# MA40188 ALGEBRAIC CURVES
# 2015/16 SEMESTER 1

ZIYU ZHANG

## 1. Affine Algebraic Sets

We introduce affine spaces and define an affine algebraic set as the common zeroes of a set of polynomials. We study some basic properties of algebraic sets, and use the Hilbert basis theorem to show that every algebraic set is the intersection of finitely many hypersurfaces.

### 1.1. Affine spaces and affine algebraic sets.

In the entire course, a ring always means a commutative ring with a multiplicative identity 1, and a field always means an algebraically closed field of characteristic 0, unless otherwise specified. Here a field $\Bbbk$ is *algebraically closed* if every non-constant polynomial $f(x) \in \Bbbk[x]$ has a root in $\Bbbk$. For example, $\mathbb{C}$ is an algebraically closed field of characteristic 0, but $\mathbb{R}$ is not algebraically closed. Although many theorems can be generalised to other fields, their statements are often simpler with these extra assumptions on the underlying field.

**Definition 1.1.** Let $\Bbbk$ be a field, $n \in \mathbb{Z}_+$. An $n$-dimensional *affine space* over $\Bbbk$ is the set

$$\{(a_1, \cdots, a_n) \mid a_1, \cdots, a_n \in \Bbbk\}.$$

denoted by $\mathbb{A}^n_{\Bbbk}$ (or simply $\mathbb{A}^n$ if the field is understood in the context).

This notion is actually quite familiar. It is simply the set $\Bbbk^n$ of $n$-tuples of elements in $\Bbbk$. However, we do not use the notation $\Bbbk^n$ in algebraic geometry because we are not just interested in its structure as a vector space. Indeed, the geometric objects that we will study are some subsets of affine spaces. More precisely,

**Definition 1.2.** A subset $X \subseteq \mathbb{A}^n_{\Bbbk}$ is called an *affine algebraic set* (or simply *algebraic set*) if there is a set $S$ of polynomials in $\Bbbk[x_1, \cdots, x_n]$, such that

$$X = \{(a_1, \cdots, a_n) \in \mathbb{A}^n_{\Bbbk} \mid f(a_1, \cdots, a_n) = 0 \text{ for all } f \in S\}.$$

In such a case we say $X$ is the algebraic set defined by $S$ and write $X = \mathbb{V}(S)$.

In this definition $S$ could have finitely many or infinitely many elements. If $S$ contains only finitely many polynomials, say, $S = \{f_1, f_2, \cdots, f_r\}$, we usually write $X = \mathbb{V}(f_1, f_2, \cdots, f_r)$ instead of $X = \mathbb{V}(\{f_1, f_2, \cdots, f_r\})$ for simplicity. In particular we have

**Definition 1.3.** An algebraic set $X \subseteq \mathbb{A}^n_{\Bbbk}$ is called a *hypersurface* if $X = \mathbb{V}(f)$ for some non-constant polynomial $f \in \Bbbk[x_1, \cdots, x_n]$.

**Example 1.4.** Consider subsets of $\mathbb{A}^1$. The set $X_1 = \{5\}$ is an algebraic set because $X_1 = \mathbb{V}(x-5)$. One can also say $X_1 = \mathbb{V}((x-5)^2)$, or even $X_1 = \mathbb{V}(x(x-5), (x-1)(x-5))$. We see that different choices of $S$ in Definition 1.2 could possibly define the same algebraic set $X$. The set $X_2 = \{5, 7\}$ is an algebraic set because $X_2 = \mathbb{V}((x-5)(x-7))$. Many other subsets of $\mathbb{A}^1$ are also algebraic sets. You will find all of them in an exercise.

**Example 1.5.** Consider subsets of $\mathbb{A}^2$. Examples of algebraic sets are $\mathbb{V}(y - x^2)$ which is a parabola, and $\mathbb{V}(xy)$ which is the union of two coordinate axes. They are both hypersurfaces in $\mathbb{A}^2$. The algebraic set $\mathbb{V}(x-5, y-7)$ contains only one point. It is not a hypersurface because we cannot define it by one non-constant polynomial (but we do not prove this fact).

*Date*: January 17, 2016.

**Example 1.6.** Let $\Bbbk = \mathbb{Q}$ (it is not algebraically closed but I just want to mention this piece of history) and $n = 2$. For every $m \geqslant 3$, the set $X = \mathbb{V}(x^m + y^m - 1) \in \mathbb{A}^2_{\mathbb{Q}}$ is a historically important algebraic set. Obviously $X$ contains points $(1, 0)$ and $(0, 1)$ for all $m$, and $(-1, 0)$ and $(0, -1)$ for even $m$. The fact that these are the only points in $X$ is one of the deepest results in mathematics. An equivalent formulation of this result is the so-called Fermat's Last Theorem, which was conjectured in 1637, and proved in 1995.

Here are some simple and useful properties of algebraic sets.

**Proposition 1.7.** *We consider subsets in $\mathbb{A}^n$.*

(1) *Let $S_1$ and $S_2$ be two sets of polynomials in $\Bbbk[x_1, \cdots, x_n]$. If $S_1 \supseteq S_2$, then $\mathbb{V}(S_1) \subseteq \mathbb{V}(S_2)$. In other words, the correspondence $\mathbb{V}$ is inclusion-reversing.*

(2) *$\varnothing$ and $\mathbb{A}^n$ are both algebraic sets.*

(3) *The intersection of any collection of algebraic sets in $\mathbb{A}^n$ is an algebraic set.*

(4) *The union of finitely many algebraic sets in $\mathbb{A}^n$ is an algebraic set.*

*Proof.* We leave the proof as an exercise. □

We introduce some algebraic language that we need to use later.

**Definition 1.8.** Let $R$ be a ring (a commutative ring with 1).

(1) For any subset $S \subseteq R$, the ideal
$$I = \{r_1 f_1 + \cdots + r_k f_k \mid k \in \mathbb{Z}_+; r_1, \cdots, r_k \in R; f_1, \cdots, f_k \in S\}$$
is called the *ideal generated by $S$*. We say $S$ is a *set of generators of $I$*.

(2) An ideal $I$ is said to be *finitely generated* if it is generated by a finite set $S = \{f_1, \cdots, f_m\} \subseteq R$. We write $I = (f_1, \cdots, f_m)$.

(3) An ideal $I$ is *principal* if it is generated by one element $f \in R$. We write $I = (f)$.

Notice that the notation in Definition 1.8 is slightly different from, indeed, simpler than what we used in Algebra 2B (which was $I = Rf_1 + \cdots + Rf_m$ if $I$ is finitely generated, or $I = Rf$ if $I$ is principal). The notation here is more often used in algebraic geometry.

**Example 1.9.** Let $I \subseteq \mathbb{Z}$ be the ideal of all even integers. Then one can say $I = (2)$, or $I = (-2)$, or $I = (2, 4)$ (4 is obviously redundant), or $I = (4, 6)$ (do you see why?). We can even take $S$ to be everything in $I$, then the ideal generated by $S$ is still $I$. Upshot: there are usually many choices for the generators of a given ideal.

**Lemma 1.10.** *For any subset $S \subseteq \Bbbk[x_1, \cdots, x_n]$, let $I \subseteq \Bbbk[x_1, \cdots, x_n]$ be the ideal generated by $S$. Then $\mathbb{V}(S) = \mathbb{V}(I)$.*

*Proof.* We need to show mutual inclusions between $\mathbb{V}(S)$ and $\mathbb{V}(I)$. The inclusion in one direction $\mathbb{V}(S) \supseteq \mathbb{V}(I)$ follows from the fact that $S \subseteq I$ and Proposition 1.7 (1).

We prove $\mathbb{V}(S) \subseteq \mathbb{V}(I)$. For every point $p = (a_1, \cdots, a_n) \in \mathbb{V}(S)$, we need to show that $p \in \mathbb{V}(I)$. Since $I$ is generated by $S$, every element $g \in I$ can be written in the form $g = r_1 f_1 + \cdots + r_k f_k$ for some $k \in \mathbb{Z}_+$, $r_1, \cdots, r_k \in \Bbbk[x_1, \cdots, x_n]$ and $f_1, \cdots, f_k \in S$. By assumption $f_1(p) = \cdots = f_k(p) = 0$, which implies $g(p) = r_1(p) f_1(p) + \cdots + r_k(p) f_k(p) = 0$. Therefore $p \in \mathbb{V}(I)$. It follows that $\mathbb{V}(S) \subseteq \mathbb{V}(I)$. □

This lemma shows that every algebraic set $X \subseteq \mathbb{A}^n$ can be defined by an ideal $I \subseteq \Bbbk[x_1, \cdots, x_n]$. Notice that different ideals could still define the same algebraic set.

**Example 1.11.** Consider $X = \{0\} \subseteq \mathbb{A}^1$. Consider two principal ideals $I_1 = (x)$ and $I_2 = (x^2)$ in $\Bbbk[x]$. Then $X = \mathbb{V}(I_1) = \mathbb{V}(I_2)$.

Among the many ideals that define the same algebraic set, we will see next week which one is "the best". Stay tuned!

1.2. **Noetherian rings and Hilbert basis theorem.** We start with some algebra. But eventually we will see its geometric applications.

Recall that a ring $R$ is a principal ideal domain (or PID) if every ideal of $R$ is generated by one element. PIDs have many good properties. But unfortunately many interesting rings in algebraic geometry, for example, $\Bbbk[x_1, \cdots, x_n]$ when $n \geqslant 2$, are not PIDs. It will be helpful to generalise the notion of PID to include examples like these.

**Definition 1.12.** A ring $R$ is *Noetherian* if every ideal of $R$ is finitely generated.

It is immediately clear from the definition that every PID is Noetherian. We want to see more examples. A powerful tool to produce such examples is the following

**Theorem 1.13** (Hilbert Basis Theorem)**.** *If a ring $R$ is Noetherian, then $R[x]$ is also Noetherian.*

*Proof.* Non-examinable. Interested reader can find the proof in [Section 3.3, Reid, Undergraduate Algebraic Geometry] or [Section 1.4, Fulton, Algebraic Curves]. □

**Corollary 1.14.** *For any field $\Bbbk$ and $n \in \mathbb{Z}_+$, the ring $\Bbbk[x_1, \cdots, x_n]$ is Noetherian.*

*Proof.* We prove by induction on $n$. When $n = 1$, we know $\Bbbk[x_1]$ is a PID, hence is Noetherian. Assume $R_n = \Bbbk[x_1, \cdots, x_n]$ is a Noetherian ring. We need to show that $R_{n+1} = \Bbbk[x_1, \cdots, x_n, x_{n+1}]$ is also Noetherian. Notice that by collecting terms with respect to the variable $x_{n+1}$, every polynomial in $R_{n+1}$ can be written as a polynomial in $x_{n+1}$ with coefficients in $R_n$. In other words, we have $R_{n+1} = R_n[x_{n+1}]$. By Hilbert Basis Theorem 1.13 and the induction assumption, we conclude that $R_{n+1}$ is Noetherian. □

There is yet another powerful tool very useful for producing examples of Noetherian rings. Before stating it we need to give an equivalent description of a Noetherian ring.

**Proposition 1.15.** *A ring $R$ is Noetherian if and only if the following ascending chain condition (or ACC) holds: for every ascending chain of ideals in $R$*

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

*there exists a positive integer $N$ such that $I_n = I_N$ for all $n \geqslant N$.*

*Proof.* (This proof is non-examinable and not covered in lectures.)

We first prove that the Noetherian condition implies ACC. Take any ascending chain of ideals in $R$, say, $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Set $I = \cup_{n=1}^{\infty} I_n$. We claim that $I$ is an ideal in $R$. Indeed, for any $r \in R$ and $a, b \in I$, assume $a \in I_i$ and $b \in I_j$. Then $a, b \in I_{\max\{i,j\}}$. It follows that $a + b \in I_{\max\{i,j\}}$, hence $a + b \in I$. Moreover, $ra \in I_i$ hence $ra \in I$. This concludes that $I$ is an ideal.

Since $R$ is Noetherian, $I$ is finitely generated, say, $I = (f_1, \cdots, f_m)$. Then each $f_i$ is an element in $I_{n_i}$ for some $n_i$. Take $N = \max\{n_1, \cdots, n_m\}$. We claim that $I_N = I$. On one hand $f_i \in I_{n_i} \subseteq I_N$ for every $i$, hence $r_1 f_1 + \cdots + r_m f_m \in I_N$ for any $r_1, \cdots, r_m \in R$, which implies $I \subseteq I_N$. On the other hand we have $I_N \subseteq I$ by the construction of $I$. It follows that $I_N = I$. For every $n \geqslant N$, we have $I_N \subseteq I_n \subseteq I = I_N$, hence $I_n = I_N$.

We then prove that ACC implies the Noetherian condition. We use contradiction. Assume $R$ has an ideal $J$ which is not finitely generated. We pick an element $g_1 \in J$ and define $I_1 = (g_1)$. Since $J$ is not finitely generated we have $I_1 \subsetneq J$, hence we can pick an element $g_2 \in J \backslash I_1$ and define $I_2 = (g_1, g_2)$. Similarly we can pick $g_3 \in J \backslash I_2$ and define $I_3 = (g_1, g_2, g_3)$. Repeat this process indefinitely, we get a chain of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ where each $I_i = (g_1, \cdots, g_i)$. Every inclusion in the chain is strict, hence the chain never stabilises, which is a contradiction to ACC. □

Now we are ready to state our second tool for producing examples of Noetherian rings.

**Proposition 1.16.** *Let $R$ be a Noetherian ring and $I$ is an ideal in $R$. Then the quotient ring $R/I$ is also Noetherian.*

*Proof.* We leave the proof as an exercise. □

**Corollary 1.17.** *For any ideal $I$ in $\Bbbk[x_1, \cdots, x_n]$, $\Bbbk[x_1, \cdots, x_n]/I$ is a Noetherian ring.*

*Proof.* This is a consequence of Corollary 1.14 and Proposition 1.16. □

Why are we so interested in Noetherian rings? Can we understand more geometry from the fact that $\Bbbk[x_1, \cdots, x_n]$ is Noetherian? The following is the answer.

**Theorem 1.18.** *Let $X \subseteq \mathbb{A}^n$ be an algebraic set, such that $\varnothing \neq X \neq \mathbb{A}^n$. Then $X$ is the intersection of finitely many hypersurfaces.*

*Proof.* By Lemma 1.10, we can write $X = \mathbb{V}(I)$ for some ideal $I$ in $\Bbbk[x_1, \cdots, x_n]$. By Corollary 1.14, $I$ is finitely generated, say, $I = (f_1, \cdots, f_m)$. By Lemma 1.10 again we can write $X = \mathbb{V}(I) = \mathbb{V}(f_1, \cdots, f_m)$. Without loss of generality, we can assume every $f_i$ is non-constant. Indeed, if a certain $f_i$ is zero, then we can simply remove it from the set of generators; if a certain $f_i$ is a non-zero constant, then $X = \varnothing$ which is excluded by the assumption. Notice that

$$\begin{aligned} X &= \mathbb{V}(f_1, \cdots, f_m) \\ &= \{p \in \mathbb{A}^n \mid f_1(p) = \cdots = f_m(p) = 0\} \\ &= \{p \in \mathbb{A}^n \mid f_1(p) = 0\} \cap \cdots \cap \{p \in \mathbb{A}^n \mid f_m(p) = 0\} \\ &= \mathbb{V}(f_1) \cap \cdots \cap \mathbb{V}(f_m). \end{aligned}$$

Since each $\mathbb{V}(f_i)$ is a hypersurface in $\mathbb{A}^n$, we conclude that $X$ is the intersection of finitely many hypersurfaces. □

Equivalently, we can say that every algebraic set in $\mathbb{A}^n$ can be defined by finitely many polynomials (this even includes the algebraic sets $\varnothing$ and $\mathbb{A}^n$, as they are defined by $\{1\}$ and $\{0\}$ respectively). Notice that a geometric result like Theorem 1.18 cannot be obtained without the algebraic theory of Noetherian rings. In fact, thoroughout this course, we will always strive to build up a bridge, or a dictionary, between geometry and algebra. How to translate a geometric question into algebra, and how to interpret an algebraic result in the geometric language, will always be our main themes in this course.

## Exercise Sheet 1

*This sheet will be discussed in the exercise class on 9 October. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 1.1.** *Examples of algebraic sets.* For each of the following $X \subseteq \mathbb{A}^2$, find a set of polynomials $S \subseteq \Bbbk[x, y]$ such that $X = \mathbb{V}(S)$. You don't need to justify your answer.

(1) $X = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

(2) $X = \{(0, 0), (1, 1)\}$.

(3) $X$ is the union of the $x$-axis and a single point $(0, 1)$.

(4) For fun: describe the algebraic set $\mathbb{V}(xy, yz, zx) \subseteq \mathbb{A}^3$ geometrically.

**Exercise 1.2.** *Prove Proposition 1.7.* Consider algebraic sets in $\mathbb{A}^n$.

(1) Suppose $S_1 \supseteq S_2$. Prove that $\mathbb{V}(S_1) \subseteq \mathbb{V}(S_2)$.

(2) Prove that $\varnothing$ and $\mathbb{A}^n$ are algebraic sets in $\mathbb{A}^n$.

(3) Prove that $\cap_\alpha(\mathbb{V}(S_\alpha)) = \mathbb{V}(\cup_\alpha S_\alpha)$.

(4) Suppose $S = \{fg \mid f \in S_1, g \in S_2\}$. Prove that $\mathbb{V}(S_1) \cup \mathbb{V}(S_2) = \mathbb{V}(S)$. Use induction to conclude that the union of finitely many algebraic sets is still algebraic.

**Exercise 1.3.** *Examples of algebraic sets.* Prove that algebraic sets in $\mathbb{A}^1$ are just the finite subsets in $\mathbb{A}^1$ (including $\varnothing$) together with $\mathbb{A}^1$ itself. You can follow these steps:

(1) Verify that they are indeed algebraic sets.

(2) Prove that if an algebraic set in $\mathbb{A}^1$ is not $\mathbb{A}^1$ itself, then it contains at most finitely many points. (*Hint:* you can use the following lemma in algebra: a non-zero polynomial $f(x) \in \Bbbk[x]$ of degree $d$ has at most $d$ roots.)

(3) As an application of this exercise, give an example of infinitely many algebraic sets, whose union is not an algebraic set.

**Exercise 1.4.** *Prove Proposition 1.16.* Prove that if $R$ is a Noetherian ring, then $R/I$ is also Noetherian for any ideal $I$ in $R$. You can follow these steps:

(1) We write the quotient ring homomorphism $q : R \to R/I$ (sending each $r \in R$ to the coset $r + I$). For any ideal $J$ in $R/I$, prove that $q^{-1}(J)$ is an ideal in $R$.

(2) For two ideals $J_1 \subseteq J_2$ in $R/I$, prove that $q^{-1}(J_1) \subseteq q^{-1}(J_2)$.

(3) Suppose $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ is an ascending chain of ideals in $R/I$. Use (1), (2) and the fact that $R$ is Noetherian to show that this chain stabilises.

(4) Use Proposition 1.15 to conclude that $R/I$ is Noetherian.

## Solutions to Exercise Sheet 1

**Solution 1.1.** *Examples of algebraic sets.* There are many possible answers.

(1) One possible answer is $X = \mathbb{V}(x(x-1), y(y-1))$.

(2) One possible answer is $X = \mathbb{V}(x(y-1), y(x-1))$.

(3) One possible answer is $X = \mathbb{V}(xy, y(y-1))$.

(4) This algebraic set is the union of the three coordinate axes. In other words, it is the set of points $(x, y, z) \in \mathbb{A}^3$ with at least two zero coordinates.

**Solution 1.2.** *Prove Proposition 1.7.*

(1) Given any $p \in \mathbb{V}(S_1)$, we have $f(p) = 0$ for every $f \in S_1$. Since every $g \in S_2$ is also an element in $S_1$, we have $g(p) = 0$. Hence $p \in \mathbb{V}(S_2)$.

(2) We have that $\varnothing = \mathbb{V}(1)$ and $\mathbb{A}^n = \mathbb{V}(0)$.

(3) We first prove $\cap_\alpha(\mathbb{V}(S_\alpha)) \subseteq \mathbb{V}(\cup_\alpha S_\alpha)$. Given any point $p \in \cap_\alpha(\mathbb{V}(S_\alpha))$, we have $p \in \mathbb{V}(S_\alpha)$ for every $\alpha$. Then for every $f \in \cup_\alpha S_\alpha$, there exists some $\alpha_0$ such that $f \in S_{\alpha_0}$, therefore $f(p) = 0$ since $p \in \mathbb{V}(S_{\alpha_0})$. This shows that $p \in \mathbb{V}(\cup_\alpha S_\alpha)$.

We then prove $\cap_\alpha(\mathbb{V}(S_\alpha)) \supseteq \mathbb{V}(\cup_\alpha S_\alpha)$. Given any point $q \in \mathbb{V}(\cup_\alpha S_\alpha)$, we have $g(p) = 0$ for every $g \in \cup_\alpha S_\alpha$. In particular, for every $\alpha$, we have $p \in \mathbb{V}(S_\alpha)$. Therefore $p \in \cap_\alpha(\mathbb{V}(S_\alpha))$.

(4) We first prove $\big(\mathbb{V}(S_1) \cup \mathbb{V}(S_2)\big) \subseteq \mathbb{V}(S)$. Given any $p \in \mathbb{V}(S_1)$, we have $f(p) = 0$ for every $f \in S_1$. Therefore for every $fg \in S$ with $f \in S_1$ and $g \in S_2$, $(fg)(p) = f(p)g(p) = 0$. Hence $p \in \mathbb{V}(S)$. This proves $\mathbb{V}(S_1) \subseteq \mathbb{V}(S)$. Similarly we have $\mathbb{V}(S_2) \subseteq \mathbb{V}(S)$. Therefore $\big(\mathbb{V}(S_1) \cup \mathbb{V}(S_2)\big) \subseteq \mathbb{V}(S)$.

We then prove $\big(\mathbb{V}(S_1) \cup \mathbb{V}(S_2)\big) \supseteq \mathbb{V}(S)$. For every $p \in \mathbb{V}(S)$, we need to show that $p \in \mathbb{V}(S_1) \cup \mathbb{V}(S_2)$. If not, then $p \notin \mathbb{V}(S_1)$ and $p \notin \mathbb{V}(S_2)$. This means there exists some $f_0 \in S_1$

and $g_0 \in S_2$, such that $f_0(p) \neq 0$ and $g_0(p) \neq 0$. It follows that $(f_0 g_0)(p) = f_0(p) g_0(p) \neq 0$. Since $f_0 g_0 \in S$, this implies $p \notin \mathbb{V}(S)$. Contradiction. This proves $\big(\mathbb{V}(S_1) \cup \mathbb{V}(S_2)\big) \supseteq \mathbb{V}(S)$.

We then use induction to prove that $\mathbb{V}(S_1) \cup \mathbb{V}(S_2) \cup \cdots \cup \mathbb{V}(S_n)$ is an algebraic set for every positive integer $n$. When $n = 1$, $\mathbb{V}(S_1)$ is by definition an algebraic set. Assume the statement holds for $n = k$, then $\mathbb{V}(S_1) \cup \mathbb{V}(S_2) \cup \cdots \cup \mathbb{V}(S_k)$ is an algebraic set, say, $\mathbb{V}(S')$. When $n = k + 1$, we can write

$$\begin{aligned} &\mathbb{V}(S_1) \cup \mathbb{V}(S_2) \cup \cdots \cup \mathbb{V}(S_k) \cup \mathbb{V}(S_{k+1}) \\ =& \big(\mathbb{V}(S_1) \cup \mathbb{V}(S_2) \cup \cdots \cup \mathbb{V}(S_k)\big) \cup \mathbb{V}(S_{k+1}) \\ =& \mathbb{V}(S') \cup \mathbb{V}(S_{k+1}) \end{aligned}$$

which is still an algebraic set by the statement we just proved.

**Solution 1.3.** *Examples of algebraic sets.*

(1) We know that $\mathbb{A}^1$ and $\varnothing$ are algebraic sets by Proposition 1.7 (2). For any non-empty finite subset of $\mathbb{A}^1$, say, $X = \{c_1, c_2, \cdots, c_k\}$, we have $X = \mathbb{V}((x - c_1)(x - c_2) \cdots (x - c_k))$, hence is an algebraic set.

(2) Say $X = \mathbb{V}(S)$ is an algebraic set in $\mathbb{A}^1$. If $S$ does not contain any non-zero polynomial, then $X = \mathbb{A}^1$. Otherwise, there is some $f(x) \in S$ which is a non-zero polynomial. Every point in $X$ must be a root of $f(x)$, hence $X$ is a subset of the all roots of $f(x)$. Since $f(x)$ has only finitely many roots, $X$ has at most finitely many elements.

(3) There are many possible counterexamples and here is one of them: for every positive integer $n$, let $X_n = \{n\}$ be a single-point set. Then $X_n$ is an algebraic set. But their union $\cup_n X_n$ is the set of all positive integers, which is an infinite set, hence is not an algebraic set by part (2).

**Solution 1.4.** *Prove Proposition 1.16.*

(1) We check that $q^{-1}(J) = \{r \in R \mid r + I \in J\}$ is an ideal in $R$. For any $a_1, a_2 \in q^{-1}(J)$, we have $a_1 + I, a_2 + I \in J$ hence $(a_1 + a_2) + I = (a_1 + I) + (a_2 + I) \in J$, which implies $a_1 + a_2 \in q^{-1}(J)$. On the other hand, for any $r \in R$ and $a \in q^{-1}(J)$, we have $a + I \in J$ hence $ra + I = (r + I)(a + I) \in J$ hence $ra \in q^{-1}(J)$. Therefore $q^{-1}(J)$ is an ideal in $R$.

(2) For every $a \in q^{-1}(J_1)$, we have $a + I \in J_1$. Since $J_1 \subseteq J_2$, we have $a + I \in J_2$. Hence $a \in q^{-1}(J_2)$. This verifies that $q^{-1}(J_1) \subseteq q^{-1}(J_2)$.

(3) Suppose $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ is an ascending chain of ideals in $R/I$. Then by parts (1) and (2) we have $q^{-1}(J_1) \subseteq q^{-1}(J_2) \subseteq q^{-1}(J_3) \subseteq \cdots$ is an ascending chain of ideals in $R$. Since $R$ is a Noetherian ring, this chain stablises by Proposition 1.15. That means, there exists some positive integer $N$, such that $q^{-1}(J_i) = q^{-1}(J_N)$ for every $i \geqslant N$. In other words, $q^{-1}(J_i)$ and $q^{-1}(J_N)$ contain precisely the same cosets of $I$ in $R$. Therefore $J_i = J_N$ for every $i \geqslant N$.

(4) We showed in part (3) that every ascending chain of ideals in $R/I$ stabilises. Therefore $R/I$ is a Noetherian ring by Proposition 1.15.

## 2. Nullstellensatz

We will introduct radical ideals, and use Nullstellensatz to establish the $\mathbb{V} - \mathbb{I}$ correspondence between radical ideals and algebraic sets. We will also see the geometric meaning of prime ideals and maximal ideals.

### 2.1. Nullstellensatz and $\mathbb{V} - \mathbb{I}$ correspondence.

Recall the $\mathbb{V}$ map in Definition 1.2. By Lemma 1.10, it defines a surjective map

$$\mathbb{V} : \{\text{ideals in } \Bbbk[x_1, \cdots, x_n]\} \longrightarrow \{\text{algebraic sets in } \mathbb{A}^n\}. \tag{2.1}$$

However the map is not injective as different ideals could possibly define the same algebraic set. Among all ideals that define the same algebraic set, we want to choose a "good" one, so that we can establish a one-to-one correspondence between "good" ideals in $\Bbbk[x_1, \cdots, x_n]$ and algebraic sets in $\mathbb{A}^n$. We start with some algebra.

**Definition 2.1.** Let $I$ be an ideal in a ring $R$. The *radical of $I$* is

$$\sqrt{I} = \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{Z}_+\}.$$

An ideal $I$ is said to be a *radical ideal* if $I = \sqrt{I}$.

**Lemma 2.2.** *Let $I$ be an ideal in a ring $R$. Then $\sqrt{I}$ is an ideal in $R$ containing $I$.*

*Proof.* We leave it as an exercise. □

This definition does not look very intuitive at a first glance. But it will be clear why we define it this way after we relate it to some geometry. We give a quick example.

**Example 2.3.** Consider the ideals $I_1 = (x)$ and $I_2 = (x^2)$ in $\Bbbk[x]$. It is not difficult to find out that $\sqrt{I_1} = \sqrt{I_2} = (x)$. Therefore $I_1$ is a radical ideal in $\Bbbk[x]$ while $I_2$ is not. We leave the details in an exercise.

**Definition 2.4.** For any subset $X \subseteq \mathbb{A}^n$,

$$\mathbb{I}(X) := \{f \in \Bbbk[x_1, \cdots, x_n] \mid f(p) = 0 \text{ for all } p \in X\}$$

is called the *ideal of $X$*.

In other words, $\mathbb{I}(X)$ consists of all polynomials that vanish on $X$. Notice that this definition makes sense for any subset $X \subseteq \mathbb{A}^n$ which is not necessarily algebraic.

**Example 2.5.** For the subset $X = \{0\} \subseteq \mathbb{A}^1$, $\mathbb{I}(X)$ is the set of all $f(x) \in \Bbbk[x]$ such that $f(0) = 0$. Therefore $\mathbb{I}(X) = (x) \subseteq \Bbbk[x]$.

**Lemma 2.6.** *The map $\mathbb{I}$ has the following properties:*

(1) *Let $X_1$ and $X_2$ be two subsets of $\mathbb{A}^n$. If $X_1 \supseteq X_2$, then $\mathbb{I}(X_1) \subseteq \mathbb{I}(X_2)$.*

(2) *For any subset $X \subseteq \mathbb{A}^n$, $\mathbb{I}(X)$ is a radical ideal in $\Bbbk[x_1, \cdots, x_n]$.*

*Proof.* (1) For any $f \in \mathbb{I}(X_1)$, we have that $f(p) = 0$ for every $p \in X_1$. In particular, since $X_1 \supseteq X_2$, $f(p) = 0$ for every $p \in X_2$. Hence $f \in \mathbb{I}(X_2)$. It follows that $\mathbb{I}(X_1) \subseteq \mathbb{I}(X_2)$.

(2) We first show $\mathbb{I}(X)$ is an ideal. For any $f, g \in \mathbb{I}(X)$ and $r \in \Bbbk[x_1, \cdots, x_n]$, we have $(f+g)(p) = f(p) + g(p) = 0$ and $(rf)(p) = r(p)f(p) = 0$ for all $p \in X$. Therefore $f + g, rf \in \mathbb{I}(X)$, hence $\mathbb{I}(X)$ is an ideal. Then we need to show that $\sqrt{\mathbb{I}(X)} = \mathbb{I}(X)$. We have that

$$\begin{aligned} f \in \sqrt{\mathbb{I}(X)} \quad &\iff \quad \exists\, m \in \mathbb{Z}_+ \text{ such that } f^m \in \mathbb{I}(X) \\ &\iff \quad \exists\, m \in \mathbb{Z}_+ \text{ such that } f(p)^m = 0 \text{ for any } p \in X \\ &\iff \quad f(p) = 0 \text{ for any } p \in X \\ &\iff \quad f \in \mathbb{I}(X). \end{aligned}$$

It follows that $\sqrt{\mathbb{I}(X)} = \mathbb{I}(X)$, hence the ideal $\mathbb{I}(X)$ is radical. □

We return to the question at the beginning of the section. The $\mathbb{V}$-map (2.1) hits all algebraic sets in $\mathbb{A}^n$, but each algebraic set can be hit by many different ideals. However, the $\mathbb{I}$-map in Definition 2.4 assigns to each algebraic set in $\mathbb{A}^n$ a radical ideal in $\Bbbk[x_1, \cdots, x_n]$. Therefore if we only consider the radical ideals, there is hope that the two maps

$$\{\text{radical ideals } I \subseteq \Bbbk[x_1, \cdots, x_n]\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \{\text{algebraic sets } X \subseteq \mathbb{A}^n\} \tag{2.2}$$

are inverse to each other, hence establish a one-to-one correspondence between radical ideals in $\Bbbk[x_1, \cdots, x_n]$ and algebraic sets in $\mathbb{A}^n$. This holds as long as $\Bbbk$ is algebraically closed. The proof relies on the so-called Nullstellensatz, which is a difficult theorem.

**Definition 2.7.** An ideal $I$ in a ring $R$ is *proper* if $I \neq R$.

**Theorem 2.8** (Hilbert's Nullstellensatz)**.** *For any algebraically closed field $\Bbbk$,*

(1) *Let $I$ be any proper ideal in $\Bbbk[x_1, \cdots, x_n]$. Then $\mathbb{V}(I) \neq \varnothing$.*
(2) *Let $I$ be any ideal in $\Bbbk[x_1, \cdots, x_n]$. Then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.*

*Proof.* Non-examinable. Interested reader can find the proof in [Section 3.10, Reid, Undergraduate Algebraic Geometry] or [Section 1.7, Fulton, Algebraic Curves]. □

**Proposition 2.9.** *For any algebraically closed field $\Bbbk$,*

(1) *Assume $I$ is a radical ideal in $\Bbbk[x_1, \cdots, x_n]$ and $X$ is an algebraic set in $\mathbb{A}^n$. Then $X = \mathbb{V}(I)$ if and only if $I = \mathbb{I}(X)$.*
(2) *Assume $I_1$ are $I_2$ radical ideals in $\Bbbk[x_1, \cdots, x_n]$, $X_1 = \mathbb{V}(I_1)$ and $X_2 = \mathbb{V}(I_2)$. Then $I_1 \subseteq I_2$ (resp. $I_1 \subsetneq I_2$) if and only if $X_1 \supseteq X_2$ (resp. $X_1 \supsetneq X_2$).*

*Proof.* (1) We prove "$\Longrightarrow$". By Nullstellensatz 2.8 we have $\mathbb{I}(X) = \mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$ since $I$ is a radical ideal.

We prove "$\Longleftarrow$". The algebraic set $X$ can be written as $X = \mathbb{V}(J)$ for some ideal $J \subseteq \Bbbk[x_1, \cdots, x_n]$. By Nullstellensatz 2.8, $\mathbb{V}(I) = \mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(\mathbb{I}(\mathbb{V}(J))) = \mathbb{V}(\sqrt{J})$. Since $\sqrt{J} \supseteq J$ by Lemma 2.2, we have $\mathbb{V}(I) = \mathbb{V}(\sqrt{J}) \subseteq \mathbb{V}(J) = X$ by Proposition 1.7 (1). It remains to show that $X \subseteq \mathbb{V}(I)$. For every point $p \in X$, by the definition of $\mathbb{V}$, we need to show that $f(p) = 0$ for every $f \in I$. This is clear since $I = \mathbb{I}(X)$.

(2) The equivalence "$I_1 \subseteq I_2 \Longleftrightarrow X_1 \supseteq X_2$" follows from Proposition 1.7 (1) and Lemma 2.6 (1). By (1), we see that if one of the inclusions is an equality, then so is the other. Therefore if one of them is a strict inclusion, then so is the other. □

In other words, Proposition 2.9 shows that $\mathbb{V}$ and $\mathbb{I}$ induce mutually inverse bijections between radical ideals in $\Bbbk[x_1, \cdots, x_n]$ and algebraic sets in $\mathbb{A}^n$. Moreover, the bijection is inclusion-reversing. Next time we will see how this correspondence relates algebra and geometry.

2.2. **Prime ideals and maximal ideals.** We have established a one-to-one corrspondence (2.2) between radical ideals in $\Bbbk[x_1, \cdots, x_n]$ and algebraic sets in $\mathbb{A}^n$. A major benefit: we can read off some geometric properties of algebraic sets from algebraic properties of the corresponding radical ideals. We will see two such examples in this lecture.

**Definition 2.10.** Let $I$ be an ideal in a ring $R$.

(1) The ideal $I$ is *prime* if it is proper, and $fg \in I$ implies $f \in I$ or $g \in I$.
(2) The ideal $I$ is *maximal* if it is proper, and for any ideal $J$ satisfying $I \subseteq J \subseteq R$, we have either $J = I$ or $J = R$.

**Example 2.11.** We look at some ideals in $\Bbbk[x]$.

(1) Consider $I_1 = (x^2 - x)$. $I_1$ is not prime because $x(x-1) \in I_1$, while $x \notin I_1$ and $x - 1 \notin I_1$. $I_1$ is not maximal because $(x^2 - x) \subsetneq (x) \subsetneq \Bbbk[x]$.
(2) Consider $I_2 = (x)$. We claim $(x)$ is prime. Assume $fg \in (x)$, then $fg = xh$ for some $h \in \Bbbk[x]$. By unique factorisation, since $x$ is irreducible, it must be a factor of $f$ or $g$. Hence $f \in (x)$ or $g \in (x)$. We claim $(x)$ is maximal. Assume $(x) \subseteq I \subseteq \Bbbk[x]$. If $I \neq (x)$, then there exists

$f \in I \backslash (x)$. Write $f = a_0 + a_1 x + \cdots + a_n x^n$, then $a_0 \neq 0$, since otherwise $f \in (x)$. We observe $f - a_0 = a_1 x + \cdots + a_n x^n \in (x) \subseteq I$. It follows that $a_0 \in I$, hence $I = \Bbbk[x]$ since $a_0$ is a unit in $\Bbbk[x]$.

(3) Consider $I_3 = (0)$. $I_3$ is prime because $fg = 0$ implies that either $f = 0$ or $g = 0$ as $\Bbbk[x]$ is an integral domain. $I_3$ is not maximal because $(0) \subsetneq (x) \subsetneq \Bbbk[x, y]$.

**Proposition 2.12.** *Let $I$ be an ideal in the ring $R$.*

(1) *$I$ is a prime ideal if and only if $R/I$ is an integral domain. $I$ is a maximal ideal if and only if $R/I$ is a field.*

(2) *Every maximal ideal is prime. Every prime ideal is radical.*

*Proof.* (1) is non-examinable. (2) is an exercise. □

Under the corrspondence (2.2), we will find out what prime and maximal ideals correspond to. Now we switch to geometry.

**Definition 2.13.** An algebraic set $X \subseteq \mathbb{A}^n$ is *irreducible* if there does not exist a decomposition of $X$ as a union of two stricly smaller algebraic sets. An irreducible (affine) algebraic set is also called an *affine variety*. An algebraic set $X \subseteq \mathbb{A}^n$ is *reducible* if it is not irreducible.

**Example 2.14.** We look at some algebraic sets in $\mathbb{A}^2$.

(1) The algebraic set $\mathbb{V}(xy) \subseteq \mathbb{A}^2$ is the union of two coordinate axes. In other words, $\mathbb{V}(xy) = \mathbb{V}(x) \cup \mathbb{V}(y)$. Since each coordinate axis is an algebraic set stricly smaller than $\mathbb{V}(xy)$, we conclude that $\mathbb{V}(xy)$ is reducible.

(2) The algebraic set $\mathbb{V}(x, y) \subseteq \mathbb{A}^2$ consists of just one point, hence there is no way to decompose it as the union of two strictly smaller algebraic sets. It follows that $\mathbb{V}(x, y)$ is irreducible. Similarly, a point is always irreducible.

Next we show that prime ideals correspond to irreducible algebraic sets.

**Proposition 2.15.** *Let $I$ be a radical ideal in $\Bbbk[x_1, \cdots, x_n]$ and $X = \mathbb{V}(I)$ the algebraic set in $\mathbb{A}^n$ defined by $I$. Then $I$ is prime if and only if $X$ is irreducible.*

*Proof.* In fact we prove the contrapositive: $X$ is reducible $\Longleftrightarrow$ $I$ is not prime.

We first prove "$\Longrightarrow$". Suppose $X = X_1 \cup X_2$ with algebraic sets $X_1, X_2 \subsetneq X$. Then $X_1 \subsetneq X$ implies that $\mathbb{I}(X_1) \supsetneq \mathbb{I}(X)$ by Proposition 2.9 (2). Hence there exists $f_1 \in \mathbb{I}(X_1) \backslash \mathbb{I}(X)$. Similarly $X_2 \subsetneq X$ implies that there exists $f_2 \in \mathbb{I}(X_2) \backslash \mathbb{I}(X)$. The product $f_1 f_2$ vanishes at all points of $X$, hence $f_1 f_2 \in \mathbb{I}(X)$. Therefore $I = \mathbb{I}(X)$ is not prime.

We then prove "$\Longleftarrow$". Since $I$ is not prime, there exist $f_1, f_2 \notin I$ such that $f_1 f_2 \in I$. Consider the set $S_1 = I \cup \{f_1\}$. Then $X_1 = \mathbb{V}(S_1)$ is an algebraic set. Since $S_1 \supseteq I$, we have $X_1 \subseteq X$ by Proposition 1.7. Moreover, since $f_1 \notin I$, there is some point $p \in X$ such that $f_1(p) \neq 0$, therefore $p \notin X_1$. It follows that $X_1 \subsetneq X$. Similarly we can consider $S_2 = I \cup \{f_2\}$, then $X_2 = \mathbb{V}(S_2) \subsetneq X$.

It remains to show that $X_1 \cup X_2 = X$. Since $X_1$ and $X_2$ are subsets of $X$, we have $X_1 \cup X_2 \subseteq X$. Conversely, for any $p \in X$, $f(p) = 0$ for every $f \in I$. Moreover $f_1(p) f_2(p) = 0$, which implies $f_1(p) = 0$ or $f_2(p) = 0$. Therefore $p \in \mathbb{V}(S_1) = X_1$ or $p \in \mathbb{V}(S_2) = X_2$. This implies $X \subseteq X_1 \cup X_2$. □

Finally we show that maximal ideals correspond to points.

**Proposition 2.16.** *Let $I$ be a radical ideal in $\Bbbk[x_1, \cdots, x_n]$ and $X = \mathbb{V}(I)$ the algebraic set in $\mathbb{A}^n$ defined by $I$. Then $I$ is maximal if and only if $X$ is a point.*

*Proof.* (This proof is non-examinable and not covered in lectures.)

In fact we prove the contrapositive: $X$ is not a point $\iff$ $I$ is not maximal.

We first prove "$\Longrightarrow$". If $X$ is not a point, then either $X = \varnothing$ or $X$ contains more than one point. If $X = \varnothing$, then by Proposition 2.9 (1), $I = \mathbb{I}(X) = \Bbbk[x_1, \cdots, x_n]$ is not a proper ideal hence not maximal. If $X$ contains more than one point, then we can pick a subset $Y$ of $X$ containing only one point. Hence we have $\varnothing \subsetneq Y \subsetneq X$. By Proposition 2.9 (2), we have $\Bbbk[x_1, \cdots, x_n] = \mathbb{I}(\varnothing) \supsetneq \mathbb{I}(Y) \supsetneq \mathbb{I}(X)$. Hence $I = \mathbb{I}(X)$ is not maximal.

We then prove "$\Longleftarrow$". If $I$ is not maximal, then either $I$ is not a proper ideal, or there exists an ideal $J$ such that $I \subsetneq J \subsetneq \Bbbk[x_1, \cdots, x_n]$. If $I$ is not proper then $I = \Bbbk[x_1, \cdots, x_n]$, hence $X = \mathbb{V}(I) = \varnothing$ which is not a point. If $I \subsetneq J \subsetneq \Bbbk[x_1, \cdots, x_n]$ for some ideal $J$, then we claim that we actually have $I \subsetneq \sqrt{J} \subsetneq \Bbbk[x_1, \cdots, x_n]$. Indeed, by Lemma 2.2, we have $I \subsetneq J \subseteq \sqrt{J}$. Moreover, by Nullstellensatz 2.8 (1), we have $\mathbb{V}(J) \neq \varnothing$, hence $\sqrt{J} = \mathbb{I}(\mathbb{V}(J)) \subsetneq \Bbbk[x_1, \cdots, x_n]$. Armed with this claim we apply Proposition 2.9 (2) to get $\mathbb{V}(I) \supsetneq \mathbb{V}(\sqrt{J}) \supsetneq \varnothing$. It follows that $\mathbb{V}(\sqrt{J})$ contains at least one point, hence $X = \mathbb{V}(I)$ contains more than one point. $\square$

In summary, the $\mathbb{V} - \mathbb{I}$ correspondences induce bijections in each row of the diagram:

$$\begin{tikzcd}
\{\text{radical ideals in } \Bbbk[x_1, \cdots, x_n]\} \arrow[r, shift left, "\mathbb{V}"] & \{\text{algebraic sets in } \mathbb{A}^n\} \arrow[l, shift left, "\mathbb{I}"] \\
\{\text{prime ideals in } \Bbbk[x_1, \cdots, x_n]\} \arrow[u, hook] \arrow[r, shift left, "\mathbb{V}"] & \{\text{irreducible algebraic sets in } \mathbb{A}^n\} \arrow[u, hook] \arrow[l, shift left, "\mathbb{I}"] \\
\{\text{maximal ideals in } \Bbbk[x_1, \cdots, x_n]\} \arrow[u, hook] \arrow[r, shift left, "\mathbb{V}"] & \{\text{points in } \mathbb{A}^n\} \arrow[u, hook] \arrow[l, shift left, "\mathbb{I}"]
\end{tikzcd}$$

## Exercise Sheet 2

*This sheet will be discussed in the exercise class on 16 October. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 2.1.** *Some proofs in lectures.* We prove Lemma 2.2 and Proposition 2.12 (2).

(1) Let $I$ be an ideal in a ring $R$. If $a^m \in I$ and $b^n \in I$ for some $a, b \in R$ and $m, n \in \mathbb{Z}_+$, show that $(a+b)^{m+n} \in I$. (*Hint:* use the binomial expansion.)

(2) Let $I$ be an ideal in a ring $R$. Prove that $\sqrt{I}$ is an ideal and $I \subseteq \sqrt{I}$.

(3) Show that every maximal ideal is prime, and every prime ideal is radical.

**Exercise 2.2.** *Examples of radical and prime ideals.* Suppose a non-zero polynomial $f \in \Bbbk[x_1, \cdots, x_n]$ is factored as $f = u f_1^{k_1} \cdots f_t^{k_t}$ for some $0 \neq u \in \Bbbk$, $k_1, \cdots, k_t \in \mathbb{Z}_+$, and irreducible polynomials $f_1, \cdots, f_t$ which are pairwisely coprime.

(1) Show that $(f)$ is a prime ideal if and only if $f$ is an irreducible polynomial.

(2) Let $\overline{f} = f_1 \cdots f_t$. Show that $\sqrt{(f)} = (\overline{f})$. (*Remark:* this justifies Example 2.3.)

(3) Conclude that $(f)$ is a radical ideal if and only if $f$ has no repeated factors.

**Exercise 2.3.** *Examples of maximal ideals.* Find all maximal ideals in $\Bbbk[x_1, \cdots, x_n]$. You can follow these steps:

(1) For any fixed point $p = (a_1, \cdots, a_n) \in \mathbb{A}^n$, consider the ring homomorphism $\varphi_p : \Bbbk[x_1, \cdots, x_n] \to \Bbbk; f(x_1, \cdots, x_n) \mapsto f(a_1, \cdots, a_n)$. Show that $m_p := \ker(\varphi_p) = (x_1 - a_1, \cdots, x_n - a_n)$. Use Proposition 2.12 to show that $m_p$ is a maximal ideal.

(2) What is $\mathbb{V}(m_p)$? Use Proposition 2.16 to show that every maximal ideal in $\Bbbk[x_1, \cdots, x_n]$ is of the form $m_p$ for some $p \in \mathbb{A}^n$. (*Remark:* historically, this was proved before Nullstellensatz was established.)

**Exercise 2.4.** *A famous example: the twisted cubic.* Prove that the subset in $\mathbb{A}^3$ given by $X = \{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in \Bbbk\}$ is an affine variety. You can follow these steps:

(1) Show that $X$ is the algebraic set $\mathbb{V}(I)$ for the ideal $I = (y - x^2, z - x^3) \subseteq \Bbbk[x, y, z]$.

(2) Show that $\Bbbk[x, y, z]/I \cong \Bbbk[t]$.

(3) Use Proposition 2.12 to conclude that $I$ is a prime ideal, hence a radical ideal. Use Proposition 2.9 to conclude that $I = \mathbb{I}(X)$. Use Proposition 2.15 to conclude that $X$ is an affine variety. (*Remark:* $X$ is called the affine *twisted cubic*.)

(*Remark:* Exercise 3.4 will be a continuation of this one.)

## Solutions to Exercise Sheet 2

**Solution 2.1.** *Some proofs in lectures.*

(1) Using the binomial expansion, we have that $(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^{m+n-i} b^i$. For every term $\binom{m+n}{i} a^{m+n-i} b^i$, if $i \leqslant n$, then this term has a factor $a^m$, hence this term is in $I$; if $i \geqslant n$, then this term has a factor $b^n$, hence this term is also in $I$. Since every such term is in $I$, it follows that their sum $(a+b)^{m+n} \in I$.

(2) Let $a, b \in \sqrt{I}$ and $r \in R$. By Definition 2.1 there exist some $m, n \in \mathbb{Z}_+$ such that $a^m, b^n \in I$. By part (1) we know that $(a+b)^{m+n} \in I$, hence $a + b \in \sqrt{I}$. We also have $(ra)^m = r^m a^m \in I$, hence $ra \in \sqrt{I}$. It follows that $\sqrt{I}$ is an ideal. To show that $I \subseteq \sqrt{I}$, we just need to realise that for every $a \in I$, $a^m \in I$ for $m = 1$. Hence $a \in \sqrt{I}$.

(3) Assume $I$ is a maximal ideal in $R$, then $R/I$ is a field by Proposition 2.12 (1). Since every field is an integral domain, $R/I$ is an integral domain. By Proposition 2.12 (1) again we conclude that $I$ is a prime ideal in $I$.

Assume $J$ is a prime ideal. For any $a \in \sqrt{J}$, there exists some $n \in \mathbb{Z}_+$, such that $a^n \in J$. We claim that $a \in J$. This can be shown by induction on $n$. When $n = 1$, $a \in J$ is automatic. Assume $a^n \in J$ implies $a \in J$. If we have $a^{n+1} = a \cdot a^n \in J$, then either $a \in J$ or $a^n \in J$. In either case we have $a \in J$. This shows that $\sqrt{J} \subseteq J$. By part (2) we also have $J \subseteq \sqrt{J}$. It follows that $J = \sqrt{J}$, hence $J$ is a radical ideal.

**Solution 2.2.** *Examples of radical and prime ideals.*

(1) Assume $(f)$ is a prime ideal. Since $(f) \neq \Bbbk[x_1, \cdots, x_n]$, $f$ is not a constant polynomial. If $f$ is not an irreducible polynomial, then assume $f = f_1 f_2$ for some non-constant polynomials $f_1$ and $f_2$. Since $f_1 f_2 = f \in (f)$, it follows that either $f_1 \in (f)$ or $f_2 \in (f)$. If $f_1 \in (f)$, then $f_1 = f \cdot g_1$ for some non-zero polynomial $g_1$. Then $f = f_1 f_2 = f g_1 f_2$ which implies $g_1 f_2 = 1$. Hence $f_2$ must be a constant, which is a contradiction. If $f_2 \in (f)$, the same argument implies $f_1$ is a constant, which is also a contradiction. This proves that $f$ is irreducible.

Now assume $f$ is an irreducible polynomial. We need to show $(f)$ is a prime ideal. By definition an irreducible polynomial is not a constant, hence $1 \notin (f)$ which means $(f) \neq \Bbbk[x_1, \cdots, x_n]$. Let $f_1 f_2 \in (f)$ for polynomials $f_1$ and $f_2$. Then we can write $f_1 f_2 = fg$ for some polynomial $g$. If $g = 0$, then either $f_1 = 0 \in (f)$ or $f_2 = 0 \in (f)$. If $g \neq 0$, then $f$ is an irreducible factor in the factorisation of $f_1 f_2$, hence $f$ is an irreducible factor of either $f_1$ or $f_2$. Therefore we still have $f_1 \in (f)$ or $f_2 \in (f)$. This proves that $(f)$ is a prime ideal.

(2) We first show that $(\overline{f}) \subseteq \sqrt{(f)}$. For any $g \in (\overline{f})$, there exists some polynomial $h$ such that $g = \overline{f} h = f_1 \cdots f_t h$. Let $m = \max\{k_1, \cdots, k_t\}$. Then $g^m = f_1^m \cdots f_t^m h^m = f \cdot f_1^{m-k_1} \cdots f_t^{m-k_t} h^m \in (f)$, hence $g \in \sqrt{(f)}$.

We prove the other inclusion $\sqrt{(f)} \subseteq (\overline{f})$. For any $g \in \sqrt{(f)}$, there exists some $m \in \mathbb{Z}_+$ such that $g^m \in (f)$, that is, $g^m = fh = f_1^{k_1} \cdots f_t^{k_t} h$ for some polynomial $h$. For every irreducible polynomial $f_i$, since $f_i$ divides the right-hand side, it must divide the left-hand side as well, i.e., $f_i$ divides $g^m$. Therefore $f_i$ divides $g$ for every $i$. It follows that each $f_i$ appears in the factorisation of $g$, hence $g = f_1 \cdots f_k g' = \overline{f} g' \in (\overline{f})$.

(3) $(f)$ is a radical ideal $\iff \sqrt{(f)} = (f) \iff (\overline{f}) = (f) \iff \overline{f}$ and $f$ differ by a unit in $\Bbbk[x_1, \cdots, x_n]$ (which is a non-zero constant). This holds if and only if $k_1 = \cdots = k_t = 1$; i.e. $f$ has no repeated factors.

**Solution 2.3.** *Examples of maximal ideals.*

(1) We claim that every polynomial $f(x_1, \cdots, x_n) \in \Bbbk[x_1, \cdots, x_n]$ can be written in the form

$$f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + c$$

for some polynomials $g_1, \cdots, g_n \in \Bbbk[x_1, \cdots, x_n]$ and a constant $c \in \Bbbk$. There are two ways to explain it (*you can choose the one you like*). The first approach: we think of $f$ as a polynomial in $x_1$ and consider the Euclidean division of $f$ by $x_1 - a_1$. We get $f = (x_1 - a_1)g_1 + r_1$ where $r_1$ has degree 0 in $x_1$, namely, $r_1 \in \Bbbk[x_2, \cdots, x_n]$. Then we think of $r_1$ as a polynomial in $x_2$, and consider the Euclidean division of $r_1$ by $x_2 - a_2$, we get $r_1 = (x_2 - a_2)g_2 + r_2$ for some $r_2 \in \Bbbk[x_3, \cdots, x_n]$. Repeat this process to get

$$\begin{aligned} f &= (x_1 - a_1)g_1 + r_1 \\ &= (x_1 - a_1)g_1 + (x_2 - a_2)g_2 + r_2 \\ &= \cdots \\ &= (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + r_n \end{aligned}$$

where $r_n$ is a constant. This justifies the claim. The second approach: we substitute $[(x_i - a_i) + a_i]$ into each occurence of $x_i$ in $f$ and expand the square brackets leaving the round brackets untouched. In the expansion every non-constant term has a factor of the form $(x_i - a_i)$. Then we can collect terms and write

$$f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + c$$

where $c$ is a constant. This justifies the claim.

Now we look at the image of $f$ under $\varphi_p$. We have $\varphi_p(f) = f(a_1, \cdots, a_n) = c$. Therefore $f \in \ker \varphi_p \iff c = 0 \iff f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n \iff f \in (x_1 - a_1, \cdots, x_n - a_n)$. This proves that $m_p = \ker \varphi_p = (x_1 - a_1, \cdots, x_n - a_n)$.

Moreover, $\varphi_p$ is surjective, because every $c \in \Bbbk$ is the image of the constant polynomial $f = c$. By the fundamental isomorphism theorem, we have

$$\Bbbk = \operatorname{im} \varphi_p = \Bbbk[x_1, \cdots, x_n]/\ker \varphi_p = \Bbbk[x_1, \cdots, x_n]/m_p.$$

Since $\Bbbk$ is a field, we know that $m_p$ is a maximal ideal by Proposition 2.12 (1).

(2) $\mathbb{V}(m_p) = \{p\}$ is a single point set. By Proposition 2.16, there is a one-to-one correspondence between maximal ideals in $\Bbbk[x_1, \cdots, x_n]$ and points in $\mathbb{A}^n$. Since the ideals of the form $m_p$ have exhausted all points in $\mathbb{A}^n$, they must be all maximal ideals in $\Bbbk[x_1, \cdots, x_n]$.

**Solution 2.4.** *A famous example: the twisted cubic.*

(1) We first show $X \subseteq \mathbb{V}(I)$. For every point $(t, t^2, t^3) \in X$, we have $y - x^2 = t^2 - t^2 = 0$ and $z - x^3 = t^3 - t^3 = 0$. We then show $\mathbb{V}(I) \subseteq X$. For every $(x, y, z) \in \mathbb{V}(I)$, we have $y - x^2 = 0$ and $z - x^3 = 0$, hence $y = x^2$ and $z = x^3$. It follows that $(x, y, z) = (x, x^2, x^3) \in X$.

(2) Consider the ring homomorphism

$$\varphi : \Bbbk[x, y, z] \longrightarrow \Bbbk[t]; \quad f(x, y, z) \longmapsto f(t, t^2, t^3).$$

By the fundamental isomorphism theorem, we have

$$\operatorname{im} \varphi \cong \Bbbk[x, y, z]/\ker \varphi.$$

We need to find out $\operatorname{im}\varphi$ and $\ker\varphi$.

We claim that $\varphi$ is surjective, because for every $p(t) \in \Bbbk[t]$, it is the image of $p(x) \in \Bbbk[x, y, z]$. Therefore $\operatorname{im}\varphi = \Bbbk[t]$.

To find out $\ker\varphi$, we first claim that every $f(x, y, z) \in \Bbbk[x, y, z]$ can be written in the form

$$f = (y - x^2)g_1 + (z - x^3)g_2 + h$$

where $g_1, g_2 \in \Bbbk[x, y, z]$ and $h \in \Bbbk[x]$. To see this, there are still two methods. The first method: think of $f$ as a polynomial in $y$, and consider the Euclidean division of $f$ by $y - x^2$. There is a quotient $g_1 \in \Bbbk[x, y, z]$ and a remainder $r_1 \in \Bbbk[x, z]$. Then think of $r_1$ as a polynomial in $z$, and consider the Euclidean division of $r_1$ by $z - x^3$. There is a quotient $g_2 \in \Bbbk[x, y, z]$ (in fact, in $\Bbbk[x, z]$) and a remainder $h \in \Bbbk[x]$. In formulas,

$$f = (y - x^2)g_1 + r_1 = (y - x^2)g_1 + (z - x^3)g_2 + h.$$

The second method: we substitute $[(y - x^2) + x^2]$ into each occurence of $y$ in $f$ and substitute $[(z - x^3) + x^3]$ into each occurence of $z$ in $f$. We then expand the square brackets leaving the round brackets untouched. In the expansion we collect terms with a factor $(y - x^2)$ or $(z - x^3)$, and write

$$f = (y - x^2)g_1 + (z - x^3)g_2 + h$$

where $h \in \Bbbk[x]$ does not involve $y$ or $z$.

Armed with this claim, we find that the image of $f$ under $\varphi$ is given by

$$\varphi(f) = (t^2 - t^2)\varphi(g_1) + (t^3 - t^3)\varphi(g_2) + h(t) = h(t).$$

Therefore $\varphi(f) = 0 \iff h = 0 \iff f = (y - x^2)g_1 + (z - x^3)g_2 \iff f \in (y - x^2, z - x^3)$. This means $\ker\varphi = (y - x^2, z - x^3) = I$.

Therefore the fundamental isomorphism theorem yields that $\Bbbk[t] \cong \Bbbk[x, y, z]/I$.

(3) Since $\Bbbk[t]$ is an integral domain, by Proposition 2.12, we conclude that $I$ is a prime ideal, hence a radical ideal. By part (1) and Proposition 2.9, $X = \mathbb{V}(I)$ implies that $I = \mathbb{I}(X)$. Since $I$ is a prime ideal, Proposition 2.15 shows that $X$ is an irreducible algebraic set, hence an affine variety.

## 3. Coordinate Rings

We define polynomial functions and coordinate rings for algebraic sets. We will also study polynomial maps between algebraic sets. Finally we will see how coordinate rings help us understand polynomial maps.

### 3.1. Coordinate rings and polynomial maps.

We look at functions on affine algebraic sets. Roughly speaking, a function on an algebraic set $X$ assigns to each point a value in $\Bbbk$. In algebraic geometry we are mostly interested in those functions defined by polynomials.

**Definition 3.1.** Let $X \subseteq \mathbb{A}^n$ be an algebraic set. A function $\varphi : X \to \Bbbk$ is a *polynomial function* if there exists $f \in \Bbbk[x_1, \cdots, x_n]$ such that $\varphi(p) = f(p)$ for every $p \in X$.

*Remark* 3.2. Two polynomials $f, g \in \Bbbk[x_1, \cdots, x_n]$ define the same function on $X$ if and only if for every point $p \in X$, $f(p) = g(p)$, or equivalently, $f(p) - g(p) = 0$. This holds if and only if $f - g \in \mathbb{I}(X)$ by the definition of $\mathbb{I}$. In other words, $f$ and $g$ define the same polynomial function on $X$ if and only if they are in the same coset of $\mathbb{I}(X)$ in $\Bbbk[x_1, \cdots, x_n]$. Therefore a polynomial function can be viewed as a coset of $\mathbb{I}(X)$, which is an element in the quotient ring $\Bbbk[x_1, \cdots, x_n]/\mathbb{I}(X)$. This leads to the following definition.

**Definition 3.3.** Let $X \subseteq \mathbb{A}^n$ be an algebraic set. The quotient ring

$$\Bbbk[X] := \Bbbk[x_1, \cdots, x_n]/\mathbb{I}(X)$$

is called the *coordinate ring* of $X$.

**Example 3.4.** For any algebraic set $X \subseteq \mathbb{A}^n$, the $i$-th coordinate defines a polynomial function $x_i : X \to \Bbbk$, which is called the $i$-th *coordinate function*. Since every polynomial function is a polynomial in the coordinate functions, we can view the coordinate functions as the generators of $\Bbbk[X]$. This is where the name "coordinate ring" comes from.

**Example 3.5.** For the algebraic set $X_1 = \mathbb{V}(x) \subseteq \mathbb{A}^2$, $\mathbb{I}(X_1) = (x)$ since $(x)$ is a prime ideal hence is radical. Therefore the coordinate ring of $X_1$ is $\Bbbk[X_1] = \Bbbk[x, y]/(x)$. We show that it is isomorphic $\Bbbk[t]$. Consider the ring homomorphism

$$\varphi : \Bbbk[x, y] \to \Bbbk[t]; \quad x \mapsto 0, \quad y \mapsto t.$$

It is surjective because each $p(t) \in \Bbbk[t]$ is the image of $p(y) \in \Bbbk[x, y]$. For any $f(x, y) \in \Bbbk[x, y]$, by collecting all terms involving $x$, we can write it as $f(x, y) = xg(x, y)+h(y)$. Its image $\varphi(f(x, y)) = h(t)$. Hence $f \in \ker(\varphi)$ is equivalent to $h(y) = 0$, which is further equivalent to $f(x, y) \in (x)$. This shows $\ker(\varphi) = (x)$. By the fundamental isomorphism theorem, we get $\Bbbk[X_1] = \Bbbk[x, y]/(x) \cong \Bbbk[t]$.

**Example 3.6.** For the algebraic sets $X_2 = \mathbb{V}(y)$ and $X_3 = \mathbb{V}(y - x^2)$ in $\mathbb{A}^2$, we can similarly find out that $\Bbbk[X_2] = \Bbbk[x, y]/(y) \cong \Bbbk[t]$ and $\Bbbk[X_3] = \Bbbk[x, y]/(y - x^2) \cong \Bbbk[t]$. It is not a coincidence that $X_1$, $X_2$ and $X_3$ have isomorphic coordinate rings. We will explain this later.

Now we study maps between algebraic sets.

**Definition 3.7.** Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be algebraic sets. A map $\varphi : X \to Y$ is a *polynomial map* if there exist polynomial functions $f_1, \cdots, f_m \in \Bbbk[X]$, such that $\varphi(p) = (f_1(p), \cdots, f_m(p)) \in Y$ for every point $p \in X$.

Notice that a polynomial function on $X$ is the same as a polynomial map from $X$ to $\mathbb{A}^1$.

**Example 3.8.** Let $X \subseteq \mathbb{A}^n$ be any algebraic set. The identity map $\mathrm{id}_X : X \to X$; $(x_1, \cdots, x_n) \mapsto (x_1, \cdots, x_n)$ is a polynomial map.

**Example 3.9.** Let $W \subseteq \mathbb{A}^2$ be any algebraic set and $X = \mathbb{A}^1$. Then $\varphi_0 : W \to X$; $(x, y) \mapsto xy$ is a polynomial map.

**Example 3.10.** Let $X = \mathbb{A}^1$. Let $Y_1 = \mathbb{V}(y - x^2)$, $Y_2 = \mathbb{V}(y^2 - x^3 - x^2)$ and $Y_3 = \mathbb{V}(y^2 - x^3)$ be algebraic sets in $\mathbb{A}^2$. Then $\varphi_1 : X \to Y_1$; $t \mapsto (t, t^2)$ is a polynomial map from $X$ to $Y_1$, since the point $(t, t^2)$ satisfies the defining equation of $Y_1$. Similarly, we can check that $\varphi_2 : X \to Y_2$; $t \mapsto (t^2-1, t^3-t)$ and $\varphi_3 : X \to Y_3$; $t \mapsto (t^2, t^3)$ are both polynomial maps.

*Remark* 3.11. Let $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$, $Z \subseteq \mathbb{A}^l$ be algebraic sets. Consider polynomial maps

$$\varphi = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)) : X \to Y,$$
$$\psi = (g_1(y_1, \cdots, y_m), \cdots, g_l(y_1, \cdots, y_m)) : Y \to Z.$$

We can compose them to get a new polynomial map

$$\psi \circ \varphi = (g_1(f_1, \cdots, f_m), \cdots, g_l(f_1, \cdots, f_m)) : X \to Z.$$

**Example 3.12.** To compose $\varphi_0 : W \to X$ in Example 3.9 and $\varphi_1 : X \to Y_1$ in Example 3.10, for any point $p = (x, y) \in W$, we have $(\varphi_1 \circ \varphi_0)(x, y) = \varphi_1(xy) = (xy, x^2y^2)$. Hence we get the polynomial map $\varphi_1 \circ \varphi_0 : W \to Y_1$; $(x, y) \mapsto (xy, x^2y^2)$.

We can now describe when two algebraic sets "look the same".

**Definition 3.13.** A polynomial map $\varphi : X \to Y$ between algebraic sets is an *isomorphism* if there exists a polynomial map $\psi : Y \to X$ such that $\psi \circ \varphi = \mathrm{id}_X$ and $\varphi \circ \psi = \mathrm{id}_Y$. Two algebraic sets $X$ and $Y$ are *isomorphic* if there exists an isomorphism between them.

**Example 3.14.** We show that $\varphi_1 : X \to Y_1$ in Example 3.10 is an isomorphism. Let $\psi_1 : Y_1 \to X$; $(x, y) \mapsto x$. Then the composition $\psi_1 \circ \varphi_1 : X \to X$ is given by $t \mapsto (t, t^2) \mapsto t$. Hence $\psi_1 \circ \varphi_1 = \mathrm{id}_X$. The other composition $\varphi_1 \circ \psi_1 : Y_1 \to Y_1$ is given by $(x, y) \mapsto x \mapsto (x, x^2)$. For every point $(x, y) \in Y_1$, we have $y - x^2 = 0$, hence $(x, y) = (x, x^2)$. This shows $\varphi_1 \circ \psi_1 = \mathrm{id}_{Y_1}$. We conclude that $\varphi_1 : X \to Y_1$ (and $\psi_1 : Y_1 \to X$) is an isomorphism; in other words, $X$ and $Y_1$ are isomorphic.

*Remark* 3.15. If a polynomial map $\varphi : X \to Y$ is an isomorphism, then it induces a bijection between the points in $X$ and $Y$. However, it is important to note that the converse is not true. We will see a counter example next time.

We will see next time that the coordinate ring captures a lot of geometry of the algebraic set. In particular, whether two algebraic sets are isomorphic can be easily seen from their coordinate rings.

3.2. **Homomophisms of coordinate rings.** We introduce a terminology which will be very convenient in our discussion.

**Definition 3.16.** A *finitely generated* $\Bbbk$*-algebra* is a ring that is isomorphic to a quotient of a polynomial ring $\Bbbk[x_1, \cdots, x_n]/I$. A $\Bbbk$*-algebra homomorphism* $\varphi : \Bbbk[y_1, \cdots, y_m]/J \to \Bbbk[x_1, \cdots, x_n]/I$ is a ring homomorphism such that $\varphi(c + J) = c + I$ for every constant polynomial $c \in \Bbbk$.

Recall that a polynomial function can be viewed as a polynomial map to $\mathbb{A}^1$.

**Definition 3.17.** Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be algebraic sets. Let $\varphi : X \to Y$ be a polynomial map and $g \in \Bbbk[Y]$ a polynomial function. The *pullback* of $g$ along $\varphi$ is the polynomial function $g \circ \varphi \in \Bbbk[X]$, denoted $\varphi^*(g)$.

The pullback map along $\varphi$ sends a polynomial function on $Y$ to a polynomial function on $X$. We show that it preserves the ring structure and constants.

**Lemma 3.18.** *For any polynomial map $\varphi : X \to Y$, the pullback map*

$$\varphi^* : \quad \Bbbk[Y] \to \Bbbk[X]; \quad g \mapsto g \circ \varphi$$

*is a $\Bbbk$-algebra homomorphism.*

*Proof.* We need to verify $\varphi^*$ preserves addition, multiplication and constants. For any $g_1, g_2 \in \Bbbk[Y]$, we need to show $(g_1 + g_2) \circ \varphi = g_1 \circ \varphi + g_2 \circ \varphi$. Indeed, for any point $p \in X$, $((g_1 + g_2) \circ \varphi)(p) = (g_1 + g_2)(\varphi(p)) = g_1(\varphi(p)) + g_2(\varphi(p)) = (g_1 \circ \varphi)(p) + (g_2 \circ \varphi)(p)$. Hence $\varphi^*$ preserves addition. Replacing additions by multiplications shows that $\varphi^*$ preserves multiplication. Now assume $g$ is a constant function on $Y$, say, there exists some $c \in \Bbbk$ such that $g(q) = c$ for every $q \in Y$. Then $(g \circ \varphi)(p) = g(\varphi(p)) = c$ for every $p \in X$. Therefore $\varphi^*(g)$ is the constant function on $X$ which takes the same value as $g$. $\square$

**Example 3.19.** The polynomial map $\varphi : \mathbb{A}^1 \to Y = \mathbb{V}(y - x^2)(\subseteq \mathbb{A}^2)$; $t \mapsto (t, t^2)$ induces a $\Bbbk$-algebra homomorphism $\varphi^* : \Bbbk[Y] \to \Bbbk[\mathbb{A}^1]$, or more precisely, $\varphi : \Bbbk[x, y]/(y - x^2) \to \Bbbk[t]$. For any polynomial function $f(x, y)$ on $Y$, $\varphi^*(f) = f(t, t^2) \in \Bbbk[t]$. In particular, for the coordinate functions $x$ and $y$ on $Y$, we have $\varphi^*(x) = t$ and $\varphi^*(y) = t^2$. For more examples, the pullback of the polynomial function $x + y$ is $t + t^2$; the pullback of $x^2y$ is $t^4$, and the pullback of $3x^3 + 5y + 1$ is $3t^3 + 5t^2 + 1$.

We have seen that every polynomial map $\varphi : X \to Y$ induces a $\Bbbk$-algebra homomorphism $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$. Next we show this is a one-to-one correspondence. This is the key property of the "pullback" construction.

**Theorem 3.20.** *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be algebraic sets. For every $\Bbbk$-algebra homomorphism $\Phi : \Bbbk[Y] \to \Bbbk[X]$, there exists a unique polynomial map $\varphi : X \to Y$, such that $\Phi = \varphi^*$.*

*Proof.* (This proof is non-examinable and not covered in lectures.)

We show the existence. For every coordinate function $y_i \in \Bbbk[Y]$, by assumption $f_i = \Phi(y_i) \in \Bbbk[X]$ is a polynomial function on $X$. Since $\Phi$ is a $\Bbbk$-algebra homomorphis, for any polynomial function $g(y_1, \cdots, y_m) \in \Bbbk[Y]$, the image $\Phi(g) = g(f_1, \cdots, f_m) \in \Bbbk[X]$.

We consider the polynomial map $\varphi = (f_1, \cdots, f_m) : X \to \mathbb{A}^m$. To show it is a polynomial map to $Y$, it must be checked that $(f_1(p), \cdots, f_m(p)) \in Y$ for every $p \in X$; that is, it must be checked

that $h(f_1(p), \cdots, f_m(p)) = 0$ for every polynomial $h \in \mathbb{I}(Y)$. Since $h$ represents the zero function in $\Bbbk[Y]$, $\Phi(h)$ is also the zero function in $\Bbbk[X]$, hence $\Phi(h)(p) = 0$ for every $p \in X$. It follows that $h(f_1(p), \cdots, f_m(p)) = \Phi(h)(p) = 0$, as desired.

To show $\Phi = \varphi^*$, it remains to show that $\Phi(g) = \varphi^*(g)$ for every $g \in \Bbbk[Y]$. Indeed, for any $p \in X$, $\Phi(g)(p) = g(f_1(p), \cdots, f_m(p)) = g(\varphi(p)) = (g \circ \varphi)(p) = \varphi^*(g)(p)$. Hence $\Phi(g) = \varphi^*(g)$, as required. This finishes the existence.

For uniqueness, assume there is another polynomial map $\varphi' = (f'_1, \cdots, f'_m) : X \to Y$ such that $\Phi = (f')^*$. Then for each $i$, $f'_i = (\varphi')^*(y_i) = \Phi(y_i) = \varphi^*(y_i) = f_i$. Hence $\varphi' = \varphi$. This finishes the uniqueness. $\square$

*Remark* 3.21. This theorem gives a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{polynomial maps} \\ \varphi : \ X \longrightarrow Y \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \Bbbk\text{-algebra homomorphisms} \\ \varphi^* : \ \Bbbk[Y] \longrightarrow \Bbbk[X] \end{array} \right\}.$$

An application of this result is the following criterion for isomorphisms.

**Proposition 3.22.** *A polynomial map $\varphi : X \to Y$ is an isomorphism if and only if $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ is a ring isomorphism.*

*Proof.* (This proof is non-examinable and not covered in lectures.)

Assume $\varphi : X \to Y$ is an isomorphism, then there exists $\psi : Y \to X$ such that $\psi \circ \varphi = \mathrm{id}_X$ and $\varphi \circ \psi = \mathrm{id}_Y$. By applying the pullback construction on both sides, we have $\varphi^* \circ \psi^* = (\psi \circ \varphi)^* = (\mathrm{id}_X)^* = \mathrm{id}_{\Bbbk[X]}$. Similarly we have $\psi^* \circ \varphi^* = \mathrm{id}_{\Bbbk[Y]}$. Therefore $\varphi^*$ and $\psi^*$ are mutually inverse ring homomorphisms. Hence $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ is an isomorphism.

Assume $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ is a ring isomorphism, then there exists $\Psi : \Bbbk[X] \to \Bbbk[Y]$ such that $\varphi^* \circ \Psi = \mathrm{id}_{\Bbbk[X]}$ and $\Psi \circ \varphi^* = \mathrm{id}_{\Bbbk[Y]}$. By the existence in Theorem 3.20 we can write $\Psi = \psi^*$ for some polynomial map $\psi : Y \to X$. Therefore we have $(\psi \circ \varphi)^* = \varphi^* \circ \psi^* = \varphi^* \circ \Psi = \mathrm{id}_{\Bbbk[X]} = (\mathrm{id}_X)^*$. By the uniqueness in Theorem 3.20, we get $\psi \circ \varphi = \mathrm{id}_X$. Similarly we can get $\varphi \circ \psi = \mathrm{id}_Y$. Hence $\varphi : X \to Y$ is an isomorphism. $\square$

This is a very powerful result as it allows us to show a certain polynomial map is an isomorphism without writing down another one going backwards. It can also be used to show a certain polynomial map is not an isomorphism, especially in some tricky situation where the map is actually bijective on points, as shown in the following example:

**Example 3.23.** We consider the polynomial map $\varphi : \mathbb{A}^1 \to X = \mathbb{V}(y^2 - x^3) \subseteq \mathbb{A}^2; t \mapsto (t^2, t^3)$; see Example 3.10. One can show that it is bijective on points in $\mathbb{A}^1$ and $X$. However, one can also show that $\varphi^* : \Bbbk[X] \to \Bbbk[\mathbb{A}^1]$ is not an isomorphism of rings, hence $\varphi$ is not an isomorphism of algebraic sets. We leave the details as an exercise.

## Exercise Sheet 3

*This sheet will be discussed in the exercise class on 23 October. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 3.1.** *Example: the graph of a polynomial function.*

(1) Show that the *projection map* $\pi : \mathbb{A}^n \to \mathbb{A}^r$, $n \geqslant r$, defined by $\pi(a_1, \cdots, a_n) = (a_1, \cdots, a_r)$ is a polynomial map.

(2) Let $X \subseteq \mathbb{A}^n$ be an algebraic set and $f \in \Bbbk[X]$. Define the subset $G(f) \subseteq \mathbb{A}^{n+1}$ by $G(f) = \{(a_1, \cdots, a_n, a_{n+1}) \in \mathbb{A}^{n+1} \mid (a_1, \cdots, a_n) \in X \text{ and } a_{n+1} = f(a_1, \cdots, a_n)\}$. Show that $G(f)$ is an algebraic set. (*Remark:* $G(f)$ is called the *graph* of $f$.)

(3) Show that the map $\varphi : X \to G(f)$; $(a_1, \cdots, a_n) \mapsto (a_1, \cdots, a_n, f(a_1, \cdots, a_n))$ is a polynomial map.

(4) Show that $\varphi$ is an isomorphism of algebraic sets by writing down the inverse polynomial map $\psi : G(f) \to X$, and checking both compositions are identities.

(5) Briefly explain why Example 3.14 is a special case of this.

**Exercise 3.2.** *Example: a nodal cubic.* Consider $X = \mathbb{V}(y^2 - x^3 - x^2) \subseteq \mathbb{A}^2$.

(1) Show that $\varphi : \mathbb{A}^1 \to X$; $t \mapsto (t^2 - 1, t^3 - t)$ is a polynomial map.

(2) Show that $\varphi$ is surjective but not injective on points, hence not an isomorphism.

(3) Show that $y^2 - x^3 - x^2$ is an irreducible polynomial. Use Exercise 2.2 to conclude that $I = (y^2 - x^3 - x^2)$ is a prime ideal, hence radical. Use Propositions 2.15 and 2.9 to conclude that $X$ is an affine variety and $\mathbb{I}(X) = I$.

**Exercise 3.3.** *Example: a cuspidal cubic.* Consider $X = \mathbb{V}(y^2 - x^3) \subseteq \mathbb{A}^2$.

(1) Show that $\varphi : \mathbb{A}^1 \to X$; $t \mapsto (t^2, t^3)$ is a polynomial map.

(2) Show that $\varphi$ is injective and surjective on points.

(3) Show that $y^2 - x^3$ is an irreducible polynomial. Conclude that $I = (y^2 - x^3)$ is a prime ideal, hence radical. Conclude that $X$ is an affine variety and $\mathbb{I}(X) = I$.

(4) Show that the $\Bbbk$-algebra homomorphism $\varphi^* : \Bbbk[X] \to \Bbbk[\mathbb{A}^1]$ is not surjective. Conclude by Proposition 3.22 that $\varphi$ is not an isomorphism.

**Exercise 3.4.** *Example: the twisted cubic, revisited.* This is a continuation of Exercise 2.4. We consider the polynomial map $\varphi : \mathbb{A}^1 \to X$; $t \mapsto (t, t^2, t^3)$.

(1) Show that $\varphi$ is an isomorphism by writing down the inverse $\psi : X \to \mathbb{A}^1$ and computing the two compositions.

(2) Show that $\varphi$ is an isomorphism by proving that $\varphi^*$ is an isomorphism.

## Solutions to Exercise Sheet 3

**Solution 3.1.** *Example: the graph of a polynomial function.*

(1) Every component of $\pi$ is given by a polynomial, and the image of any point in $\mathbb{A}^n$ is clearly in $\mathbb{A}^r$, so $\pi$ is a polynomial map.

(2) Since $X$ is an algebraic set, we can write $X = \mathbb{V}(S)$ where $S$ is a set of polynomials in $x_1, \cdots, x_n$. Each polynomial in $S$ can also be thought as a polynomial in $x_1, \cdots, x_n, x_{n+1}$. Assume the polynoial function $f$ is represented by a polynomial $F \in \Bbbk[x_1, \cdots, x_n]$. Then consider the set of polynomials $T = S \cup \{x_{n+1} - F\} \subseteq \Bbbk[x_1, \cdots, x_n, x_{n+1}]$. We claim $G(f) = \mathbb{V}(T)$.

To prove the claim, we need to show mutual inclusions. Given any point $p = (a_1, \cdots, a_n, a_{n+1}) \in G(f)$, we have $(a_1, \cdots, a_n) \in X$ and $a_{n+1} = f(a_1, \cdots, a_n)$. The former implies that $p$ is a solution to all polynomials in $S$, and the latter implies that $p$ is a solution to the polynomial $x_{n+1} - F$. It follows that $p \in \mathbb{V}(T)$.

Given any point $q = (a_1, \cdots, a_n, a_{n+1}) \in \mathbb{V}(T)$, since $x_{n+1}$ does not occur in any polynomial in $S$, we know that $(a_1, \cdots, a_n) \in \mathbb{V}(S)$. Moreover $a_{n+1} - F(a_1, \cdots, a_n) = 0$ implies that $a_{n+1} = F(a_1, \cdots, a_n) = f(a_1, \cdots, a_n)$. Hence $q \in G(f)$. This finishes the proof of the claim $G(f) = \mathbb{V}(T)$, which implies $G(f)$ is an algebraic set.

(3) The first $n$ components of $\varphi$ are obviously polynomials in $a_1, \cdots, a_n$. Since $f$ is a polynomial map, it can also be represented by a polynomial $F \in \Bbbk[x_1, \cdots, x_n]$. It remains to check the image of $\varphi$ is always in $G(f)$, which is clear from the definition of $G(f)$.

(4) We define $\psi : G(f) \to X$ as the projection map to the first $n$ components. Namely, $\psi(x_1, \cdots, x_{n+1}) = (x_1, \cdots, x_n)$. It is clearly a polynomial map. We compute both compositions. Given any $p = (a_1, \cdots, a_n) \in X$, we have

$$(\psi \circ \varphi)(p) = \psi(a_1, \cdots, a_n, f(a_1, \cdots, a_n)) = (a_1, \cdots, a_n) = p.$$

Given any $q = (a_1, \cdots, a_n, a_{n+1}) \in G(f)$, we have

$$(\varphi \circ \psi)(q) = \varphi(a_1, \cdots, a_n) = (a_1, \cdots, a_n, f(a_1, \cdots, a_n)) = (a_1, \cdots, a_n, a_{n+1}) = q.$$

Therefore $\varphi$ (hence also $\psi$) is an isomorphism.

(5) Let $X = \mathbb{A}^1$, and $f(x) = x^2 \in \Bbbk[x]$, then part (4) recovers Example 3.14.

**Solution 3.2.** *Example: a nodal cubic.*

(1) Both components in $\varphi$ are polynomials in $t$. Since

$$\begin{aligned} y^2 - x^3 - x^2 &= (t^3 - t)^2 - (t^2 - 1)^3 - (t^2 - 1)^2 \\ &= t^6 - 2t^4 + t^2 - t^6 + 3t^4 - 3t^2 + 1 - t^4 + 2t^2 - 1 = 0, \end{aligned}$$

we conclude $\varphi(t) \in X$ for every $t \in \mathbb{A}^1$. Hence $\varphi$ is a polynomial map.

(2) To show $\varphi$ is surjective but not injective on points, take any point $q = (x, y) \in X$. There are two cases. If $x = 0$, then by the defining equation of $X$ we also have $y = 0$. It is easy to see that the point $q = (0, 0)$ is the image of the point $t = 1$ or $t = -1$. Hence $\varphi$ is not injective on points. If $x \neq 0$, then consider $t = \frac{y}{x}$. To find its image, notice that

$$\begin{aligned} t^2 - 1 &= \frac{y^2}{x^2} - 1 = \frac{y^2 - x^2}{x^2} = \frac{x^3}{x^2} = x; \\ t^3 - t &= t \cdot (t^2 - 1) = \frac{y}{x} \cdot x = y. \end{aligned}$$

Therefore $\varphi(t) = (x, y)$, which means the point $q = (x, y)$ is in the image of $\varphi$. The two cases together show that $\varphi$ is surjective on points. Since we have proved $\varphi$ is not injective on points, it cannot be an isomorphism by Remark 3.15.

(3) Use contradiction. Assume $y^2 - x^3 - x^2 = f(x, y)g(x, y)$ for non-constant polynomials $f, g \in \Bbbk[x, y]$. Since the left-hand side has degree 2 in $y$, the degrees of $f$ and $g$ in $y$ must be either 2 and 0, or 1 and 1. In the first case we can write

$$y^2 - x^3 - x^2 = (y^2 f_2(x) + y f_1(x) + f_0(x)) \cdot g(x).$$

Comparing coefficients of $y^2$ we find $f_2(x)g(x) = 1$, hence $g(x)$ must be a constant. Contradiction. In the second case we can write

$$y^2 - x^3 - x^2 = (y f_1(x) + f_0(x)) \cdot (y g_1(x) + g_0(x)).$$

Comparing coefficients of $y^2$ we find $f_1(x)g_1(x) = 1$. Without loss of generality we can assume $f_1(x) = g_1(x) = 1$. Comparing coefficients of $y$ we find $f_0(x) + g_0(x) = 0$. Comparing constant terms we find $-x^3 - x^2 = f_0(x)g_0(x) = -f_0(x)^2$, hence $f_0(x)^2 = x^3 + x^2$, which is also a contradiction since $x^3 + x^2 = x^2(x + 1)$ is not a square. So we conclude that $y^2 - x^3 - x^2$ is irreducible. By Exercise 2.2 (1) we know $I = (y^2 - x^3 - x^2)$ is a prime ideal. By Proposition 2.12 (2) we know $I$ is a radical ideal. By Proposition 2.9 (1) we know $\mathbb{I}(X) = I$. By Proposition 2.15 we know $X$ is an irreducible algebraic set, i.e. an affine variety.

**Solution 3.3.** *Example: a cuspidal cubic.*

(1) Both components in $\varphi$ are polynomials in $t$. Since

$$y^2 - x^3 = (t^3)^2 - (t^2)^3 = 0,$$

we conclude $\varphi(t) \in X$ for every $t \in \mathbb{A}^1$. Hence $\varphi$ is a polynomial map.

(2) To show $\varphi$ is injective and surjective on points, take any point $q = (x, y) \in X$. There are two cases. If $x = 0$, then by the defining equation of $X$ we also have $y = 0$. Assume $\varphi(t) = (0, 0)$, then there is a unique point $t = 0$ whose image is $(0, 0)$. If $x \neq 0$, assume $\varphi(t) = (x, y)$, then we must have $t = \frac{y}{x}$, so there is at most one point whose image is $(x, y)$. To check that its image is indeed $(x, y)$, notice that

$$t^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2}x;$$
$$t^3 = t \cdot t^2 = \frac{y}{x} \cdot x = y.$$

Therefore $\varphi(t) = (x, y)$, which means there is a unique point $t \in \mathbb{A}^1$ whose image is the point $q = (x, y)$. The two cases together show that $\varphi$ is injective and surjective on points.

(3) Use contradiction. Assume $y^2 - x^3 = f(x, y)g(x, y)$ for non-constant polynomials $f, g \in \Bbbk[x, y]$. Since the left-hand side has degree 2 in $y$, the degrees of $f$ and $g$ in $y$ must be either 2 and 0, or 1 and 1. In the first case we can write

$$y^2 - x^3 = (y^2 f_2(x) + y f_1(x) + f_0(x)) \cdot g(x).$$

Comparing coefficients of $y^2$ we find $f_2(x)g(x) = 1$, hence $g(x)$ must be a constant. Contradiction. In the second case we can write

$$y^2 - x^3 = (y f_1(x) + f_0(x)) \cdot (y g_1(x) + g_0(x)).$$

Comparing coefficients of $y^2$ we find $f_1(x)g_1(x) = 1$. Without loss of generality we can assume $f_1(x) = g_1(x) = 1$. Comparing coefficients of $y$ we find $f_0(x) + g_0(x) = 0$. Comparing constant terms we find $-x^3 = f_0(x)g_0(x) = -f_0(x)^2$, hence $f_0(x)^2 = x^3$, which is also a contradiction since $x^3$ is not a square. So we conclude that $y^2 - x^3$ is irreducible. By Exercise 2.2 (1) we know $I = (y^2 - x^3)$ is a prime ideal. By Proposition 2.12 (2) we know $I$ is a radical ideal. By Proposition 2.9 (1) we know $\mathbb{I}(X) = I$. By Proposition 2.15 we know $X$ is an irreducible algebraic set, i.e. an affine variety.

(4) By part (3) we have $\Bbbk[X] = \Bbbk[x, y]/(y^2 - x^3)$. To write down the pullback map explicitly, we notice that $\varphi^*(x) = t^2$ and $\varphi^*(y) = t^3$. Therefore for any polynomial map on $X$ represented by a polynomial $f(x, y) \in \Bbbk[x, y]$, its image $\varphi^*(f) = f(t^2, t^3)$; that means, we simply replace every occurence of $x$ by $t^2$ and $y$ by $t^3$. It is clear that $\varphi^*(f)$ is a polynomial in $t$. We claim that it has no term of degree 1 in $t$. Indeed, the image of the constant term of $f$ is still the same constant, and the image of any other monomial of $f$ is a monomial in $t$ of degree at least 2. This claim implies that $\varphi^*$ is not surjective, because any polynomial in $t$ with a non-zero degree 1 term is not in the image of $\varphi^*$. In particular, $t \in \Bbbk[t] = \Bbbk[\mathbb{A}^1]$ is not in the image of $\varphi^*$. Hence $\varphi^*$ is not an isomorphism. By Proposition 3.22, $\varphi$ is not an isomorphism.

**Solution 3.4.** *Example: the twisted cubic, revisited.*

(1) We define the polynomial map $\psi : X \to \mathbb{A}^1$ by $\psi(x, y, z) = x$. It is clearly a polynomial map as its only component is a polynomial. For any $t \in \mathbb{A}^1$, we have $(\psi \circ \varphi)(t) = \psi(t, t^2, t^3) = t$. For any $(x, y, z) \in X$, we have $(\varphi \circ \psi)(x, y, z) = \varphi(x) = (x, x^2, x^3) = (x, y, z)$. This shows that $\varphi$ is an isomorphism.

(2) We first write down the pullback map $\varphi^*$ explicitly. By Exercise 2.4 (3), we have $\Bbbk[X] = \Bbbk[x, y, z]/\mathbb{I}(X) = \Bbbk[x, y, z]/(y - x^2, z - x^3)$. We also have $\Bbbk[\mathbb{A}^1] = \Bbbk[t]$. The pullback of the coordinate functions are given by $\varphi^*(x) = t$, $\varphi^*(y) = t^2$ and $\varphi^*(z) = t^3$. Therefore $\varphi^*$ is given by

$$\varphi^* : \quad \Bbbk[x, y, z]/(y - x^2, z - x^3) \longrightarrow \Bbbk[t]; \quad f(x, y, z) \longmapsto f(t, t^2, t^3).$$

We actually have proved in Exercise 2.4 (2) that $\varphi^*$ is an isomorphism. Indeed, $\varphi^*$ is surjective because every $p(t) \in \Bbbk[t]$ is the image of $p(x) \in \Bbbk[x, y, z]$ (or rather, the coset $p(x) + \mathbb{I}(X)$ in the quotient ring). Moreover, $\varphi^*$ is injective because if the image of $f(x, y, z)$ is the zero polynomial in $\Bbbk[t]$, it must be in $\mathbb{I}(X)$, which means that the only element in the kernel of $\varphi^*$

is the coset $0+\mathbb{I}(X)$, which is the zero element in the quotient ring. Therefore by Proposition 3.22, we conclude that $\varphi$ is an isomorphism.

## 4. Projective Algebraic Sets

Instead of affine spaces, it is more natural to study algebraic geometry in projective spaces. We first introduce projective spaces, then study projective algebraic sets. There is a similar projective Nullstellensatz and $\mathbb{V}-\mathbb{I}$ correspondence.

4.1. **Projective spaces.** We will study algebraic geometry in projective spaces. We prefer projective spaces because results in projective spaces are usually nicer. One such example is that: two curves in $\mathbb{A}^2$ may or may not intersect each other. When they intersect, the number of intersection is not known until one solves the system of equations. However, in projective spaces $\mathbb{P}^2$, two curves always intersect, and the number of intersection points can be easily read off from their equations. In this lecture we will understand the projective space $\mathbb{P}^n$ from the following three different points of views:

- $\mathbb{P}^n$ is the set of 1-dimensional subspaces in $\mathbb{A}^{n+1}$ (definition);
- $\mathbb{P}^n$ is covered by $n+1$ subsets which are all $\mathbb{A}^n$ (aka from projective to affine);
- $\mathbb{P}^n$ is obtained by adding to $\mathbb{A}^n$ a "boundary at infinity", whose points correspond to "asymptotic directions" in $\mathbb{A}^n$ (aka from affine to projective).

**Definition 4.1.** For every integer $n \geqslant 0$, the *projective space* $\mathbb{P}^n_{\Bbbk}$ (or $\mathbb{P}^n$ if $\Bbbk$ is understood) of dimension $n$ over a field $\Bbbk$ is the set of 1-dimensional vector subspaces in $\mathbb{A}^{n+1}_{\Bbbk}$.

*Remark* 4.2. Each point $a=(a_0,a_1,\cdots,a_n)\neq(0,0,\cdots,0)$ in $\mathbb{A}^{n+1}$ determines a 1-dimensional subspace. Two such points $a=(a_0,a_1,\cdots,a_n)$ and $b=(b_0,b_1,\cdots,b_n)$ define the same subspace if and only if there is some $\lambda\neq 0$ such that $b_i=\lambda a_i$ for each $0\leqslant i\leqslant n$. We say two such points are equivalent, and write $a\sim b$. Then points in $\mathbb{P}^n$ can be identified with such equivalence classes. More precisely,

$$\mathbb{P}^n=\left(\mathbb{A}^{n+1}\backslash\{(0,\cdots,0)\}\right)/\sim.$$

**Definition 4.3.** If a point $p\in\mathbb{P}^n$ is determined by $(a_0,a_1,\cdots,a_n)\in\mathbb{A}^{n+1}\backslash\{(0,\cdots,0)\}$, we say that $a_0,a_1,\cdots,a_n$ are *homogeneous coordinates* of $p$, denoted $p=[a_0:a_1:\cdots:a_n]$.

*Remark* 4.4. The homoeneous coordinates of $p\in\mathbb{P}^n$ are only determined up to a non-zero scalar multiplication, so the $i$-th coordinate $a_i$ is not a well-defined number. However, it is a well-defined notion to say whether $a_i$ is zero or non-zero; and if $a_i\neq 0$, the ratios $a_j/a_i$ are also well-defined (since they remain unchanged under equivalence).

We want to relate projective spaces to our familiar affine spaces, so that we can "visualise" them easily. There are two typical ways to do this.

**Construction 4.5** (From projective to affine)**.** We will see how to find subsets in $\mathbb{P}^n$ which are affine spaces. For each $0\leqslant i\leqslant n$, consider the subset

$$U_i=\{[a_0:a_1:\cdots:a_n]\in\mathbb{P}^n\mid a_i\neq 0\}.$$

Each point $p\in U_i$ can be written as

$$p=\left[\frac{a_0}{a_i}:\cdots:\frac{a_{i-1}}{a_i}:1:\frac{a_{i+1}}{a_i}:\cdots:\frac{a_n}{a_i}\right].$$

Since we insist that the $i$-th coordinate is 1, the other $n$ coordinates are uniquely determined, which can be used to identify $U_i$ with $\mathbb{A}^n$. Moreover, since every point in $\mathbb{P}^n$ has at least one non-zero homogeneous coordinate, it lies in at least one of the $U_i$'s. This implies

$$\mathbb{P}^n=\cup_{i=0}^n U_i. \tag{4.1}$$

So $\mathbb{P}^n$ is covered by $n+1$ subsets, each of which looks just like $\mathbb{A}^n$.

**Definition 4.6.** Each subset $U_i = \{[a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^n \mid a_i \neq 0\}$ of $\mathbb{P}^n$ is called a *standard affine chart* of $\mathbb{P}^n$. For every point $p = [a_0 : a_1 : \cdots : a_n] \in U_i$, the $n$-tuple $\left(\frac{a_0}{a_i}, \cdots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \cdots, \frac{a_n}{a_i}\right)$ are called the *non-homogeneous coordinates* of $p$ with respect to $U_i$. The cover $\mathbb{P}^n = \cup_{i=0}^n U_i$ is called a *standard affine cover* of $\mathbb{P}^n$.

**Example 4.7.** $\mathbb{P}^1$ has two standard affine charts. The point $[2 : 3] \in \mathbb{P}^1$ has non-homogeneous coordinate $\frac{3}{2}$ with respect to $U_0$, and $\frac{2}{3}$ with respect to $U_1$. $\mathbb{P}^2$ has three standard affine charts. The point $[2 : 3 : 0] \in \mathbb{P}^2$ has non-homogeneous coordinates $(\frac{3}{2}, 0)$ with respect to $U_0$, and $(\frac{2}{3}, 0)$ with respect to $U_1$. This point is not in $U_2$ because the corresponding coordinate is 0.

**Construction 4.8** (From affine to projective)**.** We will see how to get $\mathbb{P}^n$ by adding "points at infinity" to the affine space $\mathbb{A}^n$. We work with $U_0$ but each $U_i$ works in the same way. The complement of $U_0$ in $\mathbb{P}^n$ is

$$H_0 = \mathbb{P}^n \backslash U_0 = \{[0 : a_1 : \cdots : a_n] \in \mathbb{P}^n\},$$

which can be identified with $\mathbb{P}^{n-1}$ as each point in $H_0$ is given by $n$ homogeneous coordinates which are not simultaneously zero. Hence $\mathbb{P}^n$ can be decomposed into an affine space $U_0 \cong \mathbb{A}^n$ and a set of "points at infinity" $H_0 \cong \mathbb{P}^{n-1}$:

$$\mathbb{P}^n = U_0 \cup H_0 \cong \mathbb{A}^n \cup \mathbb{P}^{n-1}. \tag{4.2}$$

Now we explain why we can view points in $H_0$ as "asymptotic directions" of lines in $U_0 = \mathbb{A}^n$. This is best illustrated for $n = 2$, but works for any positive integer $n$.

**Example 4.9.** Consider two lines $\mathbb{V}(x_2 - x_1 + 1)$ and $\mathbb{V}(x_2 - x_1 - 1)$ in $\mathbb{A}^2 \cong U_0$. They are parallel since they have the same slope. We can regard $x_1$ and $x_2$ as the non-homogeneous coordinates with respect to $U_0$, and substitute $x_i$ by $\frac{a_i}{a_0}$. Then the defining equations of the two lines become

$$\frac{a_2}{a_0} - \frac{a_1}{a_0} \pm 1 = 0.$$

We clear the denominators to get

$$a_2 - a_1 \pm a_0 = 0.$$

Notice that after clearing the denominator, we no longer require $a_0$ to be non-zero. Therefore we could possibly get extra solutions corresponding to points in $H_0$. To see which points in $H_0$ satisfy the equation, we set $a_0 = 0$. Then the equation becomes

$$a_2 - a_1 = 0.$$

Up to a non-zero scalar multiplication we get one extra solution $[a_0 : a_1 : a_2] = [0 : 1 : 1]$. So we can say both lines pass through (and intersect at) the point $[0 : 1 : 1]$ at infinity. Since parallel lines always acquire the same point at infinity, we get an idea that points in $H_0$ correspond to "asymptotic directions".

This example shows us how to understand points at infinity. We use the line $\mathbb{V}(x_2 - x_1 + 1)$ to preview some notions that will come up later. After clearing the denominators, we get a polynomial $a_2 - a_1 + a_0$ in which every monomial has the same degree. We say such a polynomial is *homogeneous*. Its solutions in $\mathbb{P}^2$ is called a *projective algebraic set*. Since it is obtained by adding the appropriate "points at infinity" to the affine algebraic set $\mathbb{V}(x_2 - x_1 + 1)$, we say this projective algebraic set is the *projective closure* of the affine algebraic set $\mathbb{V}(x_2 - x_1 + 1)$. In fact, every affine algebraic set in $\mathbb{A}^n$ (not necessarily a line) has a projective closure in $\mathbb{P}^n$ obtained by adding the appropiate "points at infinity", which can be computed using a similar calculation. We will see more examples later.

4.2. **Projective algebraic sets and projective Nullstellensatz.** We develop the theory of projective algebraic sets. Most of the results and proofs are similar to those in the affine case. We will be brief on the similar part, but careful on a few special features.

**Definition 4.10.** A non-zero polynomial $f \in \Bbbk[z_0, z_1, \cdots, z_n]$ is *homogeneous of degree $d$* if each term of $f$ has the same total degree $d$.

As easy examples, $z_2 - z_1^2$ is not homogeneous while $z_0z_2 - z_1^2$ is homogeneous of degree 2. The importance of this notion is the following. If $f$ is homogeneous of degree $d$, then

$$f(\lambda a_0, \lambda a_1, \cdots, \lambda a_n) = \lambda^d f(a_0, a_1, \cdots, a_n). \tag{4.3}$$

In particular this means $f(\lambda a_0, \lambda a_1, \cdots, \lambda a_n) = 0$ if and only if $f(a_0, a_1, \cdots, a_n) = 0$ for any $\lambda \neq 0$. Therefore for any point $p = [a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^n$, the condition $f(p) = 0$ is independent of the choice of its homogeneous coordinates. Hence the zero locus of $f$

$$\{[a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^n \mid f(a_0, a_1, \cdots, a_n) = 0\}$$

is also well-defined.

*Remark* 4.11. Since the zero polynomial satisfies (4.3) for every non-negative integer $d$, as a convention, the zero polynomial is considered to be a homogeneous polynomial of any degree. By doing so, we can avoid many unnecessary exceptions. For instance, the sum of two homogeneous polynomial of degree $d$ is again a homogeneous polynomial of degree $d$ when we include the zero polynomial.

**Definition 4.12.** For any non-zero polynomial $f \in \Bbbk[z_0, z_1, \cdots, z_n]$ of degree $m$, we say $f = f_0 + f_1 + \cdots + f_m$ is the *homogeneous decomposition* of $f$, if for each $i$, $0 \leqslant i \leqslant m$, $f_i$ is homogeneous of degree $i$. Each $f_i$ is called a *homogeneous component* of $f$.

**Definition 4.13.** An ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$ is *homogeneous* if for every non-zero polynomial $f \in I$, each of its homogeneous components $f_i \in I$.

In practice, this condition for an ideal being homogeneous is not very easy to check. The following criterion is usually more convenient.

**Proposition 4.14.** *An ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$ is homogeneous if and only if it can be generated by a finite set of homogeneous polynomials.*

*Proof.* We leave the proof as an exercise. □

**Example 4.15.** The ideals $(x)$ and $(x, y^2)$ in $\Bbbk[x, y]$ are both homogeneous, while the ideal $(x + y^2)$ in $\Bbbk[x, y]$ is not homogeneous, because the degree 1 part of $x + y^2$ is $x$, which is not in this ideal.

Notice that an ideal could have many different sets of generators. The statement only requires one set of generators consists of only homogeneous polynomials. It is still possible that some other generating set is not given by homogeneous polynomials. Next we can define the correspondences $\mathbb{V}$ and $\mathbb{I}$.

**Definition 4.16.** For any homogeneous ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$, the set

$$\mathbb{V}(I) = \{p \in \mathbb{P}^n \mid f(p) = 0 \text{ for every homogeneous polynomial } f \in I\}$$

is called the *projective algebraic set* defined by $I$.

Similar to the affine case, the following result is usually convenient in practice.

**Lemma 4.17.** *Suppose a homogeneous ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$ is generated by a finite set of homogeneous polynomials $S = \{f_1, \cdots, f_m\}$. Let*

$$\mathbb{V}(S) = \{p \in \mathbb{P}^n \mid f_1(p) = \cdots f_m(p) = 0\}.$$

*Then $\mathbb{V}(S) = \mathbb{V}(I)$.*

*Proof.* Similar to the proof of Lemma 1.10. We leave it as an exercise. □

**Corollary 4.18.** *Every projective algebraic set $X \subseteq \mathbb{P}^n$ can be written as $\mathbb{V}(S)$ for a finite set $S$ of homogeneneous polynomials in $\Bbbk[z_0, \cdots, z_n]$.*

*Proof.* It follows immediately from Propositions 4.14 and 4.17. □

**Example 4.19.** In $\mathbb{P}^1$, the projective algebraic set $\mathbb{V}(3z_0 - 2z_1)$ is the single-point set $\{[2:3]\}$. In $\mathbb{P}^2$, the projective algebraic set $\mathbb{V}(z_2 - z_1 + z_0)$ is one of the affine lines in Example 4.9 together with the corresponding point at infinity.

**Definition 4.20.** A projective algebraic set $X \subseteq \mathbb{P}^n$ is called a *hypersurface* if $X = \mathbb{V}(f)$ for some non-constant homogeneous polynomial $f \in \Bbbk[z_0, z_1, \cdots, z_n]$.

**Definition 4.21.** For any subset $X \subseteq \mathbb{P}^n$, the set

$$\mathbb{I}(X) = \left\{ f \in \Bbbk[z_0, z_1, \cdots, z_n] \;\middle|\; \begin{array}{c} f(p) = 0 \text{ for every choice of homogeneous} \\ \text{coordinates of every point } p \in X \end{array} \right\}$$

is called the *ideal of* $X$.

**Lemma 4.22.** *For any subset $X \subseteq \mathbb{P}^n$, $\mathbb{I}(X)$ is a homogeneous radical ideal.*

*Proof.* The proof of Lemma 2.6 (2) works literally here to show $\mathbb{I}(X)$ is a radical ideal. To show it is homogeneous, let $f \in \mathbb{I}(X)$ and write $f = f_0 + f_1 + \cdots + f_m$ for the homogeneous decomposition of $f$ where $m$ is the degree of $f$. For each $p = [a_0 : a_1 : \cdots : a_n] \in X$ and $\lambda \in \Bbbk \backslash \{0\}$, we can also write $p = [\lambda a_0 : \lambda a_1 : \cdots : \lambda a_n]$, hence we have

$$\begin{aligned} 0 = f(p) &= f(\lambda a_0, \lambda a_1, \cdots, \lambda a_n) \\ &= \sum_{i=0}^{m} f_i(\lambda a_0, \lambda a_1, \cdots, \lambda a_n) \\ &= \sum_{i=0}^{m} \lambda^i f_i(a_0, a_1, \cdots, a_n) = \sum_{i=0}^{m} \lambda^i f_i(p). \end{aligned}$$

This means that every $\lambda \in \Bbbk \backslash \{0\}$ is a root of the polynomial $\sum_{i=0}^{m} f_i(p) x^i \in \Bbbk[x]$. This must be a zero polynomial, because the number of roots of any non-zero polynomial is at most equal to its degree $m$. It follows that $f_i(p) = 0$ for every $0 \leqslant i \leqslant m$, so $f_i \in \mathbb{I}(X)$. $\square$

*Remark* 4.23. We have used the same notation $\mathbb{V}$ and $\mathbb{I}$ in both affine and projective cases. In practice it is usually clear which is meant; but if there is any danger of confusion, we will write $\mathbb{V}_p$ and $\mathbb{I}_p$ for the projective operations, $\mathbb{V}_a$ and $\mathbb{I}_a$ for the affine ones.

Now we state the projective Nullstellensatz. It is similar to the affine version, but there is one point where care is needed. Clearly the trivial ideal $(1) = \Bbbk[z_0, z_1, \cdots, z_n]$ defines the empty set in $\mathbb{A}^{n+1}$, hence the empty set in $\mathbb{P}^n$, as it should be. However, the ideal $(z_0, z_1, \cdots, z_n)$ defines a single-point set $\{(0, \cdots, 0)\}$ in $\mathbb{A}^{n+1}$, which also corresponds to the empty set in $\mathbb{P}^n$. This ideal $(z_0, z_1, \cdots, z_n)$ is an awkward exception to several statements in the theory, and is traditionally known as the "irrelevant ideal". Keeping that in mind, we state the projective version of Nullstellensatz.

**Theorem 4.24** (Projective Nullstellensatz)**.** *Let $\Bbbk$ be an algebraically closed field. For any homogeneous ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$,*

(1) $\mathbb{V}(I) = \varnothing$ *if and only if* $\sqrt{I} \supseteq (z_0, z_1, \cdots, z_n)$.

(2) *If* $\mathbb{V}(I) \neq \varnothing$, *then* $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

*Proof.* This is an easy consequence of the affine Nullstellensatz. Non-examinable. Interested reader can find the proof in [Section 5.3, Reid, Undergraduate Algebraic Geometry] or [Section 4.2, Fulton, Algebraic Curves]. $\square$

## Exercise Sheet 4

*This sheet will be discussed in the exercise class on 30 October. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 4.1.** *Get familiar with projective spaces.* Answer the following quick questions.

(1) What is $\mathbb{P}^0$? Why does $\mathbb{P}^1$ have only one more point than $\mathbb{A}^1$? When $\Bbbk = \mathbb{C}$, can you picture $\mathbb{P}^1_{\mathbb{C}}$ as a bubble (or a ball, something like that)? Which points in $\mathbb{P}^n$ belong to only one of the $U_i$'s in the standard affine cover of $\mathbb{P}^n$?

(2) Follow Example 4.9 to find the points at infinity for the affine algebraic set $\mathbb{V}_a(x_2^2 - x_1^2 - 1) \subseteq \mathbb{A}^2$. Do the same for $\mathbb{V}_a(x_2^2 - x_1^2)$ and $\mathbb{V}_a(x_2^2 - x_1^3)$ in $\mathbb{A}^2$.

**Exercise 4.2.** *Properties of homogeneous polynomials and ideals.*

(1) Let $f \in \Bbbk[z_0, \cdots, z_n]$ be a non-zero homogeneous polynomial. Assume $f = gh$ for some $g, h \in \Bbbk[z_0, \cdots, z_n]$. Show that $g$ and $h$ are also homogeneous polynomials.

(2) Show that an ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$ is homogeneous if and only if it can be generated by a finite set of homogeneous polynomials.

(3) Suppose a homogeneous ideal $I \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$ is generated by a finite set of homogeneous polynomials $S = \{f_1, \cdots, f_m\}$. Show that $\mathbb{V}_p(I) = \mathbb{V}_p(S)$.

**Exercise 4.3.** *Projective spaces are better than affine spaces!* A *line* in $\mathbb{P}^2$ is a projective algebraic set $\mathbb{V}_p(f)$ defined by a homogeneous linear polynomial $f = a_0 z_0 + a_1 z_1 + a_2 z_2 \in \Bbbk[z_0, z_1, z_2]$ for some $a_0, a_1, a_2 \in \Bbbk$ not simultaneously zero.

(1) Show that two distinct points in $\mathbb{P}^2$ determine a unique line.

(2) Show that two distinct lines in $\mathbb{P}^2$ intersect at a unique point.

(*Hint:* How to compute the dimension of the null space of a matrix? Rank-nullity!)

**Exercise 4.4.** *Example of projective algebraic sets.* Recall that we always assume $\Bbbk$ is algebraically closed. Prove that projective algebraic sets in $\mathbb{P}^1$ are just the finite subsets in $\mathbb{P}^1$ (including $\varnothing$) together with $\mathbb{P}^1$ itself. You can follow these steps:

(1) Verify that they are indeed projective algebraic sets.

(2) Show that every non-constant homogeneous polynomial $f(z_0, z_1) \in \Bbbk[z_0, z_1]$ can be factored into a product of homogeneous polynomials of degree 1. (*Hint:* you can use the following lemma in algebra: a non-constant polynomial $g(x) \in \Bbbk[x]$ can be factored into a product of polynomials of degree 1.)

(3) Show that if a projective algebraic set in $\mathbb{P}^1$ is not $\mathbb{P}^1$ itself, then it contains at most finitely many points.

## Solutions to Exercise Sheet 4

**Solution 4.1.** *Get familiar with projective spaces.*

(1) Since there is only one 1-dimensional linear subspace in $\mathbb{A}^1$, $\mathbb{P}^0$ is a point. $\mathbb{P}^1 = U_0 \cup H_0$ where $U_0 \cong \mathbb{A}^1$ is an affine space and $H_0 \cong \mathbb{P}^0$ is a point. Therefore $\mathbb{P}^1$ has just one more point than $\mathbb{A}^1$. When $\Bbbk = \mathbb{C}$, $U_0 \cong \mathbb{A}^1_{\mathbb{C}} = \mathbb{C}^1$ is the complex plane. To view $\mathbb{P}^1$ as a bubble, imagine we remove a point from the surface of a bubble (or a globe), the remaining part can be stretched into the complex plane.

A point $p \in \mathbb{P}^n$ belongs to only one of the standard affine chart $U_i$ if and only if $p$ has only one non-zero homogeneous coordinate. We can assume this non-zero homogeneous coordinate to be 1, otherwise we can divide all components by it. So the point $p$ can be given by $p = [0 : \cdots : 0 : 1 : 0 : \cdots : 0]$ with 1 at a certain position and 0 at all other positions. There are $n + 1$ such points.

(2) We regard $x_1$ and $x_2$ as non-homogeneous coordinates and substitute $x_1 = \frac{z_1}{z_0}$ and $x_2 = \frac{z_2}{z_0}$. The equation $x_2^2 - x_1^2 - 1 = 0$ becomes $\frac{z_2^2}{z_0^2} - \frac{z_1^2}{z_0^2} - 1 = 0$. We clear the denominators to allow $z_0$ to be zero, then we get $z_2^2 - z_1^2 - z_0^2 = 0$. To find the points at infinity, set $z_0 = 0$, then we have $z_2^2 - z_1^2 = 0$, hence $z_2 = \pm z_1$. As points in $\mathbb{P}^2$ we get two solutions $[z_0 : z_1 : z_2] = [0 : 1 : 1]$ or $[0 : 1 : -1]$, which are the points at infinity for $\mathbb{V}_a(x_2^2 - x_1^2 - 1)$. This example tells us that a hyperbola has two "asymptotic directions", which is easy to understand since a hyperbola has two asymptotes.

For $\mathbb{V}_a(x_2^2 - x_1^2)$, we still substitute $x_1 = \frac{z_1}{z_0}$ and $x_2 = \frac{z_2}{z_0}$. The equation $x_2^2 - x_1^2 = 0$ becomes $\frac{z_2^2}{z_0^2} - \frac{z_1^2}{z_0^2} = 0$. We clear the denominators to allow $z_0$ to be zero, then we get $z_2^2 - z_1^2 = 0$. To find the points at infinity, set $z_0 = 0$, then we still have $z_2^2 - z_1^2 = 0$, hence $z_2 = \pm z_1$. As points in $\mathbb{P}^2$ we get two solutions $[z_0 : z_1 : z_2] = [0 : 1 : 1]$ or $[0 : 1 : -1]$, which are the points at infinity for $\mathbb{V}_a(x_2^2 - x_1^2)$. The result is not surprising, because the polynomial $x_2^2 - x_1^2$ defines precisely the two asymptotes of the hyperbola in the previous case.

For $\mathbb{V}_a(x_2^2 - x_1^3)$, we still substitute $x_1 = \frac{z_1}{z_0}$ and $x_2 = \frac{z_2}{z_0}$. The equation $x_2^2 - x_1^3 = 0$ becomes $\frac{z_2^2}{z_0^2} - \frac{z_1^3}{z_0^3} = 0$. We clear the denominators to allow $z_0$ to be zero, then we get $z_0 z_2^2 - z_1^3 = 0$. To find the points at infinity, set $z_0 = 0$, then we get $-z_1^3 = 0$, hence $z_1 = 0$. As points in $\mathbb{P}^2$ we get one solution $[z_0 : z_1 : z_2] = [0 : 0 : 1]$, which is the point at infinity for $\mathbb{V}_a(x_2^2 - x_1^3)$.

**Solution 4.2.** *Properties of homogeneous polynomials and ideals.*

(1) We write the homogeneous decompositions of $g$ and $h$ as

$$g = g_M + g_{M-1} + \cdots + g_{m+1} + g_m,$$
$$h = h_N + h_{N-1} + \cdots + h_{n+1} + h_n,$$

where $M$ and $m$ are the maximal and minimal degrees of non-zero monomials in $g$ respectively; similarly $N$ and $n$ are the maximal and minimal degrees of non-zero monomials in $h$ respectively. Then the degree of every monomial in the product $f = gh$ is between $m+n$ and $M+N$. Moreover, the sum of all degree $M + N$ monomials in $f$ is given by $g_M h_N$, which is non-zero since both $g_M$ and $h_N$ are non-zero. Similarly, the sum of all degree $m + n$ monomials in $f$ is given by $g_m h_n$, which is non-zero since both $g_m$ and $h_n$ are non-zero. If $f$ is homogeneous, we must have $M + N = m + n$, which is only possible when $M = m$ and $N = n$. Therefore both $g$ and $h$ are homogeneous.

(2) Assume $I$ is a homogeneous ideal. Since $\Bbbk[z_0, \cdots, z_n]$ is a Noetherian ring, $I$ is finitely generated. So we can write $I = (f_1, \cdots, f_m)$ for some $f_1, \cdots, f_m \in I$ which are not necessarily homogeneous polynomials. However, each $f_i$ has a homogeneous decomposition, say, $f_i = f_{i,0} + f_{i,1} + \cdots + f_{i,d_i}$ where $d_i$ is the degree of $f_i$. We claim that $I$ is generated by all the $f_{i,j}$'s; that is,

$$I = (f_{1,0}, \cdots, f_{1,d_1}, f_{2,0}, \cdots, f_{2,d_2}, \cdots\cdots, f_{m,0}, \cdots f_{m,d_m}).$$

On one hand, since $I$ is a homogeneous ideal, each $f_{i,j} \in I$, which proves "$\supseteq$". On the other hand, we notice that every element $h \in I$ can be written as $h = f_1 g_1 + \cdots + f_m g_m$ for some $g_1, \cdots, g_m \in \Bbbk[z_0, \cdots, z_n]$, which can be expanded as $h = f_{1,0} g_1 + \cdots + f_{1,d_1} g_1 + \cdots\cdots + f_{m,0} g_m + \cdots + f_{m,d_m} g_m$, which proves "$\subseteq$". The claim shows that $I$ can be generated by finitely many homogeneous polynomials.

Conversely, assume $I = (p_1, \cdots, p_l)$ for finitely many homogeneous polynomials $p_1, \cdots, p_l \in \Bbbk[z_0, \cdots, z_n]$, with $\deg p_i = e_i$. Given any polynomial $q \in I$, assume the homogeneous decomposition of $q$ is $q = q_0 + \cdots + q_k$, where $k$ is the degree of $q$. We need to show that every $q_j \in I$. Since $q \in I$, we can write $q = p_1 r_1 + \cdots + p_l r_l$ for some $r_1, \cdots, r_l \in \Bbbk[z_0, \cdots, z_n]$. For each $j$ with $0 \leqslant j \leqslant k$, by comparing the degree $j$ terms we get $q_j = p_1 r_{1,j-e_1} + \cdots + p_l r_{l,j-e_l}$, where each $r_{i,j-e_i}$ is the sum of all degree $j - e_i$ monomials in $r_i$. Since $I = (p_1, \cdots, p_l)$, we conclude that $q_j \in I$ for every $j$, which implies $I$ is a homogeneous ideal.

(3) Given any point $p \in \mathbb{V}(I)$, we have $g(p) = 0$ for every homogeneous polynomial $g \in I$. In particular, $f_i(p) = 0$ for every $i$. Therefore $p \in \mathbb{V}(S)$. This proves $\mathbb{V}(I) \subseteq \mathbb{V}(S)$.

On the other hand, given any point $q \in \mathbb{V}(S)$, we have $f_i(q) = 0$ for every $i$. For any homogeneous polynomial $g \in I$, we can write $g = f_1 g_1 + \cdots + f_m g_m$ for some $g_1, \cdots, g_m \in \Bbbk[z_0, \cdots, z_n]$. Then $g(q) = f_1(q)g_1(q) + \cdots + f_m(q)g_m(q) = 0$. (Rigorously speaking, one should argue that each $g_i$ can be chosen to be a homogeneous polynomial of degree equal to $\deg g - \deg f_i$, which can be achieved by replacing each $g_i$ with its homogeneous part of degree equal to $\deg g - \deg f_i$.) This proves that $\mathbb{V}(S) \subseteq \mathbb{V}(I)$.

**Solution 4.3.** *Projective spaces are better than affine spaces!*

(1) Let the two points be $p = [p_0 : p_1 : p_2]$ and $q = [q_0 : q_1 : q_2]$. A line $\mathbb{V}(a_0z_0 + a_1z_1 + a_2z_2)$ passes through these two points if and only if the following system of linear equations in $a_0, a_1, a_2$ hold

$$\begin{aligned} p_0a_0 + p_1a_1 + p_2a_2 &= 0, \\ q_0a_0 + q_1a_1 + q_2a_2 &= 0. \end{aligned}$$

Since $p$ and $q$ are distinct points in $\mathbb{P}^2$, the two rows in the coefficient matrix

$$\begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \end{pmatrix}$$

are linearly independent, hence the matrix has rank 2. By the theorem of rank-nullity, the solution space to the system has dimension 1. Let $\mathbf{v} = (a_0, a_1, a_2)$ be a non-zero solution, then every solution can be written as $\lambda\mathbf{v}$ for some $\lambda \in \Bbbk$. The solution $\mathbf{v}$ defines a line $\mathbb{V}(a_0z_0 + a_1z_1 + a_2z_2)$ through the points $p$ and $q$. It remains to show the uniqueness. When $\lambda = 0$, we have $\lambda\mathbf{v} = (0, 0, 0)$ which does not define a line. For every $\lambda \in \Bbbk\backslash\{0\}$, the line $\mathbb{V}(\lambda a_0z_0 + \lambda a_1z_1 + \lambda a_2z_2)$ is the same as $\mathbb{V}(a_0z_0 + a_1z_1 + a_2z_2)$. Therefore the line through $p$ and $q$ is unique.

(2) Let the two lines by $\mathbb{V}(a_0z_0 + a_1z_1 + a_2z_2)$ and $\mathbb{V}(b_0z_0 + b_1z_1 + b_2z_2)$. A point $[z_0 : z_1 : z_2]$ lies on both lines if and only if it is a solution of the following system of linear equations in $z_0, z_1, z_2$

$$\begin{aligned} a_0z_0 + a_1z_1 + a_2z_2 &= 0, \\ b_0z_0 + b_1z_1 + b_2z_2 &= 0. \end{aligned}$$

Since the two lines are distinct, the two rows in the coefficient matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix}$$

are linearly independent, hence the matrix has rank 2. By the theorem of rank-nullity, the solution space to the system has dimension 1. Let $\mathbf{w} = (z_0, z_1, z_2)$ be a non-zero solution, then every solution can be written as $\lambda\mathbf{w}$ for some $\lambda \in \Bbbk$. The solution $\mathbf{w}$ defines a point $[z_0 : z_1 : z_2]$ of intersection. It remains to show the uniqueness. When $\lambda = 0$, we have $\lambda\mathbf{w} = (0, 0, 0)$ which does not define a point in $\mathbb{P}^2$. For every $\lambda \in \Bbbk\backslash\{0\}$, the point $[\lambda z_0 : \lambda z_1 : \lambda z_2]$ is the same as the point $[z_0 : z_1 : z_2]$. Therefore the two lines meet at a unique point in $\mathbb{P}^2$.

**Solution 4.4.** *Example of projective algebraic sets.*

(1) The empty set $\varnothing = \mathbb{V}(1)$ and the entire $\mathbb{P}^1 = \mathbb{V}(0)$. For any non-empty finite subset of $\mathbb{P}^1$, say $\{[u_1 : v_1], [u_2 : v_2], \cdots, [u_k : v_k]\}$, it can be written as $\mathbb{V}(f)$ for a homogeneous polynomial $f = (v_1z_0 - u_1z_1)(v_2z_0 - u_2z_1)\cdots(v_kz_0 - u_kz_1) \in \Bbbk[z_0, z_1]$. Therefore every set stated in the question is a projective algebraic set in $\mathbb{P}^1$.

(2) Let $f \in \Bbbk[z_0, z_1]$ be a homogeneous polynomial of degree $d$. Assume $z_0^e$ be the highest power of $z_0$ dividing $f$ for some $e \leqslant d$. Then we can write

$$\begin{aligned} f &= c_0 z_0^d + c_1 z_0^{d-1} z_1 + \cdots + c_{d-e} z_0^e z_1^{d-e} \\ &= z_0^d \cdot \left( c_0 + c_1 \frac{z_1}{z_0} + \cdots + c_{d-e} \frac{z_1^{d-e}}{z_0^{d-e}} \right). \end{aligned}$$

We consider the polynomial $g(x) = c_0 + c_1 x + \cdots + c_{d-e} x^{d-e}$. If $g$ is constant, then $f = c_0 z_0^d$ is a product of $d$ homogeneous polynomials of degree 1. If $g$ is not a constant, then it can be factored into a product of polynomials of degree 1 as $g(x) = (a_1 + b_1 x) \cdots (a_{d-e} + b_{d-e} x)$. Then we have

$$\begin{aligned} f &= z_0^d \cdot \left( a_1 + b_1 \cdot \frac{z_1}{z_0} \right) \cdots \left( a_{d-e} + b_{d-e} \cdot \frac{z_1}{z_0} \right) \\ &= z_0^e \cdot (a_1 z_0 + b_1 z_1) \cdots (a_{d-e} z_0 + b_{d-e} z_1) \end{aligned}$$

which is also a product of $d$ homogeneous polynomials of degree 1.

(3) Let $X \subseteq \mathbb{P}^1$ be a projective algebraic set. By Corollary 4.18, we assume $X = \mathbb{V}(S)$ for a finite set $S$ of homogeneous polynomials in $\Bbbk[z_0, z_1]$. If $S$ does not have any non-zero polynomial then $X = \mathbb{P}^1$. Otherwise, assume $f \in S$ is a non-zero homogeneous polynomial of degree $d$. By part (2) we can write $f = (a_1 z_0 + b_1 z_1) \cdots (a_d z_0 + b_d z_1)$ (each factor $z_0$ can be written as $1 \cdot z_0 + 0 \cdot z_1$). For every $p = [u : v] \in X$, we have $f(p) = 0$, hence a certain factor of $f$ vanishes at $p$; more precisely, $a_i u + b_i v = 0$ for some $i$. Therefore $p = [b_i : -a_i]$. There are at most $d$ points of this kind, hence $X$ contains only finitely many points.

## 5. Rational Maps

We have seen projective algebraic sets. Now we study $\mathbb{V} - \mathbb{I}$ correspondence for projective algebraic sets and maps between them.

### 5.1. $\mathbb{V} - \mathbb{I}$ correspondence and rational maps.

We have introduced the projective Nullstellensatz. The following notion is parallel to the same one in the affine case.

**Definition 5.1.** A projective algebraic set $X \subseteq \mathbb{P}^n$ is *irreducible* if there does not exist a decomposition of $X$ as a union of two stricly smaller projective algebraic sets. An irreducible projective algebraic set is also called an *projective variety*. A projective algebraic set $X \subseteq \mathbb{P}^n$ is *reducible* if it is not irreducible.

Not very surprisingly, we also have the projective version of $\mathbb{V} - \mathbb{I}$ correspondences. Each row in the following diagram is a bijection:

$$\begin{tikzcd}
\left\{ \begin{array}{c} \text{homogeneous radical ideals} \\ I \subseteq \Bbbk[z_0, z_1, \cdots, z_n] \\ \text{with } I \not\supseteq (z_0, z_1, \cdots, z_n) \end{array} \right\} \arrow[r, shift left, "\mathbb{V}"] & \left\{ \begin{array}{c} \text{non-empty projective} \\ \text{algebraic sets } X \subseteq \mathbb{P}^n \end{array} \right\} \arrow[l, shift left, "\mathbb{I}"] \\
\left\{ \begin{array}{c} \text{homogeneous prime ideals} \\ I \subseteq \Bbbk[z_0, z_1, \cdots, z_n] \\ \text{with } I \not\supseteq (z_0, z_1, \cdots, z_n) \end{array} \right\} \arrow[u, hook] \arrow[r, shift left, "\mathbb{V}"] & \left\{ \begin{array}{c} \text{non-empty} \\ \text{irreducible projective} \\ \text{algebraic sets } X \subseteq \mathbb{P}^n \end{array} \right\} \arrow[u, hook] \arrow[l, shift left, "\mathbb{I}"]
\end{tikzcd}$$

We summarise the content in the diagram in words for later reference.

**Proposition 5.2.** *Let $X$ be a non-empty projective algebraic set in $\mathbb{P}^n$ and $I$ a homogeneous radical ideal in $\Bbbk[z_0, \cdots, z_n]$ such that $(z_0, \cdots, z_n) \not\subseteq I$. Then $X = \mathbb{V}(I)$ if and only if $I = \mathbb{I}(X)$. In such a case, $X$ is irreducible if and only if $I$ is prime.*

*Proof.* Non-examinable. Interested reader can find the proof in [Section 5.3, Reid, Undergraduate Algebraic Geometry]. □

*Remark* 5.3. Comparing with the affine $\mathbb{V} - \mathbb{I}$ correspondence, the bijection between maximal ideals and points is no longer valid in the projective setting. In fact, the only homogeneous maximal ideal in $\Bbbk[z_0, z_1, \cdots, z_n]$ is the irrelevant ideal $(z_0, z_1, \cdots, z_n)$, which gives the empty set in $\mathbb{P}^n$ as we discussed above.

In practice it is usually not easy to determine whether a projective algebraic set is irreducible. It is clear that $\mathbb{P}^n$ is irreducible since $\mathbb{I}(\mathbb{P}^n) = (0)$ is a prime ideal. In case of hypersurfaces, the following result usually helps.

**Lemma 5.4.** *Let $I = (f) \subseteq \Bbbk[z_0, z_1, \cdots, z_n]$. Then $I$ is a prime ideal if and only if $f$ is an irreducible polynomial; $I$ is a radical ideal if and only if $f$ has no repeated irreducible factors.*

*Proof.* It was proved in Exercise 2.2. □

Now we turn to maps between projective algebraic sets.

**Definition 5.5.** For projective algebraic sets $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$, a *rational map* $\varphi : X \dashrightarrow Y$ is an equivalence class of expressions $[f_0 : \cdots : f_m]$ satisfying

(1) $f_0, \cdots, f_m \in \Bbbk[z_0, \cdots, z_n]$ are homogeneous of the same degree;

(2) $[f_0(p) : \cdots : f_m(p)] \neq [0 : \cdots : 0]$ for some point $p \in X$;

(3) For each point $p \in X$, if $[f_0(p) : \cdots : f_m(p)]$ is defined, then it is a point in $Y$.

Two such expressions $[f_0 : \cdots : f_m]$ and $[g_0 : \cdots : g_m]$ are equivalent if $[f_0(p) : \cdots : f_m(p)] = [g_0(p) : \cdots : g_m(p)]$ for every $p \in X$ at which both are defined.

**Definition 5.6.** Let $\varphi : X \dashrightarrow Y$ be a rational map between projective algebraic sets. We say $\varphi$ is *regular* at $p \in X$ if $[f_0(p) : \cdots : f_m(p)]$ is well-defined for some expression $[f_0 : \cdots : f_m]$ representing $\varphi$.

**Definition 5.7.** For projective algebraic sets $X$ and $Y$, a *morphism* $\varphi : X \longrightarrow Y$ is a rational map which is regular at every point in $X$.

*Remark* 5.8. The condition (1) in Definition 5.5 guarantees that the image is independent of the choice of the homogeneous coordinates of $p$. More precisely, suppose $f_i$'s are homogeneous of degree $d$, and $p = [a_0 : \cdots : a_n]$. For any $\lambda \neq 0$, we can also write $p = [\lambda a_0 : \cdots : \lambda a_n]$. Then we have by (4.3) that

$$\begin{aligned} & [f_0(\lambda a_0, \cdots, \lambda a_n) : \cdots : f_m(\lambda a_0, \cdots, \lambda a_n)] \\ = & [\lambda^d f_0(a_0, \cdots, a_n) : \cdots : \lambda^d f_m(a_0, \cdots, a_n)] \\ = & [f_0(a_0, \cdots, a_n) : \cdots : f_m(a_0, \cdots, a_n)]. \end{aligned}$$

The condition (2) in Definition 5.5 guarantees that the expression $[f_0 : \cdots : f_m]$ is defined on a non-empty subset of $X$.

*Remark* 5.9. We can view a rational function $\varphi : X \dashrightarrow Y$ as a piecewise and partially defined function. Each expression $[f_0 : \cdots : f_m]$ representing $\varphi$ is defined on a subset of $X$. Two such expressions that agree on the locus where both are defined can be glued together to represent the same function $\varphi$. However, there could still be some points in $X$ where none of the expressions is defined.

**Example 5.10.** We check the following is a morphism

$$\varphi : \quad \mathbb{P}^1 \longrightarrow \mathbb{P}^2; \quad [u : v] \longmapsto [u^2 : uv : v^2].$$

All components of $\varphi$ are homogeneous polynomials of degree 2. For each point $p = [u : v] \in \mathbb{P}^1$, either $u \neq 0$ or $v \neq 0$, hence either $u^2 \neq 0$ or $v^2 \neq 0$. Therefore $\varphi$ is regular on the entire $\mathbb{P}^1$. Since the target is $\mathbb{P}^2$, $\varphi(p) \in \mathbb{P}^2$ is automatic for every $p \in \mathbb{P}^1$.

**Example 5.11.** Consider the projective algebraic set $C = \mathbb{V}(z_0z_2 - z_1^2) \subseteq \mathbb{P}^2$. We check the following is a morphism

$$\varphi : \quad \mathbb{P}^1 \longrightarrow C; \quad [u : v] \longmapsto [u^2 : uv : v^2].$$

We need to check everything that we checked in Example 5.10. In addition we need to check $\varphi(p) \in C$ for every $p \in \mathbb{P}^1$. To see that we need to show $[u^2 : uv : v^2]$ satisfies the defining equation of $C$, which is clear since $(u^2)(v^2) - (uv)^2 = 0$.

**Example 5.12.** For the same $C$ as in Example 5.11, we check the following is a morphism

$$\psi : \quad C \longrightarrow \mathbb{P}^1; \quad [z_0 : z_1 : z_2] \longmapsto \begin{cases} [z_0 : z_1] & \text{if } z_0 \neq 0; \\ [z_1 : z_2] & \text{if } z_2 \neq 0. \end{cases}$$

As we can see $\psi$ is defined by two expressions, whose components are all homogeneous polynomials of degree 1. They are both defined on a non-empty subset of $C$; e.g. both are defined at $[1 : 1 : 1] \in C$. It is clear that the image is always in $\mathbb{P}^1$. For any point $[z_0 : z_1 : z_2] \in C$ with $z_0 \neq 0$ and $z_2 \neq 0$, we have $z_1^2 = z_0z_2$ hence $z_1 \neq 0$. Set $\lambda = \frac{z_1}{z_0} = \frac{z_2}{z_1} \neq 0$, then $[z_0 : z_1] = [\lambda z_0 : \lambda z_1] = [z_1 : z_2]$. Therefore the two expressions agree on the locus where they are both defined. To show $\psi$ is regular everywhere on $C$, we observe that for any point $p = [z_0 : z_1 : z_2] \in C$, $z_0$ and $z_2$ cannot be both zero, since otherwise $z_1^2 = z_0z_2 = 0$ and $p$ is not a valid point. This concludes that $\psi$ is a morphism.

**Example 5.13** (Cremona transformation)**.** We check the following is a rational map

$$\varphi : \quad \mathbb{P}^2 \dashrightarrow \mathbb{P}^2; \quad [x : y : z] \longmapsto [yz : zx : xy].$$

All components of $\varphi$ are homogeneous of degree 2. For every point $p \in \mathbb{P}^2$ with at least two non-zero coordinates, $\varphi(p)$ is a well-defined point in $\mathbb{P}^2$. Hence $\varphi$ is a rational map.

5.2. **Dominant rational maps and birational maps.** We have seen rational maps between projective algebraic sets. We now consider the composition of two rational maps. Suppose $f : X \dashrightarrow Y$ and $g : Y \dashrightarrow Z$ are rational maps. It is not always true that they can be composed to get $g \circ f : X \dashrightarrow Z$, because the image of $f$ could be disjoint from the locus where $g$ is defined. We will deal with this problem.

**Definition 5.14.** Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be projective varieties. A rational map $\varphi : X \dashrightarrow Y$ is *dominant* if there does not exist a projective algebraic set $W \subsetneq Y$, such that $\varphi(p) \in W$ for every $p \in X$ where $\varphi$ is defined.

**Example 5.15.** We claim the morphism $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^2$ in Example 5.10 is not dominant. To see this, we consider $W = \mathbb{V}(z_0z_2 - z_1^2) \subset \mathbb{P}^2$. We see that $W \subsetneq \mathbb{P}^2$ because $[1 : 1 : 0] \in \mathbb{P}^2 \backslash W$. But for every $p \in \mathbb{P}^1$, $\varphi(p) \in W$ because $(u^2)(v^2) - (uv)^2 = 0$.

The definition is handy for showing a rational map is not dominant. The following criterion is usually more convenient for showing a rational map is dominant.

**Lemma 5.16.** *Let $\varphi : X \dashrightarrow Y$ be a rational map between projective varieties. Suppose there exists a projective algebraic set $Z \subsetneq Y$, such that every $q \in Y \backslash Z$ can be written as $q = \varphi(p)$ for some $p \in X$. Then $\varphi$ is dominant.*

*Proof.* Suppose on the contrary that there exists some projective algebraic set $W \subsetneq Y$ such that $\varphi(p) \in W$ for every $p \in X$ at which $\varphi$ is defined. It is clear $Y \supseteq W \cup Z$. For every $q \in Y$, if $q = \varphi(p)$ for some $p \in X$, then $q \in W$; otherwise $q \in Z$. It follows that $Y \subseteq W \cup Z$. Therefore $Y = W \cup Z$ where both $W$ and $Z$ are projective algebraic sets strictly smaller than $Y$. This contradicts the irreducibility of $Y$. $\square$

*Remark* 5.17. In explicit examples there are usually many possible choices for $W$ in Definition 5.14 and $Z$ in Lemma 5.16. You can choose the one that you find easy to use.

**Example 5.18.** We consider the morphism $\varphi : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ in Example 5.13. We know $\mathbb{P}^2$ is a projective variety. We claim $\varphi$ is dominant. If not, then we can find a projective algebraic set $W \subsetneq \mathbb{P}^2$, such that $\varphi(p) \in W$ for every $p \in \mathbb{P}^2$ at which $\varphi$ is defined.

We observe that the projective algebraic set $Z = \mathbb{V}(xyz)$ consists of all points in $\mathbb{P}^2$ with at least one zero coordinate, so $Z \subsetneq \mathbb{P}^2$. For every point $[a : b : c] \in \mathbb{P}^2 \backslash Z$, all coordinates are non-zero. It is in the image of $\varphi$ since

$$\varphi([bc : ca : ab]) = [a^2bc : ab^2c : abc^2] = [a : b : c].$$

It follows from Lemma 5.16 that $\varphi$ is dominant.

Now we answer the question asked at the beginning and give a sufficient condition for the existence of compositions.

**Lemma 5.19.** *Let $\varphi : X \dashrightarrow Y$ and $\psi : Y \dashrightarrow Z$ be rational maps between projective varieties. If $\varphi$ is dominant, then $\psi \circ \varphi : X \dashrightarrow Z$ is a rational map.*

*Proof.* Non-examinable. Interested reader can find more details in [Section 4.10, Reid, Undergraduate Algebraic Geometry]. □

The following is another special class of rational maps.

**Definition 5.20.** Let $\varphi : X \dashrightarrow Y$ be a rational map between projective varieties. It is said to be a *birational map* if there exists another rational map $\psi : Y \dashrightarrow X$, such that $\psi \circ \varphi$ is a well-defined rational map equivalent to the identity map on $X$, and $\varphi \circ \psi$ is a well-defined rational map equivalent to the identity map on $Y$. We say a birational map $\varphi$ is an isomorphism if both $\varphi$ and $\psi$ can be chosen to be morphisms.

*Remark* 5.21. More precisely, the condition that $\psi \circ \varphi$ is equivalent to $\mathrm{id}_X$ means that $(\psi \circ \varphi)(p) = p$ for every point $p \in X$ at which $\psi \circ \varphi$ is defined. A similar condition holds for the other composition $\varphi \circ \psi$.

**Example 5.22.** We claim that the rational map $\varphi : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ discussed in Examples 5.13 and 5.18 is a birational map. Let $\psi$ be the same rational map as $\varphi$, then the composition $\psi \circ \varphi$ is given by the expression

$$(\psi \circ \varphi)([x : y : z]) = \psi([yz : zx : xy]) = [x^2yz : xy^2z : xyz^2].$$

For any point $[x : y : z]$ with all coordinates nonzero, we have $(\psi \circ \varphi)([x : y : z]) = [x^2yz : xy^2z : xyz^2] = [x : y : z]$. The same is true for $\varphi \circ \psi$. Therefore the claim holds.

**Example 5.23.** We claim that the morphism $\varphi : \mathbb{P}^1 \longrightarrow C$ in Example 5.11 is an isomorphism, with an inverse $\psi$ given by the morphism in Example 5.12. For any $[u : v] \in \mathbb{P}^1$, either $u \neq 0$ or $v \neq 0$. If $u \neq 0$, then $u^2 \neq 0$, hence

$$(\psi \circ \varphi)([u : v]) = \psi([u^2 : uv : v^2]) = [u^2 : uv] = [u : v].$$

If $v \neq 0$, then $v^2 \neq 0$. We can similarly have

$$(\psi \circ \varphi)([u : v]) = \psi([u^2 : uv : v^2]) = [uv : v^2] = [u : v].$$

For the other composition, take any point $[z_0 : z_1 : z_2] \in C$. We showed in Example 5.12 that either $z_0 \neq 0$ or $z_2 \neq 0$. If $z_0 \neq 0$, then

$$(\varphi \circ \psi)([z_0 : z_1 : z_2]) = \varphi([z_0 : z_1]) = [z_0^2 : z_0z_1 : z_1^2] = [z_0^2 : z_0z_1 : z_0z_2] = [z_0 : z_1 : z_2].$$

If $z_0 \neq 0$, we can similarly have

$$(\varphi \circ \psi)([z_0 : z_1 : z_2]) = \varphi([z_1 : z_2]) = [z_1^2 : z_1z_2 : z_2^2] = [z_0z_2 : z_1z_2 : z_2^2] = [z_0 : z_1 : z_2].$$

Therefore both compositions are equivalent to identity maps hence $\varphi$ is a rational map. Since $\varphi$ and $\psi$ are both morphisms, $\varphi$ is in fact an isomorphism.

**Definition 5.24.** Two projective varieties $X$ and $Y$ are said to be *birational* if there exists a birational map $\varphi : X \dashrightarrow Y$. A projective variety $X$ is said to be *rational* if it is birational to $\mathbb{P}^n$ for some non-negative integer $n$.

**Definition 5.25.** Two projective varieties $X$ and $Y$ are said to be *isomorphic* if there exists an isomorphism $\varphi : X \longrightarrow Y$.

*Remark* 5.26. In fact, being birational is an equivalence relation among projective varieties. This is an extremely important and profound notion in algebraic geometry. Determining which projective varieties are in the same birational equivalence class, and finding a good representative in each class, are the fundamental questions in a major branch of algebraic geometry, called *birational geometry*. As these questions are in general very difficult, a complete answer is far from being achieved. We will see some examples later.

## Exercise Sheet 5

*This sheet will be discussed in the exercise class on 6 November. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 5.1.** *Example: linear embedding and linear projection.*

(1) Show that $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^3; [z_0 : z_1] \longmapsto [z_0 : z_1 : 0 : 0]$ is a morphism. Is it dominant? (*Remark:* in general, for any $n \leqslant m$, there is a *linear embedding* from $\mathbb{P}^n$ to $\mathbb{P}^m$ by identifying homogeneous coordinates in $\mathbb{P}^n$ with a subset of homogeneous coordinates in $\mathbb{P}^m$ and setting the remaining coordinates 0.)

(2) Show that $\psi : \mathbb{P}^3 \dashrightarrow \mathbb{P}^1; [z_0 : z_1 : z_2 : z_3] \longmapsto [z_2 : z_3]$ is a rational map. Is it dominant? (*Remark:* in general, for any $m \geqslant n$, there is a *linear projection* from $\mathbb{P}^m$ to $\mathbb{P}^n$ by choosing a subset of the homogeneous coordinates in $\mathbb{P}^m$.)

(3) Is the composition $\psi \circ \varphi$ a well-defined rational map? Explain your reason.

**Exercise 5.2.** *Example: the cooling tower.* Consider $Y = \mathbb{V}(y_0y_3 - y_1y_2) \subseteq \mathbb{P}^3$.

(1) Show that $y_0y_3 - y_1y_2$ is irreducible. Conclude that $Y$ is a projective variety.

(2) Show that $\varphi : \mathbb{P}^2 \dashrightarrow Y; [x_0 : x_1 : x_2] \longmapsto [x_0^2 : x_0x_1 : x_0x_2 : x_1x_2]$ is a rational map. Show that $\varphi$ is dominant. (*Hint:* first show that each point $q = [y_0 : y_1 : y_2 : y_3] \in Y$ with $y_0 \neq 0$ is in the image of $\varphi$, then use Lemma 5.16.)

(3) Show that $\psi : Y \dashrightarrow \mathbb{P}^2; [y_0 : y_1 : y_2 : y_3] \longmapsto [y_0 : y_1 : y_2]$ is a rational map. Show that $\psi$ is dominant. (*Hint:* first show that each point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$ with $x_0 \neq 0$ is in the image of $\psi$, then use Lemma 5.16.)

(4) Show that $\varphi$ and $\psi$ are birational maps. Conclude that $Y$ is rational.

**Exercise 5.3.** *Example: the projective twisted cubic.* Consider the projective variety $Y = \mathbb{V}(y_0y_2 - y_1^2, y_1y_3 - y_2^2, y_0y_3 - y_1y_2) \subseteq \mathbb{P}^3$.

(1) Show that $\varphi : \mathbb{P}^1 \longrightarrow Y; [u : v] \longmapsto [u^3 : u^2v : uv^2 : v^3]$ is a morphism.

(2) Show that $\varphi$ is an isomophism by finding the inverse morphism $\psi : Y \longrightarrow \mathbb{P}^1$ and computing their compositions. Conclude that $Y$ is isomorphic to $\mathbb{P}^1$.

**Exercise 5.4.** *A famous example: blow-up at a point.* Consider the projective variety $Y = \mathbb{V}(y_0y_2 - y_1^2,\ y_0y_4 - y_1y_3,\ y_1y_4 - y_2y_3) \subseteq \mathbb{P}^4$.

(1) Show $\varphi : \mathbb{P}^2 \dashrightarrow Y; [x_0 : x_1 : x_2] \longmapsto [x_0^2 : x_0x_1 : x_1^2 : x_0x_2 : x_1x_2]$ is a rational map.

(2) Show that $\varphi$ is a birational map by finding the inverse rational map $\psi : Y \dashrightarrow \mathbb{P}^2$ and computing their compositions. Conclude that $Y$ is rational.

(3) Show that $\psi$ can be chosen to be a morphism. Show that $\psi$ is surjective on points. Find all points $q \in Y$, such that $\psi(q) = [0 : 0 : 1]$.

## Solutions to Exercise Sheet 5

**Solution 5.1.** *Example: linear embedding and linear projection.*

(1) All components are given by homogeneous polynomials of degree 1. For every point $[z_0 : z_1] \in \mathbb{P}^1$, we have either $z_0 \neq 0$ or $z_1 \neq 0$, hence $\varphi([z_0 : z_1]) = [z_0 : z_1 : 0 : 0]$ has at least one non-zero coordinate, hence is clearly a point in $\mathbb{P}^3$. Therefore $\varphi$ is a morphism. It is not dominant, because for the projective algebraic set $W = \mathbb{V}(z_2, z_3) \subseteq \mathbb{P}^3$, we have $\varphi([z_0 : z_1]) \in W$ for every point $[z_0 : z_1] \in \mathbb{P}^1$.

(2) All components are given by homogeneous polynomials of degree 1. The map is not defined at every point in $\mathbb{P}^3$, but for every point $[z_0 : z_1 : z_2 : z_3] \in \mathbb{P}^3$ with $z_2 \neq 0$ or $z_3 \neq 0$, its image $\psi([z_0 : z_1 : z_2 : z_3]) = [z_2 : z_3]$ has at least one non-zero coordinate, and is clearly a point in $\mathbb{P}^1$. Therefore $\psi$ is a rational map. To see it is dominant, we first claim that $\psi$ is surjective. In fact, for every point $[z_2 : z_3] \in \mathbb{P}^1$, we have that $[z_2 : z_3] = \psi([z_0 : z_1 : z_2 : z_3])$ for any choice of $z_0, z_1 \in \Bbbk$. Since $\psi$ is surjective, we can apply Lemma 5.16 and choose $Z = \varnothing$ to conclude that $\psi$ is dominant.

(3) The composition is not well-defined because for every $[z_0 : z_1] \in \mathbb{P}^1$, we have $(\psi \circ \varphi)([z_0 : z_1]) = \psi([z_0 : z_1 : 0 : 0]) = [0 : 0]$ which is not a point in $\mathbb{P}^1$. This shows that $\psi \circ \varphi$ is nowhere well-defined, which violates the second condition in the definition of a rational map.

**Solution 5.2.** *Example: the cooling tower.*

(1) Assume we can write $y_0y_3 - y_1y_2 = fg$ for some $f, g \in \Bbbk[y_0, y_1, y_2, y_3]$. Since the polynomial $y_0y_3 - y_1y_2$ has degree 1 in $y_0$, the degrees of $f$ and $g$ in $y_0$ should be 0 and 1 respectively. Without loss of generality we assume $f = y_0f_1 + f_0$ and $g = g_0$, where $f_1, f_0, g_0 \in \Bbbk[y_1, y_2, y_3]$. By comparing the coefficients of terms of degree 1 and 0 in $y_0$, we get $f_1g_0 = y_3$ and $f_0g_0 = -y_1y_2$. Therefore $g_0$ is a common factor of $y_3$ and $-y_1y_2$, which has to be a constant. This implies $g$ is a constant, hence $y_0y_3 - y_1y_2$ is irreducible. Since it is a homogeneous polynomial, $\mathbb{V}(y_0y_3 - y_1y_2)$ is a projective algebraic set. By Lemma 5.4, the principal ideal $I = (y_0y_3 - y_1y_2)$ in $\Bbbk[y_0, y_1, y_2, y_3]$ is a prime ideal. Hence by Lemma 4.17, $\mathbb{V}(y_0y_3 - y_1y_2) = \mathbb{V}(I)$, which is a projective variety by Proposition 5.2.

(2) It is clear that all components of $\varphi$ are given by homogeneous polynomials of degree 2. For any point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$, if $x_0$ is non-zero, or $x_1$ and $x_2$ are simultaneously non-zero, the image $\varphi(p)$ has at least one non-zero component. Hence $\varphi$ is defined on a non-empty subset of $\mathbb{P}^2$. To show its image is always in $Y$, we find that $y_0y_3 - y_1y_2 = (x_0^2)(x_1x_2) - (x_0x_1)(x_0x_2) = 0$. Therefore $\varphi$ is a rational map.

To show that $\varphi$ is dominant, we observe that every point $q = [y_0 : y_1 : y_2 : y_3] \in Y$ with $y_0 \neq 0$ is the image of the point $p = [y_0 : y_1 : y_2]$. Indeed, $\varphi(p) = [y_0^2 : y_0y_1 : y_0y_2 : y_1y_2] = [y_0^2 : y_0y_1 : y_0y_2 : y_0y_3] = [y_0 : y_1 : y_2 : y_3] = q$. Set $Z = \mathbb{V}(y_0y_3 - y_1y_2, y_0)$, then $Z \subseteq Y$, and is strictly smaller than $Y$ (e.g. $[1 : 0 : 0 : 0] \in Y \backslash Z$). And every point $q \in Y \backslash Z$ is in the image of $\varphi$. By Lemma 5.16, $\varphi$ is dominant.

(3) We first realise that every component of $\psi$ is a homogeneous polynomial of degree 1. $\psi$ is well-defined at every point $q = [y_0 : y_1 : y_2 : y_3] \in Y$ such that $y_0, y_1, y_2$ are not simultaneously zero (e.g. $[1 : 0 : 0 : 0]$ is such a point). Hence it is defined on a non-empty subset of $Y$. The image $\psi(q)$ is always a point in $\mathbb{P}^2$ if it is defined. Therefore $\psi$ is a rational map.

To show $\psi$ is dominant, we first observe that each point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$ with $x_0 \neq 0$ is the image of the point $q = [x_0 : x_1 : x_2 : \frac{x_1x_2}{x_0}]$. Indeed, $q$ is a well-defined point since $x_0 \neq 0$, and $q \in Y$ since it satisfies the defining equation of $Y$. The expression that defines $\psi$ gives $\psi(q) = p$. If we set $Z = \mathbb{V}(x_0)$, then $Z \subsetneq \mathbb{P}^2$. Since every point in $\mathbb{P}^2 \backslash Z$ is in the image of $\psi$, we conclude that $\psi$ is dominant by Lemma 5.16.

(4) We show that $\varphi$ and $\psi$ are mutually inverse rational maps. For every point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$ at which $\psi \circ \varphi$ is defined, we have $(\psi \circ \varphi)(p) = \psi([x_0^2 : x_0x_1 : x_0x_2 : x_1x_2]) = [x_0^2 : x_0x_1 : x_0x_2] = [x_0 : x_1 : x_2] = p$. For every point $q = [y_0 : y_1 : y_2 : y_3] \in Y$ at which $\varphi \circ \psi$ is defined, we have $(\varphi \circ \psi)(q) = \varphi([y_0 : y_1 : y_2]) = [y_0^2 : y_0y_1 : y_0y_2 : y_1y_2] = [y_0^2 : y_0y_1 : y_0y_2 : y_0y_3] = [y_0 : y_1 : y_2 : y_3] = q$. Therefore $\varphi$ and $\psi$ are mutually inverse birational maps. It follows that $Y$ is birational to $\mathbb{P}^2$, hence $Y$ is rational.

**Solution 5.3.** *Example: the projective twisted cubic.*

(1) All components of $\varphi$ are homogeneous of the same degree 3. For every point $[u : v] \in \mathbb{P}^1$, we have either $u \neq 0$ or $v \neq 0$, therefore either $u^3 \neq 0$ or $v^3 \neq 0$, hence $\varphi([u : v]) = [u^3 : u^2v : uv^2 : v^3]$ is always a well-defined point. To show that $\varphi([u : v]) \in Y$, we need to check all defining polynomial of $Y$ are satisfied. Indeed, we have

$$\begin{aligned} y_0y_2 - y_1^2 &= (u^3)(uv^2) - (u^2v)^2 = 0; \\ y_1y_3 - y_2^2 &= (u^2v)(v^3) - (uv^2)^2 = 0; \\ y_0y_3 - y_1y_2 &= (u^3)(v^3) - (u^2v)(uv^2) = 0. \end{aligned}$$

We conclude that $\varphi$ is a morphism.

(2) We define $\psi : Y \longrightarrow \mathbb{P}^1$ in the following way: for every point $[y_0 : y_1 : y_2 : y_3] \in Y$, let $\psi([y_0 : y_1 : y_2 : y_3]) = [y_0 : y_1]$ or $[y_2 : y_3]$. We first check that $\psi$ is a morphism.

Both expressions used to define $\psi$ are given by homogeneous polynomials of degree 1. For any point $[y_0 : y_1 : y_2 : y_3]$, if either $y_0$ or $y_1$ is non-zero (e.g. $[1 : 0 : 0 : 0]$), then the first expression applies; if either $y_2$ or $y_3$ is non-zero (e.g. $[0 : 0 : 0 : 1]$), then the second expression applies. This shows that both expressions are defined on non-empty subsets of $Y$. Moreover, for any point $[y_0 : y_1 : y_2 : y_3]$, at least one of its coordinates is non-zero, hence at least one of the expressions can be used to compute its image under $\psi$, hence $\psi$ is defined at every point in $Y$. The image $\psi(q)$ for any point $q \in Y$ is clearly a point in $\mathbb{P}^1$.

To show $\psi$ is a morphism, it remains to show that, if the two expressions are both defined at a certain point $q = [y_0 : y_1 : y_2 : y_3] \in Y$, then they give the same image. For such a point $q$, we claim $y_0 \neq 0$; otherwise $y_1^2 = y_0y_2 = 0$, which implies the first expression is invalid. Similarly, we claim $y_3 \neq 0$; otherwise $y_2^2 = y_1y_3 = 0$, which implies the second expression is invalid. Therefore $y_1y_2 = y_0y_3 \neq 0$, which implies $y_1 \neq 0$ and $y_2 \neq 0$. So all coordinates of $q$ are non-zero. For such a point $q$, we have $[y_0 : y_1] = [y_0y_3 : y_1y_3] = [y_1y_2 : y_1y_3] = [y_2 : y_3]$, hence both expressions give the same image of $q$.

Finally we check that $\varphi$ and $\psi$ are mutually inverse to each other. Given any point $p = [u : v] \in \mathbb{P}^1$, we have

$$(\psi \circ \varphi)(p) = \psi([u^3 : u^2v : uv^2 : v^3]) = \begin{cases} [u^3 : u^2v] = [u : v]; \\ [uv^2 : v^3] = [u : v]. \end{cases}$$

For any point $q = [y_0 : y_1 : y_2 : y_3] \in Y$, we notice that $y_0y_1^2 = y_0 \cdot y_0y_2 = y_0^2y_2$ and $y_1^3 = y_1 \cdot y_0y_2 = y_0 \cdot y_1y_2 = y_0 \cdot y_0y_3 = y_0^2y_3$. Therefore if we use the first expression that defines $\psi$, we have

$$\begin{aligned} (\varphi \circ \psi)(q) &= \varphi([y_0 : y_1]) \\ &= [y_0^3 : y_0^2y_1 : y_0y_1^2 : y_1^3] \\ &= [y_0^3 : y_0^2y_1 : y_0^2y_2 : y_0^2y_3] \\ &= [y_0 : y_1 : y_2 : y_3]. \end{aligned}$$

Similarly, noticing that $y_2^2y_3 = y_1y_3 \cdot y_3 = y_1y_3^2$ and $y_2^3 = y_2 \cdot y_1y_3 = y_1y_2 \cdot y_3 = y_0y_3 \cdot y_3 = y_0y_3^2$, we can use the second expression that defines $\psi$ to compute

$$\begin{aligned}(\varphi \circ \psi)(q) &= \varphi([y_2 : y_3]) \\ &= [y_2^3 : y_2^2y_3 : y_2y_3^2 : y_3^3] \\ &= [y_0y_3^2 : y_1y_3^2 : y_2y_3^2 : y_3^3] \\ &= [y_0 : y_1 : y_2 : y_3].\end{aligned}$$

The above calculation shows that $\varphi$ and $\psi$ are mutually inverse to each other, hence they are birational. Since they are both morphisms, they are isomorphisms. We conclude that $Y$ is isomorphic to $\mathbb{P}^1$.

**Solution 5.4.** *A famous example: blow-up at a point.*

(1) All components of $\varphi$ are homogeneous of degree 2. Given a point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$, if $x_0 \neq 0$ or $x_1 \neq 0$, then $x_0^2 \neq 0$ or $x_1^2 \neq 0$, hence at least one component of $\varphi(p)$ is non-zero, which implies $\varphi(p)$ is defined. When $\varphi(p)$ is defined, we need to check it is a point in $Y$. This can be verified by

$$\begin{aligned}y_0y_2 - y_1^2 &= (x_0^2)(x_1^2) - (x_0x_1)^2 = 0; \\ y_0y_4 - y_1y_3 &= (x_0^2)(x_1x_2) - (x_0x_1)(x_0x_2) = 0; \\ y_1y_4 - y_2y_3 &= (x_0x_1)(x_1x_2) - (x_1^2)(x_0x_2) = 0.\end{aligned}$$

This proves $\varphi$ is a rational map.

(2) We first write down the formula for $\psi$, then prove $\psi$ is a morphism, finally show that the two compositions of $\varphi$ and $\psi$ are identities.

The morphism $\psi : Y \longrightarrow \mathbb{P}^2$ is defined as follows: for every point $q = [y_0 : y_1 : y_2 : y_3 : y_4]$, let $\psi(q) = [y_0 : y_1 : y_3]$ or $[y_1 : y_2 : y_4]$. It is clear that both expressions in the definition of $\psi$ are given by homogeneous polynomials of degree 1. When $y_0$, $y_1$ and $y_3$ are not simultaneously zero (e.g. $[1 : 0 : 0 : 0 : 0]$), then the first expression applies. When $y_1$, $y_2$ and $y_4$ are not simultaneously zero (e.g. $[0 : 0 : 0 : 0 : 1]$), then the second expression applies. Hence both expressions are defined on non-empty subsets of $Y$. For every point $q \in Y$, at least one of its coordinates is non-zero, which means at least one of two expressions is well-defined at $q$. And the image of $q$ is clearly a point in $\mathbb{P}^2$, no matter which expression we use to compute the image.

We still need to show that the two expressions define the same image of $q$ when they both apply. There are a few cases to consider. *Case 1:* if $y_0$, $y_1$ and $y_3$ are all non-zero, then set $\lambda = \frac{y_1}{y_0} = \frac{y_2}{y_1} = \frac{y_4}{y_3}$. Indeed, the three fractions are equal because of the defining equations of $Y$. Then $[y_0 : y_1 : y_3] = [\lambda y_0 : \lambda y_1 : \lambda y_3] = [y_1 : y_2 : y_4]$. *Case 2:* if $y_0 = 0$, then $y_1^2 = y_0y_2 = 0$ implies $y_1 = 0$. Since we assumed the expression $[y_0 : y_1 : y_3]$ is well-defined at $q$, we must have $y_3 \neq 0$. Then $y_2y_3 = y_1y_4 = 0$ implies $y_2 = 0$. Since we assumed the expression $[y_1 : y_2 : y_4]$ is well-defined at $q$, we must have $y_4 \neq 0$. Now $[y_0 : y_1 : y_3] = [0 : 0 : y_3] = [0 : 0 : y_4] = [y_1 : y_2 : y_4]$. *Case 3:* if $y_0 \neq 0$ and $y_1 = 0$, then $y_0y_2 = y_1^2 = 0$ implies $y_2 = 0$, and $y_0y_4 = y_1y_3 = 0$ implies $y_4 = 0$, then the expression $[y_1 : y_2 : y_4]$ is not defined at $q$. Hence this case cannot happen. *Case 4:* if $y_0 \neq 0$ and $y_1 \neq 0$ and $y_3 = 0$, then $y_0y_4 = y_1y_3 = 0$ implies $y_4 = 0$. Set $\lambda = \frac{y_1}{y_0} = \frac{y_2}{y_1}$. Then $[y_0 : y_1 : y_3] = [y_0 : y_1 : 0] = [\lambda y_0 : \lambda y_1 : 0] = [y_1 : y_2 : 0] = [y_1 : y_2 : y_4]$. In summary, we always have $[y_0 : y_1 : y_3] = [y_1 : y_2 : y_4]$. This finishes the proof of the fact that $\psi$ is a morphism.

We compute the two compositions of $\varphi$ and $\psi$. Given any point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$ at which $\psi \circ \varphi$ is defined, we have

$$\begin{aligned}(\psi \circ \varphi)(p) &= \psi([x_0^2 : x_0x_1 : x_1^2 : x_0x_2 : x_1x_2]) \\ &= \begin{cases}[x_0^2 : x_0x_1 : x_0x_2] = [x_0 : x_1 : x_2]; \\ [x_0x_1 : x_1^2 : x_1x_2] = [x_0 : x_1 : x_2].\end{cases}\end{aligned}$$

Now pick any point $q = [y_0 : y_1 : y_2 : y_3 : y_4] \in Y$ at which $\varphi \circ \psi$ is defined. If we use the first expression to compute $\psi(q)$, then we have

$$\begin{aligned}(\varphi \circ \psi)(q) &= \varphi([y_0 : y_1 : y_3]) = [y_0^2 : y_0y_1 : y_1^2 : y_0y_3 : y_1y_3] \\ &= [y_0^2 : y_0y_1 : y_0y_2 : y_0y_3 : y_0y_4] = [y_0 : y_1 : y_2 : y_3 : y_4].\end{aligned}$$

If we use the second expression to compute $\psi(q)$, then we have

$$\begin{aligned}(\varphi \circ \psi)(q) &= \varphi([y_1 : y_2 : y_4]) = [y_1^2 : y_1y_2 : y_2^2 : y_1y_4 : y_2y_4] \\ &= [y_0y_2 : y_1y_2 : y_2^2 : y_2y_3 : y_2y_4] = [y_0 : y_1 : y_2 : y_3 : y_4].\end{aligned}$$

The above calculation shows that $\varphi$ and $\psi$ are mutually inverse rational maps. Hence $Y$ and $\mathbb{P}^2$ are birational to each other. It follows that $Y$ is rational.

(3) We have proved that $\psi$ is a morphism. We first find all points $q \in Y$ such that $\psi(q) = [0 : 0 : 1]$. Let $q = [y_0 : y_1 : y_2 : y_3 : y_4] \in Y$. Then depending on which expression we use to compute $\psi(q)$, there are two possibilities. If $[y_0 : y_1 : y_3] = [0 : 0 : 1]$, then $y_0 = y_1 = 0$ and $y_3 \neq 0$. From $y_2y_3 = y_1y_4 = 0$ we obtain $y_2 = 0$. Hence $q = [0 : 0 : 0 : y_3 : y_4]$ for any $y_3 \neq 0$ and $y_4 \in \Bbbk$. Similarly, if $[y_1 : y_2 : y_4] = [0 : 0 : 1]$, then$y_1 = y_2 = 0$ and $y_4 \neq 0$. From $y_0y_4 = y_1y_3 = 0$ we obtain $y_0 = 0$. Hence $q = [0 : 0 : 0 : y_3 : y_4]$ for any $y_3 \in \Bbbk$ and $y_4 \neq 0$. Combining the two cases, all points $q \in Y$ satisfying $\psi(q) = [0 : 0 : 1]$ are given by points of the form $q = [0 : 0 : 0 : y_3 : y_4]$ where $y_3$ and $y_4$ not simultaneously zero.

Finally we need to show that $\psi$ is surjective. We have seen that $[0 : 0 : 1]$ is in the image of $\psi$. For any point $p = [x_0 : x_1 : x_2] \in \mathbb{P}^2$ such that $p \neq [0 : 0 : 1]$, we claim that $p = \psi(q)$ for $q = [x_0^2 : x_0x_1 : x_1^2 : x_0x_2 : x_1x_2]$. Indeed, when $p \neq [0 : 0 : 1]$, we have either $x_0 \neq 0$ or $x_1 \neq 0$. In such a case, we have checked in part (1) that $q = [x_0^2 : x_0x_1 : x_1^2 : x_0x_2 : x_1x_2]$ is a well-defined point in $Y$. It remains to show $\psi(q) = p$. If $x_0 \neq 0$, then we can use the first expression of $\psi$ to get $\psi(q) = [x_0^2 : x_0x_1 : x_0x_2] = [x_0 : x_1 : x_2] = p$. If $x_1 \neq 0$, then we can use the second expression of $\psi$ to get $\psi(q) = [x_0x_1 : x_1^2 : x_1x_2] = [x_0 : x_1 : x_2] = p$. In summary, $p$ is always in the image of $\psi$. Hence $\psi$ is surjective.

## 6. Function Fields

We will study rational functions on projective varieties, and pullback of rational functions along dominant rational maps. Similar to the affine case, we will see that the field of rational functions determines the birational class of a projective variety.

### 6.1. Bridge between affine and projective algebraic sets.

We have seen affine and projective algebraic sets as subsets of affine and projective spaces defined by polynomial equations. They are related in a way that is similar to affine and projective spaces. Recall that $\mathbb{P}^n$ is covered by standard affine charts $U_i$ for $i = 0, 1, \cdots, n$.

**Proposition 6.1** (From projective to affine)**.** *Let $X \subseteq \mathbb{P}^n$ be a projective algebraic set, and $U_i$ a standard affine chart of $\mathbb{P}^n$. Then $X_i := X \cap U_i$ is an affine algebraic set in $U_i$.*

*Proof.* Without loss of generality, we prove the statement for $i = 0$. Assume $X = \mathbb{V}_p(f_1, \cdots, f_m)$ for some homogeneous polynomials $f_1, \cdots, f_m \in \Bbbk[z_0, \cdots, z_n]$. Then

$$\begin{aligned}p = [a_0 : \cdots : a_n] \in X \cap U_0 &\iff f_j(a_0, a_1 \cdots, a_n) = 0 \text{ for each } j \\ &\iff f_j\left(1, \frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) = 0 \text{ for each } j \\ &\iff g_j\left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) = 0 \text{ for each } j\end{aligned}$$

where $g_j = f_j(1, z_1, \cdots, z_n)$. Hence $X_i = \mathbb{V}_a(g_1, \cdots, g_m)$ is an affine algebraic set. $\square$

*Remark* 6.2. As in the proof, given a homogeneous polynomial (i.e. $f_j$), we can set one of its variables to be 1 to obtain a (not necessarily homogeneous) polynomial (i.e. $g_j$). This process is often called *dehomogenisation*.

**Definition 6.3.** Let $X \subseteq \mathbb{P}^n$ be a projective algebraic set, and $U_i$ a standard affine chart of $\mathbb{P}^n$. The affine algebraic set $X_i = X \cap U_i$ is called a *standard affine piece* of $X$. The decomposition $X = \cup_{i=0}^n X_i$ is called the *standard affine cover* of $X$.

**Example 6.4.** Consider the projective algebraic sets $X = \mathbb{V}_p(xy - z^2) \subseteq \mathbb{P}^2$. By setting one of the variables to be 1, we obtain the three standard affine pieces of $X$, which are $X_0 = \mathbb{V}_a(y - z^2) \subseteq \mathbb{A}^2$, $X_1 = \mathbb{V}_a(x - z^2) \subseteq \mathbb{A}^2$, and $X_2 = \mathbb{V}_a(xy - 1) \subseteq \mathbb{A}^2$.

We turn to another relation between affine and projective algebraic sets. Recall that $\mathbb{P}^n$ can be understood as $\mathbb{A}^n$ together with "points at infinity". We have also seen in Example 4.9 how to find points at infinity for a line in $\mathbb{A}^2$. More generally we have

**Definition 6.5** (From affine to projective)**.** For any affine algebraic set $X \subseteq \mathbb{A}^n$, let $I = \mathbb{I}_a(X)$ and $\overline{I}$ be the ideal in $\Bbbk[z_0, \cdots, z_n]$ generated by the set of homogeneous polynomials

$$\left\{ z_0^{\deg f} f\left(\frac{z_1}{z_0}, \cdots, \frac{z_n}{z_0}\right) \,\middle|\, f(x_1, \cdots, x_n) \in I \right\}.$$

Then the projective algebraic set $\overline{X} = \mathbb{V}_p(\overline{I})$ is called the *projective closure* of $X$. The points in $\{[z_0 : \cdots : z_n] \in \overline{X} \mid z_0 = 0\}$ are called *points at infinity* for $X$.

*Remark* 6.6. We have already used the above modification of a polynomial in Example 4.9; that is, first replacing all non-homogeneous coordinates by ratios of homogeneous coordinates, then clearing the denominators. This process is often called *homogenisation*. More precisely, for a polynomial $f(x_1, \cdots, x_n) \in \Bbbk[x_1, \cdots, x_n]$, assume $\deg f = d$ and let

$$f = f_0 + f_1 + \cdots + f_{d-1} + f_d$$

be its homogeneous decomposition, then the homogenisation of $f$ is given by

$$z_0^d \cdot f\left(\frac{z_1}{z_0}, \cdots, \frac{z_n}{z_0}\right) = z_0^d f_0 + z_0^{d-1} f_1 + \cdots + z_0 f_{d-1} + f_d.$$

**Example 6.7.** The projective closure of $\mathbb{A}^n$ is $\mathbb{P}^n$. The points at infinity are all points in $H_0$, namely, all points $\{[z_0 : z_1 : \cdots : z_n] \in \mathbb{P}^n \mid z_0 = 0\}$.

This definition is not easy to use in general, as it requires to homogenise infinitely many polynomials in $\mathbb{I}_a(X)$. The following criterion is more convenient for computations.

**Proposition 6.8.** *Let $X = \mathbb{V}_a(f) \subseteq \mathbb{A}^n$ be an affine hypersurface for some polynomial $f \in \Bbbk[x_1, \cdots, x_n]$ of degree $d$. Let*

$$\overline{f}(z_0, z_1, \cdots, z_n) = z_0^d f\left(\frac{z_1}{z_0}, \cdots, \frac{z_n}{z_0}\right)$$

*be the homogenisation of $f$. Then $\overline{X} = \mathbb{V}_p(\overline{f})$.*

*Proof.* Non-examinable. □

*Remark* 6.9. In general, when an affine algebraic set $X$ is defined by more than one polynomial, the projective closure of $X$ is not defined by homogenisation of the generators of $\mathbb{I}_a(X)$. We will see an example in Exercise 6.3.

**Example 6.10.** In Example 4.9, we have seen that the projective closure of $\mathbb{V}_a(x_2 - x_1 + 1) \subseteq \mathbb{A}^2$ is $\mathbb{V}_p(x_2 - x_1 + x_0) \subseteq \mathbb{P}^2$, and that the projective closure of $\mathbb{V}_a(x_2 - x_1 - 1) \subseteq \mathbb{A}^2$ is $\mathbb{V}_p(x_2 - x_1 - x_0) \subseteq \mathbb{P}^2$. The point at infinity for both affine algebraic sets is $[0 : 1 : 1]$.

**Example 6.11.** We compute the projective closure and points at infinity for the heart curve $X = \mathbb{V}_a((x^2+y^2-1)^3 - x^2y^3)$. We use $z$ for the extra variable. By Proposition 6.8, the projective closure is given by one homogeneous equation of degree 6; that is

$$\overline{X} = \mathbb{V}_p((x^2+y^2-z^2)^3 - x^2y^3z).$$

To find the points at infinity, we set $z = 0$. Then we have $(x^2+y^2)^3 = 0$, hence $y = \pm\sqrt{-1}x$. It follows that there are two points at infinity given by $[x : y : z] = [1 : \sqrt{-1} : 0]$ and $[1 : -\sqrt{-1} : 0]$.

Finally we briefly mention the relation of the two constructions. They are almost inverse to each other, subject to some assumptions. For simplicity, we only state the correspondece in the case of varieties. We have the following bijection. Recall that $H_0 = \mathbb{P}^n \backslash U_0$.

$$\left\{ \begin{array}{c} \text{projective varieties } X \subseteq \mathbb{P}^n \\ \text{such that } X \not\subseteq H_0 \end{array} \right\} \underset{X=\overline{Y}}{\overset{Y=X\cap U_0}{\rightleftarrows}} \left\{ \begin{array}{c} \text{affine varieties } Y \subseteq U_0 \cong \mathbb{A}^n \\ \text{such that } Y \neq \varnothing \end{array} \right\}$$

We summarise the content of the correspondence in the following result:

**Proposition 6.12.** *There is a bijection between projective varieties in $\mathbb{P}^n$ which are not contained in $H_0 = \mathbb{P}^n \backslash U_0$ and non-empty affine varieties in $U_0$, given by the mutually inverse correspondences of taking the standard affine piece in $U_0$ and taking the projective closure.*

*Proof.* Non-examinable. Interested reader can find the proof in [Section 5.5, Reid, Undergraduate Algebraic Geometry] or [Section 4.3, Fulton, Algebraic Curves]. □

The importance of the two constructions relating affine and projective varieties is that they allow us to study some properties in a relatively easier context, i.e., either affine or projective, and deduce some similar properties in the other context. We will see two examples in future lectures.

6.2. **Rational functions and function fields.** As we have seen, polynomials cannot be used to define functions on projective algebraic sets. Therefore we have to find a more flexible way to define functions on them, namely, rational functions. For simplicity, we only consider varieties. We will first define rational functions on affine varieties, then on projective varieties.

For any affine variety $X \subseteq \mathbb{A}^n$, $\mathbb{I}(X)$ is a prime ideal in $\Bbbk[x_1, \cdots, x_n]$ by Proposition 2.15. It follows that $\Bbbk[X] = \Bbbk[x_1, \cdots, x_n]/\mathbb{I}(X)$ is an integral domain by Proposition 2.12 (1).

**Definition 6.13.** Let $X \subseteq \mathbb{A}^n$ be an affine variety. Its *function field* $\Bbbk(X)$ is the field of fractions of the integral domain $\Bbbk[X]$. In other words,

$$\Bbbk(X) := \left\{ \frac{\varphi}{\psi} \mid \varphi, \psi \in \Bbbk[X] \text{ with } \psi \neq 0 \right\} / \sim,$$

where $\sim$ is an equivalence relation defined by

$$\frac{\varphi_1}{\psi_1} \sim \frac{\varphi_2}{\psi_2} \quad \Longleftrightarrow \quad \varphi_1\psi_2 - \psi_1\varphi_2 = 0 \in \Bbbk[X].$$

An element in $\Bbbk(X)$ is called a *rational function* on $X$.

*Remark* 6.14. Recall that $\varphi$ and $\psi$ can be given by polynomials, so we can also write

$$\Bbbk(X) = \left\{ \frac{f}{g} \mid f, g \in \Bbbk[x_1, \cdots, x_n] \text{ with } g \notin \mathbb{I}(X) \right\} / \sim,$$

where $\sim$ is an equivalence relation defined by

$$\frac{f_1}{g_1} \sim \frac{f_2}{g_2} \quad \Longleftrightarrow \quad f_1g_2 - g_1f_2 \in \mathbb{I}(X).$$

As a quick example, $\frac{1}{x}$ defines a rational function on the affine variety $X = \mathbb{A}^1$. Every polynomial function is clearly a rational function which is defined everywhere on $X$. But in general, a rational function is only a partially defined function on $X$.

**Example 6.15.** The coordinate ring of the affine variety $X = \mathbb{A}^n$ is $\Bbbk[\mathbb{A}^n] = \Bbbk[x_1, \cdots, x_n]$. By Definition 6.13, its function field is the field of fractions of $\Bbbk[x_1, \cdots, x_n]$, usually written as $\Bbbk(\mathbb{A}^n) = \Bbbk(x_1, \cdots, x_n)$. A rational function on $X = \mathbb{A}^n$ is given by a fraction of the form $\frac{f}{g}$ with $g \neq 0$. Two such fractions are considered to define the same rational function if and only if they can be reduced to the same form after cancelling common factors in the numerator and the denomirator.

We want to find out how to make a similar definition on projective varieties. Recall from equation (4.3) that a non-constant homogeneous polynomial cannot define a function on a projective algebraic set, because its value at a point depends on the choice of the homogeneous coordinates. However, for two homogeneous polynomials $f, g \in \Bbbk[z_0, \cdots, z_n]$ of the same degree $d$, their ratio $\frac{f}{g}$ is well-defined at any point $p = [a_0 : \cdots : a_n]$ provided that $g(p) \neq 0$, because for any $\lambda \neq 0$, we have

$$\frac{f(\lambda a_0, \cdots, \lambda a_n)}{g(\lambda a_0, \cdots, \lambda a_n)} = \frac{\lambda^d f(a_0, \cdots, a_n)}{\lambda^d g(a_0, \cdots, a_n)} = \frac{f(a_0, \cdots, a_n)}{g(a_0, \cdots, a_n)},$$

which is independent of the choice of the homogeneous coordinates of $p$. Therefore $\frac{f}{g}$ can be thought as a partially defined function on a projective variety. More precisely,

**Definition 6.16.** Let $X \subseteq \mathbb{P}^n$ be a projective variety. The *function field* of $X$ is

$$\Bbbk(X) := \left\{ \frac{f}{g} \;\middle|\; f, g \in \Bbbk[z_0, \cdots, z_n] \text{ are homogeneous of the same degree, } g \notin \mathbb{I}(X) \right\} / \sim,$$

where $\sim$ is an equivalence relation defined by

$$\frac{f_1}{g_1} \sim \frac{f_2}{g_2} \iff f_1 g_2 - f_2 g_1 \in \mathbb{I}(X).$$

An element in $\Bbbk(X)$ is called a *rational function* on $X$.

It is in general not easy to explicitly compute the function field of a projective variety. However, the following result allows one to reduce the question to the affine situation.

**Lemma 6.17.** *Let $X \subseteq \mathbb{A}^n$ be an affine variety and $\overline{X} \subseteq \mathbb{P}^n$ its projective closure. Then $\Bbbk(X) \cong \Bbbk(\overline{X})$.*

*Sketch of proof.* (This proof is non-examinable and not covered in lectures.)

We sketch a proof. For every rational function on $X$

$$\frac{f(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)} \in \Bbbk(X),$$

assume $m = \max\{\deg f, \deg g\}$, then we can get a rational function on $\overline{X}$

$$\frac{z_0^m f(\frac{z_1}{z_0}, \cdots, \frac{z_n}{z_0})}{z_0^m g(\frac{z_1}{z_0}, \cdots, \frac{z_n}{z_0})} \in \Bbbk(\overline{X}),$$

since it is the ratio of two homogeneous polynomials of degree $m$. In this way we can define a map $\Bbbk(X) \to \Bbbk(\overline{X})$. On the other hand, for every rational function on $\overline{X}$

$$\frac{p(z_0, \cdots, z_n)}{q(z_0, \cdots, z_n)} \in \Bbbk(\overline{X}),$$

we have a rational function on $X$

$$\frac{p(1, x_1, \cdots, x_n)}{q(1, x_1, \cdots, x_n)} \in \Bbbk(X).$$

In this way we can define a map $\Bbbk(\overline{X}) \to \Bbbk(X)$. We need to verify that both maps are well-defined (i.e., independent of the choice of the representative in each equivalence class), and are homomorphisms. More work is required to check that they are inverse of each other hence are isomorphisms. $\square$

**Example 6.18.** By Example 6.15 we know $\Bbbk(\mathbb{A}^n) = \Bbbk(x_1, \cdots, x_n)$. Since $\mathbb{P}^n$ is the projective closure of $\mathbb{A}^n$ by Example 6.7, we have $\Bbbk(\mathbb{P}^n) \cong \Bbbk(x_1, \cdots, x_n)$ by Lemma 6.17.

Recall that polynomial maps can pullback polynomial functions on affine algebraic sets. Similarly, a dominant rational map can pullback rational functions on projective varieties.

**Definition 6.19.** Let $\varphi : X \dashrightarrow Y$ be a dominant rational map between projective varieties. For every rational function $g$ on $Y$, the *pullback* of $g$ along $\varphi$ is the rational function $g \circ \varphi$ on $X$, denoted $\varphi^*(g)$.

**Example 6.20.** Consider the dominant rational map $\varphi : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ studied in Example 5.18. Then the pullback of the rational function $\frac{x}{y+z} \in \Bbbk(\mathbb{P}^2)$ along $\varphi$ is

$$\varphi^*\left(\frac{x}{y+z}\right) = \frac{yz}{zx+xy} \in \Bbbk(\mathbb{P}^2).$$

Recall that two affine algebraic sets are isomorphic if and only if they have isomorphic coordinate rings. A similar result holds for projective varieties.

**Proposition 6.21.** *A rational map $\varphi : X \dashrightarrow Y$ between projective varieties is a birational map if and only if $\varphi$ is dominant and $\varphi^* : \Bbbk(Y) \longrightarrow \Bbbk(X)$ is a field isomorphism. Two projective varieties $X$ and $Y$ are birational if and only if $\Bbbk(X) \cong \Bbbk(Y)$.*

*Proof.* Non-examinable. Interested reader can find the proof in [Section 5.8, Reid, Undergraduate Algebraic Geometry] or [Section 6.6, Fulton, Algebraic Curves]. □

## Exercise Sheet 6

*This sheet will be discussed in the exercise class on 13 November. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 6.1.** *Example: the cooling tower, revisited.* Consider the projective algebraic set $Y = \mathbb{V}(y_0y_3 - y_1y_2) \subseteq \mathbb{P}^3$. We know by Exercise 5.2 (1) that $Y$ is a projective variety.

(1) Write down all standard affine pieces of $Y$.

(2) Explain why its function field $\Bbbk(Y) \cong \Bbbk(x_1, x_2)$. (*Hint:* you can use the results in Exercise 5.2 and any results mentioned in lectures.)

**Exercise 6.2.** *Example: irreducible cubic curves.*

(1) Show that the affine algebraic set $X = \mathbb{V}_a(y^2 - (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)) \subseteq \mathbb{A}^2$ is an affine variety for any $\lambda_1, \lambda_2, \lambda_3 \in \Bbbk$.

(2) Find the projective closure $\overline{X} \subseteq \mathbb{P}^2$ of $X$ and the points at infinity. Use Proposition 6.12 to conclude that $\overline{X}$ is a projective variety.

**Exercise 6.3.** *A caution for the projective closure.* We demonstrate Remark 6.9.

(1) Let $X = \mathbb{V}_a(I) \subseteq \mathbb{A}^3$ for the ideal $I = (f_1, f_2)$ in $\Bbbk[x, y, z]$ where $f_1 = y - x^2$ and $f_2 = z - x^3$. Using $w$ as the extra variable, find polynomials $\overline{f_1}$ and $\overline{f_2}$ in $\Bbbk[w, x, y, z]$ which are the homogenisations of $f_1$ and $f_2$ respectively.

(2) We have seen in Exercise 2.4 (3) that $I = \mathbb{I}_a(X)$. Let $\overline{I}$ be the homogeneous ideal in $\Bbbk[w, x, y, z]$ defined as in Definition 6.5. Show that $y^2 - xz \in \overline{I}$ but $y^2 - xz \notin (\overline{f_1}, \overline{f_2})$. Conclude that $\overline{I} \neq (\overline{f_1}, \overline{f_2})$. Show that $\overline{X} \neq \mathbb{V}_p(\overline{f_1}, \overline{f_2})$.

*Remark:* this example demonstrates that the projective closure of an affine algebraic set $X$ is not obtained simply by homogenising the generators of $\mathbb{I}_a(X)$ in general.

**Exercise 6.4.** *Geometric interpretation of the projective closure.* We consider $\mathbb{A}^n$ as the standard affine chart $U_0 \subseteq \mathbb{P}^n$. Then an affine algebraic set $X \subseteq \mathbb{A}^n$ can be thought as a subset of $\mathbb{P}^n$. Prove that its projective closure $\overline{X}$ is the smallest projective algebraic set in $\mathbb{P}^n$ containing $X$. You can follow these steps:

(1) Let $W \subseteq \mathbb{P}^n$ be any projective algebraic set that contains $X$. Let $g(z_0, z_1, \cdots, z_n) \in \mathbb{I}_p(W)$ be a homogeneous polynomial and $f(z_1, \cdots, z_n) = g(1, z_1, \cdots, z_n)$ the dehomogenisation of $g$. Show that $f \in \mathbb{I}_a(X)$.

(2) Let $\overline{f}$ be the homogenisation of $f$. Show that $g = z_0^k \cdot \overline{f}$ for some non-negative integer $k$. Conclude that $g \in \overline{I}$ where $\overline{I}$ is the homogenisation of the ideal $\mathbb{I}_a(X)$ defined as in Definition 6.5. Conclude that $\overline{X} \subseteq W$.

(3) Conclude that $\overline{X}$ is the smallest projective algebraic set in $\mathbb{P}^n$ containing $X$.

## Solutions to Exercise Sheet 6

**Solution 6.1.** *Example: the cooling tower, revisited.*

(1) We can get the standard affine pieces $Y_i = Y \cap U_i$ by setting $y_i = 1$. Therefore the standard affine pieces of $Y$ are given by $Y_0 = \mathbb{V}_a(y_3 - y_1y_2)$, $Y_1 = \mathbb{V}_a(y_0y_3 - y_2)$, $Y_2 = \mathbb{V}_a(y_0y_3 - y_2)$ and $Y_3 = \mathbb{V}_a(y_0 - y_1y_2)$.

(2) We proved in Exercise 5.2 that $Y$ is birational to $\mathbb{P}^2$. By Proposition 6.21 and Example 6.18, we have $\Bbbk(X) \cong \Bbbk(\mathbb{P}^2) \cong \Bbbk(x_1, x_2)$.

**Solution 6.2.** *Example: irreducible cubic curves.*

(1) We claim that $y^2 - (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ is an irreducible polynomial. Use contradiction. Assume $y^2 - (x - \lambda_1)(x - \lambda_2)(x - \lambda_3) = f(x, y)g(x, y)$ for non-constant polynomials $f, g \in \Bbbk[x, y]$. Since the left-hand side has degree 2 in $y$, the degrees of $f$ and $g$ in $y$ must be either 2 and 0, or 1 and 1. In the first case we can write

$$y^2 - (x - \lambda_1)(x - \lambda_2)(x - \lambda_3) = (y^2 f_2(x) + yf_1(x) + f_0(x)) \cdot g(x).$$

Comparing coefficients of $y^2$ we find $f_2(x)g(x) = 1$, hence $g(x)$ must be a constant. Contradiction. In the second case we can write

$$y^2 - (x - \lambda_1)(x - \lambda_2)(x - \lambda_3) = (yf_1(x) + f_0(x)) \cdot (yg_1(x) + g_0(x)).$$

Comparing coefficients of $y^2$ we find $f_1(x)g_1(x) = 1$. Without loss of generality we can assume $f_1(x) = g_1(x) = 1$. Comparing coefficients of $y$ we find $f_0(x) + g_0(x) = 0$. Comparing constant terms we find $-(x - \lambda_1)(x - \lambda_2)(x - \lambda_3) = f_0(x)g_0(x) = -f_0(x)^2$, hence $f_0(x)^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$, which is also a contradiction since the right-hand side is not a square. So we conclude that $y^2 - (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ is irreducible. By Lemma 5.4 we know $I = (y^2 - (x - \lambda_1)(x - \lambda_2)(x - \lambda_3))$ is a prime ideal. By Proposition 2.15 we know $X$ is an irreducible algebraic set, i.e. an affine variety.

(2) Using $z$ as the extra variable, the projective closure is given by $\overline{X} = \mathbb{V}_p(y^2z - (x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z))$. To find points at infinity, we set $z = 0$ to get $-x^3 = 0$. It follows that $x = 0$, hence the only point at infinity for $X$ is given by $[x : y : z] = [0 : 1 : 0]$. One direction of Proposition 6.12 shows that the projective closure of a non-empty affine variety is a projective variety. Hence by part (1), we conclude that $\overline{X}$ is a projective variety.

**Solution 6.3.** *A caution for the projective closure.*

(1) The homogenisation of $f_1$ and $f_2$ are given by $\overline{f_1} = wy - x^2$ and $\overline{f_2} = w^2z - x^3$.

(2) We first claim $y^2 - xz \in I = (y - x^2, z - x^3)$. This can be seen by realising $y^2 - xz = (y^2 - x^4) + (x^4 - xz) = (y - x^2)(y + x^2) - x(z - x^3)$ which is a sum of a term with $y - x^2$ as a factor and a term with $z - x^3$ as a factor. Since $y^2 - xz$ is an element in $I$, by Definition 6.5, the

homogenisation of $y^2 - xz$ is an element in $\overline{I}$. However, since $y^2 - xz$ is already homogeneous, its homogenisation is still $y^2 - xz$. Therefore $y^2 - xz \in \overline{I}$.

We prove that $y^2 - xz \notin (\overline{f_1}, \overline{f_2})$. Use contradiction. Assume we can write $y^2 - xz = \overline{f_1} \cdot g_1 + \overline{f_2} \cdot g_2 = (wy - x^2) \cdot g_1 + (w^2 z - x^3) \cdot g_2$ for some $g_1, g_2 \in \Bbbk[w, x, y, z]$. There are many different ways to find a contradiction. Here is one approach: when $w = x = 0$ and $y = z = 1$, the left-hand side is 1 while the right-hand side is 0, which is a contradiction.

Finally we prove that $\overline{X} \neq \mathbb{V}_p(\overline{f_1}, \overline{f_2})$. There are also many different approaches to this. Here is one of them: On one hand, we can verify directly that $\overline{f_1} = 0$ and $\overline{f_2} = 0$ at the point $[w : x : y : z] = [0 : 0 : 1 : 1]$, hence $[0 : 0 : 1 : 1] \in \mathbb{V}_p(\overline{f_1}, \overline{f_2})$. On the other hand, since $\overline{X} = \mathbb{V}_p(\overline{I})$, a point in $\overline{X}$ has to be a solution to every homogeneous polynomial in $\overline{I}$, in particular, it has to be a solution to the polynomial $y^2 - xz$ by what we just proved. We can check directly that the point $[w : x : y : z] = [0 : 0 : 1 : 1]$ is not a solution to this polynomial, hence $[0 : 0 : 1 : 1] \notin \overline{X}$. This finishes the proof.

Indeed, one can see that the value of $z$ is irrelavant. For any $\lambda \in \Bbbk$, the point $[w : x : y : z] = [0 : 0 : 1 : \lambda]$ would do the trick.

**Solution 6.4.** *Geometric interpretation of the projective closure.*

(1) We need to show that $f(p) = 0$ for every point $p \in X$. Let $p = (a_1, \cdots, a_n) \in X$, where $a_1, \cdots, a_n \in \Bbbk$ are the non-homogeneous coordinates of $p$ as a point in $\mathbb{A}^n \cong U_0$. Then as a point in $\mathbb{P}^n$, the homogeneous coordinates of $p$ can be given by $p = [1 : a_1 : \cdots : a_n]$. Since $X \subseteq W$, we have $p \in W$, therefore $g(p) = 0$. In other words, $g(1, a_1, \cdots, a_n) = 0$. Therefore we have $f(a_1, \cdots, a_n) = g(1, a_1, \cdots, a_n) = 0$, which proves $f(p) = 0$. Since $p$ is an arbitrary point in $X$, we conclude that $f \in \mathbb{I}_a(X)$.

(2) We assume $g$ is a homogeneous polynomial with $\deg g = d$. Assume that $z_0^k$ is the highest power dividing $g$, then $k$ is a non-negative integer, and each term in $g$ has a factor of $z_0^k$. We collect terms in $g$ which have the degree with respect to $z_0$, so we can write

$$g = z_0^k \cdot f_{d-k} + z_0^{k+1} \cdot f_{d-k-1} + \cdots + z_0^{d-1} \cdot f_1 + z_0^d \cdot f_0$$

where $f_i \in \Bbbk[z_1, \cdots, z_n]$ is homogeneous of degree $i$ for $i = 0, 1, \cdots, d-k$, and $f_{d-k} \neq 0$. Since $f$ is the dehomogenisation of $g$ with respect to $z_0$, we have

$$f = f_{d-k} + f_{d-k-1} + \cdots + f_1 + f_0$$

which is precisely the homogeneous decomposition of $f$. We observe that $\deg f = d - k$. Since $\overline{f}$ is the homogenisation of $f$ with respect to $z_0$, we have

$$\overline{f} = f_{d-k} + z_0 \cdot f_{d-k-1} + \cdots + z_0^{d-k-1} \cdot f_1 + z_0^{d-k} \cdot f_0.$$

Comparing the formula for $g$ and $\overline{f}$, we find out that $g = z_0^k \cdot \overline{f}$.

Now we prove $g \in \overline{I}$. Since $f \in \mathbb{I}_a(X)$ by part (1), we have $\overline{f} \in \overline{I}$ by Definition 6.5. Since $\overline{I}$ is an ideal, we have $g = z_0^k \cdot \overline{f} \in \overline{I}$.

Since $g$ is an arbitrary homogeneous polynomial in $\mathbb{I}_p(W)$, we conclude that every homogeneous polynomial in the ideal $\mathbb{I}_p(W)$ is a homogeneous polynomial in the ideal $\overline{I}$. It follows that $\mathbb{V}_p(\mathbb{I}_p(W)) \supseteq \mathbb{V}_p(\overline{I})$. We have $\mathbb{V}_p(\mathbb{I}_p(W)) = W$ by Proposition 5.2, and $\mathbb{V}_p(\overline{I}) = \overline{X}$ by Definition 6.5. Therefore $W \supseteq \overline{X}$.

(3) We proved in parts (1) and (2) that every projective algebraic set $W$ that contains $X$ must contain $\overline{X}$. Since $\overline{X}$ itself is also a projective algebraic set that contains $X$ (it is $X$ together with points at infinity), we conclude that $\overline{X}$ is the smallest one having this property.

## 7. Non-singularity

The non-singularity is an algebraic version of smoothness in analysis. We will find out how to determine the non-singularity of a variety from its defining equations, and study the related notions of tangent spaces and dimensions.

7.1. **Non-singularity of irreducible hypersurfaces.** In this lecture we consider the case of irreducible hypersurfaces. We start with the affine case. Let $f \in \Bbbk[x_1, \cdots, x_n]$ be a non-constant irreducible polynomial. By Lemma 5.4, we know that $\mathbb{V}(f) \subseteq \mathbb{A}^n$ is an affine irreducible hypersurface.

**Definition 7.1.** Let $X = \mathbb{V}(f) \subseteq \mathbb{A}^n$ be an affine irreducible hypersurface defined by a non-constant irreducible polynomial $f \in \Bbbk[x_1, \cdots, x_n]$. For any point $p \in X$, we say $X$ is *singular* at $p$ if $\frac{\partial f}{\partial x_i}(p) = 0$ for every $i$, $1 \leqslant i \leqslant n$; otherwise we say $X$ is *non-singular* at $p$. If $X$ is non-singular at every point $p \in X$, then we say $X$ is *non-singular*; otherwise we say $X$ is *singular*.

*Remark* 7.2. From Definition 7.1 we see that the singular points in $X = \mathbb{V}(f)$ form an affine algebraic set $X_{\text{sing}} = \mathbb{V}(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}) \subseteq X$. To find all singular points, we just need to solve the system of equations given by $f$ and all its partial derivatives.

**Example 7.3.** Consider the affine variety $X = \mathbb{V}(f) \subseteq \mathbb{A}^2$ where $f = x^3 + y^3 - 3xy$. To find all singular points, we need to solve the system of equations given by $f = x^3 + y^3 - 3xy = 0$ and the partial derivatives $\frac{\partial f}{\partial x} = 3x^2 - 3y = 0$ and $\frac{\partial f}{\partial y} = 3y^2 - 3x = 0$. From the two partial derivatives we get $x = y^2 = x^4$, therefore $x(x^3 - 1) = 0$, which implies $x = 0$ or $x^3 = 1$. When $x = 0$, we have $y = 0$. It is clear that $(x, y) = (0, 0)$ is a solution to the system of equations. When $x^3 = 1$, we have $x^3 + y^3 - 3xy = x^3 + x^6 - 3x^3 = -1 \neq 0$. Contradition. Therefore the only point at which $X$ is singular is $(0, 0)$.

The following result shows that $X = \mathbb{V}(f)$ cannot be singular everywhere. Recall that we always assume the underlying field $\Bbbk$ is an algebraically closed field of charasteristic 0.

**Theorem 7.4.** *Let $X = \mathbb{V}(f) \subseteq \mathbb{A}^n$ be an affine hypersurface defined by a non-constant irreducible polynomial $f \in \Bbbk[x_1, \cdots, x_n]$. Then the set of non-singular points in $X$ is non-empty.*

*Proof.* The set of singular points in $X$ is given by

$$X_{\text{sing}} = \mathbb{V}\left(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}\right) \subseteq X.$$

Suppose on the contrary that $X_{\text{sing}} = X$, then $\frac{\partial f}{\partial x_i} \in \mathbb{I}(X)$ for every $i$.

Since $f$ is an irreducible polynomial, $(f)$ is a prime ideal by Lemma 5.4. It follows by Proposition 2.9 that $\mathbb{I}(X) = (f)$. Therefore for every $i$, we have

$$\frac{\partial f}{\partial x_i} = f \cdot g_i$$

for some $g_i \in \Bbbk[x_1, \cdots, x_n]$. Assume $f$ has degree $d_i$ in $x_i$. If $d_i > 0$, then $\frac{\partial f}{\partial x_i}$ has degree $d_i - 1$ in $x_i$, while $f \cdot g_i$ has degree at least $d_i$ in $x_i$. Contradiction. Therefore $d_i = 0$. In other words, $x_i$ does not occur in $f$. Since this holds for every $i$, $f$ must be a constant polynomial. Contradiction. This finishes the proof of existence of non-singular points in $X = \mathbb{V}(f)$. □

**Definition 7.5.** Let $X = \mathbb{V}(f) \subseteq \mathbb{A}^n$ be an affine irreducible hypersurface defined by a non-constant irreducible polynomial $f \in \Bbbk[x_1, \cdots, x_n]$. For any point $p = (a_1, \cdots, a_n) \in X$, the *tangent space* of $X$ at $p$ is the affine variety

$$T_pX := \mathbb{V}\left(\frac{\partial f}{\partial x_1}(p) \cdot (x_1 - a_1) + \cdots + \frac{\partial f}{\partial x_n}(p) \cdot (x_n - a_n)\right) \subseteq \mathbb{A}^n.$$

**Example 7.6.** Following Example 7.3, we compute the tangent spaces of $X$ at two points $p_1 = (\frac{4}{3}, \frac{2}{3})$ and $p_2 = (0, 0)$. Recall that $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}) = (3x^2 - 3y, 3y^2 - 3x)$. It is easy to compute that $(\frac{\partial f}{\partial x}(p_1), \frac{\partial f}{\partial y}(p_1)) = (\frac{10}{3}, -\frac{8}{3})$ and $(\frac{\partial f}{\partial x}(p_2), \frac{\partial f}{\partial y}(p_2)) = (0, 0)$. Therefore

$$T_{p_1}X = \mathbb{V}\left(\frac{10}{3}\left(x - \frac{4}{3}\right) - \frac{8}{3}\left(y - \frac{2}{3}\right)\right) = \mathbb{V}(5x - 4y - 4),$$
$$T_{p_2}X = \mathbb{V}\left(0 \cdot (x - 0) + 0 \cdot (y - 0)\right) = \mathbb{A}^2$$

are the tangent spaces of $X$ at $p_1$ and $p_2$ respectively.

*Remark* 7.7. In Definition 7.5, when $p$ is singular point of $X$, the defining equation of $T_pX$ is a zero polynomial hence $T_pX = \mathbb{A}^n$, which has dimension $n$ as a vector space over $\Bbbk$; when $X$ is non-singular at $p$, the tangent space $T_pX$ is a shift of the vector subspace $\mathbb{V}\left(\frac{\partial f}{\partial x_1}(p)\cdot x_1 + \cdots + \frac{\partial f}{\partial x_n}(p)\cdot x_n\right)$, which has dimension $n-1$. Therefore we can say, the irreducible hypersurface $X \subseteq \mathbb{A}^n$ is non-singular at $p$ if and only if $\dim T_pX = n-1$; $X$ is singular at $p$ if and only if $\dim T_pX > n-1$. We will generalise this conclusion to arbitrary affine varieties in next lecture.

Finally we briefly mention the case of projective irreducible hypersurfaces. Let $f \in \Bbbk[z_0, \cdots, z_n]$ be a non-constant homogeneous irreducible polynomial. By Lemma 5.4, we know that $\mathbb{V}(f) \subseteq \mathbb{P}^n$ is a projective irreducible hypersurface.

**Definition 7.8.** Let $X = \mathbb{V}(f) \subseteq \mathbb{P}^n$ be a projective irreducible hypersurface defined by a non-constant homogeneous irreducible polynomial $f \in \Bbbk[z_0, \cdots, z_n]$. For any point $p \in X$, we say $X$ is *singular* at $p$ if the affine hypersurface $X_i = X \cap U_i$ is singular at $p$ for any standard affine piece $X_i$ containing $p$; otherwise we say $X$ is *non-singular* at $p$. The *tangent space* $T_pX$ of $X$ at $p$ is the projective closure of $T_pX_i$ for any standard affine piece $X_i$ containing $p$. If $X$ is non-singular at every point $p \in X$, then we say $X$ is *non-singular*; otherwise we say $X$ is *singular*.

*Remark* 7.9. A point $p \in X$ could be contained in several standard affine pieces of $X$. To check whether $X$ is singular at $p$, and compute the tangent space of $X$ at $p$, it suffices to choose one standard affine piece of $X$ containing $p$. The result does not depend on the choice of the standard affine piece.

**Example 7.10.** Consider the projective variety $Y = \mathbb{V}_p(\overline{f}) \subseteq \mathbb{P}^2$ where $\overline{f} = x^3 + y^3 - 3xyz$. The standard affine piece $Y \cap U_2$ is the affine variety in Examples 7.3 and 7.6. The results in the two examples imply that $Y$ is non-singular at $p_1 = [\frac{4}{3} : \frac{2}{3} : 1] = [4 : 2 : 3]$ and singular at $p_2 = [0 : 0 : 1]$. Moreover, the tangent spaces of $Y$ at $p_1$ and $p_2$ are given by $T_{p_1}Y = \mathbb{V}_p(5x - 4y - 4z)$ and $T_{p_2}Y = \mathbb{P}^2$.

7.2. **Non-singularity of varieties.** We generalise our discussion from last time and study non-singularity of varieties. Similarly, we first consider the case of affine varieties. for any affine variety $X$, we know by Corollary 1.14 that $\mathbb{I}(X)$ is finitely generated.

**Definition 7.11.** Let $X \subseteq \mathbb{A}^n$ be a non-empty affine variety. Assume $\mathbb{I}(X) = (f_1, \cdots, f_m)$ for some $f_1, \cdots, f_m \in \Bbbk[x_1, \cdots, x_n]$. For any point $p = (a_1, \cdots, a_n) \in X$, the *tangent space* of $X$ at $p$ is the affine variety

$$T_pX := \bigcap_{i=1}^{m} \mathbb{V}\left(\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}(p)\cdot(x_j - a_j)\right) \subseteq \mathbb{A}^n.$$

*Remark* 7.12. We can view the tangent space $T_pX$ as a shift of the linear subspace

$$\bigcap_{i=1}^{m} \mathbb{V}\left(\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}(p)\cdot x_j\right) \subseteq \mathbb{A}^n$$

which is the null space of the matrix

$$M_p := \left(\frac{\partial f_i}{\partial x_j}(p)\right)_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}.$$

By the rank-nullity theorem, the dimension of $T_pX$ is given by

$$\dim T_pX = n - \operatorname{rank} M_p.$$

**Definition 7.13.** Let $X \subseteq \mathbb{A}^n$ be a non-empty affine variety. The *dimension* of $X$ is

$$\dim X = \min\{\dim T_pX \mid p \in X\}.$$

For any point $p \in X$, we say $X$ is *singular* at $p$ if $\dim T_pX > \dim X$; we say $X$ is *non-singular* at $p$ if $\dim T_pX = \dim X$. If $X$ is non-singular at every point $p \in X$, then we say $X$ is *non-singular*; otherwise we say $X$ is *singular*.

*Remark* 7.14. By Remark 7.7, we find that Definition 7.1 for hypersurfaces is consistent with the more general Definition 7.11. We also point out: although our definition of tangent spaces and dimension involve a choice of generators in $\mathbb{I}(X)$, they are in fact independent of the choice. In other words, different choices of generators in $\mathbb{I}(X)$ always give the same tangent spaces and dimension.

**Example 7.15.** As a simple example, let $X = \mathbb{A}^n$, then $\mathbb{I}(X) = \{0\}$. For any point $p \in X$, it is clear that $M_p$ is a zero matrix and $T_pX = \mathbb{A}^n$. Therefore $\dim T_pX = n - \operatorname{rank} M_p = n$. It follows that $\dim X = n$, and $X$ is non-singular.

**Example 7.16.** Remark 7.7 together with Theorem 7.4 shows that $\dim X = n-1$ for any irreducible hypersurface $X \subseteq \mathbb{A}^n$.

**Example 7.17.** As another simple example, let $X = \{p\} \subseteq \mathbb{A}^n$ be a single point set, where $p = (a_1, \cdots, a_n)$. By Exercise 2.3 we know $\mathbb{I}(X) = (x_1 - a_1, \cdots, x_n - a_n)$. Then we have $M_p = I_n$ is the identity matrix, and that $T_pX = \cap_{i=1}^n \mathbb{V}(x_i - a_i) = \{p\}$. It follows that $\dim X = 0$ and $X$ is non-singular.

Now we consider projective varieties. Similar to the hypersurface case, the non-singularity and dimension of a projective variety can be reduced to its standard affine pieces.

**Definition 7.18.** Let $X \subseteq \mathbb{P}^n$ be a non-empty projective variety. The *dimension* of $X$ is defined to be $\dim X_i$ for any non-empty standard affine piece $X_i = X \cap U_i$, denoted $\dim X$. For any point $p \in X$, we say $X$ is *singular* at $p$ if $X_i$ is singular at $p$ for any standard affine piece $X_i = X \cap U_i$ containing $p$; otherwise we say $X$ is non-singular at $p$. If $X$ is non-singular at every point $p \in X$, then we say $X$ is non-singular; otherwise we say $X$ is singular.

*Remark* 7.19. The dimension of a projective variety can be computed on any of its non-empty standard affine piece. Similarly whether $X$ is singular at $p$ can be computed on any of its standard affine piece containing $p$. Different standard affine pieces always give the same answer. However, in order to find all singular points in a projective variety $X$, we need to work with more than one standard affine piece to avoid missing any point.

A very surprising property of the dimension is its intrinsic nature.

**Theorem 7.20.** *Let $X$ and $Y$ be (affine or projective) varieties. If $\Bbbk(X) \cong \Bbbk(Y)$, then $\dim X = \dim Y$.*

*Proof.* Non-examinable. Interested reader can find the proof in [Sections 6.7 and 6.8, Reid, Undergraduate Algebraic Geometry] or [Section 6.5, Fulton, Algebraic Curves]. □

*Remark* 7.21. Theorem 7.20 shows that the dimension of a variety $X$ only depends on its function field $\Bbbk(X)$. In particular, by Proposition 6.21, if two projective varieties $X$ and $Y$ are birational, then $\dim X = \dim Y$.

**Definition 7.22.** An affine (resp. projective) *algebraic curve* $C \subseteq \mathbb{A}^n$ (resp. $C \subseteq \mathbb{P}^n$) is a finite union of affine (resp. projective) varieties of dimension 1.

Finally we look at a comprehensive example.

**Example 7.23.** Consider the projective variety $X = \mathbb{V}_p(w + x + y + z, w^2 + x^2 + y^2 + z^2) \subseteq \mathbb{P}^3$. We will show that $X$ is a non-singular curve. By Definition 7.18, we need to show every standard affine piece of $X$ is non-singular of dimension 1.

We look at the standard affine piece $X_0 = X \cap U_0 = \{p = [w : x : y : z] \in X \mid w \neq 0\}$. Then $X_0 = \mathbb{V}_a(1+x+y+z, 1+x^2+y^2+z^2) \subseteq \mathbb{A}^3$. To use Definition 7.11, we need to know that $\mathbb{I}_a(X_0) = (1+x+y+z, 1+x^2+y^2+z^2)$. This can be verified by showing the ideal $(1+x+y+z, 1+x^2+y^2+z^2)$ is prime and applying Proposition 2.9 (1). We skip the proof of this step and simply assume it is true.

For any point $p \in X_0$, we have

$$M_p = \begin{pmatrix} 1 & 1 & 1 \\ 2x & 2y & 2z \end{pmatrix}.$$

Since there are two rows in $M_p$ and the first row is non-zero, we know that $1 \leqslant \operatorname{rank} M_p \leqslant 2$ for every point $p \in X_0$. We claim that $\operatorname{rank} M_p = 2$ for every $p \in X_0$. Otherwise, assume $\operatorname{rank} M_p = 1$ for some $p \in X_0$, then the two rows must be proportional hence $x = y = z$. However $p \in X_0$ implies that $1 + x + y + z = 0$ and $1 + x^2 + y^2 + z^2 = 0$, which become $1 + 3x = 0$ and $1 + 3x^2 = 0$. It is easy to see that they do not have common solutions. Hence such a point $p$ does not exist. It follows that $\dim T_p X_0 = 3 - \operatorname{rank} M_p = 1$ for every $p \in X_0$. That means $X_0$ is non-singular, and $\dim X = \dim X_0 = 1$.

Since the defining equations of $X$ are completely symmetric with respect to all variables, the same computation would show that all other standard affine pieces of $X$ are non-singular. Therefore $X$ is a non-singular curve.

## Exercise Sheet 7

*This sheet will be discussed in the exercise class on 20 November. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 7.1.** *Examples of affine varieties.* Find all singular points on the affine variety $X$, if there is any. In parts (1) – (3), you can assume the polynomial $f$ is irreducible. In part (4), we know the two given polynomials generate $\mathbb{I}_a(X)$ by Exercise 2.4.

(1) $X = \mathbb{V}(f) \subseteq \mathbb{A}^2$ for $f = (x^2 + y^2)^3 - 4x^2y^2 \in \Bbbk[x, y]$.

(2) $X = \mathbb{V}(f) \subseteq \mathbb{A}^3$ for $f = xy^2 - z^2 \in \Bbbk[x, y, z]$.

(3) $X = \mathbb{V}(f) \subseteq \mathbb{A}^3$ for $f = xy + x^3 + y^3 \in \Bbbk[x, y, z]$.

(4) $X = \mathbb{V}(f, g) \subseteq \mathbb{A}^3$ for $f = y - x^2 \in \Bbbk[x, y, z]$ and $g = z - x^3 \in \Bbbk[x, y, z]$.

**Exercise 7.2.** *Example of projective varieties.* Show that the projective variety $X = \mathbb{V}(f) \subseteq \mathbb{P}^2$ for $f = xy - z^2 \in \Bbbk[x, y, z]$ is non-singular. Although one can achieve this by showing all three standard affine pieces are non-singular, it is not necessary to check every individual piece. Follow these steps for an easier approach.

(1) Show that the standard affine piece $X_0 = X \cap U_0$ is non-singular.

(2) Find out all points in $X \backslash X_0$. For each point $p \in X \backslash X_0$, use a standard affine piece of $X$ that contains $p$ to show $X$ is non-singular at $p$.

(3) Using this method to find all singular points on the projective variety $\mathbb{V}(f) \subseteq \mathbb{P}^2$ for $f = x^3z + x^2yz + y^3z + x^4 + y^4$. You do not need to prove the irreducibility of any polynomial in this problem – just assume they are.

**Exercise 7.3.** *Example: plane cubics.* Find all singular points on the projective variety $\mathbb{V}(f) \subseteq \mathbb{P}^2$ where $f = y^2z - (x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z)$ for some $\lambda_1, \lambda_2, \lambda_3 \in \Bbbk$, if there is any. You do not need to prove irreducibility of any polynomial in this problem.

(1) $\lambda_1$, $\lambda_2$ and $\lambda_3$ are distinct.

(2) $\lambda_1 = \lambda_2 \neq \lambda_3$.

(3) $\lambda_1 = \lambda_2 = \lambda_3$.

**Exercise 7.4.** *Example: projective twisted cubic.* Consider the projective variety $Y = \mathbb{V}_p(y_0y_2 - y_1^2, y_1y_3 - y_2^2, y_0y_3 - y_1y_2) \subseteq \mathbb{P}^3$. Follow the method in Example 7.23 to

(1) Determine whether $Y$ is non-singular or singular.

(2) Compute the dimension of $Y$.

*Remark:* For any standard affine piece $Y_i$ of $Y$, you can assume without proof that the dehomogenisation of the above three polynomials generate $\mathbb{I}_a(Y_i)$.

**Solution 7.1.** *Examples of affine varieties.*

(1) The singular points are defined by $f = 0$ and the two partial derivatives $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$. We have $\frac{\partial f}{\partial x} = 6x(x^2+y^2)^2 - 8xy^2 = 2x \cdot (3(x^2+y^2)^2 - 4y^2)$ and $\frac{\partial f}{\partial y} = 6y(x^2+y^2)^2 \cdot 2y - 8x^2y = 2y \cdot (3(x^2+y^2)^2 - 4x^2)$. If $x = 0$ or $y = 0$, then $f = 0$ forces $x = y = 0$. The point $(0,0)$ satisfies all equations hence is a singular point. If neither $x$ nor $y$ is 0, then we have $3(x^2+y^2)^2 = 4x^2 = 4y^2$, hence $3(x^2+x^2)^2 = 4x^2$ which implies $x^2 = \frac{1}{3} = y^2$. But then $f = (\frac{1}{3}+\frac{1}{3})^3 - 4 \cdot \frac{1}{3} \cdot \frac{1}{3} \neq 0$. Therefore the only singular point is $(0,0)$.

(2) The singular points are defined by $f = xy^2 - z^2 = 0$, and $\frac{\partial f}{\partial x} = y^2 = 0$, $\frac{\partial f}{\partial y} = 2xy = 0$, $\frac{\partial f}{\partial z} = -2z = 0$. From the second and fourth equations we have $y = z = 0$. No matter what value $x$ takes, $(x,y,z) = (x,0,0)$ always satisfies all the four equations. Therefore the singular points of $\mathbb{V}(f)$ are all points of the form $(x,0,0)$.

(3) The singular points are given by $f = xy + x^3 + y^3 = 0$, and $\frac{\partial f}{\partial x} = y + 3x^2 = 0$, $\frac{\partial f}{\partial y} = x + 3y^2 = 0$, $\frac{\partial f}{\partial z} = 0$. From $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$ we get $x = -3y^2 = -27x^4$, hence $x = 0$ or $x^3 = -\frac{1}{27}$. If $x = 0$, then $f = 0$ forces $y = 0$. It is clear that every point of the form $(x,y,z) = (0,0,z)$ is a solution to all the required equations hence is a singular point on $\mathbb{V}(f)$. If $x \neq 0$, then $x^3 = -\frac{1}{27}$. Then we have $f = xy + x^3 + y^3 = x(-3x^2) + x^3 + (-3x^2)^3 = -3x^3 + x^3 - 27x^6 = \frac{1}{9} - \frac{1}{27} - \frac{1}{27} = \frac{1}{27} \neq 0$. Contradiction. Therefore $(x,y,z) = (0,0,z)$ are the only singular points of $\mathbb{V}(f)$.

(4) At every point $p = (x,y,z) \in X$, we consider the matrix $M_p$ given by the partial derivatives

$$M_p = \begin{pmatrix} -2x & 1 & 0 \\ -3x^2 & 0 & 1 \end{pmatrix}.$$

It is clear that the two rows of $M_p$ are linearly independent, therefore $\operatorname{rank} M_p = 2$ for every $p \in X$. It follows that $\dim T_pX = 3 - \operatorname{rank} M_p = 1$ for every $p \in X$. Therefore $\dim X = 1$ and $\dim T_pX = \dim X$ for every $p \in X$. By Definition 7.13, $X$ is non-singular at every point $p \in X$.

**Solution 7.2.** *Example of projective varieties.*

(1) The standard affine piece $X_0 = X \cap U_0$ is given by setting $x = 1$ in $f$. Hence $X_0 = \mathbb{V}(f_0)$ where $f_0 = y - z^2$. For any point $(y,z) \in X_0$, $\frac{\partial f_0}{\partial y} = 1$ which never vanishes. Therefore $X_0$ does not have any singular point, hence is non-singular.

(2) The set of points in $X \backslash X_0$ is given by $\{[x:y:z] \in X \mid x = 0\}$. When $x = 0$, $f = xy - z^2 = 0$ implies $z = 0$. Hence the only point in $X \backslash X_0$ is $p = [x:y:z] = [0:1:0]$. This point is in the standard affine piece $X_1 = X \cap U_1$ because its $y$-coordinate is non-zero. The standard affine piece $X_1$ is obtained by setting $y = 1$ hence $X_1 = \mathbb{V}_a(f_1)$ where $f_1 = x - z^2$. The point $p = [0:1:0]$ has non-homogeneous coordinates $p = (0,0)$ in the standard affine piece $X_1$. To check whether $X_1$ is singular at $p = (0,0)$, we need to compute the partial derivatives of the defining equation $f_1$. Notice that $\frac{\partial f_1}{\partial x} = 1$ which does not vanish at $p$. We conclude that $p$ is a non-singular point of $X_1$, hence by Definition 7.8, $p$ is a non-singular point of $X$.

Parts (1) and (2) together show that $X = \mathbb{V}(xy - z^2) \subseteq \mathbb{P}^2$ is non-singular.

(3) We first consider the standard affine piece $X_0 = X \cap U_0$. By setting $x = 1$, we get $X_0 = \mathbb{V}(f_0) \subseteq \mathbb{A}^2$ where $f_0 = z + yz + y^3z + 1 + y^4$. To find singular points in $X_0$, we need to consider the equations

$$f_0 = z + yz + y^3z + 1 + y^4 = 0;$$
$$\frac{\partial f_0}{\partial y} = z + 3y^2z + 4y^3 = 0;$$
$$\frac{\partial f_0}{\partial z} = 1 + y + y^3 = 0.$$

We now solve the system. From the first equation we observe that $f_0 = z(1+y+y^3)+(1+y^4) = 0$. Together with the third equation we find that $1+y^4=0$. I claim that the two equations $1+y+y^3=0$ and $1+y^4=0$ do not have a common solution for $y$. There are many ways to prove the claim. One possible way is to use the Euclidean division. We divide $y^4+1$ by $y^3+y+1$ to get

$$y^4+1 = y(y^3+y+1)-(y^2+y-1),$$

which implies $y^2+y-1=0$. We further divide $y^3+y+1$ by $y^2+y-1$ to get

$$y^3+y+1 = (y-1)(y^2+y-1)+3y,$$

which implies $3y=0$ hence $y=0$. Therefore if the two equations have a common solution for $y$ then we must have $y=0$, which is not a solution. This proves the claim, which implies that $X_0$ is non-singular.

Finally we need to check whether the points in $X\backslash X_0$ are singular points. To find all points in $X\backslash X_0$, we set $x=0$ in $f=0$. Then we get $y^3z+y^4=0$, which implies $y=0$ or $y+z=0$. Therefore there are two points in $X\backslash X_0$, given by $p_1=[0:0:1]$ and $p_2=[0:-1:1]$ respectively. To check whether they are singular points, we need to find a standard affine piece which contain them. Since the $z$-coordinates of $p_1$ and $p_2$ are non-zero, we can choose $X_2 = X\cap U_2$. The standard affine piece $X_2=\mathbb{V}(f_2)$ where $f_2 = x^3+x^2y+y^3+x^4+y^4$. The non-homogeneous coordinates of $p_1$ and $p_2$ are given by $p_1=(0,0)$ and $p_2=(0,-1)$ respectively. The partial derivatives of $f_2$ are

$$\frac{\partial f_2}{\partial x} = 3x^2+2xy+4x^3;$$
$$\frac{\partial f_2}{\partial y} = x^2+3y^2+4y^3.$$

It is easy to see that at the point $p_1=(0,0)$, we have $f_2(p_1) = \frac{\partial f_2}{\partial x}(p_1) = \frac{\partial f_2}{\partial y}(p_1) = 0$. Therefore $p_1$ is a singular point on $X_2$. At the point $p_2=(0,-1)$, we have $\frac{\partial f_2}{\partial y}(p_2) = -1 \neq 0$. Therefore $p_2$ is a non-singular point on $X_2$. By Definition 7.8, the only singular point of $X$ is $p_1=[0:0:1]$.

**Solution 7.3.** *Example: plane cubics.* There are three cases to deal with in this question. Most of the calculations are the same in all the three cases. First of all we look at a standard affine piece of $X=\mathbb{V}(f)\subseteq\mathbb{P}^2$. You can choose any standard affine piece of $X$ to start with. For example, we choose the standard affine pice $X_2 = X\cap U_2$, which is given by setting $z=1$ in $f$. Therefore we have

$$X_2 = \mathbb{V}(y^2-(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)) \subseteq \mathbb{A}^2.$$

To find the singular points on $X_2$, we need to solve the system

$$\begin{aligned} y^2-(x-\lambda_1)(x-\lambda_2)(x-\lambda_3) &= 0;\\ -(x-\lambda_2)(x-\lambda_3)-(x-\lambda_1)(x-\lambda_3)-(x-\lambda_1)(x-\lambda_2) &= 0;\\ 2y &= 0. \end{aligned}$$

The third equation implies $y=0$, then the first equation implies $x=\lambda_1$ or $\lambda_2$ or $\lambda_3$. Now there is some difference in the three cases.

(1) If $\lambda_1$, $\lambda_2$ and $\lambda_3$ are distinct, then it is clear that none of them is a solution to the second equation. Therefore $X_2$ is non-singular in this case.

(2) If two of the three are equal, say, $\lambda_1=\lambda_2\neq\lambda_3$, then it is clear that $x=\lambda_1$ (or $\lambda_2$) is a solution to the second equation while $x=\lambda_3$ is not a solution. Therefore $X_2$ has a singular point $(\lambda_1,0)$, which has homogeneous coordinates $[\lambda_1:0:1]$ as a point in $X$.

(3) If all the three are equal, then $x=\lambda_1$ (or $\lambda_2$ or $\lambda_3$) is a solution to the second equation. Therefore $X_2$ has a singular point $(\lambda_1,0)$, which has homogeneous coordinates $[\lambda_1:0:1]$ as a point in $X$.

It remains to consider the points in $X \backslash X_2$. To find these points we set $z = 0$ in the equation $f = 0$. We get $-x^3 = 0$ hence $x = 0$. Therefore the only point in $X \backslash X_2$ is $p = [x : y : z] = [0 : 1 : 0]$. Since the $y$-coordinate of $p$ is non-zero, it is a point in the standard affine piece $X_1 = X \cap U_1$, given by the non-homogeneous coordinates $p = (0, 0)$. To write down the defining polynomial for $X_1$ we set $y = 1$ and get $X_1 = \mathbb{V}(f_1) \subseteq \mathbb{A}^2$ where

$$f_1 = z - (x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z).$$

Its partial derivative with respect to $z$ is given by

$$\frac{\partial f_1}{\partial z} = 1 + \lambda_1(x - \lambda_2 z)(x - \lambda_3 z) + \lambda_2(x - \lambda_1 z)(x - \lambda_3 z) + \lambda_3(x - \lambda_1 z)(x - \lambda_2 z).$$

It is clear that at the point $p = (0, 0)$, we have $\frac{\partial f_1}{\partial z}(p) = 1 \neq 0$. Therefore $p = (0, 0)$ is a non-singular point of $X_1$, hence $p = [0 : 1 : 0]$ is a non-singular point of $X$. This holds in all the three cases. We have the following conclusion:

(1) If $\lambda_1$, $\lambda_2$ and $\lambda_3$ are distinct, $X$ is non-singular.

(2) If two of the three are equal, say, $\lambda_1 = \lambda_2 \neq \lambda_3$, then $X$ has a unique singular point $[\lambda_1 : 0 : 1]$.

(3) If all the three are equal, then $X$ has a unique singular point $[\lambda_1 : 0 : 1]$.

**Solution 7.4.** *Example: projective twisted cubic.* We first consider the standard affine piece $Y_0 = Y \cap U_0$. By settin $z_0 = 1$ we get

$$Y_0 = \mathbb{V}_a(y_2 - y_1^2, y_1 y_3 - y_2^2, y_3 - y_1 y_2).$$

To find the dimension of the tangent space at any point $p = (y_1, y_2, y_3)$, we consider the matrix of partial derivatives:

$$M_p = \begin{pmatrix} -2y_1 & 1 & 0 \\ y_3 & -2y_2 & y_1 \\ -y_2 & -y_1 & 1 \end{pmatrix}.$$

We need to find $\operatorname{rank} M_p$. First we compute the determinant of $M_p$:

$$\det M_p = 4y_1 y_2 - y_1 y_2 - y_3 - 2y_1^3 = 4y_1 y_2 - y_1 y_2 - y_1 y_2 - 2y_1 y_2 = 0.$$

Therefore $\operatorname{rank} M_p \leqslant 2$. Notice that the first and third rows of $M_p$ are linearly independent (or the second and third columns). Therefore $\operatorname{rank} M_p = 2$, which implies $\dim T_p Y_0 = 1$ at every $p \in Y_0$. It follows that $Y_0$ is non-singular and $\dim Y = \dim Y_0 = 1$.

Now we consider the points in $Y \backslash Y_0$. Let $p = [y_0 : y_1 : y_2 : y_3]$ be such a point, then $y_0 = 0$, which implies $y_1^2 = y_0 y_2 = 0$ and $y_2^2 = y_1 y_3 = 0$. Therefore the only point $p \in Y \backslash Y_0$ is given by $p = [0 : 0 : 0 : 1]$. To determine whether $p$ is a singular point, we need to look at the standard affine piece $Y_3 = Y \cap U_3$. We could perform a similar calculation as above to show that $Y_3$ is non-singular. More precisely, we have

$$Y_3 = \mathbb{V}_a(y_0 y_2 - y_1^2, y_1 - y_2^2, y_0 - y_1 y_2).$$

For any point $q = (y_0, y_1, y_2) \in Y_3$, the matrix

$$M_q = \begin{pmatrix} y_2 & -2y_1 & y_0 \\ 0 & 1 & -2y_2 \\ 1 & -y_2 & -y_1 \end{pmatrix}.$$

We notice that

$$\det M_q = -y_1 y_2 + 4y_1 y_2 - y_0 - 2y_2^3 = -y_1 y_2 + 4y_1 y_2 - y_1 y_2 - 2y_1 y_2 = 0.$$

Therefore $\operatorname{rank} M_q \leqslant 2$. Moreover the second and the third rows are linearly independent, hence $\operatorname{rank} M_q = 2$ for every $q \in Y_3$. It follows that $Y_3$ is non-singular. To summarise, $Y$ is non-singular and has dimension 1.

## 8. Algebraic Curves

We study plane curves of degree up to 3.

8.1. **Lines and conics.** From now on we focus on plane curves.

**Definition 8.1.** A *plane curve* is a hypersurface $C = \mathbb{V}(f) \subseteq \mathbb{P}^2$ for some non-constant homogeneous polynomial $f \in \Bbbk[x, y, z]$ without repeated factors. The *degree* of $C$ is defined to be $\deg f$. Plane curves of degrees 1, 2, 3 and 4 are called *lines*, *conics*, *cubics* and *quartics* respectively.

**Example 8.2.** Let $[x : y : z]$ be the homogeneous coordinates in $\mathbb{P}^2$. Every line is defined by a polynomial $f(x, y, z) = ax + by + cz$ for some $a, b, c \in \Bbbk$ which are not simultaneously zero. A line is always irreducible.

**Example 8.3.** Every conic is defined by a non-zero polynomial of the form $g(x, y, z) = ax^2 + 2bxy + cy^2 + 2dxz + 2eyz + fz^2$. It is sometimes more convenient to write it in the matrix form

$$g(x, y, z) = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

We consider the factorisation of $g$ into irreducibles. By Exercise 4.2 (1), each irreducible factor of $g$ is also homogeneous. There are three cases:

(1) If $g$ is an irreducible polynomial, then $\mathbb{V}(g)$ is an irreducible conic;

(2) If $g = g_1 g_2$ for coprime irreducible homogeneous polynomials $g_1$ and $g_2$ of degree 1, then $\mathbb{V}(g) = \mathbb{V}(g_1) \cup \mathbb{V}(g_2)$ is the union of two distinct lines;

(3) If $g = g_0^2$ for an irreducible homogeneous polynomial $g_0$ of degree 1. Since $g$ has repeated factors, $\mathbb{V}(g)$ is not a conic. Instead, $\mathbb{V}(g) = \mathbb{V}(g_0)$ is a line. However, sometimes it is convenient to say that $g$ defines a "double line", just to indicate that the factor $g_0$ is repeated.

**Definition 8.4.** Let $[x : y : z]$ be the homogeneous coordinates of any point in $\mathbb{P}^2$. For a fixed $3 \times 3$ invertible matrix $A$, define a new set of coordinates $[x' : y' : z']$ by the equation

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

This is called the *linear change of homogeneous coordinates* defined by $A$.

*Remark* 8.5. Why it makes sense: Multiplication of $[x : y : z]$ by any scalar $\lambda \in \Bbbk \backslash \{0\}$ results in the multiplication of $[x' : y' : z']$ by the same scalar $\lambda$, and $x', y', z'$ cannot be all 0 unless $x, y, z$ are all zero since $A$ is nonsingular. So $[x' : y' : z']$ are a new system of homogeneous coordinates for points in the projective plane. Why we care: We can often reduce the defining equation of a curve to a very simple form by choosing a new system of coordinates.

**Lemma 8.6.** *Every line in $\mathbb{P}^2$ can be written as $\mathbb{V}(x)$ after a suitable linear change of homogeneous coordinates. A non-zero homogeneous polynomial $g(x, y, z) = ax^2 + 2bxy + cy^2 + 2dxz + 2eyz + fz^2$ defines an irreducible conic if and only if the matrix*

$$G = \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}$$

*has rank 3; $g$ defines a union of two lines if and only if $G$ has rank 2; $g$ defines a double line if and only if $G$ has rank 1. Every irreducible conic in $\mathbb{P}^2$ can be written as $\mathbb{V}(xz - y^2)$ after a suitable linear change of homogeneous coordinates.*

*Proof.* Non-examinable. The proof follows from the Gram-Schmidt orthogonalisation in linear algebra. □

**Proposition 8.7.** *A line (or an irreducible conic) is isomorphic to $\mathbb{P}^1$, hence is rational.*

*Proof.* By Lemma 8.6, we can assume the line is $\mathbb{V}(x)$ and the conic is $\mathbb{V}(xz - y^2)$ without loss of generality. The case of a line is easy; we leave the details to the reader. The case of a conic was proved in Example 5.23. □

The following results are special cases of a famous theorem.

**Theorem 8.8.** *Let $L$ be a line and $D$ a plane curve of degree $d$. If $L$ is not a component of $D$, then $L \cap D$ has at most $d$ distinct points. When counting with multiplicities, $L$ and $D$ meet in precisely $d$ points.*

*Proof.* Assume $L = \mathbb{V}(ax + by + cz)$ where $a$, $b$ and $c$ are not simultaneously zero. Without loss of generality, we can assume $c \neq 0$. Then a point $p \in L$ can be written as $p = [x : y : -\frac{a}{c}x - \frac{b}{c}y]$. Assume $D = \mathbb{V}(f)$ where $f(x, y, z)$ is a non-zero homogeneous polynomial of degree $d$. Then $p \in D$ if and only if $f\left(x, y, -\frac{a}{c}x - \frac{b}{c}y\right) = 0$. The left-hand side is a homogeneous polynomial of degree $d$ in $x$ and $y$. By Exercise 4.4 (2), it can be factored into a product of $d$ homogeneous factors of degree 1 as

$$f\left(x, y, -\frac{a}{c}x - \frac{b}{c}y\right) = (r_1x + s_1y) \cdots (r_dx + s_dy) = 0.$$

Each factor $r_ix + s_iy$ determines a solution $[x : y] = [-s_i : r_i]$ which gives point $p_i = [-s_i : r_i : \frac{a}{c}s_i - \frac{b}{c}r_i] \in L \cap D$. Some of these points may be the same, so $L$ and $D$ meet in at most $d$ points. When counting with the number of times each distinct point occurs as a solution, we have precisely $d$ points. □

*Remark* 8.9. If $p \in L \cap D$ occurs $m$ times as a solution, then we say $L$ and $D$ meet at $p$ with *multiplicity* $m$. The current proof provides a systematic method to compute all intersection points of a line and a curve with multiplicities.

*Remark* 8.10. We briefly explain what it means by saying $L$ is not a component of $D$. For example, if $D$ is a conic, it could be the union of two lines. If $L$ happens to be one of them, then $L$ and $D$ meet in more than $d$ points, indeed, infinitely many points. The theorem indicates that if $L$ and $D$ meet in more than $d$ points, then $L$ must be a component of $D$.

**Proposition 8.11.** *Let $D$ be an irreducible non-singular plane curve of degree $d \geqslant 2$. For any point $p \in D$, the tangent line $T_pD$ and $D$ meet at $p$ with multiplicity at least 2.*

*Proof.* Non-examinable. But we will see some examples in exercises. □

**Theorem 8.12.** *Let $C$ be a conic and $D$ a plane curve of degree $d$. If $C$ and $D$ have no common component, then $C \cap D$ has at most $2d$ distinct points. When counting with multiplicities, $C$ and $D$ meet in precisely $2d$ points.*

*Proof.* Similar to the proof of Theorem 8.8. We leave it as an exercise. □

The more general version of the theorem is the following

**Theorem 8.13** (Bézout's Theorem)**.** *Let $D_1$ and $D_2$ be plane curves of degree $d_1$ and $d_2$ respectively. Assume $D_1$ and $D_2$ have no common component, then $D_1$ and $D_2$ meet in at most $d_1d_2$ distinct points. When these points are counted with multiplicities, $D_1$ and $D_2$ meet in precisely $d_1d_2$ points.*

*Proof.* Non-examinable. Interested reader can find the proof in [Section 5.3, Fulton, Algebraic Curves]. □

*Remark* 8.14. This theorem shows that the number of intersection points of two plane curves can be read off easily from their defining equations without solving them, which is a big advantage for projective spaces. A special case of this theorem is Exercise 4.3 (2), when both plane curves have degree 1. In the other direction, this theorem can be generalised in many different ways, thus has become the starting point of a major branch of algebraic geometry, called *intersection theory*.

8.2. **Cubics.** Now we consider cubic curves. We first give a classification.

**Example 8.15.** Every cubic curve is defined by a non-zero homogeneous polynomial $f \in \Bbbk[x, y, z]$ of degree 3. By Exercise 4.2 (1), each irreducible factor of $f$ is also homogeneous. There are a few cases:

(1) If $f$ is an irreducible polynomial, then $\mathbb{V}(f)$ is an irreducible cubic;

(2) If $f$ is the product of two irreducible factors of degree 1 and 2 respectively, then the cubic $\mathbb{V}(f) = L \cup C$ is the union of a line $L$ and a conic $C$ (in this case we still say $\mathbb{V}(f)$ is singular, although we have not discussed the singularity of reducible algebraic sets);

(3) If $f$ is the product of three irreducible factors of degree 1, then $\mathbb{V}(f)$ could be the union of three distinct lines, or the union of a single line and a double line, or a triple line. The union of three distinct lines is a cubic. The other two are not.

We have seen that there is only one line and one irreducible conic up to linear changes of homogeneous coordinates. The situation is different for irreducible cubics.

**Lemma 8.16.** *Up to a linear change of homogeneous coordinates, every irreducible cubic curve $C$ can be written in one of the following three forms*

(1) $C_0 = \mathbb{V}_p\left(y^2z - x(x-z)(x-\lambda z)\right)$ *for some* $\lambda \in \Bbbk\backslash\{0, 1\}$;

(2) $C_1 = \mathbb{V}_p\left(y^2z - x^2(x-z)\right)$;

(3) $C_2 = \mathbb{V}_p\left(y^2z - x^3\right)$.

*Proof.* Non-examinable. □

*Remark* 8.17. The defining equations in Lemma 8.16 are called the *normal forms* of irreducible cubics. By Exercise 6.2, we see that these formulas do give irreducible cubics. Moreover, by Exercise 7.3, $C_0$ is always non-singular; $C_1$ is singular at the point $[0 : 0 : 1]$, where $C_1$ intersects with itself; $C_2$ is singular at the point $[0 : 0 : 1]$, where $C_2$ has a corner. They are known respectively as an *non-singular cubic*, the *nodal cubic* and the *cuspidal cubic*. Each of them can be understood as the projective closure of the corresponding affine variety $\mathbb{V}_a(y^2 - x(x-1)(x-\lambda))$ or $\mathbb{V}_a(y^2 - x^2(x-1))$ or $\mathbb{V}_a(y^2 - x^3)$, with the only point at infinity $[0 : 1 : 0]$.

**Proposition 8.18.** *A nodal cubic curve (or a cuspidal cubic curve) is rational.*

*Proof.* To show a nodal cubic is rational, by Lemma 8.16, we can assume the nodal cubic is $C_1 = \mathbb{V}\left(y^2z - x^2(x-z)\right)$ without loss of generality. Consider the rational maps

$$\begin{aligned} \varphi_1 : &\quad \mathbb{P}^1 \dashrightarrow C_1; \quad [u : v] \longmapsto [u(u^2+v^2) : v(u^2+v^2) : u^3] \\ \psi_1 : &\quad C_1 \dashrightarrow \mathbb{P}^1; \quad [x : y : z] \longmapsto [x : y]. \end{aligned}$$

We will verify they are rational maps and they are inverse to each other. They are both given by homogeneous polynomials of the same degree. Moreover, $\varphi_1$ is defined, for example, at the point $[1 : 0]$; $\psi_1$ is defined, for example, at the point $[0 : 1 : 0]$. The image of $\psi_1$ is always in $\mathbb{P}^1$. To verify the image of $\varphi_1$ is in $C$, one just needs to compute

$$[v(u^2+v^2)]^2[u^3] - [u(u^2+v^2)]^2[u(u^2+v^2) - u^3] = v^2(u^2+v^2)^2u^3 - u^2(u^2+v^2)^2uv^2 = 0.$$

Finally we show they are inverse to each other. For any point $[x : y : z] \in C_1$, we have

$$(\varphi_1 \circ \psi_1)([x : y : z]) = \varphi_1([x : y]) = [x(x^2+y^2) : y(x^2+y^2) : x^3].$$

By the equation of $C_1$ we know $y^2z - x^2(x-z) = 0$, which implies $x^3 = (x^2+y^2)z$. Therefore

$$[x(x^2+y^2) : y(x^2+y^2) : x^3] = [x(x^2+y^2) : y(x^2+y^2) : z(x^2+y^2)] = [x : y : z].$$

Moreover, for any point $[u : v] \in \mathbb{P}^1$, we have

$$(\varphi_1 \circ \psi_1)([u : v]) = \varphi_1([u(u^2+v^2) : v(u^2+v^2) : u^3]) = [u(u^2+v^2) : v(u^2+v^2)] = [u : v].$$

This shows that $C_1$ is birational to $\mathbb{P}^1$, hence $C_1$ is rational.

To show a cuspidal cubic is rational, by Lemma 8.16, we can assume the cuspidal cubic is $C_2 = \mathbb{V}\left(y^2z - x^3\right)$ without loss of generality. Consider the rational maps

$$\begin{aligned} \varphi_2 : \quad & \mathbb{P}^1 \dashrightarrow C_2; \quad [u:v] \longmapsto [uv^2 : v^3 : u^3]; \\ \psi_2 : \quad & C_2 \dashrightarrow \mathbb{P}^1; \quad [x:y:z] \longmapsto [x:y]. \end{aligned}$$

A similar proof shows $C_2$ is rational. We leave the details as an exercise. □

**Proposition 8.19.** *A non-singular cubic curve is not rational.*

*Proof.* Non-examinable. The idea is to show that the function field of a non-singular cubic is not isomorphic to that of $\mathbb{P}^1$. Interested reader can find the proof in [Section 2.2, Reid, Undergraduate Algebraic Geometry]. This is a fun proof. The method in the proof is called "infinite descent". There are a few famous applications of this method in the history of mathematics. It was used to prove that $\sqrt{2}$ is not a rational number, which unfortunately caused the first crisis in the foundations of mathematics. This crisis led to the discovery of irrational numbers, which was a big step forward in the development of mathematics. Another famous application of the descent method was in the proof of Fermat's last theorem. Fermat conjectured that the equation $x^m + y^m = z^m$ has no solutions in positive integers for any positive integer $m \geqslant 3$. The proof of the theorem in $m = 3$ and $m = 4$ cases was given by the descent method shortly after that. But it took mathematicians more than 300 years to completely solve the problem. The Andrew Wiles Building in University of Oxford was named after the British mathematician who finally proved this conjecture. □

Finally we look at some special points on a non-singular cubic.

**Definition 8.20.** Given a non-singular cubic curve $C$, a point $p \in C$ is said to be an *inflection point* of $C$ if the tangent line $T_pC$ meets $C$ at $p$ with multiplicity 3.

*Remark* 8.21. Recall from Proposition 8.11 that $T_pC$ meets $C$ at $p$ with multiplicity at least 2. By Theorem 8.8, if $p$ is an inflection point, then $p$ is the only intersection point of $T_pC$ and $C$; if $p$ is not an inflection point, then $T_pC$ and $C$ meet at another point with multiplicity 1.

**Example 8.22.** We show that the point $p = [0:1:0]$ is an inflection point on the non-singular cubic $C = \mathbb{V}_p(f)$ where $f = y^2z - x^3 + xz^2$. First of all we need to find out the tangent line $T_pC$, which can be computed on the standard affine piece $C_1 = C \cap U_1 = \mathbb{V}_a(f_1)$ where $f_1 = z - x^3 + xz^2$. The non-homogeneous coordinates of $p$ in $U_1$ is $p = (0,0)$. Since $\frac{\partial f_1}{\partial x} = -3x^2 + z^2$ and $\frac{\partial f_1}{\partial z} = 1 + 2xz$, the tangent line $T_pC_1 = \mathbb{V}_a(0(x-0) + 1(z-0)) = \mathbb{V}_a(z)$. Its projective closure is $T_pC = \mathbb{V}_p(z)$. To find the intersection points of $C$ and $T_pC$, we follow the method in the proof of Theorem 8.8. A point on $T_pC$ is given by $[x:y:0]$. It lies in $C$ if and only if $f(x,y,0) = 0$, where $f(x,y,0) = -x^3$ which has one solution $[x:y] = [0:1]$ with multiplicity 3. Therefore $T_pC$ and $C$ meet at the point $[0:1:0]$ with multiplicity 3, which proves $p = [0:1:0]$ is an inflection point on $C$.

## Exercise Sheet 8

*This sheet will be discussed in the exercise class on 27 November. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 8.1.** *Examples of rational curves.* Complete proofs of Propositions 8.7 and 8.18.

(1) Show that $L = \mathbb{V}(z) \subseteq \mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$. Conclude that $L$ is rational.

(2) Show that $\varphi_2$ and $\psi_2$ defined in the proof of Proposition 8.18 are rational maps. Show that they are mutually inverse to each other. Conclude that the cuspidal cubic curve $C_2 = \mathbb{V}(y^2z - x^3) \subseteq \mathbb{P}^2$ is rational.

**Exercise 8.2.** *Example: Fermat cubic.* Consider the cubic curve $C = \mathbb{V}(x^3 + y^3 + z^3) \subseteq \mathbb{P}^2$.

(1) Show that $C$ is non-singular.

(2) Show that the line $L = \mathbb{V}(z)$ meets $C$ at 3 distinct points. Find all of them.

(3) For any $p = [a : b : c] \in C$, show that the tangent line $T_pC = \mathbb{V}(a^2x + b^2y + c^2z)$.

(4) Show that every point you find in part (2) is an inflection point.

**Exercise 8.3.** *Bézout's theorem for conics.* Prove Theorem 8.12 in these steps.

(1) If the conic $C = L_1 \cup L_2$ is the union of two lines, use Theorem 8.8 to conclude that $C \cap D$ comprises at most $2d$ distinct points; or precisely $2d$ points when multiplicities are counted. (*Remark:* if $L_1 \cap D$ and $L_2 \cap D$ have a common point $p$, the multiplicity at $p$ is defined to be the sum of the two multiplicities at $p$.)

(2) If the conic $C$ is irreducible, without loss of generality, we can assume $C = \mathbb{V}(xz - y^2)$ by Lemma 8.6. We have proved in Example 5.23 that every point in $C$ can be given by $[p^2 : pq : q^2]$ for some $[p : q] \in \mathbb{P}^1$. Use the method in the proof of Theorem 8.8 to finish the proof.

**Exercise 8.4.** *An interesting application of Bézout's theorem.* Let $p_1, \cdots, p_5 \in \mathbb{P}^2$ be distinct points, and assume that no 4 of them are on the same line. Prove that there exists exactly one conic through all 5 points. You can follow these steps.

(1) Show that there exists at least one conic through all 5 points. (*Hint:* rank-nullity.)

(2) Suppose there are two distinct conics $C_1$ and $C_2$ through all 5 points. Use Bézout's theorem to conclude that they have a common component.

(3) If one of them is an irreducible conic, which has only one component, then the other must be the same irreducible conic, otherwise they cannot have a common component. Therefore both conics must be unions of two lines. Explain why we can assume $C_1 = L_0 \cup L_1$ and $C_2 = L_0 \cup L_2$ for distinct lines $L_0$, $L_1$ and $L_2$. Explain why this leads to a contradiction.

## Solutions to Exercise Sheet 8

**Solution 8.1.** *Examples of rational curves.*

(1) We claim that $\varphi : \mathbb{P}^1 \longrightarrow L;\ [x : y] \longmapsto [x : y : 0]$ is a morphism. It is given by homogeneous polynomials of the same degree, and is everywhere defined, since $x$ and $y$ cannot be both zero. The image of any point under $\varphi$ lies in $L$ because the last coordinate is zero. This justifies the claim. Similarly we claim that $\psi : L \longrightarrow \mathbb{P}^1;\ [x : y : z] \longmapsto [x : y]$ is a morphism. It is given by homogeneous polynomials of the same degree. Since $z = 0$, $x$ and $y$ cannot be both zero, hence it is defined for every point in $L$. The image of any point in $L$ under $\varphi$ is clearly in $\mathbb{P}^1$. This justifies the claim. Finally we check $\varphi$ and $\psi$ are inverse to each other. For any point $[x : y] \in \mathbb{P}^1$, $(\psi \circ \varphi)([x : y]) = \psi([x : y : 0]) = [x : y]$. For any point $[x : y : z] \in L$, $(\varphi \circ \psi)([x : y : z]) = \varphi([x : y]) = [x : y : 0] = [x : y : z]$ since $z = 0$. Therefore $L$ is isomorphic to $\mathbb{P}^1$. In particular, they are birational, hence $L$ is rational.

(2) Define rational maps $\varphi_2 : \mathbb{P}^1 \dashrightarrow C_2$ by $\varphi_2([u : v]) = [uv^2 : v^3 : u^3]$ and $\psi_2 : C_2 \dashrightarrow \mathbb{P}^1$ by $\psi_2([x : y : z]) = [x : y]$. To show $\varphi_2$ is a rational map, we observe: all components are homogeneous of degree 3; $\varphi_2$ is defined at every point $[u : v] \in \mathbb{P}^1$ since either $u^3$ or $v^3$ is non-zero; the image $[uv^2 : v^3 : u^3]$ is a point in $C_2$ since it satisfies the defining equation of $C_2$. To show $\psi_2$ is a rational map, we observe: all components are homogeneous of degree 1; $\psi_2$ is well-defined at every point on $C_2$ except $[0 : 0 : 1]$; image of $\psi_2$ is clearly in $\mathbb{P}^1$. It remains to show $\varphi_2$ and $\psi_2$ are mutually inverse to each other. For every $[u : v] \in \mathbb{P}^1$ where $\psi_2 \circ \varphi_2$ is defined, we have $(\psi_2 \circ \varphi_2)([u : v]) = \psi_2([uv^2 : v^3 : u^3]) = [uv^2 : v^3] = [u : v]$. For every $[x : y : z] \in C$ where $\varphi_2 \circ \psi_2$ is defined, we have $(\varphi_2 \circ \psi_2)([x : y : z]) = \varphi_2([x : y]) = [xy^2 : y^3 : x^3] = [xy^2 : y^3 : y^2z] = [x : y : z]$. Therefore $C_2$ is birational to $\mathbb{P}^1$, hence is rational.

**Solution 8.2.** *Example: Fermat cubic.*

(1) We consider the standard affine piece $C_0 = C \cap U_0 = \mathbb{V}_a(f_0) \subseteq \mathbb{A}^2$ where $f_0 = 1 + y^3 + z^3$. Since $\frac{\partial f_0}{\partial y} = 3y^2$ and $\frac{\partial f_0}{\partial z} = 3z^2$, the two derivatives vanish if and only if $y = z = 0$. But then $f_0 = 1 \neq 0$. Therefore $f_0 = \frac{\partial f_0}{\partial y} = \frac{\partial f_0}{\partial z} = 0$ have no common solution, which means $C_0$ is non-singular. Since the equation of $C$ is symmetric with respect to the variables, the same calculation shows that all other standard affine pieces are also non-singular. Therefore $C$ is non-singular.

(2) A point on the line $L$ can be given by $p = [x : y : 0]$. If $p \in C$, then we have $x^3 + y^3 = 0$, hence $y = -x$ or $-\omega x$ or $-\omega^2 x$ where $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$ is a primitive third root of unity. So the three points in $L \cap C$ are $p_1 = [1 : -1 : 0]$, $p_2 = [1 : -\omega : 0]$ and $p_3 = [1 : -\omega^2 : 0]$.

(3) At least one of the three coordinates is non-zero. Without loss of generality, we can assume $a \neq 0$. Then the point $p = [a : b : c] \in C_0 = C \cap U_0 = \mathbb{V}_a(f_0) \subseteq \mathbb{A}^2$, in which its non-homogeneous coordinates are given by $p = (\frac{b}{a}, \frac{c}{a})$. The tangent space of $p$ in the standard affine piece $C_0$ is given by

$$T_pC_0 = \mathbb{V}_a\left(3 \cdot \frac{b^2}{a^2} \cdot (y - \frac{b}{a}) + 3 \cdot \frac{c^2}{a^2} \cdot (z - \frac{c}{a})\right).$$

The tangent space $T_pC$ is the projective closure of $T_pC_0$, which is given by the homogenisation of the above polynomial

$$T_pC = \mathbb{V}_p\left(3 \cdot \frac{b^2}{a^2} \cdot (y - \frac{b}{a}x) + 3 \cdot \frac{c^2}{a^2} \cdot (z - \frac{c}{a}x)\right).$$

Since we assumed $a \neq 0$, we can multiply this polynomial by $\frac{a^3}{3}$ without changing its vanishing locus. Then we get

$$\begin{aligned} T_pC &= \mathbb{V}_p(b^2(ay - bx) + c^2(az - cx)) \\ &= \mathbb{V}_p((-b^3 - c^3)x + ab^2y + ac^2z) \\ &= \mathbb{V}_p(a^3x + ab^2y + ac^2z) \\ &= \mathbb{V}_p(a^2x + b^2y + c^2z). \end{aligned}$$

In the last step above is valid since we assumed $a \neq 0$.

Since $a$, $b$ and $c$ are symmetric, a similar calculation will give the same equation for the tangent space $T_pC$ when $b \neq 0$ or $c \neq 0$.

(4) At the point $p_1 = [1 : -1 : 0]$, the tangent space $T_{p_1}C = \mathbb{V}_p(x + y)$. For any point $q = [x : y : z] \in T_{p_1}C$, we have $x = -y$. If $q \in C$, we then have $(-y)^3 + y^3 + z^3 = 0$ hence $z^3 = 0$, which has one solution with multiplicity 3. This means $T_{p_1}C$ meet $C$ at one point with multiplicity 3, hence $p_1$ is an inflection point.

Similarly, at the point $p_2 = [1 : -\omega : 0]$, the tangent space $T_{p_2}C = \mathbb{V}_p(x + \omega^2 y)$. For any point $q = [x : y : z] \in T_{p_2}C$, we have $x = -\omega^2 y$. If $q \in C$, we then have $(-\omega^2 y)^3 + y^3 + z^3 = 0$ hence $z^3 = 0$, which has one solution with multiplicity 3. This means $T_{p_2}C$ meet $C$ at one point with multiplicity 3, hence $p_2$ is an inflection point.

Moreover, at the point $p_3 = [1 : -\omega^2 : 0]$, the tangent space $T_{p_3}C = \mathbb{V}_p(x + \omega y)$. For any point $q = [x : y : z] \in T_{p_3}C$, we have $x = -\omega y$. If $q \in C$, we then have $(-\omega y)^3 + y^3 + z^3 = 0$ hence $z^3 = 0$, which has one solution with multiplicity 3. This means $T_{p_3}C$ meet $C$ at one point with multiplicity 3, hence $p_3$ is an inflection point.

**Solution 8.3.** *Bézout's theorem for conics.*

(1) If $C = L_1 \cup L_2$, then every common point of $C$ and $D$ must be either a common point of $L_1$ and $D$, or a common point of $L_2$ and $D$. We know by Theorem 8.8 that $L_1 \cap D$ comprises at most $d$ points, or precisely $d$ points when counting with multiplicities; $L_2 \cap D$ comprises at most $d$ points, or precisely $d$ points when counting with multiplicities. Therefore $C \cap D$ comprises at most $2d$ points, or precisely $2d$ points when counting with multiplicities.

(2) We have proved in Example 5.23 that $C$ is isomorphic to $\mathbb{P}^1$. In particular, every point in $C$ can be given by $[p^2 : pq : q^2]$ for some $[p : q] \in \mathbb{P}^1$. Let $D = \mathbb{V}(f)$ for some homogeneous polynomial $f(x, y, z)$ of degree $d$. Then $[p^2 : pq : q^2] \in \mathbb{V}(f)$ if and only if $f(p^2, pq, q^2) = 0$. The left-hand side is a homogeneous polynomial of degree $2d$ in $p$ and $q$. By Exercise 4.4 (2), it can be completely factored into $2d$ homogeneous factors of degree 1 as

$$f(p^2, pq, q^2) = (a_1p + b_1q) \cdots (a_{2d}p + b_{2d}q) = 0.$$

Each factor $a_ip + b_iq$ determines a point $[p : q] = [b_i : -a_i] \in \mathbb{P}^1$, hence $f = 0$ has at most $2d$ solutions $[p : q] = [b_i : -a_i] \in \mathbb{P}^1$, which give at most $2d$ points $[p^2 : pq : q^2] = [b_i^2 : -a_ib_i : a_i^2] \in (C \cap D)$. When counting the number of times each point occurs as a solution, we get precisely $2d$ points.

**Solution 8.4.** *An interesting application of Bézout's theorem.*

(1) By Example 8.3, every conic $C$ is given by a homogeneous polynomial $g(x, y, z) = 0$ of degree 2 with 6 coefficients $a, b, c, d, e$ and $f$. For each $i$, since $p_i = [x_i : y_i : z_i] \in C$, we can plug in $x = x_i$, $y = y_i$ and $z = z_i$ to get an equation $g(x_i, y_i, z_i) = 0$, which is a homogeneous linear equation in $a, b, c, d, e$ and $f$. In this way the 5 points give a system of 5 linear equations. Since there are 5 equations and 6 indeterminants, by the theorem of rank-nullity, there is a solution for $a, b, c, d, e$ and $f$ such that they are not simultaneously zero. This solution determines the homogeneous polynomial $g(x, y, z)$ of degree 2. We claim that $g$ has no repeated factors. If $g$ has repeated factors, then $g$ is the square of a linear polynomial hence gives a double line which passes through all the 5 given points. This is a contradiction since no 4 of the given points are allowed to be on the same line. Hence we conclude that $g$ defines a conic.

(2) Assume that there are two distinct conics $C_1$ and $C_2$, both of which pass through the 5 points. By Theorem 8.12, if they do not have any common component, then they can meet in at most 4 common points. Hence they must have a common component.

(3) If either $C_1$ or $C_2$ is an irreducible conic, which has only one component, then the other must be the same conic. Under the assumption that $C_1$ and $C_2$ are distinct conics, both of them must be the unions of two lines. Since they have a common component, the other component in the two conics must be distinct. Hence we can assume $C_1 = L_0 \cup L_1$ and $C_2 = L_0 \cup L_2$, where $L_0$, $L_1$ and $L_2$ are distinct lines. We know the 5 points $p_1, \cdots, p_5$ are on both conics. For each $p_i$, there are two possibilities: $p_i \in L_0$, or $p_i \notin L_0$. If the second possibility happens, then $p_i \in L_1$ since $p_i \in C_1$, and $p_i \in L_2$ since $p_i \in C_2$. This implies $p_i$ is a common point of $L_1$ and $L_2$. Since $L_1$ and $L_2$ are distinct lines, by Theorem 8.8, they have only 1 common point. It follows that among the 5 points $p_1, \cdots, p_5$, at most one of them is not on $L_0$; in other words, at least 4 of them are on the line $L_0$. This is a contradiction because no 4 of them are allowed to be on the same line.

## 9. Elliptic Curves

A very special feature of a non-singular cubic curve $C$ is the existence of an abelian group structure on the set of points in $C$. We will see how that works.

9.1. **The group law on non-singular cubics.** Given any non-singular cubic $C$ and any point $O \in C$, there exists an abelian group structure on the set of points in $C$, with $O$ being the identity element in the group law. That means, there is a binary operation "+" defined on the set of points in $C$, which satisfies the conditions required in the definition of an abelian group. The identity element $O$ in the group law is also called the *neutral point*. We will first describe the operation geometrically, then show some explicit computations, finally explain why the construction defines an abelian group structure.

**Construction 9.1** (The group law)**.** Given a non-singular cubic curve $C$ with a point $O \in C$, there is an abelian group law on the set of points on $C$ such that $O$ is the identity element. For any two points $A, B \in C$, their sum $A + B$ is obtained in two steps

(1) The line $AB$ meets the cubic $C$ at a third point $R$;

(2) The line $OR$ meets the cubic $C$ at a third point $\overline{R} = A + B$.

If $A = B$ (resp. $O = R$), then the line $AB$ (resp. $OR$) is defined to be the tangent line $T_A C$ (resp. $T_O C$). □

We can follow the above construction to make explicity computations. In each step, we need to write down the equation of a certain line, and compute its intersection points with the cubic. The reason for the existence of the third intersection point of a line and a cubic and the method for computing it has been discussed in the proof of Theorem 8.8. To find the line $AB$ (or similarly $OR$), we need Definition 7.8 if $A = B$, or the follow simple result if $A \neq B$.

**Lemma 9.2.** *Given two distinct points $A = [a_0 : a_1 : a_2]$ and $B = [b_0 : b_1 : b_2]$ in $\mathbb{P}^2$, there is a unique line $L$ passing through the two points, defined by the polynomial*

$$f(x, y, z) = \det \begin{pmatrix} x & a_0 & b_0 \\ y & a_1 & b_1 \\ z & a_2 & b_2 \end{pmatrix}.$$

*Proof.* We have seen in Exercise 4.3 (1) that there is a unique line $L$ passing through $A$ and $B$. It remains to verify that the given polynoial defines such a line. Notice that the given polynomial is non-zero and homogeneous of degree 1 hence defines a line. When $[x : y : z] = [a_0 : a_1 : a_2]$ or $[b_0 : b_1 : b_2]$, two columns of the matrix are identical hence the determinant is zero. This shows that $A$ and $B$ are points on this line. □

**Example 9.3.** Consider the cubic $C = \mathbb{V}(y^2z - x^3 + 4xz^2 - z^3)$ with the identity element $O = [0 : 1 : 0]$. Take two points $A = [2 : 1 : 1]$ and $B = [-2 : 1 : 1]$ on $C$. By Lemma 9.2, the line $AB$ is defined by

$$\det \begin{pmatrix} x & 2 & -2 \\ y & 1 & 1 \\ z & 1 & 1 \end{pmatrix} = -4y + 4z.$$

By the method in the proof of Theorem 8.8, we can find the third intersection point $R$ of $AB$ and $C$ to be $R = [0 : 1 : 1]$. By Lemma 9.2, the line $OR$ is defined by

$$\det \begin{pmatrix} x & 0 & 0 \\ y & 1 & 1 \\ z & 0 & 1 \end{pmatrix} = x.$$

By the method in the proof of Theorem 8.8, we can find the third intersection point $\overline{R}$ of $OR$ and $C$ to be $\overline{R} = [0 : -1 : 1]$. Therefore $A + B = [0 : -1 : 1]$.

Construction 9.1 works for any non-singular cubic with any point on it as the identity element. In some special cases, the group law becomes particularly nice and simple. This simplified group law is applicable only when the following two conditions are satisfied

(1) The non-singular cubic is given by $C = \mathbb{V}_p(y^2z - x^3 - ax^2z - bxz^2 - cz^3)$ for some $a, b, c \in \Bbbk$, which is the projective closure of the affine curve $C_2 = \mathbb{V}_a(y^2 - x^3 - ax^2 - bx - c)$ with the only point $O = [0 : 1 : 0]$ at infinity;

(2) The point at infinity $O = [0 : 1 : 0]$ is the identity element.

It is important to observe that the graph of $C_2$ is symmetric with respect to the $x$-axis.

**Construction 9.4** (Simplified group law)**.** Let $C = \mathbb{V}_p(y^2z - x^3 - ax^2z - bxz^2 - cz^3)$ be a non-singular cubic for some $a, b, c \in \Bbbk$. Let $O = [0 : 1 : 0]$ be the identity element of the group law and $C_2 = \mathbb{V}_a(y^2 - x^3 - ax^2 - bx - c)$ a standard affine piece of $C$. Given two points $A, B \in C$, we have:

(1) If $A = O$, then $A + B = B$; if $B = O$, then $A + B = A$;

(2) If $A, B \in C_2$, assume the line $AB$ meet the cubic $C$ at a third point $R$. If $A = B$, the line $AB$ is defined to be the tangent line $T_AC$.

   (a) If $A$ and $B$ are symmetric with respect to the $x$-axis, then $A + B = O$;

   (b) Otherwise, let $R = (p, q) \in C_2$, then $\overline{R} = (p, -q) = A + B$. □

*Remark* 9.5. The simplified group law 9.4 also gives an easy way to compute the inverse of any point $A \in C$. If $A = O$, then $-A = O$. Otherwise, let $A = (x, y) \in C_2$, then the inverse $-A = (x, -y) \in C_2$ which is the reflection of $A$ across the $x$-axis.

**Example 9.6.** We look at Example 9.3 again. It is clear that both conditions required for the simplified group law are met. The affine curve $C_2 = \mathbb{V}_a(y^2 - x^3 + 4x - 1)$. Neither $A$ nor $B$ is the identity element $O = [0 : 1 : 0]$. In non-homogeneous coordinates, $A = (2, 1)$ and $B = (-2, 1)$. The line $AB$ in the affine plane is given by $L_2 = \mathbb{V}_a(y - 1)$. Solving the system given by equations $y^2 - x^3 + 4x - 1 = 0$ and $y - 1 = 0$, we get the third point of intersection $R = (0, 1)$. Therefore $A + B = \overline{R} = (0, -1)$, or in homogeneous coordinates $[0 : -1 : 1]$. This answer is consistent with that of Example 9.3.

**Definition 9.7.** A non-singular cubic curve with a chosen point on it (hence a group law is determined) is called an *elliptic curve*.

The theory of elliptic curves is extremely rich and deep, and provides a good example of the profound connections between abstract algebraic geometry, complex analysis, and number theory. It constitutes an active area of current research, and plays a crucial role in the recent proof of Fermat's Last Theorem. Elliptic curves also have important applications in various aspects of cryptography, such as encryption, digital signatures, (pseudo-)random generators and so on. There are other higher dimensional projective varieties, on which there exist abelian group laws. They are called *abelian varieties*, which is also a major branch of algebraic geometry.

9.2. **Linear systems and associativity.** We are aiming to prove that Construction 9.1 does define an abelian group law. The difficulty here is the associativity. We clear up the easy bits first.

**Proposition 9.8.** *In Construction 9.1 of the group law on a non-singular cubic curve $C$: the addition is commutative; $O$ is the identity element; and every point has an inverse.*

*Proof.* For two points $A, B \in C$, there is no difference between the line $AB$ and the line $BA$, hence $A + B = B + A$ is obvious. This justifies the commutativity.

To find $A + O$, the first step gives the third intersection point $R$ of the line $AO$ and $C$; the second step gives the third intersection point of the line $OR$ and $C$, which is $A$. Hence $A + O = A$ is also obvious. This justifies that $O$ is the identity element in the group law.

Given any $A \in C$, we claim its inverse can be given like this: assume the tangent line $T_OC$ meets $C$ at a third point $\overline{O}$, and the line $A\overline{O}$ meets $C$ at a third point $B$, then $B$ is the inverse of $A$. We need to verify $A + B = O$. To compute $A + B$, the first step gives the third intersection point of the line $AB$ and $C$, which is $\overline{O}$; the second step gives the third intersection point of the line $O\overline{O}$ and $C$, which is $O$ by Proposition 8.11. This justifies $A + B = O$, hence the inverse of $A$ is well-defined. □

*Remark* 9.9. Here is a special case that is worth mentioning: if $O$ is an inflection point, then $T_OC$ meet $C$ at $O$ three times hence $\overline{O} = O$. In such a case the inverse of $A$ is simply the third intersection point of the line $AO$ and the curve $C$.

It remains to check the associativity in the group law. This requires some preparation, which is very interesting in their own stand.

*Notation* 9.10. Given finitely many points $P_1, \cdots, P_k \in \mathbb{P}^2$. For every $d \geqslant 0$, we write

$$S_d(P_1, \cdots, P_k) := \left\{ f \in \Bbbk[x, y, z] \;\middle|\; \begin{array}{c} f \text{ is homogeneous of degree } d \\ f(P_1) = \cdots = f(P_k) = 0 \end{array} \right\}.$$

It is easy to see that $S_d(P_1, \cdots, P_k)$ is a vector space over $\Bbbk$, as it is closed under addition and scalar multiplication. This vector space is sometimes called a *linear system*, but we do not need this terminology. In the following results we will need to look at $S_3(P_1, \cdots, P_8)$.

**Lemma 9.11.** *Let $C_1$ and $C_2$ be two cubic curves whose intersection consists of precisely 9 distinct points $P_1, \cdots, P_9$. Then $\dim_{\Bbbk} S_3(P_1, \cdots, P_8) = 2$.*

*Proof.* Non-examinable. We do not prove it but we explain what the proof is really about. It is easy to find out that a homogeneous polynomial $f \in \Bbbk[x, y, z]$ of degree 3 is determined by 10 coefficients. For each given point $P_i$, the requirement $f(P_i) = 0$ imposes one linear condition on the coefficients of $f$. If all the 8 linear conditions on the coeffcients are independent, then the remaining freedom in the coefficient is 2, which is precisely what we need. Therefore the whole point is to show that these linear conditions are guaranteed to be independent given the assumptions. The key ingredient in the proof is Bézout's Theorem 8.13. Interested reader can find the proof in [Proposition 2.6, Reid, Undergraduate Algebraic Geometry]. □

**Lemma 9.12.** *Let $C_1 = \mathbb{V}(F_1)$ and $C_2 = \mathbb{V}(F_2)$ be two cubic curves whose intersection consists of precisely 9 distinct points $P_1, \cdots, P_9$. Then any cubic curve $D = \mathbb{V}(G)$ through $P_1, \cdots, P_8$ also passes through $P_9$.*

*Proof.* By Lemma 9.11, we have $\dim_{\Bbbk} S_3(P_1, \cdots, P_8) = 2$. It is clear that $F_1, F_2 \in S_3(P_1, \cdots, P_8)$. Moreover $F_1$ and $F_2$ are linearly independent, as otherwise they would define the same cubic. Therefore $F_1$ and $F_2$ form a basis of $S_3(P_1, \cdots, P_8)$. Since $G \in S_3(P_1, \cdots, P_8)$, we can write $G = \lambda_1 F_1 + \lambda_2 F_2$ for some $\lambda_1, \lambda_2 \in \Bbbk$. Now $G(P_9) = \lambda_1 F_1(P_9) + \lambda_2 F_2(P_9) = 0$, hence $D$ passes through $P_9$. □

Now we are ready to prove the associativity. To avoid excessive technicality while still keeping a grasp of the main idea in the proof, we will prove it under an extra mild assumption, which will be stated in the proof. Some extra work will be required if this assumption is not met, which we do not discuss.

**Proposition 9.13.** *In Construction 9.1 of the group law on a non-singular cubic curve $C$, the addition is associative.*

*Proof.* Let $A, B, E \in C$. The construction of $(A + B) + E = \overline{S}$ uses 4 lines:

$$L_1 : ABR; \quad L_2 : RO\overline{R}; \quad L_3 : E\overline{R}S; \quad L_4 : SO\overline{S}.$$

The construction of $A + (B + E) = \overline{T}$ uses 4 lines:

$$M_1 : BEQ; \quad M_2 : QO\overline{Q}; \quad M_3 : A\overline{Q}T; \quad M_4 : TO\overline{T}.$$

We need to show $\overline{S} = \overline{T}$, for which it suffices to show $S = T$. We consider two cubics

$$D_1 = L_1 \cup M_2 \cup L_3 \qquad \text{and} \qquad D_2 = M_1 \cup L_2 \cup M_3.$$

Then by construction we have

$$C \cap D_1 = \{A, B, E, O, R, \overline{R}, Q, \overline{Q}, S\};$$
$$C \cap D_2 = \{A, B, E, O, R, \overline{R}, Q, \overline{Q}, T\}.$$

Now we need a mild assumption that the 9 points in $C \cap D_1$ are distinct. Then the two cubics $C$ and $D_1$ satisfy the conditions of Lemma 9.12. Since the cubic $D_2$ passes through 8 of the 9 points, it must pass through $S$ as well, which means $S \in C \cap D_2$. Therefore $S = T$ since $S$ cannot be any of the other points by the mild assumption that we imposed. This finishes the proof under this assumption. Extra work has to be done when this assumption is not met. □

*Remark* 9.14. This is a very beautiful piece of argument in projective algebraic geometry. Bézout's theorem plays a key role in the course of the proof, mostly in the proof of Lemma 9.11. A similar argument can be used to prove many other results, including the famous Pascal's theorem (aka the mystic hexagon), which we will see in the exercise.

## Exercise Sheet 9

*This sheet will be discussed in the exercise class on 4 December. You are welcome to submit your solutions at the end of the exercise class or anytime earlier.*

**Exercise 9.1.** *Example: understanding the simplified group law.*

(1) Show that $[0:1:0]$ is an inflection point of $C$ in the simplified group law 9.4.

(2) In the simplified group law 9.4, explain briefly how to find all points $P \in C$ such that $P+P=O$.

(3) Consider the curve and the group law in Example 9.6. Let $A=[2:1:1]$ and $B=[-2:-1:1]$. Use the simplified group law to find out $-A$, $-B$ and $A+B$.

**Exercise 9.2.** *Example of group law.* Consider the non-singular cubic curve $C=\mathbb{V}(y^2z-x^3-4xz^2)\subseteq \mathbb{P}^2$. Let $O=[0:1:0]$ be the identity element in the group law.

(1) Find all points where $C$ meets the line $L_1=\mathbb{V}(z)$ and specify their multiplicities. Do the same for the lines $L_2=\mathbb{V}(x)$ and $L_3=\mathbb{V}(y-2x)$.

(2) Find the order of the subgroup generated by the point $P=[2:4:1]\in C$.

(3) Find all points $Q\in C$ such that $Q+Q=O$.

**Exercise 9.3.** *Example: Tate's normal form.* Consider the projective closure $C$ of the cubic curve $C_2=\mathbb{V}(y^2+sxy-ty-x^3+tx^2)\subseteq \mathbb{A}^2$ for some fixed $s,t\in \Bbbk$ where $t\neq 0$. Assume $C$ is non-singular. Let the point at infinity $O=[0:1:0]$ be the identity element in the group law on $C$.

(1) For any point $P=(a,b)\in C_2$, show that $-P=(a,-b-sa+t)$ in the group law.

(2) Suppose $Q=(0,0)\in C_2$. Show that $Q+Q=(t,t(1-s))$ in the group law.

**Exercise 9.4.** *Pascal's mystic hexagon.* Let $X\subseteq \mathbb{P}^2$ be an irreducible conic. Let $ABCDEF$ be a hexagon whose vertices are inscribed in $X$. Assume the three pairs of opposite sides meet in points $P,Q,R$ respectively. (To be precise, the lines $FA$ and $CD$ meet at $P$; the lines $AB$ and $DE$ meet at $Q$; the lines $BC$ and $EF$ meet at $R$.) Show that $P,Q,R$ are colinear. (That means, the three points are on the same line in $\mathbb{P}^2$.) You can follow these steps (the idea is already used in the proof of Proposition 9.13):

(1) Sketch a picture to illustrate the given situation.

(2) The three lines $FA$, $BC$ and $DE$ form a cubic curve $C_1$; the three lines $AB$, $CD$ and $EF$ form a cubic curve $C_2$. Find $C_1\cap C_2$.

(3) Consider a third cubic $C_3$ given by the union of the conic $X$ and the line $PQ$. Then apply Lemma 9.12.

## Solutions to Exercise Sheet 9

**Solution 9.1.** *Understanding the simplified group law.*

(1) We show that the point $p=[0:1:0]$ is an inflection point on the non-singular cubic $C=\mathbb{V}_p(f)$ where $f=y^2z-x^3-ax^2z-bxz^2-cz^3$. First of all we need to find out the tangent line $T_pC$, which can be computed on the standard affine piece $C_1=C\cap U_1=\mathbb{V}_a(f_1)$ where $f_1=z-x^3-ax^2z-bxz^2-cz^3$. The non-homogeneous coordinates of $p$ in $U_1$ is $p=(0,0)$. Since $\frac{\partial f_1}{\partial x}=-3x^2-2axz-bz^2$ and $\frac{\partial f_1}{\partial z}=1-ax^2-2bxz-3cz^2$, the tangent line

$T_pC_1 = \mathbb{V}_a(0(x-0)+1(z-0)) = \mathbb{V}_a(z)$. Its projective closure is $T_pC = \mathbb{V}_p(z)$. To find the intersection points of $C$ and $T_pC$, we follow the method in the proof of Theorem 8.8. A point on $T_pC$ is given by $[x:y:0]$. It lies in $C$ if and only if $f(x,y,0)=0$, where $f(x,y,0)=-x^3$ which has one solution $[x:y]=[0:1]$ with multiplicity 3. Therefore $T_pC$ and $C$ meet at the point $[0:1:0]$ with multiplicity 3, which proves $p=[0:1:0]$ is an inflection point on $C$.

(2) First of all, since $O$ is the identity element in the group law, we always have $O+O=O$, so $O$ is one of such point. It remains to find all such points $P \in C_2$. The condition $P+P=O$ can be interpreted as $P=-P$. If the non-homogeneous coordinates of $P$ in $C_2$ is given by $P=(x,y)$, then by the simplified group law 9.4, $-P=(x,-y)$. The condition $P=-P$ holds if and only if $y=0$. Therefore all points $P \in C$ satisfying $P+P=O$ are precisely the identity element $O=[0:1:0]$ and those points $P=(x,y) \in C_2$ such that $y=0$.

(3) In the standard affine piece $C_2 = \mathbb{V}(y^2-x^3+4x-1)$, the non-homogeneous coordinates of the two points are $A=(2,1)$ and $B=(-2,-1)$. The line $AB$ is given by $x-2y=0$. To find its third intersection points with $C_2$, we need to solve the system

$$\begin{aligned} y^2-x^3+4x-1&=0,\\ x-2y&=0. \end{aligned}$$

We substitute $x$ by $2y$ in the first equation to get $y^2-8y^3+8y-1=0$, which can be factored as $(y^2-1)(1-8y)=0$. The solutions are $y=\pm 1$ and $y=\frac{1}{8}$. Therefore the third intersection point is $(\frac{1}{4},\frac{1}{8})$, whose reflection across the $x$-axis is the sum of $A$ and $B$; that is $A+B=(\frac{1}{4},-\frac{1}{8})$, or $[\frac{1}{4}:-\frac{1}{8}:1]$ in homogeneous coordinates (or $[2:-1:8]$ if you prefer). The inverse $-A$ is the reflection of $A$ across the $x$-axis, so $-A=(2,-1)$, or $[2:-1:1]$ in homogeneous coordinates. The inverse $-B$ is the reflection of $B$ across the $x$-axis, so $-B=(-2,1)$, or $[-2:1:1]$ in homogeneous coordinates.

**Solution 9.2.** *Example of group law.*

(1) For $L_1 \cap C$, set $z=0$ in the equation defining $C$ to obtain $x^3=0$, which gives solutions $[x:y]=[0:1]$ with multiplicity 3. Hence $[x:y:z]=[0:1:0]$ is the only intersection point with multiplicity 3. For $L_2 \cap C$, set $x=0$ in the equation defining $C$ to obtain $y^2z=0$, which gives solutions $[y:z]=[0:1]$ with multiplicity 2 and $[1:0]$ with multiplicity 1. Hence the line $L_2$ meets $C$ at $[0:0:1]$ with multiplicity 2 and $[0:1:0]$ with multiplicity 1. For $L_3 \cap C$, set $y=2x$ to obtain $x(4xz-x^2-4z^2)=0$, which can be written as $-x(x-2z)^2=0$. Its solutions are $[x:z]=[0:1]$ with multiplicity 1, and $[x:z]=[2:1]$ with multiplicity 2. Therefore $L_3$ meets C at $[x:y:z]=[0:0:1]$ with multiplicity 1 and $[2:4:1]$ with mulplicity 2.

(2) We can use the simplified group law 9.4. The standard affine piece $C_2=\mathbb{V}_a(f_2) \subseteq \mathbb{A}^2$ where $f_2=y^2-x^3-4x$. We first compute $P+P$. The non-homogeneous coordinates of $P$ are $(2,4)$. To compute the tangent line $T_PC_2$, we find $\frac{\partial f_2}{\partial x}=-3x^2-4$ and $\frac{\partial f_2}{\partial y}=2y$. Therefore $\frac{\partial f_2}{\partial x}(P)=-16$ and $\frac{\partial f_2}{\partial y}=8$. It follows that $T_PC_2=\mathbb{V}_a(-16(x-2)+8(y-4))=\mathbb{V}_a(-2(x-2)+(y-4))=\mathbb{V}_a(-2x+y) \subseteq \mathbb{A}^2$. To find the third intersection point of $T_PC_2$ and $C$, we solve the system of equations

$$\begin{aligned} y^2-x^3-4x&=0,\\ -2x+y&=0. \end{aligned}$$

We substitute $y$ by $2x$ in the first equation to get $4x^2-x^3-4x=0$, which is $-x(x-2)^2=0$. Therefore the system has a solution $(x,y)=(2,4)$ with multiplicity 2 and a solution $(x,y)=(0,0)$ with multiplicity 1. The solution $(2,4)$ corresponds to the point $P$, hence the third intersection point is $R=(0,0)$. The sum $P+P$ is the reflection $\overline{R}$ of $R$ across the $x$-axis, which is still $(0,0)$. Hence $P+P=\overline{R}=(0,0)=R$.

Now we compute $R+R$. Since $R=(0,0)$, by the simplified group law 9.4 (2a), we immediately have $R+R=O$. Therefore $P+P+P+P=O$. It follows that the order of $P$ must divide 4, which can only be 1 or 2 or 4. Since $P \neq O$, the order of $P$ is not 1. Since

$P + P = R \neq O$, the order of $P$ is not 2. Therefore the order of $P$ is 4, which means the subgroup generated by $P$ has order 4.

(3) To find all points $Q \in C$ such that $Q+Q = O$, we use Exercise 9.1 (2). First of all $O = [0 : 1 : 0]$ is such a point. It remains to find all points $Q = (x, y) \in C_2$ such that $y = 0$. In the equation $f_2 = y^2 - x^3 - 4x = 0$ we set $y = 0$. Then we have $-x^3 - 4x = -x(x^2 + 4) = 0$. Hence $x = 0$ or $2\sqrt{-1}$ or $-2\sqrt{-1}$. The corresponding points are $Q = (0, 0)$ or $(2\sqrt{-1}, 0)$ or $(-2\sqrt{-1}, 0)$. In summary, we found 4 points $Q \in C$ such that $Q + Q = O$, which are $[0 : 1 : 0]$, $[0 : 0 : 1]$, $[2\sqrt{-1} : 0 : 1]$ and $[-2\sqrt{-1} : 0 : 1]$.

**Solution 9.3.** *Example: Tate's normal form.*

Notice that the defining polynomial of the cubic does not meet the conditions required for using the simplified group law. So we need to use the group law 9.1.

(1) To find the inverse, we use the method in the proof of Proposition 9.8. We need to find the third intersection point $\overline{O}$ of $T_OC$ and $C$, then find the third intersection point of $\overline{O}P$ and $C$, which is $-P$.

Since $C$ is the projective closure of $C_2$, we can write down its defining equation as $C = \mathbb{V}_p(y^2z + sxyz - tyz^2 - x^3 + tx^2z) \subseteq \mathbb{P}^2$. It is easy to see that $O = [0 : 1 : 0]$ is the only point at infinity. To find the tangent line $T_OC$, we need to consider the standard affine piece $C_1 = C \cap U_1$ which contains the point $O$. We have $C_1 = \mathbb{V}_a(f_1) \subseteq \mathbb{A}^2$ where $f_1 = z + sxz - tz^2 - x^3 + tx^2z$ and $O = (0, 0) \in C_1$. Since $\frac{\partial f_1}{\partial x} = sz - 3x^2 + 2txz$ and $\frac{\partial f_1}{\partial z} = 1 + sx - 2tz + tx^2$, we have $\frac{\partial f_1}{\partial x}(O) = 0$ and $\frac{\partial f_1}{\partial z}(O) = 1$, hence $T_OC_1 = \mathbb{V}_a(z) \subseteq \mathbb{A}^2$. Taking its projective closure, we get $T_OC = \mathbb{V}_p(z) \subseteq \mathbb{P}^2$. To find the intersection points of $T_OC$ and $C$, we consider an arbitrary point $[x : y : z] = [x : y : 0] \in T_OC$. If this point is also in $C$, then we set $z = 0$ in the defining equation of $C$ to get $-x^3 = 0$. Therefore $T_OC$ and $C$ meet at the only point $[x : y : z] = [0 : 1 : 0]$ with multiplicity 3, which means that the third intersection point $\overline{O}$ of $T_OC$ and $C$ is still $\overline{O} = O = [0 : 1 : 0]$.

To find $-P$, we need to write down the line $\overline{O}P$. We first make an observation. Since $P = (a, b) \in C_2$, its coordinates have to satisfy the defining polynomial of $C_2$, namely

$$b^2 + sab - tb - a^3 + ta^2 = 0,$$

or equivalently

$$-a^3 + ta^2 = -b(b + sa - t).$$

The homogeneous coordinates of $P$ are given by $P = [a : b : 1]$. By Lemma 9.2 the line is given by

$$\det \begin{pmatrix} x & 0 & a \\ y & 1 & b \\ z & 0 & 1 \end{pmatrix} = x - az = 0.$$

To find the third intersection point of $\overline{O}P$ and $C$, we consider an arbitrary point $[x : y : z] = [az : y : z] \in \overline{O}P$. Since this point is also in $C$, we get

$$y^2z + sayz^2 - tyz^2 - a^3z^3 + ta^2z^3 = 0.$$

Using the observation above, we get

$$y^2z + (sa - t)yz^2 - b(b + sa - t)z^3 = 0$$

which can be factored into

$$z(y - bz)(y + (b + sa - t)z) = 0.$$

The three solutions are $[y : z] = [1 : 0]$, $[b : 1]$ and $[-b - sa + t : 1]$. Since $x = az$, the three intersection points of $\overline{O}P$ and $C$ are $[x : y : z] = [0 : 1 : 0]$, $[a : b : 1]$ and $[a : -b - sa + t : 1]$. The first two points are $\overline{O}$ and $P$, hence $-P = [a : -b - sa + t : 1]$. The non-homogeneous coordinates of $-P$ with respect to $C_2$ is $-P = (a, -b - sa + t)$.

(2) To compute $Q+Q$, we need to find the tangent line $T_QC$. We know that $Q \in C_2 = \mathbb{V}_a(f_2) \subseteq \mathbb{A}^2$ where $f_2 = y^2 + sxy - ty - x^3 + tx^2$. The partial derivatives are given by $\frac{\partial f_2}{\partial x} = sy - 3x^2 + 2tx$ and $\frac{\partial f_2}{\partial y} = 2y + sx - t$. At the point $Q = (0,0)$, their values are $\frac{\partial f_2}{\partial x}(Q) = 0$ and $\frac{\partial f_2}{\partial y}(Q) = -t$. Since $t \neq 0$, we have $T_QC_2 = \mathbb{V}_a(-ty) = \mathbb{V}_a(y) \subseteq \mathbb{A}^2$, hence $T_QC = \mathbb{V}_p(y) \subseteq \mathbb{P}^2$. To find the third intersection point $R$ of the line $T_QC$ and $C$, we consider an arbitrary point $[x : y : z] = [x : 0 : z] \in T_QC$. When this point is also on $C$, we can set $y = 0$ in the defining equation of $C$ to get $-x^3 + tx^2z = 0$. It has solutions $[x : z] = [0 : 1]$ with multiplicity 2 and $[t : 1]$ with multiplicity 1. Therefore the intersection points of $T_QC$ and $C$ are given by $[x : y : z] = [0 : 0 : 1]$ with multiplicity 2 and $[t : 0 : 1]$ with multiplicity 1. Hence third intersection point $R$ of $T_QC$ and $C$ is $R = [t : 0 : 1]$.

It remains to find the third intersection point of $OR$ and $C$, which is the sum $Q + Q$. Fortunately we have done the computation in part (1). Indeed, we have seen that, given a point $P = [a : b : 1] \in C$, the line $OP(= \overline{O}P)$ meets $C$ at a third point $[a : -sa+t-b : 1]$. Let $a = t$ and $b = 0$, then $OR$ meets $C$ at a third point $[t : -st + t : 1]$, or in non-homogeneous coordinates $(t, -st + t)$. Therefore $Q + Q = (t, -st + t) = (t, t(1 - s))$.

**Solution 9.4.** *Pascal's mystic hexagon.*

(1) A picture has been given in the exercise class. You can also find the same picture in [Section 2.11, Reid, Undergraduate Algebraic Geometry].

(2) From the picture we can see that $C_1$ and $C_2$ meet at 9 distinct points, i.e.

$$C_1 \cap C_2 = \{A, B, C, D, E, F, P, Q, R\}.$$

Indeed, the first six points are distinct by the assumption. None of the last three points is on $X$ (otherwise a certain line meets $X$ in 3 points), so none of them can coincide with any of the first six points. The last three points must also be distinct (otherwise two certain lines meet each other in 2 points).

(3) By assumption, the cubic curve $C_3$ passes through 8 of the above 9 points with the point $R$ being the only possible exception. By Lemma 9.12, $R$ must be on $C_3$ as well. Therefore $R$ is either on the conic $X$ or the line $PQ$. We claim that $R$ is not on $X$. Otherwise, the line $BCR$ and the conic $X$ meet at three distinct points $B$, $C$ and $R$, which violates Bézout's theorem 8.8. Therefore $R$ is on the line $PQ$, which means that the points $P, Q, R$ are colinear.

## 10. Algebraic Surfaces

We look at a few aspects of hypersurfaces in $\mathbb{P}^3$ of low degrees.

### 10.1. **Planes and quadric surfaces.** From now on we focus on hypersurfaces in $\mathbb{P}^3$.

**Definition 10.1.** A hypersurface $S = \mathbb{V}(f) \subseteq \mathbb{P}^3$ defined by some non-constant homogeneous polynomial $f \in \Bbbk[z_0, z_1, z_2, z_3]$ without repeated factors is called a *surface*. The *degree* of $S$ is defined to be $\deg f$. Surfaces of degree 1, 2, 3 and 4 are called *planes*, *quadrics*, *cubics* and *quartics* respectively.

**Example 10.2.** Let $[z_0 : z_1 : z_2 : z_3]$ be the homogeneous coordinates in $\mathbb{P}^3$. Every plane is defined by a polynomial $f(z_0, z_1, z_2, z_3) = a_0z_0 + a_1z_1 + a_2z_2 + a_3z_3$ for some $a_0, a_1, a_2, a_3 \in \Bbbk$ which are not simultaneously zero. A plane is always irreducible.

**Example 10.3.** Every quadric surface is defined by a non-zero homogeneous polynomial $g \in \Bbbk[z_0, z_1, z_2, z_3]$ of degree 2. Similar to the case of conics, it is sometimes more convenient to write it in the matrix form

$$g(z_0, z_1, z_2, z_3) = (z_0, z_1, z_2, z_3) \cdot M \cdot (z_0, z_1, z_2, z_3)^T$$

where $M$ is a $4 \times 4$ symmetric matrix. The classification of quadric surfaces is controlled by the rank of $M$.

There is a notion of linear change of homogeneous coordinates in $\mathbb{P}^3$, which is literally almost the same as Definition 8.4, with all vectors having 4 components and $A$ being a $4 \times 4$ invertible matrix.

**Lemma 10.4.** *Every plane in $\mathbb{P}^3$ can be written as $\mathbb{V}(z_0)$ after a suitable linear change of homogeneous coordinates. A non-zero homogeneous polynomial of degree 2*

$$g(z_0, z_1, z_2, z_3) = (z_0, z_1, z_2, z_3) \cdot M \cdot (z_0, z_1, z_2, z_3)^T$$

*defines a non-singular irreducible quadric surface if and only if $M$ has rank 4; $g$ defines a singular irreducible quadric surface if and only if $M$ has rank 3; $g$ defines a union of two planes if and only if $M$ has rank 2; $g$ defines a double plane if and only if $M$ has rank 1. Every non-singular quadric surface can be written as $\mathbb{V}(z_0z_3 - z_1z_2)$ after a suitable linear change of homogeneous coordinates.*

*Proof.* Non-examinable. Application of Gram-Schmidt orthogonalisation again. □

*Remark* 10.5. A union of two planes can be thought as a singular algebraic set. A double plane is not a quadric surface. So a "non-singular quadric surface" always means a "non-singular irreducible quadric surface".

Now we turn to the rationality problem. Recall from Proposition 8.7 that a line or a non-singular conic is always isomorphic to $\mathbb{P}^1$ hence is rational. Something similar happens to surfaces.

**Proposition 10.6.** *A plane is isomorphic to $\mathbb{P}^2$, hence is rational. A non-singular quadric surface is birational to $\mathbb{P}^2$, hence is rational.*

*Proof.* By Lemma 10.4, we can assume the plane is $\mathbb{V}(z_0)$ and the non-singular quadric is $\mathbb{V}(z_0z_3 - z_1z_2)$ without loss of generality. It is easy to show that $\mathbb{V}(z_0)$ is isomorphic to $\mathbb{P}^2$; we leave the details to the reader. We have proved in Exercise 5.2 that $\mathbb{V}(z_0z_3 - z_1z_2)$ is birational to $\mathbb{P}^2$. □

This result suggests that a non-singular quadric surface is not isomorphic to $\mathbb{P}^2$. Indeed, it follows from the fact that two curves in $\mathbb{P}^2$ always intersect while two curves in a quadric surface could be disjoint. The details are left as an exercise. We would like to know what precisely a quadric surface looks like. For that purpose we need the theory of multi-projective spaces. We will not discuss the theory systematically. Instead, we will only focus on this particular example and mention a few ingredients of the theory along the way. Some details in the proof are left to the reader.

**Proposition 10.7.** *A non-singular quadric surface is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$.*

*Proof.* We assume the quadric surface is $S = \mathbb{V}(z_0z_3 - z_1z_2)$. We need to find morphisms $\varphi : \mathbb{P}^1 \times \mathbb{P}^1 \to S$ and $\psi : S \to \mathbb{P}^1 \times \mathbb{P}^1$, such that both compositions are identities.

The product $\mathbb{P}^1 \times \mathbb{P}^1$ is the simplest example of a *bi-projective space*. A point in it is given by a pair of points $(p, q)$ in $\mathbb{P}^1$. If $p = [x_0 : x_1]$ and $q = [y_0 : y_1]$, then the *bi-homogeneous coordinates* of $(p, q)$ are given by $([x_0 : x_1], [y_0 : y_1])$. Notice that for any $\lambda, \mu \in \Bbbk \backslash \{0\}$, we have $([\lambda x_0 : \lambda x_1], [\mu y_0 : \mu y_1]) = ([x_0 : x_1], [y_0 : y_1])$. We construct two morphisms:

$$\varphi : \quad \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow S; \quad ([x_0 : x_1], [y_0 : y_1]) \longrightarrow [x_0y_0 : x_1y_0 : x_0y_1 : x_1y_1];$$

$$\psi : \quad S \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1; \quad [z_0 : z_1 : z_2 : z_3] \longmapsto \begin{cases} ([z_0 : z_1], [z_0 : z_2]) & \text{if } z_0 \neq 0; \\ ([z_0 : z_1], [z_1 : z_3]) & \text{if } z_1 \neq 0; \\ ([z_2 : z_3], [z_0 : z_2]) & \text{if } z_2 \neq 0; \\ ([z_2 : z_3], [z_1 : z_3]) & \text{if } z_3 \neq 0. \end{cases}$$

We need to check they are morphisms. We have not defined the notion of a morphism in this setting, but it is very similar to a morphism between two projective varieties. All components of $\varphi$ are homogeneous of the same degree with respect to the coordinates $x_0$ and $x_1$ of $p$, and the coordinates $y_0$ and $y_1$ of $q$ (aka *bi-homogeneous*). All components of $\psi$ are also homogeneous of the same degree. We observe that $\varphi$ and $\psi$ are both well-defined at every point in their domains (we leave the details to

the reader). Moreover, the image of $\varphi$ satisfies the defining equation of $S$. Hence $\varphi$ is a morphism. To show $\psi$ is a morphism, we need to verify that the image of any point in $S$ is independent of the choice of any valid expression. More precisely, we need to verify $[z_0 : z_1] = [z_2 : z_3]$ and $[z_0 : z_2] = [z_1 : z_3]$, both of which follow from the defining equation $z_0z_3 = z_1z_2$ of $S$.

We check the composition $\psi \circ \varphi$ is identity. Given any point $([x_0 : x_1], [y_0 : y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1$, using the first expression of $\psi$, we have

$$\begin{aligned}(\psi \circ \varphi)([x_0 : x_1], [y_0 : y_1]) &= \psi([x_0y_0 : x_1y_0 : x_0y_1 : x_1y_1]) \\ &= ([x_0y_0 : x_1y_0], [x_0y_0 : x_0y_1]) \\ &= ([x_0 : x_1], [y_0 : y_1]).\end{aligned}$$

Similarly we can check that $\psi \circ \varphi$ is identity in all the other three cases.

We check the composition $\varphi \circ \psi$ is identity. Given any point $[z_0 : z_1 : z_2 : z_3] \in S$, using the first expression of $\psi$, we have

$$\begin{aligned}(\varphi \circ \psi)([z_0 : z_1 : z_2 : z_3]) &= \varphi([z_0 : z_1], [z_0 : z_2]) \\ &= [z_0^2 : z_0z_1 : z_0z_2 : z_1z_2] \\ &= [z_0^2 : z_0z_1 : z_0z_2 : z_0z_3] \\ &= [z_0 : z_1 : z_2 : z_3].\end{aligned}$$

Similarly we can check $\varphi \circ \psi$ is identity in all the other three cases.

To summarise, $\varphi$ and $\psi$ are mutually inverse isomorphisms. Therefore a quadric surface is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. $\square$

Quadric surfaces are very useful in civil engineering. According to the literature, the Shukhov water tower (in Polibino, Russia, 1896, designed by Shukhov) is the first structure of this shape ever built in the world. Similar design can also be found at a few places inside and outside Sagrada Família (in Barcelona, Spain, designed by Gaudi). Nowaways numerous cooling towers in power plants are built in this shape.

10.2. **Non-singular cubic surfaces.** We have seen that non-singular cubic curves have very rich geometry. The situation is similar for cubic surfaces. The theory of cubic surfaces has a long history. It is known since 1849 that a non-singular cubic surface contains 27 lines. This discovery is one of the first results on surfaces of higher degree and is considered by many as the start of modern algebraic geometry. Many mathematicians contributed to the understanding of rich geometry of non-singular cubic surfaces. In this lecture we will take a glimpse of the theory of non-singular cubic surfaces via examples.

**Definition 10.8.** A *line* in $\mathbb{P}^3$ is a projective variety $\mathbb{V}(f, g)$, where $f, g \in \Bbbk[z_0, z_1, z_2, z_3]$ are non-zero homogeneous polynomials of degree 1 which are not proportional to each other.

*Remark* 10.9. The definition shows that a line in $\mathbb{P}^3$ is defined by the system of equations

$$\begin{cases} a_0z_0 + a_1z_1 + a_2z_2 + a_3z_3 = 0 \\ b_0z_0 + b_1z_1 + b_2z_2 + b_3z_3 = 0 \end{cases}$$

such that the coefficient matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$$

has rank 2. We know from linear algebra that its reduced row echelon form has two pivots, therefore the two variables corresponding to the pivots can be written as linear functions of the other variables. For example, if the pivots are in the first two columns, then

$$\begin{cases} z_0 = r_2z_2 + r_3z_3 \\ z_1 = s_2z_2 + s_3z_3 \end{cases}$$

for some $r_2, r_3, s_2, s_3 \in \Bbbk$.

**Proposition 10.10.** *The Fermat cubic surface $S = \mathbb{V}(z_0^3 + z_1^3 + z_2^3 + z_3^3)$ contains exactly 27 lines.*

*Proof.* Assume a line $L$ in $\mathbb{P}^3$ is given by $z_0 = r_2 z_2 + r_3 z_3$ and $z_1 = s_2 z_2 + s_3 z_3$ for some $r_2, r_3, s_2, s_3 \in \Bbbk$ (i.e. pivots in first two columns). Such a line lies in $S$ if and only if

$$(r_2 z_2 + r_3 z_3)^3 + (s_2 z_2 + s_3 z_3)^3 + z_2^3 + z_3^3 = 0$$

holds for all $z_2, z_3 \in \Bbbk$, hence is an identity. By comparing the coefficients, we get

$$r_2^3 + s_2^3 = -1 \tag{1}$$
$$r_3^3 + s_3^3 = -1 \tag{2}$$
$$r_2^2 r_3 = -s_2^2 s_3 \tag{3}$$
$$r_2 r_3^2 = -s_2 s_3^2 \tag{4}$$

If $r_2, r_3, s_2, s_3$ are all non-zero, then $(3)^2/(4)$ gives $r_2^3 = -s_2^3$, in contradiction to (1). Hence for a line in the cubic at least one of these numbers must be zero. By (3) $r_2$ and $r_3$ cannot be both non-zero.

If $r_2 = 0$, then by (1) $s_2^3 = -1$, hence by (3) $s_3 = 0$, which by (2) implies $r_3^3 = -1$. This gives 9 solutions $r_2 = s_3 = 0$, $s_2 = -\omega^j$, $r_3 = -\omega^k$ for $0 \leqslant j, k \leqslant 2$ and $\omega = \exp\left(\frac{2\pi\sqrt{-1}}{3}\right)$ is a primitive third root of unity. We thus obtain 9 lines given by

$$z_0 + \omega^k z_3 = z_1 + \omega^j z_2 = 0, \qquad 0 \leqslant j, k \leqslant 2.$$

If $r_3 = 0$, we can similarly find out that $s_2 = 0$ and $r_2^3 = s_3^3 = -1$, hence we obtain another 9 lines given by

$$z_0 + \omega^k z_2 = z_1 + \omega^j z_3 = 0, \qquad 0 \leqslant j, k \leqslant 2.$$

As the equation of $S$ is symmetric with respect to all variables, we can allow permutations of variables to find other lines in the cubic (i.e. pivots not necessarily in first two columns). Some of the lines show up repeatedly after permutations of variables, but we get 9 new lines given by

$$z_0 + \omega^k z_1 = z_2 + \omega^j z_3 = 0, \qquad 0 \leqslant j, k \leqslant 2.$$

In summary, we have equations of all 27 lines. □

**Proposition 10.11.** *The cubic surface $S = \mathbb{V}(z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_3 + z_3^2 z_0)$ is rational.*

*Proof.* We write down two mutually inverse rational maps

$$\varphi: \quad S \dashrightarrow \mathbb{P}^2; \quad [z_0 : z_1 : z_2 : z_3] \longmapsto [z_0 z_3 : z_1 z_2 : z_2 z_3];$$
$$\psi: \quad \mathbb{P}^2 \dashrightarrow S; \quad [r : s : t] \longmapsto [rt(rt + s^2) : -s(r^2 s + t^3) : t^2(rt + s^2) : -t(r^2 s + t^3)].$$

To check they are rational maps, we observe that they are both given by homogeneous polynomials of the same degree. It is easy to check that $\varphi([1 : -1 : 1 : -1]) = [1 : 1 : 1]$ and $\psi([1 : 1 : 1]) = [1 : -1 : 1 : -1]$), hence both $\varphi$ and $\psi$ are defined on non-empty sets. We need to show the image of $\psi$ satisfies the defining equation of $S$, which can be computed directly.

It remains to show that both $\psi \circ \varphi$ and $\varphi \circ \psi$ are identity maps on the loci where they are well-defined. This is also a simple calculation. We leave the details to the reader. This shows that $S$ and $\mathbb{P}^2$ are birational. By definition, $S$ is rational. □

The phenomenons in the above examples hold for every non-singular cubic surface. We summarise it in the following result.

**Theorem 10.12.** *Every non-singular cubic surface contains exactly 27 lines. Every non-singular cubic surface is rational.*

*Proof.* Non-examinable. Interested reader can find the proof in [Chapter 7, Reid, Undergraduate Algebraic Geometry]. □

*Remark* 10.13. If we fix the degree and vary the dimension, there is major difference between non-singular cubic curves and surfaces: the former is not rational while the latter is rational. In higher dimensions, whether a cubic hypersurface is rational is a very difficult question. (There is an answer in dimension 3, but mostly unknown in dimension 4 or higher.)

Moreover, if we fix the dimension, then the number of lines in a non-singular surface depends on its degree: planes and non-singular quadric surfaces contain infinitely many lines (which we will see in an exercise); a non-singular cubic surface has 27 lines; most non-singular surfaces of higher degrees have no lines at all.

Counting special curves in various kinds of spaces turns out to be a fascinating topic in algebraic geometry, which is usually called *enumerative geometry*. These questions are not only interesting to mathematicians, but also have been extensively studied in physics, as they play an important role in string theory. The 27 lines in non-singular cubic surfaces is a first example of this type.

## Exercise Sheet 10

*This sheet will be discussed in the exercise class on 7 December. You do not need to submit your solutions.*

**Exercise 10.1.** *Infinitely many lines on planes.*

(1) Without loss of generality, we consider the plane $P = \mathbb{V}(z_0) \subseteq \mathbb{P}^3$. For every $[a : b : c] \in \mathbb{P}^2$, show that $\mathbb{V}(z_0, az_1 + bz_2 + cz_3)$ defines a line in $P$.

(2) Show that two such lines always meet at exactly one point.

**Exercise 10.2.** *Infinitely many lines on non-singular quadric surfaces.*

(1) Without loss of generality, we consider the quadric surface $Q = \mathbb{V}(z_0z_3 - z_1z_2) \subseteq \mathbb{P}^3$. Show that for every $[a : b] \in \mathbb{P}^1$, $\mathbb{V}(az_0 + bz_1, az_2 + bz_3)$ defines a line in $Q$.

(2) Show that two such lines are always disjoint.

(3) Show that every point in $Q$ lies on exactly one of such lines.

(4) Can you write down another family of pairwisely disjoint lines in $Q$, such that every point in $Q$ lies on exactly one of them?

*Remark:* the family of lines constructed in part (1) (or part (4)) is called a *ruling* on $Q$. We have seen in Exercise 5.2 that $Q$ is birational to $\mathbb{P}^2$. This exercise shows that $Q$ is not isomorphic to $\mathbb{P}^2$. The reason is: two lines in the same ruling on $Q$ do not meet, while any two curves on $\mathbb{P}^2$ meet by Bézout's theorem. Since $Q$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, it follows that $\mathbb{P}^1 \times \mathbb{P}^1$ is not isomorphic to $\mathbb{P}^2$.

**Exercise 10.3.** *Rationality of a cubic surface.* Finish the proof of Proposition 10.11.

(1) Show that any point in the image of $\psi$ satisfies the defining equation of $S$.

(2) Show that $\psi \circ \varphi$ and $\varphi \circ \psi$ are both identity maps on the loci where they are well-defined.

*Remark:* there is a general method to find out the explicit formula for a birational map between any given non-singular cubic surface $S$ and $\mathbb{P}^2$. For that purpose we need to know the explicit equations of two disjoint lines on $S$. We do not discuss the details. However, the formula is usually very messy. The example in Proposition 10.11 is one of the very rare good-looking ones.

**Exercise 10.4.** *Thank you and have a wonderful Christmas vacation!*

Thank you all for your participation in this course. Please complete the Unit Evaluation for this course whenever convenient. If you have any questions during your revision, please feel free to ask me. There will be extra office hours after the vacation. You are also welcome to contact me by email at any time. Good luck with your exams!

**Solution 10.1.** *Infinitely many lines on planes.*

(1) Since $z_0$ and $az_1+bz_2+cz_3$ are both homogeneous polynomials of degree 1 and not proportional to each other, $L = \mathbb{V}(z_0, az_1 + bz_2 + cz_3)$ defines a line in $\mathbb{P}^2$. To show that the line $L$ is in $P$, we just need to observe that every point on $L$ satisfies the equation $z_0 = 0$, hence is a point in $P$.

(2) Let $L = \mathbb{V}(z_0, az_1 + bz_2 + cz_3)$ and $L' = \mathbb{V}(z_0, a'z_1 + b'z_2 + c'z_3)$ be two such lines, where $[a : b : c] \neq [a' : b' : c']$. If a point $p = [z_0 : z_1 : z_2 : z_3]$ is an intersection point of $L$ and $L'$, then its coordinates satisfy the system of equations

$$\begin{aligned} z_0 &= 0; \\ az_1 + bz_2 + cz_3 &= 0; \\ a'z_1 + b'z_2 + c'z_3 &= 0. \end{aligned}$$

The first equation fixes the $z_0$ coordinate. For the other coordinates, we look at the second and the third equations. We look at the coefficient matrix

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}.$$

Since $[a : b : c]$ and $[a' : b' : c']$ represent different points in $\mathbb{P}^2$, both rows are non-zero and linearly independent. Hence the matrix has rank 2. It follows that the null-space has dimension 1, which means that there is a unique solution for $[z_1 : z_2 : z_3]$ (up to scaling). Therefore there is a unique intersection point $[z_0 : z_1 : z_2 : z_3]$ for the lines $L$ and $L'$.

**Solution 10.2.** *Infinitely many lines on non-singular quadric surfaces.*

(1) It is clear that for every point $[a : b] \in \mathbb{P}^1$, the two polynomials $az_0 + bz_1$ and $az_2 + bz_3$ are non-zero and homogeneous of degree 1. They are not propotional to each other, so $\mathbb{V}(az_0 + bz_1, az_2+bz_3)$ defines a line $L$ in $\mathbb{P}^2$. We still need to show that every point in $L$ is a point in $Q$. Since $[a : b] \in \mathbb{P}^1$, we have either $a \neq 0$ or $b \neq 0$. If $a \neq 0$, then a point $p = [z_0 : z_1 : z_2 : z_3] \in L$ satisfies $z_0 = -\frac{b}{a}z_1$ and $z_2 = -\frac{b}{a}z_3$. Then

$$z_0z_3 - z_1z_2 = \left(-\frac{b}{a}\right) \cdot z_1 \cdot z_3 - z_1 \cdot \left(-\frac{b}{a}\right) \cdot z_3 = 0.$$

Hence $p \in Q$. If $b \neq 0$, a similar calculation shows that every point $p \in L$ also satisfies the equation $z_0z_3 - z_1z_2 = 0$ hence is a point in $Q$. We conclude that $L$ is a line in $Q$.

(2) Consider two lines $L = \mathbb{V}(az_0 + bz_1, az_2 + bz_3)$ and $L' = \mathbb{V}(a'z_0 + b'z_1, a'z_2 + b'z_3)$ where $[a : b]$ and $[a' : b']$ are two different points in $\mathbb{P}^1$. If the two lines have a common point $[z_0 : z_1 : z_2 : z_3]$, then the system of equations

$$\begin{aligned} az_0 + bz_1 &= 0, \\ az_2 + bz_3 &= 0, \\ a'z_0 + b'z_1 &= 0, \\ a'z_2 + b'z_3 &= 0 \end{aligned}$$

must have a non-zero solution. However, the coefficient matrix for the first and the third equations is $\begin{pmatrix} a & b \\ a' & b' \end{pmatrix}$. Since $[a : b]$ and $[a' : b']$ are two different points in $\mathbb{P}^1$, the two rows are both non-zero and linearly independent. Hence the matrix has rank 2, which means that the only solution to these two equations is $z_0 = z_1 = 0$. For the same reason the only solution to the second and fourth equations is $z_2 = z_3 = 0$. Since the system of four equations has only a zero solution, $L$ and $L'$ do not have any common point. In other words, they are disjoint.

(3) For any point $p = [z_0 : z_1 : z_2 : z_3] \in Q$, we first show that $p$ lies on a certain line $L = \mathbb{V}(az_0 + bz_1, az_2 + bz_3)$. There are two cases. *Case 1.* If $z_0$ and $z_1$ are not simultaneously zero, then we choose $[a : b] = [z_1 : -z_0]$ for the line $L$. We claim that $p \in L$. Indeed, for such a choice of $[a : b]$ we have $az_0 + bz_1 = z_1z_0 - z_0z_1 = 0$ and $az_2 + bz_3 = z_1z_2 - z_0z_3 = 0$. The claim holds. *Case 2.* If $z_0$ and $z_1$ are both zero, then $z_2$ and $z_3$ are not simultaneously zero. We can choose $[a : b] = [z_3 : -z_2]$ for the line $L$. A similar calculation shows that $p \in L$. In both cases, the point $p$ lies on a certain line $L = \mathbb{V}(az_0 + bz_1, az_2 + bz_3)$ for a suitable choice of $[a : b]$.

It remains to prove that $p$ lies on only one of such lines. This is clear because we have seen from part (2) that two such lines are always disjoint.

(4) For every $[a : b] \in \mathbb{P}^1$, $\mathbb{V}(az_0 + bz_2, az_1 + bz_3)$ also defines a line. These lines are pairwisely disjoint, and every point in $Q$ lies on exactly one of them. The proof can be obtained simply by switching $z_1$ and $z_2$ in the proof for the above three parts.

**Solution 10.3.** *Rationality of a cubic surface.*

(1) We need to verify that every point in the image of $\psi$ satisfies the defining equation of $S$. Indeed, we have

$$\begin{aligned}
&z_0^2z_1 + z_1^2z_2 + z_2^2z_3 + z_3^2z_0 \\
&= -r^2t^2(rt+s^2)^2 \cdot s(r^2s+t^3) + s^2(r^2s+t^3)^2 \cdot t^2(rt+s^2) \\
&\quad - t^4(rt+s^2)^2 \cdot t(r^2s+t^3) + t^2(r^2s+t^3)^2 \cdot rt(rt+s^2) \\
&= -(r^2t^2s+t^5) \cdot (rt+s^2)^2 \cdot (r^2s+t^3) + (s^2t^2+rt^3) \cdot (r^2s+t^3)^2 \cdot (rt+s^2) \\
&= -t^2(r^2s+t^3) \cdot (rt+s^2)^2 \cdot (r^2s+t^3) + t^2(s^2+rt) \cdot (r^2s+t^3)^2 \cdot (rt+s^2) \\
&= -t^2 \cdot (rt+s^2)^2 \cdot (r^2s+t^3)^2 + t^2 \cdot (r^2s+t^3)^2 \cdot (rt+s^2)^2 \\
&= 0.
\end{aligned}$$

Therefore the statement holds.

(2) Let $[z_0 : z_1 : z_2 : z_3]$ be a point in $S$. Then these coordinates satisfy

$$z_0^2z_1 + z_1^2z_2 + z_2^2z_3 + z_3^2z_0 = 0.$$

Then we have

$$\begin{aligned}
&(\psi \circ \varphi)([z_0 : z_1 : z_2 : z_3]) \\
&= \psi([z_0z_3 : z_1z_2 : z_2z_3]) \\
&= [z_0z_2z_3^2(z_0z_2z_3^2 + z_1^2z_2^2) : -z_1z_2(z_0^2z_1z_2z_3^2 + z_2^3z_3^3) : \\
&\qquad : z_2^2z_3^2(z_0z_2z_3^2 + z_1^2z_2^2) : -z_2z_3(z_0^2z_1z_2z_3^2 + z_2^3z_3^3)] \\
&= [z_0z_2^2z_3^2(z_3^2z_0 + z_1^2z_2) : -z_1z_2^2z_3^2(z_0^2z_1 + z_2^2z_3) : \\
&\qquad : z_2^3z_3^2(z_3^2z_0 + z_1^2z_2) : -z_2^2z_3^3(z_0^2z_1 + z_2^2z_3)] \\
&= [z_0z_2^2z_3^2(z_3^2z_0 + z_1^2z_2) : z_1z_2^2z_3^2(z_3^2z_0 + z_1^2z_2) : \\
&\qquad : z_2^3z_3^2(z_3^2z_0 + z_1^2z_2) : z_2^2z_3^3(z_3^2z_0 + z_1^2z_2)] \\
&= [z_0 : z_1 : z_2 : z_3]
\end{aligned}$$

wherever the composition $\psi \circ \varphi$ is well-defined. This shows that $\psi \circ \varphi$ is equivalent to the identity map on $S$.

Now let $[r : s : t]$ be a point in $\mathbb{P}^2$. Then we have

$$\begin{aligned}
&(\varphi \circ \psi)([r : s : t]) \\
&= \varphi([rt(rt+s^2) : -s(r^2s+t^3) : t^2(rt+s^2) : -t(r^2s+t^3)]) \\
&= [-rt^2(rt+s^2)(r^2s+t^3) : -st^2(r^2s+t^3)(rt+s^2) : -t^3(rt+s^2)(r^2s+t^3)] \\
&= [r : s : t]
\end{aligned}$$

wherever the composition $\varphi \circ \psi$ is well-defined. This shows that $\varphi \circ \psi$ is equivalent to the identity map on $\mathbb{P}^2$.

## Appendix A. Brief Review of Algebra 2B

*This is an outline of the topics in Algebra 2B that were reviewed during the exercise class in the first week of the semester.*

**Ring.** A ring is a set of elements with two operations: addition and multiplication, which have to satisfy various algebraic laws. Check your Algebra 2B notes to make sure you know the full definition. We are only interested in commutative rings with 1. More precisely, we mainly focus on polynomial rings $\Bbbk[x_1, \cdots, x_n]$ and their quotient rings. (In particular, $\Bbbk[x_1, \cdots, x_n]$ can be realised as a quotient of itself by the zero ideal.)

**Ideal.** An ideal $I$ is a non-empty subset of a ring $R$, satisfying two closedness conditions: "$a, b \in I \Longrightarrow a - b \in I$", and "$r \in R, a \in I \Longrightarrow ra \in I$". When $R$ is a commutative ring with 1, the first condition $a - b \in I$ can be replaced by the equivalent condition $a + b \in I$.

**Quotient ring.** For any ideal $I$ in a ring $R$, there is a quotient ring $R/I$, whose elements are cosets $r + I$ for any $r \in R$. Two cosets $r_1 + I$ and $r_2 + I$ are the same if and only if $r_1 - r_2 \in I$. If $R$ is a commutative ring with 1, then so is $R/I$.

**Ring homomorphism.** A homomorphism $\varphi : R \longrightarrow S$ between two rings is a map which preserves addition and multiplication. Nice and easy.

**Special rings.** We have "rings $\supset$ integral domains $\supset$ UFDs $\supset$ PIDs $\supset$ fields". Make sure you know the definition of each. It is important to us that $\Bbbk[x_1, \cdots, x_n]$ is a UFD; namely, every polynomial can be factored into a product of irreducible polynomials, which is unique up to the order of factors and units (non-zero constants). It is a PID only when $n = 1$. (We now know that it is a Noetherian ring for every $n$.)

**Polynomial.** A polynomial $f(x_1, \cdots, x_n) \in \Bbbk[x_1, \cdots, x_n]$ is a finite sum of monomials. If $f$ is not zero, then the degree of $f$ is the highest degree of its non-zero monomials. But the degree of the zero polynomial is quite arguable. There are different ways to treat this problem. We will adopt one opinion and define the degree of the zero polynomial to be any non-negative integer. Details will be explained in week 4.

**Irreducible polynomial.** When $\Bbbk$ is algebraic closed, the only irreducible polynomials in $\Bbbk[x]$ are the ones of degree 1. For polynomial rings in more than 1 variable, there is no such a general rule, but irreducible polynomials can still be determined in some cases.

**Example A.1.** We claim that $y^2 - x^3 + x \in \Bbbk[x, y]$ is an irreducible polynomial. We assume on the contrary that it can be written as the product of two non-constant factors. As a polynomial in $y$ with coefficients in $\Bbbk[x]$, $y^2 - x^3 + x$ has degree 2 in $y$. Hence the two factors have degrees either 2 and 0 in $y$ respectively, or 1 and 1 respectively. More precisely,

$$y^2 - x^3 + x = \big(f_2(x)y^2 + f_1(x)y + f_0(x)\big) \cdot g(x) \quad \text{or} \quad \big(f_1(x)y + f_0(x)\big) \cdot \big(g_1(x)y + g_0(x)\big).$$

In the first case, we have the identity $f_2(x)g(x) = 1$, hence $g(x)$ is a non-zero constant. Contradiction. In the second case, we similarly have the identity $f_1(x)g_1(x) = 1$. Therefore both factors are non-zero constants. Without loss of generality we can assume $f_1(x) = g_1(x) = 1$. Then we have

$$y^2 - x^3 + x = (y + f_0(x))(y + g_0(x)).$$

Comparing the coefficients of $y$ we have $f_0(x) + g_0(x) = 0$, hence $g_0(x) = -f_0(x)$. Comparing the terms without $y$ we have $f_0(x)g_0(x) = -x^3 + x$, hence $f_0(x)^2 = x^3 - x = x(x + 1)(x - 1)$. The right hand side is not a square. Contradiction. This concludes that $y^2 - x^3 + x$ is an irreducible polynomial.

**Algebra.** You might not like the definition of a $\Bbbk$-algebra, since it is kind of long and hard to remember. We need to work with a special type of algebras called *finitely generated* $\Bbbk$*-algebras*. You might think the definition is even more involved, but it is actually very simple and explicit. A finitely generated algebra is a ring which is isomorphic to some $\Bbbk[x_1, \cdots, x_n]/I$. A $\Bbbk$*-algebra homomorphism* $\varphi : \Bbbk[x_1, \cdots, x_n]/I \longrightarrow \Bbbk[y_1, \cdots, y_m]/J$ is simply a ring homomorphism that sends a coset $c + I$ to $c + J$ for every constant $c$. They are formally defined in week 3.

**Fundamental isomorphism theorem.** The fundamental isomorphism theorem for rings is the following statement: for a ring homomorphism $f : R \longrightarrow S$, there is a canonical isomorphism

$$\operatorname{im}(f) \cong R/\ker(f).$$

This is a very important theorem for our purpose. Look at the following example.

**Example A.2.** We claim that $\Bbbk[x, y]/(y - x^2) \cong \Bbbk[t]$. To see this, we construct a ring homomorphism (in fact, a $\Bbbk$-algebra homomorphism)

$$\varphi : \Bbbk[x, y] \longrightarrow \Bbbk[t]; \quad x \longmapsto t; \quad y \longmapsto t^2.$$

This means that every monomial $ax^iy^j$ is sent to $at^i(t^2)^j = at^{i+2j}$, where $a \in \Bbbk$ is the coefficient. By the fundamental isomorphism theorem, we have

$$\operatorname{im}(\varphi) \cong \Bbbk[x, y]/\ker(\varphi).$$

We need to identify $\operatorname{im}(\varphi)$ and $\ker(\varphi)$.

For any $p(t) \in \Bbbk[t]$, we have $\varphi(p(x)) = p(t)$. This shows $\varphi$ is surjective, hence $\operatorname{im}(\varphi) = \Bbbk[t]$.

For any $f(x, y) \in \Bbbk[x, y]$, I claim it can be written as

$$f = (y - x^2) \cdot g + h,$$

for some $g(x, y) \in \Bbbk[x, y]$ and $h(x) \in \Bbbk[x]$. For this, one only need to replace every single occurrence of $y$ in $f(x, y)$ by $[(y - x^2) + x^2]$, and then multiply out the square brackets leaving the terms in round brackets untouched. Armed with this claim, we see that

$$\varphi(f) = \varphi(y - x^2) \cdot \varphi(g) + \varphi(h) = (t^2 - t^2) \cdot \varphi(g) + h(t) = h(t).$$

It follows that $\varphi(f) = 0 \iff h = 0 \iff f \in (y - x^2)$. Hence $\ker(\varphi) = (y - x^2)$. Therefore the fundamental isomorphism theorem implies that $\Bbbk[t] \cong \Bbbk[x, y]/(y - x^2)$.

**Field.** A field is a commutative ring with 1 such that every non-zero element has a multiplicative inverse. Check your Algebra 2B notes to make sure you know the *characteristic* of a field and the *field of fractions* of an integral domain (which are used in week 6).

## Acknowledgements

I would like to thank all 53 students in the class for their enthusiasm and participation in this course. I am also grateful to Alastair Craw and Gregory Sankaran for sharing their experience and lecture notes used for this unit in previous years, as well as David Calderbank and Alastair King for their helpful advices.

## References

[1] Alastair Craw, *Lecture notes on algebraic curves*, 2013.
[2] William Fulton, *Algebraic curves – An introduction to algebraic geometry*, Advanced Book Classics, Addison-Wesley Publishing Company, Redwood City, CA, 1989.
[3] Miles Reid, *Undergraduate algebraic geometry*, London Mathematical Society Student Text 12, Cambridge University Press, Cambridge, 1988.
[4] Gregory Sankaran, *Lecture notes on algebraic curves*, 2007.