

# Algebraic Geometry

David Philipson

1 4 April 2008

Notes for this day courtesy of Yakov Shlapentokh-Rothman.

## 1.1 Basic Definitions

Throughout this course, we let  $k$  be an algebraically closed field with  $\text{ch } k = 0$ .

**Definition.** The *affine  $n$ -space*, denoted  $\mathbb{A}^n$ , is simply  $k^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in k\}$ .

**Definition.** Let  $S \subseteq k[x_1, \dots, x_n]$ . The *affine algebraic set*  $\mathcal{Z}(S)$  or  $V(S)$  is  $\{p \in \mathbb{A}^n : f(p) = 0 \forall f \in S\}$ .

### Examples

- If  $S = \emptyset$ , then  $\mathcal{Z}(S) = \mathbb{A}^n$ .
- If  $S = \{1\}$ , then  $\mathcal{Z}(S) = \emptyset$ .
- If  $S = \{x_1 - a_1, \dots, x_n - a_n\}$ , then  $\mathcal{Z}(S) = \{(a_1, \dots, a_n)\}$ .

*Remark.* All rings in this course are commutative and have 1.

*Remark.* If  $A$  is a ring, then any subset  $S \subseteq A$  generates a minimal ideal  $\langle S \rangle \subseteq A$ . In fact, we have  $\langle S \rangle = \{\sum a_j x_j : a_j \in A, x_j \in S\}$ .

**Lemma.**  $\mathcal{Z}(S) = \mathcal{Z}(\langle S \rangle)$  for all  $S \subseteq k[x_1, \dots, x_n]$ .

*Proof.* Since  $\langle S \rangle$  consists of combinations of elements in  $S$ , we have  $\mathcal{Z}(S) \subseteq \mathcal{Z}(\langle S \rangle)$ . Since  $S \subseteq \langle S \rangle$ , we have  $\mathcal{Z}(\langle S \rangle) \subseteq \mathcal{Z}(S)$  as well.  $\square$

## 1.2 Noetherian Rings

**Lemma.** Let  $A$  be a ring. The following are equivalent:

- (1) Any ideal  $\mathfrak{i} \subseteq A$  can be finitely generated.
- (2)  $A$  satisfies the ascending chain condition (ACC). That is, any sequence of ideals  $\mathfrak{i}_0 \subseteq \mathfrak{i}_1 \subseteq \dots \subseteq A$  becomes stationary. More precisely, there exists some  $m$  such that  $\mathfrak{i}_m = \mathfrak{i}_{m+1} = \dots$ .

*Proof.* We first show that (1) implies (2). Pick an ascending sequence of ideals. Let  $\mathfrak{i} = \bigcup \mathfrak{i}_j \subseteq A$ . This is clearly an ideal. Therefore, by (1)  $\mathfrak{i}$  is finitely generated by  $f_1, \dots, f_s$ . There is some  $m$  such that  $f_1, \dots, f_s \in \mathfrak{i}_m$ . Then  $\mathfrak{i}_m = \mathfrak{i}_{m+1} = \dots$ .

Conversely, suppose  $\mathfrak{i} \subseteq A$  is not finitely generated. Then we can find  $f_1 \in \mathfrak{i}$  such that  $f_1 \neq 0$ . We have  $\mathfrak{i} \setminus \langle f_1 \rangle \neq \emptyset$ . Now we have  $f_2 \in \mathfrak{i} \setminus \langle f_1 \rangle$  with  $\mathfrak{i} \setminus \langle f_1, f_2 \rangle \neq \emptyset$ . We can continue this inductively to define  $\mathfrak{i}_j = \langle f_1, \dots, f_j \rangle$ . Thus we have  $\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \dots$ , which does not stabilize.  $\square$

**Definition.** We call such a ring a *Noetherian Ring*.

## Examples

- If  $A$  is a field, then  $A$  is Noetherian.
- $\mathbb{Z}$  is a Noetherian ring.
- Any PID is a Noetherian ring.
- $k[x_1, x_2, \dots]$  is not a Noetherian ring. Consider  $\mathfrak{i} = \langle x_1, x_2, \dots \rangle$ , which is not finitely generated.

## 2 7 April 2008

### 2.1 From last time ...

Last time, we were proving that affine algebraic sets can be defined by finitely many polynomials. This came down to proving that  $k[x_1, \dots, x_n]$  is Noetherian (Chapter 2).

**Theorem (Hilbert Basis).** *If  $A$  is Noetherian, then  $A[x]$  is Noetherian.*

*Proof.* Let us assume  $A[x]$  is not Noetherian. Let  $\mathfrak{i} \subseteq A[x]$  be an ideal which is not finitely generated. Pick  $f_1 \in \mathfrak{i}$ ,  $f_1 \neq 0$ ,  $\deg(f_1)$  is minimal. Then  $\mathfrak{i} \neq \langle f_1 \rangle$ , so pick  $f_2 \in \mathfrak{i} \setminus \langle f_1 \rangle$ ,  $\deg f_2 \geq \deg f_1$ . Since  $\mathfrak{i}$  is not finitely generated,  $\mathfrak{i} \neq \langle f_1, f_2 \rangle$ . Pick  $f_3 \in \mathfrak{i} \setminus \langle f_1, f_2 \rangle$ ,  $\deg f_3 \geq \deg f_2$ . Continue, and produce  $f_1, f_2, \dots, f_l, \dots$  such that  $f_l \notin \langle f_1, \dots, f_{l-1} \rangle$  and  $\deg f_1 \leq \deg f_2 \leq \dots$ . Let  $L(f)$  be the leading coefficient of a polynomial  $f \in A$ . Define  $\mathfrak{f}_m$  as the ideal spawned by  $L(f_1), \dots, L(f_m)$  in  $A$ . Clearly,  $\mathfrak{f}_1 \subseteq \mathfrak{f}_2 \subseteq \dots \subseteq A$  is an ascending chain. Then, since  $A$  is Noetherian,  $\mathfrak{f}_m = \mathfrak{f}_{m+1} = \dots$  for some  $m$ . This means that  $L(f_{m+1}) \in \mathfrak{f}_m$ , so there exist  $a_1, \dots, a_m \in A$  such that  $L(f_{m+1}) = a_1 L(f_1) + \dots + a_m L(f_m)$ . Let

$$f = f_{m+1} - \sum_{i=1}^m a_i X^{\deg f_{m+1} - \deg f_i} f_i \in \mathfrak{i}$$

Now notice that

- $L(f) = 0$  and  $\deg f < \deg f_{m+1}$ .
- $f \notin \langle f_1, \dots, f_m \rangle$ . This violates the fact that  $\deg(f_{m+1})$  is minimal in  $\mathfrak{i} \setminus \langle f_1, \dots, f_m \rangle$ .

This shows  $A[x]$  is Noetherian. □

### 2.2 More on affine algebraic sets

**Lemma.** *If  $S_i \subseteq k[x_1, \dots, x_n]$  for each  $i$ , then*

- (1) *If  $S_1 \subseteq S_2$ , then  $\mathcal{Z}(S_2) \subseteq \mathcal{Z}(S_1) \subseteq \mathbb{A}^n$ .*
- (2)  $\bigcap_i \mathcal{Z}(S_i) = \mathcal{Z}(\bigcup_i S_i)$
- (3) *Let  $S_1, S_2$  be arbitrary. Define  $S = S_1 S_2 = \{fg : f \in S_1, g \in S_2\}$ . Then  $\mathcal{Z}(S_1) \cup \mathcal{Z}(S_2) = \mathcal{Z}(S)$*   
(1) and (2) are easy, so we prove (3).

*Proof.*

( $\subseteq$ ) Pick  $p \in \mathcal{Z}(S_1)$ . We want  $p \in \mathcal{Z}(S)$ . Indeed, for all  $f \in S_1$ ,  $f(p) = 0$ , hence  $fg(p) = 0$ , hence  $p \in \mathcal{Z}(S)$ .

( $\supseteq$ ) Pick  $p \in \mathcal{Z}(S)$ . Assume  $p \notin \mathcal{Z}(S_1) \cup \mathcal{Z}(S_2)$ . This means there exist  $f_1 \in S_1$ ,  $f_1(p) \neq 0$  and  $f_2 \in S_2$ ,  $f_2(p) \neq 0$ . Hence,  $f_1 f_2(p) \neq 0$ , contradiction.

□

## 2.3 Aside on topological spaces

**Definition.** Let  $X$  be any set. Let  $\mathcal{F}$  be a collection of subsets of  $X$  such that

- (1)  $\emptyset, X$  are in  $\mathcal{F}$ .
- (2) finite unions of sets in  $\mathcal{F}$  are still in  $\mathcal{F}$
- (3) arbitrary intersections of sets in  $\mathcal{F}$  are still in  $\mathcal{F}$ .

Then  $(X, \mathcal{F})$  is said to be a *topological space*. The sets in  $\mathcal{F}$  are called the *closed sets* of  $X$ . Their complements in  $X$  are called the *open sets* of  $X$ .

### Examples

- $X, \mathcal{F} = \{Y : Y \subseteq X\} = \mathcal{P}(X)$ . All subsets of  $X$  are closed.
- $(\mathbb{R}, \text{usual topology})$ . A set is open if it is a union of open intervals  $(a, b)$ .
- $(\mathbb{R}, \text{cofinite topology})$ . The closed sets are  $\mathbb{R}, \emptyset$ , all finite sets.
- If  $k$  is any field, define the *Zariski topology* on  $\mathbb{A}^n$  as the topology whose closed sets are all  $\mathcal{Z}(S)$ . By the lemma, this is indeed a topology on  $\mathbb{A}^n$ .

We may check that when  $k = \mathbb{R}, n = 1$ , this recovers the cofinite topology.

- Generally, if  $(X, \mathcal{F})$  is any topological space and  $Y \subseteq X$ , then  $Y$  inherits a topology from  $X$ . The closed sets of  $Y$  are the sets  $F \cap Y$  where  $F \in \mathcal{F}$ . Any  $Y \subseteq \mathbb{A}^n$  comes equipped with the Zariski topology from  $\mathbb{A}^n$ .

## 3 9 April 2008

Last time, we defined  $\mathcal{Z} \equiv \{\text{ideals in } k[x_1, \dots, x_n]\} \rightarrow \{\text{affine algebraic sets in } \mathbb{A}^n\}$ . We don't know when  $\mathcal{Z}(\mathfrak{i}) = \emptyset$ . It is clear that if  $\mathfrak{i} = (1)$ , then  $\mathcal{Z}(\mathfrak{i}) = \emptyset$ . If  $k = \mathbb{R}, \mathfrak{i} = (x^2 + 1)$ ,  $\mathcal{Z}(\mathfrak{i}) = \emptyset$ . From now on, assume  $k = \bar{k}$  (that is,  $k = \mathbb{C}$ ).

**Theorem** (Weak Hilbert Nullstellensatz). *If  $\mathfrak{i} \subseteq \mathbb{C}[x_1, \dots, x_n], \mathfrak{i} \neq (1)$ , then  $\mathcal{Z}(\mathfrak{i}) \neq \emptyset$ .*

(Proof deferred.)

### 3.1 Ideals of algebraic sets

**Definition.** If  $X \subseteq \mathbb{A}^n$  is an algebraic set, define

$$I(X) = \{f \in k[x_1, \dots, x_n] : f(p) = 0 \forall p \in X\} \xrightarrow{\text{ideal}} k[x_1, \dots, x_n]$$

## Examples

- If  $X = \emptyset$ , then  $I(X) = k[x_1, \dots, x_n]$  and  $\mathcal{Z}I(X) = \emptyset = X$ .
- If  $X = \mathbb{A}^n$ , then  $I(X) = \{0\}$  and  $\mathcal{Z}I(X) = \mathbb{A}^n = X$ .
- If  $X = \{(0, \dots, 0)\} \subseteq \mathbb{A}^n$ , then  $I(X) = (x_1, \dots, x_n)$  and  $\mathcal{Z}I(X) = \{(0, \dots, 0)\} = X$ .
- If  $X = \{y = x^2\} \subseteq \mathbb{A}^n$ . If  $f \in I(X)$ , then  $f(x, x^2) = 0$  for all  $x$ .  
*Claim.*  $f \in (y - x^2)$

*Proof.*  $f = \sum a_{ij}x^i y^j = \sum a_{ij}x^i (y - x^2 + x^2)^j = \sum b_{ij}x^i (y - x^2)^j$ . Since  $f(x, x^2) = 0$ , we see that  $b_{i0} = 0$  for all  $i$ , so  $f \in (y - x^2)$   $\square$

Again,  $\mathcal{Z}I(X) = X$ .

- $X = \{x = 0 \text{ or } y = 0\} = \{xy = 0\}$ . Then  $I(X) = (xy)$  and  $\mathcal{Z}I(X) = X$ .

**Lemma.** Suppose  $X_1, X_2, X \subseteq \mathbb{A}^n$ .

- (1) If  $X_1 \subseteq X_2$  then  $I(X_2) \subseteq I(X_1)$ .
- (2)  $\mathcal{Z}I(X) = X$

*Proof.* Part 1 is clear, so we prove 2.

( $\supseteq$ ) Pick  $p \in X$  and  $f \in I(X)$ . Then  $f(p) = 0$  for all  $f \in I(X)$ , hence  $p \in \mathcal{Z}I(X)$ .

( $\subseteq$ ) We know  $X = \mathcal{Z}(J)$ . We want  $\mathcal{Z}I(\mathcal{Z}(J)) \subseteq \mathcal{Z}(J)$ . It is sufficient to show  $J \subseteq I\mathcal{Z}(J)$ . To see this, pick  $f \in J$ , so for all  $P \in \mathcal{Z}(J)$ ,  $f(P) = 0$ . Hence,  $f \in I\mathcal{Z}(J)$ .

$\square$

Is  $I$  truly the inverse of  $\mathcal{Z}$ ? True or false: if  $\mathfrak{i} \subseteq k[x_1, \dots, x_n]$ , then  $I(\mathcal{Z}(\mathfrak{i})) = \mathfrak{i}$ ?

## Examples

- $\mathfrak{i} = (x_1, \dots, x_n)$ . Then  $\mathcal{Z}(\mathfrak{i}) = (0, \dots, 0)$  and  $I\mathcal{Z}(\mathfrak{i}) = (x_1, \dots, x_n) = \mathfrak{i}$ . Check.
- $\mathfrak{i} = (f)$  ( $f$  is single variable). Write  $f = (x - a_1)^{\alpha_1} \cdots (x - a_m)^{\alpha_m}$ . Then  $\mathcal{Z}(\mathfrak{i}) = \{a_1, \dots, a_m\}$  and  $I\mathcal{Z}(\mathfrak{i}) = \langle (x - a_1) \cdots (x - a_m) \rangle \neq \mathfrak{i}$ .

But we can see the problem in the second example; it is the differing values of  $\alpha_1, \dots, \alpha_m$ . This motivates the following definitions:

**Definition.** The *radical* of an ideal  $\mathfrak{i}$  is

$$\sqrt{\mathfrak{i}} = \{f : f^r \in \mathfrak{i} \text{ for some } r > 0\}$$

**Example.**  $\sqrt{\langle (x - a_1)^{\alpha_1} \cdots (x - a_m)^{\alpha_m} \rangle} = \langle (x - a_1) \cdots (x - a_m) \rangle$ .

**Definition.** An ideal  $\mathfrak{i}$  is *radical* if  $\sqrt{\mathfrak{i}} = \mathfrak{i}$ .

**Lemma.**  $\sqrt{\mathfrak{i}}$  is an ideal.

*Proof.* Let  $a, b \in \sqrt{i}$ , so  $a^n \in i$  and  $b^m \in i$  for some  $n, m$ . We want  $a + b \in \sqrt{i}$ . In fact,  $(a + b)^{m+n} \in i$ . To see this, we compute

$$(a + b)^{m+n} = \sum_{\alpha+\beta=m+n} \binom{m+n}{\alpha} a^\alpha b^\beta$$

For each summand, either  $\alpha \geq n$  or  $\beta \geq m$ , hence  $a^\alpha \in i$  or  $b^\beta \in i$ , hence the expression is in  $i$ .  $\square$

**Theorem** (Strong Nullstellensatz).  $I\mathcal{Z}(i) = \sqrt{i}$

*Remark.* Strong Nullstellensatz implies Weak Nullstellensatz. Indeed, if  $\mathcal{Z}(i) = \emptyset$ , then  $I\mathcal{Z}(i) \ni 1$ , hence  $1 \in \sqrt{i}$ , hence  $1 \in i$ , hence  $i = (1) = k[x_1, \dots, x_n]$ .

**Example.**  $i = (x^3y, xy^4) \subseteq k[x, y]$ . Then  $(xy)^3 = x^3y \cdot y^2 \in i$ , and so  $xy \in \sqrt{i}$ . If  $f \in \sqrt{i}$ , then  $f^r = x^3y_{--} + xy^4_{--} = xy(\_)$ , hence  $\sqrt{i} = (xy)$ .  $\mathcal{Z}(i) = \{x = 0 \text{ or } y = 0\}$ . Then  $I\mathcal{Z}(i) = (xy) = \sqrt{i}$ .

## 4 11 April 2008

We want to show that if  $i \subseteq k[x_1, \dots, x_n]$  and  $1 \notin i$ , then  $\mathcal{Z}(i) \neq \emptyset$ .

### 4.1 Resultants

Let  $A$  be a ring and  $f, g \in A[x]$ ,  $n = \deg(f)$ ,  $m = \deg(g)$ , with

$$\begin{aligned} f &= a_0 + a_1x + \dots + a_nx^n \\ g &= b_0 + b_1x + \dots + b_mx^m \end{aligned}$$

Do  $f$  and  $g$  have common zeroes?

**Definition.** The *resultant* of  $f$  and  $g$  is the  $(m+n) \times (m+n)$  determinant (Sylvester determinant):

$$R_{f,g} = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 \\ 0 & 0 & a_0 & \cdots & a_{n-2} & a_{n-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & \cdots & 0 \\ 0 & b_0 & \cdots & b_{m-1} & b_m & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix} \in A$$

**Example.**  $f = x - a$ ,  $g = b_0 + b_1x + b_2x^2$ . Then

$$R_{f,g} = \begin{vmatrix} -a & 1 & 0 \\ 0 & -a & 1 \\ b_0 & b_1 & b_2 \end{vmatrix} = -a(-ab_2 - b_1) - (-b_0) = b_2a^2 + b_1a^2 + b_0 = g(a)$$

We conclude that  $R_{f,g} = 0$  implies that  $f, g$  have common roots.

**Theorem.**  $R_{f,g}$  belongs to the ideal  $(f, g)$  in  $A[x]$ .

*Proof.* With column operations, replace the first column with

$$\text{1st column} + x \text{ 2nd column} + x^2 \text{ 3rd column} + \dots + x^{m+n-1} \text{ last column}$$

It becomes  $(f(x), xf(x), \dots, x^{m-1}f(x), g(x), xg(x), \dots, x^{n-1}g(x))^T$ . Then expand the determinant along the first column to get

$$R_{f,g} = f(x)P(x) + g(x)Q(x)$$

for some polynomials  $P$  and  $Q$ . □

**Theorem.**

(1) If  $f, g$  have a common non-constant factor, then  $R_{f,g} = 0$ .

(2) If  $f = \prod_{i=1}^n (x - \lambda_i)$  and  $g = \prod_{j=1}^m (x - \mu_j)$ , then  $R_{f,g} = \prod_{i,j} (\mu_j - \lambda_i)$ .

*Proof of (1).* Let  $h$  be a common non-constant factor. Then  $f = \bar{f}h$  and  $g = \bar{g}h$  for some  $\bar{f}, \bar{g}$  with  $\deg \bar{f} < n$  and  $\deg \bar{g} < m$ . Then  $\bar{f}g = \bar{g}f$ . Write

$$\begin{aligned}\bar{f} &= \alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} \\ \bar{g} &= \beta_0 + \beta_1 x + \dots + \beta_{m-1} x^{m-1}\end{aligned}$$

where at least one  $\alpha_i$  and one  $\beta_i$  is nonzero. That is,

$$\begin{aligned}(\alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1})(\beta_0 + \beta_1 x + \dots + \beta_{m-1} x^{m-1}) = \\ (\beta_0 + \beta_1 x + \dots + \beta_{m-1} x^{m-1})(\alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1})\end{aligned}$$

Expanding and equating like coefficients, we find

$$\begin{aligned}a_0 \beta_0 - b_0 \alpha_0 &= 0 \\ a_0 \beta_1 + a_1 \beta_0 - b_1 \alpha_0 - b_0 \alpha_1 &= 0 \\ a_0 \beta_2 + a_1 \beta_1 + a_2 \beta_0 - b_2 \alpha_0 - b_1 \alpha_1 - b_2 \alpha_2 &= 0 \\ &\dots\end{aligned}$$

That is, we get  $(m+n)$  equations in  $(\beta_0, \dots, \beta_{m-1}, -\alpha_0, \dots, -\alpha_{n-1})$ , which is  $(m+n)$  variables. Therefore, the system must have zero determinant (because it has a non-trivial solution), and its matrix of coefficients is the matrix from the definition of  $R_{f,g}$ . □

*Remark.* Let  $f, g$  be monic polynomials,  $f = \prod_{i=1}^n (x - \lambda_i)$  and  $g = \prod_{j=1}^m (x - \mu_j)$ . Then  $R_{f,g} = \prod_{i,j} (\mu_j - \lambda_i) = \prod_{j=1}^m f(\mu_j)$ . In particular,

$$R_{f_1 f_2, g} = R_{f_1, g} R_{f_2, g}$$

Moreover, if  $g$  and  $r$  are any polynomials with  $r$  monic, then

$$R_{gQ+r, g} = \prod_j (gQ+r)(\mu_j) = \prod_j r(\mu_j) = R_{r, g}$$

## 5 14 April 2008

Last time, we looked at  $f, g \in A[x]$  for a ring  $A$ .

*Remark.* If  $f, g$  have a common factor, then  $R_{f,g} = 0$ . We wrote  $f = h\bar{f}$ ,  $\deg \bar{f} < \deg f$  and likewise for  $g = h\bar{g}$ .

Let us assume in addition that  $A$  is an integral domain, e.g. whenever  $a \neq 0, b \neq 0$ , then  $ab \neq 0$ .

*Remark.* If  $A$  is UFD (unique factorization domain), then  $R_{f,g} = 0$  implies  $f$  and  $g$  have a common factor.

*Check.* If  $R_{f,g} = 0$ , then  $f\bar{g} = \bar{f}g$  for some  $\bar{f}, \bar{g}$ , hence  $f$  and  $g$  have a common factor.  $\square$

We need to show: if  $A$  is a domain and  $f(x) = \prod_i (x - \lambda_i)$ ,  $g(x) = \prod_j (x - \mu_j)$ , then  $R_{f,g} = \prod_{i,j} (\mu_j - \lambda_i)$ .

*Proof.* Let  $f(x) = a_0 + a_1x + \dots + x^n$  and  $g(x) = b_0 + b_1x + \dots + x^m$ . Since  $f(x) = (x - \lambda_1) \dots (x - \lambda_n)$ , we can write

$$\begin{aligned} a_0 &= (-\lambda_1) \dots (-\lambda_n) && \text{degree } n \text{ in } \lambda\text{'s} \\ a_1 &= \sum (\lambda_1) \dots (-\lambda_n) && \text{degree } n - 1 \text{ in } \lambda\text{'s} \\ &\dots \\ a_{n-1} &= (-\lambda_1) + \dots + (-\lambda_n) && \text{degree } 1 \text{ in } \lambda\text{'s} \end{aligned}$$

Let us regard  $\lambda$ 's and  $\mu$ 's as variables of degree 1, so  $\deg(a_i) = n - i$ ,  $\deg(b_i) = m - i$ .

*Claim.*  $R_{f,g}$  is a polynomial in  $\lambda, \mu$ 's of degree  $nm$ .

Moreover,  $R_{f,g}$  vanishes if  $\lambda_i = \mu_j$  for some  $(i, j)$ . This implies  $\prod_{i,j} (\mu_j - \lambda_i) \mid R_{f,g}$ , hence  $R_{f,g} = (\text{constant}) \prod_{i,j} (\mu_j - \lambda_i)$ . To determine the constant ( $c = 1$ ), pick  $f = x^n + a_{n-1}x^{n-1} + \dots + a_0$ ,  $g = x^m$ . Get  $R_{f,g} = a_0^m = (-\lambda_0)^m \dots (-\lambda_n)^m = \prod_{i,j} (\mu_j - \lambda_i)$ , hence  $c = 1$ .

*Proof of claim.* Let  $(r_{ij})$  be entries of the matrix  $R_{f,g}$ . Then

$$\deg(r_{ij}) = \begin{cases} n + i - j & \text{if } 1 \leq i \leq m \\ i - j & \text{if } m + 1 \leq i \leq m + n \end{cases}$$

By the explicit formula for determinant,  $R_{f,g} = \sum_{\sigma \in S_{m+n}} (-1)^\sigma r_{1,\sigma(1)} \dots r_{m+n,\sigma(m+n)}$ . Then

$$\begin{aligned} \deg R_{f,g} &= \sum_{i=1}^m (n - i - \sigma(i)) + \sum_{i=m+1}^{m+n} (i - \sigma(i)) \\ &= mn + \sum_{i=m+1}^{m+n} (i - \sigma(i)) \\ &= mn \end{aligned}$$

$\square$

$\square$

## 5.1 More remarks about resultants

- If  $f = a_n \prod (x - \lambda_i)$  and  $g = b_m \prod (x - \mu_j)$ , then  $R_{f,g} = a_n^m b_m^n \prod (\mu_j - \lambda_i)$ . In particular,  $R_{f_1 f_2, g} = R_{f_1, g} R_{f_2, g}$  if  $f_1, f_2, g$  split.
- This relation holds even if  $f_1, f_2, g$  don't split as a product of linear forms. Why?

**Lemma** (optional). *Any domain  $A$  is contained in an algebraically closed field where  $f_1, f_2, g$  split.*

(Proof omitted)

- If  $f, g \in k[x, y] = A[y]$  where  $A = k[x]$ , then  $R_{f,g}^{(1)} \in k[x]$  by regarding  $f, g$  as polynomials in  $y$ . Likewise, when regarding  $f, g$  as a polynomial in  $x$ , have  $R_{f,g}^{(2)} \in k[y]$ , which is different.

*Note.* If  $f, g$  have a common factor in  $k[x, y]$ , it is *not* true that  $R_{f,g}^{(1)} = 0$ . It could be that the common factor is a polynomial in  $X$ , but then in this case  $R_{f,g}^{(2)} = 0$ .

- If  $f, g$  are homogeneous of degrees  $n$  and  $m$  respectively, then  $R_{f,g}^{(1)}$  or  $R_{f,g}^{(2)}$  have degree  $nm$  as polynomials in  $k[x]$  and  $k[y]$ .

*Proof.* Write  $f = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \dots + a_0(x)y^0$  and  $g = b_m(x)y^m + a_{m-1}y^{m-1} + \dots + b_0(x)y^0$ . Then  $\deg a_n(x) = 0$ ,  $\deg a_{n-1}(x) = 1$ , etc., and likewise for the  $b_i$ 's. That is,  $\deg a_i = n - i$  and  $\deg b_i = m - i$ , which is the only assumption used when proving the claim above.  $\square$

- If  $f, g \in k[x_1, \dots, x_n]$ , then get  $n$  resultants  $R_{f,g}^{(1)}, \dots, R_{f,g}^{(n)}$ . If  $f, g$  are homogenous of degree  $d, e$ , then each of the resultants has degree  $de$ .

## 6 16 April 2008

### 6.1 The weak Nullstellensatz revisited

**Theorem** (Weak Nullstellensatz). *Let  $k$  be algebraically closed and let  $I \subseteq k[x_1, \dots, x_n]$  be an ideal with  $1 \notin I$ . Then  $\mathcal{Z}(I) \neq \emptyset$ .*

*Proof.* We induct on  $n$ . For  $n = 1$ ,  $I \subseteq k[x]$ , so  $I = \langle f \rangle$  for some non-constant  $f$ . Since  $f$  has a root  $a \in k$ , all polynomials in  $I$  vanish at  $a$ , hence  $a \in \mathcal{Z}(I) \neq \emptyset$ .

For the inductive step, we examine  $n = 2$ , which is representative. Take  $I \subseteq k[x, y]$  with  $1 \notin I$ . Let  $f \in I$  with  $\deg f = d$ .

**Lemma** (Noether normalization). *There exists  $\lambda \in k$  such that  $f(x + \lambda y, y) = cy^d + (\text{lower terms in } y)$ , where  $c \neq 0$ .*

*Proof.* Let  $f$  be written as a sum of homogeneous pieces  $f_{(d)} + f_{(d-1)} + \dots + f_{(0)}$  (i.e.  $f_{(i)}$  collects all terms of degree  $i$ ). It suffices only to consider  $f_{(d)}$ . Write

$$f_{(d)} = \sum_{i=0}^d a_i x^i y^{d-i} \quad a_i \in k, \text{ not all zero}$$

Then

$$f_{(d)}(x + \lambda y, y) = \sum_{i=0}^d a_i (x + \lambda y)^i y^{d-i} = \left( \sum_{i=0}^d a_i \lambda^i \right) y^d + (\text{lower terms})$$

We can pick  $\lambda \in k$  such that  $\sum_{i=0}^d a_i \lambda^i \neq 0$ , thus  $c \neq 0$ .  $\square$

Thus, changing coordinates  $x_{\text{new}} = x + \lambda y$ , we may assume  $I$  contains  $f$  of the form

$$f = y^d + y^{d-1}f_{d-1}(x) + \cdots + f_0(x)$$

Let  $\mathfrak{i} = I \cap k[x] \hookrightarrow k[x]$ . Clearly  $\mathfrak{i}$  is an ideal and  $1 \notin \mathfrak{i}$ . Thus, by the  $n = 1$  case, there exists  $a \in k$  such that all polynomials in  $\mathfrak{i}$  vanish at  $a$ . Let

$$J = \{f(a, y) : f \in I\} \xrightarrow{\text{ideal}} k[y]$$

By induction, if  $1 \notin J$  then there will exist  $b \in k$  such that  $b \in \mathcal{Z}(J)$  and thus  $f(a, b) = 0$  for all  $f \in I$ . This will give us  $\mathcal{Z}(I) \neq \emptyset$  as desired.

To show  $1 \notin J$ , assume on the contrary that  $1 \in J$ . Then there exists  $g \in I$  with  $g(a, y) = 1$ . Let  $g = Y^e g_e(x) + y^{e-1} g_{e-1}(x) + \cdots + g_0(x)$ , and we must have that  $g_0(a) = 1$  and all other  $g_i(a) = 0$ . Now regard  $g$  and  $f$  as polynomials in  $y$  and look at the resultant  $R_{g,f} \in k[x]$ . Also,  $R_{g,f} \in \langle f, g \rangle \hookrightarrow \mathfrak{i}$ , so we must have  $R_{g,f}(a) = 0$ . On the other hand,

$$R_{g,f}(a) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & 0 \\ * & * & \cdots & 1 & 0 \\ * & * & * & \cdots & 1 \end{vmatrix} = 1$$

(That is, the matrix is lower triangular with 1's on the diagonal). This is a contradiction, completing the proof.  $\square$

## 6.2 The strong Nullstellensatz revisited

**Theorem** (Strong Nullstellensatz).  $I(\mathcal{Z}(\mathfrak{i})) = \sqrt{\mathfrak{i}}$ .

*Proof.* We first show  $\sqrt{\mathfrak{i}} \subseteq I(\mathcal{Z}(\mathfrak{i}))$ . If  $f \in \sqrt{\mathfrak{i}}$ , then for any  $p \in \mathcal{Z}(\mathfrak{i})$  we have  $f^r(p) = 0$  for some  $r > 0$ . Hence  $f(p) = 0$  for all  $p \in \mathcal{Z}(\mathfrak{i})$ , hence  $f \in I(\mathcal{Z}(\mathfrak{i}))$  as needed.

For the reverse inclusion, let  $f \in I(\mathcal{Z}(\mathfrak{i}))$ , and let  $f_1, \dots, f_r$  be generators for the ideal  $\mathfrak{i}$ . We want that  $f^N$  can be expressed as  $f_1 g_1 + \cdots + f_r g_r \in \mathfrak{i}$  (hence  $f \in \sqrt{\mathfrak{i}}$ ). Let  $J = \langle f_1, \dots, f_r, tf - 1 \rangle \subseteq k[x_1, \dots, x_n, t]$ .

*Claim.*  $\mathcal{Z}(J) = \emptyset$ , therefore by the weak Nullstellensatz,  $1 \in J$ .

*Proof.* If all  $f_1(p) = \cdots = f_r(p) = tf(p) - 1 = 0$  for some  $(p, t)$ , then we have  $p \in \mathcal{Z}(\mathfrak{i})$  but  $f(p) \neq 0$ , a contradiction.  $\square$

How does this complete the proof? Find out next time.  $\square$

## 7 18 April 2008

### 7.1 Irreducible components

*See handout.*

## 8 21 April 2008

We still have a theorem to prove from last time.

**Theorem.**  $X$  is irreducible iff  $I(X)$  is prime.

*Proof.* We prove that  $X$  is reducible iff  $I(X)$  is not prime. Assume  $X$  is reducible, and write  $X = X_1 \cup X_2$ , with  $X_1, X_2 \subsetneq X$ . Then  $I(X_1) \neq I(X)$ . Pick  $f \in I(X_1) \setminus I(X)$  and  $g \in I(X_2) \setminus I(X)$ . Then  $fg$  vanishes on  $X_1$  because  $f = 0$  on  $X_1$ , and it vanishes on  $X_2$  because  $g = 0$  on  $X_2$ . Hence,  $fg = 0$  on  $X = X_1 \cup X_2$ , so  $fg \in I(X)$ .

Conversely, assume  $I(X)$  is not prime, and pick  $f, g \notin I(X)$  with  $fg \in I(X)$ . Define  $X_1$  as the vanishing of the ideal  $(f) + I(X)$ , so  $f = 0$  on  $X_1$  but not on  $X$ , hence  $X_1 \neq X$ . Likewise, define  $X_2$  as the vanishing of the ideal  $(g) + I(X)$ . Then  $X_1 \cup X_2 \supseteq X$ . If  $x \in X$ , then  $fg(x) = 0$ , hence  $f(x) = 0$  or  $g(x) = 0$ , hence  $x \in X_1$  or  $x \in X_2$ .  $\square$

**Theorem.** Any  $X$  algebraic set in  $\mathbb{A}^n$  can be written as  $X = \bigcup x_i$ , where the  $x_i$  are irreducible algebraic sets such that  $X_i \not\subseteq x_j$  if  $i \neq j$ . Moreover, this decomposition is unique (homework).

*Remark.* We may refer to algebraic sets as “closed” in reference to the Zariski topology.

*Proof.* Assume the theorem is false for  $X$ . In particular,  $X$  is not irreducible, so write  $X = X_1 \cup X'_1$ . The theorem must be false for  $X_1$  or for  $X'_1$ . Assume it is false for  $X'_1$ , and break  $X'_1 = X_2 \cup X'_2$ . Continue in this fashion. We claim that the process stops. Indeed, otherwise we will produce an infinite chain  $X \supsetneq X'_1 \supsetneq X'_2 \supsetneq X'_3 \subsetneq \dots$ , thus  $X$  is not Noetherian. By homework 2,  $\mathbb{A}^n$  is Noetherian, and by homework 1  $X \subseteq \mathbb{A}^n$  is Noetherian, contradiction.  $\square$

*Remark.* Any radical ideal in  $k[x_1, \dots, x_n]$  is an intersection of prime ideals. In fact, this holds for radical ideals in any Noetherian ring.

### Examples.

(1)  $X = \{y^3 - xy = 0\} \subseteq \mathbb{A}^2$ . Then  $y(y^2 - x) = 0$ , so  $y = 0$  or  $y^2 - x = 0$ . The irreducible components are the line  $y = 0$  and the parabola  $y^2 - x = 0$ , which are irreducible because they are defined by irreducible polynomials.

(2)  $X = \{xz - y^2 = x^3 - yz = 0\}$ .

- If  $x \neq 0$ , then  $xz = y^2$  gives  $z = y^2/x$ , so  $x^3 = yz$  implies  $x^3 = y^3/x$ . Hence  $x = (y/x)^3$ . Let  $t = y/x$ , so  $x = t^3, y = t^4, z = t^5$ .
- If  $x = 0$  and  $y = 0$ , the equations are satisfied, hence the  $z$ -axis is contained in  $X$ .

We get that  $X = X_1 \cup X_2$ , where  $X_1 = \{(t^3, t^4, t^5)\}$  and  $X_2$  is the  $z$ -axis. We claim that  $X_1$  is irreducible, which is a consequence of the following lemma.

**Lemma.** Let  $f: \mathbb{A}^n \rightarrow \mathbb{A}^m$  be a polynomial map and let  $X \subseteq \mathbb{A}^n$  be irreducible. Then  $f(X)$  is irreducible in  $\mathbb{A}^m$ .

*Remark.* It is false that the preimage of an irreducible set is irreducible. As a counterexample, let  $f: \mathbb{A}^2 \rightarrow \mathbb{A}^1$  by  $(x, y) \mapsto xy$ . Then  $f^{-1}(0)$  is the union of the axes.

*Proof of lemma.* If  $f(X) \subseteq X_1 \cup X_2$  where  $X_1$  and  $X_2$  are algebraic subsets, then  $X \subseteq f^{-1}(X_1) \cup f^{-1}(X_2)$ . By homework 1,  $f^{-1}(X_1)$  and  $f^{-1}(X_2)$  are algebraic sets, hence  $f(X) \subseteq X_1$  or  $f(X) \subseteq X_2$ , which is a contradiction.  $\square$

## 9.1 Dimension

**Definition.** Let  $X$  be an irreducible algebraic set (or an irreducible Noetherian topological space). Consider all chains

$$X \supsetneq X_1 \supsetneq \dots \supsetneq X_n \neq \emptyset$$

where the  $X_i$  are irreducible algebraic subsets of  $X$ . The maximal length of such chains is called the *dimension* of  $X$ .

**Examples.**

- (1)  $\dim \mathbb{A}^1 = 1$ . Indeed,

$$\mathbb{A}^1 \supsetneq \{\text{point}\} \neq \emptyset$$

hence  $\dim \mathbb{A}^1 \geq 1$ . There are no chains

$$\mathbb{A}^1 \supsetneq X_1 \supsetneq X_2 \neq \emptyset$$

since  $X_1$  and  $X_2$  must be points, so  $X_1 = X_2$ .

- (2)  $\dim \mathbb{A}^2 = 2$ . A chain of length 2 is

$$\mathbb{A}^2 \supsetneq \{x\text{-axis}\} \supsetneq \{\text{point}\} \neq \emptyset$$

There are no chains of length 3, since if

$$\mathbb{A}^2 \supsetneq X_1 \supsetneq X_2 \supsetneq X_3 \neq \emptyset$$

Irreducible subsets of  $\mathbb{A}^2$  are points or  $\mathcal{Z}(f)$  for irreducible  $f$ . Then  $X_1 = \mathcal{Z}(f)$  and  $X_2 = \mathcal{Z}(g)$  for  $f$  and  $g$  irreducible. Since  $\mathcal{Z}(f) \supset \mathcal{Z}(g)$ , we must thus have  $\sqrt{(f)} \subseteq \sqrt{(g)}$ . Thus,  $f^r \in (g)$  for some  $r$ , i.e.  $g \mid f^r$ , hence  $g = f$  since  $g$  and  $f$  are irreducible.

- (3)  $\dim \mathbb{A}^n \geq n$ , since we have the chain

$$\mathbb{A}^n \supsetneq \{(0, x_2, \dots, x_n)\} \supsetneq \{(0, 0, x_3, \dots, x_n)\} \supsetneq \dots \supsetneq \{(0, \dots, 0)\}$$

- (4) If  $X = \mathcal{Z}(f)$  where  $f \in \mathbb{C}[x, y]$  is a nonconstant irreducible polynomial, then  $\dim \mathcal{Z}(f) = 1$ .

*Proof.* The chain of length 1  $\mathcal{Z}(f) \supsetneq \{\text{point}\}$  exists by Nullstellensatz. There are no chains of length 2, since we would then have

$$\mathbb{A}^2 \supsetneq \mathcal{Z}(f) \supsetneq X_1 \supsetneq X_2 \neq \emptyset$$

and we have seen from example (2) that this cannot happen.  $\square$

- (5) If  $f: \mathbb{A}^1 \rightarrow \mathbb{A}^m$  is a non-constant polynomial map, then  $f(\mathbb{A}^1)$  has dimension 1. It cannot have more since we know

$$\mathbb{A}^1 \supsetneq f^{-1}(X_1) \supsetneq f^{-1}(X_2) \neq \emptyset$$

is impossible from above, and hence

$$f(\mathbb{A}^1) \supsetneq X_1 \supsetneq X_2 \neq \emptyset$$

is impossible.

In particular, for the map  $t \mapsto (t^3, t^4, t^5)$ , the image has dimension 1.

If  $X$  is not irreducible, then  $\dim X$  is defined to be the maximum dimension of its irreducible components.

## 9.2 Functions on algebraic sets

Let  $X \subseteq \mathbb{A}^n$  be an affine algebraic set and consider

$$\{f: X \rightarrow k : \text{polynomial functions on } k\} \cong A(X) \cong k[x_1, \dots, x_n]$$

That is, there exists  $P(x_1, \dots, x_n)$  such that  $f$  is the restriction of  $P$  to  $X$ .  $P, Q$  give the same function  $f$  iff  $P - Q = 0$  on  $X$  iff  $P - Q \in I(X)$ . We call  $A(X)$  the *coordinate ring* of  $X$ .

### Examples.

- (1) If  $X = \mathbb{A}^1$ , then  $A(X) = k[X]$ . If  $X = \mathbb{A}^n$ , then  $A(X) \cong k[x_1, \dots, x_n]$ .
- (2) If  $X = \{y = 0\} \hookrightarrow \mathbb{A}^2$ , then  $A(X) = k[x, y]/(y) \cong k[x]$ .
- (3) If  $X$  is irreducible, then  $A(X)$  is an integral domain.

**Definition.** If  $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$ , then a *morphism*  $f: X \rightarrow Y$  is a polynomial map  $\mathbb{A}^n \rightarrow \mathbb{A}^m$  which sends  $X$  to  $Y$ .

**Definition.** A morphism  $f: X \rightarrow Y$  is an *isomorphism* if

- (1)  $f$  is bijective.
- (2)  $f^{-1}: Y \rightarrow X$  is also a morphism.

### Theorem.

- (1) If  $f: X \rightarrow Y$  is a morphism, then  $f^*: A(Y) \rightarrow A(X)$  is a ring homomorphism, where  $f^*$  is given by

$$\{g: Y \rightarrow \mathbb{A}^1\} \mapsto \{(g \circ f): X \rightarrow \mathbb{A}^1\}$$

- (2) Any ring homomorphism  $A(Y) \rightarrow A(X)$  comes from a morphism  $X \rightarrow Y$ .

**Corollary.**  $f: X \rightarrow Y$  is an isomorphism iff  $f^*: A(Y) \rightarrow A(X)$  is an isomorphism.

**Example.** Take  $f: \mathbb{A}^1 \rightarrow X$  given by  $t \mapsto (t^2, t^3)$ , where  $X = \{y^2 = x^3\} \supseteq \mathbb{A}^2$ . Is  $f$  an isomorphism? We check the conditions in the definition.  $f$  is bijective, but  $f^{-1}$  is not a polynomial map, since it is given by  $(x, y) \mapsto y/x$ . Hence,  $f$  is not an isomorphism.

## 10 25 April 2008

### 10.1 Morphisms continued

*Proof of theorem.* (1) is obvious, so we prove (2). Call the coordinates of  $X$   $x_1, \dots, x_n$  and the coordinates of  $Y$   $y_1, \dots, y_m$ . If  $\Phi = f^*$  where  $f = (f_1, \dots, f_m)$ , then  $\Phi(y_i) = f_i$ . For an arbitrary  $\Phi$ , set  $f_i = \Phi(y_i) \in A(X)$ , and so it can be represented by a polynomial. Set  $f = (f_1, \dots, f_m)$ , a polynomial function.

*Claim.*

- $f(X) \subseteq Y$ .
- $\Phi = f^*$

The latter is obvious because  $\Phi(y_i) = f^*(y_i) = f_i$ , hence  $\Phi(\sum a_I Y^I) = f^*(\sum a_I Y^I)$ . For the first point, let  $x \in X$  and  $f(x) \in Y$ . Let  $G \in I_Y$  (the ideal of  $Y$ ). We check that  $G(f(x)) = 0$ , which will show that  $f(x) \in \mathcal{Z}I(Y) = Y$ . That is, we must show that  $G \circ f|_x \equiv 0$ . We know  $G \equiv 0$  on  $Y$ , hence  $\Phi(G) \equiv 0$  on  $X$  (since  $\Phi$  is a homomorphism). It remains to check that  $\Phi \circ G = G \circ f$ , but we showed this in above (let  $G = \sum a_I Y^I$  in the above equality).  $\square$

### Examples.

- (1)  $\mathbb{A}^1$  and  $\mathbb{A}^2$  are not isomorphic, or equivalently there does not exist  $\mathbb{C}[x, y] \xrightarrow{\sim} \mathbb{C}[t]$ . Indeed, we would have  $x \mapsto \lambda t - a$  and  $y \mapsto \mu t - b$ , but then  $\mu x = \lambda y \mapsto (\text{constant})$  and  $(\text{constant}) \mapsto (\text{constant})$ .
- (2) Let  $X = \{y^2 = x^3\}$ , which is a *cuspidal curve*. Then  $f: \mathbb{A}^1 \rightarrow X$  given by  $t \mapsto (t^2, t^3)$  is a bijection. However,  $f$  is not an isomorphism, as  $f^*: \mathbb{C}[x, y]/(y^2 - x^3) \xrightarrow{\sim} \mathbb{C}[t]$ . Then  $f^*$  maps  $x \mapsto t^2$  and  $y \mapsto t^3$  and the image of  $f^*$  is  $\mathbb{C}[t^2, t^3]$ , so  $f^*$  is not bijective.  
*Claim.* But on the other hand,  $\mathbb{A}^1 \setminus \{0\} \cong X \setminus \{0\}$ .
- (3) Let  $X = \{y^2 = x^2(x + 1)\}$ , which appears as a loop with an X shape at the origin. Letting  $t = y/x$  and  $x + 1 = t^2$ , we get  $f: \mathbb{A}^1 \mapsto X$  by  $t \mapsto (t^2 - 1, t(t^2 - 1))$ . This  $f$  is not an isomorphism because it is not bijective, e.g.  $f(1) = f(-1) = (0, 0)$ .

## 10.2 Rational functions

Let  $X$  be an irreducible affine set, so  $A(X) = k[x_1, \dots, x_n]/I(X)$  is an integral domain. Let  $K(X)$  be the field of fractions of  $A(X)$ . That is,

$$K(X) \equiv \left\{ \frac{f(x)}{g(x)} : f, g \in A(X), g \neq 0 \text{ in } A(X) \right\}$$

and we define the equivalence relation

$$\frac{f(x)}{g(x)} = \frac{f'(x)}{g'(x)} \Leftrightarrow f g' - f' g = 0 \text{ in } A(X)$$

We can check that “=” is transitive.

**Definition.** A *rational function* on  $X$  is a partially defined function  $h \in K(X)$  on  $X$ . By partially defined, we mean that  $h = f/g$ , which is undefined at the points  $p$  for which  $g(p) = 0$ .

**Definition.** A rational function  $h$  is *regular* at  $p$  if  $h = f/g$  such that  $g(p) \neq 0$ . The *domain* of  $h$ , written  $\text{Dom}(h)$ , is  $\{p : h \text{ is regular at } p\}$ .

### Examples.

- (1) For  $X = \{y^2 = x^3\}$ ,  $h = y/x$  is a rational function.
- (2) For  $X = \{xy = zw\}$ ,  $h = z/x$  is a rational function. Note that  $h$  can also be written  $y/w$ .  $z/x$  is undefined where  $x = 0$ ,  $y/w$  is undefined where  $w = 0$ , and so  $\text{Dom } h = X \setminus \{x = w = 0\}$ .

**Definition.** A *rational map*  $f: X \dashrightarrow \mathbb{A}^m$  is a partially defined map, for which we may write  $f = (f_1, \dots, f_m)$  where  $f_i \in K(X)$ . A rational map  $f: X \dashrightarrow Y$  is a rational map  $f: X \dashrightarrow \mathbb{A}^m$  such that  $f(\text{Dom } f) \subseteq Y$ .

# 11 28 April 2008

## 11.1 Rational maps continued

**Lemma.** *If  $f$  is regular everywhere on  $X$ , then  $f \in A(X)$ .*

For this reason,  $A(X)$  is sometimes called the *ring of regular functions* on  $X$ .

*Proof.* Let  $I_f$  be the ideal of denominators of  $f$ . That is,

$$I_f = \{h \in A(X) : hf \in A(X)\} = \{h : f = g/h \text{ for some } g, h\} \cup \{0\}$$

Then  $\text{Dom } f = X \setminus \mathcal{Z}(I_f)$ . So,  $f$  is regular on  $X$  iff  $\mathcal{Z}(I_f) = \emptyset$  iff (by Nullstellensatz)  $1 \in I_f$  iff  $f \in A(X)$ .  $\square$

Do rational maps exist? Does  $\text{Dom } f = \bigcap \text{Dom } f_i \neq \emptyset$ ? Yes, otherwise  $X = \bigcup \mathcal{Z}(I_{f_i})$ . This cannot happen if  $x$  is irreducible.

*Remark.* Rational maps may not be possible to compose. For example, if  $f: X \dashrightarrow Y$  and  $g: Y \dashrightarrow Z$ , then  $g \circ f$  may be undefined because  $\text{Im}(\text{Dom } f)$  and  $\text{Dom } g$  may not intersect (homework).

**Definition.** An open set  $U \subseteq X$  has the form  $X \setminus \mathcal{Z}(I)$  (zero locus of polynomials).

**Example.**  $\mathbb{A}^1 \setminus \{0\}$  is open in  $\mathbb{A}^1$ , and  $\mathbb{A}^2 \setminus \{0\}$  is open in  $\mathbb{A}^2$ .

**Definition.** An open set  $U \subseteq X \subseteq \mathbb{A}^n$  is said to be a *quasi-affine algebraic set*.

**Definition.** A *morphism*  $f: U \rightarrow V$ , where  $U$  and  $V$  are respectively quasi-affine algebraic sets in  $X$  and  $Y$ , is a rational map  $f: X \dashrightarrow Y$  which is regular on  $U$  and  $f(U) \subseteq V$ .

An *isomorphism* is a morphism  $f$  which is bijective and for which  $f^{-1}: V \rightarrow U$  is also a morphism.

**Definition.**  $X$  and  $Y$  are *birational* if there exist open  $U \subseteq X, V \subseteq Y$  with an isomorphism  $U \rightarrow V$ .

An open question: classify all algebraic sets up to birational maps.

**Lemma.**  *$X$  and  $Y$  are birational if and only if  $K(X) \cong K(Y)$ . (Proof omitted, but fairly obvious).*

Note that by contrast,  $X \cong Y$  if and only if  $A(X) \cong A(Y)$ .

**Examples.**

- (1)  $X = \{y^2 = x^3\}$ . Consider the map  $f: \mathbb{A}^1 \rightarrow X$  by  $t \mapsto (t^2, t^3)$ . Then  $f$  is a birational isomorphism: it is bijective, and it has inverse  $g: X \dashrightarrow \mathbb{A}^1$  by  $(x, y) \mapsto y/x$ . But  $g$  is not defined at  $(0, 0)$ , so we instead take the same map  $g: X \setminus \{(0, 0)\} \rightarrow \mathbb{A}^1 \setminus \{0\}$ . Hence, although  $f$  is a birational isomorphism it is not a general isomorphism.
- (2)  $X = \{y^2 = x^2(x + 1)\}$ . Then  $f: \mathbb{A}^1 \rightarrow X$  by  $t \mapsto (t^2 - 1, t^3 - t)$  is not an isomorphism, but it is a birational isomorphism with inverse  $g: X \dashrightarrow \mathbb{A}^1$  by  $(x, y) \mapsto y/x$ , which is defined on  $X \setminus \{(0, 0)\} \xrightarrow{\sim} \mathbb{A}^1 \setminus \{\pm 1\}$ . Again,  $\mathbb{A}^1$  and  $X$  are birationally isomorphic, but not generally isomorphic.

Think about what happens here:  $X$  is a loop which crosses itself. We pull the loop apart to get  $\mathbb{A}^1$ . In the other direction, we glue  $\mathbb{A}^1$  to itself, specifically the points  $\pm 1$ .

- (3)  $X = \{y^2 = f(x)\}$  where  $\deg f = 3$ . Assume  $f(x) = x(x-1)(x-\lambda)$ , where  $\lambda \neq 0, 1$ . Graphing this, we plot  $y = \pm \sqrt{x(x-1)(x-\lambda)}$ , which intersects the  $x$ -axis at  $0, 1, \lambda$  and generally looks weird.  $X$  is said to be an *elliptic curve*.

There are no morphisms (other than constants) of  $\mathbb{A}^1 \rightarrow X$  (homework). Further, there are no nontrivial rational maps  $\mathbb{A}^1 \dashrightarrow X$  (for later).

- (4)  $X = \{xy = 1\} \subseteq \mathbb{C}^2$ , which is affine. Take  $f: X \rightarrow \mathbb{A}^1 \setminus \{0\}$  by  $(x, y) \mapsto x$ . Then  $g: \mathbb{A}^1 \setminus \{0\} \rightarrow X$  by  $x \mapsto (x, 1/x)$  is an inverse. So,  $f$  is an affine isomorphism. By abuse, a set isomorphic to an affine set will also be affine.
- (5)  $\mathbb{A}^2 \setminus \{0\}$  is not isomorphic to an affine set (homework).

## 12 30 April 2008

We have seen

$$\begin{array}{lll} \{\text{affine varieties}\} & \subsetneq & \{\text{quasi-affine varieties}\} \\ \{\text{morphisms}\} & \subsetneq & \{\text{morphisms}\} \\ \{XY = 1\} & \leftrightarrow & \mathbb{A}^1 \setminus \{0\}, \mathbb{A}^2 \setminus \{0\} \\ & & \text{(and next)} \\ \{\text{projective varieties}\} & \subseteq & \{\text{quasi projective}\} \end{array}$$

### 12.1 Intersections

- (1) (Line and conic). Take  $L = \{y = \lambda x\}$  and  $C = \{x^2 - y^2 = 1\}$ . We solve for the intersections and find they are

$$x = \pm \frac{1}{\sqrt{1 - \lambda^2}} \quad y = \pm \frac{\lambda}{\sqrt{1 - \lambda^2}}$$

that is, there are two intersections as long as  $\lambda \neq \pm 1$ , in which case there are no intersections.

- (2)  $L_1 = \{y = 0\}$ ,  $L_2 = \{y = 1 - \lambda x\}$ . Then  $L_1 \cap L_2 = \{(1/\lambda, 0)\} \rightarrow \infty$  as  $\lambda \rightarrow 0$ .

- (3) Two conics intersect in four points at most.

To do these justice, we need to count infinity as a point as well.

### 12.2 Projective space

The *projective space*  $\mathbb{P}_k^n = k^{n+1} \setminus 0$  with the equivalence

$$\mathbb{P}^n \ni (x_0, \dots, x_{n+1}) = (\lambda x_0, \dots, \lambda x_{n+1}) \quad \text{if } \lambda \in k \setminus \{0\}$$

We write this

$$[x_0 : x_1 : x_2 : \dots : x_n] = [\lambda x_0 : \lambda x_1 : \dots : \lambda x_n]$$

- (1)  $\mathbb{P}^1 \ni [x_0 : x_1]$  where  $x_0, x_1$  are not both zero. We can regard this as a single number  $x_0/x_1 \in \mathbb{C}$  if  $x_1 \neq 0$ . If  $x_1$  does equal zero, we might consider this  $\infty$ . Hence,  $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ .

(2) Is  $\mathbb{P}^n = \mathbb{A}^n \cup \{\infty\}$ ? No. As before, we might try converting

$$[x_0 : \dots : x_n] \leftrightarrow \left( \frac{x_0}{x_n}, \dots, \frac{x_{n-1}}{x_n} \right)$$

if  $x_n \neq 0$ . However, if  $x_n$  does equal 0, then we get

$$[x_0 : \dots : x_{n-1} : 0] \leftrightarrow [x_0 : x_1 : \dots : x_{n-1}]$$

A way to think of this recursively:  $\mathbb{P}^0 = \{\infty\}$ . Then  $\mathbb{P}^n = \mathbb{P}^{n-1} \cup \mathbb{C}^n$ .

### 12.3 Projective algebraic sets

**Definition.**  $f \in k[x_0, \dots, x_n]$  is *homogeneous of degree  $d$*  if  $f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$ . An ideal is *homogeneous* if it can be generated by homogeneous polynomials (not necessarily all of the same degree).

**Definition.** A *projective algebraic set* can be written

$$\mathcal{Z}(\mathfrak{a}) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n : f(x_0 : \dots : x_n) = 0 \forall f \in \mathfrak{a}\}$$

for a homogeneous ideal  $\mathfrak{a}$ .

If  $X \subseteq \mathbb{P}^n$  is a projective algebraic set, then  $I(X) \subseteq \mathbb{C}[x_0, \dots, x_n]$  as

$$I(X) = \{f \in \mathbb{C}[x_0, \dots, x_n] : f \equiv 0 \text{ on } X\}$$

We may check that  $I(X)$  is a homogeneous ideal.

#### Projective Nullstellensatz

There is a one-to-one correspondence

$$\begin{array}{ccc} \{\text{radical homogeneous ideals } \mathfrak{a} \neq \mathbb{C}[x_0, \dots, x_n]\} & \leftrightarrow & \{\text{projective algebraic sets in } \mathbb{P}^n\} \\ \mathfrak{a} & \mapsto & \mathcal{Z}(\mathfrak{a}) \\ I_X & \leftarrow & X \end{array}$$

A twist (Weak Projective Nullstellensatz):  $\mathcal{Z}(\mathfrak{a}) = \emptyset$  iff  $(x_0, \dots, x_n) \subseteq \sqrt{\mathfrak{a}}$ .

*Proof.* For the leftward direction, if  $(x_0, \dots, x_n) \subseteq \sqrt{\mathfrak{a}}$  then

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\sqrt{\mathfrak{a}}) \subseteq \mathcal{Z}(x_0, \dots, x_n) = (0, \dots, 0)$$

hence  $\mathcal{Z}(\mathfrak{a}) = \emptyset$ .

Conversely, if  $\mathcal{Z}(\mathfrak{a}) = \emptyset$  in  $\mathbb{P}^n$ , then in  $\mathbb{A}^{n+1}$ ,  $\mathcal{Z}(\mathfrak{a}) \subseteq \{0\}$ , hence by Nullstellensatz  $(x_0, \dots, x_n) \subseteq \sqrt{\mathfrak{a}}$ .  $\square$

#### Examples.

- (1) If  $f \in \mathbb{C}[X : Y : Z]$  is homogeneous of degree  $d$ , then  $\mathcal{Z}(f) \subseteq \mathbb{P}^2$  is called a *projective plane curve* of degree  $d$ .
- (2) When  $d = 1$ ,  $\mathcal{Z}(f)$  is called a *projective line*. Take  $L = \mathcal{Z}(f) = \{\alpha X + \beta Y + \gamma Z = 0\} \hookrightarrow \mathbb{P}^2$ . If  $Z \neq 0$ , then we may rewrite  $L = \{\alpha X/Z + \beta Y/Z + \gamma = 0\}$ , which is the usual equation of a line. If  $Z = 0$ , then  $[-\beta : \alpha : 0]$  lives on  $L$ , the "point at  $\infty$ ." If  $\alpha = \beta = 0$ , then  $L = \{Z = 0\}$ , the "line at  $\infty$ ."

### 13.1 Conics in $\mathbb{P}^2$

Take  $f \in \mathbb{C}[X : Y : Z]$ ,  $\deg f = d$ ,  $f$  homogeneous,  $\mathcal{Z}(f) \subseteq \mathbb{P}^2$  is a projective curve of degree  $d$ . When  $d = 2$ ,  $\mathcal{Z}(f)$  is a conic. In  $\mathbb{A}^2$ , there are two irreducible conics,  $XY - 1 = 0$  and  $Y = X^2$  (we saw this on homework). In  $\mathbb{P}^2$ , all irreducible conics are “the same” up to changing coordinates.

Let  $F = aX^2 + bY^2 + cZ^2 + 2dXZ + 2eXZ + 2fYZ$ . Then

$$F = \begin{pmatrix} X & Y & Z \end{pmatrix} \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

Let  $A$  be the symmetric matrix in the above expression. By the spectral theorem, there exists an orthonormal basis of eigenvectors for  $A$ . Let  $C$  be the change of basis matrix,  $C^{-1} = C^T$ . Then

$$C^T A C = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

Let  $T: \mathbb{P}^2 \rightarrow \mathbb{P}^2$  by

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = C^{-1} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

Such a  $T$  is called a *homogeneous change of coordinates*. We may check that  $F = \lambda_1 X'^2 + \lambda_2 Y'^2 + \lambda_3 Z'^3$ .

If  $\lambda_1 = 0$ , then  $F = (\sqrt{\lambda_2}Y' + \sqrt{-\lambda_3}Z')(\sqrt{\lambda_2}Y' - \sqrt{-\lambda_3}Z')$ , and so the conic was reducible. Hence, we must have  $\lambda_1 \neq 0$ ,  $\lambda_2 \neq 0$ , and  $\lambda_3 \neq 0$ .

Let  $X'' = \sqrt{\lambda_1}X'$ ,  $Y'' = \sqrt{\lambda_2}Y'$ ,  $Z'' = \sqrt{\lambda_3}Z'$ . Then  $F = X''^2 + Y''^2 + Z''^2$ . In particular, any conic can be written as  $XZ - Y^2 = 0$  (this may be useful on midterm).

#### Examples.

- (1)  $H = \{XY - 1 = 0\}$  in  $\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$ . This is not a homogeneous polynomial, so it is not a conic in  $\mathbb{P}^2$ . Instead, look at  $C = \{XY - Z^2 = 0\} \subseteq \mathbb{A}^2$ . If  $Z \neq 0$ , we can write  $X^{new} = X/Z$ ,  $Y^{new} = Y/Z$ , and get  $X^{new}Y^{new} - 1 = 0$ . That is,  $C \setminus \{[X : Y : 0]\} \cong'' H$ . If instead  $Z = 0$ , then  $XY = 0$ , hence  $X = 0$  or  $Y = 0$ . These are the points  $[0 : 1 : 0]$  and  $[1 : 0 : 0]$  respectively. Thus,  $C'' \cong'' H \cup \{[0 : 1 : 0], [1 : 0 : 0]\}$ . These new points can be thought of as  $\infty$  on the  $y$ - and  $x$ -axes respectively. This makes some sense looking at the graph of  $XY = 1$ , since the curve approaches those points.

$C$  is called the *projective closure* of  $H$ .

- (2)  $P = \{Y = X^2\} \subseteq \mathbb{A}^2$ . Again, the polynomial is not homogeneous, so we add a  $Z$  to get  $D = \{YZ - X^2 = 0\}$ .

*Claim.*  $D$  is the projective closure of  $P$  (whatever that means).

If  $Z \neq 0$ , then we can define  $X^{new} = X/Z$ ,  $Y^{new} = Y/Z$ , then  $Y^{new} - (X^{new})^2 = 0$ . If instead  $Z = 0$ , then  $X = 0$  and we get  $[0 : 1 : 0]$ . Hence,  $D = P \cup \{[0 : 1 : 0]\}$ .  $C$  and  $D$  are “isomorphic” via  $[X : Y : Z] \mapsto [Z : Y : X]$ .

We can see this as the two conics in  $\mathbb{A}^2$  both closing up to the same conic in  $\mathbb{P}^2$ .

## 13.2 Rational maps for projective varieties

Let  $X \subseteq \mathbb{P}^n$  be a projective variety. A rational function  $f: X \dashrightarrow k$  is a partially defined map which can be written as  $f = g/h$ , where  $g$  and  $h$  are homogeneous polynomials of the same degree. We make this restriction to ensure that

$$\frac{g([\lambda x_0 : \dots : \lambda x_n])}{h([\lambda x_0 : \dots : \lambda x_n])} = \frac{\lambda^{\deg g} g([x_0 : \dots : x_n])}{\lambda^{\deg h} h([x_0 : \dots : x_n])} = \frac{g([x_0 : \dots : x_n])}{h([x_0 : \dots : x_n])}$$

**Example.**  $f: \mathbb{P}^1 \dashrightarrow k$  by  $f([x_0, x_1]) = x_1/x_0^2$  is not a rational function.

**Definition.**  $f$  is *regular at  $p$*  if it may be written  $f = g/h$  where  $h(p) \neq 0$ .  $f$  is a *regular function on  $X$*  if  $f$  is regular everywhere.

A rational map  $f: X \subseteq \mathbb{P}^n \dashrightarrow Y \subseteq \mathbb{P}^m$  is a partially defined map  $f = [f_0 : f_1 : \dots : f_m]$  where the  $f_i$  are rational functions on  $X$  such that  $f(\text{Dom } f) \subseteq Y$ . As before,  $\text{Dom } f$  is  $\{p : \text{all } f_i \text{ are regular at } p \text{ and } f_i(p) \neq 0 \text{ for some } i\}$ .

A morphism  $f: X \subseteq \mathbb{P}^n \rightarrow Y \subseteq \mathbb{P}^m$  is a rational map with  $\text{Dom } f = X$ . In particular, if  $f = [f_0 : \dots : f_m]$  where the  $f_i$  are homogeneous polynomials of the same degree such that  $\mathcal{Z}(f_0, \dots, f_m) = \emptyset$ , then  $f$  defines a homomorphism. Note that the converse is false; there are more morphisms out there than polynomials. Nonetheless, if  $X = \mathbb{P}^1$ , don't worry about the difference.

An isomorphism is, surprisingly, a bijective morphism whose inverse is a morphism.

## 14 5 May 2008

Let  $S(X) = k[x_0 : \dots : x_n]/I(X)$ , the *homogeneous coordinate ring*. This is the analogy to  $A(X)$ , the ring of regular functions on  $X$ . However, we will see that  $X \cong Y$  is *not* equivalent to  $S(X) \cong S(Y)$ , which is different. This is because polynomials in  $k[x_0 : \dots : x_n]$  do not define functions on  $X$ .

**Lemma.** Let  $f_0, \dots, f_m$  be homogeneous polynomials of the same degree in  $n + 1$  variables, with common vanishing possibly only at  $(0, \dots, 0)$ . Then

$$f(p) = [f_0(p) : f_1(p) : \dots : f_m(p)]$$

is a morphism  $f: \mathbb{P}^n \rightarrow \mathbb{P}^m$ .

*Proof.* Since  $f = [f_0/f_m : f_1/f_m : \dots : f_{m-1}/f_m : 1]$  where each coordinate is a rational function,  $f: \mathbb{P}^n \dashrightarrow \mathbb{P}^m$  is a rational map. We show  $f$  is a morphism. Let  $p \in \mathbb{P}^n$ . Then there exists  $i$  such that  $f_i(p) \neq 0$ . Rewrite  $f = [f_0/f_i : f_1/f_i : \dots : 1 : \dots : f_m/f_i]$ , which is regular at  $p$ . Therefore,  $f$  is a morphism.  $\square$

**Example.**  $f: \mathbb{P}^1 \rightarrow \mathbb{P}^2$  given by  $[s : t] \mapsto [s^2 : st : t^2]$  is a morphism (by the lemma). Let  $Q$  be the image of  $f$ , and so  $Q = \{XZ = Y^2\}$ . Next, look at  $g: Q \rightarrow \mathbb{P}^1$  by  $[x : y : z] \mapsto [x : y]$ , which is a rational map.

*Claim.*  $g$  is a morphism.

This is clear everywhere except the point  $[0 : 0 : 1]$ , where  $g([0 : 0 : 1]) \stackrel{?}{=} [0 : 0]$ . Observe that on  $Q$ ,  $X/Y = Y/Z$ . Then

$$g[x : y : z] = \begin{cases} [x : y] & \text{when } (x, y) \neq (0, 0) \\ [y : z] & \text{when } (y, z) \neq (0, 0) \end{cases}$$

The first case is regular except possibly at  $[0 : 0 : 1]$ , while the second is regular except possibly at  $[1 : 0 : 0]$ . Written like this,  $g$  is a morphism (rational function). Hence,  $g: Q \rightarrow \mathbb{P}^1$  is a well-defined morphism.

**Example.** Any regular function  $f: \mathbb{P}^1 \rightarrow k$  must be constant.

The analogy here is that with the “infinity” point included,  $\mathbb{P}^1$  tries to be compact. This is sometimes called *Louville’s theorem*.

*Proof.* Let us cover  $\mathbb{P}^1$  by  $U_0$  and  $U_\infty$ , where

$$U_0 = \{[x_0 : x_1] : x_1 \neq 0\} \quad U_\infty = \{[x_0 : x_1] : x_0 \neq 0\}$$

Let  $j_0: U_0 \rightarrow \mathbb{A}^1$  by  $[x_0 : x_1] \mapsto x_0/x_1$ , and let  $j_\infty: U_\infty \rightarrow \mathbb{A}^1$  by  $[x_0 : x_1] \mapsto x_1/x_0$ . We claim that  $j_0$  and  $j_\infty$  are isomorphisms; indeed, they have inverse maps  $j_0^{-1}(t) = [t : 1]$  and  $j_\infty^{-1}(s) = [1 : s]$ . On  $U_0 \cap U_\infty$ ,  $s = 1/t$  ( $\mathbb{P}^1$  is called an *algebraic manifold*). Let  $f: \mathbb{P}^1 \rightarrow k$ . Restrict  $f$  to  $U_0$ , and look at  $f \circ j_0^{-1}: \mathbb{A}^1 \rightarrow k$ , which is regular. Thus,  $f \circ j_0^{-1} = P_0(t)$ , where  $P_0$  is a polynomial. On the other hand, over  $U_\infty$  we have  $f \circ j_\infty^{-1} = P_\infty(s)$ . We get  $f[x_0 : x_1] = P_\infty(s)$  over  $U_\infty$ . Hence, over  $U_0 \cap U_\infty$ ,  $P_0(t) = P_\infty(s) = P_\infty(1/t)$ , and since  $P_0$  and  $P_\infty$  are polynomials, we conclude  $P_0, P_\infty$  are constant, and therefore  $f$  is constant.  $\square$

*Remark.* This is true for  $\mathbb{P}^n$  and also for any projective  $X \subseteq \mathbb{P}^n$ .

*Remark.* We have shown that  $\mathbb{P}^1$  is *not* an affine variety, because affine varieties have a lot of regular functions, in particular their coordinates. In fact, no projective variety will be affine.

Next time, we will see an example of  $X$  and  $Y$  which are isomorphic projective varieties such that  $S(X) \not\cong S(Y)$ .

## 15 7 May 2008

### 15.1 Projective morphisms continued

Look again at  $Q = \{XZ = Y^2\}$ , which we saw in last lecture was isomorphic to  $\mathbb{P}^1$ .

*Claim.* The homogeneous coordinate rings  $S(Q) \not\cong S(\mathbb{P}^1)$ .

*Proof.* Assume  $\Phi: \mathbb{C}[X : Y : Z]/(XZ - Y^2) \rightarrow \mathbb{C}[s : t]$  is an isomorphism. Let  $\Phi(X) = F$ ,  $\Phi(Y) = G$ , and  $\Phi(Z) = H$ . Since  $XZ - Y^2 = 0$  in  $S(Q)$ ,  $FH = G^2$ .  $F$  and  $H$  cannot both be irreducible, since their product is a perfect square. Assume  $F$  is reducible, and write  $F = F_1F_2$ , so  $X = \underbrace{\Phi^{-1}(F_1)}_{P_1} \underbrace{\Phi^{-1}(F_2)}_{P_2}$  in  $\mathbb{C}[X : Y : Z]/(XZ - Y^2)$ . Then  $X = P_1(X : Y : Z)P_2(X : Y : Z) +$

(elements in the ideal  $XZ - Y^2$ ). Set  $X = s^2, Y = ts, Z = t^2$ . Then  $s^2 = P_1(s^2 : st : t^2)P_2(s^2 : st : t^2)$ . This can only happen if the two factors here are  $s^1, 1$  in some order or  $s, s$ .  $P_1(s^2 : st : t^2) = s$  is impossible because if  $t = 0$ ,  $P_1(s^2 : 0 : 0) \neq s$ . The other case implies that  $P_1$  or  $P_2$  has to be constant.  $\square$

## 15.2 The rational normal curve

In general, there is a well-defined morphism  $f_n: \mathbb{P}^1 \rightarrow \mathbb{P}^n$  with  $[s : t] \mapsto [s^n : s^{n-1}t : \dots : st^{n-1} : t^n]$ . The previous example was this with  $n = 2$ . Let  $Q_n$  be the image of  $f_n$ . The image of  $Q_n$  is defined by homogeneous equations:  $x_0x_2 = x_1^2, x_0x_3 = x_1x_2, \dots$ . That is,

$$Q_n = \left\{ [x_0 : \dots : x_n] : \text{rank} \begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix} \leq 1 \right\}$$

and so for any  $2 \times 2$  block the determinant is zero. Hence,  $Q_n = \{x_i x_{j+1} = x_{i+1} x_j \forall i, j\}$ .  $f_n: \mathbb{P}^1 \rightarrow Q_n$  is an isomorphism with inverse

$$g_n[x_0 : \dots : x_n] = \begin{cases} [x_0 : x_1] & \text{if } (x_0, x_1) \neq (0, 0) \\ [x_1 : x_2] & \text{if } (x_1, x_2) \neq (0, 0) \\ \vdots & \vdots \\ [x_{n-1} : x_n] & \text{if } (x_{n-1}, x_n) \neq (0, 0) \end{cases}$$

$Q_n$  is called the *rational normal curve*.  $Q_3$  is called the *twisted cubic*.

## 15.3 Veronese morphism

More generally, consider  $f: \mathbb{P}^n \rightarrow \mathbb{P}^N$ . Let  $M_0, M_1, \dots, M_N$  be an enumeration of the monomials of degree  $d$  in  $x_0, \dots, x_n$ , so  $N = \binom{n+d}{d} - 1$ . Then  $[x_0 : \dots : x_n] \mapsto [M_0(x) : \dots : M_N(x)]$  is a well-defined morphism, called the *Veronese morphism*. The image of  $f$  is given by homogeneous equations.

In particular, take  $n = 2, N = 5, d = 2$ . and consider  $f: \mathbb{P}^2 \rightarrow \mathbb{P}^5$  given by

$$[s : t : u] \mapsto [s^2 : t^2 : u^2 : st : tu : us]$$

$f(\mathbb{P}^2)$  is called the *veronese surface*. It is also a *twisted surface*.

## 15.4 The Serge morphism

$\mathbb{P}^n \times \mathbb{P}^m \not\cong \mathbb{P}^{n+m}$ . However, consider the map  $\Phi: \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$  by

$$\Phi([x_0 : \dots : x_n], [y_0 : \dots : y_m]) = [Z_{00} : Z_{01} : \dots : Z_{(n+1)(m+1)}]$$

where  $Z_{ij} = x_i y_j$ . For example, with  $n = m = 1$ , we have  $\Phi: \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$  by

$$[x_0 : x_1] \times [y_0 : y_1] \mapsto [x_0 y_0 : x_0 y_1 : x_1 y_0 : x_1 y_1]$$

Then  $\text{Im } \Phi \subseteq Q = \{Z_{00}Z_{11} = Z_{01}Z_{10}\}$ .  $Q$  is a quadric in  $\mathbb{P}^3$ .

*Claim.*  $\text{Im } \Phi = Q$  and  $\Phi$  is bijective.

It will turn out that  $Q$  admits two *rulings*. That is, through every single point  $\Phi(A, B)$  of the quadric, there pass exactly two projective lines

$$\{A\} \times \mathbb{P}^1 \xrightarrow{\Phi} \text{line in } \mathbb{P}^3$$

$$\mathbb{P}^1 \times \{B\} \xrightarrow{\Phi} \text{line in } \mathbb{P}^3$$

*Proof of claim.* To construct  $\Phi^{-1}: Q \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ , assume first that  $Z_{00} \neq 0$ . Then let  $\Phi^{-1}([Z_{00} : Z_{01} : Z_{10} : Z_{11}]) = [Z_{00} : Z_{10}] \times [Z_{00} : Z_{01}] = [x_0 y_0 : x_1 y_0] \times [x_0 y_0 : x_0 y_1] = [x_0 : x_1] \times [y_0 : y_1]$ . (Proof continued next time?).  $\square$

## 16.1 Serge morphisms continued

Note that  $Q$  can be written

$$Q = \left\{ [z_{ij}] : \text{rank} \begin{pmatrix} z_{00} & z_{01} & \cdots & z_{0m} \\ z_{10} & z_{11} & \cdots & z_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n0} & z_{z1} & \cdots & z_{nm} \end{pmatrix} \leq 1 \right\}$$

that is, every  $2 \times 2$  minor has determinant 0. This is a projective set cut out by quadrics. This will endow  $\mathbb{P}^n \times \mathbb{P}^m$  with the structure of a projective variety.

*Remark.* The projective subvarieties of  $\mathbb{P}^n \times \mathbb{P}^m$  are given by homogeneous polynomials in the  $z_{ij}$ 's, i.e. bihomogeneous polynomials in  $x_i$ 's and  $y_i$ 's of the same degree. Conversely, any bihomogeneous polynomial in  $x_i$  and  $y_i$  (not necessarily of the same degree) will define a subvariety of  $\mathbb{P}^n \times \mathbb{P}^m$ . For example, if we have a degree  $d$  polynomial in the  $x_i$ 's and a degree  $e$  polynomial in the  $y_i$ 's with  $d < e$ , then multiply by all monomials of degree  $e - d$ , to equalize the degree.

**Example.**  $x^2v - y^2u = 0$  in  $\mathbb{P}^1 \times \mathbb{P}^1$ , where  $x, y$  are from the first  $\mathbb{P}^1$  and  $u, v$  from the other. Then this is as  $(x^2v - y^2u)u = 0$  and  $(x^2v - y^2u)v = 0$ .

**Corollary.** *If  $X \subseteq \mathbb{P}^n$  and  $Y \subseteq \mathbb{P}^m$  are projective, then  $X \times Y \subseteq \mathbb{P}^n \times \mathbb{P}^m$  is projective. (In the homework, if  $X, Y$  are affine then  $X \times Y$  is affine.)*

**Example.** If  $f: X \subseteq \mathbb{P}^n \rightarrow Y \subseteq \mathbb{P}^m$  is a projective map, then the graph  $\Gamma_f = \{(x, f(x)) : x \in X\} \subseteq X \times Y$  is a projective variety. To see this, observe that  $[y_0 : \dots : y_m] = [f_0(x) : \dots : f_m(x)]$ , which is equivalent to saying

$$\text{rank} \begin{pmatrix} y_0 & \cdots & y_m \\ f_0(x) & \cdots & f_m(x) \end{pmatrix} \leq 1$$

which is equivalent to saying  $y_i f_j(x) = y_j f_i(x)$  for each  $i, j$ . Therefore,

$$\Gamma_f = \{y_i f_j(x) = y_j f_i(x) + (\text{the equations of } X)\}$$

This statement is true for any morphism  $f$ .

## 16.2 Main theorem on projective varieties

**Theorem.** *Let  $X \subseteq \mathbb{P}^n, Y \subseteq \mathbb{P}^m$  be projective. If  $f: X \rightarrow Y$  is a morphism, then  $f(X) \subseteq \mathbb{P}^m$  is also projective.*

*Remark.*

- (1) This fails for affine varieties.
- (2) If  $X$  is irreducible and  $f: X \rightarrow k$  is regular, then  $f$  is constant.

Indeed, look at  $\bar{f}: X \rightarrow \mathbb{P}^1$  where we view  $k \hookrightarrow \mathbb{P}^1$  and  $\bar{f} = \iota \circ f$ . Then  $\bar{f}$  is a morphism, and so  $\bar{f}(X)$  is projective inside  $\mathbb{P}^1$ .  $\bar{f}(X) \neq \mathbb{P}^1$  since  $\infty \notin \text{Im } \bar{f}$ . Therefore,  $\bar{f}(X) = (\text{point})$ , and so  $f$  is constant.

*Proof of theorem.*

*Claim.* The projection map  $\pi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^m$  satisfies the theorem. This will imply that if  $f : X \rightarrow Y$  is a morphism then  $\Gamma_f \subseteq \mathbb{P}^n \times \mathbb{P}^m$  is projective, and so  $\pi(\Gamma_f) = f(X)$  will be projective.

Let  $X \subseteq \mathbb{P}^n \times \mathbb{P}^m$ , and let  $f_1(x : y), \dots, f_r(x : y)$  be the equations defining  $X$ .  $\pi(X)$  is given by homogeneous polynomials. Assume that  $f_1, \dots, f_r$  are bihomogeneous in  $x$  and  $y$  of the same degree. Let  $p \in \pi(X)$ . This is equivalent to saying there exists  $q$  such that  $(q, p) \in X$ , which is equivalent to saying  $f_1(x : p), \dots, f_r(x : p)$  have a common zero. By projective Nullstellensatz, this is equivalent to saying that for all  $s$ ,  $(x_0 \cdots x_s)^s \notin \langle f_1(y : p), \dots, f_r(y : p) \rangle$ . Let  $\mathcal{A}_s$  be the set of all  $p$ 's such that this occurs. Therefore,  $\pi(X) = \bigcap_s \mathcal{A}_s$ . We will show that each  $\mathcal{A}_s$  is cut out by homogeneous polynomials (next time).  $\square$

## 17 12 May 2008

*Proof continued.*

*Claim.*  $\mathcal{A}_s$  is cut out in  $\mathbb{P}^m$  by homogeneous polynomials.

If  $s < d$ , then  $\mathcal{A}_s = \mathbb{P}^m$ . Assume  $s > d$ , and look at  $\mathbb{P}^m \setminus \mathcal{A}_s \ni p$ . Let  $M_1(x), \dots, M_D(x)$  be all monomials of degree  $s$  listed in any order. Then  $M_1(x), \dots, M_D(x) \in \langle f_1(x : p), \dots, f_r(x : p) \rangle$ , and so  $M_j(x) = \sum f_i(x : p)g_{ij}(x)$  for some  $g_{ij}$ . The  $M_j$ 's have degree  $s$  while the  $f_i(x : p)$  have degree  $d$ . We may thus assume that each  $g_{ij}$  has degree  $s - d$ . Let  $N_1(x), \dots, N_E(x)$  be all monomials of degree  $s - d$ , listed in any order. Then  $M_j(x)$  can be expressed as a linear combination of  $f_i(x : p)N_k(x)$  for  $i \leq r$  and  $1 \leq k \leq E$ . That is,  $\langle f_i(x : p)N_k(x) \rangle$  span the vector space of homogeneous degree  $s$  polynomials in  $x$ . Expand  $f_i(x : p)$  into monomials and collect the coefficients into a matrix  $B$ . The entries of  $B$  are homogeneous polynomials in  $p$ 's. Then  $\text{rank } B \geq D$  for  $p \in \mathbb{P}^m \setminus \mathcal{A}_s$ , hence for  $p \in \mathcal{A}_s$ ,  $\text{rank } B < D$ , e.g. any  $D \times D$  minor vanishes. These minors are homogeneous polynomials in  $p$ 's (of degree  $e^D$ ). Therefore,  $\mathcal{A}_s$  is cut out by homogeneous polynomials.

Furthermore, each implication in this proof is in fact an if and only if, so we have the converse as well.  $\square$

### 17.1 Singularities of curves in $\mathbb{A}^2$

**Definition.** Let  $f \in k[x, y]$  (assume  $\text{ch } k = 0$ , or even that  $k = \mathbb{C}$ ). A point  $p \in \mathbb{A}^2$  is a *singular point* for  $f$  if  $f(p) = 0$ ,  $\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = 0$ . A *non-singular point* of  $f$  is a point where  $f(p) = 0$  but  $\frac{\partial f}{\partial x}(p) \neq 0$  or  $\frac{\partial f}{\partial y}(p) \neq 0$ .

**Example.**  $f(x, y) = y^2 - x(x - 1)(x - \lambda)$ . Then  $\frac{\partial f}{\partial x} = -\frac{\partial}{\partial x}(x^3 - (\lambda + 1)x^2 + \lambda x) = -3x^2 + 2(\lambda + 1)x - \lambda$ , and  $\frac{\partial f}{\partial y} = 2y$ . At singular points,  $y = 0$ ,  $x = 0, 1$ , or  $\lambda$ .

- If  $x = 0, y = 0$ , then  $\frac{\partial f}{\partial x} = 0$  forces  $\lambda = 0$ . If  $\lambda = 0$ , then  $(0, 0)$  is a singular point.
- If  $x = 1, y = 0$ , then  $\frac{\partial f}{\partial x} = 0$  implies  $\lambda = 1$ . If  $\lambda = 1$ , then  $(1, 0)$  is singular.
- If  $x = \lambda, y = 0$ , then  $\frac{\partial f}{\partial x} = 0$  gives  $-\lambda^2 + \lambda = 0$ , and so  $\lambda = 0$  or  $1$ , cases we have already covered.

There are no singular points when  $\lambda \neq 0, 1$ .

*Remark.* If  $p = (a, b)$  is a non-singular point, then the tangent line of  $f$  at  $p$  is the line given by

$$\frac{\partial f}{\partial x}(p)(x - a) + \frac{\partial f}{\partial y}(p)(y - b) = 0$$

**Definition.** WLOG assume  $p = (0, 0)$  (otherwise work with  $f(x + a, y + b)$  instead).  $(0, 0)$  is a point of *multiplicity*  $m$  of  $f$  if

$$\frac{\partial^{i+j} f}{\partial x^i \partial y^j}(p) = 0 \quad \text{if } i + j < m$$

and at least one  $(m + 1)$ st derivative is nonzero.

Singular points have multiplicity  $\geq 2$  while non-singular points have multiplicity 1.  $f$  has multiplicity  $m$  at  $(0, 0)$  if the smallest degree monomial in  $f$  has degree  $m$ .

**Examples.**

- (1)  $y^2 = x^2(x + 1)$ .  $(0, 0)$  has multiplicity 2, a “node” (looks like an X).
- (2)  $y^2 = x^3$ .  $(0, 0)$  has multiplicity 2, a “cusp.”
- (3)  $y^2 = x^4$ .  $(0, 0)$  has multiplicity 2, a “tacnode” (looks like two parabolas meeting).

## 18 14 May 2008

### 18.1 Singularities continued

Let  $f \in \mathbb{C}[X, Y]$  and suppose  $p = (0, 0)$  is a singularity for  $f$ , i.e.  $f(p) = 0$  and  $\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = 0$ . Write  $f = f_{(r)} + f_{(r+1)} + \cdots + f_{(n)}$ , where  $f_{(i)}$  is homogeneous of degree  $i$  for each  $i$ . In this case,  $\text{mult}_p(f) = r$ . Since  $f_r$  is homogeneous of degree  $r$ , then  $f_r = \prod_{i=1}^r (a_i x + b_i y)$ . [To justify this: if  $f_r = \alpha_0 x^r + \alpha_1 x^{r-1} y + \cdots + \alpha_r y^r$ , let  $y = x/y$ . Factor  $\alpha_0 t^r + \cdots + \alpha_r = \prod_{i=1}^r (a_i t + b_i)$ , etc.]

These  $a_i x + b_i y = 0$  are called the tangent directions for  $p$ .

**Examples.**

- (1)  $y = x^2(x + 1)$ ,  $p = (0, 0)$ . Then  $f_{(2)} = y^2 - x^2 = (y - x)(y + x)$ ,  $f_{(3)} = -x^3$ . Tangent directions  $y = x$  and  $y = -x$ .  $p$  is an *ordinary* double point (it has distinct tangent directions).
- (2)  $y^2 = x^2$ ,  $p = (0, 0)$  (cusp). Then  $f_{(2)} = y^2$ . The tangent directions are  $y = 0$  (twice).  $p$  is a double point, but not ordinary. Hence, (1) and (2) are not isomorphic.
- (3)  $x^2 y + x y^2 = x^4 + y^4$ . Then  $f_{(3)} = x^2 y + x y^2 = x y(x + y)$ . There are three tangent directions at  $(0, 0)$ :  $x = 0$ ,  $y = 0$ , and  $x + y = 0$ .  $(0, 0)$  is thus an ordinary triple point.

*Remark.* Singularities are invariants not of  $\mathcal{Z}(f)$  but rather of  $f$ . For example,  $\mathcal{Z}(y) \subseteq \mathbb{A}^2$  has no singularities, but  $\mathcal{Z}(y^2) \subseteq \mathbb{A}^2$  is singular at  $(0, 0)$ , a double point. This occurs even though  $\mathcal{Z}(y) = \mathcal{Z}(y^2)$ .

*Remark* (Singularities of  $fg$ ). Take  $X = \mathcal{Z}(f)$ ,  $Y = \mathcal{Z}(g)$ , and so  $X \cup Y = \mathcal{Z}(fg)$ . Then  $\text{Sing}(fg) = \text{Sing}(f) \cup \text{Sing}(g) \cup \{f = g = 0\}$ .

*Remark.* This works for  $f \in \mathbb{C}[x_1, \dots, x_n]$ .

**Example.**  $f = x^2 + y^2 - z^2$  in  $\mathbb{A}^3$  has a singularity at  $(0,0,0)$ . Visually, the set looks like cones meeting at the origin, and  $(0,0,0)$  is called a *conical singularity*.

**Example.** In  $\mathbb{A}^2$ , conics are  $xy - 1 = 0$  and  $x - y^2 = 0$ . Both conics are non-singular. In  $\mathbb{A}^2$ , all irreducible conics are non-singular.

**Example.** In  $\mathbb{A}^2$ , cubics can have nodes ( $y^2 = x^2(x+1)$ ), cusps ( $y^2 = x^3$ ), or have no singularities (elliptic curves).

*Remark.* Singularities can be resolved. If  $X \subseteq \mathbb{A}^2$  is singular, then there exists another curve  $X'$  without singularities such that there is a birational isomorphism  $X' \rightarrow X$ . (The proof is about 400 pages, at least for  $\mathbb{A}^n$ ).

**Examples.**

- (1) The cusp  $y^2 = x^3$  is resolved by  $\mathbb{A}^1 \rightarrow \{y^2 = x^3\}$  by  $t \mapsto (t^2, t^3)$ .
- (2) The node  $y^2 = x^2(x+1)$  can be resolved by  $\mathbb{A}^1 \rightarrow \{y^2 = x^2(x+1)\}$  by  $(t^2 - 1, t(t^2 - 1))$ .

## 18.2 Projective singularities

**Definition.** Let  $f \in \mathbb{C}[x : y : z]$  and let  $p \in \mathbb{P}^2$ .  $p$  is a *singular point* if  $f(p) = 0$  and  $\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = \frac{\partial f}{\partial z}(p) = 0$ .

**Examples.**

- (1) In  $\mathbb{P}^2$ , any irreducible conic is  $x^2 + y^2 + z^2 = 0$ . There are singularities, and so conics in  $\mathbb{P}^2$  are non-singular.
- (2) The elliptic curve  $y^2z = x(x-z)(x-\lambda z)$  for  $\lambda \neq 0, 1$  is non-singular. We check:  $f = y^2z - x(x-z)(x-\lambda z)$ .  $f_x = -(3x^2 - 2(\lambda+1)xz + \lambda z^2)$ .  $f_y = 2yz$ .  $f_z = y^2 - x(-(\lambda-1)x + 2\lambda z)$ . Setting  $f_y = 0$ , we have  $y = 0$  or  $z = 0$ . If  $z = 0$ , then  $x = 0$  and so we have only the point  $[0 : 1 : 0]$ , but then  $f_z = 1$ , hence non-singular. If  $y = 0$  and  $z \neq 0$ , then look at  $x = z$ ,  $z = \lambda z$ , and  $x = 0$ , and observe that one derivative does not vanish.

*Remark* (Euler relation). If  $f$  is homogeneous of degree  $d$ , then  $d \cdot f = xf_x + yf_y + zf_z$ . To show this, it is enough to look at the case  $f = x^i y^j z^k$ , which is clear enough.

From the remark, to find singularities of  $f$  we only need to look at  $\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = \frac{\partial f}{\partial z}(p) = 0$ , which by the Euler relation implies  $f(p) = 0$ .

*Remark.* If  $f(x : y : z)$  is a homogeneous polynomial, then look at singularities of the affine curve  $f(x : y : 1) = 0$ . There may also be singularities at  $z = 0$  (consider them separately). That is,  $\text{Sing}(\overline{X}) = \text{Sing}(X) \cup \{\text{possibly with points at } \infty\}$ .

## 19 16 May 2008

### 19.1 Blow-ups

(We will do a simplified version of blow-ups.) Let  $\pi: \mathbb{A}^2 \rightarrow \mathbb{A}^2$  by  $(u, v) \mapsto (u, uv)$ . This is a blow-up.

Consider the axes in the first  $\mathbb{A}^2$  and follow the  $v$ -axis under  $\pi$ . Its image is just  $(0,0)$  in the second  $\mathbb{A}^2$ . That is,  $\ell = \{u = 0\}$  is contracted to  $(0,0)$ . We say  $\pi$  is a blow-up at  $(0,0)$  (of  $\mathbb{A}^2$ ), and  $\ell$  is an exceptional set/divisor/line. Note that  $\pi$  is birational, with inverse  $\pi^{-1}: \mathbb{A}^2 \dashrightarrow \mathbb{A}^2$  by  $(x,y) \mapsto (x,y/x)$ .

Let  $C$  be a curve in  $\mathbb{A}^2$  through  $(0,0)$  which is singular at  $(0,0)$ . We want to compute  $\pi^{-1}(C)$ . Let  $f$  be the equation of the curve, and write

$$f = \sum_{i+j=m} a_{ij}x^i y^j + (\text{higher order terms}), \quad m = \text{mult}_{(0,0)} f$$

$\pi^{-1}(C)$  will be given by

$$\begin{aligned} f(u, uv) &= \sum_{i+j=m} a_{ij}u^i (uv)^j + (\text{higher order terms}) \\ &= u^m \left( \sum_{i+j=m} a_{ij}v^j + (\text{higher terms}) \right) = 0 \\ &\quad \underbrace{\hspace{10em}}_{f_1(u,v)} \end{aligned}$$

We have  $u = 0$  (with multiplicity  $m$ ) or  $f_1(u, v) = 0$ . Let  $\tilde{C} = \mathcal{Z}(f_1)$ , and so  $\pi^{-1}(C) = \tilde{C} \cup \ell$ .  $\tilde{C}$  is called the *strict transform* of  $C$ . Then  $\pi: \tilde{C} \rightarrow C$ , which is a birational map.

We claim that  $\tilde{C}$  is a “less-singular” curve than  $C$ . Eventually, we would obtain a birational map  $\tilde{C} \rightarrow C$  where  $\tilde{C}$  is non-singular.

### Examples.

- (1)  $c = \{y^2 = x^2(x+1)\}$ , for which  $(0,0)$  is an ordinary double point.  $f = y^2 - x^2(x+1)$ , so  $f(u, uv) = (uv)^2 - u^2(u+1) = u^2(v^2 - u - 1)$ . Take  $f_1 = v^2 - u - 1$ . Then  $\tilde{C} = \mathcal{Z}(f_1)$  is the parabola  $v^2 = u + 1$ , and we have  $\pi: \tilde{C} \rightarrow C$ . Furthermore, note that  $(0, 1)$  and  $(0, -1)$  on  $\tilde{C}$  both map to  $(0,0)$  on  $C$ ; we have “pulled apart” the singularity.
- (2) The tacnode,  $y^2 = x^4 + x^5$ . We have  $f(u, uv) = (uv)^2 - u^4 - u^5 = u^2(v^2 - u^3 - u^2)$ , and take  $f_1$  as  $v^2 = u^2(u+1)$ . But this is precisely the example we had before, the ordinary double point. That is,  $C$  is a tacnode, resolved into the node  $\tilde{C}$ . If we do another blow-up, we can resolve the tacnode.

Speculation: What about in higher dimensions? You might try  $\pi: (u, v, w) \mapsto (u, uv, uvw)$ , which works fine for points. However, in higher dimensions you might want to separate entire curves, which is harder.

## 19.2 Inflection points

Our goal is to show that any non-singular cubic can be written  $y^2z = x(x-z)(x-\lambda z)$  for  $\lambda \neq 0, 1$ . Suppose  $f$  is homogeneous of degree  $d$ ,  $f(p) = 0$ . Define the *Hessian* of  $f$

$$Hf = \begin{vmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{vmatrix}$$

**Definition.**  $p$  is a *point of inflection* if  $f(p) = 0$  and  $Hf(p) = 0$ . A *flex* is the tangent line,

$$\frac{\partial f}{\partial x}(p)(x-a) + \frac{\partial f}{\partial y}(p)(y-b) + \frac{\partial f}{\partial z}(p)(z-c) = 0$$

We will see that the flex is a tangent line “touching  $\mathcal{Z}(f)$  with multiplicity 3.”

**Examples.**

- (1)  $d = 1$ , then every point on a line is an inflection point.
- (2)  $d = 2$ . Change coordinates so  $f = x^2 + y^2 + z^2$ , then  $Hf = \det 2I$ , so no inflection points.
- (3)  $\overline{E}_\lambda$ , i.e.  $f = y^2z - x(x - z)(x - \lambda z)$ . There are nine inflection points, but we will not compute all of them.  $[0 : 1 : 0]$  is one inflection point; the Hessian at  $[0 : 1 : 0]$  is

$$\begin{vmatrix} 0 & 0 & - \\ 0 & 0 & 2 \\ - & 2 & - \end{vmatrix}$$

which is enough to see that the determinant is zero.

- (4) If  $d \geq 3$ , then  $f$  will have an inflection point if and only if  $\mathcal{Z}(f)$  and  $\mathcal{Z}(Hf)$  intersect in  $\mathbb{P}^2$ . By homework 5, problem 2(iv), this intersection is non-empty. Furthermore,  $\deg Hf = 3(d - 2)$  while  $\deg f = d$ , so there are at most  $3d(d - 2)$  points of intersection. Note that this gives nine points of intersection for the elliptic curve example above.

**20 19 May 2008**

**Lemma.** *Given a point  $p \in \mathbb{P}^2$  and a line  $\ell$  with  $p \in \ell$ , we can change coordinates in  $\mathbb{P}^2$  such that  $p = [0 : 1 : 0]$  and  $\ell = \{z = 0\}$ .*

*Proof.* Let  $g \neq p$  be another point on  $\ell$ . Change coordinates so that  $p \mapsto [0 : 1 : 0]$ ,  $g \mapsto [1 : 0 : 0]$ . (This is possible, as we did something stronger on the midterm.) Then  $p, g$  determine the line  $\ell$  uniquely, thus  $\ell = \{z = 0\}$ . □

**Proposition.** *Any non-singular cubic in  $\mathbb{P}^2$  can be written (after changing coordinates) as  $\overline{E}_\lambda$ :*

$$y^2z = x(x - z)(x - \lambda z) \quad \text{for } \lambda \neq 0, 1$$

This means that “the moduli space of cubics in  $\mathbb{P}^2$  is one-dimensional.”

*Proof.* Pick a point  $p$  on the cubic which is an inflectionary point. Using the lemma, let  $p = [0 : 1 : 0]$  and let the flex at  $p$  be the line  $\{z = 0\}$ . Let  $f = 0$  with  $\deg f = 3$  be the equation of the cubic. Then  $f([0 : 1 : 0]) = 0$ . Furthermore, since  $\{z = 0\}$  is the tangent line, we must have  $f_x[0 : 1 : 0] = 0$ ,  $f_y[0 : 1 : 0] = 0$ , and then  $f_z[0 : 1 : 0] \neq 0$  (if  $f_z$  were zero as well, then the curve would be singular). Write

$$f = ax^3 + by^3 + cz^3 + dx^2y + exy^2 + fx^2z + gxz^2 + hy^2z + kyz^2 + ixyz.$$

From  $f([0 : 1 : 0]) = 0$ ,  $b = 0$ . From the next equation,  $e = 0$ . The third equation does not give any additional information (it gives  $b = 0$  again), but the last gives  $h \neq 0$ . Computing the Hessian,

$$Hf = \begin{vmatrix} f_{xx} & 0 & ? \\ 0 & 0 & 2h \\ ? & 2h & ? \end{vmatrix} = -4h^2 f_{xx}[0 : 1 : 0]$$

We know that  $Hf = 0$ , therefore  $f_{xx}[0 : 1 : 0] = 0$ . Thus, the coefficient  $d = 0$  as well. We have now eliminated three of the ten terms of  $f$ .

We know that  $f = \phi(x, z) + yz(ix + hy + kz)$ , where  $\phi(x, z)$  is a homogeneous polynomial in  $x$  and  $z$ . Make change of coordinates by completing the square:  $y^{\text{new}} = y + (ix + kz)/(2h)$ . We obtain  $f = \psi(x, z) + hzy^2$ . We may assume  $f = \psi(x, z) + y^2z$  after dividing by  $h$  (which is nonzero, from above). A homogeneous cubic in two variables factors into linear terms, so we may write

$$y^2z = (x - az)(x - bz)(x - cz)$$

where we know  $\psi$  has a nonzero coefficient of  $x^3$ , because otherwise  $z$  would divide  $f$ , which is irreducible. Make change of coordinates  $x^{\text{new}} = (x - az)/(b - a)$  (we will need to check that  $b - a \neq 0$ ). We produce

$$y^2x = [(b - a)x][(b - a)x - (b - a)z][(b - a)x - (c - a)z] = (b - a)^3x(x - z) \left( x - \frac{c - a}{b - a}z \right)$$

Making one last change of coordinates  $y^{\text{new}} = y/(b - a)^{3/2}$  and letting  $\lambda = (c - a)/(b - a)$ , we get

$$y^2 = x(x - z)(x - \lambda z)$$

Furthermore,  $\lambda \neq 0, 1$  because  $a \neq b$ ,  $b \neq c$ , and  $c \neq a$ . To see this, first if  $a = b$  then  $y^2z = (x - az)^2(x - cz)$ , but then  $z = 1$ ,  $(a, 0)$  is a point of multiplicity 2 and therefore singular. A similar argument works to show  $b \neq c$  and  $c \neq a$ .  $\square$

*Remark.* Note that we used  $\lambda = (c - a)/(b - a)$  in the proof, but we could just as well have used  $\lambda = (b - a)/(c - a)$  or  $(a - c)/(b - c)$ , etc. Different  $\lambda$ 's may give isomorphic  $\bar{E}_\lambda$ . We will work with the curves  $E_\lambda$  given by  $y^2 = x(x - a)(x - \lambda)$  in  $\mathbb{A}^2$ .

- If  $\mu = 1/\lambda$ , then  $E_\lambda \cong E_\mu$ .
- If  $\mu = 1 - \lambda$ ; then  $E_\lambda \cong E_\mu$ .

For the first point, note that

$$y^2 = x(x - 1) \left( x - \frac{1}{\lambda} \right) \Leftrightarrow y^2 = \frac{(\lambda x)}{\lambda} \frac{(\lambda x - \lambda)}{\lambda} \frac{(\lambda x - 1)}{\lambda}$$

then with the change of coordinates  $y' = y\lambda^{3/2}$ , we get  $y'^2 = x(x - \lambda)(x' - 1)$ .

For the second point, from  $y^2 = x(x - 1)(x - 1 + \lambda)$ , make the change of coordinates  $x^{\text{new}} = 1 - x$ . Then  $y^2 = (1 - x)(-x)(-x + \lambda)$ , and  $y^{\text{new}} = (-1)^{3/2}y$  finishes.

Combining the two items in the remark, we get  $E_\lambda \cong E_\mu$  if

$$\mu \in \left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1 - \lambda}, \frac{\lambda - 1}{\lambda}, \frac{\lambda}{\lambda - 1} \right\}$$

We would like to package this into one characteristic.

**Definition.**

$$j(\lambda) = 256 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

It is easy to see that  $j(\lambda) = j(1/\lambda)$  and  $j(\lambda) = j(1 - \lambda)$ . Therefore,  $j(\mu) = j(\lambda)$  if  $\mu$  is in the set given above.

**Theorem.** *Two elliptic curves  $\bar{E}_\lambda$  and  $\bar{E}_\mu$  are isomorphic if and only if  $j(\lambda) = j(\mu)$ .*

(Proof omitted.)

### 21.1 More on the $j$ characteristic

Examples.

- (1) (Fermat cubic).  $x^3 + y^3 = z^3$ , a cubic curve. We will see  $j = 0$ . Let  $u = z - y$  so  $z = u + y$ . We get

$$x^3 = u^3 + 3u^2y + 3uy^2 = u \left( \sqrt{3}y + \frac{\sqrt{3}}{2}u \right)^2 + \frac{u^3}{4}$$

Take  $y^{\text{new}}$  to be the expression in parentheses, and we have

$$\begin{aligned} x^3 &= uy^2 + \frac{u^3}{4} \\ y^2u &= x^3 - \frac{u^3}{4} \\ &= (x - a_1u)(x - a_2u)(x - a_3u) \end{aligned}$$

where  $a_1, a_2, a_3$  are the cubic roots of  $1/4$ . As in the last proof, take  $\lambda = (a_2 - a_1)/(a_3 - a_1)$ . Write  $a_2 = a_1\omega$  and  $a_3 = a_1\omega^2$ , where  $\omega = e^{2\pi i/3}$ . So,  $\lambda = (\omega - 1)/(\omega^2 - 1) = -\omega$ . Finally,  $j(-\omega) = 256(\omega^2 + \omega + 1)^3/(\omega^2(\omega + 1)^2) = 0$ . (This will come up on homework.)

- (2)  $j = 1728$ . Look at  $y^3 = x^3 - n^2x$  for  $n \in \mathbb{Z}$ . Then  $y^2 = x(x - n)(x + n)$  and  $\lambda = (-n - 0)(n - 0) = -1$ .  $j(-1) = 256 \cdot (27/4) = 1728$ .

*Remark.* This last elliptic curve is related to the congruent number problem.  $n \in \mathbb{Z}$  is congruent if there exists a right triangle with sides  $a, b, c \in \mathbb{Q}$  and  $\text{area}(\Delta) = n$ . Find the  $n$ ? Find the triangles? The problem looks at  $a^2 + b^2 = c^2$  and  $ab/2 = n$ . Pick  $(x, y)$  with  $y^2 = x^3 - n^2x$  with  $x, y \in \mathbb{Q}$ . Set  $a = (x^2 - n^2)/y$ ,  $b = 2xn/y$ , and  $c = (x^2 + n^2)/y$ . Then  $ab/2 = (x^2 - n^2)xn/y^2 = n$ .

### 21.2 Group structure on $\overline{E}_\lambda$

Our next goal is to show that  $\overline{E}_\lambda$  has the structure of an abelian group with  $p_0 = [0 : 1 : 0]$  as the zero-element. For  $P, Q \in \overline{E}_\lambda$ , we will define  $P \oplus Q \in \overline{E}_\lambda$ . We might try to do so by drawing a line through  $P$  and  $Q$ ; we know that a line and a cubic intersect in at most three places, so supposing that the line intersects the cubic again at  $R$ , we might try to define  $P \oplus Q = R$ . But this does not work: for example, it would give  $P \oplus Q = R$ ,  $P \oplus R = Q$ , and  $Q \oplus R = P$ .

Instead, the idea is to define  $P \oplus Q \oplus R = 0$  provided that  $P, Q, R$  lie on a common line. The sum  $P \oplus Q$  is the reflection of  $R$  across the  $x$ -axis.

Details: What if  $P = Q$ ? What if  $\overline{PQ}$  does not intersect  $\overline{E}_\lambda$ ? Why does  $P \oplus P_0 = P$ ? Why does  $P \oplus Q = Q \oplus P$ ? What are the inverses? And why does  $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ ? This last question will turn out to be the hardest.

### 21.3 Weak Bezout (projectively)

**Theorem.** Let  $f$  and  $g$  be two polynomials of degrees  $d$  and  $e$ , homogeneous in  $x, y, z$ .  $f$  and  $g$  may be reducible, but without common factors. Then

$$\#(\mathcal{Z}(f) \cap \mathcal{Z}(g)) \leq de$$

*Proof.* In the homework, we have seen this in  $\mathbb{A}^2$  when we assumed  $f$  and  $g$  were irreducible. We will derive the general case from this. We may assume  $f$  and  $g$  are irreducible, since if  $f = f_1 f_2$  where  $\deg f_1 = d_1 < d$  and  $\deg f_2 = d_2 < d$ , then  $\mathcal{Z}(f) \cap \mathcal{Z}(g) = (\mathcal{Z}(f_1) \cap \mathcal{Z}(g)) \cup (\mathcal{Z}(f_2) \cap \mathcal{Z}(g))$ . If we have proved the theorem for irreducibles then the first intersection has at most  $d_1 e$  points while the second has at most  $d_2 e$  points, hence a total number of points at most  $(d_1 + d_2)e = de$ .

We prove that  $\#(\mathcal{Z}(f) \cap \mathcal{Z}(g))$  is finite. We have finitely many intersections in  $\mathbb{A}^2$ , and we will embed  $\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$ . Let  $L = \{z = 0\}$  be the line at infinity. Then either  $\mathcal{Z}(f) \cap L$  is finite or  $\mathcal{Z}(g) \cap L$  is finite. Therefore,  $\mathcal{Z}(f) \cap \mathcal{Z}(g) \cap L$  is finite, and so  $\mathcal{Z}(f) \cap \mathcal{Z}(g)$  is finite in  $\mathbb{P}^2$ .

Change coordinates such that these finitely many points do not lie on the line at infinity. [To do so, pick a line  $\ell$  not passing through any of the points, and send  $\ell$  to the line at infinity.] Then  $\mathcal{Z}(f) \cap \mathcal{Z}(g)$  intersect in  $\mathbb{A}^2$ . By homework 3, this intersection has at most  $de$  points.  $\square$

## 22 25 May 2008

### 22.1 The group law on cubics

**Lemma.** *Let  $C$  be any non-singular cubic and  $L$  a line. Either*

- (1)  $L$  intersects  $C$  in distinct points  $p, q, r$ , or
- (2)  $L$  intersects  $C$  in  $p \neq q$ .  $L$  is the tangent line at  $p$  ( $p$  has multiplicity 2), or
- (3)  $L$  intersects  $C$  at  $p$ .  $L$  is the tangent line at  $p$ , which is an inflection point ( $p$  has multiplicity 3).

*That is,  $L \cap C$  has exactly three points, counted with multiplicity.*

*Proof.* Since  $L \not\subseteq C$ , pick  $b \in L \setminus C$  and  $a \in L$ . Make a change of coordinates such that  $a = [0 : 0 : 1]$  and  $b = [1 : 0 : 0]$ , and so  $L = \{y = 0\}$  and  $[1 : 0 : 0] \notin C$ . Let  $f$  be a cubic polynomial. For  $L \cap C$  we need  $f(x : 0 : z) = 0$ . Write  $f(x : 0 : z) = \mu(x - a_1 z)(x - a_2 z)(z - a_3 z)$ . Since  $[1 : 0 : 0] \notin C$ ,  $\mu \neq 0$ . Thus,  $L \cap C = \{[a : 0 : 1], [a_2 : 0 : 1], [a_3 : 0 : 1]\}$ . If  $a_1, a_2, a_3$  are distinct, then (1) is satisfied. If  $a_1 = a_2$ , then  $L$  is the tangent line, since at  $[a_1 : 0 : 1]$ ,  $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial z} = 0$ , and so (2) is satisfied. If  $a_1 = a_2 = a_3$ , then  $L$  has to be tangent by the same argument. Then

$$Hf = \begin{vmatrix} 0 & ? & 0 \\ ? & ? & ? \\ 0 & ? & 0 \end{vmatrix} = 0$$

and so  $p$  is an inflection point.  $\square$

**Theorem.** *Let  $C$  be any nonsingular cubic in  $\mathbb{P}^2$  with  $p_0 \in C$  an inflection point. Then there exists an abelian group law  $\oplus$  on  $C$  with  $p_0$  being the zero element, such that  $p, q, r \in C$  are collinear if and only if  $p \oplus q \oplus r = 0 (= p_0)$ .*

*Proof.* The inverse of  $p$  is the point defined by taking the line  $\overline{pp_0}$  and intersecting with  $C$  and  $\ominus p$ . [Then  $p, p_0, \ominus p$  are collinear if and only if  $p \oplus p_0 \oplus (\ominus p) = 0$ .] Note that  $\ominus p_0 = p_0$ .

In general,  $p \oplus q$  is defined as follows: take line  $\overline{pq}$  (or if  $p = q$ , take  $\overline{pq}$  as the tangent line), intersect it with  $C$  at  $r$ , then take the inverse of  $r$ , as above. We claim  $p_0$  is the zero element, e.g.  $p \oplus (\ominus p) = p_0$ , which holds by definition. Likewise,  $p \oplus p_0 = p$  by definition. It remains to check associativity, which we will do next time.  $\square$

*Remark.* For  $y^2z = x(x-z)(x-\lambda z)$ ,  $\ominus[x : y : z] = [x : -y : z]$ . This is because  $[0 : 1 : 0]$ ,  $[x : y : z]$ , and  $[x : -y : z]$  are collinear.

**Example.**  $C = \{y^2 = x^3 + x - 1\} \subseteq \mathbb{A}^2$ ,  $P = (1, 1)$  and  $Q = (2, -3)$ . The line through  $P, Q$  is  $y = -4x + 5$ . The point  $R$  is found by solving  $(-4x + 5)^2 = x^3 + x - 1$ , a cubic for which we already know two roots (1 and 2). The third root is 13, so the third point is  $(13, -47)$ . Then  $P \oplus Q = (13, 47)$ .

## 22.2 Proof of associativity

**Lemma.** *Let  $C, D$  be two cubics which intersect in nine points. If a third cubic passes through eight points of intersection, then it passes through the ninth.*

## 23 28 May 2008

**Example.** For the cubic  $y^2 - y = x^3 - x$ ,  $p_0 = [0 : 1 : 0]$ . Let  $P = (0, 0)$  and  $Q = (-1, 1)$ , and we compute  $P \oplus Q$ . The line  $PQ$  is  $\{y = -x\}$ , so we find the intersections by solving  $y^2 - y = -y^3 + y \Leftrightarrow y^3 + y^2 - 2y = 0$ . We find the third point of intersection  $R = (2, -2)$ . To find  $\bar{R}$ , we need  $R, \bar{R}, P_0$  to be collinear. The line  $RP_0$  is  $x = 2z$ . The intersection  $RP_0$  and cubic will occur at  $(2, 3, 1)$  Therefore,  $\bar{R} = P \oplus Q = (2, 3)$ .

### 23.1 Proving associativity

**Proposition** (Main proposition). *Let  $C, D$  be two projective cubics intersecting in nine points. Any cubic containing eight of these points passes through the ninth.*

We will prove this later, but first we check how to use it to prove associativity.

*Proof of associativity.* Let  $A, B, C$  be three points on a cubic. Let  $R$  be the third point of intersection with  $AB$ , let  $S$  be the third point of intersection with  $\bar{R}C$ , let  $L$  be the third point of intersection with  $BC$ , and let  $T$  be the third point of intersection with  $\bar{L}A$ . Note that  $\bar{S} = (A \oplus B) \oplus C$  and  $\bar{T} = A \oplus (B \oplus C)$ . We define the following lines:

$$\begin{array}{llll} L_1 : \text{line } ABR & L_2 : \text{line } R\bar{R}P_0 & L_3 : \text{line } C\bar{R}S & L_4 : \text{line } SP_0S \\ M_1 : \text{line } BCL & M_2 : \text{line } LP_0\bar{L} & M_3 : \text{line } A\bar{L}T & M_4 : \text{line } TP_0T \end{array}$$

We will show  $S = T$ . Look at cubic  $C$  and the reducible cubic  $L_1 \cup M_2 \cup L_3$ . They intersect in  $A, B, R, L, P_0, \bar{L}, C, \bar{R}$ , and  $S$ . Next look at the cubic  $M_1 \cup L_2 \cup M_3$ , which passes through the first eight of these nine points. By the main proposition, it passes through  $S$  as well. Therefore,  $S = T$ .

Note that if these points were not distinct, then we would perturb the points to separate them. By continuity, the argument still holds.  $\square$

Another application of the main proposition is Pascal's theorem. Pascal proved this theorem when he was 16 and gave 400 corollaries.

**Theorem** (Pascal's theorem). *Let  $A, B, C, D, E, F$  be points on a conic. Suppose  $AF$  intersects  $CD$  in  $P$ ,  $AB$  intersects  $DE$  in  $Q$ , and  $BC$  intersects  $FE$  in  $R$ . Then  $P, Q, R$  are collinear. (Think about intersecting the opposite edges of a hexagon).*

*Remark.* If the conic is the union of two lines, then this is Pappus' theorem.

*Proof.* Let  $L_1$  be the line  $AFP$ ,  $L_2$  be the line  $QDE$ , and  $L_3$  the line  $RBC$ . Likewise, draw the lines  $M_1 : PCD$ ,  $M_2 : QAB$ , and  $M_3 : RFE$ . The two conics  $L_1 \cup L_2 \cup L_3$  and  $M_1 \cup M_2 \cup M_3$  intersect at  $A, B, C, D, E, F, P, Q, R$ . The third cubic will be the conic plus the line through  $P, Q$ . This passes through the first eight of the points, hence it passes through the last,  $R$ . Since  $R$  is not on the conic, it must be on the line  $PQ$ . Therefore,  $P, Q, R$  are collinear. (Continued next class).  $\square$

*Proof of main proposition.* Let  $S_3$  be the space of all degree three homogeneous polynomials in three variables. Let  $p_1, \dots, p_n \in \mathbb{P}^2$  be the set  $S_3(p_1, \dots, p_n) = \{f \text{ polynomial of degree 3} : f(p_1) = \dots = f(p_n) = 0\}$ . Note that  $\dim S_3 = 10$ . It follows that  $S_3(p_1, \dots, p_n)$  is a subspace of  $S_3$ . Each  $f(p_i) = 0$  is a linear condition on the coefficient of  $f$ . Therefore,  $\dim S_3(p_1, \dots, p_{n+1}) \geq \dim S_3(p_1, \dots, p_n) - 1$ .

**Definition.** Points  $p_1, \dots, p_9$  are in *general position* if

- (1) no four of them lie on a line, and
- (2) no seven of them lie on an irreducible conic.

Next time, we will prove that if two cubics in  $\mathbb{P}^2$  intersect in nine points, then those points are in general position. We will also show that  $\dim S_3(p_1, \dots, p_8) = 2$  if  $p_1, \dots, p_8$  are in general position.

## 24 30 May 2008

### 24.1 Proof of main proposition continued

We saw last time that  $\dim S_3(p_1, \dots, p_{n+1}) \geq \dim S_3(p_1, \dots, p_n) - 1$ . Call the eight points that the third cubic passes through  $p_1, \dots, p_8$ .

*Claim.*  $p_1, \dots, p_8$  are in general position, e.g. no four lie on a line and no seven lie on an irreducible conic.

*Proof.* A line  $L$  intersects  $C$  in at most 3 points, or else  $L \subseteq C$ , likewise for  $D$ . But  $L \not\subseteq C \cap D$ , hence  $L$  contains at most three of  $p_1, \dots, p_8$ . Next, if seven points lie on a conic  $Q$ , then  $\#Q \cap C \geq 7$ , hence  $Q \subseteq C$ , and likewise for  $D$ , again a contradiction since  $C$  and  $D$  do not intersect along  $Q$ .  $\square$

*Claim.*  $S_3(p_1, \dots, p_8)$  is two-dimensional for  $p_1, \dots, p_8$  in general position.

This will finish the proof since  $C$  and  $D$  are in  $S_3(p_1, \dots, p_9)$ . Any other cubic  $E$  in  $S_3(p_1, \dots, p_8)$  must be  $E = \lambda C + \mu D$ , hence  $E$  vanishes at  $p_9$  since both  $C$  and  $D$  do.

*Proof.* In any case,  $\dim S_3(p_1, \dots, p_8) \geq 2$  since it has decreased by 1 from 10 at most eight times. Let us assume that  $\dim S_3(p_1, \dots, p_8) \geq 3$ . We will reach a contradiction in three cases.

For the main case, assume no three points lie on a line and no six lie on an irreducible conic. Let  $q, r$  be points on the line  $p_1 p_2 = L$ . Look at  $S_3(p_1, \dots, p_8, q, r)$ , which has dimension at least  $3 - 2 = 1$ . Let  $\Sigma$  be a cubic. The line  $p_1 p_2 q r$  intersects  $\Sigma$ . Thus,  $\Sigma = L \cup (\text{a conic})$ , where the conic contains  $p_3, \dots, p_8$ . Thus, the conic is reducible, hence it is a union of two lines. At least three of the points  $p_3, \dots, p_8$  will be on this line, a contradiction.

For the second case, suppose three points  $p_1, p_2, p_3$  lie on a line  $L$ . Let  $g \in L$ , and then  $\dim S_3(p_1, \dots, p_8, g) \geq 2$ . Let  $\Sigma$  be a cubic in this space, and  $\#\Sigma \cap L \geq 4$ , namely  $p_1, p_2, p_3, g$ . Then  $\Sigma = L \cup (\text{conic})$ , where the conic contains the remaining five points  $p_4, \dots, p_8$ . There is a unique conic through five points, hence  $\Sigma$  is unique, contradiction.

For the third case, suppose six points  $p_1, \dots, p_6$  lie on an irreducible conic  $T$ . Let  $g \in T$ . Then  $\dim S_3(p_1, \dots, p_6, g) \geq 2$  (again, the dimension drops by at most 1). Let  $\Sigma$  be a cubic in this space. Then  $\#\Sigma \cap T \geq 7$ , namely  $p_1, \dots, p_6, g$ . But  $\Sigma \cap T$  is at most six points, unless  $\Sigma = T \cup (\text{line})$ , where the line contains  $p_7, p_8$ . Then the line must be unique, hence  $\Sigma$  is unique, a contradiction.  $\square$

We have finally proved associativity on elliptic curves!

## 24.2 Elliptic curve encryption

Main idea: multiplication is easy, division is hard. Let  $C$  be a cubic curve with  $p_0$  an inflection point. Usually, these cubic curves are defined over finite fields.  $C$  is still a group under the usual addition.

### Multiplication is easy

For  $n \geq 1, P \in C$ , how hard is it to compute  $n \odot P = \underbrace{P \oplus \dots \oplus P}_{n \text{ times}}$ . Let  $n = 2^{a_1} + \dots + 2^{a_l}$  (that is, write  $n$  in binary). Then compute

$$P, 2 \odot P, 2 \odot (2 \odot P), \dots, 2^k \odot (P) \quad \text{for all } 2^k \leq n$$

where takes only  $\log n$  time. Then

$$n \odot P = 2^{a_1} \odot P \oplus \dots \oplus 2^{a_l} \odot P.$$

### Division is hard

If we know  $Q = n \odot P$ , then  $n$  is hard to find even if we know  $P, Q$ .

**Example.**  $y^2 = x^3 - 6x - 4$ ,  $P = (-1, 1)$ ,  $Q = \left(\frac{-131432401}{121462441}, \frac{-1481841884199}{1338637562261}\right)$ . It turns out that  $n = 5$ .

## 25 2 June 2008

### 25.1 Elliptic curve cryptography continued

**Encryption Procedure.** Alice and Bob want to exchange the message  $M$ . Think of  $M$  as a number. You need a key  $K$ , which both Alice and Bob know. Alice sends  $M + K$  to Bob. How to generate  $K$  using cubic curves? Pick  $C, p_0$ , pick  $P \in C$ . Make them really complicated. Alice picks a number  $a$  and tell Bob the point  $aP$ . Bob picks a number  $b$  and tells Alice the point  $bP$ . Then let  $K = abP$ .

*Claim.* Alice and Bob both know  $K$ , but nobody else knows  $K$ .

Indeed, Bob knows  $aP$  hence  $b(aP) = abP = K$ . Likewise, Alice knows  $bP$ , hence  $a(bP) = abP = K$ . The evil person does not know  $a, b$  even though he knows  $aP, bP$ , and  $P$ . Thus, he cannot know  $K$ .

The crux of the matter:  $(C, p_0)$  is an abelian group, e.g.  $a(bP) = b(aP) = abP$ . The same works for any other abelian group, e.g.  $C \cong \mathbb{Z}$ .

It is important to produce cubic curves with a lot of rational points. It is not known how to do this efficiently. The following theorem relates to this.

**Theorem** (Mordell-Weil). *If  $C$  is a cubic curve, there exist finitely many points  $P_1, \dots, P_n$  with rational coefficients on  $C$  such that any point with rational coefficients is  $\alpha_1 P_1 + \dots + \alpha_n P_n$  with  $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ . No known algorithm will tell you these points.*

Faltings: a degree  $d \geq 4$  curve in  $\mathbb{P}^2$  with rational coefficients has finitely many rational points.

## 25.2 Rank of a cubic curve

Let  $C$  be a cubic curve and let  $C(\mathbb{Q})$  be the set of rational points.  $C(\mathbb{Q})$  is a finitely generated abelian group (by Mordell-Weil), hence it should equal

$$\mathbb{Z}^r \times \underbrace{\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}}_{\text{torsion part } T}$$

Then  $r$  is the rank of  $C$ .

**Theorem** (Barry Mazur, 1976). *The torsion part  $T$  can be one of the following 15 groups:*

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n \leq 12 \text{ and } n \neq 11, \text{ and } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ when } n \leq 4.$$

How do you compute the rank  $r$ ? How big can the rank be?

**Conjecture.** *The rank grows to infinity.*

However, the highest known rank is 28 (Elkies, 2006).

Let  $C$  be a cubic curve with integer coefficients, e.g.  $y^2 = x^3 - 2$ . Let  $p$  be a prime and let  $n_p$  be the number of points in  $C \pmod{p}$ . We may find that the points are  $(3, 0), (1, 2), (1, -2), (2, 1), (2, -1)$ , so here  $n_5 = 5$ .

**Theorem** (Riemann hypothesis).  $p - 1 - 2\sqrt{p} \leq n_p \leq p - 1 + 2\sqrt{p}$ . *(This is a theorem, not a conjecture).*

Let

$$f(x) = \prod_{p \leq x} \frac{n_p}{p}$$

**Conjecture** (Birch-Swinerton-Dyer).  $f(x) \sim (\log x)^r$ , where  $r$  is the rank of the curve.

This problem is open and worth a lot of money; and it's open especially in rank at least 2.