{div} : \Omega_C \to \mathrm{Div}(C)$ *is a homomorphism of abelian groups.*

proposition 7.7. *For $\omega_1, \omega_2 \in \Omega_C$, we have* $\mathrm{div}(\omega_1) + \mathrm{div}(C) = \mathrm{div}(\omega_2) + \mathrm{div}(C) \in \mathrm{Pic}(C)$.

Definition 7.6. The **canonical divisor class** on C is defined as

$$K_C := \mathrm{div}(\omega) + \mathrm{div}(C)$$

whatever the choice of $\omega \in \Omega_C$ due to 7.7. Any divisor in the canonical divisor class is called a **canonical divisor**.

8 Riemann Roch Theorem

Definition 8.1. For $D \in \mathrm{Div}(C)$, the **Riemann-Roch space** associate to D is the set

$$\mathcal{L}(D) := \{f \in \mathbb{K}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}$$

proposition 8.1. *For $D \in \mathrm{Div}(C)$, $\mathcal{L}(D)$ is a finite-dimensional $\mathbb{K}$-linear space.*

Definition 8.2. $\ell(D) := \dim_{\mathbb{K}}(\mathcal{L}(D))$

Theorem 8.2 (Riemann-Roch)**.** *For smooth curve C, there exists $g \in \mathbb{N}$, such that*

$$\ell(D) - \ell(\mathbb{K}_C - D) = \deg D - g + 1$$

Such g is called the genus of C.