MATH 953: ALGEBRAIC GEOMETRY

BRIAN HARBOURNE

Abstract. These are notes for an introductory course on Algebraic Geometry taught at the University of Nebraska-Lincoln, Spring 2011.

Lecture 1. January 12, 2011

Fundamentally, Algebraic Geometry is the study of the solution sets of systems of polynomial equations. So it seems appropriate to start at the beginning, as it is now known.

1.1. **In the beginning (of recorded history).** The British Museum has a cuneiform table [see http://www.malhatlantica.pt/mathis/Babilonia/BM13901.htm for a photo], BM 13901 (ca. 1700 BC) which has a problem and solution which reads:

Problem 1.1.1. *I totalled the area and (the side of) my square: it is 0;45. You put down 1, the unit. You break in half 1. You multiply 0;30 and 0;30. You add 0;15 to 0;45. The square root of 1 is 1. Subtract 0;30 that you multiplied (with itself) from 1 and 0;30 is (the side of) the square. [see http://www.maa.org/reviews/lsahoyrup.html]*

In the sexagesimal (i.e., base 60) number system used by the Babylonians, 0;45 means 45/60. Thus, in more familiar terms, the problem is to find x, given $x^2 + 1x = 3/4$. To find x, the tablet says to take half the coefficient of x, i.e., half of 1 which is $1/2 = 0;30$, square it and add to both sides to get $x^2 + x + (1/2)^2 = 3/4 + 1/4$, or $(x + 1/2)^2 = 1$. We have thus completed the square; taking square roots gives $x + 1/2 = 1$, and subtracting $1/2 = 0;30$ from both sides gives $x = 1/2$; i.e., $x = 0;30$. Never mind about the other solution $x = -3/2$; since it's negative, it was regarded as being fictitious to the Babylonians.

In any case, 4700 years ago, the Babylonians knew how to solve a quadratic equation by completing the square. In modern terms, if

$$x^2 + ax = b,$$

then $(x + a/2)^2 = b + (a/2)^2$ so

$$x = -a/2 \pm \sqrt{b + (a/2)^2}.$$

1.2. **Some time later in Medieval Italy.** In Italy in the Middle Ages, academicians put on public scholarly competitions. (This lives on today in the system of concorsi in modern Italy; to earn a university position in Italy, one must win a concorso, a competition among the various candidates, except today the problems are posed by a panel of professors, not by the candidates to each other. However, recent reforms may result in this system finally being abandoned. These competitions typically involved two people who each would propose problems for the other to solve. The one who could better solve the other's problems won the competition. You could make your reputation and establish your livelihood by doing well in these competitions. Thus if you made a discovery, such as how to solve certain equations, you had a strong incentive to keep it a secret, so you could pose problems to opponents that perhaps only you knew how to do.

An important such competition occurred in 1535. A certain Antonio Maria Fior challenged a certain self-taught Niccolo Fontana (who, due to a saber wound to his jaw suffered as a child when

Date: May 7, 2011.

French soldiers attacked his town, was nicknamed Tartaglia, pronounced Tartalya and meaning Stutterer) [see p. 99 of *The Ellipse: A Historical and Mathematical Journey*, by Arthur Mazer, Wiley, 2010]. Fior posed thirty problems to Fontana, each of which involved solving a cubic equation of the form $ax^3 + cx + d = 0$. One of the problems, for example, was the following:

Problem 1.2.1. *Two men together gain 1000 ducats. The gain of the first is the cube root of the gain of the second. What is the gain of each?*

I.e., if x is the gain of the first, then x^3 is the gain of the second so $x^3 + x = 1000$ and we must solve for x.

The source of the solution of the cubic is uncertain. Somehow Fior's teacher, Scipione del Ferro, a professor in Bologna, came to know how to solve certain cases of cubic equations, and he shared his method with Fior. Fior's challenge motivated Fontana to figure out those cases and possibly others also, with the result that Fontana prevailed in the competition. This attracted the attention of one Gerolamo Cardano, who pestered Fontana to reveal the secret. Eventually, under an oath of secrecy, Fontana shared his solution with Cardano, who (possibly after tracking down del Ferro's solution, thereby no longer being bound by the oath) then published it anyway in his 1545 work *Ars Magnus*, but giving credit to del Ferro, Fior and Fontana. (Cardano seems to have been at the forefront of the tradition of making one's reputation by publishing what one knows, rather than keeping it secret.)

Note that one can always reduce a cubic equation $ax^3+bx^2+cx+d = 0$ to the form $u^3+eu+f = 0$: first divide by a, then substitute $u - b/(3a)$ in for x to eliminate the term of degree $3 - 1 = 2$ (this is analogous to completing the square, which eliminates the term of degree $2 - 1 = 1$).

Now use the identity $(s + t)^3 = s^3 + 3s^2t + 3st^2 + t^3$, rewritten as:

$$(s + t)^3 - 3st(s + t) = s^3 + t^3.$$

This means $u = s + t$ is a solution of $u^3 + eu + f = 0$ if we choose s and t to solve the following system of equations:

$$-3st = e$$

and

$$s^3 + t^3 = -f.$$

But this is easy: substitute $s = -e/(3t)$ into the second equation and clear denominators to get

$$(t^3)^2 + ft^3 - e^3/27 = 0.$$

The Babylonians showed us how to solve this for t^3; then take cube roots to get t. Knowing t gives us s, since $s = -e/(3t)$, and from this we get $u = s + t$ and finally $x = u - b/(3a)$.

Cardano's student and former servant, Lodovico Ferrari, found the solution to a quartic equation. As usual, it is enough to solve $x^4 + cx^2 + dx + e = 0$. His solution is to rewrite it as $x^4 + 2cx^2 + c^2 = cx^2 - dx + c^2 - e$, or

$$(x^2 + c)^2 = cx^2 - dx + c^2 - e.$$

Now insert a supplementary variable y:

$$(x^2 + c + y)^2 = (c + 2y)x^2 - dx + (c^2 + 2cy + y^2 - e).$$

Note that the RHS is a quadratic polynomial in x. It would be nice if it were of the form $(\alpha x+\beta)^2$, a perfect square. The idea is to choose a value of y to make this happen. So choose y so that the RHS is a perfect square in x; i.e., choose y so that $(c + 2y)x^2 - dx + (c^2 + 2cy + y^2 - e)$ has discriminant $d^2 - 4(c+2y)(c^2 - e+2cy+y^2)$ equal to 0. This involves solving a cubic, which thanks to del Ferro/Fontana/Cardano we know how to do. Thus we get an equation of the form

$$(x^2 + c + y)^2 = (\alpha x + \beta)^2$$

hence $x = \pm\sqrt{-(c + y) \pm (\alpha x + \beta)}$.

Exercises:

Exercise 1.1. Find an exact solution for $x^3 + x = 1000$.

Solution by Ashley Weatherwax (also presented by her in class). Using the identity $(r+s)^3 - 3rs(r+s) = r^3 + s^3$, we get that $x = r + s$ is a solution to $x^3 + x = 1000$ whenever

$$1 = -3rs \text{ and } r^3 + s^3 = 1000$$

Solving for r in the first equation, we get $r = \frac{-1}{3s}$. Plugging this into the second equation, we get

$$(\frac{-1}{3s})^3 + s^3 = 1000$$

Multiplying through by s^3 and then substituting $v = s^3$, we get the above equation is quadratic in v:

$$\frac{-1}{27} + v^2 = 1000v \Rightarrow v^2 - 1000v - \frac{1}{27} = 0$$

Using the quadratic equation to solve for v, we get

$$v = \frac{1000 \pm \sqrt{(1000)^2 - 4(1)(\frac{-1}{27})}}{2} = \frac{4500 \pm \sqrt{20250003}}{9}$$

But recall that $v = s^3$, so in fact we have

$$s = \sqrt[3]{\frac{4500 \pm \sqrt{20250003}}{9}}$$

Finally, recall that $r = \frac{-1}{3s}$, and so

$$r + s = \frac{-1}{3\sqrt[3]{\frac{4500 \pm \sqrt{20250003}}{9}}} + \sqrt[3]{\frac{4500 \pm \sqrt{20250003}}{9}}$$

As a final note, both solutions (one with both $+$ and one with both $-$) are equal, and are approximately 9.96666679053. □

Exercise 1.2. Find an exact solution for $x^3 + 3x^2 - 3x - 11 = 0$.

Solution by Nora Youngs. To use the method given in class:

First we must remove the quadratic term, so we perform a variable change: Let $x = u - 1$.

$$\begin{aligned} x^3 + 3x^2 - 3x - 11 &= (u-1)^3 + 3(u-1)^2 - 3(u-1) - 11 \\ &= u^3 - 3u^2 + 3u - 1 + 3u^2 - 6u + 3 - 3u + 3 - 11 \\ &= u^3 - 6u - 6 \end{aligned}$$

The new equation is of the form $u^3 + cx + d = 0$ where $c = -6$, $d = -6$.

Thus, following again from the method $u = r + s$ is a solution if s is a solution to $(s^3)^2 - 6x - \frac{(-6)^3}{27} = 0$ and $r = \frac{6}{3(s)}$.

Solving the quadratic:

$$\begin{aligned}(s^3)^2 - 6x + 8 &= 0\\ (s^3)^2 - 6x + 9 &= 1\\ (s^3 - 3)^2 &= 1\\ s^3 - 3 &= 1\\ s^3 &= 4\\ s &= \sqrt[3]{4}\end{aligned}$$

Then $r = \frac{6}{3\sqrt[3]{4}} = \frac{6\sqrt[3]{16}}{12} = \frac{\sqrt[3]{16}}{2} = \sqrt[3]{2}$.
So $u = \sqrt[3]{4} + \sqrt[3]{2}$ is a solution to $u^3 - 6u - 6 = 0$.

And therefore, $x = u - 1 = \sqrt[3]{4} + \sqrt[3]{2} - 1$ is a solution to the original equation.

Note also that if we take the other option, $\sqrt{1}$ to be -1 instead of 1, we have $s = \sqrt[3]{2}$, $r = \sqrt[3]{4}$, and the solution is $x = \sqrt[3]{2} + \sqrt[3]{4} - 1$, the same as before.

□

Exercise 1.3. Find an exact solution for $x^4 + 4x^3 + 10x^2 - 76x - 104 = 0$.

Solution presented in class by Zheng Yang but typed up by BH. Making the substitution $u = x + 1$ converts $x^4 + 4x^3 + 10x^2 - 76x - 104 = 0$ to $u^4 + 4u^2 - 88u - 21 = 0$. Rewriting gives $u^4 + 8u^2 + 16 = 4u^2 + 88u + 21 + 16$ or $(u^2 + 4)^2 = 4u^2 + 88u + 37$. Now introduce a new variable y as follows:

$$(u^2 + 4 + y)^2 = (4 + 2y)u^2 + 88u + 37 + 8y + y^2$$

We pick y so that $(4+2y)u^2 + 88u + (37 + 8y + y^2)$ is a perfect square; i.e., we need the discriminant $88^2 - 4(37 + 8y + y^2)(4 + 2y)$ to vanish. This is a cubic (known as the resolvent cubic), which we now know how to solve. One solution is $y = 6$. Using this value of y the equation $(u^2 + 4 + y)^2 = (4 + 2y)u^2 + 88u + 37 + 8y + y^2$ becomes $(u^2 + 10)^2 = 16u^2 + 88u + 121$ or

$$(u^2 + 10)^2 = (4u + 11)^2.$$

Thus $u^2 + 10 = \pm(4u + 11)$. Taking the plus sign gives $u^2 - 4u - 1 = 0$ which has root $u = 2 \pm \sqrt{5}$, and thus $x = 1 \pm \sqrt{5}$ is a root of the original polynomial. □

Lecture 2. January 14, 2011

The scene expands to northern Europe. In 1824, Niels Henrik Abel and Paolo Ruffini independently prove that there is no general formula for solutions of quintic equations just in terms of the usual field operations (addition, subtraction, multiplication and division) and taking radicals. However, early in the 1800s it was proved that any non-constant polynomial with complex coefficients has a root (this is usually attributed to C. F. Gauss, but it is not clear that he actually had the first correct proof):

Theorem 2.1 (Fundamental Theorem of Algebra)**.** *If $f \in \mathbb{C}[x]$ is not a constant, then it has a root (i.e., the field of complex numbers $\mathbb{C}$ is algebraically closed).*

Corollary 2.2. *If $f \in \mathbb{C}[x]$ has degree $\deg(f) = d > 0$, then $f(x) = a(x - c_1)\cdots(x - c_d)$ for constants $a, c_1, \ldots, c_d \in \mathbb{C}$; i.e., f has d roots, counted with multiplicity.*

Proof. Let $f(c) = 0$, so c is a root. Using polynomial division, we have $f(x) = q(x)(x - c) + r(x)$ where r is a constant (since the remainder term can always be taken to have degree less than the divisor, $x - c$). Since $f(c) = 0$, we have $r = 0$, so $f(x) = q(x)(x - c)$, but $\deg(q(x)) = \deg(f(x)) - 1$. The result follows by induction. □

Thus a polynomial of degree d determines a choice (unique up to reindexing) of d constants $c_1, \ldots, c_d$ (repeats allowed), and any such d choices of constants determines a unique monic polynomial $(x - c_1) \cdots (x - c_d)$ of degree d. The following definition formalizes this interplay between algebra and geometry:

Definition 2.3. Given a subset $S \subseteq \mathbb{C}[x]$, let $Z(S)$ be the set of simultaneous solutions to $f(x) = 0$ for all $f \in S$; i.e., $Z(S) = \{c \in \mathbb{C} : f(c) = 0 \text{ for all } f \in S\} \subseteq \mathbb{C}$ is the *zero set* of S. And given any subset $V \subset \mathbb{C}$, let $I(V) \subseteq \mathbb{C}[x]$ be the set of all $f \in \mathbb{C}[x]$ such that $f(c) = 0$ for all $c \in V$.

Note that if $S \subseteq \mathbb{C}[x]$, there is a unique smallest ideal, denoted $I(S)$, that contains S, called the ideal generated by S. The intersection of any collection of ideals is itself an ideal; $I(S)$ is the intersection of all ideals that contain S. Alternatively, $I(S)$ is the set of all finite sums of the form $\sum_i g_i f_i$ where $g_i \in \mathbb{C}[x]$ and $f_i \in S$.

When $n > 1$, note that $\mathbb{C}[x_1, \ldots, x_n]$ is a UFD but not a PID. Nevertheless, we can define $Z(S)$ and $I(S)$ for $S \subseteq \mathbb{C}[x_1, \ldots, x_n]$ as before, and likewise also $I(V)$ for $V \subseteq \mathbb{C}^n$, and we have $Z(S) = Z(I(S))$ exactly as before.

Definition 2.4. We say a subset $V \subseteq \mathbb{C}^n$ is an *algebraic subset* of $\mathbb{C}^n$ if $V = Z(S)$ for some subset $S \subseteq \mathbb{C}[x_1, \ldots, x_n]$.

Exercises:

Exercise 2.1. Let $V \subseteq \mathbb{C}^n$. Show that $I(V)$ is an ideal.

Solution by Philip Gipson. Certainly $0 \in I(V)$ and if $f \in I(V)$ then $-f(v) = -0 = 0$ for all $v \in V$ and so $-f \in I(V)$. If $f, g \in I(V)$ then for all $v \in V$ we have $f(v) + g(v) = 0 + 0 = 0$ and so $f + g \in I(V)$. Thus $I(V)$ is a group under addition.

If $f \in I(V)$ and $h \in \mathbb{C}[x_1, \ldots, x_n]$, then for all $v \in V$ we have that $h(v)f(v) = 0 \cdot 0 = 0$ and so $hf \in I(V)$. Therefore $I(V)$ is an ideal. □

Exercise 2.2. If $S \subseteq \mathbb{C}[x]$, show that $Z(S) = Z(I(S))$.

Solution by Jason Hardin. Suppose that $\alpha \in Z(S)$, so that $f(\alpha) = 0$ for all $f \in S$. Since we know that $I(S) = \left\{ \sum_{i=1}^{n} g_i f_i \mid g_i \in \mathbb{C}[x], f_i \in S, n \in \mathbb{N} \right\}$, given any $\sum_{i=1}^{n} g_i f_i \in I(S)$, we have $\left(\sum_{i=1}^{n} g_i f_i \right)(\alpha) = \sum_{i=1}^{n} g_i(\alpha) f_i(\alpha) = 0$, as $f_i \in S$ and thus $f_i(\alpha) = 0$ for $i = 1, \ldots, n$. So $\alpha \in Z(I(S))$ and $Z(S) \subseteq Z(I(S))$.

Conversely, if $f(\alpha) = 0$ for all $f \in I(S)$, then of course $f(\alpha) = 0$ for all $f \in S$, as $S \subseteq I(S)$. So $Z(I(S)) \subseteq Z(S)$, and equality follows. □

Exercise 2.3. Show that the algebraic subsets of $\mathbb{C}$ are precisely the finite subsets together with $\varnothing$ and $\mathbb{C}$; in particular, no infinite proper subset of $\mathbb{C}$ is an algebraic subset of $\mathbb{C}$.

Solution by Kat Shultis. It is clear that $\varnothing = Z(1)$ and $\mathbb{C} = Z(0)$. Let $A \subseteq \mathbb{C}$ be a finite set and write $A = \{c_1, \ldots, c_n\}$. Let $f(x) = (x - c_1) \cdots (x - c_n)$ so that $Z(f) = A$. Thus we know that $\varnothing$, $\mathbb{C}$, and any finite subset of $\mathbb{C}$ are algebraic subsets of $\mathbb{C}$. Now, let $A = Z(I)$ for some ideal I of $\mathbb{C}[x]$ and assume that A is an infinite set. Choose any $f \in I$. Then for every $p \in A$, we have that $f(p) = 0$. However, any non-zero polynomial f, has exactly the same number of zeros as its degree,

and since the degree of a non-zero polynomial is finite, we cannot have that f vanishes at infinitely many points. Thus, if A is an infinite but proper subset of $\mathbb{C}$, we cannot have A as an algebraic subset of $\mathbb{C}$. $\square$

Exercise 2.4. Give an example of an infinite proper subset of $\mathbb{C}^2$ which is an algebraic subset.

Solution by Doug Heltibridle. Let $S = \{x + y\}$, then $Z(S)$ has infinitely many elements, but it is a proper subset of $\mathbb{C}^2$ as $(1, 1)$ and $(-1, -1)$ are not solutions of $x + y$. Thus $V = Z(S)$ is an infinite proper subset of $\mathbb{C}^2$, which is algebraic by construction. $\square$

Exercise 2.5. Show that $(x_1, x_2) \subset \mathbb{C}[x_1, x_2]$ is not a principal ideal.

Solution. Say $(x_1, x_2) = (f)$ for some $f \in \mathbb{C}[x_1, x_2]$. Clearly f is not 0, and f divides x_1. Thus $\deg(f) \leq \deg(x_1) = 1$. I.e., $f = ax + b$ for constants $a, b \in \mathbb{C}$, so either $f = ax_1$ and a is non-zero, or $f = b$ and b is non-zero. In the latter case $(f) = \mathbb{C}[x_1, x_2]$ hence $(x_1, x_2) \subsetneq (f)$, while in the former case $(f) = (x_1)$, but x_1 does not divide x_2, so $x_2 \notin (f)$, hence again $(f) \neq (x_1, x_2)$. $\square$

Exercise 2.6. Let $I \subseteq J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be ideals and let $V \subseteq W \subseteq \mathbb{C}^n$. Show that $Z(J) \subseteq Z(I)$ and that $I(W) \subseteq I(V) \subseteq \mathbb{C}[x_1, \ldots, x_n]$.

Solution. If $p \in Z(J)$, then $f(p) = 0$ for all $f \in J$, and since $I \subseteq J$ it follows that $f(p) = 0$ for all $f \in I$, hence $p \in Z(I)$, so $Z(J) \subseteq Z(I)$.

If $f \in I(W)$, then $f(p) = 0$ for all $p \in W$, and since $V \subseteq W$ it follows that $f(p) = 0$ for all $p \in V$, hence $f \in I(V)$, so $I(W) \subseteq I(V)$. $\square$

Exercise 2.7. Let $I_1, \ldots, I_r \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be ideals. Define $\Pi_j I_j = I_1 \cdots I_r$ to be the ideal generated by all elements of the form $f_1 \cdots f_r$, where $f_j \in I_j$ for $1 \leq j \leq r$. Show that $Z(\cap_j I_j) = Z(\Pi_j I_j) = \cup_j Z(I_j)$.

Solution by Becky Egg. Let $p \in Z(\cap_{j=1}^r I_j)$, but suppose that $p \notin \cup_{j=1}^r Z(I_j)$. So in particular, $p \notin Z(I_j)$ for $1 \leq j \leq r$. So for each j, $1 \leq j \leq r$, there exists $f_j \in I_j$ such that $f_j(p) \neq 0$. Note that $f_1 \cdots f_r \in \cap_{j=1}^r I(J)$, and so we have

$$(f_1 \cdots f_r)(p) = f_1(p) \cdots f_r(p) = 0,$$

a contradiction, as each $f_i(p) \neq 0$. Thus $p \in \cup_{j=1}^r Z(I_j)$, and we have $Z(\cap_{j=1}^r I_j) \subseteq \cup_{i=1}^n Z(I_r)$.

Now let $p \in \cup_{j=1}^r Z(I_j)$, and suppose that $p \in Z(I_k)$ for some k with $1 \leq k \leq r$. Choose $f_j \in I_j$ for $1 \leq j \leq r$, and note that

$$(f_1 \cdots f_k \cdots f_r)(p) = f_1(p) \cdots f_k(p) \cdots f_r(p) = 0,$$

as $f_k(p) = 0$. Since $\prod_{j=1}^r I_j$ is generated by elements of the form $f_1 \cdots f_r$, we have that $f(p) = 0$ for all $f \in \prod_{j=1}^r I_j$, and hence $p \in Z(\prod_{j=1}^r I_j)$, so $\cup_{j=1}^r Z(I_j) \subseteq Z(\prod_{j=1}^r I_j)$.

Finally, let $p \in Z(\prod_{j=1}^r I_j)$, and let $f \in \cap_{j=1}^r I_j$. Then $f^r \in \prod_{j=1}^r I_j$, and so $f^r(p) = 0$, i.e., $(f(p))^r = 0$. So $f(p) = 0$, and hence $p \in Z(\cap_{j=1}^r I_j)$. Therefore we have

$$Z(\cap_{j=1}^r I_j) \subseteq \cup_{i=1}^n Z(I_r) \subseteq Z(\prod_{j=1}^r I_j) \subseteq Z(\cap_{j=1}^r I_j)$$

and thus

$$Z(\cap_j I_j) = Z(\Pi_j I_j) = \cup_j Z(I_j).$$

$\square$

Exercise 2.8. If $I_j \subseteq \mathbb{C}[x_1, \ldots, x_n]$ is a family of ideals, show that $\cap_j Z(I_j) = Z(\cup_j I_j)$ and that $\cup_j Z(I_j) \subseteq Z(\cap_j I_j)$, with equality if the family is a finite family. Conclude that set $\mathcal{T}$ of all algebraic subsets of $\mathbb{C}^n$ comprise the closed sets of a topology on $\mathbb{C}^n$; i.e., conclude that $\varnothing, \mathbb{C}^n \in \mathcal{T}$, that $\mathcal{T}$ is closed under arbitrary intersections and that $\mathcal{T}$ is closed under finite unions. This topology is

called the *Zariski* topology on $\mathbb{C}^n$. Given any algebraic subset $V \subseteq \mathbb{C}^n$, we thus have the subspace topology on V (in which a closed subset of V is a set of the form $V \cap C$, where C is a closed subset of $\mathbb{C}^n$), called the Zariski topology on V. [Note: this is named after Oscar Zariski. His son, the late Raphael Zariski, was a long-time professor of political science here at UNL.]

Solution. By Exercise 2.2, we have $Z(\cup_j I_j) = Z(I(\cup_j I_j))$. Since $I_j \subseteq \cup_j I_j \subseteq I(\cup_j I_j)$, it follows from Exercise 2.6 that $Z(\cup_j I_j) = Z(I(\cup_j I_j)) \subseteq Z(I_j)$ for every j, and hence that $Z(\cup_j I_j) \subseteq \cap_j Z(I_j)$. If $p \in \cap_j Z(I_j)$, then $f(p) = 0$ for all $f \in I_j$ for every j; i.e., $f(p) = 0$ for all $f \in \cup_j I_j$, hence $p \in Z(\cup_j I_j)$, so $\cap_j Z(I_j) \subseteq Z(\cup_j I_j)$ and thus $\cap_j Z(I_j) = Z(\cup_j I_j)$.

If $p \in \cup_j Z(I_j)$, then $p \in Z(I_j)$ for some j, but $\cap_j I_j \subseteq I_j$ so by Exercise 2.2 we have $p \in Z(I_j) \subseteq Z(\cap_j I_j)$ and hence $\cup_j Z(I_j) \subseteq Z(\cap_j I_j)$. Exercise 2.7 shows equality holds when j runs over a finite index set.

Clearly, $\varnothing, \mathbb{C}^n \in \mathcal{T}$ since $\varnothing = Z(1)$ and $\mathbb{C}^n = Z(0)$. And if C_j is a family of closed subsets, then for each j there is an ideal I_j such that $Z(I_j) = C_j$, so $\cap_j C_j = \cap_j Z(I_j) = Z(I(\cup_j I_j)) \in \mathcal{T}$, while $\cup_j C_j = \cup_j Z(I_j) = Z(\cap_j I_j) \in \mathcal{T}$ if j runs over a finite index set. Thus $\mathcal{T}$ satisfies the axioms for a topology. □

Exercise 2.9. Given any subset $V \subseteq \mathbb{C}^n$, show that $Z(I(V))$ is the Zariski closure $\overline{V}$ of V (i.e., that $Z(I(V))$ is the intersection of all algebraic subsets that contain V).

Solution by Katie Morrison. It is clear by definition that $V \subseteq Z(I(V))$ and $Z(I(V))$ is closed in the Zariski topology; thus, $\overline{V} \subseteq Z(I(V))$. Thus it suffices to show for any ideal J such that $V \subseteq Z(J)$, that $Z(I(V)) \subseteq Z(J)$ since then $Z(I(V))$ will be in the intersection of all such sets. Let J be such an ideal, then $V \subseteq Z(J)$ implies that for all $f \in J$, $f(v) = 0$ for all $v \in V$. Each such f lies in $I(V)$ by definition of $I(V)$. Thus, $J \subseteq I(V)$, and so by Exercise 2.6, $Z(I(V)) \subseteq Z(J)$. Thus $Z(I(V)) \subseteq \overline{V}$, and so $Z(I(V)) = \overline{V}$. □

Lecture 3. January 19, 2011

Hilbert's Nullstellensatz and the Basis Theorem. We start by restating the Fundamental Theorem of Algebra:

Theorem 3.1 (Fundamental Theorem of Algebra)**.** *Let $I \subsetneq \mathbb{C}[x]$ be an ideal. Then $Z(I) \neq \varnothing$.*

Proof. Since $\mathbb{C}[x]$ is a PID we know $I = (f)$ for some $f \in \mathbb{C}[x]$. Since $I \subsetneq \mathbb{C}[x]$, we know f is not a nonzero constant. By Exercise 2.2, $Z(I) = Z(f)$. If $f = 0$, then $Z(I) = Z(f) = \mathbb{C} \neq \varnothing$. If $f \neq 0$, then f is not a constant, so $\deg(f) > 0$, so f has a root by the FTA, so $Z(I) = Z(f) \neq \varnothing$. □

There are various equivalent versions of the Nullstellensatz. The FTA can be thought of as a special case of one of them.

Theorem 3.2 (Hilbert's Nullstellensatz, version 1)**.** *Let $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then $Z(I) \neq \varnothing$.*

Example 3.3. Given a subset $V \subseteq \mathbb{C}^n$, Exercise 2.9 shows that $Z(I(V)) = \overline{V}$. This raises the question of what happens when we start with an ideal $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ and consider $I(Z(J))$. In the special case that $J = I(V)$, this is now easy. Clearly $V \subseteq Z(I(V))$, hence $I(Z(I(V))) \subseteq I(V)$. To show $I(V) \subseteq I(Z(I(V)))$, let $f \in I(V)$. Then $Z(I(V)) \subseteq Z(f)$, so $f \in I(Z(f)) \subseteq I(Z(I(V)))$, hence $I(V) \subseteq I(Z(I(V)))$.

Example 3.3 answers what $I(Z(J))$ is when J is an ideal of the form $J = I(V)$. Another version of the Nullstellensatz answers the question of how $I(Z(J))$ is related to J in general.

> **Aside**: The Nullstellensatz (or zero points theorem) was only one of the results Hilbert proved around 1890 related to his work on invariant theory. Another possibly

more amazing result in this string is the Hilbert Basis Theorem, which says that ideals of $\mathbb{C}[x_1, \ldots, x_n]$ are finitely generated.

Theorem 3.4 (Hilbert's Basis Theorem)**.** *Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then $I = I(S)$ for some finite set $S \subset \mathbb{C}[x_1, \ldots, x_n]$.*

Note: this result holds if we replace $\mathbb{C}$ by any field.

The problem Hilbert was working on was to show that certain rings of invariants were finitely generated. For example, consider the multiplicative group $G = \{-1, 1\}$. This acts on $\mathbb{C}[x_1, \cdots, x_n] = R$ via $(c*f)(x_1, \ldots, x_n) = f(cx_1, \ldots, cx_n)$, where $c \in G$ and $f \in R$. The ring of invariants is the subset $R^G \subseteq R$ of all $f \in R$ such that $c*f = f$ for all $c \in G$. It's easy to see that $\mathbb{C} \subseteq R^G$ and that $x_i x_j \in R^G$. It's not too hard to see that in fact every element of R^G is a polynomial in the expressions $x_i x_j$ with coefficients in $\mathbb{C}$; i.e., $\{x_i x_j\}$ generate R^G over $\mathbb{C}$, so R^G is finitely generated.

Hilbert was mainly interested in an action where $G = \mathrm{SL}_n(\mathbb{C})$, the group of $n \times n$ matrices of determinant 1 with entries in $\mathbb{C}$. For example, in 1868 Paul Gordan (Emmy Noether was later to become Gordan's student) found a finite set of generators for R^G when $n = 2$ and $G = \mathrm{SL}_2(\mathbb{C})$. Hilbert used his Basis Theorem to prove finite generation for all n, but without finding an actual generating set. Gordan's reaction to Hilbert's proof is said to have been "Das ist nicht Mathematik, das ist Theologie" (although there is some question as to whether Gordan actually did say this). In any case, Hilbert recognized that it would be desirable to provide a constructive proof, and this led him to a partial solution, based on his Nullstellensatz. At this point Gordan (according to Constance Reid's biography on Hilbert) responded "I have convinced myself that theology also has its merits."

We need to recall some facts from commutative algebra in order to talk about additional versions of the Nullstellensatz.

Definition 3.5. An ideal I in a ring R (we'll always assume rings are commutative with $1 \neq 0$) is a *maximal* ideal if $I \subsetneq R$ and if J is an ideal with $I \subseteq J \subsetneq R$, then $I = J$.

The facts we need are: (1) every proper ideal is (by Zorn's Lemma) contained in a maximal ideal; and (2) an ideal I in a ring R is maximal if and only if I is maximal.

Last semester Tom Marley proved the following statement, whose proof is due to Artin and Tate (see Atiyah-MacDonald, Corollary 5.24, for a proof):

Theorem 3.6. *Let k be a field and let E be a finitely generated k-algebra which is a field; i.e., $E = k[x_1, \ldots, x_n]/I$ for some maximal ideal $I \subsetneq k[x_1, \ldots, x_n]$. Then E is a finite algebraic extension of k.*

This is often regarded as another version of the Nullstellensatz, but one in which the field is arbitrary. When $k = \mathbb{C}$ this is equivalent to version 1 above, as we shall see.

Exercises:

Exercise 3.1. Show that the Nullstellensatz is false if we replace $\mathbb{C}$ by $\mathbb{R}$.

Solution by Melissa DeVries. Consider the ideal $I = (x^2 + 1)$ in $\mathbb{R}[x]$. Note $\mathbb{R}[x]/I \cong \mathbb{C}$ by sending $\mathbb{R} \to \mathbb{R}$ identically and $x \mapsto i$, so I is a maximal ideal of $\mathbb{R}[x]$.

By Exercise 2.2 (the proof is the same for $\mathbb{R}$ in place of $\mathbb{C}$), $Z(I) = Z(x^2 + 1)$. As $x^2 + 1$ has no real roots, $Z(I) = Z(x^2 + 1) = \varnothing$.

As $\mathbb{R}[x]$ has a proper ideal I with an empty zero set, we see the Nullstellensatz fails with $\mathbb{R}$ in place of $\mathbb{C}$. $\square$

Lecture 4. January 21, 2011

Class started with Ashley and Zheng presenting solutions to homework problems. We then looked at another version of the Nullstellensatz:

Theorem 4.1 (Hilbert's Nullstellensatz, version 2)**.** *Let $M \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be a maximal ideal. Then there are constants $c_1, \ldots, c_n \in \mathbb{C}$ such that $M = (x_1 - c_1, \ldots, x_n - c_n)$.*

Proof. By the Nullstellensatz, version 1, there is a point $(c_1, \ldots, c_n) \in Z(M)$. Thus $x_i - c_i \in M$ for all i, hence $(x_1 - c_1, \ldots, x_n - c_n) \subseteq M$. But $(x_1 - c_1, \ldots, x_n - c_n)$ is a maximal ideal (since $\mathbb{C}[x_1, \ldots, x_n]/(x_1 - c_1, \ldots, x_n - c_n) \cong \mathbb{C}$), hence $(x_1 - c_1, \ldots, x_n - c_n) = M$. $\square$

Exercises:

Exercise 4.1. Show that versions 1 and 2 of the Nullstellensatz are equivalent.

Solution by Anisah Nu'Man. ($1 \Rightarrow 2$:) Proof in notes page 9. ($2 \Rightarrow 1$:) Let $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$. Since every proper ideal is contained in a maximal ideal, there exists an ideal $M \subseteq \mathbb{C}[x_1, \ldots x_n]$ such that $I \subseteq M$. By assumption we have $I \subseteq M = (x_1 - c_1, \ldots, x_n - c_n)$ for some $c_i \in \mathbb{C}$. Also since $I \subseteq M$ we have $Z(M) \subseteq Z(I)$, from exercise 2.6. Since $(c_1, \ldots, c_n) \in Z(M) \subseteq Z(I)$ we have $Z(I) \neq \varnothing$. $\square$

Exercise 4.2. Show that version 2 of the Nullstellensatz is equivalent to the following: If $M \subset \mathbb{C}[x_1, \ldots, x_n]$ is a maximal ideal, then there is an isomorphism $h : \mathbb{C}[x_1, \ldots, x_n]/M \to \mathbb{C}$ such that $\mathbb{C} \subset \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]/M \to \mathbb{C}$ is the identity on $\mathbb{C}$. [Aside: Note that this is essentially just Theorem 3.6 in case $k = \mathbb{C}$.]

Solution. Assume $M \subset \mathbb{C}[x_1, \ldots, x_n]$ is a maximal ideal, such that there is an isomorphism $h : \mathbb{C}[x_1, \ldots, x_n]/M \to \mathbb{C}$ inducing the identity on $\mathbb{C}$. Then for each i we have $h(x_i) = c_i \in \mathbb{C}$, so $x_i - c_i \in M$ for all i. Thus $(x_1 - c_1, \ldots, x_n - c_n) \subseteq M$. Since $(x_1 - c_1, \ldots, x_n - c_n)$ is maximal, we have $(x_1 - c_1, \ldots, x_n - c_n) = M$.

Conversely, assume $M = (x_1 - c_1, \ldots, x_n - c_n)$ for some constants $c_i \in \mathbb{C}$. Define a ring homomorphism $H : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ by setting $H|_{\mathbb{C}} = \mathrm{id}_{\mathbb{C}}$ and $H(x_i) = x_i$ for all i. Then $\ker(H) = M$, so H induces an isomorphism $h : \mathbb{C}[x_1, \ldots, x_n]/M \to \mathbb{C}$ which is the identity on $\mathbb{C}$. $\square$

Lecture 5. January 24, 2011

5.1. More on the Nullstellensatz.

Definition 5.1.1. Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. The *radical* $\sqrt{I}$ of I is the ideal generated by all $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that $f^r \in I$ for some $r \geq 1$. If $I = \sqrt{I}$ we say I is a radical ideal.

Theorem 5.1.2 (Hilbert's Nullstellensatz, version 3)**.** *Let $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal and let $f \in \mathbb{C}[x_1, \ldots, x_n]$. If $Z(J) \subseteq Z(f)$, then $f \in \sqrt{J}$.*

Proof. We have an inclusion $\mathbb{C}[x_1, \ldots, x_n] \subset \mathbb{C}[x_0, x_1, \ldots, x_n]$. Thus we can regard J and f as being in $\mathbb{C}[x_0, x_1, \ldots, x_n]$. Given $Z(J) \subseteq Z(f)$, we thus have $\varnothing = Z(J \cup \{x_0 f - 1\}) \subset \mathbb{C}^{n+1}$. By the Nullstellensatz, version 1, this means that J together with $x_0 f - 1$ generates the unit ideal; i.e., $1 \in I(J \cup \{x_0 f - 1\})$, so there exist $a, h \in \mathbb{C}[x_0, \ldots, x_n]$ and $g \in J$ such that $1 = ag + (x_0 f - 1)h$. Substitute $1/y$ for x_0 in $1 = ag + (x_0 f - 1)h$ and multiply by a large enough power y^N to clear the denominator. We get $a'g + (f - y)h' = y^N$, where $a' = y^N a(1/y, x_1, \ldots, x_n), h' = y^{N-1} h(1/y, x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n, y]$. Now substitute f in for y to get $a''g = f^N$. Since $g \in J$, this shows that $f \in \sqrt{J}$. $\square$

Theorem 5.1.3 (Hilbert's Nullstellensatz, version 4)**.** *Let $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then $I(Z(J)) = \sqrt{J}$.*

We leave the proof as an exercise (see Exercise 5.5).

5.2. **The Basis Theorem.** We now look at some consequences of Hilbert's Basis Theorem.

Definition 5.2.1. A topological space X is said to be *Noetherian* if it satisfies the Descending Chain Condition on closed subsets; i.e., every chain $\mathcal{C}$ of closed sets of X (i.e., every collection $\mathcal{C}$ totally ordered by inclusion), has a minimal element (i.e., an element $C \in \mathcal{C}$ such that $C \subseteq D$ for all $D \in \mathcal{C}$).

Example 5.2.2. The reals $\mathbb{R}$ with the standard topology is not Noetherian. For example, $\{[0, 1 + \frac{1}{n}] : n \geq 1\}$ is a chain of closed sets with no minimal element. However, the reals with the finite complement topology (in which the closed sets, other than the empty set and the whole space, are the finite subsets) *is* Noetherian, since then clearly every chain of closed sets has a minimal element.

Lemma 5.2.3. *The Zariski topology on an algebraic set $V \subseteq \mathbb{C}^n$ is Noetherian.*

Proof. Since closed subsets of closed subsets are closed, it's enough to prove that the Zariski topology on $\mathbb{C}^n$ is Noetherian. Let $\{C_j\}$ be a chain of closed subsets of $\mathbb{C}^n$. Let $I_j = I(C_j)$. Since $\{C_j\}$ is a chain, so is $\{I_j\}$, hence $\cup_j I_j$ is an ideal. By the Basis Theorem, $\cup_j I_j$ is finitely generated, so $\cup_j I_j = I_t$ for some t. By Exercise 2.8, $\cap_j Z(I_j) = Z(\cup_j I_j) = Z(I_t) = C_t$, hence C_t is a minimal element of $\{C_j\}$. □

Definition 5.2.4. A non-empty closed subset C of a topological space X is said to be *irreducible* if C is not the union $D_1 \cup D_2$ of closed subsets $D_i \subsetneq C$.

Exercises:

Exercise 5.1. Show that $(x - 1) \subset \mathbb{C}[x]$ is a radical ideal. Show that $\sqrt{((x-1)^2)} = (x - 1)$, so $((x - 1)^2)$ is not a radical ideal.

Solution presented in class by Nora Youngs. Recall that $\mathbb{C}[x]$ is a UFD. Let $S = \{f \in \mathbb{C}[x] : f^r \in (x - 1)\text{for some } r \geq 1\}$. Suppose $f \in S$. By the Fundamental Theorem of Algebra, we can write $f = (x - c_1) \cdots (x - c_n)$ for some complex numbers $c_1, \ldots, c_n$. Then $f^r = (x - c_1)^r \cdots (x - c_n)^r$.

We know $f^r \in (x - 1)$, so $f^r \in (x - 1)g$ for some $g \in \mathbb{C}[x]$. By our previous factorization of f, we have $c_i = 1$ for some i. Thus $x - 1$ divides f so $f \in (x - 1)$. Hence $S \subseteq (x - 1)$, so $\sqrt{(x - 1)} = I(S) \subseteq (x - 1)$ since $(x - 1)$ is an ideal containing S.

However, if $f \in (x - 1)$, then then $f^r \in (x - 1)$ for $r = 1$ so $f \in S \subseteq I(S) = \sqrt{(x - 1)}$. Thus $(x - 1) \subseteq \sqrt{(x - 1)}$. By the double containment we have $\sqrt{(x - 1)} = (x - 1)$.

Now consider $((x-1)^2)$. Let $S = \{f \in \mathbb{C}[x] : f^r \in ((x-1)^2)\text{for some } r \geq 1\}$. Note that $x-1 \in S$, as $(x - 1)^2 \in ((x - 1)^2)$. So $(x - 1) = I((x - 1)) \subseteq I(S) = \sqrt{((x - 1)^2)}$. However, if $f^r \in ((x - 1)^2)$ then again by the Fundamental Theorem of Algebra, 1 is a zero of f so $x - 1 \mid f$. Thus $f \in (x - 1)$, so $S \subseteq (x-1)$ and $\sqrt{((x - 1)^2)} = I(S) \subseteq (x-1)$. Therefore $\sqrt{((x - 1)^2)} = (x-1) \neq ((x-1)^2)$. □

Exercise 5.2. Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Let $S = \{f \in \mathbb{C}[x_1, \ldots, x_n] : f^r \in I \text{ for some } r \geq 1\}$, hence $\sqrt{I} = I(S)$. Show that $I(S) = S$; i.e., not only does S generate I but S is itself an ideal.

Solution presented in class by Douglas Heltibridle. Note that if I is a non-empty ideal, then $S \neq \emptyset$ as $I \subseteq S$. First to show that S has the absorption property, let $g \in \mathbb{C}[x_1, ..., x_n]$ and $f \in S$ such that $f^r \in I$. Then $(gf)^r = g^r f^r \in I$ as $f^r \in I$, which is an ideal.

Next, we show that S is closed under addition and contains inverses. Let $g \in \mathbb{C}[x_1, ..., x_n]$ and let $f, h \in S$ with $f^r \in I$ and $h^k \in I$. Then $(g(f-h))^{2rk} = a_{2rk}f^{2rk} + a_{2rk-1}f^{2rk-1}h + ... + a_1 f h^{2rk-1} + a_0 h^{2rk}$ and as each term has either h^k or f^r in it we know that it is in I as I is closed under addition. Thus $g(f-h) \in S$. which means that S is closed under addition and inverses. Thus S is an ideal and it contains itself, which means that $I(S) = S$. □

Exercise 5.3. Let $I, J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be ideals.

(a) Show that $I \subseteq \sqrt{I}$.
(b) Show that $Z(\sqrt{I}) = Z(I)$; conclude that $Z(I) = Z(J)$ if $\sqrt{I} = \sqrt{J}$.

Solution by Kat Shultis. (a) This is clear as if $f \in I$, then the first power of f is in I, $f = f^1 \in I$, so that $f \in \sqrt{I}$.

(b) We now have that $I \subseteq \sqrt{I}$, and so by Exercise 2.6, we know that $Z(\sqrt{I}) \subseteq Z(I)$. In order to show the other inclusion, let $p \in Z(I)$ and $f \in \sqrt{I}$ with $f^n \in I$. Then as $p \in Z(I)$ we have that $f^n(p) = 0$, which means that $f(p) = 0$ because $\mathbb{C}^n$ is an integral domain. Thus we have that for any $p \in Z(I)$ and $f \in \sqrt{I}$, that $f(p) = 0$, meaning that $Z(I) \subseteq Z(\sqrt{I})$, and hence $Z(I) = Z(\sqrt{I})$. □

Exercise 5.4. Show that versions 1 and 3 of the Nullstellensatz are equivalent.

Solution. The class notes show that version 1 implies version 3, so assume version 3. Let $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. If $Z(I) = \varnothing$, then $Z(I) \subseteq Z(1)$, hence $1 \in \sqrt{I}$ so $1 = 1^r \in I$ for some $r \geq 1$, contradicting $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$. □

Exercise 5.5. Show that versions 3 and 4 of the Nullstellensatz are equivalent.

Solution by Becky Egg. First suppose that version 3 holds. Let $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal, and $g \in \sqrt{J}$. Then $g^k \in J$ for some k. Given any $c \in Z(J)$, we have

$$0 = (g^k)(c) = (g(c))^k.$$

So $g(c) = 0$, and thus $g \in I(Z(J))$. Let $h \in I(Z(J))$ and $c \in Z(J)$. Then $h(c) = 0$ by definition, so $c \in Z((h))$. So $Z(J) \subseteq Z((h))$, and hence by version 3 of the Nullstellensatz, $h \in \sqrt{J}$. Thus $I(Z(J)) = \sqrt{J}$.

Now suppose that version 4 holds. Let $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$, and $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that $Z(J) \subseteq Z((f))$. By version 4, we have $I(Z(J)) = \sqrt{J}$. Since $I(Z((f)) \subseteq I(Z(J)))$, we have $f \in \sqrt{J}$, and thus version 3 holds. □

Exercise 5.6. If J is a radical ideal in $\mathbb{C}[x_1, \ldots, x_n]$, show that $J = I(V)$ for some algebraic subset $V \subseteq \mathbb{C}^n$.

Solution. Since $I(Z(J)) = \sqrt{J}$ by the Nullstellensatz, and since $J = \sqrt{J}$ by hypothesis, we have $I(V) = \sqrt{J} = J$ for $V = Z(J)$. □

Exercise 5.7. If J is an ideal in $\mathbb{C}[x_1, \ldots, x_n]$, show that $\sqrt{J} = \cap_{M \in S} M$, where S is the set of all maximal ideals containing J.

Solution by Katie Morrison. Let $M \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be a maximal ideal. Then $\sqrt{M} \subsetneq \mathbb{C}[x_1, \ldots, x_n]$ because $1 \neq \sqrt{M}$ since $1^r = 1 \neq M$ for all $r \geq 0$. Thus, $M \subseteq \sqrt{M} \subsetneq \mathbb{C}[x_1, \ldots, x_n]$, and so $M = \sqrt{M}$ since M is maximal. Thus, every maximal ideal is a radical ideal.

($\subseteq$) Observe that $J \subseteq \cap_{M \in S} M$, and so $\sqrt{J} \subseteq \sqrt{\cap_{M \in S} M}$. We stated in class (and will prove in Exercise 6.3) that $\sqrt{\cap_{M \in S} M} = \cap_{M \in S} \sqrt{M}$. Then by the earlier observation, $\cap_{M \in S} \sqrt{M} = \cap_{M \in S} M$. Thus, $\sqrt{J} \subseteq \cap_{M \in S} M$.

($\supseteq$) For each $\mathbf{z} \in Z(\sqrt{J})$, define $M_{\mathbf{z}} := (x_1 - z_1, \ldots, x_n - z_n)$ so that $Z(M_{\mathbf{z}}) = \mathbf{z}$. Now $M_{\mathbf{z}}$ is maximal since $\mathbb{C}[x_1, \ldots, x_n]/M_{\mathbf{z}} \cong \mathbb{C}$, which is a field. Furthermore, since $\mathbf{z} \in Z(J)$ we have that $J \subseteq I(Z(J)) \subseteq I(\mathbf{z}) = M_{\mathbf{z}}$, and so $J \subseteq M_{\mathbf{z}}$. Thus, $M_{\mathbf{z}} \in S$ for all $\mathbf{z} \in \sqrt{J}$. Then

$Z(\sqrt{J}) = \cup_{\mathbf{z}\in Z(\sqrt{J})} Z(M_{\mathbf{z}}) \subseteq \cup_{M\in S} Z(M)$. By Exercise 2.8, $\cup_{M\in S} Z(M) \subseteq Z(\cap_{M\in S} M)$, and so $Z(\sqrt{J}) \subseteq Z(\cap_{M\in S} M)$. Then by Exercise 2.6, $I(Z(\cap_{M\in S} M)) \subseteq I(Z(\sqrt{J}))$. Finally since $\cap_{M\in S} M \subseteq I(Z(\cap_{M\in S} M))$ and $\sqrt{J} = I(Z(\sqrt{J}))$, we have that $\cap_{M\in S} M \subseteq \sqrt{J}$, and so equality holds. □

Exercise 5.8. Consider the subring $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{C}$ consisting of all complex numbers of the form $a + b\sqrt{-5}$ where a and b are integers. Show that 2 and 3 are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ but not prime. [Hint: use the norm, and then factor 6 in two different ways.]

Solution by Anisah Nu'Man. For sake of a contradiction suppose 2 is reducible. Then there exists an $x = a+b\sqrt{-5}$ and $y = c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that x, y are not units and $N(xy) = N(x)N(y) = N(2)$. Thus we have $N(x)N(y) = N(2) = 4$ Since x, y are not units we know the $N(x), N(y) \neq 1$, so we have the $N(x) = N(y) = 2$. Therefore we have $N(x) = N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$. This implies that $b^2 = 0$ and $a^2 = 2$. But there is no integer such that $a^2 = 2$. Thus the $N(x) \neq 2$, and so we must have, without loss of generality, that $N(x) = 1$ and the $N(y) = 4$. Thus x is a unit and 2 is irreducible. Using an identical argument we can show that 3 is also irreducible. Last we have (2) is not prime since $6 = (1+\sqrt{-5})(1-\sqrt{-5}) \in (2)$ but neither $(1+\sqrt{-5})$ or $(1-\sqrt{-5})$ are in (2). Similarly, (3) is not prime since $6 \in (3)$, but using the same factorization $6 = (1 + \sqrt{-5})(1 - \sqrt{5})$ we have $(1 + \sqrt{-5})$ and $(1 - \sqrt{-5})$ are not in (3). □

Exercise 5.9. In an integral domain (i.e., a commutative ring with $1 \neq 0$ and with no zero divisors) show that every prime element is irreducible, and in a UFD, show that every irreducible element is prime.

Solution by Katie Morrison. Let D be an integral domain, and let $a \in D$ be a prime element. Suppose $a = bc$ for some $b, c \in D$. Then $a|bc$, and so $a|b$ or $a|c$ since a is prime. Without loss of generality, say $a|b$, then there exists $k \in D$ such that $b = ak$. Observe that

$$b \cdot 1 = ak = (bc)k = b(ck).$$

Since D is a domain, cancellation holds, and so we have that $1 = ck$. Thus, c is a unit, and so a cannot be written as the product of non-units.

Let R be a UFD, and let a be an irreducible. Suppose $a|bc$ for some $b, c \in R$, i.e. $ak = bc$ for some $k \in R$. Since R is a UFD, there exist irreducibles $p_1, \ldots, p_l, q_1, \ldots, q_m, r_1, \ldots, r_n \in R$ such that b can be uniquely written as $p_1 \cdots p_l$, c can be uniquely written as $q_1, \ldots, q_m$, and k can be uniquely written as $r_1 \cdots r_n$. Then $bc = p_1 \cdots p_l \cdot q_1 \cdots q_m$, $ak = a \cdot r_1 \cdots r_n$, and these decompositions are unique. Thus, the multiset $\{p_1, \ldots, p_l, q_1, \ldots, q_m\}$ equals the multiset $\{a, r_1, \ldots, r_n\}$, and so there exists some p_i or q_j that equals a. Without loss of generality, say that $a = p_i$ for some $1 \leq i \leq l$. Then we have that $b = a \cdot \Pi_{j\neq i} p_j$, and so $a|b$. Thus, a is prime. □

Lecture 6. January 26, 2011

Note: An algebraic set which is not irreducible is said to be *reducible*.

Example 6.1. Consider the algebraic set $V = Z(xy) \subset \mathbb{C}^2$; here our polynomial ring is $\mathbb{C}[x, y]$. Then in the Zariski topology, $V = Z(x) \cup Z(y)$ is the union of two proper closed subsets, so V is reducible.

Example 6.2. Now consider the algebraic set $V = Z(xy - 1) \subset \mathbb{C}^2$. This time V is irreducible. Every closed subset of V is of the form $V \cap C$ for some $C = Z(J)$, where $J \subseteq \mathbb{C}[x, y]$ is an ideal. But $\mathbb{C}[x, y]$ is Noetherian, so C is the intersection of a finitely many closed subsets of the form $Z(f)$, where $f \in \mathbb{C}[x, y]$. But consider $V \cap Z(f)$, where f is a non-zero element of $\mathbb{C}[x, y]$. Then any $p = (a, b) \in V \cap Z(f)$ satisfies $b = 1/a$ and $0 = f(a, b) = f(a, 1/a)$. For some $N \gg 0$, $x^N f(x, 1/x)$ is a polynomial in x, and any non-zero root of $f(x, 1/x)$ is also a root of h and vice versa. But h has only finitely many roots, hence the same is true of $f(x, 1/x)$, and thus $V \cap Z(f)$ is finite. Since

any proper closed subset of V is finite yet V is infinite, we see that V is irreducible in the Zariski topology (but not, it is easy to see, in the standard topology).

Lemma 6.3. *Every non-empty closed subset C of a Noetherian topological space X is the union $C = C_1 \cup \cdots \cup C_r$ of finitely many irreducible closed subsets C_j. Moreover, the union can be chosen to be* irredundant *(i.e., so that none of the C_i contains any of the others), in which case the decomposition is unique up to order.*

Proof. (The proof in class didn't use Zorn's lemma. For variety, here's a different proof.) Let $\mathcal{F}$ be the set of all non-empty closed subsets of X which are not finite unions of irreducible closed subsets. If $\mathcal{F}$ is not empty, then by Zorn's lemma (using the fact that X is Noetherian, so that we know descending chains of closed sets are bounded below), $\mathcal{F}$ has a minimal element D, and clearly D cannot be irreducible. Write $D = D_1 \cup D_2$ for non-empty proper closed subsets D_i. Since D is minimal, neither D_i is in $\mathcal{F}$, hence each is the union of finitely many irreducible closed subsets, and thus so is D, contradicting our assumption that $D \in \mathcal{F}$. Thus $\mathcal{F}$ is empty and hence every non-empty closed set is a finite union of irreducible closed subsets.

Therefore, given any closed subset C, we can write $C = C_1 \cup \cdots \cup C_r$ for some choice of irreducible closed subsets C_i. Whenever there is an i and j such that $C_i \subseteq C_j$, we can remove C_i from the union. Thus we obtain a union where we can assume that no C_j contains any C_i.

Suppose we have two such unions, $C_1 \cup \cdots \cup C_r = D_1 \cup \cdots \cup D_s$. Then $D_i = \cup_j (C_j \cap D_i)$ and since D_i is irreducible, $D_i = C_j \cap D_i$ for some j, hence $D_i \subseteq C_j$. Likewise, $C_j \subseteq D_t$ for some t, hence $D_i \subseteq D_t$, so $j = t$ and $D_i = C_j$. Thus each of the D's equals one of the C's and vice versa, so $r = s$ and after reordering we can assume $D_l = C_l$ for $l = 1, \ldots, r$. Thus the decomposition is unique up to order. $\square$

Note that the proof of the preceding lemma is similar to the proof of prime factorization in the integers: given any positive integer n, we can write $n = p_1^{m_1} \cdots p_r^{m_r}$ for primes p_i in an essentially unique way. If we rephrase this in terms of ideals, we have for any n that $(n) = (p_1)^{m_1} \cap \cdots \cap (p_r)^{m_r}$; i.e., every ideal is the intersection of powers of prime ideals in an essentially unique way (if we aren't silly, such as $(0) = (0) \cap (2)$). This is an example of a primary decomposition. Nice ideals can be written as intersections of prime ideals in a unique way (see Exercise 6.4; the preceding lemma is the geometric manifestation of this (i.e., the geometric version of primary decompositions).

As we see already from the integers, ideals in general cannot be written as intersections of prime ideals. We can however, in a Noetherian ring, write every ideal as a finite intersection of primary ideals (but we lose uniqueness in general). We pause to recall the definitions.

A *prime* ideal $P \subset R$ in a ring R (commutative with $1 \neq 0$ as usual) is a proper ideal such that if $fg \in P$, then either $f \in P$ or $g \in P$. A proper ideal $Q \subset R$ is said to be *primary* if $fg \in Q$, then either $f \in Q$ or $g \in \sqrt{Q}$. Note that prime ideals are primary, but the reverse is not usually true. Writing an ideal J as a finite intersection of primary ideals is said to be a *primary decomposition* of J.

Exercises:

Exercise 6.1. Let $P \subset \mathbb{C}[x_1, \ldots, x_n]$ be a prime ideal. Show that $P = \sqrt{P}$.

Solution by Anisah Nu'Man. Clearly $P \subseteq \sqrt{P}$ since for $f \in P$ we have $f^1 = f \in P$. Now let $g \in \sqrt{P}$, thus $g^r \in P$ for some $r \geq 1$. Then $g \cdot g^{r-1} \in P$, and so either $g \in P$ or $g^{r-1} \in P$. If $g \in P$ we are done. If not $g^{r-1} = g \cdot g^{r-1} \in P$. Therefore either $g \in P$ or $g^{r-2} \in P$. If $g \in P$ we're done. If not, iteratively, this process must stop and so we have $g \in P$. By double containment we have $P = \sqrt{P}$. $\square$

Exercise 6.2. Let $C \subset \mathbb{C}^n$ be an irreducible algebraic set and let $P \subset \mathbb{C}[x_1, \ldots, x_n]$ be a prime ideal. Show that $I(C)$ is a prime ideal and show that $Z(P)$ is irreducible. Conclude that a closed subset D is irreducible if and only if $I(D)$ is prime.

Solution by Kat Shultis. First, we will show that $I(C)$ is prime by proving that if $I(C)$ is not prime, then C is reducible. So assume that $I(C)$ is not prime. This means that there exist elements $f, g \in \mathbb{C}[x_1, \ldots, x_n] \setminus I(C)$ such that $fg \in I(C)$. Consider the two closed sets $Z(f)$ and $Z(g)$ in $\mathbb{C}^n$. We know by Exercise 2.2 that $Z(f) = Z((f))$ and $Z(g) = Z((g))$. We also know, by Exercise 2.7 that $Z(f) \cup Z(g) = Z(fg)$. If $p \in C$, then $f(p)g(p) = 0$ as $fg \in I(C)$, meaning that $C \subseteq Z(fg) = Z(f) \cup Z(g)$. Notice that as neither f nor g is in $I(C)$, that there exists some point $p \in C$ such that $f(p) \neq 0$, meaning that $C \cap Z(f) \subsetneq C$, and similarly for g. Also, the intersection of finitely many closed sets is closed, so that $C = (C \cap Z(f)) \cup (C \cap Z(g))$ is a decomposition of C, and C is reducible.

Next, we show that $Z(P)$ is irreducible by contradiction. So, assume that $Z(P)$ is reducible. In other words there exist finitely many Zariski closed and irreducible sets $\{A_\alpha\}_{\alpha \in I}$ which are properly contained in $Z(P)$ such that $Z(P) = \cup_{\alpha \in I} A_\alpha$. This means that for each $\alpha \in I$ there exists an ideal $J_\alpha \subseteq C[x_1, \ldots, x_n]$, such that $A_\alpha = Z(J_\alpha)$. By Exercise 2.7, this is equivalent to saying that

$$Z(P) = \bigcup_{\alpha \in I} Z(J_\alpha) = Z\left(\bigcap_{\alpha \in I} J_\alpha\right) = Z\left(\prod_{\alpha \in I} J_\alpha\right).$$

As P is prime, we know that $I(Z(P)) = \sqrt{P} = P$ by exercise 6.1 and the Nullstellensatz, version 4. Thus, by exercise 6.1 we have that

$$P = I(Z(P)) = I\left(Z\left(\prod_{\alpha \in I} J_\alpha\right)\right) \supseteq \prod_{\alpha \in I} J_\alpha.$$

By definition of a prime ideal, we must have that $J_\alpha \subseteq P$ for some α. Then, by exercise 2.6, we have that $Z(P) \subseteq Z(J_\alpha)$ for some $\alpha \in I$ so that our original decomposition of $Z(P)$ was not actually a decomposition, providing a contradiction, and showing that $Z(P)$ is irredicuble. □

Exercise 6.3. Let $J = \cap_{i=1}^r J_i$ for ideals $J_i \subseteq \mathbb{C}[x_1, \ldots, x_n]$. Show that $\sqrt{J} = \cap_{i=1}^r \sqrt{J_i}$.

Solution by Ashley Weatherwax. We want to show that $\sqrt{\cap_{i=1}^r J_i} = \cap_{i=1}^r \sqrt{J_i}$. Let $f \in \sqrt{\cap_{i=1}^r J_i}$. The for some n, $f^n \in \cap_{i=1}^r J_i$. But then $f^n \in J_i$ for all i, and so $f\sqrt{J_i}$ for all i. Therefore, $f \in \cap\sqrt{J_i}$.

Now let $f \in \cap\sqrt{J_i}$. Then $f \in \sqrt{J_i}$ for all i, so there exists n_i such that $f^{n_i} \in J_i$ for each i. Let $m = n_1 \cdots n_r$. As J_i are ideals, $f^m \in J_i$ for all i, hence $f^m \in \cap J_i$ and thus $f \in \sqrt{\cap J_i}$. □

Exercise 6.4. Let $J \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Show that $\sqrt{J}$ can be written as the intersection of finitely many prime ideals, none of which contains another. [Aside: this is an analog of the fact that a square-free non-zero integer is a product of distinct primes.] Conclude that $\sqrt{J}$ is the intersection of all prime ideals that contain J.

Solution. We have seen that $Z(J) = Z(\sqrt{J})$ is a finite union $C_1 \cup \cdots \cup C_r$ of Zariski closed irreducible subsets C_i. Thus $I(C_i)$ is prime for each i, and $I(C_1 \cup \cdots \cup C_r) = \cap_i I(C_i)$, but by the Nullstellensatz $I(Z(J)) = \sqrt{J}$, so $\sqrt{J} = \cap_i I(C_i)$, as claimed. Since $\sqrt{J}$ is the intersection of some of the primes which contain J, it is certainly the intersection of all primes which contain J. □

Lecture 7. January 28, 2011

More on primary decomposition. By Exercise 6.4, given any ideal $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$, $\sqrt{J}$ is the intersection $P_1 \cap \cdots \cap P_r$ for prime ideals P_i. This is a primary decomposition of $\sqrt{J}$, which we may assume is *irredundant* (i.e., we may assume $P_i \not\subseteq P_j$ if $i \neq j$).

In fact, the primes P_i are the minimal primes that contain J, as we see from the following lemma. The geometric version of this lemma states: if C is an irreducible closed set contained in a union $C_1 \cup \cdots \cup C_r$ of closed sets C_i, then C is already contained in C_i for some i.

Lemma 7.1. *Let $P, J_i \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be ideals with P prime. If $J_1 \cap \cdots \cap J_r \subseteq P$, then $J_i \subseteq P$ for some i.*

Proof. If for each i we have $J_i \not\subseteq P$, then for each i we can pick $f_i \in J_i$ with $f_i \notin P$. Now $f = f_1 \cdots f_r \in J_1 \cap \cdots \cap J_r \subseteq P$, but because P is prime and $f_i \notin P$ for all i, we must have $f \notin P$. Thus by contradiction we must have $J_i \subseteq P$ for some i. □

Remark 7.2. Let $P_1, \ldots, P_r \subset \mathbb{C}[x_1, \ldots, x_n]$ be prime ideals. This lemma shows that if $P_i \not\subseteq P_j$ holds whenever $i \neq j$, then in fact we have the stronger property that $\cap_{i \neq j} P_i \not\subseteq P_j$. However, for primary ideals $Q_1, \ldots, Q_r \subset \mathbb{C}[x_1, \ldots, x_n]$, even if $Q_i \not\subseteq Q_j$ holds whenever $i \neq j$, there can be a j such that $\cap_{i \neq j} Q_i \subseteq Q_j$. For example, consider $Q_1 = (x^4, y^2), Q_2 = (x^3, xy, y^3), Q_3 = (x^2, y^3) \subset \mathbb{C}[x, y]$. In Figure 7.1, Q_1 is the ideal spanned by the monomials $x^i y^j$ such that the integer lattice point (i, j) is on or above the blue lines; Q_2 corresponds to the lattice points on or above the heavy black lines, Q_3 the red and $Q_1 \cap Q_3$ the green. Then $Q_i \not\subseteq Q_j$ if $i \neq j$ holds but $Q_1 \cap Q_3 =$

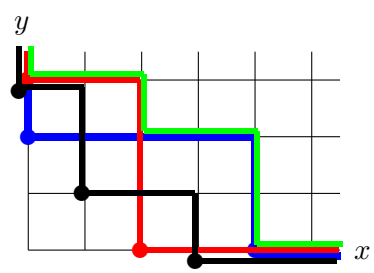


FIGURE 7.1. The monomial ideals Q_1 (blue), Q_2 (black), Q_3 (red) and $Q_1 \cap Q_3$ (green) from Remark 7.2.

$(x^4, x^2y^2, y^3) \subsetneq Q_2$. In this case, Q_1, Q_2 and Q_3 all have the same associated prime, $P = (x, y)$, but this is not essential. Consider $Q_1' = (x^4, y^2, a), Q_2' = (x^3, xy, y^3, a, b), Q_3' = (x^2, y^3, b) \subset \mathbb{C}[a, b, x, y]$. Then the associated primes are $P_1' = (a, x, y)$, $P_2' = (a, b, x, y)$ and $P_3' = (b, x, y)$ respectively, and $Q_i' \not\subseteq Q_j'$ holds whenever $i \neq j$, but again $Q_1' \cap Q_3' = (x^4, x^2y^2, y^3, ax^2, by^2, ab) \subsetneq Q_2'$.

Let $Q \subset \mathbb{C}[x_1, \ldots, x_n]$ be a primary ideal. By Exercise 7.1, $\sqrt{Q}$ is prime; we say that $\sqrt{Q}$ *belongs* to Q, or that Q is $\sqrt{Q}$-primary. Given an intersection $Q_1 \cap \cdots \cap Q_r$ of primary ideals Q_i, by Exercise 7.2 we may assume that the primes belonging to each Q_i are all different, and it is clear that we can remove $Q_i's$ if need be from the intersection $Q_1 \cap \cdots \cap Q_r$ so that we end up with an intersection such that for each j we have $\cap_{i \neq j} Q_i \not\subseteq Q_j$.

Definition 7.3. We say an intersection $Q_1 \cap \cdots \cap Q_r$ of primary ideals Q_i is *irredundant* if the primes belonging to each ideal Q_i are different and if for each i we have $\cap_{j \neq i} Q_j \not\subseteq Q_i$.

Given an irredundant primary decomposition $J = \cap Q_i$ of an ideal $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$, we refer to the primes belonging to the ideals Q_i as *belonging* to (or as being *associated* with) J. The primes belonging to an ideal J include the minimal primes containing J, but there may be additional primes too (see Exercise 7.4).

Definition 7.4. Let $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal, and let $P_1, \ldots, P_r$ be the distinct associated primes (i.e., the primes belonging to J). The minimal primes in the set $\{P_1, \ldots, P_r\}$ are called *isolated* primes. These correspond to the irreducible components of $Z(J)$. The non-minimal primes in the set $\{P_1, \ldots, P_r\}$ are called *embedded* primes.

Note that the isolated primes belonging to an ideal J are uniquely determined by J, since they are just the minimal primes containing J. In fact, all of the primes belonging to J are uniquely determined by J (see Atiyah-Macdonald, Theorem 4.5), as are the primary ideals corresponding to the minimal primes (see Atiyah-Macdonald, Corollary 4.11). The primary ideals corresponding to embedded primes are not in general uniquely determined however (see Exercise 7.4).

One way that embedded primes arise naturally is when taking powers.

Example 7.5. Let $J = (x, y) \cap (x, z) \cap (y, z) = (xy, xz, yz) \subset \mathbb{C}[x, y, z]$. Then J is radical; it is the ideal of the union of the coordinate axes in $\mathbb{C}^3$. It is easy to see that $J^2 \subsetneq (x, y)^2 \cap (x, z)^2 \cap (y, z)^2$: J^2 is generated by products of pairs of the generators of J, and each such product is in $(x, y)^2 \cap (x, z)^2 \cap (y, z)^2$ and has degree 4, hence $xyz \notin J^2$ even though $xyz \in (x, y)^2 \cap (x, z)^2 \cap (y, z)^2$. In fact, $J^2 = (x, y)^2 \cap (x, z)^2 \cap (y, z)^2 \cap (x, y, z)^4$ is an irredundant primary decomposition of J^2, so (x, y, z) is an embedded prime.

It's good to become familiar working with symbolic algebra programs, such as Macaulay 2. Here is the preceding example worked out using Macaulay 2 (but working over a finite field of characteristic 31991). This also demonstrates the use of the `primaryDecomposition` command.

```
> M2

Macaulay 2, version 0.9.2
--Copyright 1993-2001, D. R. Grayson and M. E. Stillman
--Singular-Factory 1.3c, copyright 1993-2001, G.-M. Greuel, et al.
--Singular-Libfac 0.3.2, copyright 1996-2001, M. Messollen

i1 : R=ZZ/31991[x,y,z]

o1 = R

o1 : PolynomialRing

i2 : X=ideal(y,z)

o2 = ideal (y, z)

o2 : Ideal of R

i3 : Y=ideal(x,z)

o3 = ideal (x, z)

o3 : Ideal of R

i4 : Z=ideal(x,y)

o4 = ideal (x, y)

o4 : Ideal of R

i5 : J=intersect(X,intersect(Y,Z))

o5 = ideal (y*z, x*z, x*y)
```

```
o5 : Ideal of R

i6 : M=ideal(x,y,z)

o6 = ideal (x, y, z)

o6 : Ideal of R

i7 : K=intersect(X^2,intersect(Y^2,intersect(Z^2,M^4)))

             2 2       2   2 2     2    2      2 2
o7 = ideal (y z , x*y*z , x z , x*y z, x y*z, x y )

o7 : Ideal of R

i8 : J^2==K

o8 = true

i9 : toString primaryDecomposition(J^2)

o9 = {monomialIdeal matrix {{x, y^2}}, monomialIdeal matrix {{x^2, y}},
monomialIdeal matrix {{x, z^2}}, monomialIdeal matrix {{x^2, y^2, z^2}},
monomialIdeal matrix {{y, z^2}}, monomialIdeal matrix {{x^2, z}},
monomialIdeal matrix {{y^2, z}}}
```

Note that `primaryDecomposition` does not give a decomposition for which each primary component has a different prime (which in principle it could do, by Exercise 7.2). But we can see from the computer output that the associated primes of J^2 are (x, y), (x, z), (y, z) and (x, y, z).

Exercises:

Exercise 7.1. Let $Q \subset \mathbb{C}[x_1, \ldots, x_n]$ be a primary ideal. Show that $\sqrt{Q}$ is prime.

Solution by Philip Gipson. Suppose $fg \in \sqrt{Q}$ but $f, g \notin \sqrt{Q}$. Then there exists an n such that $f^n g^n = (fg)^n \in Q$. Since Q is primary, we know that either $f^n \in Q$ of $g^n \in \sqrt{Q}$. If $f^n \in Q$, then by definition $f \in \sqrt{Q}$, contradicting our hypothesis. If $g^n \in \sqrt{Q}$, then $g^{nk} = (g^n)^k \in Q$ for some k, so $g \in \sqrt{Q}$, again contradicting our hypothesis. Therefore we conclude that either $f \in \sqrt{Q}$ of $g \in \sqrt{Q}$, and so $\sqrt{Q}$ is prime. □

Exercise 7.2. Let $Q_1, Q_2 \subset \mathbb{C}[x_1, \ldots, x_n]$ be primary ideals belonging to the same prime P. Show that $Q_1 \cap Q_2$ is also primary and belongs to P.

Solution by Jason Hardin. Observe that by Exercise 6.3, $\sqrt{Q_1 \cap Q_2} = \sqrt{Q_1} \cap \sqrt{Q_2} = P \cap P = P$, so if $Q_1 \cap Q_2$ is primary, then it must be P-primary.

Let $ab \in Q_1 \cap Q_2$. If $a \in Q_1 \cap Q_2$, we're done. So suppose $a \notin Q_1 \cap Q_2$. Wlog, suppose $a \notin Q_1$. Since $ab \in Q_1$ and Q_1 is primary, we must have $b \in \sqrt{Q_1} = P = \sqrt{Q_1 \cap Q_2}$. So $Q_1 \cap Q_2$ is primary. □

Exercise 7.3. Let $J \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal such that $\sqrt{J}$ is a maximal ideal. Show that J is primary. [Hint: if $g \notin \sqrt{J}$, show that there are polynomials $a \in J$ and b with $a + bg = 1$, and thus if $fg \in J$, then $(1 - a)f = bfg \in J$ and hence $f \in J$. Or see Atiyah-Macdonald, Proposition 4.2.]

Conclude that primary ideals (unlike what happens in $\mathbb{Z}$) are not always powers of prime ideals, by giving a simple example.

Solution by Zheng Yang. Suppose $fg \in J$ and $g \notin \sqrt{J}$. Since $\sqrt{J}$ is a maximal ideal (hence also prime), we have $(\sqrt{J}, g) \supsetneq \sqrt{J}$ and so $(\sqrt{J}, g) = (1)$. Then we have an equation $a + bg = 1$, for some $a \in \sqrt{J}$ (so $a^r \in J$ for some $r \geq 1$) and $b \in \mathbb{C}[x_1, \ldots, x_n]$. On the one hand, we have $(1-a)f = bfg \in J$ as $fg \in J$; on the other hand, we have $1-a$ is not in $\sqrt{J}$ (otherwise, $1 = 1-a+a \in \sqrt{J}$). Thus $(1-a^r)f = (1+a+\cdots+a^{r-1})(1-a)f = bfg \in J$, hence $f = (bg+a^r)f \in J$, since $a^r \in J$. Thus, $f \in (1-a)^{-1}J \subseteq J$ (note J is an ideal).

The ideal $(x^2, y) \subset \mathbb{C}[x, y]$ is an example of a primary ideal that is not a power of a prime ideal; see Lecture 8. Here is another example taken from Atiyah-Macdonald's book, Exercise 4.4. In $\mathbb{Z}[t]$, $m = (2, t)$ is a maximal, as $\mathbb{Z}[t]/m \cong \mathbb{Z}/2\mathbb{Z}$. The ideal $q = (4, t)$ is primary (because $\mathbb{Z}[t]/q \cong \mathbb{Z}/4\mathbb{Z}$, of which the only zero-divisors are $\bar{2}$ and it is nilpotent). But $m^2 = (4, t^2, 2t) \subsetneq q \subsetneq m$. So q is not a power of a power of prime ideal m. □

Exercise 7.4. Consider the ideal $J = (x^2, xy) \subset \mathbb{C}[x, y]$. Show $J = (x) \cap (x^2, y)$ and $J = (x) \cap (x^2, xy, y^n)$ for any $n \geq 1$ are primary decompositions of J. Conclude that the primes associated to J are (x) and (x, y).

Solution. First, (x), (x^2, y) and (x^2, xy, y^n) are primary, since (x) is prime and $\sqrt{(x^2, y)} = (x, y) = \sqrt{(x^2, xy, y^n)}$ are maximal. Thus $(x) \cap (x^2, y)$ and $(x) \cap (x^2, xy, y^n)$ are irredundant primary decompositions. Also it is easy to see that $J \subseteq (x) \cap (x^2, y)$ and $J \subseteq (x) \cap (x^2, xy, y^n)$. Consider an element $f \in (x) \cap (x^2, y)$. Since $f \in (x)$, we see $x|f$ so every term of f is divisible by x; in particular, f has no constant term and no terms that are pure powers of y. But $f \in (x^2, y)$, so every term of f is divisible by either x^2 or y (and hence also by xy since f has no terms that are pure powers of y). Thus f is in (x^2, xy), so $J = (x) \cap (x^2, y)$.

Now consider $f \in (x) \cap (x^2, xy, y^n)$ for any $n \geq 1$. As before, f has no terms that are pure powers of y, and since $f \in (x^2, xy, y^n)$, every terms is divisible by either x^2, xy or y^n but any term divisible by y^n also is divisible by x and hence by xy, so $f \in (x^2, xy)$ and we have $J = (x) \cap (x^2, xy, y^n)$.

This shows irredundant primary decompositions need note be unique. □

Lecture 8. January 31, 2011

Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and $J = (f) \subseteq \mathbb{C}[x_1, \ldots, x_n]$. Using the fact that $\mathbb{C}[x_1, \ldots, x_n]$ is a UFD, it is not hard to see that J is primary if and only if $\sqrt{J}$ is prime, and if J is primary, then $J = (\sqrt{J})^r$ for some $r \geq 1$. (This is Exercise 8.1.) We also know by Exercise 7.3 that M^r is primary for every $r \geq 1$ if M is a maximal idea, and as we will see in a later lecture, if J is a prime ideal in a polynomial ring with J generated by monomials (i.e., if J is a monomial ideal), then J^r is primary for every $r \geq 1$.

But principal, monomial and maximal ideals are rather special in this regard, since: it is not always true that an ideal is primary if its radical is prime; it is not always true that every primary ideal is a power of a prime ideal; and it is not always true that powers of prime ideals are primary.

For example, $(x^2, y) \subset \mathbb{C}[x, y]$ is primary by Exercise 7.3, since $\sqrt{(x^2, y)} = (x, y)$ is maximal, and thus the only prime that contains (x^2, y) is (x, y), but $(x, y)^2 \subsetneq (x^2, y) \subsetneq (x, y)$ so (x^2, y) is not $(x, y)^r$ for any r.

By Exercise 7.1 we know the radical of a primary ideal is prime. To show ideals with prime radical need not be primary, consider $J = (x^2, xy) \subset \mathbb{C}[x, y]$. Then $(x) \cap (x^2, y)$ is a primary decomposition, so (x^2, xy) is not primary (an alternative way to see this is that although $xy \in J$, we have $x \notin (x^2, xy)$ and $y \notin \sqrt{(x^2, xy)} = \sqrt{(x) \cap (x^2, y)} = \sqrt{(x)} \cap \sqrt{(x^2, y)} = (x) \cap (x, y) = (x)$), even though $P = \sqrt{(x^2, xy)} = (x)$ is prime. Note in this case that J has an associated prime $P' = \sqrt{(x^2, y)} = (x, y)$ other than P, and thus $P \subsetneq P'$; i.e., P' is an embedded prime. This must

always be the case when a non-primary ideal J has prime radical. (For suppose J is not primary, but has prime radical P. Consider an irredundant primary decomposition $J = Q_1 \cap \cdots \cap Q_r$. By assumption $P = \sqrt{J} = \sqrt{Q_1 \cap \cdots \cap Q_r} = \cap_i \sqrt{Q_i}$, so $P \subset \sqrt{Q_i}$ for all i and by Lemma 7.1 we know $\sqrt{Q_j} \subseteq P$ for some j and hence $P = \sqrt{Q_j}$; we may as well assume $P = \sqrt{Q_1}$. Since J is not primary, we also must have $r > 1$, so $P \subsetneq \sqrt{Q_2}$. Thus $\sqrt{Q_2}$ is an embedded prime.)

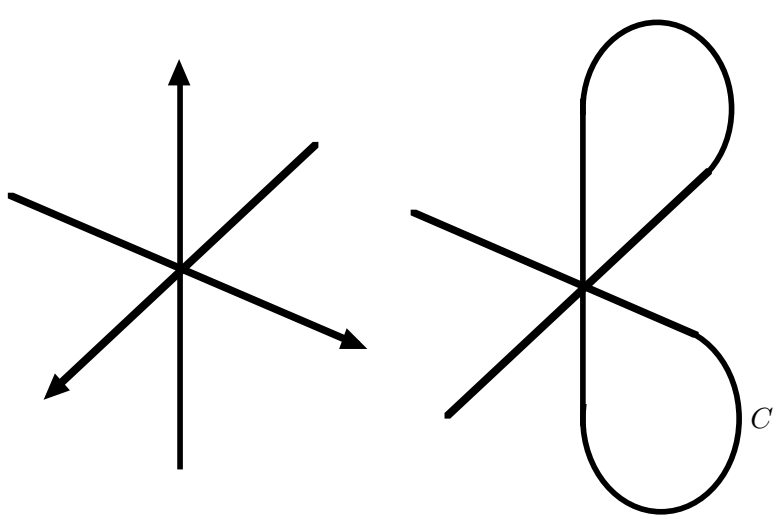
We now would like to give an example of an ideal (in a polynomial ring, even) which is a power of a prime ideal but which is not primary. Such examples tend to be a bit complicated. Example 3, p. 51 of Atiyah-Macdonald, gives an example of an ideal I which is power of a prime ideal yet is not primary, but the ring is not a polynomial ring. Example 8.18 of *Introduction to Algebraic Geometry* by Brendan Hassett gives an example of an ideal I which is a power of a prime ideal yet is not primary, and in this case the ring is a polynomial ring, but in 6 variables. It turns out that polynomial ring examples need at least 3 variables (this will be an exercise in a later lecture). Our example will use 3 variables.

Thus we need a prime ideal $P \subset \mathbb{C}[x, y, z]$ such that P^r is not primary and as noted above P^r must have an embedded associated prime. We already have an example of an ideal having a power with an embedded prime: J^2 has an embedded associated prime if J is the ideal of Example 7.5. Unfortunately, J is not prime, so we'd like to modify J to get a prime ideal without losing the square having an embedded associated prime.

In order to make a good guess about what to try, it's helpful to know what to pay attention to. Note that the zero locus of the embedded prime of J is a point which is *singular* on the curve $Z(J)$. Being a singular point essentially means that the curve crosses itself there. (A point which is not singular is said to be *smooth*. Smoothness is an important geometrical concept which we'll discuss more later. The point here is that embedded primes are related to smoothness. In fact, if $P \subset \mathbb{C}[x_1, \ldots, x_n]$ is a prime ideal and Q is an embedded prime of P^r for some $r > 0$, then $P \subsetneq Q$ so $Z(Q) \subsetneq Z(P)$, and it turns out that the points of $Z(Q)$ must be singular points of $Z(P)$.) Thus when we modify J to get a prime ideal we want to preserve the singularity at the origin.

One way to see that J is not prime is to note that $Z(J)$ is not irreducible; its irreducible components are the three coordinate axes. The conceptual idea is to take the coordinate axes (as shown at left in Figure 8.1) and connect them together to get (as shown at right in Figure 8.1) an "irreducible curve" $C \subset \mathbb{C}^3$ that has three branches at the origin (thus preserving the singularity), each branch tangent to a coordinate axis.

FIGURE 8.1. Coordinate axes and resulting irreducible heuristic curve C.



To a very small observer located at the origin the curve C would appear to be the union of the coordinate axes. If we can produce such a C which is an algebraic set, we might hope $I(C)$ and J would behave similarly in having embedded components at the origin. This is in fact the case in the example which we now do more rigorously, using computer calculations to guide us.

Example 8.1. Let $C \subset \mathbb{C}^3$ be the curve defined parametrically for all $t \in \mathbb{C}$ by

$$t \mapsto (t(t-1)^2(t+1)^2, t^2(t-1)(t+1)^2, t^2(t-1)^2(t+1)).$$

Note that three values of t map to $(0,0,0)$, these being $t = -1, 0, 1$, and otherwise (it is easy to see) the map $\mathbb{C} \to \mathbb{C}^3$ is injective.

Let P be the kernel of the homomorphism $h : \mathbb{C}[x,y,z] \to \mathbb{C}[t]$ which is the identity on $\mathbb{C}$ and otherwise is defined by

$$\begin{aligned} h(x) &= t\ (t-1)^2(t+1)^2, \\ h(y) &= t^2(t-1)\ (t+1)^2, \\ h(z) &= t^2(t-1)^2(t+1). \end{aligned}$$

We now discuss the ideal P. Note that if $g \in P$, then for any point $p = (a,b,c) \in C$ we have $(a,b,c) = (s(s-1)^2(s+1)^2, s^2(s-1)(s+1)^2, s^2(s-1)^2(s+1))$ for some value s of t and thus $g(a,b,c) = 0$, since

$$g(t(t-1)^2(t+1)^2, t^2(t-1)(t+1)^2, t^2(t-1)^2(t+1)) = h(g) = 0,$$

and so in particular

$$g(a,b,c) = g(s(s-1)^2(s+1)^2, s^2(s-1)(s+1)^2, s^2(s-1)^2(s+1)) = 0.$$

Thus $P \subseteq I(C)$, but for any $g \in I(C)$ we have $g(a,b,c) = 0$ for all $(a,b,c) \in C$ and hence $g(t(t-1)^2(t+1)^2, t^2(t-1)(t+1)^2, t^2(t-1)^2(t+1)) = 0$ for all $t \in \mathbb{C}$, so $h(g) = 0$ and thus $g \in \ker h = P$. In particular, $P = I(C)$. Moreover, P is a prime ideal (since $\mathbb{C}[t]$ is a domain).

The curve C passes through the origin when $t = 0$, $t = -1$ and $t = 1$, and each of these three branches is tangent to a different coordinate axis, giving the desired singularity at the origin. We next will investigate the possible existence of embedded primes.

Here we show some views of the curve C. Figure 8.2 shows two plots of the curve C. The one on the left was done using Maple (a very old version) with the following commands (the color varies from blue to red as the z-coordinate increases):

```
> with(plots):
> spacecurve([t*(t-1)^2*(t+1)^2,t^2*(t-1)*(t+1)^2,t^2*(t-1)^2*(t+1),
numpoints=1000], t=-1.1..1.1,axes=NORMAL);
```

The plot on the right was drawn using LaTeX picture environment commands. The LaTeX picture environment allows drawings to be done internally to LaTeX. The graph was done by plotting 3000 points on the curve. The coordinates of the points were computed ahead of time using AWK (see the file SpaceCurveData.tex for the very short AWK script). This graph is drawn so that parts of the curve closer to the observer are thicker, in an attempt to give perspective without color. Finally, Figure 8.3 gives a stereoscopic view of the curve C (created using 3D-Xplor-Math-J, available at http://3d-xplormath.org/).

FIGURE 8.2. Two views of the curve C.

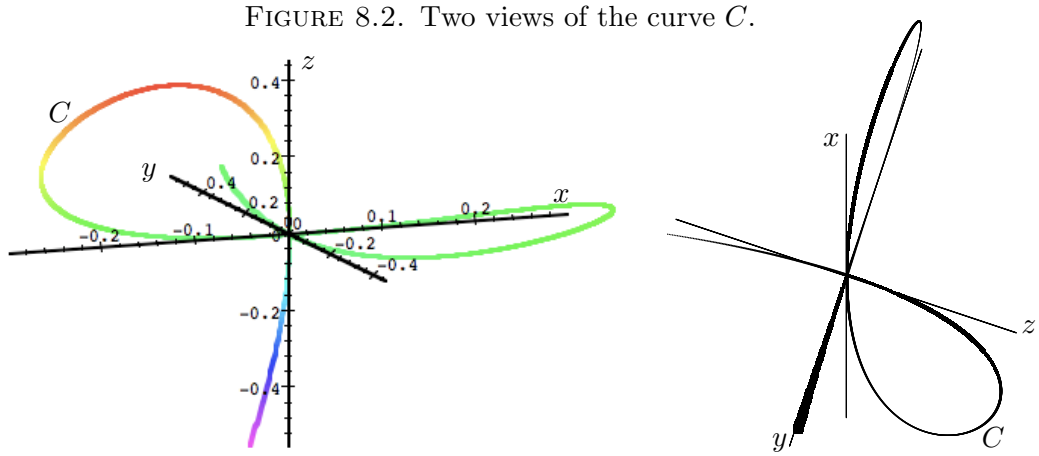
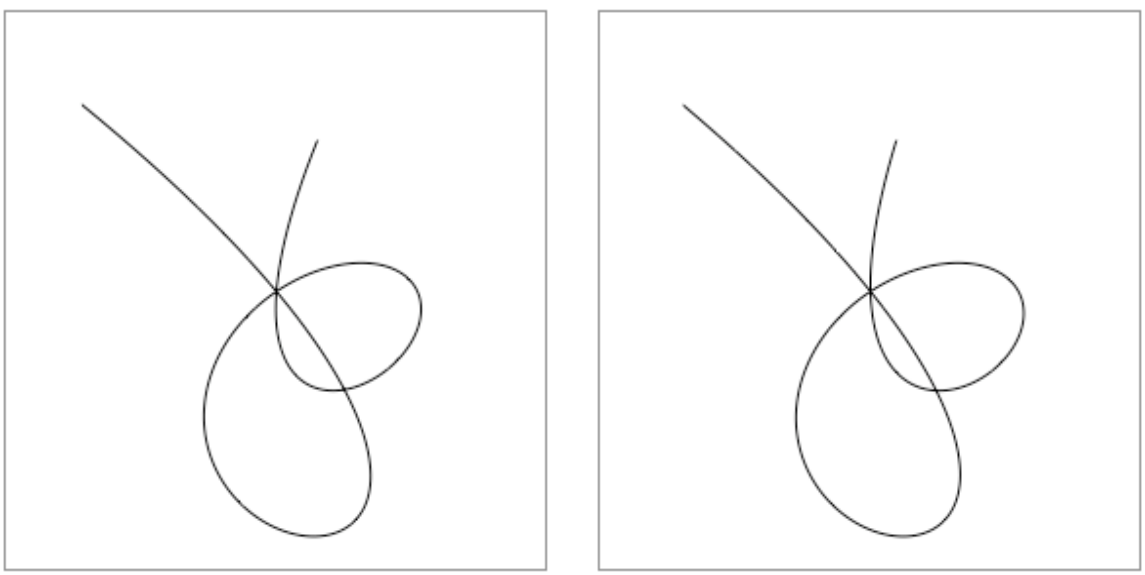


FIGURE 8.3. Stereoscopic view of the curve C.



Exercises:

Exercise 8.1. Let $J = (f) \subset \mathbb{C}[x_1, \ldots, x_n]$. Show that J is primary if and only if $\sqrt{J}$ is prime, and if J is primary, then $J = (\sqrt{J})^r$ for some $r \geq 1$.

Solution. Since primary ideals have prime radicals, if J is primary, then $\sqrt{J}$ is prime.

Before proving the converse, we note a fact about principal ideals. Let $f = f_1^{m_1} \cdots f_s^{m_s}$ be a factorization of f as a product of irreducibles, where $m_i \geq 1$ for all i and where f_i and f_j have no common irreducible factor if $i \neq j$. Let $I = (\phi)$, where $\phi = f_1 \cdots f_s$. Then $\phi^m \in J$ for $m = \max(m_1, \ldots, m_s)$, so $I \subseteq \sqrt{J}$. And if $g \in \sqrt{J}$, then $g^s \in (f)$ so $f | g^s$, hence $f_i | g^s$ for all i, so $f_i | g$ for all i, hence $\phi | g$ and we have $g \in I$. Thus $\sqrt{(J)} = I$.

Now assume $\sqrt{(J)}$ is prime. Then so is ϕ, hence $r = 1$; i.e., the prime factorization of f has only one prime factor. Thus $J = (f_1^{m_1}) = (\phi)^{m_1} = \sqrt{J}^{m_1}$, so if $ab \in J$ but $a \notin J$, then in the prime

factorization of ab, m_1 factors of f_1 occur but not all of them occur in the factorization of a, hence $f_1|b$, so $f_1^{m_1}|b^{m_1}$ and thus $b^{m_1} \in J$, so $b \in \sqrt{J}$, and so J is primary.

Finally, if J is primary, then $\sqrt{J}$ is prime, and as we saw above $J = \sqrt{J}^{m_1}$. □

Lecture 9. February 2, 2011

If $I = Q_1 \cap \cdots \cap Q_r$ is an irredundant primary decomposition we refer to each Q_i as the $\sqrt{Q_i}$-primary component of the decomposition. When $\sqrt{Q_i}$ is an isolated prime, the $\sqrt{Q_i}$-primary component is uniquely determined by I (it is the same in any primary decomposition of I; see Atiyah-Macdonald, Corollary 4.11).

When $I = Q^r$ for a prime ideal Q, then Q is the unique isolated prime, so the Q-primary component of I is uniquely determined by I. It is the smallest Q-primary ideal containing I, denoted $Q^{(r)}$ and referred to as the rth *symbolic power* of Q. Symbolic powers are very important geometrically. The fact that powers and symbolic powers do not always agree is at the root of various unsolved problems in algebraic geometry.

9.1. **A theorem of Zariski and Nagata and orders of vanishing.** Recall for any ideal $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$, that by the Nullstellensatz $\sqrt{I} = \cap M$, where the intersection is over all maximal ideals M containing I. A theorem of Zariski and Nagata (see Theorem 3.14, p. 106, of Eisenbud's book *Commutative Algebra with a view toward Algebraic Geometry*) generalizes this:

Theorem 9.1.1. *Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be a prime ideal. Then $I^{(r)} = \cap\, M^r$, where the intersection is over all maximal ideals M containing I.*

Definition 9.1.2. Let $p \in \mathbb{C}^n$ and let $M_p = I(p) \subset \mathbb{C}[x_1, \ldots, x_n]$ be the corresponding maximal ideal. Let f be a non-zero element of $\mathbb{C}[x_1, \ldots, x_n]$. If $f \in M^r$ but $f \notin M^{r+1}$, we say the *order of vanishing* of f at p is r and write $\mathrm{ord}_p(f) = r$. We regard the constant 0 as having infinite order of vanishing at all p.

Example 9.1.3. If $f(p) \neq 0$, then f does not vanish at p And we have $\mathrm{ord}_p(f) = 1$. If $p = (0, \ldots, 0)$ and f is not trivial, then $\mathrm{ord}_p(f)$ is the degree of a term of least degree. So for example $f = x^2y + y^5$ has order of vanishing 3 at the origin. If $p = (a_1, \ldots, a_n)$, then $\mathrm{ord}_p(f)$ is the degree of a term of $f(x_1 + a_1, \ldots, x_n + a_n)$ of least degree; i.e., find the degree of a term of least degree with respect to coordinates centered at the point p. If $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ is an ideal, the fact that $\sqrt{I} = \cap M$, where the intersection is over all maximal ideals M containing I, is just saying that the polynomials that vanish at all points $p \in Z(I)$ are precisely the elements of the radical of I. Theorem 9.1.1 says that the polynomials that vanish to order at least r at all points of an irreducible closed set V are exactly the elements of $Q^{(r)}$, where $Q = I(V)$.

9.2. **Return to our example of the last lecture.** Let J be the ideal of the union of the coordinate axes in $\mathbb{C}^3$ and let P be the ideal of the curve C defined parametrically in the previous lecture. Recall that $J^2 = (x, y)^2 \cap (x, z)^2 \cap (y, z)^2 \cap (x, y, z)^4$ is a primary decomposition of J^2. One way to see that $J^2 \subsetneq (x, y)^2 \cap (x, z)^2 \cap (y, z)^2$ is to note that $xyz \in (x, y)^2 \cap (x, z)^2 \cap (y, z)^2$ but (since $J = (xy, xz, yz)$ so J^2 has no elements of degree less than 4) that $xyz \notin J^2$.

Our goal is to find an element f that plays the same role for P^2 as xyz does for J^2, in the sense that f is in the P-primary component of an irredundant primary decomposition of P^2 but $f \notin P^2$, thus showing that P^2 has an embedded prime and hence P^2 is not primary.

By Theorem 9.1.1, it is enough to find an element f which is in M^2 for all maximal ideals M containing P, but such that $f \notin P^2$. In order to do this we need to find all such maximal ideals M, and we need to find our candidate element f. It follows by Exercise 9.1 that $C = \overline{C}$, and hence that a maximal ideal M_p contains C if and only if $p \in C$. We will verify $C = \overline{C}$ explicitly, with the help of Macaulay 2. We will also use Macaulay 2 to find f and verify that $f \in M^2$ for all $p \in C$;

it turns out that $f = xyz +$ higher order terms. We will see that $f \notin P^2$ follows from the fact that $Z(P)$ is singular at the origin.

Exercises:

Exercise 9.1. Let $f_1, \ldots, f_n \in \mathbb{C}[t]$ and define the map $h : \mathbb{C} \to \mathbb{C}^n$ given by $h(t) = (f_1(t), \ldots, f_n(t))$. Show that the image $h(\mathbb{C})$ of $\mathbb{C}$ under h is a Zariski closed subset of $\mathbb{C}^n$. [Hint: Apply the going-up theorem, Atiyah-Macdonald, Theorem 5.10, p. 62.]

Solution. If h maps $\mathbb{C}$ to a point, then clearly $h(\mathbb{C})$ is closed. Suppose h is not constant. Then f_i is a non-constant polynomial for some i. Hence $\mathbb{C}[f_i] \subseteq h^*(\mathbb{C}[x_0, \ldots, x_n]) \subseteq \mathbb{C}[t]$. Since f_i is non-constant, $\mathbb{C}[f_i] \subseteq \mathbb{C}[t]$ is an integral extension of rings, hence so is $h^*(\mathbb{C}[x_0, \ldots, x_n]) \subseteq \mathbb{C}[t]$.

Let $p \in \overline{h(\mathbb{C})}$; then $I(p)$ is a maximal ideal, hence prime. Since $\ker(h) = I(h(\mathbb{C})) = I(\overline{h(\mathbb{C})})$, and since $p \in \overline{h(\mathbb{C})}$, we have $I(\overline{h(\mathbb{C})}) \subseteq I(p)$. Now by Theorem 5.10 of Atiyah-Macdonald, for any prime ideal $Q \subseteq h^*(\mathbb{C}[x_0, \ldots, x_n])$, there is a prime ideal $P \subset \mathbb{C}[t]$ such that $P \cap h^*(\mathbb{C}[x_0, \ldots, x_n]) = Q$. In particular, there is a prime ideal $P \subset \mathbb{C}[t]$ such that $P \cap h^*(\mathbb{C}[x_0, \ldots, x_n]) = I(p)/\ker(h)$. This means $(h^*)^{-1}(P) = I(p)$. Moreover, P is maximal since if not $P = (0)$ (these are the only choices in $\mathbb{C}[t]$) but $P = (0)$ would mean $I(p) = \ker(h)$ which would in turn mean that $I(p) = I(h(\mathbb{C}))$, which implies $h(\mathbb{C}) = p$. Since P is maximal, $P = I(q)$ for some point $q \in \mathbb{C}$, and $(h^*)^{-1}(P) = I(p)$ means $h(q) = p$. I.e., $h(\mathbb{C}) = \overline{h(\mathbb{C})}$, so $h(\mathbb{C})$ is closed. $\square$

Lecture 10. February 4, 2011

In order to show that P^2 is not primary when P is the prime ideal defined in Example 8.1, we want to show $C = \overline{C}$ and we need to find a certain element f. Macaulay 2 will be helpful. We use it to gain some insight about P and P^2.

```
i1 : R=QQ[x,y,z];

i2 : S=QQ[t];

i3 : H=map(S,R,matrix{{t*(t-1)^2*(t+1)^2,t^2*(t-1)*(t+1)^2,t^2*(t-1)^2*(t+1)}});

o3 : RingMap S <--- R

i4 : P=ker H;

o4 : Ideal of R

i5 : toString P

o5 = ideal(x*y+x*z-2*y*z,y^3-8*x^2*z-7*y^2*z-8*x*z^2+23*y*z^2-z^3-8*y*z,
x^3-7/4*x^2*y+x*y^2-3/16*y^3-5/4*x^2*z+3/2*x*y*z-7/16*y^2*z+1/2*x*z^2
-5/16*y*z^2-1/16*z^3+1/2*x*y-1/2*x*z+1/2*y*z)

i6 : K=primaryDecomposition(P^2);

i7 : toString K

o6 = {ideal(x^2*y^2+2*x^2*y*z-4*x*y^2*z+x^2*z^2-4*x*y*z^2
+4*y^2*z^2,x*y^4-8*x^3*y*z-6*x*y^3*z-2*y^4*z-8*x^3*z^2+
```

```
8*x^2*y*z^2+16*x*y^2*z^2+14*y^3*z^2-8*x^2*z^3+38*x*y*z^3-46*y^2*z^3
-x*z^4+2*y*z^4-8*x*y^2*z-8*x*y*z^2+16*y^2*z^2,x^4*y+x^4*z-3*x^3*y*z
+1/4*x*y^3*z-x^3*z^2+4*x^2*y*z^2-7/4*x*y^2*z^2-1/2*y^3*z^2+2*x^2*z^3
-25/4*x*y*z^3+4*y^2*z^3-1/4*x*z^4+1/2*y*z^4-x^2*y*z-x^2*z^2+2*x*y*z^2,x^5
-1/32*y^5-5*x^3*y*z-5/4*x*y^3*z+15/32*y^4*z-5/2*x^2*y*z^2+25/2*x*y^2*z^2
-15/16*y^3*z^2-5/2*x^2*z^3+35/4*x*y*z^3-175/16*y^2*z^3+15/32*y*z^4
-1/32*z^5+x^3*y+1/8*x*y^3-x^3*z-x^2*y*z-7/8*x*y^2*z+1/4*y^3*z-x^2*z^2
+39/8*x*y*z^2-2*y^2*z^2-1/8*x*z^3-1/4*y*z^3-x*y*z,y^6-14*y^5*z+64*x^4*z^2
-80*x*y^3*z^2+95*y^4*z^2+128*x^3*z^3-640*x^2*y*z^3+624*x*y^2*z^3
-260*y^3*z^3-64*x^2*z^4+208*x*y*z^4-33*y^2*z^4+16*x*z^5-46*y*z^5
+z^6-16*y^4*z+128*x^2*y*z^2+112*y^3*z^2+128*x*y*z^3-368*y^2*z^3
+16*y*z^4+64*y^2*z^2), ideal(z,x^2*y^2,x*y^4,x^4*y,y^6,x^6)}
```

According to Macaulay 2, P is generated (over $\mathbb{Q}$) by

$$\begin{aligned}
g_1 =& xy + xz - 2yz,\\
g_2 =& y^3 - z^3 - 8x^2z - 7y^2z - 8xz^2 + 23yz^2 - 8yz,\\
g_3 =& x^3 - (3/16)y^3 - (7/4)x^2y + xy^2 - (5/4)x^2z + 3/2xyz - (7/16)y^2z\\
&+ (1/2)xz^2 - (5/16)yz^2 - (1/16)z^3 + (1/2)xy - (1/2)xz + (1/2)yz.
\end{aligned}$$

Certainly g_1, g_2 and g_3 are in P, because checking this just amounts to plugging in the parametric equations and checking to see that the expression simplifies to 0, and this is independent of the ground field.

Let $p = (a, b, c) \in Z(P)$. We wish to show $p \in C$. Since $g_1 \in P$, we see that if any of the coordinates of p are 0, then one of the other two coordinates is also 0. For example, if $a = 0$, then since $g_1(a, b, c) = 0$ we have $-2bc = 0$ so either $b = 0$ or $c = 0$. Now from $g_2 \in P$, given that $a = 0$, we see that $b = 0$ if and only if $c = 0$. Thus $a = 0$ implies $b = c = 0$. Similarly, if $b = 0$, then either $a = 0$ or $c = 0$, and we just saw that $a = 0$ implies $c = 0$. If $b = c = 0$, then $g_3 \in P$ implies $a = 0$. Finally, if $c = 0$, then as noted above either $a = 0$ or $b = 0$, but in either case all three coordinates are 0. Thus if any coordinate of p is 0, the point p must be the origin, and hence $p \in C$.

Now assume none of the coordinates of p is 0. If $a = b$, then g_1 gives $a = c$. Likewise, if $a = c$, then also $a = b$, and if $b = c$, then $b = a$. I.e., if any two of the coordinates are equal, all three are equal. But if $a = b = c$, then g_2 gives that $a = 0$. We thus see that if none of the coordinates is 0, then no two of them are equal. If $a = 2b$, then $g_1(a, b, c) = 0$ implies $c = 0$, so now we also know that $a \neq 2b$.

Now we wish to find a value of t such that

$$t \mapsto (t(t-1)^2(t+1)^2, t^2(t-1)(t+1)^2, t^2(t-1)^2(t+1)) = (a, b, c). \qquad (\star)$$

Let $t = \frac{b}{b-a}$, which is defined since $a \neq b$. Let (α, β, γ) be the image of $t = \frac{b}{b-a}$ under the map $(\star)$, so $\in C$. We also see that none of α, β or γ is 0, since this only happens if t is -1, 0 or 1, but $t = -1$ is ruled out since $2b \neq a$, $t = 0$ is ruled out since $b \neq 0$ and $t = 1$ is ruled out since $a \neq 0$. It is easy to check that

$$\frac{\alpha}{\beta} = \frac{t-1}{t} = \frac{a}{b}$$

and hence that $(\alpha, \beta) = d(a, b)$ for some non-zero constant d, and thus

$$\frac{\alpha}{2\beta - \alpha} = \frac{a}{2b - a}.$$

Since $g_1(\alpha, \beta, \gamma) = 0$ by definition of P, we have $\frac{\gamma}{\beta} = \frac{\alpha}{2\beta-\alpha}$ and since $g_1(a, b, c) = 0$ since $p \in Z(P)$, we have $\frac{c}{b} = \frac{a}{2b-a}$. Thus $\frac{\gamma}{\beta} = \frac{c}{b}$ so $(\alpha, \beta, \gamma) = d(a, b, c)$.

If we show $d = 1$, then $p = (a, b, c) = (\alpha, \beta, \gamma) \in C$, and we conclude that $C = \overline{C}$. Plug $(\alpha, \beta, \gamma) = d(a, b, c)$ into g_2. We get

$$0 = (\beta^3 - \gamma^3 - 8\alpha^2\gamma - 7\beta^2\gamma - 8\alpha\gamma^2 + 23\beta\gamma^2) - 8\beta\gamma = (b^3 - c^3 - 8a^2c - 7b^2c - 8ac^2 + 23bc^2)d^3 - 8bcd^2,$$

and since $d \neq= 0$, this means $(b^3 - c^3 - 8a^2c - 7b^2c - 8ac^2 + 23bc^2) - 8bc/d = 0$. But $0 = g_2(a, b, c) = (b^3 - c^3 - 8a^2c - 7b^2c - 8ac^2 + 23bc^2) - 8bc$, so $d = 1$.

Now consider the polynomial $f = x^5 - (1/32)y^5 - 5x^3yz - (5/4)xy^3z + (15/32)y^4z - (5/2)x^2yz^2 + (25/2)xy^2z^2 - (15/16)y^3z^2 - (5/2)x^2z^3 + (35/4)xyz^3 - (175/16)y^2z^3 + (15/32)yz^4 - (1/32)z^5 + x^3y + (1/8)xy^3 - x^3z - x^2yz - (7/8)xy^2z + (1/4)y^3z - x^2z^2 + (39/8)xyz^2 - 2y^2z^2 - (1/8)xz^3 - (1/4)yz^3 - xyz$. According to the Macaulay 2 output above, $f \in P^{(2)}$. We will give a proof of this in a moment, and we will also show that $f \notin P^2$, which proves that P^2 is not primary.

To show that $f \in P^{(2)}$, it suffices to show $f \in M^2$ for all maximal ideals M containing P. To show $f \notin P^2$, it suffices to show that $P \subseteq (x, y, z)^2$ and hence $P^2 \subseteq (x, y, z)^4$, but that $f \notin (x, y, z)^4$. But f has a term of degree 3 (namely xyz), so $f \notin (x, y, z)^4$, and hence $f \notin P^2$.

To show that $f \in M^2$ for all maximal ideals M containing P, we just need to show that $f \in M_p^2$ for all $p \in C$, since $C = \overline{C}$. Since we have a parameterization of C, we may assume every point $p = (a, b, c) \in C$ is of the form $p = (t(t-1)^2(t+1)^2, t^2(t-1)(t+1)^2, t^2(t-1)^2(t+1))$ for some value of t. Thus we just need to check that

$$f(x, y, z) \in (x - (t(t-1)^2(t+1)^2, y - t^2(t-1)(t+1)^2, z - t^2(t-1)^2(t+1))^2$$

holds for all t. Alternatively, by doing a translation we just need to check that

$$f(x + (t(t-1)^2(t+1)^2, y + t^2(t-1)(t+1)^2, z + t^2(t-1)^2(t+1)) \in (x, y, z)^2.$$

This is easy to do: just plug $x + (t(t-1)^2(t+1)^2$, $y + t^2(t-1)(t+1)^2$, and $z + t^2(t-1)^2(t+1)$ into $f(x, y, z)$ for x, y and z respectively, simplify and see if the resulting expression has any terms of total degree in x, y and z less than 2. Here's what we get when we do the substitution (with Macaulay 2 doing the actual algebra):

```
-10*x^2*t^15+10*x*y*t^15-5/2*y^2*t^15+10*x*z*t^15-5*y*z*t^15-5/2*z^2*t^15
+10*x^2*t^14-30*x*y*t^14+25/2*y^2*t^14+10*x*z*t^14+5*y*z*t^14-15/2*z^2*t^14
+25*x^2*t^13+5*x*y*t^13-75/4*y^2*t^13-35*x*z*t^13+45/2*y*z*t^13+5/4*z^2*t^13
-30*x^2*t^12+70*x*y*t^12-15/2*y^2*t^12-30*x*z*t^12-25*y*z*t^12+45/2*z^2*t^12
+5*x^3*t^10-35/2*x^2*y*t^10+35/4*x*y^2*t^10-5/8*y^3*t^10-55/2*x^2*z*t^10
+95/2*x*y*z*t^10-115/8*y^2*z*t^10+75/4*x*z^2*t^10-135/8*y*z^2*t^10-25/8*z^3*t^10
-85*x*y*t^11+55*y^2*t^11+35*x*z*t^11-30*y*z*t^11+15*z^2*t^11+20*x^2*y*t^9
-25*x*y^2*t^9+5/2*y^3*t^9-50*x*y*z*t^9+85/2*y^2*z*t^+35*x*z^2*t^9-25/2*y*z^2*t^9
-25/2*z^3*t^9+28*x^2*t^10-21/2*x*y*t^10-217/4*y^2*t^10+29/2*x*z*t^10
+49*y*z*t^10-67/4*z^2*t^10-25*x^3*t^8+95/2*x^2*y*t^8-5/4*x*y^2*t^8-5/8*y^3*t^8
+135/2*x^2*z*t^8-165/2*x*y*z*t^8-135/8*y^2*z*t^8-125/4*x*z^2*t^8
+425/8*y*z^2*t^8-85/8*z^3*t^8-52*x^2*t^9+118*x*y*t^9-89/4*y^2*t^9+6*x*z*t^9
+3/2*y*z*t^9-105/4*z^2*t^9-55*x^2*y*t^7+50*x*y^2*t^7-25/4*y^3*t^7+15*x^2*z*t^7
+90*x*y*z*t^7-225/4*y^2*z*t^7-80*x*z^2*t^7+105/4*y*z^2*t^7+65/4*z^3*t^7-6*x^2*t^8
-81*x*y*t^8+315/4*y^2*t^8+37*x*z*t^8-46*y*z*t^8-51/4*z^2*t^8+5*x^4*t^5
-5*x^3*y*t^5-5/4*x*y^3*t^5+5/16*y^4*t^5-5*x^3*z*t^5-20*x^2*y*z*t^5
+85/4*x*y^2*z*t^5-5/4*y^3*z*t^5-10*x^2*z^2*t^5+185/4*x*y*z^2*t^5
-185/8*y^2*z^2*t^5+15/4*x*z^3*t^5-45/4*y*z^3*t^5+5/16*z^4*t^5
+45*x^3*t^6-85/2*x^2*y*t^6-95/4*x*y^2*t^6+25/8*y^3*t^6-105/2*x^2*z*t^6
+15/2*x*y*z*t^6+615/8*y^2*z*t^6+25/4*x*z^2*t^6-465/8*y*z^2*t^6+225/8*z^3*t^6
+58*x^2*t^7-53*x*y*t^7-137/4*y^2*t^7-29*x*z*t^7+57/2*y*z*t^7+39/4*z^2*t^7
+5*x^3*y*t^4+5/4*x*y^3*t^4-5/8*y^4*t^4-5*x^3*z*t^4+5*x^2*y*z*t^4-115/4*x*y^2*z*t^4
+15/4*y^3*z*t^4+5*x^2*z^2*t^4-5/4*x*y*z^2*t^4+30*y^2*z^2*t^4+35/4*x*z^3*t^4
```

```
-95/4*y*z^3*t^4+5/8*z^4*t^4+52*x^2*y*t^5-51/2*x*y^2*t^5+43/8*y^3*t^5-36*x^2*z*t^5
-24*x*y*z*t^5-153/8*y^2*z*t^5+115/2*x*z^2*t^5-119/8*y*z^2*t^5+37/8*z^3*t^5
-2*x^2*t^6+133/2*x*y*t^6-109/4*y^2*t^6-101/2*x*z*t^6+19*y*z*t^6+89/4*z^2*t^6
-10*x^4*t^3+5*x^3*y*t^3+5/4*x*y^3*t^3-5/16*y^4*t^3+5*x^3*z*t^3+35*x^2*y*z*t^3
-85/4*x*y^2*z*t^3+5/2*y^3*z*t^3+10*x^2*z^2*t^3-165/4*x*y*z^2*t^3+85/8*y^2*z^2*t^3
+5/4*x*z^3*t^3+5/2*y*z^3*t^3-5/16*z^4*t^3-33*x^3*t^4+27/2*x^2*y*t^4+35/2*x*y^2*t^4
-17/8*y^3*t^4+27/2*x^2*z*t^4+31*x*y*z*t^4-327/8*y^2*z*t^4+23/2*x*z^2*t^4
+169/8*y*z^2*t^4-97/8*z^3*t^4-25*x^2*t^5+6*x*y*t^5+24*y^2*t^5+14*x*z*t^5
-25*y*z*t^5+8*z^2*t^5-5*x^3*y*t^2-5/4*x*y^3*t^2+5/8*y^4*t^2+5*x^3*z*t^2
-5*x^2*y*z*t^2+115/4*x*y^2*z*t^2-15/4*y^3*z*t^2-5*x^2*z^2*t^2+5/4*x*y*z^2*t^2
-30*y^2*z^2*t^2-35/4*x*z^3*t^2+95/4*y*z^3*t^2-5/8*z^4*t^2-20*x^2*y*t^3
+1/2*x*y^2*t^3-7/4*y^3*t^3+24*x^2*z*t^3-14*x*y*z*t^3+135/4*y^2*z*t^3
-21/2*x*z^2*t^3-15/4*y*z^2*t^3-33/4*z^3*t^3-17*x*y*t^4-9/4*y^2*t^4
+21*x*z*t^4-y*z*t^4-27/4*z^2*t^4+x^5-1/32*y^5-5*x^3*y*z-5/4*x*y^3*z
+15/32*y^4*z-5/2*x^2*y*z^2+25/2*x*y^2*z^2-15/16*y^3*z^2-5/2*x^2*z^3
+35/4*x*y*z^3-175/16*y^2*z^3+15/32*y*z^4-1/32*z^5+5*x^4*t-15*x^2*y*z*t
-5/4*y^3*z*t-5*x*y*z^2*t+25/2*y^2*z^2*t-5*x*z^3*t+35/4*y*z^3*t+8*x^3*t^2
-x^2*y*t^2-5/4*x*y^2*t^2+1/4*y^3*t^2-x^2*z*t^2-7/2*x*y*z*t^2-19/4*y^2*z*t^2
-21/4*x*z^2*t^2+3/4*y*z^2*t^2-9/4*z^3*t^2+4*x^2*t^3-x*y*t^3-5/4*y^2*t^3
-x*z*t^3+17/2*y*z*t^3-21/4*z^2*t^3+x^3*y+1/8*x*y^3-x^3*z-x^2*y*z-7/8*x*y^2*z
+1/4*y^3*z-x^2*z^2+39/8*x*y*z^2-2*y^2*z^2-1/8*x*z^3-1/4*y*z^3+3*x^2*y*t
+1/8*y^3*t-3*x^2*z*t-2*x*y*z*t-7/8*y^2*z*t-2*x*z^2*t+39/8*y*z^2*t-1/8*z^3*t
+2*x*y*t^2-2*x*z*t^2-y*z*t^2-z^2*t^2-x*y*z-y*z*t
```

As can be seen by a careful inspection (most reliably done using grep, for example), there are no constant terms and no terms which involve only t (i.e., there are no terms of degree 0 in x, y and z) and there are no terms of degree 1 in x and y and z, so for every t the polynomial g is in $(x, y, z)^2$ and hence $f \in P^{(2)}$.

Exercises:

Exercise 10.1. If $f, g \in \mathbb{C}[x_1, x_2]$ are non-constant polynomials with no non-constant common factor and if $\deg(g) = 1$, show $|Z(f, g)| \leq \deg(f)$. [Hint: apply the FTA.] Give a simple example showing that equality can fail.

Solution (with example by Philip Gipson). Since $\deg(g) = 1$, we have $g = ax_1 + bx_2 + c$ and either $a \neq 0$ or $b \neq 0$. Let's say $b \neq 0$. Then $g = 0$ implies $x_2 = -ax_1/b - c$. Plugging this in to f gives a polynomial $h(x_1) = f(x_1, -ax_1/b - c)$ in one variable. If h is identically 0, then $Z(g) \subseteq Z(f)$, hence $f \in \sqrt{(g)}$, but g is irreducible, so $g|f$, contradicting f and g having no non-constant common factor. Thus h is a nonzero polynomial, of degree r say, hence has at most r roots. I.e., there are at most r points of $Z(g)$ at which f also vanishes, so $|Z(f, g)| \leq \deg(f)$.

For an example where $|Z(f, g)| < \deg(f)$, let $g(x_1, x_2) = x_1 - x_2$ (hence $Z(g)$ is the diagonal line through the point $(1, 1)$) and let $f(x_1, x_2) = x_1x_2 - x_1 - x_2 + 1 = (x_1 - 1)(x_2 - 1)$ (hence $Z(f)$ is the union of the horizontal and vertical lines through the point $(1, 1)$). In this case, $Z(f, g) = Z(f) \cap Z(g) = \{(1, 1)\}$ but $\deg(f) = 2$. □

Exercise 10.2. More generally, if $f, g \in \mathbb{C}[x_1, x_2]$ are non-constant polynomials with no non-constant common factor, show there are non-zero polynomials $h_i \in \mathbb{C}[x_i]$ such that $Z(f, g) \subseteq Z(h_1) \cap Z(h_2)$. [Hint: to find h_i, consider the gcd of f and g in $\mathbb{C}(x_i)[x_j]$.] Conclude that $Z(f, g)$ is a finite set. [Note: This is a weak version of Bézout's Theorem. The classical version of Bézout's Theorem says more precisely that $|Z(f, g)| \leq \deg(f)\deg(g)$, with equality if you count the points of $Z(f, g)$ with appropriate multiplicities, including *points at infinity*.]

Solution. We have $f, g \in \mathbb{C}[x_1, x_2] \subseteq \mathbb{C}(x_1)[x_2]$. Let $(f, g) = (h)$ be the ideal generated by f and g in $\mathbb{C}(x_1)[x_2]$. Since non-zero elements $\mathbb{C}[x_1]$ are units in $\mathbb{C}(x_1)$, we may assume that $h \in \mathbb{C}[x_1, x_2]$. In fact, we claim that $h \in \mathbb{C}[x_1]$. To see this, note that $h|f$ and $h|g$ in $\mathbb{C}(x_1)[x_2]$, so there are elements $\phi, \gamma \in \mathbb{C}[x_1]$ such that $h|\phi f$ and $h|\gamma g$ in $\mathbb{C}[x_1, x_2]$. If $h \notin \mathbb{C}[x_1]$, then the prime factorization of h in $\mathbb{C}[x_1, x_2]$ has an irreducible factor e involving x_2, and e divides both ϕf and γg. Since x_2 does not appear in ϕ nor in γ, e does not divide ϕ or γ, hence $e|f$ and $e|g$, contrary to the assumption that f and g have no non-constant common factor. Thus $h \in \mathbb{C}[x_1]$.

Continuing, since $(f, g) = (h)$, we have $h = af + bg$ for some $a, b \in \mathbb{C}(x_1)[x_2]$. Pick some polynomial $d \in \mathbb{C}[x_1]$ such that $da, db \in \mathbb{C}[x_1, x_2]$. (The coefficients of a and b are elements of $\mathbb{C}(x_1)$, so take d to be a common denominator for all of these coefficients.) Let $h_1 = dh$, $A = da$ and $B = db$. Then $dh = daf + dbg$ is $h_1 = Af + Bg$, with $A, B \in \mathbb{C}[x_1, x_2]$ and $h_1 \in \mathbb{C}[x_1]$.

Since f and g are non-constant, h cannot be identically 0, so neither can h_1. Thus h_1, being a non-zero polynomial in $\mathbb{C}[x_1]$, has finitely many roots. But for any point $(p_1, p_2) = p \in Z(f, g)$ we have $h_1(p_1) = A(p)f(p) + B(p)g(p) = 0$, so p_1 is one of these finitely many roots.

Similarly, there is a non-zero polynomial $h_2 \in \mathbb{C}[x_2]$ such that if $(p_1, p_2) = p \in Z(f, g)$, then $h_2(p_2) = 0$. Thus $Z(f, g) \subseteq Z(h_1, h_2) = Z(h_1) \cap Z(h_2)$, but since h_1 is 0 for only finitely many values of x_1 and h_2 is 0 for only finitely many values of x_2, we see $Z(h_1) \cap Z(h_2)$ is finite. □

Exercise 10.3. Show that every prime ideal $P \subset \mathbb{C}[x_1, x_2]$ is either principal or maximal. [Hint: One way to do this is to apply Exercise 10.2.]

Solution 1, by Kat Shultis (with added details). We know from commutative algebra that

$$\dim(R[x_1, \ldots, x_n]) = \dim(R) + n.$$

As $\mathbb{C}$ is a field, it has dimension zero. Thus, in terms of Krull dimension, $\dim(\mathbb{C}[x_1, x_2]) = 2$, meaning that if $P \subset \mathbb{C}[x_1, x_2]$ is a prime ideal but not (0) or maximal, then there is a maximal ideal M such that $(0) \subsetneq P \subsetneq M$ and no other prime ideals fit in this chain. If $0 \neq f \in P$ is an irreducible element (which must exist since $P \neq (0)$ and P is prime), then we have $(0) \subsetneq (f) \subseteq P \subsetneq M$, and hence $(f) = P$ so P is principal. Thus all prime ideals of $\mathbb{C}[x_1, x_2]$ are principal or maximal. □

Solution 2, by Douglas Heltibridle (with added details). First, assume $P \subset \mathbb{C}[x_1, x_2]$ is a prime ideal that is not principal. Pick generators $f_1, \ldots, f_r$ of P. Since P is prime, each f_i has an irreducible factor in P. Let g_i be such a factor for each i. Then $P = (f_1, \ldots, f_r) \subseteq (g_1, \ldots, g_r) \subseteq P$, so $P = (g_1, \ldots, g_r)$. By choosing a subset of the g_i we may assume that $g_1, \ldots, g_r$ is a minimal generating set (i.e, that no proper subset of the g_i generates P). Thus if $i \neq j$ then g_i does not divide g_j. Also, since P is not principal, we know $r > 1$. Let $f = g_1$ and let $g = g_2$. Then both are irreducible and neither divides the other, so in particular f and g have no non-constant common factor.

Thus we can apply Exercise 10.2 so that we have $h_1 \in \mathbb{C}[x_1]$ and $h_2 \in \mathbb{C}[x_2]$ such that $Z(f, g) \subseteq Z(h_1) \cap Z(h_2)$. We have $Z(h_1) \supseteq Z(h_1) \cap Z(h_2)$ and $Z(h_2) \supseteq Z(h_1) \cap Z(h_2)$, and since $f, g \in P$ we have $Z(f, g) \supseteq Z(P)$. Thus $Z(h_1) \supseteq Z(P)$ and $Z(h_2) \supseteq Z(P)$ and by version three of the Nullstellensatz we know $h_1 \in P$ and $h_2 \in P$.

Now, if h_1 is not prime then we can factor it and one of its factors must be in P. Continuing to factor we find an irreducible factor of h_1, which is also in P and $\mathbb{C}[x_1]$. Similarly we find an irreducible factor of h_2 in P and $\mathbb{C}[x_2]$. These are of the form $x_1 - z_1$ and $x_2 - z_2$ for some $z_1, z_2 \in \mathbb{C}$. So we know that $P \supseteq (x_1 - z_1, x_2 - z_2)$. However, $\mathbb{C}[x_1, x_2]/(x_1 - z_1, x_2 - z_2)$ is a field, which means that $(x_1 - z_1, x_2 - z_2)$ is a maximal ideal. Thus $P = (x_1 - z_1, x_2 - z_2)$. Therefore we have that P is maximal as desired. □

Exercise 10.4. Show that P^m for a prime ideal $P \subset \mathbb{C}[x_1, \ldots, x_n]$ is always P-primary if P is either maximal or principal. Conclude that P^m is P-primary for all primes $P \subset \mathbb{C}[x_1, \ldots, x_n]$ and all m if and only if $n \leq 2$.

Solution. If P is maximal, then P^m is P-primary by Exercise 7.3, since $\sqrt{P^m} = P$. Say $P = (f)$. Since P is prime, f cannot be a non-zzero scalar. If $f = 0$, then $P^m = P$ for all $m \geq 1$, hence P^m is P-primary. If f is not a scalar, then f is irreducible. Say $gh \in P^m = (f^m) \subseteq P = (f)$. Thus f^m divides gh. If $g \notin P^m$, then the largest power of f that divides g is f^{m-1}, hence (since $\mathbb{C}[x_1, \ldots, x_n]$ is a UFD) f must divide h, so $h^m \in P^m$; i.e., $h \in P = \sqrt{P^m}$. Thus P^m is P-primary. □

Lecture 11. February 7, 2011

11.1. **The Example continued.** To finish the example from last lecture, we must check that $P \subseteq (x, y, z)^2$. This follows from the fact that no non-zero polynomial with terms of degree less than 2 can vanish on C. For let $u \in P \subset \mathbb{C}[x, y, z]$. Intuitively, if u had a non-zero constant term, then u does not vanish at the origin, but the origin is a point of C, so $u \notin I(C) = P$. If u had any non-zero linear terms, say $u = ax + by + cz +$ higher order terms for $a, b, c \in \mathbb{C}$ not all 0, then the zero locus $Z(u)$ near $(0, 0, 0)$ would look like a plane (the plane in question would be the zero-locus $Z(ax + by + cz)$ of the non-zero linear terms, which is the plane tangent to the surface defined by $u = 0$). But C has branches with tangents in three linearly independent directions, so $u = 0$ could not encompass all of them.

We now show more rigorously that u has no terms of degree less than 2. Since $(0, 0, 0) \in C$ and u vanishes on C, we have $u(0, 0, 0) = 0$ so u has no constant term (or, if you prefer, the constant term is 0). Now consider the image $h(u) = h(u(x, y, z)) = u(h(x), h(y), h(z))$ of u under the homomorphism h corresponding to our parameterization of C. In principle $h(u)$ is a function of t, but since u vanishes on C (or because $u \in P = \ker h$), in fact $u(h(x), h(y), h(z))$ is indentically zero, and hence $du(h(x), h(y), h(z))/dt = 0$. Thus

$$0 = \frac{du(h(x), h(y), h(z))}{dt} = \frac{\partial u}{\partial x}\frac{dh(x)}{dt} + \frac{\partial u}{\partial y}\frac{dh(y)}{dt} + \frac{\partial u}{\partial z}\frac{dh(z)}{dt}.$$

At $t = 0$, explicit computation (using the fact that $h(x) = t(t-1)^2(t+1)^2$, $h(y) = t^2(t-1)(t+1)^2$, and $h(z) = t^2(t-1)^2(t+1)$) shows that $dh(y)/dt = 0$ and $dh(z)/dt = 0$, but $dh(x)/dt = 1$, thus we must have $\partial u/\partial x = 0$ at $(0, 0, 0)$; i.e., there can be no x term. Similar calculations at $t = \pm 1$ show that $\partial u/\partial y$ and $\partial u/\partial z$ vanish at $(0, 0, 0)$, and hence there are no y or z terms, and hence no terms of degree 1. Thus $u \in (x, y, z)^2$.

Remark 11.1.1. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and let $p = (a_1, \ldots, a_n) \in \mathbb{C}^n$. Then

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n} \frac{1}{i_1! \cdots i_n!} \frac{\partial^{i_1 + \ldots + i_n} f}{\partial^{i_1} x_1 \cdots \partial^{i_n} x_n}(p)(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}.$$

This is just a Taylor series expansion for f near the point p. Since f is a polynomial, the expansion is itself a polynomial. The terms of least degree in the $x_i - a_i$ in this expansion give useful information about the behavior of $Z(f)$ near p. For example, if $\frac{\partial f}{\partial x_i}(p) \neq 0$ for some i, then the zero locus of the linear terms define the hyperplane tangent to $Z(f)$ at the point p; i.e., the tangent hyperplane is

$$Z\Big(\sum_i \frac{\partial f}{\partial x_i}(p)(x_i - a_i)\Big). \qquad (\star)$$

For example, if $n = 2$, $p = (0, 0)$ and we take our variables to be x and y with $f = y - x^3 + x$, then from calculus the tangent line to $y = x^3 - x$ at $x = 0$ is $y = -x$, whereas $(\star)$ gives $Z(y + x)$, which is the same thing.

11.2. **Algebraic maps.**

Definition 11.2.1. We say a map $F : \mathbb{C}^n \to \mathbb{C}^m$ is an *algebraic map* if there exist $g_1, \ldots, g_m \in \mathbb{C}[x_1, \ldots, x_n]$ such that for every $(a_1, \ldots, a_n) \in \mathbb{C}^n$ we have

$$F((a_1, \ldots, a_n)) = (g_1(a_1, \ldots, a_n), \ldots, g_m(a_1, \ldots, a_n)).$$

If $C \subseteq \mathbb{C}^n$ and $D \subseteq \mathbb{C}^m$ are algebraic subsets (i.e., Zariski closed subsets), we say a map $f : C \to D$ is an *algebraic map* if there exists an algebraic map $F : \mathbb{C}^n \to \mathbb{C}^m$ such that $f = F|_C$.

Lecture 12. February 9, 2011

Example 12.1. Simple examples of algebraic maps are identity maps $\mathrm{id}_C : C \to C$, where C is an algebraic set, and the inclusion maps $i_C : C \to \mathbb{C}^n$, where C is a Zariski closed subset of $\mathbb{C}^n$. Moreover, if $f : C \to D$ and $h : D \to E$ are algebraic maps, then so is $h \circ f$; i.e., compositions of algebraic maps are algebraic.

Definition 12.2. We say an algebraic map $f : C \to D$ is an *isomorphism* if there exists an algebraic map $g : D \to C$ such that $f \circ g = \mathrm{id}_D$ and $g \circ f = \mathrm{id}_C$, in which case we write $C \cong D$ and say C and D are isomorphic algebraic sets.

Notation 12.3. We refer to $\mathbb{C}^n$ as *affine n-space*, and denote it as $\mathbb{A}^n_{\mathbb{C}}$, or just $\mathbb{A}^n$.

Example 12.4. Let $C = Z(y - x^2) \subset \mathbb{A}^2$, and let $D = \mathbb{A}^1$. Then $C \cong D$. Specifically, define $f : C \to D$ by $f((a, b)) = a$. Note that $(a, b) \in C$ means $b = a^2$. Then f is an algebraic map, and $g : D \to C$, where $g(a) = (a, a^2)$, is an algebraic inverse.

Example 12.5. Let $C = \mathbb{A}^1$, and let $D = Z(y^3 - x^2) \subset \mathbb{A}^2$. Then $f : C \to D$ defined by $a \mapsto (a^3, a^2)$ is algebraic and a bijection, but it turns out that f is not an isomorphism. If it were, there would be a polynomial $g \in \mathbb{C}[x, y]$ such that $a = g(a^3, a^2)$ for all $a \in \mathbb{C}$. But this would mean that $a - g(a^3, a^2) = 0$ for all $a \in \mathbb{C}$, hence $t - g(t^3, t^2) = 0 \in \mathbb{C}[t]$, so $g(t^3, t^2) = t$. But $g(x, y)$ is in the $\mathbb{C}$-vector space span of all monomials $x^i y^j$, hence $g(t^3, t^2)$ is in the span of the monomials t^{3i+2j}; i.e., $g(t^3, t^2)$ is in the $\mathbb{C}$-vector space span of $\{1, t^2, t^3, t^4, \cdots\}$. But $\{1, t, t^2, t^3, t^4, \cdots\}$ is a vector space basis for $\mathbb{C}[t]$ hence t is not in the span of $\{1, t^2, t^3, t^4, \cdots\}$. Thus $g(t^3, t^2) = t$ is impossible and f is not an isomorphism.

Proposition 12.6. *Let $C \subseteq \mathbb{C}^n$ and $D \subseteq \mathbb{C}^m$ be algebraic sets. An algebraic map $f : C \to D$ is continuous in both the standard and the Zariski topologies.*

Proof. Let $F : \mathbb{C}^n \to \mathbb{C}^m$ be an algebraic map such that $F|_C = f$. Since polynomials are continuous in the standard topology, an algebraic map $F : \mathbb{C}^n \to \mathbb{C}^m$ is continuous in the standard topology, hence so is f, since $f = F|_C$, and C has the subspace topology. Similarly, to show f is continuous in the Zariski topology, it suffices to show that F is. Now, $F = (f_1, \ldots, f_m)$ for polynomials $f_i \in \mathbb{C}[x_1, \ldots, x_n]$. Each closed subset of $\mathbb{C}^m$ is of the form $\cap_j Z(g_j)$ for some family of polynomials $g_j \in \mathbb{C}[y_1, \ldots, y_m]$, and $F^{-1}(\cap_j Z(g_j)) = \cap_j F^{-1}(Z(g_j))$, so it's enough to show that $F^{-1}(Z(g_j))$ is closed. But $F^{-1}(Z(g_j)) = F^{-1}(g_j^{-1}(0)) = (g_j F)^{-1}(0) = Z(g_j \circ F)$ is closed, since $g_j \circ F = g_j(f_1, \ldots, f_m) \in \mathbb{C}[x_1, \ldots, x_n]$. $\square$

Remark 12.7. Since algebraic maps are continuous in both the standard and the Zariski topologies, isomorphic algebraic sets are homeomorphic in both topologies.

We now associate a ring, called the affine coordinate ring, to each algebraic set.

Definition 12.8. Let $V \subseteq \mathbb{A}^n$ be an algebraic set. The *affine coordinate ring* (or simply the coordinate ring) of $\mathbb{A}^n$ is $\mathbb{C}[x_1, \ldots, x_n]$, denoted $\mathbb{C}[\mathbb{A}^n]$. The affine coordinate ring $\mathbb{C}[V]$ of V is $\mathbb{C}[\mathbb{A}^n]/I(V)$. Note that V comes with a canonical quotient homomorphism, $\overline{} : \mathbb{C}[\mathbb{A}^n] \to \mathbb{C}[V]$. This homomorphism is actually given by restriction; i.e., $f \mapsto \overline{f} = f|_V$.

Exercises:

Exercise 12.1. Let C be $Z(xy - 1)$ in $\mathbb{A}^2$. Show that C and $\mathbb{A}^1$ are homeomorphic in the Zariski topology but not in the usual topology. [Hint: use algebraic topology.] Conclude that C and $\mathbb{A}^1$ are not isomorphic algebraic sets.

Solution. First note that $xy-1$ is irreducible. To see this, suppose $gh = xy-1$. Note that $\deg(gh) = \deg(g) + \deg(h)$. Thus if neither g nor h is invertible, then $\deg(g) = \deg(h) = 1$, which implies that $Z(xy-1)$ is either a line or a union of two lines. But any line intersects either the horizontal or vertical coordinate axis, while $xy-1=0$ has no solution where either $x=0$ or $y=0$. Thus $xy-1$ must be irreducible. Since $xy-1$ is irreducible, $(xy-1)$ is prime so $I(Z(xy-1)) = (xy-1)$.

Now let D be a non-empty proper closed subset of C. Then there is a polynomial $f \in I(D)$ which does not vanish on all of C. Thus $f \notin (xy-1)$, so f and $xy-1$ have no common factor. By Exercise 10.2, $Z(f, xy-1)$ is a finite set, but $D \subseteq Z(f, xy-1)$ so D is finite. Thus C has the finite complement topology. Since C and $\mathbb{A}^1$ have the same cardinality there is a bijection, and since for both the Zariski topology is the finite complement topology, any bijection is a homeomorphism (and in fact it's not hard to write down an explicit bijection).

However, $C = Z(xy-1)$ is homeomorphic in the standard topology to $\mathbb{A}^1 \setminus \{\text{origin}\}$, and thus C is not simply connected. Since $\mathbb{A}^1$ is simply connected (contractible even), C and $\mathbb{A}^1$ are not homeomorphic. In particular, there do not exist inverse algebraic maps f and g between C and $\mathbb{A}^1$, so C and $\mathbb{A}^1$ are not isomorphic algebraic sets. $\square$

Lecture 13. February 11, 2011

Given an algebraic subset $V \subseteq \mathbb{A}^n$, the coordinate ring $\mathbb{C}[V]$ on V is the set of restrictions of polynomials on $\mathbb{A}^n$. Among these are the constant functions, and thus we have a canonical inclusion $i_V : \mathbb{C} \subset \mathbb{C}[V]$. We say that $\mathbb{C}[V]$ is a $\mathbb{C}$-algebra.

If $W \subseteq \mathbb{A}^m$ is an algebraic subset, and if $h : \mathbb{C}[W] \to \mathbb{C}[V]$ is a ring homomorphism, we say h is a $\mathbb{C}$-homomorphism if $h \circ i_W = i_V$. In particular, the canonical quotient homomorphism $\overline{} : \mathbb{C}[\mathbb{A}^n] \to \mathbb{C}[V]$ is a $\mathbb{C}$-homomorphism, since $\overline{}(g) = g|_V$ is just restriction, and constants restrict to constants.

Construction I. Given algebraic subsets $C \subseteq \mathbb{A}^n$ and $D \subseteq \mathbb{A}^m$ and an algebraic map $f : C \to D$, we construct a $\mathbb{C}$-homomorphism $f^* : \mathbb{C}[D] \to \mathbb{C}[C]$ and we show that if $\phi : C \to D$ is an algebraic map with $\phi^* = f^*$, then $\phi = f$.

First we define f^* in case $C = \mathbb{A}^n$ and $D = \mathbb{A}^m$. In that case for each $g \in \mathbb{C}[\mathbb{A}^m]$ we define $f^*(g) = g \circ f$. Since $f = (f_1, \ldots, f_m)$ for $f_i \in \mathbb{C}[\mathbb{A}^n]$ and $g = g(y_1, \ldots, y_m)$, where we assume that $\mathbb{C}[\mathbb{A}^m] = \mathbb{C}[y_1, \ldots, y_m]$ is a polynomial ring in the variables y_i, we have $f^*(g) = g \circ f = g(f_1, \ldots, f_m) \in \mathbb{C}[\mathbb{A}^n]$. Moreover, for any $g_i \in \mathbb{C}[\mathbb{A}^m]$, $f^*(g_1 + g_2) = (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f = f^*(g_1) + f^*(g_2)$ and likewise $f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$, and clearly f^* is the identity on constants, so f^* is a $\mathbb{C}$-homomorphism.

Now consider the general case. Then $f = F|_C$ for some algebraic mapping $F = (f_1, \ldots, f_m) : \mathbb{A}^n \to \mathbb{A}^m$. Let $\gamma \in \mathbb{C}[D]$ and pick $g \in \mathbb{C}[\mathbb{A}^m]$ such that $\gamma = \overline{g}$. We define $f^*(\overline{g}) = \overline{F *^{(} g)}$. Note that $\overline{F *^{(} g)} = g \circ F|_C \in \mathbb{C}[C]$. Also note that $\overline{F *^{(} g)} = f^*(\overline{g})$: $\overline{F *^{(} g)} = g \circ F|_C$ is equal to $g|_D \circ F|_C = \overline{g} \circ f = f^*(\overline{g})$ since $F(C) \subseteq D$. In particular, f^* is well-defined, since $f^*(\gamma) = \overline{\gamma} \circ f$ is independent of the choice of g. As before f^* is a $\mathbb{C}$-homomorphism.

Finally, consider an algebraic map $\phi : C \to D$ with $\phi^* = f^*$, but suppose $\phi \neq f$. Since $\phi \neq f$, there is a $c \in C$ such that $f(c) \neq \phi(c)$, and hence the coordinates of the points $f(c)$ and $\phi(c)$ are not all the same. Say they differ in the ith coordinate. Then $y_i(f(c)) \neq y_i(\phi(c))$, and hence $f^*(\overline{y_i}) \neq \phi^*(\overline{y_i})$, so $\phi^* \neq f^*$, contradicting our hypothesis.

In the next lecture, given a $\mathbb{C}$-homomorphism $h : \mathbb{C}[D] \to \mathbb{C}[C]$, we will construct an algebraic map $f : C \to D$ such that $f^* = h$.

Lecture 14. February 14, 2011

Construction II. Given algebraic subsets $C \subseteq \mathbb{A}^n$ and $D \subseteq \mathbb{A}^m$ and a $\mathbb{C}$-homomorphism $h : \mathbb{C}[D] \to \mathbb{C}[C]$, we find an algebraic map $f : C \to D$ such that $h = f^*$.

We have the canonical quotients $\overline{}: \mathbb{C}[\mathbb{A}^n] \to \mathbb{C}[C]$ and $\overline{}: \mathbb{C}[\mathbb{A}^m] \to \mathbb{C}[D]$. Suppose $\mathbb{C}[\mathbb{A}^m]$ is a polynomial ring $\mathbb{C}[y_1, \ldots, y_m]$ in variables y and $\mathbb{C}[\mathbb{A}^n]$ is a polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ in variables x. Let $\phi_i = h(\overline{y_i})$ and choose elements $f_i \in \mathbb{C}[\mathbb{A}^n]$ such that $\overline{f_i} = \phi_i$ for $i = 1, \ldots, m$. Let $H : \mathbb{C}[\mathbb{A}^m] \to \mathbb{C}[\mathbb{A}^n]$ be the unique $\mathbb{C}$-homomorphism such that $H(y_i) = f_i$ for $i = 1, \ldots, m$. Then we have $\overline{H(g)} = h(\overline{g})$ for all $g \in \mathbb{C}[\mathbb{A}^m]$. Now $F = (f_1, \ldots, f_m)$ defines an algebraic map $F : \mathbb{A}^n \to \mathbb{A}^m$, and clearly $H = F^*$.

First we claim that $F(C) \subseteq D$. To see this it's enough to check that $g(F(c)) = 0$ for all $c \in C$ and all $g \in I(D)$. Note that $\overline{g} = 0$ since $g \in I(D)$. Thus

$$g(F(c)) = (F^*(g))(c) = (H(g))(c) = (H(g))|_C(c) = \overline{H(g)}(c) = (h(\overline{g}))(c) = (h(0))(c) = 0$$

for all $c \in C$ and all $g \in I(D)$. Since as we now see $F(C) \subseteq D$, F restricts to an algebraic map $f = F|_C : C \to D$. Moreover, for any $\gamma \in \mathbb{C}[D]$ there is a $g \in \mathbb{C}[\mathbb{A}^m]$ with $\overline{g} = \gamma$ and we have $f^*(\overline{g}) = g|_D \circ F|_C = g \circ F|_C = \overline{H(g)} = h(\overline{g})$ so $f^* = h$, as we wanted.

We thus have the following theorem:

Theorem 14.1. *The $*$-operation $f \mapsto f^*$ gives a bijective correspondence from algebraic maps of algebraic sets to $\mathbb{C}$-homomorphisms of their coordinate rings.*

Proof. The mapping $f \mapsto f^*$ is injective by Construction I and it's surjective by Construction II. □

Corollary 14.2. *A mapping $f : C \to D$ of algebraic sets is an isomorphism if and only if $f^* : \mathbb{C}[D] \to \mathbb{C}[C]$ is an isomorphism.*

Proof. Suppose f is an isomorphism. Then there is a mapping $g : D \to C$ such that $g \circ f = \mathrm{id}_C$ and $f \circ g = \mathrm{id}_D$. Thus $f^* \circ g^* = (g \circ f)^* = (\mathrm{id}_C)^* = \mathrm{id}_{\mathbb{C}[C]}$ and similarly $g^* \circ f^* = \mathrm{id}_{\mathbb{C}[D]}$, so f^* is an isomorphism with inverse g^*.

Conversely, suppose f^* is an isomorphism and let h be its inverse. Then there is a mapping $g : D \to C$ with $h = g^*$, and we have $(g \circ f)^* = f^* \circ g^* = \mathrm{id}_{\mathbb{C}[C]} = (\mathrm{id}_C)^*$, hence $g \circ f = \mathrm{id}_C$ and similarly $f \circ g = \mathrm{id}_D$. Thus f is an isomorphism with inverse g. □

Example 14.3. Exercise 12.1 asks you to give a topological explanation for why $C = Z(xy - 1)$ in $\mathbb{A}^2$ is not isomorphic to $D = \mathbb{A}^1$. We can use Corollary 14.2 to give an algebraic reason. If $f : D \to C$ were an isomorphism, then $f^* : \mathbb{C}[C] \to \mathbb{C}[D]$ would be an isomorphism too. But $\mathbb{C}[C] = \mathbb{C}[x, y]/(xy-1) \cong \mathbb{C}[x, \frac{1}{x}]$ and $\mathbb{C}[D] = \mathbb{C}[t]$. Let $h : \mathbb{C}[x, \frac{1}{x}] \to \mathbb{C}[t]$ be any $\mathbb{C}$-homomorphism. Then since $h(x)$ has inverse $h(\frac{1}{x})$, but the only invertible elements of $\mathbb{C}[t]$ are non-zero constants, then $h(x) \in \mathbb{C}$, hence $\mathrm{Im}(\mathbb{C}[C]) = \mathbb{C}$, so h is not an isomorphism. Since $\mathbb{C}[C]$ and $\mathbb{C}[D]$ are not isomorphic, neither are C and D.

Exercises:

Exercise 14.1. Show that every algebraic mapping $f : \mathbb{A}^1 \to \mathbb{A}^n$ is closed (i.e., that the image of each Zariski-closed subset is closed).

Solution by Jason Hardin. Write $f = (f_1, \ldots, f_n)$. Let $C \subseteq \mathbb{A}^1$ be a closed subset. If $C = \emptyset$, then $f(C) = \emptyset$ is closed. If $C = \mathbb{A}^1$, then Ex 9.1 shows that $f(C)$ is closed.

If $C \neq \emptyset, \mathbb{A}^1$, then by Ex 2.3 we know $C = \{c_1, \ldots, c_m\}$. For $i = 1, \ldots, m$, define ideals $I_i \subset \mathbb{C}[y_1, \ldots, y_n]$ by $I_i := (y_1 - f_1(c_i), \ldots, y_n - f_n(c_i))$. Note that $Z(I_i) = (f_1(c_i), \ldots, f_n(c_i)) = f(c_i)$. Thus, $f(C) = \bigcup_{i=1}^m f(c_i) = \bigcup_{i=1}^m Z(I_i) = Z\left(\bigcap_{i=1}^m I_i\right)$ is closed. □

Exercise 14.2. For some m and n, give an example of an algebraic mapping $f : \mathbb{A}^n \to \mathbb{A}^m$ which is surjective but not closed.

Solution by Becky Egg. Consider $f : \mathbb{A}^2 \to \mathbb{A}^1$ defined by $f(a_1, a_2) = a_1$. So f is clearly surjective. To see that f is not closed, consider $V = Z(xy - 1) \subseteq \mathbb{A}^2$. Note that V is closed in $\mathbb{A}^2$, with $V = \{(x, 1/x) | x \neq 0\}$. So $f(V) = \mathbb{A}^1 \backslash \{0\}$. Note $f(V) = \mathbb{A}^1 \backslash Z(1)$, so $f(V)$ is open in $\mathbb{A}^1 = \mathbb{C}$. Since $\mathbb{C}$ is connected, the only subsets of it which are both open and closed are $\mathbb{C}$ and $\emptyset$. So $f(V)$ is not closed, and hence f is not a closed map. □

Exercise 14.3. Let $f : C \to D$ be an algebraic mapping of algebraic sets. If C is irreducible, show that the Zariski closure of $f(C)$ is irreducible.

Solution by Zheng Yang (with added details). By Exercise 6.2, it suffices to show $I(Z(I(f(C)))$ is a prime ideal. We justify and then use the fact for any subset $B \subset C$ that $I(f(B)) = (f^*)^{-1}(I(B))$. (Note $g \in I(f(B))$ if and only if g vanishes on $f(B)$ if and only if $f^*(g) = g \circ f$ vanishes on B if and only if $f^*(g) \in I(B)$ if and only if $g \in (f^*)^{-1}(I(B))$.) But $I(C)$ is prime by Exercise 6.2, and contraction of a prime ideal is prime under f^* so $I(f(C)) = (f^*)^{-1}(I(C))$ is prime. But $I(f(C)) = I(Z(I(f(C)))$ by the Nullstellensatz (Theorem 5.1.3) and $Z(I(f(C))) = \overline{f(C)}$ by Exercise 2.9. And by Exercise 6.2 again $I(f(C)) = I(\overline{f(C)})$ is prime. □

Exercise 14.4. For each $n \geq 1$, show that an algebraic mapping $f : \mathbb{A}^n \to \mathbb{A}^1$ is either surjective or constant (i.e, has image a single point).

Solution by Nora Youngs. Let $f : \mathbb{A}^n \to \mathbb{A}^1$ be an algebraic mapping. Then, by definition, there is some $g_1 \in \mathbb{C}[x_1, ..., x_n]$ such that for every $(a_1, ..., a_n) \in \mathbb{A}^n$ we have $f(a_1, ..., a_n) = g(a_1, ..., a_n)$.

If g_1 is a constant polynomial, then f is constant.

If g_1 is not a constant polynomial: Let $c \in \mathbb{C}$ be given. To show that f is surjective, we need to show that $g_1(x_1, ..., x_n) = c$ has a solution. Equivalently, we must show $g_1 - c = 0$ has a solution.

Let $I = (g_1 - c)$. Note $g_1 - c$ is not constant, so I is a proper ideal of $\mathbb{C}[x_1, ..., x_n]$. Thus, by Version 1 of the Nullstellensatz, $g_1 - c$ has a zero.

Thus, there is a solution to $g_1 - c = 0$; hence, f is surjective. □

Exercise 14.5. For some m and n, give an example of an algebraic mapping $f : \mathbb{A}^n \to \mathbb{A}^m$ that is neither surjective nor constant.

Solution by Philip Gipson. Consider the embedding $f : \mathbb{C} \to \mathbb{C}^2$ via $f(x) = (x, 0)$. This is certainly algebraic but neither constant nor surjective. □

Exercise 14.6. Let $F : \mathbb{A}^{n+m} \to \mathbb{A}^m$ be the projection mapping $(a_1, \ldots, a_n, b_1, \ldots, b_m) \mapsto (b_1, \ldots, b_m)$. It is well known that F is an open mapping in the standard topology (i.e., that the image of an open subset is open). Show that F is an open algebraic mapping for the Zariski topology.

Solution by Katie Morrison. It is that clear that F is algebraic since it is given by the collection of polynomials $f(x_1, \ldots, x_{n+m}) = (x_{n+1}, \ldots, x_{n+m})$. To see F is open, let $A \subseteq \mathbb{A}^{n+m}$ be an open set, then there exists some polynomials $g_i \subseteq \mathbb{C}[x_1, \ldots, x_{n+m}]$, $i \in I$, such that $\mathbb{A}^{n+m} \setminus A = \cap_{i \in I} Z(g_i)$ or equivalently, $A = \cup_{i \in I}(\mathbb{A}^{n+m} \setminus Z(g_i))$. Since $F\left(\cup_{i \in I}(\mathbb{A}^{n+m} \setminus Z(g_i))\right) = \cup_{i \in I} F(\mathbb{A}^{n+m} \setminus Z(g_i))$ and the union of open sets is open, it suffices to show that each $F(\mathbb{A}^{n+m} \setminus Z(g_i))$ is open, and so we restrict to $A = \mathbb{A}^{n+m} \setminus Z(g)$ for some $g \in \mathbb{C}[x_1, \ldots, x_{n+m}]$. Then

$$A = \{(a_1, \ldots, a_{n+m}) \ : \ g(a_1, \ldots, a_{n+m}) \neq 0\},$$

and so

$$F(A) = \{(a_{n+1}, \ldots, a_{n+m}) \mid \exists\ a_1, \ldots, a_n \text{ s.t. } g(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+m}) \neq 0\}.$$

Let $i_{(b_1, \ldots, b_n)} : \mathbb{A}^m \to \mathbb{A}^{n+m}$ denote the inclusion map where $(c_1, \ldots, c_m) \mapsto (b_1, \ldots, b_n, c_1, \ldots, c_m)$. Then we see

$$\begin{aligned} \mathbb{A}^m \setminus F(A) &= \{(b_{n+1}, \ldots, b_{n+m}) \ : \ \forall\ b_1, \ldots, b_n,\ g(b_1, \ldots, b_n, b_{n+1}, \ldots, b_{n+m}) = 0\} \\ &= \cap_{(b_1, \ldots b_n) \in \mathbb{C}^n} Z(g \circ i_{(b_1, \ldots b_n)}), \end{aligned}$$

which is a closed set since it is the intersection of closed sets. Thus we have that $F(A)$ is open, and so F is an open map. □ □

Exercise 14.7. Consider the standard topology on the closed interval $X = [-1, 1]$. Give an example of continuous maps $f, g : X \to X$ such that $f \circ g = \mathrm{id}_X$ but such that $g \circ f \neq \mathrm{id}_X$. Conclude that g is not a homeomorphism.

Solution by Nora Youngs. Let $f = \sin(\pi x)$ and $g = \frac{\arcsin(x)}{\pi}$. [Note that arcsin has been scaled to have image points only in the interval $[-1, 1]$.

Then, for any $x \in [-1, 1]$

$$(f \circ g)(x) = \sin\left(\pi \frac{\arcsin(x)}{\pi}\right) = \sin(\arcsin(x)) = x$$

by definition of arcsin.

However, $g \circ f$ is not the identity: Consider $x = 1$.

Then

$$(g \circ f)(1) = \frac{\arcsin(\sin(\pi \cdot 1))}{\pi} = \frac{\arcsin(0)}{\pi} = 0,$$

so $g \circ f$ is not the identity for $x = 1$. □

Exercise 14.8. Let $f, g : \mathbb{A}^n \to \mathbb{A}^n$ be algebraic maps such that $f \circ g = \mathrm{id}_{\mathbb{A}^n}$. Show that $g \circ f = \mathrm{id}_{\mathbb{A}^n}$ and hence that g is an isomorphism. [Hint: Look up and apply Ax's Theorem, sometimes also called the Ax-Grothendieck theorem.]

Solution by Ashley Weatherwax. We'll begin by showing that g is bijective. Let $c, d \in \mathbb{A}^n$ such that $g(c) = g(d)$. Then $f \circ g(c) = f \circ g(d)$. However, as we assumed that $f \circ g = id_{\mathbb{A}^n}$, we get immediately that $c = d$, and thus g is injective. Then, by the Ax-Grothendieck theorem, g is, in fact, bijective.

Now, let $c \in \mathbb{A}^n$ and consider $g \circ f(c)$. As g is bijective, there exists and $a \in \mathbb{A}^n$ such that $g(a) = c$. Then

$$g \circ f(c) = g \circ f(g(a)) = g(a) = c$$

as $f \circ g = id_{\mathbb{A}^n}$. Therefore $g \circ f = id_{\mathbb{A}^n}$ and g is an isomorphism. □

Lecture 15. February 16, 2011

MaxSpec.

Lemma 15.1. *Let $V \subset \mathbb{A}^n$ be an algebraic set. Then the following are equivalent:*

(a) *specifying a point $v \in V$;*
(b) *specifying a $\mathbb{C}$-homomorphism $\mathbb{C}[V] \to \mathbb{C}$; and*
(c) *specifying a maximal ideal $M \subset \mathbb{C}[V]$.*

Proof. (a) implies (b): Having $v \in V$ is the same as $\{v\} \subseteq V$, which we know induces a $\mathbb{C}$-homomorphism $\mathbb{C}[V] \to \mathbb{C}[v] = \mathbb{C}$.

(b) implies (c): Given a $\mathbb{C}$-homomorphism $h : \mathbb{C}[V] \to \mathbb{C}$, let $M = \ker(h)$. Since h is surjective and $\mathbb{C}$ is a field, M is a maximal ideal.

(c) implies (a): Given a maximal ideal $M \subset \mathbb{C}[V]$, consider

$$\mathbb{C}[\mathbb{A}^n] \xrightarrow{q_1} \mathbb{C}[V] \xrightarrow{q_2} \mathbb{C}[V]/M = \mathbb{C}.$$

Since $q_2 \circ q_1$ is surjective with image a field, $N = \ker(q_2 \circ q_1)$ is a maximal ideal of $\mathbb{C}[\mathbb{A}^n]$, hence $N = I(v)$ for some point $v \in \mathbb{A}^n$, by Theorem 4.1, version 2 of the Nullstellensatz. Since clearly $I(V) \subseteq N = I(v)$, we see that $v \in V$. □

Remark 15.2. By Lemma 15.1, we see that the maximal ideals of $\mathbb{C}[V]$ are exactly the ideal of the form $I(v)/I(V)$ for points $v \in V$. We will denote $I(v)/I(V)$ by $I_V(v)$.

Corollary 15.3. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be algebraic sets. Let $h : \mathbb{C}[W] \to \mathbb{C}[V]$ be a $\mathbb{C}$-homomorphism. Then $h^{-1}(M)$ is a maximal ideal for every maximal ideal $M \subset \mathbb{C}[V]$.*

Proof. Note that

$$\mathbb{C}[W] \xrightarrow{h} \mathbb{C}[V] \xrightarrow{q_2} \mathbb{C}[V]/M = \mathbb{C}$$

is a surjection to a field, so has kernel a maximal ideal $N = h^{-1}(M)$. □

Example 15.4. If $h : R \to S$ is a homomorphism of rings, it is not in general true that the inverse image of a maximal ideal is maximal. For example, let $h : \mathbb{Z} \to \mathbb{Q}$ be inclusion of the integers in the rationals. Then $(0) \subset \mathbb{Q}$ is maximal, and $h^{-1}((0)) = ((0))$, but $(0) \subset \mathbb{Z}$ is not maximal.

Remark 15.5. If $f : V \to W$ is the algebraic map corresponding to the homomorphism h in Corollary 15.3, if $v \in V$ is the point with $I_V(v) = M$ and if $w \in W$ is the point with $I_W(w) = h^{-1}(M)$, then $w = f(v)$ and $(f^*)^{-1}(I_V(v)) = I_W(f(v))$. See Exercise 15.1.

Definition 15.6. Let R be a commutative ring with $1 \neq 0$. Then $\mathrm{MaxSpec}\,(R)$ is defined to be the topological space whose point set is the set of maximal ideals of R, and where the closed sets are the subsets $C \subseteq \mathrm{MaxSpec}\,(R)$ of the form $C = C_J$ for some ideal $J \subseteq R$, where $C_J = \{M \in \mathrm{MaxSpec}\,(R) : J \subseteq M\}$. This topology is, as you might guess, called the Zariski topology.

Exercises:

Exercise 15.1. Let $f : V \to W$ be an algebraic map of algebraic sets. Let $v \in V$. Show that $(f^*)^{-1}(I_V(v)) = I_W(f(v))$.

Solution by Becky Egg. Let $V \subseteq \mathbb{C}[x_1, \ldots, x_n]$ and $W \subseteq \mathbb{C}[y_1, \ldots, y_m]$ be algebraic sets, and $f : V \to W$ an algebraic map. Let $\overline{h} = h + I(W) \in I_W(f(v))$. So $h \in \mathbb{C}[y_1, \ldots, y_m]$, with $h(f(v)) = 0$. Then

$$[f^*(h)](v) = h(f(v)) = 0,$$

so $h \circ f = f^*(h) \in I(v)$, and hence $\overline{f^*h} \in I_V(v)$. So $\overline{h} \in (f^*)^{-1}(I_V(v))$.
Now let $\overline{g} = g + I(W) \in (f^*)^{-1}(I_V(v))$. So $g \in \mathbb{C}[y_1, \ldots, y_m]$, and $f^*(g) = g \circ f \in I(v)$. So $g(f(v)) = 0$ implies that $g \in I(f(v))$, and hence $\overline{g} \in I_W(f(v))$. Thus we have $(f*)^{-1}(I_V(v)) = I_W(f(v))$.

□

Exercise 15.2. Show that the sets of the form C_J as given in Definition 15.6 do indeed comprise the closed sets of a topology.

Solution 1, by Douglas Heltibridle. Recall that in Definition 15.1.6 we have $C_J = \{M \in \mathrm{MaxSpec}(R) : J \subseteq M\}$ where J is an ideal in R. As $(0) \subseteq M$ for all $M \in \mathrm{MaxSpec}(R)$ we have that $C_{(0)} = \mathrm{MaxSpec}(R)$, and as $R \not\subseteq M$ for any $M \in \mathrm{MaxSpec}(R)$ we have $C_R = \emptyset$.

Now let C_J and C_I be closed sets. Since $J \cap I \subseteq J$ and $J \cap I \subseteq I$ we have $I \subseteq M$ and $J \subseteq M$ both imply $J \cap I \subseteq M$. Thus $C_{I \cap J} \supseteq C_J \cup C_I$. Now, let $M \in C_{J \cap I}$, and suppose that $I \not\subseteq M$ and $J \not\subseteq M$, then there exists $i \in I$ such that $i \notin M$ and $j \in J$ such that $j \notin M$. However, as I and J are ideals $ij \in I \cap J$. Since M is prime, $ij \notin M$ and thus $M \not\supseteq I \cap J$. Thus we have a contradiction and so either $M \supseteq I$ or $M \supseteq J$, which means $M \in C_J \cup C_I$. Therefore $C_{J \cap I} \subseteq C_J \cup C_I$ and we have equality. Thus the union of the arbitrary closed sets C_I and C_J is itself a closed set.

Next, let $\{C_I\}_{I \in \mathcal{I}}$ be a family of closed sets with $\mathcal{I}$ the set of ideals in R. First, $M \in \cap_{\mathcal{I}} C_I$ if and only if $M \in C_J$ for each $J \in \mathcal{I}$. Then, $M \in C_J$ for each $J \in \mathcal{I}$ if and only if $J \subseteq M$ for all $J \in \mathcal{I}$. Finally $J \subseteq M$ for all $J \in \mathcal{I}$ if and only if $\cup_{\mathcal{I}} J \subseteq M$. Therefore $M \in C_{\cap_{\mathcal{I}} C_I}$ if and only

if $M \in \cap_{\mathcal{I}} C_I$, which means $\cap_{\mathcal{I}} C_I = C_{\cap_{\mathcal{I}} C_I}$. Thus arbitrary intersections of closed sets are closed, and so we have that the closed sets of the form C_J give a topology for MaxSpec(R). □

Solution 2, by Kat Shultis. Let $C_J := \{M \in \text{MaxSpec}(R) | J \subseteq M\}$ be sets in MaxSpec(R) which are defined for any ideal J of R. Then $C_R = \emptyset$ and $C_{(0)} = \text{MaxSpec}(R)$. Thus we have the emptyset and the whole set in the collection of C_J. Let I, J be ideals in R. Then as $M \in \text{MaxSpec}(R)$ are all prime, we know that $IJ \subseteq M$ if and only if $I \subseteq M$ or $J \subseteq M$. Hence $C_I \cup C_J = C_{IJ}$ so that the collection of C_J is closed under finite intersections. Next, let $\{I_\alpha\}_{\alpha \in A}$ be an arbitrary collection of ideals in R. Then, $J = \bigoplus_{\alpha \in A} I_\alpha$ is an ideal of R. Also, $M \in C_J$ if and only if $\bigoplus_{\alpha \in A} I_\alpha = J \subseteq M$, which is true if and only if $I_\alpha \subseteq M$ for all $\alpha \in A$. Hence $C_J = \bigcap_{\alpha \in A} C_{I_\alpha}$, and our collection of C_J is closed under arbitrary intersections. Hence, the collection of C_J define the closed sets of a topology on MaxSpec(R). □

Exercise 15.3. Let $V \subseteq \mathbb{A}^n$ be an algebraic set. Define a map $h_V : V \to \text{MaxSpec}\,(\mathbb{C}[V])$ by $h_V : v \mapsto I_V(v)$. Show that h_V is a homeomorphism in the Zariski topologies.

Solution by Philip Gipson. We already know from Lemma 15.1 that this correspondence is bijective, so all that remains to be shown is that it is Zariski-continuous. To that end consider a closed set $C_J \subseteq \text{MaxSpec}(\mathbb{C}[V])$. We know that $C_J = \{M : J \subseteq M\}$ for some ideal $J \subseteq \mathbb{C}[V]$. Since each maximal ideal M is uniquely expressible as $M = I_V(v_M)$ for some $v_M \in V$ we have that

$$C_J = \{M : J \subseteq M\} = \{I_V(v_M) : J \subseteq I_V(v_M)\} = \{I_V(v_M) : v_M \in Z(J)\}$$

and therefore

$$h_V^{-1}(C_J) = \{h_V^{-1}(I_V(v_M)) : v_M \in Z(J)\} = \{v_M : v_M \in Z(J)\} = Z(J).$$

Since h_V is bijective, we also have $h_V(Z(J)) = C_J$. Thus both h_V and h_V^{-1} are continuous and so h_V is a homeomorphism. □

Lecture 16. February 18, 2011

16.1. **More on MaxSpec.** Let V and W be algebraic sets, and let $f : \text{MaxSpec}\,(\mathbb{C}[V]) \to \text{MaxSpec}\,(\mathbb{C}[W])$ be any map. Then $\widetilde{f} = h_W^{-1} \circ f \circ h_V$ (where h_V is as defined in Exercise 15.3) is a map $\widetilde{f} : V \to W$ such that $f(I_V(v)) = I_W(\widetilde{f}(v))$.

Definition 16.1.1. Let V and W be algebraic sets, and let $f : \text{MaxSpec}\,(\mathbb{C}[V]) \to \text{MaxSpec}\,(\mathbb{C}[W])$ be a map. We say f is *algebraic* if there is a $\mathbb{C}$-homomorphism $\phi : \mathbb{C}[W] \to \mathbb{C}[V]$ such that $f(I_V(v)) = \phi^{-1}(I_V(v))$ for all $v \in V$.

By Exercise 16.2, the algebraic maps $V \to W$ correspond bijectively via h_V and h_W to the algebraic maps MaxSpec $(\mathbb{C}[V]) \to$ MaxSpec $(\mathbb{C}[W])$. Thus we can in some sense regard an algebraic set V as being the same thing as MaxSpec$(\mathbb{C}[V])$. But the elements of $\mathbb{C}[V]$ can be regarded as being functions on V. We might ask in what sense do they give functions on MaxSpec$(\mathbb{C}[V])$.

If $f \in \mathbb{C}[V]$, then $f : V \to \mathbb{C}$ is algebraic, hence corresponds to the $\mathbb{C}$-homomorphism $f^* : \mathbb{C}[t] = \mathbb{C}[\mathbb{C}] to \mathbb{C}[V]$ defined by $t \mapsto f$. Similarly, $f \in \mathbb{C}[V]$ corresponds to the algebraic map $\widetilde{f} : \text{MaxSpec}(\mathbb{C}[V]) \to \text{MaxSpec}(\mathbb{C}[\mathbb{C}]) = \mathbb{C}$. There are several ways to think about $\widetilde{f}$. Given $v \in V$, then $\widetilde{f}(I_V(v)) = I_{\mathbb{C}}(f(v)) \subset \mathbb{C}[\mathbb{C}]$, or $\widetilde{f}(I_V(v)) = f + I_V(v) \in \mathbb{C}[V]/I_V(v)$, or $\widetilde{f}(I_V(v)) = (f^*)^{-1}(I_V(v)) = (t - f(v)) \subset \mathbb{C}[\mathbb{C}]$.

The advantage of MaxSpec is that MaxSpec(R) makes sense for any commutative ring R with $1 \neq 0$. The problem with MaxSpec is that whereas for algebraic sets V and W the algebraic maps MaxSpec $(\mathbb{C}[V]) \to$ MaxSpec $(\mathbb{C}[W])$ correspond to $\mathbb{C}$-homomorphisms $\mathbb{C}[W] \to \mathbb{C}[V]$, it's not clear how to define algebraic maps MaxSpec $(R) \to$ MaxSpec (S) for arbitrary rings R and S.

16.2. **France to the fore: Grothendieck and the Paris school.** The solution is Grothendieck's notion of *affine scheme*:

Definition 16.2.1. Let R be a commutative ring with $1 \neq 0$. Then $\mathrm{Spec}(R)$ is a topological space whose point set is the set of all prime ideals of R and where the closed sets are the subsets of the form $C_J = \{P \in \mathrm{Spec}\, R : J \subseteq P\}$ where $J \subseteq R$ is an ideal. (Given ideals $J \subseteq I$, note that $C_I \subseteq C_J$.) The topology is referred to as the Zariski topology on $\mathrm{Spec}(R)$, and we refer to $\mathrm{Spec}(R)$ as an affine scheme.

Example 16.2.2. If $R = \mathbb{C}[V]$ for an algebraic set V, we can by Exercise 16.3 regard V as a dense (but usually proper) subset of $\mathrm{Spec}(\mathbb{C}[V])$. The points of $\mathrm{Spec}(\mathbb{C}[V])$ are the prime ideals of $\mathbb{C}[V]$, which correspond to the irreducible subsets of V; i.e., for every irreducible subset of V we get a point of $\mathrm{Spec}(\mathbb{C}[V])$. These points are not always closed. If $P \in \mathrm{Spec}(\mathbb{C}[V])$, then the Zariski closure $\overline{P} \subseteq \mathrm{Spec}(\mathbb{C}[V])$ is

$$\overline{P} = \cap_{P \in C_J} C_J = \cap_{J \subseteq P} C_J = C_P = \{Q \in \mathrm{Spec}(\mathbb{C}[V]) : P \subseteq Q\}.$$

So, for example, if $V = \mathbb{A}^2$, where $\mathbb{C}[\mathbb{A}^2] = \mathbb{C}[x, y]$, and if $P = (x)$, then $\overline{P}$ consists of all prime ideals that contain x. In addition to P itself, these are precisely the maximal ideals $(x, y - c)$ for $c \in \mathbb{C}$; i.e., the ideals of points on $Z(x)$.

Exercise 15.3 suggests that it makes sense to identify an algebraic set V with $\mathrm{MaxSpec}(\mathbb{C}[V])$. Under this identification the points of V are identified with the maximal ideals of the coordinate ring. However, Spec has nicer formal properties than MaxSpec. One reason is that given any homomorphism $f : A \to B$ of commutative rings (we'll always assume rings have $1 \neq 0$ and that a homomorphism takes 1_A to 1_B), if $P \subset B$ is a prime ideal, then $f^{-1}(P)$ is a prime ideal of A, but it need not be true that $f^{-1}(M)$ is a maximal ideal of A just because M is a maximal ideal of B.

The first person to think of replacing the points of V by the primes of $\mathbb{C}[V]$ may have been Emmy Noether in the 1920s (although regarding the mathematics of her time—she died in 1935–Noether remarked "it is all already in Dedekind".) Wolfgang Krull suggested thinking of prime ideals in arbitrary commutative rings as points in a topological space in some lectures in the 1930s, but his ideas were not taken seriously at the time. The advantages of doing so became apparent to the Paris school of the 1950s, especially in the work of Jean-Pierre Serre and Alexander Grothendieck. Given a commutative ring R, Grothendieck referred to $\mathrm{Spec}(R)$ as an *affine scheme* and used it as the foundation for his general theory of schemes (although Serre has said that no one invented schemes; they were in the air in Paris in the 1950s.) [For a fun and interesting article exploring the history of these ideas, and which I used as a source for this paragraph, see: http://www.math.jussieu.fr/~leila/grothendieckcircle/mclarty1.pdf.]

Exercises:

Exercise 16.1. Let V and W be algebraic sets, and let $f : \mathrm{MaxSpec}\,(\mathbb{C}[V]) \to \mathrm{MaxSpec}\,(\mathbb{C}[W])$ be a map.

(a) Show that f is algebraic if and only if $\widetilde{f} : V \to W$ is algebraic.
(b) If f is algebraic, show that $f(I_V(v)) = (\widetilde{f}^*)^{-1}(I_V(v)) = I_W(\widetilde{f}(v))$ for all $v \in V$.

Solution by Katie Morrison (with minor changes). (a) ($\Leftarrow$) If $\widetilde{f}$ is algebraic, we have the following diagram:

$$\begin{tikzcd}
\mathrm{MaxSpec}(\mathbb{C}[V]) \arrow[r, "f"] & \mathrm{MaxSpec}(\mathbb{C}[W]) \\
V \arrow[u, "h_V"] \arrow[r, "\widetilde{f}"] \arrow[d, "I_V"] & W \arrow[u, "h_W"] \arrow[d, "I_W"] \\
\mathrm{MaxSpec}(\mathbb{C}[V]) \arrow[r, "(\widetilde{f}^*)^{-1}"'] & \mathrm{MaxSpec}(\mathbb{C}[W])
\end{tikzcd}$$

where h_V, h_W are defined as in Exercise 15.3, and $\widetilde{f}^* : \mathbb{C}[W] \to \mathbb{C}[V]$, defined by $g \mapsto g \circ \widetilde{f}$, is a $\mathbb{C}$-homomorphism. Now the top square commutes by definition of $\widetilde{f}$, so $f(I_V(v)) = I_W(\widetilde{f}(v))$, and the bottom square commutes since $I_W(\widetilde{f}(v)) = (\widetilde{f}^*)^{-1}(I_V(v))$ by Exercise 15.1. Thus, $f(I_V(v)) = (\widetilde{f}^*)^{-1}(I_V(v))$ for the $\mathbb{C}$-homomorphism $\widetilde{f}^*$, so f is algebraic.

($\Rightarrow$) If f is algebraic, then there exists some $\mathbb{C}$-homomorphism $\phi^* : \mathbb{C}[W] \to \mathbb{C}[V]$ such that $f(I_V(v)) = (\phi^*)^{-1}(I_V(v))$ (and hence we have the corresponding algebraic map $\phi : V \to W$) and we obtain the following commutative diagram

$$\begin{tikzcd}
\mathrm{MaxSpec}(\mathbb{C}[V]) \arrow[r, "f"] & \mathrm{MaxSpec}(\mathbb{C}[W]) \\
V \arrow[u, "h_V"] \arrow[r, "\phi"] \arrow[d, "I_V"] & W \arrow[u, "h_W"] \arrow[d, "I_W"] \\
\mathrm{MaxSpec}(\mathbb{C}[V]) \arrow[r, "(\phi^*)^{-1}"'] & \mathrm{MaxSpec}(\mathbb{C}[W])
\end{tikzcd}$$

Since $\widetilde{f}$ also makes the diagram commute and the maps h_V and h_W are bijective by Lemma 15.1, we have $\widetilde{f} = \phi$, so $\widetilde{f}$ is algebraic.

(b) Since f is algebraic, $\widetilde{f}$ is algebraic as well by part (a). Then $f(I_V(v)) = I_W(\widetilde{f}(v))$ since the diagram from part (a) commutes, and $I_W(\widetilde{f}(v)) = (\widetilde{f}^*)^{-1}(I_V(v))$ by Exercise 15.1. Thus $f(I_V(v)) = (\widetilde{f}^*)^{-1}(I_V(v)) = I_W(\widetilde{f}(v))$ for all $v \in V$. $\square$

Exercise 16.2. Let V and W be algebraic sets. Show that $f \mapsto \widetilde{f}$ gives a bijection from the set of algebraic maps $\mathrm{MaxSpec}(\mathbb{C}[V]) \to \mathrm{MaxSpec}(\mathbb{C}[W])$ to the set of algebraic maps $V \to W$.

Solution. Since h_V and h_W are bijective and $h_W \circ \widetilde{f} = f \circ h_V$, we see that $f \mapsto \widetilde{f}$ is a bijection from the set of all maps $\mathrm{MaxSpec}(\mathbb{C}[V]) \to \mathrm{MaxSpec}(\mathbb{C}[W])$ to the set of all maps $V \to W$, and by Exercise 16.1 $\widetilde{f}$ is algebraic if and only if f is. Hence $f \mapsto \widetilde{f}$ gives a bijection from the set of algebraic maps $\mathrm{MaxSpec}(\mathbb{C}[V]) \to \mathrm{MaxSpec}(\mathbb{C}[W])$ to the set of algebraic maps $V \to W$. $\square$

Exercise 16.3. Let V be an algebraic set. Let $i_V : V \to \mathrm{Spec}(\mathbb{C}[V])$ be the map $i_V : v \to I_V(v)$. Show that i_V is a continuous injective map such that the closure of $i_V(V)$ is $\mathrm{Spec}(\mathbb{C}[V])$.

Solution. Note that $\mathrm{MaxSpec}(\mathbb{C}[V])$ is a subset of $\mathrm{Spec}(\mathbb{C}[V])$, and that a subset $C \subseteq \mathrm{MaxSpec}(\mathbb{C}[V])$ is closed if and only if there is an ideal $J \subseteq \mathbb{C}[V]$ such that $C = \{M \in \mathrm{MaxSpec}(\mathbb{C}[V]) : J \subseteq M\}$. But a subset $D \subseteq \mathrm{Spec}(\mathbb{C}[V])$ is closed if and only if there is an ideal $J \subseteq \mathbb{C}[V]$ such that $D = \{P \in \mathrm{Spec}(\mathbb{C}[V]) : J \subseteq P\}$. Thus the closed sets C of $\mathrm{MaxSpec}(\mathbb{C}[V])$ are precisely the sets of the form $C = D \cap \mathrm{MaxSpec}(\mathbb{C}[V])$ where D is closed in $\mathrm{Spec}(\mathbb{C}[V])$. Thus $\mathrm{MaxSpec}(\mathbb{C}[V])$

is a topological subspace of $\mathrm{Spec}(\mathbb{C}[V])$, hence the inclusion $\mathrm{MaxSpec}(\mathbb{C}[V]) \subseteq \mathrm{Spec}(\mathbb{C}[V])$ is continuous. However, h_V is a homeomorphism and i_V factors as

$$V \xrightarrow{h_V} \mathrm{MaxSpec}(\mathbb{C}[V]) \subseteq \mathrm{Spec}(\mathbb{C}[V]).$$

Thus i_V is a composition of injective continuous maps, hence is itself injective and continuous. We now show that $i_V(V)$ is dense in $\mathrm{Spec}(\mathbb{C}[V])$. Since V is an algebraic set, we have $V = Z(J)$ for some ideal $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ for some n. By Exercise 5.7, $\sqrt{J} = \cap M$, where the intersection is over all maximal ideals M of $\mathbb{C}[x_1, \ldots, x_n]$ containing J. Since $\mathbb{C}[V] = \mathbb{C}[x_1, \ldots, x_n]/\sqrt{J}$, we see that $\sqrt{(0)} = \cap \overline{M}$ where now the intersection is over all maximal ideals $\overline{M} \subset \mathbb{C}[V]$ containing 0. Thus if D is a closed subset of $\mathrm{Spec}(\mathbb{C}[V])$ containing all maximal ideals $\overline{M}$ of $\mathbb{C}[V]$, then $D = C_J$ for some ideal $J \subseteq \mathbb{C}[V]$ such that $J \subseteq \overline{M}$ for all maximal ideals $\overline{M}$, hence $J \subseteq \sqrt{(0)}$, so $D = C_J = C_{(0)} = \mathrm{Spec}(\mathbb{C}[V])$, so $i_V(V)$ is dense. □

Exercise 16.4. Let R be a commutative ring. Show that $P \in \mathrm{Spec}(R)$ is a closed point if and only if P is a maximal ideal.

Solution by Anisah Nu'Man. Suppose P is a maximal ideal. Clearly by definition we have $P \in C_P$. Let $Q \in C_P$. Then $P \subseteq Q$ and Q is a prime ideal of R. Since Q is a proper ideal we have $Q = P$. Therefore we have $C_P = \{P\}$, and so is a closed point. Now Suppose $P \in \mathrm{Spec}(R)$ is a closed point, hence $C_P = \{P\}$. Since every ideal is contained in a maximal ideal there exists a maximal ideal M such that $P \subseteq M$. Thus $M \in C_P = \{P\}$ so we have $M = P$. Therefore P is a maximal ideal. □

Exercise 16.5. Let R be a commutative ring. Since every maximal ideal is a prime ideal we have the inclusion $\mathrm{MaxSpec}(R) \subseteq \mathrm{Spec}(R)$. Show that this is continuous in the Zariski topology, but give an example to show that $\mathrm{MaxSpec}(R)$ need not be dense in $\mathrm{Spec}(R)$. [Hint: for the example, do not pick R to be of the form $\mathbb{C}[V]$ for some algebraic set V, since by Exercises 15.3 and 16.3, $\mathrm{MaxSpec}(\mathbb{C}[V])$ is dense in $\mathrm{Spec}(\mathbb{C}[V])$.]

Solution. The proof that the inclusion $\mathrm{MaxSpec}(R) \subseteq \mathrm{Spec}(R)$ is continuous (i.e., that $\mathrm{MaxSpec}(R)$ is a topological subspace of $\mathrm{Spec}(R)$) was given in the solution to Exercise 16.3. For the example, let R be any integral domain which is not a field but which has a single maximal ideal M. Since R is not a field, $(0) \subsetneq M$, and since R is an integral domain, (0) is a prime ideal. But now $\mathrm{MaxSpec}(R)$ is the single closed point of $\mathrm{Spec}(R)$, hence not dense.

Here is a specific example of such an R. Let R be the set of rational numbers with odd denominators. It's easy to check this is a subring of the rationals, and hence a domain. Suppose $M \subseteq R$ is a maximal ideal. Let $a \in M$ be an element. The $a = f/g$ where f and g are integers with g odd. Since g is a unit, we have $(a) = (f)$. Since $M \subsetneq R$, we cannot have a being odd (since then a would be invertible). Since odds are invertible, we can assume f is either 0 or a power of 2. Thus $a \in (2)$, and hence $M \subseteq (2)$. Since 2 is not invertible, we see $(2) \subsetneq R$, hence $M = (2)$. I.e., (2) is a maximal ideal of R and it is the only maximal ideal of R, but $2 \neq 0$. □

Lecture 17. February 21, 2011

17.1. **Morphisms of affine schemes.** A morphism $\phi : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ of affine schemes is a pair $\phi : (f, f^\#)$, where $f^\# : R \to S$ is a ring homomorphism and $f : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is the map $f(Q) = (f^\#)^{-1}(Q)$. Clearly, $f^\#$ determines f. The utility of defining a morphism as a pair is clearer for morphisms of schemes that are not affine. As we will see, schemes are built by gluing together affine schemes, in much the same way that an n-dimensional manifold is built by gluing together open balls of $\mathbb{R}^n$. I.e., a scheme in general is locally an affine scheme and morphisms of schemes are defined by gluing together morphisms of affine schemes, but if $\phi = (f, f^\#) : X \to Y$ is a morphism of schemes X and Y, $f : X \to Y$ is a globally defined continuous map, but there

is no globally defined ring of functions and hence no globally defined homomorphism of rings $f^\#$. Instead $f^\#$ is essentially a collection of locally defined homomorphisms, whose relationships to each other are codified by a *sheaf* and depend on f.

One of the most important examples of non-affine schemes are projective spaces. But instead of defining them scheme theoretically to start with, we again take a historical approach first.

Example 17.1.1. Let $f^\# : \mathbb{C} \to \mathbb{C}$ be the identity and let $g^\# : \mathbb{C} \to \mathbb{C}$ be complex conjugation. Define $\phi_i : \mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(\mathbb{C})$ as $\phi_1 = (f, f^\#)$ and $\phi_2 = (g, g^\#)$, where $f = g = \mathrm{id}_\mathbb{C}$. Then both ϕ_1 and ϕ_2 are morphisms, but $\phi_1 \neq \phi_2$.

17.2. **Projective Space.** Intuitively, projective space is a compactification of affine space obtained by adding points at infinity. For example, $\mathbb{P}^1$ is the one point compactification of $\mathbb{A}^1$; in the standard topology, $\mathbb{P}^1_\mathbb{C}$ is the 2-sphere.

But $\mathbb{P}^2$ is not the one point compactification of $\mathbb{A}^2$. A basic result about $\mathbb{P}^2$ is that any two lines intersect in a single point. We regard parallel lines as being equivalent, and for each equivalence class of parallel lines we add a point at infinity. For any two parallel lines we regard this point at infinity as where the two lines meet. Of course, two lines are parallel exactly when they have the same slope (which can be infinite if the lines are vertical). Thus the points at infinity can be regarded as an $\mathbb{C} = \mathbb{A}^1$ (representing the possible slopes) plus a point representing infinity; i.e., the points at infinity that we add to $\mathbb{A}^2$ to get $\mathbb{P}^2$ themselves comprise a $\mathbb{P}^1$, so $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$. I.e., the points at infinity for $\mathbb{P}^2$ form a *line* at infinity, and this line is a $\mathbb{P}^1$. In general, $\mathbb{P}^n$ is defined in such a way that $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$.

More rigorously, $\mathbb{C} \setminus \{0\}$ acts on $\mathbb{C}^{n+1}\{0\}$ by scalar multiplication. Then $\mathbb{P}^n$ is the quotient space $(\mathbb{C}^{n+1}\{0\})/(\mathbb{C} \setminus \{0\})$; its points are the orbits of $\mathbb{C} \setminus \{0\}$ under the action (i.e., the lines through the origin). It's conventional in this context to think of $\mathbb{C}[\mathbb{C}^{n+1}]$ as being $\mathbb{C}[x_0, \ldots, x_n]$. Each non-zero point $p = (a_0, \ldots, a_n)$ is contained in a unique orbit which we denote by $[p]$, and each orbit is $[p]$ for some non-zero point $p \in \mathbb{C}^{n+1}$.

One can think of $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$ in the following way. For each $0 \leq i \leq n$, let $U_0 = Z(x_0 = 1)$. Thus there is a bijection $\mathbb{A}^n \to U_i$ given by inserting a 1 in the 0th spot: $(a_1, \ldots, a_n) \mapsto (1, a_1, \ldots, a_n)$. Every line through the origin, except those lying in the plane $x_0 = 0$ intersect U_0 in a unique point. The lines through the origin lying in the plane $x_0 = 0$ form a $\mathbb{P}^{n-1}$. Thus $\mathbb{A}^n \cong U_0$ and $U_0 \cup \mathbb{P}^{n-1} = \mathbb{P}^n$.

Figure 17.1 shows a figurative way to think of $\mathbb{P}^2$, with the points at infinity comprising a line $z = 0$. Also shown are two lines which in $\mathbb{A}^2$ are parallel, but which intersect at a point at infinity.

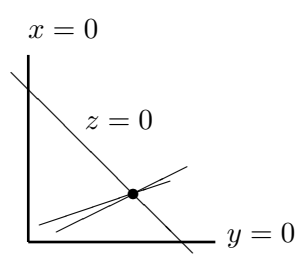


FIGURE 17.1. Figurative representation of $\mathbb{P}^2$.

Exercises:

Exercise 17.1. Let $\phi : (f, f^\#)$ be a morphism $\phi : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ of affine schemes. Show that $f : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is continuous in the Zariski topology.

Solution by Katie Morrison. Let $C \subseteq \mathrm{Spec}(R)$ be a Zariski-closed set. Then C is the intersection of sets of the form C_J for ideals $J \subseteq R$. Since the pre-image of an intersection of sets is the intersection of the pre-images of the sets and the intersection of closed sets is closed, it suffices to show that the pre-image of $C = C_J$ is closed. Tracing through definitions of C_J and f, we see

$$\begin{aligned} f^{-1}(C_J) &= \{P \in \mathrm{Spec}(S) \ : \ f(P) \supseteq J\} \\ &= \{P \in \mathrm{Spec}(S) \ : \ (f^{\#})^{-1}(P) \supseteq J\} \\ &= \{P \in \mathrm{Spec}(S) \ : \ P \supseteq f^{\#}(J)\} \\ &= \{P \in \mathrm{Spec}(S) \ : \ P \supseteq (f^{\#}(J))\} \\ &= C_{(f^{\#}(J))}. \end{aligned}$$

Thus, the pre-image of closed sets is closed, and so f is continuous. □

Lecture 18. February 23, 2011

Homogeneity.

Definition 18.1. Let $F \in \mathbb{C}[x_0, \ldots, x_n]$. We say F is *homogeneous* if either $F = 0$ or each monomial term appearing in F has the same total degree, this being $\deg(F)$. And if $I \subseteq \mathbb{C}[x_0, \ldots, x_n]$ is an ideal, we say I is *homogeneous* if $I = (F_1, \ldots, F_r)$ for some homogeneous polynomials F_i.

Example 18.2. Consider $F = x_0^2 - x_1 \in \mathbb{C}[x_0, x_1]$. Then F is not homogeneous. On the other hand $H = 3x_0^2 - x_0x_1 \in \mathbb{C}[x_0, x_1]$ is homogeneous, since each term has the same total degree, 2.

Example 18.3. The ideal $I = (3x_0^2 - x_0x_1, x_0^3) \subset \mathbb{C}[x_0, x_1]$ is homogeneous, since each generator is homogeneous. However the ideal $J = (x_0^2 - x_1) \subset \mathbb{C}[x_0, x_1]$ is not homogeneous (see Exercise 18.1). On the other hand, the ideal $L = (x_0^2 - x_1, x_1) \subset \mathbb{C}[x_0, x_1]$ is homogeneous since $L = (x_0^2, x_1)$ has a set of homogeneous generators.

Terminology: Let $R = \mathbb{C}[x_0, \ldots, x_n]$ and $F \in R$. Let F_i be the sum of the monomial terms of F of total degree i. If F has ho terms of degree i, set $F_i = 0$. Note that F_i is homogeneous for all i, and $F = \sum_i F_i$. We refer to F_i as the *homogeneous component* of F of degree i. If we denote by R_j the $\mathbb{C}$-vector space span of the monomials in R of total degree j, note that $R_iR_j = R_{i+j}$. This gives a ring structure to $R_0 \oplus R_1 \oplus \cdots$, and the map $h : R_0 \oplus R_1 \oplus \cdots \to R$ induced by sending each monomial to itself is a ring isomorphism (see Exercise 18.4). We refer to R_j as the *homogeneous component* of R of degree j. If $I \subseteq R$ is a homogeneous ideal, then h also induces an isomorphism $I_0 \oplus I_1 \oplus \cdots \to I$ where $I_j = I \cap R_j$ (see Exercise 18.5). We refer to I_j as the *homogeneous component* of I of degree j. Note that $R_iR_j = R_{i+j}$

Example 18.4. For $F = 6x_1^4 + x_0x_1 + x_0^2 - x_1$, we have $F_0 = 0$, $F_1 = -x_1$, $F_2 = x_0x_1 + x_0^2$, $F_3 = 0$, $F_4 = 6x_1^4$ and $F_i = 0$ for $i > 4$.

Remark 18.5. Let $F \in \mathbb{C}[x_0, \ldots, x_n]$. One can check homogeneity F by looking at the zero-locus of F: by Exercise 18.6, F is homogeneous if and only if $Z(F) \subseteq \mathbb{C}^{n+1}$ is either the origin or a union of lines through the origin. For example, consider $F = x^2 + y \in \mathbb{C}[x, y]$. Then F is not homogeneous and $Z(F)$ is neither the origin nor a union of lines through the origin, but $Z(G)$ for $G = x^2 + xy$ is the union of two lines through the origin.

Notation 18.6. For each point $p \in \mathbb{C}^{n+1} \setminus \{\text{origin}\}$, let $[p] \in \mathbb{P}^n$ denote the orbit of p under the action of $\mathbb{C}^*$ on $\mathbb{C}^{n+1} \setminus \{\text{origin}\}$. Note that every point of $\mathbb{P}^n$ is of the form $[p]$ for some $p \in \mathbb{C}^{n+1} \setminus \{\text{origin}\}$.

If F is a non-constant homogeneous polynomial $F \in \mathbb{C}[x_0, \ldots, x_n]$, then F does not give a well-defined function on $\mathbb{P}^n$, since $F(tp) = t^dF(p)$, where $t = \deg(F)$. Thus F can take different values at different representatives $tp \in [p]$. But the zero-locus of F is well-defined, since for any $t \neq 0$ we have $F(p) = 0$ if and only if $F(tp) = 0$.

Definition 18.7. A projective algebraic subset V of $\mathbb{P}^n$ is a subset of the form $V = Z(F_1, \dots, F_r)$ for homogeneous polynomials $F_i \in \mathbb{C}[x_0, \dots, x_n]$, where $Z(F_1, \dots, F_r)$ means $Z(F_1) \cap \cdots \cap Z(F_r)$. More generally, if $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ is a homogeneous ideal, we define $Z(I)$ to be $\cap Z(F)$, where the intersection is over all homogeneous $F \in I$. By Exercise 18.7, $Z(I) = Z(F_1, \dots, F_r)$ for any set of homogeneous generators F_i of I.

The projective algebraic subsets of $\mathbb{P}^n$ comprise the closed sets of a topology on $\mathbb{P}^n$, called the Zariski topology. However, the interplay between closed sets and ideals is more complicated than for affine space:

Example 18.8. If $I \subseteq \mathbb{C}[\mathbb{A}^n]$ has $Z(I) = \varnothing \subseteq \mathbb{A}^n$, then $I = (1)$. However, if $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ has $Z(I) = \varnothing \subseteq \mathbb{P}^n$, then $I = (1)$ is only one of many possibilities. We will see the other possibilities next time.

Exercises:

Exercise 18.1. Show that the ideal $J = (x_0^2 - x_1) \subset \mathbb{C}[x_0, x_1]$ is not homogeneous.

Solution. By Exercise 18.3. if J were homogeneous, then we would have $x_0^2, x_1 \in J$. But this would mean, in particular, that $x_0^2 - x_1$ divides x_1, which it does not. Thus J is not homogeneous. [Note that it is not enough to just show that $x_0^2 - x_1$ is not homogeneous, since for example neither of the given generators of $(x_0^2 - x_1, x_0^2 + x_1)$ is homogeneous, but $(x_0^2 - x_1, x_0^2 + x_1) = (x_0^2, x_1)$ is homogeneous since we can find another set of generators each element of which is homogeneous.] □

Exercise 18.2. Let $0 \neq F \in \mathbb{C}[x_0, \dots, x_n]$ be homogeneous, $d = \deg(F)$.

(a) Show that $F(tx_0, \dots, tx_n) = t^d F(x_0, \dots, x_n)$.
(b) (Euler's formula) Show that $\sum_i x_i \frac{\partial F}{\partial x_i} = dF$.

Solution by Jason Hardin. (a) Since $F(x_0, \dots, x_n)$ is homogeneous of degree d, each term of $F(x_0, \dots, x_n)$ has the form $cx_0^{e_0} \cdots x_n^{e_n}$, where $c \in \mathbb{C}$ and e_i are non-negative integers satisfying $e_0 + \cdots + e_n = d$. The corresponding term in $F(tx_0, \dots, tx_n)$ is $c(tx_0)^{e_0} \cdots (tx_n)^{e_n} = t^{e_0 + \cdots + e_n} cx_0^{e_0} \cdots x_n^{e_n} = t^d cx_0^{e_0} \cdots x_n^{e_n}$. So each term of $F(tx_0, \dots, tx_n)$ is t^d times the original term of $F(x_0, \dots, x_n)$. Factoring out the common factor t^d, we obtain the result.

(b) By (a), F satisfies the equation $F(tx_0, \dots, tx_n) = t^d F(x_0, \dots, x_n)$. Differentiating both sides of this equation with respect to t via the chain rule of partial differentiation, we obtain

$$\sum_{i=0}^{n} \frac{\partial F(tx_0, \dots, tx_n)}{\partial tx_i} \cdot \frac{\partial tx_i}{\partial t} = dt^{d-1} F(x_0, \dots, x_n).$$

Since $\dfrac{\partial tx_i}{\partial t} = x_i$, this yields

$$\sum_{i=0}^{n} x_i \frac{\partial F(tx_0, \dots, tx_n)}{\partial tx_i} = dt^{d-1} F(x_0, \dots, x_n).$$

Finally, setting $t = 1$ we obtain the desired result:

$$\sum_{i=0}^{n} x_i \frac{\partial F(x_0, \dots, x_n)}{\partial x_i} = dF(x_0, \dots, x_n).$$

□

Exercise 18.3. Let $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ be an ideal. Show that I is homogeneous if and only if whenever $F \in I$, then $F_i \in I$ for each homogeneous component F_i of F.

Solution, presented in class by Jason Hardin. Suppose I is homogeneous. Write $I = (F^1, \dots, F^m)$, where $F^1, \dots, F^m \in \mathbb{C}[x_0, \dots, x_n]$ are homogeneous polynomials. Let $F \in I$. Then there are polynomials $G^1, \dots, G^m \in \mathbb{C}[x_0, \dots, x_n]$ such that $F = \sum_{j=1}^m G^j F^j$. Since $F^j \in I$, we have $G_i^j F^j \in I$ for all i, and $G_i^j F^j$ is homogeneous as it is a product of homogeneous polynomials. Thus, $(G^j F^j)_i = G^j_{i-\deg(F^j)} F^j \in I$ for all i and $j = 1, \dots, m$. Hence, we have $F_i = \sum_{j=1}^m (G^j F^j)_i \in I$, as required.

Conversely, suppose that whenever $F \in I$ we have $F_i \in I$ for all i. Write $I = (F^1, \dots, F^m)$ with $\deg(F^j) = d_j$. Let J be the ideal generated by all the homogenous components of $F^1, \dots, F^m$, i.e., $J = (F_0^1, \dots, F_{d_1}^1, F_0^2, \dots, F_{d_2}^2, \dots, F_0^m, \dots, F_{d_m}^m)$. Observe that J is a homogeneous ideal as it's generated by homogeneous polynomials. We have $I \subseteq J$ since each generator of I is the sum of its homogeneous components, which are all in J. Also, $J \subseteq I$ since $F_i^j \in I$ by the hypothesis. Thus, $I = J$ is homogeneous. □

Exercise 18.4. Show that the map $h : R_0 \oplus R_1 \oplus \cdots \to R$ induced by sending each monomial to itself is a ring isomorphism.

Solution by Nora Youngs (with minor additions). Since the monomials of degree i give a basis of R_i, h restricted to R_i is the identity, so h is defined by $(r_0, r_1, ...) \mapsto r_0 + r_1 + \cdots$. It is now easy to check that h preserves addition and multiplication, so we will show that h is injective and surjective.

Suppose $h(r_0, r_1, ...) = h(s_0, s_1, ...)$. Then, $r_0 + r_1 + \cdots = s_0 + s_1 + \cdots$. Since r_i, s_i are the homogeneous components of degree i and the polynomials are equal, we must have $r_i = s_i$ for all i. Thus, $(r_0, ...) = (s_0, ...)$ and so h is injective.

To see that h is surjective, let $f \in R$. If $f = 0$, then $h(0) = f$, so assume $f \neq 0$. Write $f = f_0 + \cdots + f_r$ where f_i is the homogeneous component of f of degree i and $r = \deg(f)$. Then $h(f_0, \dots, f_r) = f_0 + \cdots + f_r = f$, so h is also surjective. □

Exercise 18.5. Let $I \subseteq R = \mathbb{C}[x_0, \dots, x_n]$ be a homogeneous ideal. Under the isomorphism $h : R_0 \oplus R_1 \oplus \cdots \to R$, show that $h(I_0 \oplus I_1 \oplus \cdots) = I$, where $I_j = I \cap R_j$.

Solution. Since h restricted to R_i is the identity, h restricted to I_j is also the identity. But $I = \sum_j I_j$, so $h(I_0 \oplus I_1 \oplus \cdots) = I$. □

Exercise 18.6. Let $F \in \mathbb{C}[x_0, \dots, x_n]$ and let $p \in \mathbb{C}^{n+1}$. Show that F is homogeneous if and only if whenever $F(p) = 0$, then $F(cp) = 0$ for all $c \in \mathbb{C}$.

Solution. First suppose F is homogeneous. If $F = 0$, then clearly $F(cp) = c^d F(p)$ for all $c \in \mathbb{C}$. So assume F is not the zero polynomial and let $d = \deg(F)$. Then $F(cp) = c^d F(p)$ by Exercise 18.2(a), so if $F(p) = 0$, then also $F(cp) = 0$ for all $c \in \mathbb{C}$.

Conversely, suppose F is not homogeneous. Write $F = F_m + \cdots + F_M$ as the sum of its homogeneous components, where m is the degree of the term of least degree, and M is the degree of the term of largest degree (and hence $m < M$). We know $Z(F)$ is not empty by the Nullstellensatz, since if $Z(F)$ were empty, then F would be a non-zero constant, but $\deg(F) = M > m \geq 0$. Also, by assumption, $F_m \neq 0$. If $m = 0$, then F has a non-zero constant term, so $F(0) \neq 0$. Pick any point $p \in Z(F)$. Then the line through the origin and p is not contained in $Z(F)$; i.e., $F(cp) = 0$ does not hold for all $c \in \mathbb{C}$. Suppose $m > 0$. Note that $Z(F) \subsetneq \mathbb{C}^{n+1}$. (If we had $Z(F) = \mathbb{C}^{n+1}$, then $F \in \sqrt{(0)} = (0)$ by the Nullstellensatz.) Since $\mathbb{C}^{n+1}$ is irreducible (since $I(\mathbb{C}^{n+1}) = (0)$ is prime), $Z(F_m) \cup Z(F_M) \neq \mathbb{C}^{n+1}$, so we can pick a point $p \notin Z(F_m) \cup Z(F_M)$. Thus $F(tp)$ is a polynomial in the single indeterminate t whose homogeneous component of least degree is $F_m(tp)$ and whose homogeneous component of maximum degree is $F_M(tp)$. Thus $F(tp)$ is not the zero polynomial, so there are values of t for which $F(tp) \neq 0$. Since $m > 0$, we see $t | F(tp)$, so 0 is a root of $F(tp)$, but $F(tp)$ is not a pure power of t, so 0 cannot be its only root. Thus F vanishes at some point $q \neq 0$ on the line tq, but not at every point of the line. □

Exercise 18.7. If $F_1, \dots, F_r$ is any set of homogeneous generators for a homogeneous ideal $I \subseteq \mathbb{C}[x_0, \dots, x_n]$, show that $Z(F_1, \dots, F_r) = Z(I)$.

Solution by Zheng Yang. If F_i vanishes on $\underline{c}$ for all i, then so does any polynomial in I, as these F_i's are generators for I, hence $Z(F_1, \dots, F_r) \subseteq Z(I)$. For the reverse inclusion, assume $F(\underline{c}) = 0$ for some $\underline{c}$ and all F in I. Then since each homogeneous component F_j of F is also in I by Exercise 18.3, we have that F_j vanishes at $\underline{c}$ too, so $Z(F_1, \dots, F_r) = Z(F_1) \cap \dots \cap Z(F_r) \supseteq Z(I)$. □

Lecture 19. February 25, 2011

19.1. **Homogeneity continued.**

Notation 19.1.1. Let $J \subseteq \mathbb{C}[x_0, \dots, x_n]$ be a homogeneous ideal. Then $Z(J)$ could denote a subset either of projective space $\mathbb{P}^n$ or affine space $\mathbb{A}^{n+1}$. To distinguish which is meant, we will use $Z_{\mathbb{A}^{n+1}}(J) \subseteq \mathbb{A}^{n+1}$ or $Z_{\mathbb{P}^n}(J) \subseteq \mathbb{P}^n$. Of course, $Z_{\mathbb{A}^{n+1}}(J)$ and $Z_{\mathbb{P}^n}(J)$ are related: if $p \in \mathbb{A}^{n+1} \setminus \{\text{origin}\}$, then $p \in Z_{\mathbb{A}^{n+1}}(J)$ if and only if $[p] \in Z_{\mathbb{P}^n}(J)$.

Example 19.1.2. As noted last lecture, $Z_{\mathbb{A}^{n+1}}((1)) = Z_{\mathbb{P}^n}((1)) = \varnothing$, but if $M = (x_0, \dots, x_n) \subset \mathbb{C}[x_0, \dots, x_n]$, and I is M-primary and homogeneous, then $Z_{\mathbb{P}^n}(I) = \varnothing$, even though $Z_{\mathbb{A}^{n+1}}(I) = \{\text{origin}\}$.

The previous example shows that different homogeneous ideals can define different projective zero loci, even if the ideals do not have the same radical. But as we will see from the projective Nullstellensatz, this phenomenon is limited to the empty zero locus. First a lemma characterizing the homogeneous ideals with empty projective zero locus. Because of this lemma, the ideal $(x_0, \dots, x_n)$ is sometimes referred to as the em irrelevant ideal.

Lemma 19.1.3. *Let $J \subseteq \mathbb{C}[x_0, \dots, x_n]$ be a homogeneous ideal. Then $Z_{\mathbb{P}^n}(J) = \varnothing$ if and only if $(x_0, \dots, x_n) \subseteq \sqrt{J}$*

Proof. If $Z_{\mathbb{P}^n}(J) = \varnothing$, then $Z_{\mathbb{A}^{n+1}}(J) \subseteq \{\text{origin}\}$ (by notational remark 19.1.1 above), hence $(x_0, \dots, x_n) = I(\{\text{origin}\}) \subseteq \mathrm{I}(\mathrm{Z}_{\mathbb{A}^{n+1}}(\mathrm{J})) = \sqrt{\mathrm{J}}$.

Conversely, $Z_{\mathbb{A}^{n+1}}(J) = Z_{\mathbb{A}^{n+1}}(\sqrt{J}) \subseteq Z_{\mathbb{A}^{n+1}}((x_0, \dots, x_n)) = \{\text{origin}\}$, hence $Z_{\mathbb{P}^n}(J) = \varnothing$ (again notational remark 19.1.1). □

Definition 19.1.4. Given any subset $S \subseteq \mathbb{P}^n$, let $I(S)$ be the ideal generated by all homogeneous $F \in \mathbb{C}[x_0, \dots, x_n]$ such that $Z_{\mathbb{P}^n}(F)$ contains S. (For emphasis, we may sometimes write $I_{\mathbb{P}^n}(S)$ for $I(S)$, although in principle this is not necessary, since given a set A, whether $I(A)$ means the ideal of all polynomials vanishing on A or the ideal generated by all homogeneous polynomials vanishing on A is determined by whether A is a subset of affine space or projective space.) We also write $\mathbb{C}[\mathbb{P}^n]$ for $\mathbb{C}[x_0, \dots, x_n]$, and refer to it as the *homogeneous coordinate ring* of $\mathbb{P}^n$.

Theorem 19.1.5 (Projective Nullstellensatz)**.** *Let $J \subseteq \mathbb{C}[\mathbb{P}^n]$ be a homogeneous ideal. If $Z_{\mathbb{P}^n}(J)$ is not empty, then $I(Z_{\mathbb{P}^n}(J)) = \sqrt{J}$.*

Proof. To show $I(Z_{\mathbb{P}^n}(J)) = \sqrt{J}$, since both ideals are homogeneous, it suffices to show that any non-zero homogeneous element of one is an element of the other.

So let $F \in I(Z_{\mathbb{P}^n}(J))$ be non-zero and homogeneous. Since $Z_{\mathbb{P}^n}(J) \neq \varnothing$, F is not constant. Let $p \in Z_{\mathbb{A}^{n+1}}(J)$. If p is the origin, then (since every homogeneous polynomial vanishes at the origin), $F(p) = 0$. If p is not the origin, then again $F(p) = 0$ since $p \in Z_{\mathbb{A}^{n+1}}(J)$ implies $[p] \in Z_{\mathbb{P}^n}(J)$. Thus $F \in \sqrt{J}$ by the Nullstellensatz, hence $I(Z_{\mathbb{P}^n}(J)) \subseteq \sqrt{J}$.

For the reverse containment, let $F \in \sqrt{J}$ be non-zero and homogeneous. Then $F^r \in J \subseteq I(Z_{\mathbb{P}^n}(J))$ so $F \in I(Z_{\mathbb{P}^n}(J))$. □

19.2. **Comparing conics, over $\mathbb{R}$ and over $\mathbb{C}$, in $\mathbb{A}^2$ and in $\mathbb{P}^2$.** There are eight different kinds of zero loci in $\mathbb{R}^2$ for degree 2 polynomials in $\mathbb{R}[x,y]$. Here are examples of each one.

(1) ellipses: $x^2+y^2-1=0$;
(2) hyperbolas: $x^2-y^2-1=0$;
(3) parabolas: $y-x^2=0$;
(4) pairs of intersecting lines: $x^2-y^2=0$;
(5) pairs of parallel lines: $(x+y)(x+y+1)=0$;
(6) doubled lines: $(x+y)^2=0$;
(7) single points: $x^2+y^2=0$; and
(8) the empty set: $x^2+y^2+1=0$.

Over $\mathbb{C}$ this reduces to only five different kinds. Note for example that under the coordinate change in which we replace y by iy, $x^2+y^2-1=0$ becomes $x^2-y^2-1=0$. Moreover, $Z_{\mathbb{A}^2}(f)$ is always an infinite set for a degree 2 polynomial $f(x,y)\in\mathbb{C}[x,y]$ (see Exercise 19.2), so cases (7) and (8) above do not occur over $\mathbb{C}$.

(1) ellipse-hyperbola category: $x^2+y^2-1=0$;
(2) parabolas: $y-x^2=0$;
(3) pairs of intersecting lines: $xy=0$;
(4) pairs of parallel lines: $(x+y)(x+y+1)=0$;
(5) doubled lines: $(x+y)^2=0$;

To compare this to what happens in projective space, we introduce the notion of homogenization.

Definition 19.2.1. Let $0\neq g\in\mathbb{C}[x_1,\dots,x_n]$ and let $d=\deg(g)$. Define the *homogenization* g_H of g to be the polynomial $g_H(x_0,\dots,x_n)=x_0^d\,g(\frac{x_1}{x_0},\dots,\frac{x_n}{x_0})\in\mathbb{C}[x_0,\dots,x_n]$. Note that g_H is indeed a homogeneous polynomial. We refer to $Z_{\mathbb{P}^n}(g_H)$ as the *projective closure* of $Z_{\mathbb{A}^n}(g)$.

Example 19.2.2. If $f=x_1^2+x_2^2-1$, then $f_H=x_1^2+x_2^2-x_0^2$. If $f=x_2-x_1^2$, then $f_H=x_0x_2-x_1^2$.

Further simplification occurs when classifying zero loci of degree 2 homogeneous polynomials in $\mathbb{P}^2$. We can regard $\mathbb{A}^2$ as an open subset of $\mathbb{P}^2$; the points $(a,b)\in\mathbb{A}^2$ can be identified with the points $[(a,b,1)]\in\mathbb{P}^2$. The points of $\mathbb{A}^2$ at infinity can be identified with $[(a,b,0)]\in\mathbb{P}^2$.

If $0\neq f(x,y)\in\mathbb{C}[x,y]$, suppose $[(a,b,0)]$ is a point at infinity which is a limit point (in the standard topology) of a sequence $[(a_i,b_i,1)]$ of points in the zero locus $Z_{\mathbb{A}^2}(f)$ in the finite affine plane $\mathbb{A}^2$. Then either $a_i\xrightarrow{i\to\infty}\infty$ or $b_i\xrightarrow{i\to\infty}\infty$; say the latter and assume for simplicity that $b\neq 0$. Then $[(\frac{a_i}{b_i},1,\frac{1}{b_i})]$ is the same sequence of points in $\mathbb{P}^2$, but the limit is $[(\frac{a}{b},1,0)]=[(a,b,0)]$. Since $f(a_i,b_i)=0$ for all i, we have $f_H(a_i,b_i,1)=f(a_i,b_i)=0$, hence we also have $b_i^d f_H(\frac{a_i}{b_i},1,\frac{1}{b_i})=f_H(a_i,b_i,1)=0$ and hence $f_H(a,b,0)=\lim_i f_H(\frac{a_i}{b_i},1,\frac{1}{b_i})=0$. Thus $Z_{\mathbb{P}^2}(f_H)$ contains (and in fact is equal to) the union of $Z_{\mathbb{A}^2}(f)$ and the limit points at infinity, hence the name projective closure.

Thus after including the points at infinity in our categories above we have the ellipse-hyperbola category, $Z_{\mathbb{P}^2}(x^2+y^2-z^2)$, the parabola category, $Z_{\mathbb{P}^2}(yz-x^2)$, the two intersecting lines, $Z_{\mathbb{P}^2}(xy)$, the parallel lines, $Z_{\mathbb{P}^2}((x+y)(x+y+z))$, and the doubled line, $Z_{\mathbb{P}^2}((x+y)^2)$. But after a change of coordinates where we substitute y for $x+iy$, z for $x-iy$ and x for z, $Z_{\mathbb{P}^2}(x^2+y^2-z^2)$ becomes $Z_{\mathbb{P}^2}(yz-x^2)$; i.e., the parabola is just another instance of the ellipse-hyperbola category.

And the two parallel lines become a pair of intersecting lines, so in $\mathbb{P}^2$ this suggests we have only 3 categories:

(1) ellipse-hyperbola-parabola category (i.e., the irreducible conics): $Z_{\mathbb{P}^2}(yz-x^2)$;
(2) two intersecting lines (the reducible conics): $xy=0$;
(3) the doubled lines (the "non-reduced" conics): $(x+y)^2=0$;

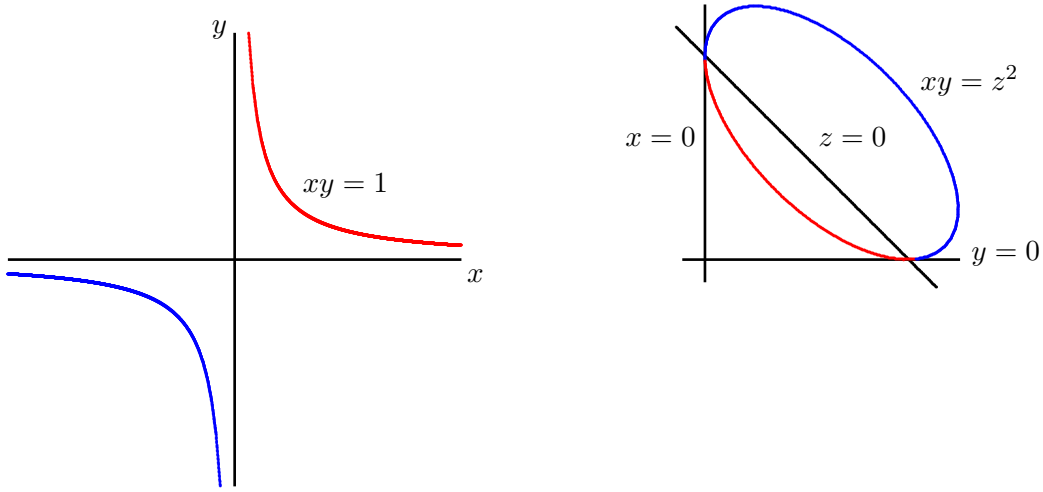


FIGURE 19.1. The hyperbola $Z_{\mathbb{A}^2}(xy - 1)$ and its projective closure $Z_{\mathbb{P}^2}(xy - z^2)$.

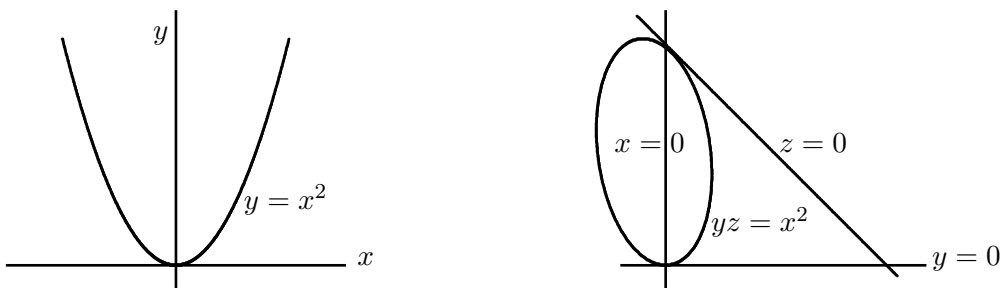


FIGURE 19.2. The parabola $Z_{\mathbb{A}^2}(y - x^2)$ and its projective closure $Z_{\mathbb{P}^2}(yz - x^2)$.

In the figures above, note that the projective closure of the hyperbola has equation $xy - z^2$ and the projective closure of the parabola has equation $yz - x^2$; these are the same equations after a permutation of the variables (i.e., up to a projective change of coordinates the projective closures are the same). In the affine plane they are different: the parabola has a single point at infinity, while the hyperbola has two.

Exercises:

Exercise 19.1. Let $J \subseteq \mathbb{C}[x_0, \ldots, x_n]$ be a homogeneous ideal. Show that $\sqrt{J}$ is homogeneous and hence that $Z_{\mathbb{P}^n}(\sqrt{J})$ is defined. Conclude that $Z_{\mathbb{P}^n}(J) = Z_{\mathbb{P}^n}(\sqrt{J})$.

Solution by Jason Hardin. Let $F \in \sqrt{J}$ and let $F = F_0 + F_1 + \cdots + F_d$ be its decomposition into homogeneous components. By exercise 18.3, it suffices to show that $F_i \in \sqrt{J}$ for $0 \leq i \leq d$.

Since $F \in \sqrt{J}$, we know $F^{m_1} \in J$ for some m_1. Observe that $(F^{m_1})_0 = (F_0)^{m_1}$. Since J is homogeneous, $(F_0)^{m_1} = (F^{m_1})_0 \in J$ by exercise 18.3. Thus, $F_0 \in \sqrt{J}$. This means that $G := F - F_0 = F_1 + \cdots + F_d \in \sqrt{J}$, so $G^{m_2} \in J$ for some m_2. Observe that $(F_1)^{m_2} = (G^{m_2})_{m_2} \in J$ since J is homogeneous, and thus $F_1 \in \sqrt{J}$. So $H := G - F_1 = F_2 + \cdots + F_d \in \sqrt{J}$. Continuing in

this fashion, we see that at each step the smallest remaining non-zero homogeneous component of F is in $\sqrt{J}$. This process terminates after $d+1$ steps, and we have $F_i \in \sqrt{J}$ for $0 \le i \le d$.

Since $\sqrt{J}$ is homogeneous, $Z_{\mathbb{P}^n}(\sqrt{J})$ is defined. Moreover, we have $[p] \in Z_{\mathbb{P}^n}(J)$ if and only if $p \in Z_{\mathbb{A}^{n+1}}(J) = Z_{\mathbb{A}^{n+1}}(\sqrt{J})$ if and only if $[p] \in Z_{\mathbb{P}^n}(\sqrt{J})$. Hence, $Z_{\mathbb{P}^n}(J) = Z_{\mathbb{P}^n}(\sqrt{J})$. □

Exercise 19.2. Show that $Z_{\mathbb{A}^2}(f)$ is infinite for every degree 2 polynomial $f(x,y) \in \mathbb{C}[x,y]$.

Solution by Kat Shultis. Let $f(x,y) \in \mathbb{C}[x,y]$ be a degree 2 polynomial. Then $f(x,y) = \alpha x^2 + \beta y^2 + \gamma xy + \delta x + \epsilon y + \eta$ and at least one of α, β, γ is nonzero. We consider each case separately. If $\alpha \neq 0$, then if we choose any $y_0 \in \mathbb{C}$, we get a quadratic polynomial $f(x, y_0)$ in one variable, x, and since $\mathbb{C}$ is algebraically closed, we know that there is an $x_0 \in \mathbb{C}$ such that $f(x_0, y_0) = 0$. Similarly, if $\beta \neq 0$, we can choose any $x_0 \in \mathbb{C}$, and get a quadratic polynomial in y, namely $f(x_0, y)$. Hence there exists some $y_0 \in \mathbb{C}$ such that $f(x_0, y_0) \in \mathbb{C}$. Thus, in either of these two cases, $Z_{\mathbb{A}^2}(f)$ has the same cardinality of $\mathbb{C}$, and hence is infinite. Next, we assume that $\gamma \neq 0$. If $x_0 \in \mathbb{C} \setminus \{0\}$, then $f(x_0, y) = \alpha x_0^2 + \beta y^2 + \gamma x_0 y + \delta x_0 + \epsilon y + \eta$ is at least a linear polynomial in y, as $\gamma \neq 0$. Thus there exists some $y_0 \in \mathbb{C}$ such that $f(x_0, y_0) = 0$. Here, $Z_{\mathbb{A}^2}(f)$ is in bijection with $\mathbb{C} \setminus \{0\}$ which is infinite. □

Lecture 20. February 28, 2011

Projective changes of coordinates. To show rigorously that all irreducible conics are in some sense the same, we formalize the notion of projective changes of coordinates. Let $M \in \mathrm{GL}_{n+1}(\mathbb{C})$, so $M = (m_{ij})$ is an $(n+1) \times (n+1)$ invertible matrix with complex entries. Let $T_M : A = \mathbb{C}^{n+1} \to B = \mathbb{C}^{n+1}$ be the linear transformation defined by M with respect to the standard basis $\mathbf{e}_0 = (1, 0, \ldots, 0)^t, \ldots, \mathbf{e}_n = (0, \ldots, 0, 1)^t$. If $\mathbf{a} = (a_0, \ldots, a_n)^t \in \mathbb{C}^{n+1}$, then

$$T_M(\mathbf{a}) = M\mathbf{a} = \Big(\sum_j m_{0j} a_j, \ldots, \sum_j m_{nj} a_j\Big) \in \mathbb{C}^{n+1},$$

so T_M is an algebraic mapping $T_M = (f_0, \ldots, f_n)$ where, taking $\mathbb{C}[A] = \mathbb{C}[x_0, \ldots, x_n]$, the coordinate functions are $f_i = \sum_j m_{ij} x_j$. If we write $\mathbb{C}[B] = \mathbb{C}[y_0, \ldots, y_n]$, then we have $T_M^* : \mathbb{C}[B] \to \mathbb{C}[A]$, given by $T_M^*(y_i) = f_i = y_i \circ T_M$.

We can regard M as giving a change of coordinates on $\mathbb{C}^{n+1}$ by taking $\varepsilon_i = (T_M)^{-1}(\mathbf{e}_i)$. Given the coordinate vector $\mathbf{a} \in \mathbb{C}^{n+1}$ of a point in A with respect to the standard basis, then $\mathbf{b} = M\mathbf{a}$ is the coordinate vector of the same point with respect to the basis $\{\varepsilon_i\}$, since

$$\sum_i b_i \varepsilon_i = \sum_i b_i (T_M)^{-1}(\mathbf{e}_i) = (T_M)^{-1}\big(\sum_i b_i \mathbf{e}_i\big) = (T_M)^{-1}(\mathbf{b}) = (T_M)^{-1} T_M(\mathbf{a}) = \mathbf{a} = \sum_i a_i \mathbf{e}_i.$$

A linear change of coordinates T_M on $\mathbb{C}^{n+1}$ gives a change of coordinates also on $\mathbb{P}^n$ (denoted T_M^P and well-defined since T_M is linear and hence takes lines through the origin to lines through the origin), since $\mathbb{P}^n$ inherits its coordinates from $\mathbb{C}^{n+1}$. We call this change of coordinates a *projective change of coordinates*. The set of all such coordinate changes T_M^P forms a group under composition, the projective linear group, denoted $\mathbb{P}GL_n(\mathbb{C})$. By Exercise 20.1, $\mathbb{P}\mathrm{GL}_n(\mathbb{C}) \cong \mathrm{GL}_{n+1}(\mathbb{C})/\mathbb{C}^*$, where we regard the non-zero complex number $\mathbb{C}^*$ as a subgroup of $\mathrm{GL}_{n+1}(\mathbb{C})$ by thinking of $c \in \mathbb{C}^*$ as cI_{n+1}; this is in fact a normal subgroup.

Note that a projective change of coordinates on $\mathbb{P}^n$ is defined by picking a basis $\varepsilon_0, \ldots, \varepsilon_n$ of $\mathbb{C}^{n+1}$. Picking the basis ε_i is equivalent to picking linear forms $y_j \in \mathbb{C}[x_0, \ldots, y_n]$, $0 \le j \le n$ (a *form* is just another word for a homogeneous polynomial). Given the basis ε_i, the forms y_j are those such that $y_j(\varepsilon_i)$ is 1 if $i = j$ and 0 otherwise, and given the forms y_j, on can recover the basis vectors ε_i by solving the equations $y_j(\varepsilon_i) = \delta_{ij}$ (where here δ_{ij} is Kronecker's delta-function; i.e., (δ_{ij}) is the identity matrix). If the basis ε_i is given by $(T_M)^{-1}(\mathbf{e}_i)$ for a matrix $M = (m_{ij})$, then the forms y_i are $\sum_j m_{ij} x_j$. This is because if $[\mathbf{a}]$ is the coordinate vector (with respect to

the standard basis) of a point in $\mathbb{P}^n$, then the coordinate vector with respect to the basis ε_i is $[\mathbf{b}]$, where $\mathbf{b} = M\mathbf{a}$. The ith coordinate of $\mathbf{b}$ is b_i, but

$$y_i(p) = y_i(\sum_j b_j\varepsilon_j) = \sum_j b_j y_i(\varepsilon_j) = b_i = \sum_j m_{ij}a_j = \sum_j m_{ij}x_j(p),$$

hence $y_i = \sum_j m_{ij}x_j$.

Exercises:

Exercise 20.1. Let $M_1, M_2 \in \mathrm{GL}_{n+1}(\mathbb{C})$. Show that $T^P_{M_1} = T^P_{M_2}$ if and only if $M_1 = cM_2$ for some non-zero scalar $c \in \mathbb{C}$.

Solution by Ashley Weatherwax. $\Leftarrow$ Suppose $M_1 = cM_2$ for a scalar $c \in \mathbb{C}$. Then

$$T^P_{M_2}([a]) = [M_2a] = [cM_2a] = T^P_{cM_2}([a]) = T^P_{M_1}([a])$$

$\Rightarrow$ Suppose $T^P_{M_1}([a]) = T^P_{M_2}([a])$. Then we can compose both sides with $T^P_{M_2^{-1}}$ to get $T^P_{M_2^{-1}M_1} = T^P_I$. Thus it suffices to show that $T^P_M = T^P_I$ implies $M = cI$ for some constant c.

Let $[a] \in \mathbb{P}^n$. Then $T^P_M([a]) = T^P_I([a])$ implies $[Ma] = [a]$, and so there exists a c_a so that

$$Ma = c_a a$$

But notice that this says that a is an eigen-vector, and as a was arbitrary, every vector is an eigen-vector. Let also $[b] \neq [a] \in \mathbb{P}^n$. Then there is an eigen-value c_b for b so that $Mb = c_b b$. But as every vector is an eigen-vector, $a + b$ is an eigen-vector. By linearity we have

$$M(a + b) = Ma + Mb = c_a a + c_b b$$

Thus $a + b$ is an eigen-vector iff $c_a = c_b = c$, and thus as a, b were arbitrary every eigen-vector has the same eigen-value. Thus for some $c \in \mathbb{C}$ we have $M = cI$. $\square$

Lecture 21. March 2, 2011

Classifying projective conics. Now that we have the notion of a projective change of coordinates, we will classify homogeneous forms of degree 2 in 3 variables; i.e., we will classify projective plane conics.

The result is that up to a projective change of coordinates, a form $0 \neq F \in \mathbb{C}[x, y, z]$ of degree 2 is either:

(a) $F = xy - z^2$;
(b) $F = xy$; or
(c) $F = x^2$

These are exactly the three cases asserted in Lecture 19.2.

We will do this first under the following assumptions. Let $F \in \mathbb{C}[X, Y, Z]$ be a non-zero form of degree 2. First, $Z_{\mathbb{P}^2}(F)$ is infinite (this is because of Exercise 19.2). Second, for each point $p \in Z_{\mathbb{P}^2}(F)$, there is a form L_p defining a line containing p such that p is the only point of $Z_{\mathbb{P}^2}(F)$ on that line. (We will justify this later.)

So, first assume that F is not irreducible; i.e., F is reducible. Since F has degree 2, then, by Exercise 21.1, $F = AB$ for linear forms A and B. If $Z_{\mathbb{P}^2}(A) = Z_{\mathbb{P}^2}(B)$, then $A = cB$ for a nonzero constant c, and we can choose a coordinate system specified by linear forms x, y, and z in which $x = \sqrt{c}B$, and in which y and z are any two additional linear forms such that $\{x, y, z\}$ are linearly independent. Then $F = AB = cB^2 = x^2$.

If $Z_{\mathbb{P}^2}(A) \neq Z_{\mathbb{P}^2}(B)$, then A is not a non-zero multiple of B, so A and B are linearly independent. This time we pick $x = A$, $y = B$ and extend this to a basis $\{x, y, z\}$ of the linear forms. Now $F = xy$.

Finally, assume F is irreducible. Since $Z_{\mathbb{P}^2}(F)$ is infinite, we can pick distinct points $p, q \in Z_{\mathbb{P}^2}(F)$. Let $x = L_p$, $y = L_q$, and let $z = 0$ be the equation of the line through p and q. Let r be the point where L_p and L_q meet. Since by assumption, $L_p \cap Z_{\mathbb{P}^2}(F) = \{p\}$ and $L_q \cap Z_{\mathbb{P}^2}(F) = \{q\}$, we see that $r \notin Z_{\mathbb{P}^2}(F)$ and we also see that neither of the points p and q is on both lines $L_p = 0$ and $L_q = 0$. Thus $L_p = 0$ and $L_q = 0$ are different lines and hence p, q and r are 3 distinct points, and not collinear. If x, y and z were dependent, there would be constants a, b, c, not all 0, such that $cx + by + cz = 0$. Evaluating at p gives $a0 + by(p) + c0 = 0$, since $p \in \{x = 0\} \cap \{z = 0\}$. But $p \notin \{y = 0\}$, so $b = 0$. Evaluating at q gives $a = 0$, and evaluating at r gives $c = 0$. This shows that x, y, and z are linearly independent and hence define a coordinate system on $\mathbb{P}^2$. The coordinates of p, q and r in this coordinate system are, respectively, $[(0, 1, 0)]$, $[(1, 0, 0)]$, and $[(0, 0, 1)]$.

Therefore we can write F as a linear combination $F = ax^2 + bxy + cy^2 + dxz + eyz + fz^2$. We have $0 = F(p) = F(0, 1, 0) = c$, $0 = F(q) = F(1, 0, 0) = a$, and $0 \neq F(r) = f$. Thus $F = bxy + dxz + eyz + fz^2$.

Now use the fact that the only common zero of F and y is q. Solving $F = 0$ and $y = 0$ simultaneously gives $F = dxz + fz^2$, which has $(-f, 0, d)$ as a root. Since $L_q \cap Z_{\mathbb{P}^2}(F) = \{q\}$, we see that $[(-f, 0, d)] = [(1, 0, 0)]$, hence $d = 0$. Likewise, solving $F = 0$ and $x = 0$ simultaneously gives $e = 0$.

Thus $F = bxy + fz^2$. Since F is irreducible we cannot have $b = 0$. Replacing x by x/b and z by $iz/\sqrt{f}$ gives $F = xy - z^2$.

We still have to justify that for each point $p \in Z_{\mathbb{P}^2}(F)$, there is a form L_p defining a line containing p such that p is the only point of $Z_{\mathbb{P}^2}(F)$ on that line.

Exercises:

Exercise 21.1. If $F \in \mathbb{C}[x_0, \ldots, x_n]$ is a non-zero homogeneous polynomial and $G \in \mathbb{C}[x_0, \ldots, x_n]$ is a factor of F, show that G is homogeneous.

Solution by Katie Morrison. Since G is a factor of F, there exists an $H \in \mathbb{C}[x_0, \ldots, x_n]$ such that $F = GH$. Let m_G be the degree of the homogeneous component of G of least degree, and let m_H be the degree of the homogeneous component of H of least degree. Then the component of least degree in GH will have degree $m_G m_H$, and the product of other components of G and H will have strictly larger degree. But $F = GH$ is homogeneous so there is only one component and it must have degree $m_G m_H$. Thus, G and H can only have one component each as well, and so G is homogeneous. □

Lecture 22. March 4, 2011

Classifying projective conics (cont.). Note: Class began with jason presenting Problem 18.3.

To finish our classification of conics, given an irreducible form $F \in \mathbb{C}[x, y, z]$ of degree 2, we need to verify for each point $p \in Z(F) \subset \mathbb{C}^3$ that there is a linear form L_p such $Z_{\mathbb{P}^2}(F, L_p) = \{[p]\}$. (In fact, L_p is the form defining the tangent line to $Z_{\mathbb{P}^2}(F)$ at p.)

So let $[p] \in Z_{\mathbb{P}^2}(F)$. To define L_p (without reference to tangent lines), pick any two linearly independent linear forms u and v which both vanish at $[p]$. Pick any third linear form w that does not vanish at $[p]$. Then u, v and w are linearly independent. (If not we have scalars a, b, c, not all 0, such that $au + bv + cw = 0$, but evaluation at $[p]$ gives $0 = au(p) + bv(p) + cw(p) = cw(p)$, hence $c = 0$ since $w(p) \neq 0$. Thus $au + bv = 0$, but we chose u and v to be independent.)

Using this coordinate system, we can write $F = au^2 + buv + cv^2 + duw + evw + fw^2$ for some scalars $a, \ldots, f$. Since $F(p) = 0$, and sicne $u(p) = 0 = v(p)$, we have $f = 0$. If $d = e = 0$, then F factors (no form in 2 variables is ever irreducible unless it's linear). Thus either $d \neq 0$ or $e \neq 0$. Let $L_p = du + ev$, and assume $e \neq 0$; the argument in case $d \neq 0$ is similar.

Now solve the system $F = 0, L_p = 0$. Since we assume $L_p = 0$, we can write $v = -du/e$. Substitute into F to get $0 = F = (a-(bd/e)+c(d/e)^2)u^2$. If $a-(bd/e)+c(d/e)^2 = 0$, then $Z_{\mathbb{P}^2}(L_p) \subseteq Z_{\mathbb{P}^2}(F)$, hence by the projective Nullstellensatz $F \in \sqrt{(L_p)} = (L_p)$, so $L_p|F$, contradicting having F be irreducible. Thus $u^2 = 0$, so $u = 0 = v$, hence the only solution is $[p]$; i.e., $Z_{\mathbb{P}^2}(F, L_p) = [p]$.

Exercises:

Exercise 22.1. Let $F \in \mathbb{C}[x, y, z]$ be an irreducible form of degree 2 and let $[p] \in Z_{\mathbb{P}^2}(F)$. Show that, up to multiplication by scalars, L_p is the only linear form vanishing at $[p]$ such that $Z_{\mathbb{P}^2}(F, L_p) = [p]$.

Solution. Pick a coordinate system x, y, z such that $L_p = x$ and let $[p] = Z_{\mathbb{P}^2}(x, y)$. Let $L = ax+by+cz$ be a linear form which is not a scalar multiple of L_p and write $F = dx^2+exy+fy^2+gxz+hyz+iz^2$. Since $F([p]) = 0$ we have $i = 0$. The restriction of $F = 0$ to the line $x = 0$ gives $fy^2 + hyz = 0$, and since $Z_{\mathbb{P}^2}(F, L_p) = [p]$, we see that $h = 0$. Thus $F = dx^2 + exy + fy^2 + gxz$ and since F is irreducible, then $f \neq 0$ and $g \neq 0$. In order for $L([p]) = 0$ we need $c = 0$. Since L is not a scalar multiple of L_p, we must have $b \neq 0$. Dividing L by b allows us to reduce to the case that $L = ax+y$. Solving $F = 0$ with $L = 0$ gives $y = -ax$ and $dx^2 - aex^2 + a^2fx^2 + gxz = 0$ and hence either $x = 0$ (which gives us $[p] \in Z_{\mathbb{P}^2}(F, L)$) or $(d - ae + a^2f)x + gz = 0$ which has the solution $[(1, -a, 0)]$ if $d - ae + a^2f = 0$ or $[(-g, ag, d - ae + a^2f)]$ if $d - ae + a^2f \neq 0$. Either way, $Z_{\mathbb{P}^2}(F, L)$ is not just $[p]$. □

Lecture 23. March 7, 2011

Maps of projective algebraic sets. It is natural to mimic what we did for affine algebraic sets in trying to define algebraic maps of projective algebraic sets. If we do this we would want to say that a map $f : V \to W$ of projective algebraic sets $V \subseteq \mathbb{P}^N$ and $W \subseteq \mathbb{P}^M$ is the restriction of V of a mapping $F : \mathbb{P}^N \to \mathbb{P}^M$, where $F = (F_0, \ldots, F_M)$ in which each F_i is a polynomial in $\mathbb{C}[\mathbb{P}^N]$. In order for F to be well-defined, we need: each F_i to be homogeneous; we need the degree of each F_i which is not the 0 polynomial to be the same; and we need $Z_{\mathbb{P}^N}(F_0, \ldots, F_M) = \varnothing$.

But it turns out this is not enough to get a good notion of maps of projective algebraic sets, as the next two examples will help us to see.

Example 23.1. Let $\mathbb{C}[\mathbb{P}^1] = \mathbb{C}[a, b]$ and let $\mathbb{C}[\mathbb{P}^2] = \mathbb{C}[x_0, x_1, x_2]$. Consider $F : \mathbb{P}^1 \to \mathbb{P}^2$ where $F = (F_0, F_1, F_2)$ with $F_0 = ab$, $F_1 = a^2$ and $F_2 = b^2$. Note that the F_i all are homogeneous of degree 2, and that if $F_1 = 0$ and $F_2 = 0$, then $a = 0$ and $b = 0$ so $Z_{\mathbb{P}^N}(F_0, F_1, F_2)$ is empty, and F gives a well-defined homomorphism of $\mathbb{P}^1$ into $\mathbb{P}^2$. In addition, F defines a homomorphism $F^* : \mathbb{C}[\mathbb{P}^2] \to \mathbb{C}[\mathbb{P}^1]$ in the usual way, by sending F_i to x_i. The kernel of F^* is $(x_0^2 - x_1x_2)$, and $x_0^2 - x_1x_2$ is in fact the equation of the image of $\mathbb{P}^1$ under F. The map F is bijective to its image $C = F(\mathbb{P}^1)$ and we'll eventually see that C is isomorphic to $\mathbb{P}^1$, but the homomorphism $\overline{F^*} : \mathbb{C}[\mathbb{P}^2]/I(C) \to \mathbb{C}[\mathbb{P}^1]$ induced by F^* is not an isomorphism. Thus the connection between homogeneous coordinate rings and projective algebraic sets is less direct than is the connection between coordinate rings and affine algebraic sets.

Example 23.2. Again let $\mathbb{C}[\mathbb{P}^1] = \mathbb{C}[a, b]$ and let $\mathbb{C}[\mathbb{P}^2] = \mathbb{C}[x_0, x_1, x_2]$. Consider another map $F : \mathbb{P}^1 \to \mathbb{P}^2$ where this time $F = (F_0, F_1, F_2)$ with $F_0 = a$, $F_1 = b$ and $F_2 = 0$. Note that the non-zero F_i both are homogeneous of degree 1, and that if $F_0 = 0$ and $F_1 = 0$, then $a = 0$ and $b = 0$ so $Z_{\mathbb{P}^N}(F_0, F_1, F_2)$ is again empty, and F gives a well-defined homomorphism of $\mathbb{P}^1$ into $\mathbb{P}^2$. The equation of the image $C = F(\mathbb{P}^1)$ of F is $x_2 = 0$, and (x_2) is the kernel of the homomorphism $F^* : \mathbb{C}[\mathbb{P}^2] \to \mathbb{C}[\mathbb{P}^1]$. In fact we get an isomorphism $\mathbb{C}[\mathbb{P}^2]/I(C) \cong \mathbb{C}[\mathbb{P}^1]$, so we might expect C and $\mathbb{P}^1$ to be isomorphic, and once we define things correctly, they will be.

The curves C in the preceding two examples turn out both to be isomorphic to $\mathbb{P}^1$, but the first example shows that the homogeneous coordinate ring is not enough to detect this, and in both examples there is no well-defined map $G : \mathbb{P}^2 \to \mathbb{P}^1$ defined by homogeneous polynomials whose restriction to C is the inverse of F. In fact, the only well-defined map $G : \mathbb{P}^2 \to \mathbb{P}^1$ defined by homogeneous polynomials are the constant maps.

We now justify this. Certainly if $G = (G_0, G_1)$ where $G_i \in \mathbb{C}$ for both i (and where the G_i are not both 0) is a well-defined map $\mathbb{P}^2 \to \mathbb{P}^1$, but it is the constant map that sends every point of $\mathbb{P}^2$ to the point (G_0, G_1). Suppose G_0 or G_1 is not a constant. Suppose for example, that G_0 is not a constant. Then G_0 is a homogeneous polynomial of some degree $d > 0$. As noted above, for G to be well-defined, G_1 is either the 0 polynomial or is homogeneous of degree d. If G_1 is the 0 polynomial, then for each $p \in \mathbb{P}^2$ where $G_0(p) \neq 0$, $G(p) = [(1, 0)]$, and for each $p \in Z_{\mathbb{P}^2}(G_0)$, $G(p) = [(0, 0)]$, which is undefined. I.e., at those points where G is defined, it's constant. So we would be in the worst of all possible worlds: G is both constant and (since by the projective Nulstellensatz $Z_{\mathbb{P}^2}(G_0) \neq \varnothing$) not well-defined!

Thus G_1 is not a constant, hence G_1 is a homogeneous polynomial of degree d. If G_0 and G_1 have a non-constant common factor F, then F is homogeneous by Exercise 21.1 and we have $\varnothing \neq Z_{\mathbb{P}^2}(F) \subseteq Z_{\mathbb{P}^2}(G_0, G_1)$, so G is not well-defined. More generally, since $(0, 0, 0) \in Z_{\mathbb{A}^3}(G_0, G_1)$, it follows that $Z_{\mathbb{A}^3}(G_0, G_1) \neq \varnothing$, and we will see that every irreducible component of $Z_{\mathbb{A}^3}(G_0, G_1)$ has dimension at least 1 (see Exercise 38.5). Since for every point $p \in Z_{\mathbb{A}^3}(G_0, G_1)$, the line L_p through the origin which also goes through p is contained in $Z_{\mathbb{A}^3}(G_0, G_1)$, it follows that L_p represents a point of $Z_{\mathbb{P}^2}(G_0, G_1)$, and hence $Z_{\mathbb{A}^3}(G_0, G_1) \neq \varnothing$. Thus G is not well-defined.

Remark 23.3. For any two homogeneous polynomials G_0 and G_1, Bézout's Theorem states that the number of points of $Z_{\mathbb{P}^2}(G_0, G_1)$ is infinite if G_0 and G_1 have a non-constant common factor, and otherwise $Z_{\mathbb{P}^2}(G_0, G_1)$ consists of exactly $\deg(G_0)\deg(G_1)$ points, if the points are counted with multiplicity. In either case Bézout implies that $Z_{\mathbb{P}^2}(G_0, G_1)$ is non-empty unless one of the G_i is a non-zero constant. Thus, if we allow ourselves to use Bézout's Theorem, we get a shorter way to show that no non-constant map $G : \mathbb{P}^2 \to \mathbb{P}^1$ is well-defined.)

Since there is no map $G : \mathbb{P}^2 \to \mathbb{P}^1$, we cannot get an isomorphism $C \to \mathbb{P}^1$ using only maps defined by homogeneous polynomials. The resolution to the problem is to define a more flexible notion of algebraic map. We do this by working locally.

Exercises:

Exercise 23.1. Consider the map F of Example 23.1. Show that $\mathrm{Im}(F) = Z_{\mathbb{P}^2}(x_0^2 - x_1x_2)$ and that $\ker(F^*) = (x_0^2 - x_1x_2)$, but that $\overline{F^*}$ is not an isomorphism.

Solution. First, $\mathrm{Im}(F) \subseteq Z_{\mathbb{P}^2}(x_0^2 - x_1x_2)$, since $F([(a, b)]) = [(ab, a^2, b^2)]$ satisfies $(ab)^2 - a^2b^2 = 0$, which also shows that $(x_0^2 - x_1x_2) \subseteq \ker(F^*)$. Conversely, say $[(c, d, e)] \in Z_{\mathbb{P}^2}(x_0^2 - x_1x_2)$. If $d = 0$, then $c^2 - de = 0$ implies $c = 0$, and we have $[(c, d, e)] = [(0, 0, 1)] = F([(0, 1)])$. If $d \neq 0$, let $b = c/d$ and let $a = 1$. Then $F([(a, b)]) = F([(1, b)]) = [(b, 1, b^2)] = [(c, d, db^2)]$, but $c^2 = de$ implies $e = c^2/d = b^2d$, so $[(c, d, db^2)] = [(c, d, e)]$. Thus $\mathrm{Im}(F) = Z_{\mathbb{P}^2}(x_0^2 - x_1x_2)$.

Note that $F^*(x_i)$ is homogeneous of degree 2 for each i. Thus if $H \in \mathbb{C}[x_0, x_1, x_2]$ and we write H as a sum $H = H_0 + \cdots + H_d$ of its homogeneous components, then for each non-zero term H_j, $F^*(H_j)$ is homogeneous of degree $2\deg(H_j)$. Thus $H \in \ker(F^*)$ if and only if $H_j \in \ker(F^*)$ for each j. In particular, $\ker(F^*)$ is a homogeneous ideal. Thus to show $\ker(F^*) = (x_0^2 - x_1x_2)$, given that we already have seen $(x_0^2 - x_1x_2) \subseteq \ker(F^*)$, it suffices to show $F^*(H) = 0$ implies $x_0^2 - x_1x_2$ divides H whenever H is homogeneous. But $F^*(H) = 0$ implies $Z_{\mathbb{P}^2}(x_0^2 - x_1x_2) = \mathrm{Im}(F) \subseteq Z_{\mathbb{P}^2}(H)$, hence by Theorem 19.1.5, the projective Nullstellensatz, that $H \in \sqrt{(x_0^2 - x_1x_2)}$, but $\sqrt{(x_0^2 - x_1x_2)} = (x_0^2 - x_1x_2)$ since $x_0^2 - x_1x_2$ is irreducible. (To see irreducibility, note that any factor of $x_0^2 - x_1x_2$

is homogeneous by Exercise 21.1. Thus were $x_0^2 - x_1x_2$ not to be irreducible, it would be a product of two linear forms, say $x_0^2 - x_1x_2 = LM$. But $Z_{\mathbb{P}^2}(L, M)$ consists of the point p where the lines defined by L and M cross. Also note that the gradient of LM is $\nabla(LM) = L\nabla(M) + M\nabla(L)$, hence vanishes at p. But $\nabla(x_0^2 - x_1x_2) = (2x_0, -x_2, -x_1)$ never vanishes. Thus $x_0^2 - x_1x_2$ cannot be the product of two linear forms and so is irreducible. In language we'll see later on, $Z_{\mathbb{P}^2}(x_0^2 - x_1x_2)$ is smooth, but a reducible conic $Z_{\mathbb{P}^2}(LM)$ is not.)

Finally, $\overline{F^*}$ is not an isomorphism, since the image of each variable is homogeneous of degree 2. Thus neither a nor b is in the image, so $\overline{F^*}$ is not onto. □

Exercise 23.2. If $I \subset \mathbb{C}[\mathbb{P}^N]$ is a homogeneous ideal and if Q is a minimal prime ideal containing I, show that Q is homogeneous. [Hint: apply Exercise 6.4.]

Solution. Let Q be minimal among all prime ideals containing I; i.e., if $I \subseteq P \subseteq Q$ with P prime, then $P = Q$. Let H be the ideal generated by all homogeneous elements of Q. Then H is homogeneous and $I \subseteq H \subseteq Q$. Say $FG \in H$. Then Q being prime tells us either F or G is in Q; say $F \in Q$. Then every homogeneous component of F is in Q hence in H, so $F \in H$. Thus H is prime, hence $H = Q$. [Note: We don't need the hint; I don't remember now what I had in mind to use the hint for. One thing it does do is tell us that $\sqrt{I}$ is the intersection of the minimal primes containing I, of which there are finitely many. Clearly, $\sqrt{I} \subseteq Q$, for each minimal prime Q containing I. By Exercise 6.4, $\sqrt{I}$ is a finite intersection of prime ideals, hence by Lemma 7.1, each Q is one of these ideals.] □

Lecture 24. March 9, 2011

To define a more flexible notion of algebraic map, we recall the notion of localization.

Localization. Let R be a commutative ring with $1 \neq 0$, let $S \subseteq R$ be a *multiplicatively closed* subset; i.e., if $a, b \in S$, then so is ab. For simplicity, we also assume $1 \in S$.

Define $S^{-1}R$ to be equivalence classes of all fractions of the form $\frac{r}{s}$, such that $r \in R$ and $s \in S$, where we say

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$$

if for some $s \in S$ we have $s(r_1s_2 - s_1r_2) = 0$. Then $S^{-1}R$ is a ring under the usual addition and multiplication operations on fractions, and we have a canonical homomorphism $R \to S^{-1}R$ defined by $r \mapsto \frac{r}{1}$.

Example 24.1. If $f \in R$, let $S = \{1, f, f^2, \ldots\}$. Then $S^{-1}R$ is denoted R_f and we have an isomorphism $R[t]/(tf - 1) \cong S^{-1}R$ induced by $r \mapsto \frac{r}{1}$ for all $r \in R$ and by $t \mapsto \frac{1}{f}$.

Example 24.2. Let $P \subset R$ be a prime ideal. Let $S = R \setminus P$. Then $S^{-1}R$ has a unique maximal ideal (which comes from P); we denote $S^{-1}R$ by R_P. (A ring with a unique maximal ideal is sometimes called a *local ring*. N.B.: Some people use local ring only for Noetherian rings with a unique maximal ideal.)

If P is a maximal ideal and $R = \mathbb{C}[V]$ for an affine algebraic set $V \subseteq \mathbb{A}^n$, then the elements of R_P can be regarded as *germs* of functions.

Definition 24.3. Given a function $f : X \to Y$ of topological spaces and a point $x \in X$, the germ of f at x is an equivalence class of functions defined on neighborhoods of x. If U_1 and U_2 are open neighborhoods of x, and if $g_i : U_i \to Y$ are functions, then we say g_1 and g_2 *represent the same germ* (or *have the same germ*) if for some open neighborhood $U_3 \subseteq U_1 \cap U_2$ of x we have $g_1|_{U_3} = g_2|_{U_3}$.

Example 24.4. Let $f : \mathcal{R} \to \mathcal{R}$ be the function $f(x) = |x|$. For each $\epsilon > 0$, let $g_\epsilon : \mathcal{R} \to \mathcal{R}$ be

$$g_\epsilon(x) = \begin{cases} |x| & \text{if } |x| \leq \epsilon, \\ \epsilon & \text{if } |x| \geq \epsilon. \end{cases}$$

Then f and g_ϵ for every $\epsilon > 0$ represent (or have) the same germ at $x = 0$.

Example 24.5. If $0 \in S$, then $S^{-1}R = \{0\}$. This is because we can use $s = 0$ in $s(r_1s_2 - s_1r_2) = 0$, and hence get $\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ for any two fractions; in particular, every fraction is equivalent to $\frac{0}{1}$.

Example 24.6. If R is a domain, then $R_{(0)}$ is a field. if $R = \mathbb{C}[V]$ for some irreducible affine algebraic set V, then we denote $R_{(0)}$ by $\mathbb{C}(V)$, and refer to it as the *function field* of V.

Example 24.7. It is easy to see that the homomorphism $R \to S^{-1}R$ is injective if R is a domain and $0 \notin S$, but otherwise injectivity can fail. For example, Let $V = Z(xy) \subset \mathbb{A}^2$, so V is the union of the coordinate axes. Let $\overline{x}$ be the image of x under the quotient $\mathbb{C}[\mathbb{A}^2] \to \mathbb{C}[V]$, where $\mathbb{C}[AAA^2] = \mathbb{C}[x, y]$ and $\mathbb{C}[V] = \mathbb{C}[x, y]/(xy)$ (note that $I(V) = (xy)$). Then $\mathbb{C}[V]_{\overline{x}} \cong \mathbb{C}[x]_x \cong \mathbb{C}[x, \frac{1}{x}]$ and $(\overline{y})$ is the kernel of $\mathbb{C}[V] \to \mathbb{C}[V]_{\overline{x}}$.

Exercises:

Exercise 24.1. Justify the claims made in Example 24.1.

Solution by Ashley Weatherwax. We'll start by refreshing what example 24.1.1 was. Let $f \in R$ and let $S = \{1, f, f^2, ...\}$. Then $S^{-1}R$ is denoted R_f and we have an isomorphism $R[t]/(tf - 1) \cong S^{-1}R$ induced by $r \mapsto \frac{r}{1}$ for all $r \in R$ and by $t \mapsto \frac{1}{f}$.

Define as above $h : R[t] \to S^{-1}R$ by $r \mapsto \frac{r}{1}$ and $t \mapsto \frac{1}{f}$. Then we get an induced map $\phi : R[t]/(tf - 1) \to S^{-1}R$. Clearly, h is a homomorphism, and we know this induced map is well defined, as $(tf - 1) \subset \ker h$.

Now define a map $g : R \to R[t]/(tf - 1)$, defined by $r \mapsto r$. Then $g(f) = f$, which is a unit in $R[t]/(tf - 1)$. So by the universal property of localization, there is a unique homomorphism $\psi : S^{-1}R \to R[t]/(tf - 1)$, which sends $\frac{r}{f^k} \mapsto g(r)g(f^k)^{-1} = rt^m$.

Claim: $\phi \circ \psi = id_{S^{-1}R}$ and $\psi \circ \phi = id_{R[t]/(tf-1)}$

Let $\frac{r}{f^k} \in S^{-1}R$. Then

$$\phi \circ \psi(\frac{r}{f^k}) = g(r)g(f^k)^{-1} = \phi(rf^{-k}) = rf^{-k} = \frac{r}{f^k}$$

Let $[a_0 + a_1t + a_2t^2 + ... + a_kt^k] \in R[t]/(tf - 1)$. Then

$$\psi \circ \phi([a_0 + ... + a_kt^k]) = \psi(a_0 + \frac{a_1}{f} + ... + \frac{a_k}{f^k}) = a_0 + a_1f^{-1} + ... + a_kf^{-k}$$

But as $f^{-1} = t$, this is equal to

$$\psi \circ \phi([a_0 + ... + a_kt^k]) = a_0 + a_1t + ... + a_kt^k$$

Then as ϕ has an inverse, it is an isomorphism. □

Exercise 24.2. Suppose we defined

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$$

by the condition that $r_1s_2 - s_1r_2 = 0$. Show that this need not be an equivalence relation by giving two examples. In one example, let $0 \in S$ for any R and S of your choice. For the other example, take $R = \mathbb{C}[x, y]/(xy)$ and $S = \{1, x, x^2, \ldots\}$.

Solution by Anisah Nu'Man. Let $R = \mathbb{Z}$ and $S = \{0, 1, a, a^2, a^3, \ldots\}$ for any $a \in \mathbb{Z}$ with $a \neq 0$. Observe we have $\dfrac{1}{0} \sim \dfrac{0}{0}$ since $1(0) = 0(0) = 0$ and $\dfrac{0}{0} \sim \dfrac{0}{a}$ since $0(a) - 0(0) = 0$. Yet $\dfrac{1}{0} \nsim \dfrac{0}{a}$ since $1(a) - 0(0) = a \neq 0$.

Now let $R = \mathbb{C}[x,y]/(xy)$ and $S = \{1, x, x^2, \dots\}$. Observe we have $\dfrac{y^2}{x} \sim \dfrac{0}{x}$ since $y^2(x) - x(0) = y(yx) - 0 = 0$ and $\dfrac{0}{x} \sim \dfrac{y}{1}$ since $0(1) - x(y) = 0 - xy = 0 - 0 = 0$. Yet $\dfrac{y^2}{x} \nsim \dfrac{y}{1}$ since $y^2(1) - xy = y^2 - 0 = y^2 \neq 0$. □

Exercise 24.3. Show that $(\overline{y})$ is the kernel of the homomorphism $\mathbb{C}[V] \to \mathbb{C}[V]_{\overline{x}}$ in Example 24.7 and that $\mathbb{C}[V]_{\overline{x}} \cong \mathbb{C}[x]_x$.

Solution by Zheng Yang. First, $\mathbb{C}[x,y]/(xy)_{\overline{x}} \cong \mathbb{C}[x,y,t]/(xy, tx-1) \cong \mathbb{C}[x,y,t]/(xy, tx-1, txy) \cong \mathbb{C}[x,y,t]/(xy, tx-1, y) \cong \mathbb{C}[x,t]/(tx-1) \cong \mathbb{C}[x]_x$. The kernel of the localization map $R \to S^{-1}R$ is $\{r : rs = 0\}$ for some $s \in S$. Here $S = \{1, x, x^2, \dots\}$, so the kernel is $(\overline{y})$. □

Lecture 25. March 11, 2011

The structure sheaf (or the sheaf of regular functions). Let $V \subseteq \mathbb{A}^n$ be an irreducible closed subset. For each non-empty open subset U of V define $\mathcal{O}_V(U)$ to be $\cap_{p \in U} \mathbb{C}[V]_{I_V(p)} \subset \mathbb{C}(V)$. For the empty set, define $\mathcal{O}_V(\varnothing) = 0$. Elements of $\mathbb{C}(V)$ are called rational functions. If $p \in V$ and if a rational function f is in $\mathbb{C}[V]_{I_V(p)}$, we say f is *regular* at p. The elements of $\mathcal{O}_V(U)$ are precisely the rational functions regular at each point $p \in U$, so we call $\mathcal{O}_V(U)$ the ring of regular functions on U (or the ring of functions regular on U).

It is not in general easy to determine $\mathcal{O}_V(U)$, given an open subset $U \subseteq V$. There are important cases where $\mathcal{O}_V(U)$ is known.

Lemma 25.1. *Let $V \subseteq \mathbb{A}^n$ be an irreducible closed subset. Let $f \in \mathbb{C}[V]$ and let $U_f = V \setminus Z_V(f)$. Then $\mathcal{O}_V(U_f) = \mathbb{C}[V]_f$.*

Proof. This is true by definition if $f = 0$, so assume $f \neq 0$. Since $p \in U_f$ implies $f(p) \neq 0$, we have $f \notin I_V(p)$. Thus $\frac{g}{f^m} \in \mathbb{C}[V]_{I_V(p)}$ for all $g \in \mathbb{C}[v]$ and all $m > 0$. Hence $\mathbb{C}[V]_f \subseteq \mathcal{O}_V(U_f)$.

Now say $h \in \mathcal{O}_V(U_f)$. Thus for each $p \in U_f$ we have $h = \frac{g_p}{f_p}$, where $g_p \in \mathbb{C}[V]$ and $f_p \notin I_V(p)$. Thus $Z_V(\{f_p : p \in U_f\}) \cap U_f = \varnothing$, so $Z_V(\{f_p : p \in U_f\}) \subseteq Z_V(f)$, hence $f \in \sqrt{((\{f_p : p \in U_f\})}$. Therefore, $f^m = a_{p_1} f_{p_1} + \cdots a_{p_r} f_{p_r}$ for some elements $a_{p_i} \in \mathbb{C}[V]$ and points $p_i \in U_f$, so $f^m h = a_{p_1} f_{p_1} h + \cdots a_{p_r} f_{p_r} h = a_{p_1} f_{p_1} \frac{g_{p_1}}{f_{p_1}} + \cdots a_{p_r} f_{p_r} \frac{g_{p_r}}{f_{p_r}} = a_{p_1} g_{p_1} + \cdots a_{p_r} g_{p_r}$. Call this g; then $g \in \mathbb{C}[V]$ and $h = \frac{g}{f^m} \in \mathbb{C}[V]_f$, so $\mathcal{O}_V(U_f) \subseteq \mathbb{C}[V]_f$. □

Example 25.2. Let V be an irreducible closed subset of $\mathbb{A}^n$. Then $\mathcal{O}_V(V) = \mathbb{C}[V]$. Just take $f = 1$, using the fact that $\mathbb{C}[V]_1 = \mathbb{C}[V]$.

Example 25.3. Let $U = \mathbb{A}^2 \setminus \{(0,0)\}$. Then $\mathcal{O}_{\mathbb{A}^2}(U) = \mathbb{C}[\mathbb{A}^2] = \mathbb{C}[x,y]$. By definition, $\mathbb{C}[\mathbb{A}^2] \subseteq \mathcal{O}_{\mathbb{A}^2}(U)$, so let $h \in \mathcal{O}_{\mathbb{A}^2}(U)$. Then $h|_{U_x} \in \mathbb{C}[\mathbb{A}^2]_x$ and $h|_{U_y} \in \mathbb{C}[\mathbb{A}^2]_y$, hence in $\mathbb{C}(\mathbb{A}^2)$ we can write $h = \frac{f}{x^m} = \frac{g}{y^n}$ for some $f, g \in \mathbb{C}[\mathbb{A}^2]$ and some $m, n \geq 0$. Thus $y^n f = x^m g$, so by unique factorization we have $f = \phi x^m$ and $g = \gamma y^n$ and $h = \phi = \gamma \in \mathbb{C}[\mathbb{A}^2]$.

Example 25.4. It can happen that $\mathcal{O}_V(U)$ is not a finitely generated $\mathbb{C}$-algebra (see A. Neeman, *Steins, affines and Hilbert's fourteenth problem*, Ann. of Math. 127 (1988), 229–244, for example) or even Noetherian. One of the most famous examples is one of (if not the) first, due to D. Rees (*On a problem of Zariski*, Illinois J. Math. 2 (1958), 145–149). Rees constructed a ring $A = \mathbb{C}[V]$ and an open subset $U = V \setminus Z_V(I)$ such that $B = \mathcal{O}_V(U)$, which is of the form (in his notation) $\cup_n I^{-n}$, is not a finitely generated $\mathbb{C}$-algebra, or even a Noetherian ring.

Exercises:

Exercise 25.1. A topological space X is said to be *quasi-compact* if every open cover has a finite subcover. (Some people reserve the use of the word compact to mean quasi-compact and Hausdorff.) Show that every open subset of an algebraic set is quasi-compact.

Solution by Jason Hardin. Let $V \subseteq \mathbb{A}^n$ be an algebraic set and $U \subseteq V$ be an open subset. Let $\{U_i\}_{i\in I}$ be an open cover for U. So $U \subseteq \cup_{i\in I} U_i$. This means that $\cap_{i\in I}(V\backslash U_i) \subseteq (V\backslash U)$. Since $V\backslash U_i$ is a closed subset of V, by the definition of the subspace topology it has the form $V\backslash U_i = Z(J_i)\cap V$, where $J_i \subseteq \mathbb{C}[x_1,\ldots,x_n]$ is an ideal. Now we have

$$\begin{aligned}\cap_{i\in I}(V\backslash U_i) &= \cap_{i\in I}(Z(J_i)\cap V) = \cap_{i\in I}(Z(J_i))\cap V = Z((\cup_{i\in I} J_i))\cap V\\ &= Z(f_{i_1},\ldots,f_{i_t})\cap V,\end{aligned}$$

where $f_{i_j} \in J_{i_j}$. Let $I' = \{i_1,\ldots,i_t\} \subseteq I$. Then

$$V\backslash U \supseteq \cap_{i\in I}(V\backslash U_i) = Z(f_{i_1},\ldots,f_{i_t})\cap V = \cap_{i\in I'}(Z(J_i)\cap V) = \cap_{i\in I'}(V\backslash U_i),$$

i.e., $U \subseteq \cup_{i\in I'} U_i$. So $\{U_i\}_{i\in I'}$ is a finite subcover of $\{U_i\}_{i\in I}$, and hence U is quasi-compact. □

Exercise 25.2. Show that the open subsets of the form U_f give a basis for the Zariski topology on an algebraic set V.

Solution 1, by Philip Gipson. Since the Zariski topology is formed by declaring $\{Z(J) : J \subseteq \mathbb{C}[V]\}$ to be the closed sets and $U_f = V \setminus Z_V(f)$ it is enough to show that the closed sets $\{U_f^c\} = \{Z_V(f)\}$ generates $\{Z(J) : J \subseteq \mathbb{C}[V]\}$.
To that end let J be any ideal in $\mathbb{C}[V]$. Since $\mathbb{C}[V]$ is noetherian J is finitely generated $J = \langle f_1, ..., f_n\rangle$. Thus $Z_V(J) = Z_V(f_1, ..., f_n) = \bigcap Z_V(f_i)$ and so we conclude that $\{Z_V(f)\}$ generates $\{Z(J)\}$ and thus is a basis for the topology. □

Solution 2, by Kat Shultis. We first check that the collection of sets of the form U_f form a basis. Notice that the polynomial 0 is zero everywhere, and so $U_0 = \emptyset$. Also, the polynomial 1 is zero nowhere, so for every $v \in V$, $v \in U_1 = V$. Now, let $v \in U_f \cap U_g$. This means that $f(v) \neq 0$ and $g(v) \neq 0$. Thus, $(fg)(v) \neq 0$. If $w \in U_{fg}$ then $(fg)(w) \neq 0$ so that $f(w) \neq 0$ and $g(w) \neq 0$, so that $v \in U_{fg} \subseteq U_f \cap U_g$. Thus, the sets U_f form a basis of some topology.

We must now check that the basis topology given by the sets of the form U_f is the Zariski topology. Let U be a set that is open in the basis topology. Then $U = \cup_\alpha U_{f_\alpha}$ for some collection $\{f_\alpha\}$. By definition, each U_f is open in the Zariski topology, and so each open set in the basis topology is also open in the Zariski topology. Now, let U be an open set in the Zariski topology. Thus, U is of the form $V \setminus Z_V(T)$ for some collection of polynomials T. However, we can write this as $U = \cup_{s\in U} U_{f_s}$ where f_s does not vanish at s. Thus, every open set in the Zariski is a union of basis elements, and so, we have that Zariski open sets are also open in the basis topology. Hence, the basis topology is the Zariski topology. □

Lecture 26. March 14, 2011

What is a sheaf? Let X be a topological sapce. We can regard the topology as specifying a category whose objects are the open subsets and whose arrows are the inclusion maps. If you are comfortable with category theory, a sheaf of abelian groups is then a contravariant functor to the category of abelian groups, but the functor must satify some conditions which essentially say that the "sections" are determined "locally".

Thus a sheaf $\mathcal{S}$ (of abelian groups) on X is a certain assignment of an abelian group $\mathcal{S}(U)$ for every open subset $U \subseteq X$. We refer to the elements of $\mathcal{S}(U)$ as *sections* of $\mathcal{S}$ over U, or *global sections* if $U = X$. For each inclusion $U_2 \subseteq U_1$ we have the "restriction" homomorphism $\rho_{12} : \mathcal{S}(U_1) \to \mathcal{S}(U_2)$. If $f \in \mathcal{S}(U_1)$, it is common to write $f|_{U_2}$ for $\rho_{12}(f)$. (This is just formal

notation, motivated by the example of sheaves of the type $\mathcal{O}_V$ where sections over open sets $U \subseteq V$ are actual functions $U \to \mathbb{C}$, since it makes sense to restrict a function on an open set to an open subset.) Moreover, if $U_2 = U_1$, then ρ_{12} is the identity. If $U_3 \subseteq U_2$, then $\rho_{23}\rho_{12} = \rho_{13}$. If $U = \varnothing$, then $\mathcal{S}(U) = 0$. So far, this just says that $\mathcal{S}$ is a contravariant functor.

In addition, we require that sections be determined locally. I.e., if $\{U_i\}$ is an open cover of an open set U, and if $f, g \in \mathcal{S}(U)$ such that $f|_{U_i} = g|_{U_i}$ for all i, we require that $f = g$, and if there are sections $f_i \in \mathcal{S}(U_i)$ for all i, such that $f_i|_{U_i \cap U_j} = f_j|_{U_j \cap U_i}$ for all i and j, then we require that there is a section $f \in \mathcal{S}(U)$ such that $f|_{U_i} = f_i$ for all i.

Example 26.1. If V is an affine algebraic set, it's not hard to check that $\mathcal{O}_V$ is a sheaf.

We can now enlarge the class (or category) objects we can deal with.

Definition 26.2. An irreducible Zariski-closed subset of $\mathbb{A}^n$ is called an affine *variety*. A *quasi-affine* variety is a non-empty Zariski-open subset of an affine variety.

Now that we have quasi-affine varieties, we need to define their morphisms.

Definition 26.3. Let V_1 and V_2 be affine varieties and let $U_i \subseteq V_i$ be quasi-affine varieties. A morphism $\phi : U_1 \to U_2$ is a continuous map such that for each point $p \in U_1$ there are affine open subsets $\phi(p) \in U_{\phi(p)} \subseteq V_2$ and $p \in U_p \subseteq \phi^{-1}(U_{f(p)}) \subseteq V_1$ such that ϕ^* (i.e., composition with ϕ) defines a $\mathbb{C}$-homomorphism $\mathcal{O}_{V_2}(U_{\phi(p)}) \to \mathcal{O}_{V_1}(U_p)$.

Lecture 27. March 16, 2011

Morphisms of quasi-affine varieties.

Example 27.1. Let $\phi : V \to W$ be an algebraic map of irreducible affine algebraic sets. Then ϕ is a morphism. By Proposition 12.6, ϕ is continuous. For each $p \in V$, take $U_p = V$ and $U_{\phi(p)} = W$. Since ϕ^* defines a $\mathbb{C}$-homomorphism $\mathbb{C}[W] \to \mathbb{C}[V]$, we see that ϕ is a morphism.

Example 27.2. Let $\phi : V \to W$ be a morphism of irreducible affine algebraic sets. Then ϕ is an algebraic map. Since ϕ is a morphism there are open subsets $p \in U_p \subseteq \phi^{-1}(U_{\phi(p)})$ and $\mathbb{C}$-homomorphisms $\phi^* : \mathcal{O}_W(U_{\phi(p)}) \to \mathcal{O}_V(U_p)$. Since U_p is affine, there is an element $f_p \in \mathbb{C}[V]$ such that $\mathcal{O}_V(U_p) = \mathbb{C}[V]_{f_p}$. Let $i_p : \mathbb{C}[W] \subseteq \mathcal{O}_W(U_{\phi(p)})$ be the canonical inclusion. Then we have $\mathbb{C}$-homomorphisms $\mathbb{C}[W] \xrightarrow{i_p} \mathcal{O}_W(U_{\phi(p)}) \xrightarrow{\phi^*} \mathcal{O}_V(U_p) = \mathbb{C}[V]_{f_p}$ which for simplicity we will refer to as ϕ_p^*.

Thus for any $h \in \mathbb{C}[W]$, we have $\phi_p^*(h) = \frac{g_p}{f_p^{m_p}}$ for elements $g_p \in \mathbb{C}[V]$. Note that

$$\frac{g_p}{f_p^{m_p}}\Big|_{U_p \cap U_q} = \phi_p^*(h)\big|_{U_p \cap U_q} = \frac{g_q}{f_q^{m_q}}\Big|_{U_q \cap U_p}$$

so in $\mathbb{C}(V)$ we have $\frac{g_p}{f_p^{m_p}} \frac{g_q}{f_q^{m_q}}$ for all p and q. Since $\{U_p\}$ is a cover of V, we have $Z_V(\{f_p : p \in V\}) = \varnothing$, so $1 = \sum_p a_p f_p^{m_p}$, where each $a_p \in \mathbb{C}[V]$ but only finitely many are non-zero. Let $\eta = \sum_p a_p g_p$. Then in $\mathbb{C}(V)$ we have

$$\eta = \sum_p a_p g_p = \sum_p a_p f_p^{m_p} \frac{g_p}{f_p^{m_p}} = \Big(\sum_p a_p f_p^{m_p}\Big) \frac{g_q}{f_q^{m_q}} = \frac{g_q}{f_q^{m_q}} = \phi_p^*(h),$$

and so $\phi_p^*(h) = \eta \in \mathbb{C}[V]$. Thus ϕ^* is a $\mathbb{C}$-homomorphism $\mathbb{C}[W] \to \mathbb{C}[V]$, so by Theorem 14.1, ϕ is an algebraic map.

Example 27.3. Let U be the quasi-affine variety $U = \mathbb{A}^1 \setminus \{0\}$ and let W be the affine variety $W = Z(xy - 1) \subset \mathbb{A}^2$. Then U and W are isomorphic. Let $f : U \to W$ be $f : s \mapsto (s, \frac{1}{s})$ and let $g : W \to V$ be $g : (a, b) \mapsto a$. It is easy to see that f and g are bijective, inverse to each other and continuous (since the U has the finite complement topology, being a subspace of $\mathbb{A}^1$,

as does W, by Exercise 10.2). If we take $\mathbb{C}[\mathbb{A}^1] = \mathbb{C}[t]$ and $\mathbb{C}[W] = \mathbb{C}[x,y]/(xy-1) \cong \mathbb{C}[x]_x$, it is also easy to see that $f^* : \mathbb{C}[W] \to \mathcal{O}_{\mathbb{A}^1}(U) = \mathbb{C}[\mathbb{A}^1]_t$ is the $\mathbb{C}$-homomorphism $x \mapsto t$ and $g^* : \mathcal{O}_{\mathbb{A}^1}(U) = \mathbb{C}[\mathbb{A}^1]_t \to \mathbb{C}[W]$ is the $\mathbb{C}$-homomorphism $t \mapsto x$, and hence f and g are morphisms and U and W are therefore isomorphic.

Exercises:

Exercise 27.1 (The Universal Property of Localization)**.** Given rings R and T, a multiplicatively closed subset $S \subset R$ and a homomorphism $f : R \to T$ such that $f(s)$ is a unit for every $s \in S$, show that there is a unique homormorphism $S^{-1}f : S^{-1}R \to T$ such that f factors as

$$R \xrightarrow{r \mapsto \frac{r}{1}} S^{-1}R \xrightarrow{S^{-1}f} T.$$

[Hint: consider $S^{-1}f : \frac{r}{s} \mapsto f(r)(f(s))^{-1}$.]

Solution by Becky Egg. Define $S^{-1}f : S^{-1}R \to T$ by $S^{-1}f(r/s) = f(r)f(s)^{-1}$. If $\frac{r}{s} \sim \frac{r'}{s'}$, then there exists $t \in S$ with $t(rs' - r's) = 0$. So $trs' = tr's$, and hence

$$f(t)f(r)f(s') = f(trs') = f(tr's) = f(t)f(r')f(s).$$

Since $f(t), f(s), f(s')$ are units of T, we have $f(r)f(s)^{-1} = f(r')f(s')^{-1}$, that is, $S^{-1}f(\frac{r}{s}) = S^{-1}f(\frac{r'}{s'})$. So $S^{-1}f$ is well-defined.

Also note that,

$$\begin{aligned} S^{-1}f(\frac{r}{s} \cdot \frac{r'}{s'}) &= f(rr')f(ss')^{-1} \\ &= f(r)f(r')[f(s)f(s')]^{-1} \\ &= f(r)f(s)^{-1}f(r')f(s')^{-1} \\ &= S^{-1}f(\frac{r}{s})S^{-1}f(\frac{r'}{s'}) \end{aligned}$$

and

$$\begin{aligned} S^{-1}f(\frac{r}{s} + \frac{r'}{s'}) &= S^{-1}f(\frac{rs' + r's}{ss'}) \\ &= f(rs' + r's)f(ss')^{-1} \\ &= [f(r)f(s') + f(r')f(s)]f(s)^{-1}f(s')^{-1} \\ &= f(r)f(s)^{-1} + f(r')f(s')^{-1} \\ &= S^{-1}f(\frac{r}{s}) + S^{-1}f(\frac{r'}{s'}), \end{aligned}$$

so $S^{-1}f$ is in fact a homomorphism. Then, given $r \in R$, we have

$$S^{-1}f(\frac{r}{1}) = f(r)f(1)^{-1} = f(r),$$

i.e., f factors through $S^{-1}R$.
To see that $S^{-1}f$ is unique, suppose that $\phi : S^{-1}R \to T$ is a homomorphism such that such that $\phi(r/1) = f(r)$ for all $r \in R$. We have

$$\phi(\frac{r}{s}) = \phi(\frac{r}{1})\phi(\frac{1}{s}) = f(r)\phi(\frac{1}{s}).$$

However,

$$\phi(\frac{1}{s})\phi(\frac{s}{1}) = \phi(\frac{1}{1}) = 1,$$

that is, $\phi(\frac{1}{s})$ is invertible, with $[\phi(\frac{1}{s})]^{-1} = \phi(\frac{s}{1})$. Thus we have $f(r) = \phi(\frac{r}{s})\phi(\frac{s}{1})$, and so

$$\begin{aligned} Sf^{-1}(\frac{r}{s}) &= f(r)f(s)^{-1} \\ &= \phi(\frac{r}{s})\phi(\frac{s}{1})f(s)^{-1} \\ &= \phi(\frac{r}{s})f(s)f(1)^{-1}f(s)^{-1} \\ &= \phi(\frac{r}{s}). \end{aligned}$$

So the homomorphism $S^{-1}f$ is the unique map such that f factors through $S^{-1}R$. □

Lecture 28. March 18, 2011

The structure sheaf for projective varieties. To define the structure sheaf for projective varieties we mimic the definitions for affine varieties. The function field $\mathbb{C}(\mathbb{P}^n)$ is defined to be all fractions $\frac{F}{G}$ such that F and G are homogeneous elements of $\mathbb{C}[\mathbb{P}^n]$ with G not the zero polynomial and with $\deg(F) = \deg(G)$.

Now let $p \in \mathbb{P}^n$ and define $\mathcal{O}_{\mathbb{P}^n,p} \subset \mathbb{C}(\mathbb{P}^n)$ to be those elements of $\mathbb{C}(\mathbb{P}^n)$ regular at p; i.e., all $\frac{F}{G} \in \mathbb{C}(\mathbb{P}^n)$ with $G(p) \neq 0$.

For any open subset $U \subseteq \mathbb{P}^n$, define $\mathbb{C}_{\mathbb{P}^n}(U)$ to be the ring of functions regular on U; i.e., $\mathbb{C}_{\mathbb{P}^n}(U) = \cap_{p\in U}\mathcal{O}_{\mathbb{P}^n,p}$.

Open sets of particular interest are those of the form $U_G = \mathbb{P}^n \setminus Z_{\mathbb{P}^n}(G)$ where $G \in \mathbb{C}[\mathbb{P}^n]$ is a homogeneous polynomial, but not the zero polynomial.

Proposition 28.1. *Let $\mathbb{C}[\mathbb{P}^n] = \mathbb{C}[x_0, \dots, x_n]$. Then $\mathcal{O}_{\mathbb{P}^n}(U_{x_i}) = \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}] = \mathbb{C}[\mathbb{A}^n]$.*

Proof. Since $\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}$ are algebraically independent, $\mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]$ is just the polynomial ring in n indeterminates, hence $\mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}] = \mathbb{C}[\mathbb{A}^n]$. So now we show $\mathcal{O}_{\mathbb{P}^n}(U_{x_i}) = \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]$.

By definition, $\frac{x_j}{x_i} \in \mathcal{O}_{\mathbb{P}^n}(U_{x_i})$, so $\mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}] \subseteq \mathcal{O}_{\mathbb{P}^n}(U_{x_i})$. Let $q \in U_{x_i}$ and let

$$\widetilde{q} = (\frac{q_0}{q_i}, \dots, \frac{q_{i-1}}{q_i}, \frac{q_{i+1}}{q_i}, \dots, \frac{q_n}{q_i}) \in \mathbb{A}^n.$$

Then $\mathcal{O}_{\mathbb{P}^n,q} = \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]_{I_{\mathbb{A}^n}(\widetilde{q})}$.

To see this, let $F/G \in \mathcal{O}_{\mathbb{P}^n,q}$, where F and G are homogeneous, $G \neq 0$, $d = \deg(G)$ and either $d = \deg(F)$ or $F = 0$. Then $F/G = (F/x_i^d)/(G/x_i^d) = f/g$, where $f = F(x_0/x_i, \dots, x_n/x_i)$ and $g = G(x_0/x_i, \dots, x_n/x_i)$. But $G(q) \neq 0$ implies $g(\widetilde{q}) \neq 0$, so $f/g \in \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]_{I_{\mathbb{A}^n}(\widetilde{q})}$. Conversely, if $f/g \in \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]_{I_{\mathbb{A}^n}(\widetilde{q})}$ for $f, g \in \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]$ with $g \notin I_{\mathbb{A}^n}(\widetilde{q})$, then either $f = 0$ and so $f/g = 0 \in \mathcal{O}_{\mathbb{P}^n,q}$ or $f \neq 0$ and we have $f/g = F/G$ for $F = x_i^d f$ and $G = x_i^d g$, where $d = \max(\deg(f), \deg(g))$. Then F and G are homogeneous of the same degree with $G(q) = g(\widetilde{q}) \neq 0$, so $f/g = F/G \in \mathcal{O}_{\mathbb{P}^n,q}$.

Therefore we have $\mathcal{O}_{\mathbb{P}^n}(U_{x_i}) = \cap_{q\in U_{x_i}}\mathcal{O}_{\mathbb{P}^n,q} = \cap_{\widetilde{q}\in\mathbb{A}^n}\mathbb{C}[\mathbb{A}^n]_{I_{\mathbb{A}^n}(\widetilde{q})} = \mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n) = \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]$. □

Example 28.2. Let $\mathbb{C}[\mathbb{P}^n] = \mathbb{C}[x_0, \dots, x_n]$. Here is an alternative way to evaluate $\mathcal{O}_{\mathbb{P}^n}(U_{x_i})$. By Exercise 28.1, we have $\mathcal{O}_{\mathbb{P}^n}(U_{x_i}) = R_{x_i}$. But for any homogeneous F of degree m, $F/x_i^m = F(x_0/x_i, \dots, x_n/x_i) \in \mathbb{C}[x_0/x_i, \dots, x_n/x_i]$, and for any $f(x_0/x_i, \dots, x_n/x_i) \in \mathbb{C}[x_0/x_i, \dots, x_n/x_i]$ of degree d we have $f = F/x_i^d \in R_{x_i}$; note that $F = x_i^d f$ is homogeneous of degree d. Thus $R_{x_i} = \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}]$.

Example 28.3. Using Exercise 28.1, we see that the global sections $\mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n)$ of $\mathcal{O}_{\mathbb{P}^n}$ are just constants; $\mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n) = R_1 = \mathbb{C}$.

Exercises:

Exercise 28.1. Let $G \in \mathbb{C}[\mathbb{P}^n]$ be homogeneous. Show that $\mathcal{O}_{\mathbb{P}^n}(U_G)$ is the ring R_G of all fractions of the form $\frac{F}{G^m} \in \mathbb{C}(\mathbb{P}^n)$ where F is either 0 or homogeneous and $\deg(F) = m\deg(G)$.

Solution by Becky Egg. We have that

$$\mathcal{O}_{\mathbb{P}^n}(U_G) = \bigcap_{p \in U_G} \mathcal{O}_{\mathbb{P}^n,p}$$

where U_G is the set of points in $\mathbb{P}^n$ at which G is not 0, and elements of $\mathcal{O}_{\mathbb{P}^n,p}$ are of the form $\frac{F}{H}$, where $H(p) \neq 0$ and $\deg(F) = \deg(H)$.

First, consider $\frac{F}{G^m} \in R_G$ with $\deg(F) = m\deg(G)$. For any $p \in U_G$, we have that $G(p) \neq 0$, and hence $G^m(p) \neq 0$. So $\frac{F}{G^m} \in \mathcal{O}_{\mathbb{P}^n,p}$ for all $p \in U_G$, and thus $\frac{F}{G^m} \in \mathcal{O}_{\mathbb{P}^n}(U_G)$.

Now suppose that $\frac{F}{H} \in \mathcal{O}_{\mathbb{P}^n}(U_G)$. Note that $H(p) \neq 0$ for all $p \in U_G$, so $q \in Z_{\mathbb{P}^n}(H)$ implies that $q \notin U_G$, and hence $G(q) = 0$. So we have

$$G \in I(Z_{\mathbb{P}^n}(H)) = \sqrt{(H)},$$

where equality of the ideals follows from the projective Nullstellensatz. So $G^m \in (H)$ for some m, i.e., $G^m = F'H$ for some $F' \in \mathbb{C}[\mathbb{P}^n]$. Thus we have

$$\frac{F}{H} = \frac{F'F}{F'H} = \frac{F'F}{G^m} \in R_G.$$

Note also that $\deg(F) = \deg(H)$, and so

$$\deg(F'F) = \deg(F'H) = \deg(G^m) = m\deg(G).$$

Thus $\mathcal{O}_{\mathbb{P}^n}(U_G)$ is the ring R_G of all fractions of the form $\frac{F}{G^m} \in \mathbb{C}(\mathbb{P}^n)$ where F is either 0 or homogeneous and $\deg(F) = m\deg(G)$. □

Lecture 29. March 28, 2011

Quasi-projective varieties.

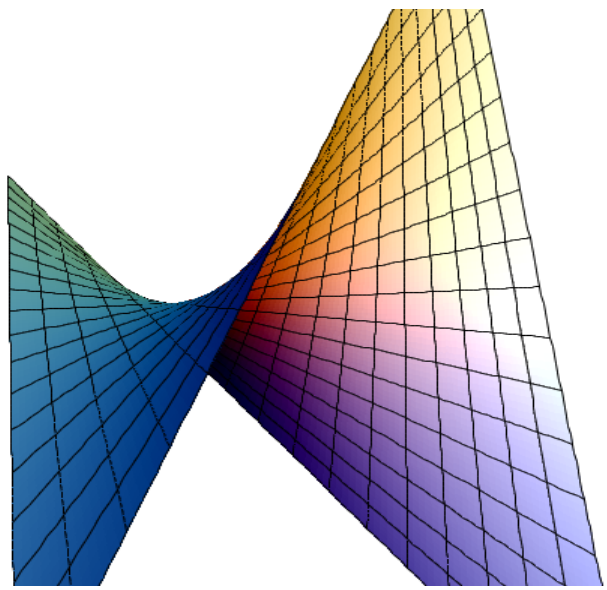
Definition 29.1. A *projective variety* is a closed irreducible subset of $\mathbb{P}^n$. A *quasi-projective variety* is a non-empty open subset of a projective variety. Given a projective variety $V \subseteq \mathbb{P}^n$, the homogeneous coordinate ring of V is $\mathbb{C}[V] = \mathbb{C}[\mathbb{P}^n]/I_{\mathbb{P}^n}(V)$ and the function field of V is the field $\mathbb{C}(V)$ of all fractions F/G such that $F, G \in \mathbb{C}[V]$ are homogeneous, and where $G \neq 0$ and F is either 0 or $\deg(F) = \deg(G)$. For $p \in V$, we define $\mathcal{O}_{V,p}$ to be the ring of functions regular at p; i.e., all fractions F/G such that $F, G \in \mathbb{C}[V]$ are homogeneous, and where $G(p) \neq 0$ and F is either 0 or $\deg(F) = \deg(G)$. Finally, we set $\mathcal{O}_V(\varnothing) = 0$ and for a non-empty open subset $U \subseteq V$, we set $\mathcal{O}_V(U) = \cap_{p \in U} \mathcal{O}_{V,p} \subseteq \mathbb{C}(V)$.

Now we establish some notation. Let $V \subset \mathbb{P}^n$ be a projective variety. Let $0 \neq G \in \mathbb{C}[V]$ be homogeneous of degree $d = \deg(G) > 0$. Let $U_G = V \setminus Z_V(G)$.

Example 29.2. Let $\mathbb{C}[\mathbb{P}^3] = \mathbb{C}[x, y, z, w]$ and let $V \subset \mathbb{P}^3$ be the zero locus of $xw - zy$. There is a map $\mathbb{P}^1 \times \mathbb{P}^1 \to V$ called the Segre embedding which we will eventually be able to see is an isomorphism, defined by $([(a, b)], [(u, v)]) \mapsto [(au, av, bu, bv)]$, so the parametric equations for the image are $x = au$, $y = av$, $z = bu$ and $w = bv$, and substituting into $xw - zy$ gives $aubv - buav = 0$. Figure 29.1 shows a graph of the map $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^3$ given by $(a, u) \mapsto (au, a, u)$. This is just the an affine image of the graph of $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$; i.e., the image in the affine complement $\mathbb{P}^3 \setminus Z_{\mathbb{P}^3}(w)$ of the locus $w = 0$ in $\mathbb{P}^3$. The grid lines are the affine images of the two $\mathbb{P}^1$ factors, called rulings. The locus $Z_V(y, w)$ is one of those lines, so the open subset $U = V \setminus Z_V(y, w) \subset V$ is the complement of the grid line defined by $y = 0 = w$.

Note that $U = U_w \cup U_y$. Thus $\mathcal{O}_V(U) = \cap_{p\in U}\mathcal{O}_{V,p} = (\cap_{p\in U_w}\mathcal{O}_{V,p}) \cap (\cap_{p\in U_y}\mathcal{O}_{V,p})$. Now, in $\mathbb{C}(V)$ we have $\frac{\overline{z}}{\overline{w}} = \frac{\overline{x}}{\overline{y}}$, since $\overline{xw} - \overline{zy} = 0$, where $\overline{\ }: \mathbb{C}[\mathbb{P}^3] \to \mathbb{C}[V]$ is the quotient homomorphism. But for $q = [(0,1,0,0)] \in U_y$, $\frac{\overline{z}}{\overline{w}}$ does not appear to meet the definition for being in $\mathcal{O}_{V,q}$ since $\overline{w}(q) = 0$. It is only when we rewrite $\frac{\overline{z}}{\overline{w}}$ as $\frac{\overline{x}}{\overline{y}}$ that we see that it is an element of $\mathcal{O}_{V,q}$. And for $q = [(0,0,1,0)] \in U_w$, $\frac{\overline{x}}{\overline{y}}$ does not appear to meet the definition for being in $\mathcal{O}_{V,q}$ since $\overline{y}(q) = 0$. It is only when we rewrite $\frac{\overline{x}}{\overline{y}}$ as $\frac{\overline{z}}{\overline{w}}$ that we see that it is an element of $\mathcal{O}_{V,q}$. Thus $\frac{\overline{x}}{\overline{y}}$, as written, is regular at the points of U_y but not at all points of U_w, and $\frac{\overline{z}}{\overline{w}}$, as written, is regular at the points of U_w but not at all points of U_y. However, $\frac{\overline{x}}{\overline{y}} = \frac{\overline{z}}{\overline{w}}$ on $U_y \cap U_w$, so we have an element regular at all points of $U = U_y \cup U_w$. It turns out that there is no non-constant homogeneous $G \in \mathbb{C}[\mathbb{P}^3]$ such that $Z_{\mathbb{P}^3}(G) \cap U = \varnothing$, so we cannot express this element by a single fraction $\frac{\overline{F}}{\overline{G}}$ such that G is non-zero at all points of U.

FIGURE 29.1. Hyperboloid $xw - zy$ defined parametrically in $\mathbb{A}^3$ by $x = au$, $y = a$, $z = u$, $w = 1$



Exercises:

Exercise 29.1. Let $V \subset \mathbb{P}^n$ be a projective variety. Let $0 \neq G \in \mathbb{C}[V]$ be homogeneous of degree $d = \deg(G) > 0$. Show that $\mathcal{O}_V(U_G)$ is the ring of all fractions F/G^m such that $m \geq 0$, $F \in \mathbb{C}[V]$ is homogeneous, and either F is 0 or $\deg(F) = m\deg(G)$. (We will later see in Exercise 33.1 that U_G is isomorphic to a closed subset of $\mathbb{A}^n$ for some n, and hence is referred to as an *open affine subset* of V.)

Solution. Clearly, all $F/G^m \in \mathcal{O}_V(U_G)$, so assume $h \in \mathcal{O}_V(U_G)$. For each $p \in U_G$ we can write $h = F_p/G_p$ where F_p and G_p are homogeneous of the same degree but $G_p(p) \neq 0$. Since

$$Z_V(\{G_p : p \in U_G\}) \cap U_G = \varnothing,$$

we have $Z_V(\{G_p : p \in U_G\}) \subseteq Z_V(G)$. By the Projective Nullstellensatz, Theorem 19.1.5, for some $m \geq 0$ we have $G^m \in I(\{G_p : p \in U_G\})$, so as elements of $\mathbb{C}[V]$ we have $G^m = \sum_p H_p G_p$

for homogeneous $H_p \in \mathbb{C}[V]$ of degree $\deg(H_p) = m\deg(G) - \deg(G_p)$ for those H_p which are not 0 (all but finitely many of the H_p are in fact 0 since the sum is a finite sum). Now we see that $h = ((\sum_p H_p G_p)/G^m)h = (\sum_p H_p h G_p)/G^m = (\sum_p H_p(F_p/G_p)G_p)/G^m = (\sum_p H_p F_p)/G^m$ has the required form. □

Lecture 30. March 30, 2011

Morphisms of quasi-projective varieties. Let U be a quasi-projective variety. Thus there is some projective variety $V \subseteq \mathbb{P}^n$ and U is a nonempty open subset of V. The structure sheaf $\mathcal{O}_U$ is defined; for any open subset $U' \subseteq U$ we have $\mathcal{O}_U(U') = \mathcal{O}_V(U')$. We can also speak of affine open subsets of U: for U' to be an open affine subset of U just means it is an open affine subset of V.

Definition 30.1. Let U_1 and U_2 be quasi-affine projective varieties. A map $\phi : U_1 \to U_2$ is a *morphism* if ϕ is continuous in the Zariski topology, such that for each point $p \in U_1$ there are open affine neighborhoods $V_p \subseteq U_1$ and $W_p \subseteq U_2$ such that $\phi(p) \in W_p$, $p \in V_p$, $\phi(V_p) \subset W_p$ and ϕ^* induces a $\mathbb{C}$-homomorphism $\phi^* : \mathcal{O}_{U_2}(W_p) \to \mathcal{O}_{U_1}(V_p)$.

Example 30.2. Let $\mathbb{C}[\mathbb{P}^n] = \mathbb{C}[x_0, \ldots, x_n]$. Then U_{x_i} is isomorphic to $\mathbb{A}^n$. For simplicity, we'll consider the case that $i = 0$, so let $U = U_{x_0}$. Define $\phi : U \to \mathbb{A}^n$ by $\phi([(a_0, \ldots, a_n)]) = (\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0})$; note that $[(a_0, \ldots, a_n)] \in U_{x_0}$ means that $a_0 \neq 0$, so division by a_0 is allowed. Since also $(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}) = (\frac{ca_1}{ca_0}, \ldots, \frac{ca_n}{ca_0})$ for any representative $(ca_0, \ldots, ca_n)$, $0 \neq c \in \mathbb{C}$, of $[(a_0, \ldots, a_n)]$, ϕ is well-defined. Let $\psi : \mathbb{A}^n \to U$ be defined by $(b_1, \ldots, b_n) \mapsto [(1, b_1, \ldots, b_n)]$. It is easy to check that ϕ and ψ are inverses of each other. By Proposition 28.1, $\mathcal{O}_U(U) = \mathbb{C}[\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}]$. Let's use y for the variables on $\mathbb{A}^n$, so $\mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n) = \mathbb{C}[y_1, \ldots, y_n]$. Given any $f(y_1, \ldots, y_n) \in \mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n)$, we have by composition the map $\phi^*(f) = f \circ \phi$. For any $[(a_0, \ldots, a_n)] \in U$, note that $(\phi^*(f))([(a_0, \ldots, a_n)]) = f(\phi([(a_0, \ldots, a_n)]) = f(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0})$ we see ϕ^* is just the $\mathbb{C}$-homomorphism $\mathbb{C}[y_1, \ldots, y_n] \to \mathbb{C}[\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}]$ given by $y_j \mapsto \frac{x_j}{x_0}$ for each j. Similarly, it is easy to check that ψ^* is the inverse $\mathbb{C}$-homomorphism. This also shows that ϕ and ψ are continuous. Consider ϕ; it suffices to show that $\phi^{-1}(U_f)$ is open for open subsets of the form U_f where $f \in \mathbb{C}[y_1, \ldots, y_n]$. But $\phi^{-1}(U_f) = U_{\phi^*(f)}$, which is open. Thus ϕ and ψ are inverse morphisms, hence ϕ is an isomorphism.

Remark 30.3. If we identify U_{x_i} with $\mathbb{A}^n$, we thus have $\mathcal{O}_{\mathbb{A}^n}(U) = \mathcal{O}_{U_{x_i}}(U) = \mathcal{O}_{\mathbb{P}^n}(U)$ for any open subset $U \subseteq \mathbb{A}^n$. From this point-of-view, we can regard the coordinate ring of $\mathbb{A}^n = U_{x_i}$ as being $\mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n) = \mathcal{O}_{U_{x_i}}(U_{x_i}) = \mathcal{O}_{\mathbb{P}^n}(U_{x_i}) = \mathbb{C}[\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}]$.

Remark 30.4. We now see that any quasi-affine variety is isomorphic to a quasi-projective variety. If U is quasi-affine, then U is a non-empty open subset of an affine variety V; i.e., $U \subseteq V \subseteq \mathbb{A}^n \cong U_{x_0} \subset \mathbb{P}^n$. If we identify U with its isomorphic image in $U_{x_0} \subset \mathbb{P}^n$, we can regard the Zariski-closure of U in $\mathbb{P}^n$ as a projective variety (see Exercise 30.1).

Example 30.5. If X is an affine variety, then we can recover X up to isomorphism from its coordinate ring $\mathbb{C}[X]$. In particular, $\mathbb{C}[X]$ is a finitely generated $\mathbb{C}$-algebra, so for some n we have a surjective homomorphism $h : \mathbb{C}[\mathbb{A}^n] \to \mathbb{C}[X]$. The kernel of h is a prime ideal. Let $Y = Z(P) \subseteq \mathbb{A}^n$. Then $X \cong Y$ since $\mathbb{C}[X] \cong \mathbb{C}[Y]$. However, with projective varieties this is not true: it is quite common to have projective varieties $X \cong Y$ such that the homogeneous coordinate rings $\mathbb{C}[X]$ and $\mathbb{C}[Y]$ are not isomorphic. For example, consider the map $\nu_2 : \mathbb{P}^1 \to \mathbb{P}^2$ given by $\nu_2([(a, b)]) = [(a^2, b^2, ab)]$, known as the 2-uple Veronese embedding of $\mathbb{P}^1$ in $\mathbb{P}^2$. Then ν_2 is an isomorphism of $X = \mathbb{P}^1$ to its image $Y = Z_{\mathbb{P}^2}(xy - z^2)$, but $\mathbb{C}[\mathbb{P}^1] = \mathbb{C}[s, t]$, while $\mathbb{C}[Y] = \mathbb{C}[x, y, z]/(xy - z^2)$. The map ν_2 induces a homomorphism $\nu_2^* : \mathbb{C}[x, y, z] \to \mathbb{C}[s, t]$ given by $x \mapsto s^2$, $y \mapsto b^2$ and $z \mapsto st$. This is not surjective so the induced homomorphism $\mathbb{C}[x, y, z]/(xy - z^2) \to \mathbb{C}[s, t]$ is certainly not an isomorphism. In fact, there is no isomorphism. One way to see this is that $\mathbb{C}[x, y, z]/(xy - z^2)$ is not a regular ring, but $\mathbb{C}[s, t]$ is. We'll discuss this in more detail later, but here's how this difference manifests itself. Let M be the maximal ideal $(\overline{x}, \overline{y}, \overline{z}) \subset \mathbb{C}[\overline{x}, \overline{y}, \overline{z}] = \mathbb{C}[x, y, z]/(xy - z^2)$. Then

M/M^2 is a 3-dimensional vector space, spanned by the images of $\overline{x}, \overline{y}$, and $\overline{z}$ in M/M^2. However, every maximal ideal of $\mathbb{C}[s,t]$ is of the form $(s-a, t-b)$ for $a, b \in \mathbb{C}$, but $(s-a,t-b)/(s-a,t-b)^2$ is a 2-dimensional vector space, spanned by the images of $s-a$ and $t-b$. If there were an isomorphism $\mathbb{C}[x,y,z]/(xy-z^2) \to \mathbb{C}[s,t]$, then $\mathbb{C}[s,t]$ would have some maximal ideal I such that I/I^2 were 3-dimensional.

The 2-uple Veronese embedding is one of several classical morphisms it's worth knowing about. More generally, for each d and n we have the d-uple Veronese embedding $\nu_d : \mathbb{P}^n \to \mathbb{P}^N$, where $N = \binom{n+d}{d} - 1$. There is also the Segre embedding $\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$, where $N = (n+1)(m+1)-1$. And there is the Plücker embedding $\rho : \mathrm{Gr}(r,n) \to \mathbb{P}^N$ of the Grassmann variety $\mathrm{Gr}(r,n)$ of r-planes in n-space to $\mathbb{P}^N$, where $N = \binom{n}{r} - 1$. More on these in the next lecture.

Exercises:

Exercise 30.1. Let U be a quasi-affine variety. I.e., U is a non-empty open subset of some closed irreducible subset $V \subseteq \mathbb{A}^n$. Thinking of $\mathbb{A}^n = U_{x_0} \subset \mathbb{P}^n$ as an open subset of $\mathbb{P}^n$, we refer to the Zariski closure of U in $\mathbb{P}^n$ as its *projective closure*. Show that the projective closure of U is irreducible, hence a projective variety.

Solution. Let $C = V \setminus U$. First, U is an irreducible topological space. For if A and B are closed subsets of U with $U = A \cup B$ so $V = A \cup (B \cup C)$. Since V is irreducible, either $V = A$ (and hence $U = A$) or $V = B \cup C$ (and hence $U = B$), so U is irreducible. Let W be the closure of U in $\mathbb{P}^n$ and let D and E be closed subsets of W such that $W = D \cup E$. Since U is irreducible, either $U \subseteq D$ or $U \subseteq E$; assume the former, the argument being the same if $U \subseteq E$. If $U \subseteq D$, then the closure W of U is also contained in D, hence W is irreducible. $\square$

Lecture 31. April 1, 2011

The Segre embedding. Let s and t be positive integers. The Segre embedding is a map of $\sigma : \mathbb{P}^s \times \mathbb{P}^t \to \mathbb{P}^N$, where $N = (s+1)(t+1)-1$. Given a point $([\mathbf{a}],[\mathbf{b}]) = [(a_0,\dots,a_s)],(b_0,\dots,b_t)] \in \mathbb{P}^s \times \mathbb{P}^t$, think of the points of $\mathbb{P}^N$ as the set of non-zero $(s+1)\times(t+1)$ matrices, modulo scalar multiplication by non-zero scalars. Then $\sigma(([\mathbf{a}],[\mathbf{b}])) = [(a_ib_j)]$, where (a_ib_j) is the $(s+1)\times(t+1)$ matrix whose entries are a_ib_j. Note that we can write this as a matrix multiplication: $\mathbf{a}^T\mathbf{b} = (a_ib_j)$, where we think of $\mathbf{a}$ and $\mathbf{b}$ as row vectors. Moreover, the map is well-defined: $\mathbf{a}^T\mathbf{b} = (a_ib_j)$ is zero if and only if both $\mathbf{a}$ and $\mathbf{b}$ are zero, and replacing $\mathbf{a}$ and $\mathbf{b}$ by possibly different representatives of the same points just replaces (a_ib_j) by a non-zero scalar multiple, which represents the same point of $\mathbb{P}^N$.

The product $\mathbb{P}^s \times \mathbb{P}^t$ does not have an intrinsic structure of algebraic variety according to our definitions, but in fact σ is injective and the image $\sigma(\mathbb{P}^s \times \mathbb{P}^t)$ is closed and irreducible, so we can regard $\mathbb{P}^s \times \mathbb{P}^t$ as an algebraic variety by identifying it with its image.

First we check that σ is injective. Let (a_ib_j) be a representative of $\sigma(([\mathbf{a}],[\mathbf{b}]))$. Pick any non-zero entry a_ib_j. Let $\mathbf{c} = (a_0b_j,\dots,a_sb_j)$ be the transpose of column j of the matrix (a_ib_j) and let $\mathbf{d} = (a_ib_0,\dots,a_ib_t)$ be row i. Then $[\mathbf{a}] = [\mathbf{c}]$, and $[\mathbf{b}] = [\mathbf{d}]$, and so we can recover $([\mathbf{a}],[\mathbf{b}])$ given $[(a_ib_j)]$, hence σ is injective.

To show that $\sigma(\mathbb{P}^s \times \mathbb{P}^t)$ is closed, note that every matrix representing a point in the image of σ has rank 1, since every row of $\mathbf{a}^T\mathbf{b}$ is a multiple of $\mathbf{b}$, and the rows are not all $\mathbf{0}$. Conversely, given any $(s+1)\times(t+1)$ rank 1 matrix M, it has some non-zero row, say $\mathbf{b_j}$, and every other row is a multiple of $\mathbf{b_j}$; say row 1 is $a_0\mathbf{b_j}$, row 2 is $a_1\mathbf{b_j}$, etc. Thus $M = \mathbf{a}^T\mathbf{b}$ for $\mathbf{a} = (a_0,\dots,a_s)$, so $[M]$ is in the image of σ. In particular, the image of σ is precisely the set of $(s+1)\times(t+1)$ rank 1 matrices.

Given an $(s+1)\times(t+1)$ rank 1 matrix M, every rectangular submatrix has rank at most 1. In particular, every 2×2 submatrix has determinant 0. If we denote the homogeneous coordinates on $\mathbb{P}^N$ by x_{ij}, corresponding to the ij entry of an $(s+1)\times(t+1)$ matrix, let I be the homogeneous ideal generated by all polynomials of the form $x_{ij}x_{kl}-x_{il}x_{kj}$, with i,j,k,l distinct. Then we see that $Z_{\mathbb{P}^N}(I)$ contains the image of σ. But any non-zero $(s+1)\times(t+1)$ matrix in $Z_{\mathbb{P}^N}(I)$ must have rank 1. To see this, suppose M is a non-zero $(s+1)\times(t+1)$ matrix which does not have rank 1. Then two columns of $M=(m_{ij})$ are linearly independent. Say the columns are columns j and l. Similarly, two rows of these two columns must be linearly independent; say the rows are rows i and k. Thus the square matrix whose entries are in rows i and k and in columns j and l has rank 2, so its determinant $m_{ij}m_{kl}-m_{il}m_{kj}\neq 0$, and therefore M is not in the zero locus of I. Thus the zero locus of I is precisely the image of σ.

Finally, we want to see that $\sigma(\mathbb{P}^s\times\mathbb{P}^t)$ is irreducible. Let $\mathbb{C}[\mathbb{P}^s]=\mathbb{C}[y_0,\dots,y_s]$ and let $\mathbb{C}[\mathbb{P}^t]=\mathbb{C}[z_0,\dots,z_t]$. Consider $U_{x_{ij}}\subset\mathbb{P}^N$. Then $\sigma^{-1}(U_{x_{ij}})=U_{y_i}\times U_{z_j}$. Thus σ gives an algebraic map (and hence a morphism) of affine varieties $\mathbb{A}^{s+t}=\mathbb{A}^s\times\mathbb{A}^t=U_{y_i}\times U_{z_j}\to U_{x_{ij}}=\mathbb{A}^N$, since the map is given by polynomial functions. But the inclusion of $U_{x_{ij}}=\mathbb{A}^N$ into $\mathbb{P}^N$ is also a morphism, hence $U_{y_i}\times U_{z_j}\to\mathbb{P}^N$ is a morphism of quasi-projective varieties by Exercise 31.1. Since $\mathbb{A}^{s+t}=U_{y_i}\times U_{z_j}$ is irreducible, so is the closure of its image in $\mathbb{P}^N$ under σ (by Exercise 31.2). But the closure of any non-empty open subset of $\mathbb{A}^{s+t}$ is all of $\mathbb{A}^{s+t}$, since $\mathbb{A}^{s+t}$ is irreducible. Consider the open subset $\cap_{i,j}U_{y_i}\times U_{z_j}$, which is just $U_{y_0\cdots y_s z_0\cdots z_t}$ inside $\mathbb{A}^{s+t}$, where we take the y's and z's as the coordinate variables on $\mathbb{A}^{s+t}$; i.e., $\mathbb{C}[\mathbb{A}^{s+t}]=\mathbb{C}[y_0,\cdots,y_s,z_0,\cdots,z_t]$. Thus the closure of $U_{y_0\cdots y_s z_0\cdots z_t}$ includes the closure of $\mathbb{A}^{s+t}=U_{y_i}\times U_{z_j}$ for all i and j, hence the closure of $\sigma(U_{y_0\cdots y_s z_0\cdots z_t})$ includes $\sigma(U_{y_i}\times U_{z_j})$ for all i and j. Thus the closure of $\sigma(U_{y_0\cdots y_s z_0\cdots z_t})$ includes the union $\cup_{i,j}\sigma(U_{y_i}\times U_{z_j})$. But $\sigma(U_{y_i}\times U_{z_j})=\sigma(\mathbb{P}^s\times\mathbb{P}^t)\cap U_{x_{ij}}$, and the open sets $U_{x_{ij}}$ cover $\mathbb{P}^N$, so $\cup_{i,j}\sigma(U_{y_i}\times U_{z_j})=\mathbb{P}^s\times\mathbb{P}^t$. In particular, $\sigma(\mathbb{P}^s\times\mathbb{P}^t)$ is the closure of the image of $\mathbb{A}^{s+t}=U_{y_i}\times U_{z_j}$ for any fixed i and j. Thus $\sigma(\mathbb{P}^s\times\mathbb{P}^t)$ is irreducible by Exercise 31.2.

Exercises:

Exercise 31.1. Let $U\to V$ and $V\to W$ be morphisms of quasi-projective varieties. Show that the composition $U\to W$ is a morphism.

Solution by Anisah Nu'man, with some changes. Let $\phi:U\to V$ and $\psi:V\to W$ be morphisms of quasi-projective varieties. We will show $(\psi\circ\phi):U\to W$ is a morphism. First note $(\psi\circ\phi)$ is continuous in the Zariski topology since the composition of continuous functions is continuous.

Let $p\in U$. Since $\phi(p)\in V$ and $\psi:V\to W$ is a morphism, there exist affine open subsets $V_{\phi(p)}\subseteq V$ and $W_{\phi(p)}\subseteq W$ such that $\psi(\phi(p))\in W_{\phi(p)}$, $\phi(p)\in V_{\phi(p)}$, $\psi(V_{\phi(p)})\subseteq W_{\phi(p)}$, and $\psi^*:\mathcal{O}_W(W_{\phi(p)})\to\mathcal{O}_V(V_{\phi(p)})$ is a $\mathbb{C}$-homomorphism. Since ϕ is a morphism, there exist affine open subsets $U_p\subseteq U$ and $V_p\subseteq V$ such that $\phi(p)\in V_p$, $p\in U_p$, $\phi(U_p)\subseteq V_p$, and $\phi^*:\mathcal{O}_V(V_p)\to\mathcal{O}_U(U_p)$ is a $\mathbb{C}$-homomorphism.

Now pick an open affine neighborhood V_p' of $\phi(p)$ in $V_p\cap V_{\phi(p)}$ and pick an open affine neighborhood U_p' of p in $U_p\cap\phi^{-1}(V_p')$. Since U_p and V_p are affine (and thus have a basis of open sets of the form $\{(U_p)_f : f\in\mathcal{O}_U(U_p)\}$ and $\{(V_p)_g : g\in\mathcal{O}_V(V_p)\}$, respectively) we may assume that $V_p'=(V_p)_g$ for some $g\in\mathcal{O}_V(V_p)$, and that $U_p'=(U_p)_f$ for some $f\in\mathcal{O}_U(U_p)$. The homomorphism $\mathcal{O}_V(V_p')\to\mathcal{O}_U(U_p')$ is the $\mathbb{C}$-homomorphism induced from $\mathcal{O}_V(V_p)\to\mathcal{O}_U(U_p)$ by inverting f and g. Thus $(\psi\circ\phi)$ induces a $\mathbb{C}$-homomorphism $(\psi\circ\phi)^*:\mathcal{O}_W(W_{\phi(p)})\to\mathcal{O}_V(V_{\phi(p)})\to\mathcal{O}_V(V_p')\to\mathcal{O}_U(U_p')$, as required. □

Exercise 31.2. Let $f:U\to V$ be a morphism of quasi-projective varieties. Show that the Zariski-closure of $f(U)$ in V is irreducible.

Solution. Say $\overline{f(U)} = A \cup B$ for closed subsets A and B. Thus $f^{-1}(A)$ and $f^{-1}(B)$ are closed subsets whose union is U, hence (since U is irreducible) either $U = f^{-1}(A)$ or $U = f^{-1}(B)$, so either $\overline{f(U)} = A$ or $\overline{f(U)} = B$, hence $\overline{f(U)}$ is closed. □

Lecture 32. April 4, 2011

The Veronese embedding. We begin with a lemma.

Lemma 32.1. *The number of monomials in $\mathbb{C}[\mathbb{P}^r] = \mathbb{C}[x_0, \ldots, x_r]$ of degree d is $\binom{r+d}{r}$.*

Proof. There is a bijection between permutations of r bars and d stars and monomials $x_0^{n_0} \cdots x_r^{n_r}$ such that $d = n_0 + \cdots + n_r$. For example, if $r = 3$ and $d = 2$, the permutations " $| \; | \; * \; * \; |$ " gives the monomial $x_0^0 x_1^0 x_2^2 x_3^0 = x_2^2$. But there are $\binom{r+d}{r}$ permutations of r bars and d stars. □

We now define a map $\nu_d : \mathbb{P}^r \to \mathbb{P}^N$ where $N = \binom{r+d}{r} - 1$. Let $\mathbb{C}[\mathbb{P}^r] = \mathbb{C}[x_0, \ldots, x_r]$ and enumerate the monomials of degree d in the variables $x_0, \ldots, x_r$ as $G_0, \ldots, G_N$. For each point $p = [(a_0, \ldots, a_r)] \in \mathbb{P}^r$, define $\nu_d(p) = [(G_0(a_0, \ldots, a_r), \ldots, G_N(a_0, \ldots, a_r)] \in \mathbb{P}^N$. It is easy to check that this is well-defined.

Note that we can also regard ν_d as an algebraic map $\mathbb{A}^{r+1} \to \mathbb{A}^{N+1}$. The corresponding $\mathbb{C}$-homomorphism

$$\nu_d^* : \mathbb{C}[\mathbb{P}^N] = \mathbb{C}[\mathbb{A}^{N+1}] = \mathbb{C}[y_0, \ldots, y_N] \to \mathbb{C}[x_0, \ldots, x_r] = \mathbb{C}[\mathbb{A}^{r+1}] = \mathbb{C}[\mathbb{P}^r]$$

is given by $y_i \mapsto G_i$.

Remark 32.2. A polynomial ring $R = \mathbb{C}[x_0, \ldots, x_r]$ is a graded ring in the sense that there is a canonical ring isomorphism $h : R_0 \oplus R_1 \oplus \cdots \to R$, where R_i is the $\mathbb{C}$-vector space span of the homogeneous polynomials of degree i. The homomorphism h is induced by the inclusions $R_i \subset R$ by the universal property of direct sums. It is typical for people to just identify $R_0 \oplus R_1 \oplus \cdots$ with R. The subring $R_0 \oplus R_d \oplus R_{2d} \oplus \cdots \subset R$ is called a Veronese subring of R. It is exactly the image of ν_d^*. [Let S be a ring. Let I be some index set, and let A_i, $i \in I$, be a family of S-modules. Recall that the direct product $\Pi_i A_i$ is the set of all maps $f : I \to \cup_i A_i$ such that $f(i) \in A_i$. For example, $A_1 \times A_2 = \{(a_1, a_2) : a_1 \in A_1, a_2 \in A_2\}$ is really the set of all maps $f : \{1, 2\} \to A_1 \cup A_2$ such that $f(1) \in A_1$ and $f(2) \in A_2$. Such a map f can be thought of as the element $(f(1), f(2))$. The direct sum $\oplus_i A_i$ is the subset of the direct product $\Pi_i A_i$ of all maps $f \in \Pi_i A_i$ such that $f(i)$ is 0 for all but finitely many i. Note for each j that there is a natural inclusion of $\phi_j : A_j \subseteq \oplus_i A_i$. Now let B be an S-module. The *universal property of direct* is the fact that if we are given S-module homomorphisms $h_i : A_i \to B$ for all i, then there is a unique S-module homomorphism $h : \oplus_i A_i \to B$ such that $h \circ \phi_j = h_j$.]

To show that $\nu_d : \mathbb{P}^r \to \mathbb{P}^N$ is a morphism, it's convenient to pick an enumeration $G_0, \ldots, G_N$ such that $G_0 = x_0^d$, $G_1 = x_1^d$, …, $G_r = x_r^d$, with the rest of the monomials enumerated in whatever way the reader desires. Let $0 \le i \le r$ and let $p \in \mathbb{P}^r$. If $\nu_d(p) \in U_{y_i}$, then $y_i(\nu_d(p)) \neq 0$, hence $G_i(p) = (\nu_d^*(y_i))(p) \neq 0$, but since $G_i = x_i^d$, we see $G_i(p) \neq 0$ if and only if $x_i(p) \neq 0$. Conversely, if $x_i(p) \neq 0$ then $G_i(p) = (nu_d^*(y_i))(p) \neq 0$, so $\nu_d(p) \in U_{y_i}$. Thus $\nu_d^{-1}(U_{y_i}) = U_{G_i} = U_{x_i}$ and we see that $\nu_d|_{U_{x_i}} : \mathbb{A}^r \cong U_{x_i} \to U_{y_i} \cong \mathbb{A}^N$ is an algebraic mapping whose corresponding $\mathbb{C}$-homomorphism $\nu_d|_{U_{x_i}}^* : \mathcal{O}_{\mathbb{P}^N}(U_{y_i}) \to \mathcal{O}_{\mathbb{P}^r}(U_{x_i})$ is the homomorphism $\mathbb{C}[y_0/y_i, \ldots, y_N/y_i] \to \mathbb{C}[x_0/x_i, \ldots, x_r/x_i]$ given by $y_j/y_i \mapsto G_j/G_i = G_j/x_i^d = G_j(x_0/x_i, \ldots, x_r/x_i)$.

Since $\nu_d|_{U_{x_i}}$ is an algebraic mapping, it is continuous for each i. Since the open sets U_{x_i} give an open cover of $\mathbb{P}^r$, it follows that $\nu_d : \mathbb{P}^r \to \mathbb{P}^N$ is continuous and since the induced homomorphisms $(\nu_d|_{U_{x_i}})^* : \mathcal{O}_{\mathbb{P}^N}(U_{y_i}) \to \mathcal{O}_{\mathbb{P}^r}(U_{x_i})$ are $\mathbb{C}$-homomorphisms, ν_d is itself a morphism.

We next want to show that ν_d is an isomorphism to its image, which is closed in $\mathbb{P}^N$.

Exercises:

Exercise 32.1. Let d be a positive integer and let $G_0, \ldots, G_t \in \mathbb{C}[\mathbb{P}^s] = \mathbb{C}[x_0, \ldots, x_s]$ be homogeneous such that for each i, G_i is either 0 or has degree i. Also assume that G_i is not zero for some i. Let $U \subseteq \mathbb{P}^r$ be the open subset $U = \mathbb{P}^r \setminus Z_{\mathbb{P}^r}(G_0, \ldots, G_N)$. Show that $f : [(a_0, \ldots, a_r)] \mapsto [G_0(a_0, \ldots, a_r), \ldots, G_N(a_0, \ldots, a_r)]$ defines a morphism $f : U \to \mathbb{P}^N$ as quasi-projective varieties and explain why f is not defined on $Z_{\mathbb{P}^r}(G_0, \ldots, G_N)$. [The closed set $Z_{\mathbb{P}^r}(G_0, \ldots, G_N)$ is called the *indeterminacy locus* of f. It is also called the *base locus* of $G_0, \ldots, G_N$.]

Solution by Katie Morrison. First note that f is well-defined because

$$\begin{aligned} f([ca_0, \ldots, ca_r)]) &= [c^d G_0(a_0, \ldots, a_r), \ldots, G_N(a_0, \ldots, a_r)] \\ &= [G_0(a_0, \ldots, a_r), \ldots, G_N(a_0, \ldots, a_r)] = f([a_0, \ldots, a_r)]), \end{aligned}$$

and so the value of f is independent of the choice of representative at which f is evaluated. To see that f is a morphism, consider the following. Let $p \in U$ then since $p \notin Z_{\mathbb{P}^r}(G_0, \ldots, G_N)$, there exists a G_i such that $G_i(p) \neq 0$. Without loss of generality, say $i = 0$. Let $V_p = U_{G_0} \subseteq U$ be an affine neighborhood of p and $W_p = U_{y_0} \subseteq \mathbb{P}^N = \mathbb{C}[y_0, \ldots, y_N]$ be an affine neighborhood of $f(p)$. By Exercise 29.1, $\mathcal{O}_U(V_p) = \{F/G_0^m \ : \ m \geq 0, F \in \mathbb{C}[V]$ is homogeneous, and either $F = 0$ or $\deg(F) = m \deg(G)\}$ and $\mathcal{O}_{\mathbb{P}^N}(W_p) = \mathbb{C}\left[\frac{y_1}{y_0}, \ldots, \frac{y_N}{y_0}\right]$. For any $H\left(\frac{y_1}{y_0}, \ldots, \frac{y_N}{y_0}\right) \in \mathcal{O}_{\mathbb{P}^N}(W_p)$, $H \circ f = H\left(\frac{G_1}{G_0}, \ldots, \frac{G_N}{G_0}\right)$, and so $H \circ f$ will have the form F/G_0^m where m is the degree of H. Thus, the image of f^* is contained in $\mathcal{O}_U(V_p)$ and it is clear that f^* is a $\mathbb{C}$-homomorphism into this image. Thus f is a morphism. Finally f is not defined on $Z_{\mathbb{P}^r}(G_0, \ldots, G_N)$ because for any $a \in Z_{\mathbb{P}^r}(G_0, \ldots, G_N)$, $f(a) = [(0, \ldots, 0)]$ which is not a valid point in projective space, thus f cannot be defined on this set. □

Lecture 33. April 6, 2011

The Veronese embedding (cont.). First we show that ν_d is injective. Let $\overline{a} = (a_0, \ldots, a_r)$ and $\overline{b} = (b_0, \ldots, b_r)$ represent points in $\mathbb{P}^r$. Suppose that $\nu_d([\overline{a}]) = \nu_d([\overline{b}])$. Since $\overline{a} \neq \overline{0}$, we know $a_i \neq 0$ for some i. But $[(a_0^d, \ldots, a_r^d, \ldots)] = \nu_d([\overline{a}]) = \nu_d([\overline{b}]) = [(b_0^d, \ldots, b_r^d, \ldots)]$, so if $a_i \neq 0$ then also $a_i^d \neq 0$ and $b_i^d \neq 0$ and hence $b_i \neq 0$. Thus we can divide by either a_i or b_i and from $\nu_d([\overline{a}]) = \nu_d([\overline{b}])$ we see $G_j(\overline{a})/a_i^d = G_j(\overline{b})/b_i^d$ for all j. But among the monomials G_j we have $x_i^{d-1}x_k$ for each k, so

$$\frac{a_k}{a_i} = \frac{a_i^{d-1}a_k}{a_i^d} = \frac{b_i^{d-1}b_k}{b_i^d} = \frac{b_k}{b_i}.$$

Thus

$$\left(1, \frac{a_1}{a_i}, \ldots, \frac{a_r}{a_i}\right) = \left(1, \frac{b_1}{b_i}, \ldots, \frac{b_r}{b_i}\right)$$

hence $[\overline{a}] = [\overline{b}]$, so ν_d is injective.

Now in fact it is a fundamental result that a morphism of projective varieties is a closed map; i.e., the image of a closed set is always closed. We will not prove this, at least not now. Instead we'll show that the image of ν_d is closed.

Note that $(\nu_d|_{U_{x_i}})^* : \mathcal{O}_{\mathbb{P}^N}(U_{y_i}) \to \mathcal{O}_{\mathbb{P}^r}(U_{x_i})$ is the homomorphism

$$\mathbb{C}\left[\frac{y_0}{y_i}, \ldots, \frac{y_N}{y_i}\right] \to \mathbb{C}\left[\frac{x_0}{x_i}, \ldots, \frac{x_r}{x_i}\right]$$

given by $\frac{y_j}{y_i} \mapsto \frac{G_j}{x_i^d}$. This is surjective, since for each k there is a j such that $G_j = x_i^{d-1}x_k$, and hence $\frac{x_k}{x_i} = G_j/x_i^{d-1}$ is in the image of $(\nu_d|_{U_{x_i}})^*$. We can identify U_{y_i} with $\mathbb{A}^N$ by regarding

a point $[(c_0, \dots, c_N)] \in U_{y_i}$ As being the point $(c_0/c_i, \dots, c_{i-1}/c_i, c_{i+1}/c_i, \dots, c_N)] \in \mathbb{A}^N$. Let $I \subseteq \mathbb{C}[\frac{y_0}{y_i}, \dots, \frac{y_N}{y_i}]$ be the kernel of $(\nu_d|_{U_{x_i}})^*$ so

$$\mathbb{C}\Big[\frac{y_0}{y_i}, \dots, \frac{y_N}{y_i}\Big]/I \cong \mathbb{C}\Big[\frac{x_0}{x_i}, \dots, \frac{x_r}{x_i}\Big]. \tag{†}$$

Thus for any point $p \in U_{y_i} = \mathbb{A}^N$ in the zero locus of I, we have a maximal ideal $M_q \subset \mathbb{C}[\frac{x_0}{x_i}, \dots, \frac{x_r}{x_i}]$ corresponding under the isomorphism (†) to M_p/I. Thus $((\nu_d|_{U_{x_i}})^*)^{-1}(M_q) = M_p$ and hence $p = (\nu_d|_{U_{x_i}})(q)$; i.e., ν_d maps $U_{y_i})(U_{x_i})$ onto the closure of its image.

Since ν_d is injective, closed and continuous, it has a continuous inverse, and since ν_d restricted to each open set $U_{x_i} \subset \mathbb{P}^r$ is an isomorphism to its image, the inverse map is a morphism, so ν_d is an isomorphism.

Exercises:

Exercise 33.1. Let $V \subset \mathbb{P}^N$ be a projective variety. Let $0 \neq G \in \mathbb{C}[V]$ be homogeneous of degree $d = \deg(G) > 0$. Show that U_G is isomorphic to a closed subset of $\mathbb{A}^n$ for some n.

Solution. We give a sketch of the proof. Let $W = \nu_d(\mathbb{P}^N) \subseteq \mathbb{P}^r$, where $r = \binom{N}{d} - 1$. Thus W is closed in $\mathbb{P}^r$ and hence so is $\nu_d(V)$. Note that G is a linear combination of monomials of degree d. Taking the same linear combination but with the corresponding variables in $\mathbb{P}^r$ replacing the monomials we get a linear form $L \in \mathbb{C}[\mathbb{P}^r]$ such that $\nu_d^*(L) = G$ and hence such that $\nu_d^{-1}(Z_{\mathbb{P}^r}(L)) = Z_{\mathbb{P}^N}(G)$. Thus ν_d gives an isomorphism from U_G to $W \cap U_L$, while $U_L \subset \mathbb{P}^r$ is isomorphic to $\mathbb{A}^r$, so U_G is isomorphic to $W \cap U_L$ which is itself isomorphic to a closed subset of $\mathbb{A}^r$. □

Lecture 34. April 8, 2011

Grassmanians. Let V be a $\mathbb{C}$-vector space of dimension n and let r be an integer with $0 \leq r \leq n$. Let $\mathrm{Gr}(r, V)$, or $\mathrm{Gr}(r, n)$, denote the set of r-dimensional $\mathbb{C}$-vector subspaces of V. We call $\mathrm{Gr}(r, n)$ the *Grassmannian* of r-planes of V. So far $\mathrm{Gr}(r, n)$ is just a set, but we will soon see how to give it topological and geometric structure, so we think of the elements of $\mathrm{Gr}(r, n)$ as points.

Example 34.1. If $r = 0$ or $r = n$, then $\mathrm{Gr}(r, n)$ consists of a single point. Thus as a space it is natural to regard $\mathrm{Gr}(r, n)$ to be 0-dimensional in these cases. If $r = 1 < n + 1$, then there is a bijection between the points of $\mathrm{Gr}(r, n + 1)$ and lines through the origin in $\mathbb{C}^{n+1}$. But there is also a bijection between the points of $\mathbb{P}^n$ and lines through the origin in $\mathbb{C}^{n+1}$, so we can regard $\mathrm{Gr}(1, n + 1)$ as being $\mathbb{P}^n$, and thus it is natural to regard $\mathrm{Gr}(1, n + 1)$ as having dimension n.

Example 34.2. A subvariety $V \subseteq \mathbb{P}^n$ is said to be *linear* if either $V = \mathbb{P}^n$ or V is the zero-locus of linear homogeneous polynomials of $\mathbb{C}[\mathbb{P}^n]$. The dimension of a linear subvariety is the minimal number of linear homogeneous generators that generate I. The Grassmannian $\mathrm{Gr}(r + 1, n + 1)$ denotes the set of $(r + 1)$-dimensional $\mathbb{C}$-vector subspaces of $\mathbb{C}^{n+1}$, but there is a bijective correspondence between $(r + 1)$-dimensional $\mathbb{C}$-vector subspaces of $\mathbb{C}^{n+1}$ and r-dimensional linear subvarieties of $\mathbb{P}^n$, so we can also regard $\mathrm{Gr}(r + 1, n + 1)$ as the set of all r-dimensional linear subvarieties of $\mathbb{P}^n$, thus generalizing the previous example of thinking of $\mathrm{Gr}(1, n + 1)$ as being the set of points of $\mathbb{P}^n$.

Example 34.3. Let V be an n-dimensional vector space. There is a natural correspondence between subspaces of V of dimension r and subspaces of the dual vector space V^* of dimension $n - r$. In particular, given an r-dimensional subspace $W \subseteq V$, let $\widehat{W}$ be the subspace of V^* of all linear functionals $\lambda : V \to \mathbb{C}$ such that the nullspace of λ contains W. Then $\widehat{W}$ has dimension $n - r$. Likewise, given a subspace $U \subseteq V^*$ of dimension $n - r$, let $\widehat{U}$ be the subspace of all $v \in V$

such that $\lambda(v) = 0$ for all $\lambda \in U$. Then $\widehat{U}$ has dimension r, and we have both $\widehat{\widehat{U}} = U$ and $\widehat{\widehat{W}} = W$. Thus we get a bijection $\mathrm{Gr}(r, V) \cong \mathrm{Gr}(n-r, V^*)$; i.e., $\mathrm{Gr}(r, n) \cong \mathrm{Gr}(n-r, n)$.

The topological structure of $\mathrm{Gr}(r, n)$ comes from its being a homogeneous space; i.e., we can regard $\mathrm{Gr}(r, n)$ as being $\mathrm{GL}_n(\mathbb{C})/G$ for some subgroup G occurring as a stabilizer subgroup with respect to an action on $\mathrm{Gr}(r, n)$ by the group $\mathrm{GL}_n(\mathbb{C})$ of $n \times n$ invertible matrices with complex entries. In particular, let $W_1, W_2 \subseteq \mathbb{C}^n$ be vector subspaces of dimension r. Using a little linear algebra, it's easy to see that there are elements $g \in \mathrm{GL}_n(\mathbb{C})$ such that $gW_i = W_2$. Thus the action of $\mathrm{GL}_n(\mathbb{C})$ on $\mathrm{Gr}(r, n)$ is transitive. If we denote by G the stabilizer subgroup $G = \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{C})}(W_1) = \{g \in \mathrm{GL}_n(\mathbb{C}) : gW_1 = W_1\}$, then there is a bijection from the G-coset space $\mathrm{GL}_n(\mathbb{C})/G$ to $\mathrm{Gr}(r, n)$. Starting with the standard complex topology on $\mathrm{GL}_n(\mathbb{C})$, if we give $\mathrm{GL}_n(\mathbb{C})/G$ the quotient topology, then $\mathrm{Gr}(r, n)$ becomes a compact complex manifold.

Although we haven't rigorously defined the notion of dimension of a manifold or of a projective variety, we have some intuition as to what it should mean. The circle is a 1-dimensional real manifold, the 2-sphere is a 2-dimensional real manifold but also a 1-dimensional complex manifold, and complex projective n-space $\mathbb{P}^n$ is an n-dimensional complex manifold. If a projective variety is also a manifold, as is true for $\mathbb{P}^n$ for example, its dimension either as a manifold or as a variety agree.

So, as a manifold, $\mathrm{Gr}(r, n)$ has some dimension. To give a heuristic argument for what that dimension is, let $\mathbf{e_1}, \ldots, \mathbf{e_n}$ be the standard basis of $\mathbb{C}^n$. Let W be the span of $\mathbf{e_1}, \ldots, \mathbf{e_r}$. Then the stabilizer subgroup $G = \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{C})}(W)$ is the group of matrices of block matrix form

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

where $A \in \mathrm{GL}_r(\mathbb{C})$, the lower left block is an $(n-r) \times r$ 0-matrix, B is an arbitrary $r \times (n-r)$ matrix, and $C \in \mathrm{GL}_{n-r}(\mathbb{C})$. Thus we expect

$$\dim(\mathrm{Gr}(r, n)) = \dim(\mathrm{GL}_n(\mathbb{C})) - \dim(G) = n^2 - (r^2 + r(n-r) + (n-r)^2) = r(n-r).$$

As expected we get $\dim(\mathrm{Gr}(r, n)) = r(n-r) = (n-r)(n-(n-r)) = \dim(\mathrm{Gr}(n-r, n))$.

Next we will be interested in giving $\mathrm{Gr}(r, n)$ the structure of a projective variety. We do this by embedding $\mathrm{Gr}(r, n)$ in $\mathbb{P}^N$ for $N = \binom{n}{r}$, using the Plücker embedding.

Exercises:

Exercise 34.1. A subvariety of $\mathbb{P}^n$ is said to be *linear* if it is the zero-locus of linear homogeneous polynomials of $\mathbb{C}[\mathbb{P}^n]$. Let $I \subset \mathbb{C}[\mathbb{P}^n]$ be generated by linear homogeneous polynomials. Show that there is an isomorphism $\mathbb{P}^r \to Z_{\mathbb{P}^n}(I)$, where r is the minimal number of linear polynomials that generate I. Conclude that $Z_{\mathbb{P}^n}(I)$ is irreducible, hence a projective variety.

Solution. If we write $\mathbb{C}[\mathbb{P}^n] = \mathbb{C}[x_0, \ldots, x_n]$, we can, up to change of coordinates, assume that one of the linear forms is x_n. By induction it is enough to show that $Z_{\mathbb{P}^n}(x_n)$ is isomorphic to $\mathbb{P}^{n-1}$. But it is easy to check that $\phi : [(a_0, \ldots, a_{n-1})] \mapsto [(a_0, \ldots, a_{n-1}, 0)]$ defines an morphism $\phi : \mathbb{P}^{n-1} \to \mathbb{P}^n$ which is an isomorphism onto its image. Since $Z_{\mathbb{P}^n}(I) \cong \mathbb{P}^r$ and $\mathbb{P}^r$ is irreducible by Exercise 30.1 (since $\mathbb{P}^r$ is the closure of $\mathbb{A}^r$ whose coordinate ring $\mathbb{C}[\mathbb{A}^r]$ is a domain, hence is itself irreducible), $Z_{\mathbb{P}^n}(I)$ is irreducible, hence a projective variety. $\square$

Lecture 35. April 11, 2011

The Plücker Embedding. The Plücker embedding is an injective map of $\mathrm{Gr}(r, n) \to \mathbb{P}^N$, where $N + 1 = \binom{n}{r}$, whose image is a closed subset of $\mathbb{P}^N$. A natural way to study this map is via *exterior algebras*. If V is a vector space, the exterior algebra is denoted $\bigwedge V$. This is an elegant way to

do it, but we will not take the time to develop the necessary background to use this approach. However, elements of exterior algebras are essentially vectors whose entries are defined in terms of determinants. So exterior algebras are lurking behind the aproach we will use.

To start, let $\mathcal{M}$ be the set of all $n \times r$ rank r complex matrices. There are $N+1 = \binom{n}{r}$ r element subsets of the set $\mathcal{S} = \{1, \ldots, n\}$. Enumerate these subsets as $\mathcal{S}_0, \ldots, \mathcal{S}_N$. We may assume that $\mathcal{S}_0 = \{1, \ldots, r\}$.

Given $M \in \mathcal{M}$, let M_i denote the submatrix of M obtained by taking the rows of M corresponding to the elements of $\mathcal{S}_i$. Thus M_0 consists of rows 1 through r of M since $\mathcal{S}_0$ consists of the numbers 1 through r. Define a map $\delta_r : \mathcal{M} \to \mathbb{C}^{N+1} \setminus \{\overline{0}\}$ by setting $\delta_r(M) = (\det(M_0), \ldots, \det(M_N))$. Note that since each M_i is an $r \times r$ matrix it makes sense to take the determinant. Since some set of r rows of a matrix of rank r are linearly independent, we know $\det(M_i) \neq 0$ for some index i, and hence we know that $\delta_r(M) \neq \overline{0}$, so the image of δ_r is contained in $\mathbb{C}^{N+1} \setminus \{\overline{0}\}$. We now make two claims.

Claim I: The map δ_r induces a well-defined map $\mathrm{Gr}(r, n) \to \mathbb{P}^N$ which we will also denote by δ_r.

Here is how this induced map is defined. Let $p \in \mathrm{Gr}(r, n)$. Then p is an r-dimensional subspace of $\mathbb{C}^n$. Pick a basis of this subspace and use the basis vectors as the columns of an $n \times r$ matrix M, which necessarily has rank r. Now define $\delta_r(p)$ to be the point $[\delta_r(M)] \in \mathbb{P}^N$ represented by the vector $\delta_r(M) \in \mathbb{C}^{N+1}$.

Since we define the induced map by picking a matrix M representing the point p and defining $\delta_r(p)$ in terms of $\delta_r(M)$, we need to check that $\delta_r(p)$ is independent of our choice of M. But if N is another such choice, then M and N have the same column space (these both being the r dimensional subspace of $\mathbb{C}^n$ specified by p). But since $\mathrm{col}(M) = \mathrm{col}(N)$, there is a change of basis matrix $g \in \mathrm{GL}_r(\mathbb{C})$ with $N = Mg$. Thus

$$\begin{aligned}\delta_r(N) = \delta_r(Mg) &= (\det((Mg)_0), \ldots, \det((Mg)_N)) \\ &= (\det(M_0)\det(g), \ldots, \det(M_N)\det(g)) = \det(g)\delta_r(M),\end{aligned}$$

so $\delta_r(N)$ and $\delta_r(M)$ represent the same point of $\mathbb{P}^N$; i.e., $[\delta_r(N)] = [\delta_r(M)]$.

Claim II: The map $\delta_r : \mathrm{Gr}(r, n) \to \mathbb{P}^N$ is injective.

Given any $M \in \mathcal{M}$, let A_M denote the augmented $n \times (r+1)$ matrix where the first r columns of A_M are the columns of M and the $(r+1)$-st column of A_M is the transpose of $\overline{x} = (x_1, \ldots, x_n)$, so

$$A_M = [M \,|\, \overline{x}^T].$$

Then $\delta_{r+1}(A_M) = (L_0, \ldots, L_t)$, where $t = \binom{n}{r+1}$ and each L_i is a linear homogeneous polynomial in the variables x_i with coefficients taken from the entries of $\delta_r(M)$.

Note that a vector $\overline{x} = \overline{a}$ is a solution to the homogeneous system of equations $L_i = 0$ if and only if no subset of $r+1$ rows of $[M \,|\, \overline{a}^T]$ is linearly independent. This holds if and only if $[M \,|\, \overline{a}^T]$ has rank less than $r+1$, and for a matrix $M \in \mathcal{M}$ this is equivalent to $[M \,|\, \overline{a}^T]$ having rank r (since $\mathrm{rank}([M \,|\, \overline{a}^T]) \geq \mathrm{rank}(M) = r$). But $[M \,|\, \overline{a}^T]$ having rank r just means $\overline{a}^T$ is in the column space of M. I.e., the column space of M is the solution set of all vectors $\overline{x} = \overline{a}$ such that $\delta_{r+1}(A_M) = \overline{0}$.

Now say $p, q \in \mathrm{Gr}(r, n)$ and assume that $\delta_r(p) = \delta_r(q)$. Represent p and q by $n \times r$ rank r matrices $P, Q \in \mathcal{M}$. Thus p is the point corresponding to the column space of P and q is the point corresponding to the column space of Q. The fact that $\delta_r(p) = \delta_r(q)$ implies that $\delta_r(P)$ is a scalar multiple of $\delta_r(Q)$ and hence that $\delta_{r+1}(A_P)$ is a scalar multiple of $\delta_{r+1}(A_Q)$. Thus $\delta_{r+1}(A_P)$ and $\delta_{r+1}(A_Q)$ give the zero vector for the same solutions $\overline{x} = \overline{a}$. Thus P and Q have the same column space, and hence $p = q$.

Example 35.1. Suppose in the preceding discussion we have

$$P = \begin{pmatrix} a & b \\ c & d \\ e & f \\ g & h \end{pmatrix},$$

so with respect to a lexicographic ordering of the 2×2 submatrices of P we have $\delta_2(P) = (a_0, a_1, a_2, a_3, a_4, a_5)$, where

$$(a_0, a_1, a_2, a_3, a_4, a_5) = \left(\begin{vmatrix} a & b \\ c & d \end{vmatrix}, \begin{vmatrix} a & b \\ e & f \end{vmatrix}, \begin{vmatrix} a & b \\ g & h \end{vmatrix}, \begin{vmatrix} c & d \\ e & f \end{vmatrix}, \begin{vmatrix} c & d \\ g & h \end{vmatrix}, \begin{vmatrix} e & f \\ g & h \end{vmatrix} \right).$$

Then

$$A_P = \begin{pmatrix} a & b & x_1 \\ c & d & x_2 \\ e & f & x_3 \\ g & h & x_4 \end{pmatrix},$$

and it turns out that $\delta_3(A_P)$ is defined purely in terms of $\delta_2(P)$; in particular, it turns out by direct calculation that

$$\delta_3(A_P) = (a_3x_1 - a_1x_2 + a_0x_3, a_4x_1 - a_2x_2 + a_0x_4, a_5x_1 - a_2x_3 + a_1x_4, a_5x_2 - a_4x_3 + a_3x_4).$$

So if $[\delta_2(P)] = [\delta_2(Q)] \in \mathbb{P}^5$, then $\delta_2(Q) = \gamma\delta_2(P)$ for some non-zero scalar $\gamma \in \mathbb{C}$, hence $\delta_3(A_P) = \gamma\delta_3(Q)$, so the linear system of equations given by setting the entries of $\delta_3(A_P)$ equal to zero has the same solution set as the system of equations given by the entries of $\delta_3(A_Q)$. But the solution sets are the 2-dimensional subspaces of $\mathbb{C}^4$ corresponding to p and q, hence $p = q$ if $[\delta_2(P)] = [\delta_2(Q)]$.

Exercises:

Exercise 35.1. Let $f : R \to S$ be a surjective $\mathbb{C}$-homomorphism, where $R = \mathbb{C}[y_0, \ldots, y_r]$ and $S = \mathbb{C}[x_0, \ldots, x_s]$. For each i, pick an element $F_i \in R$ such that $f(F_i) = x_i$. Let $G_j(x_0, \ldots, x_s) = f(y_j)$. Show that the kernel of f is generated by the elements $y_j - G_j(F_0, \ldots, F_s)$.

Solution. Let $Q = \mathbb{C}[z_0, \ldots, z_{r+s+1}]$ and let $g : Q \to R$ be defined by $z_i \mapsto F_i$ for $0 \le i \le s$, $z_j \mapsto y_{j-s-1}$ for $s+1 \le j \le r+s+1$. Then generators of the kernel of $f \circ g$ map via g to generators of the kernel of f. Thus it suffices to show that $z_{s+1+i} - G_i(z_0, \ldots, z_s)$, $0 \le i \le r$, generate $\ker(f \circ g)$.

But $f \circ g : z_i \mapsto x_i$ for $0 \le i \le s$, and $f \circ g : z_i \mapsto G_{i-s-1}$ for $s+1 \le i \le r+s+1$. This reduces us to showing that the kernel of $\Phi : R \to S$ is generated by $y_i - G_i(x_0, \ldots, x_s)$ in the case that $R = \mathbb{C}[x_0, \ldots, x_s, y_0, \ldots, y_r]$ with $\Phi : x_i \mapsto x_i$ and $\Phi : y_i \mapsto G_i(x_0, \ldots, x_s)$.

Clearly, $y_i - G_i(x_0, \ldots, x_s) \in \ker(\Phi)$, so Φ induces a homomorphism

$$\phi : \overline{R} = R/(y_0 - G_0(x_0, \ldots, x_s), \ldots, y_r - G_r(x_0, \ldots, x_s)) \to S,$$

and it is enough to show this is an isomorphism. It's clearly surjective (since $\phi(\overline{x_i}) = x_i$). To see that it's injective, note that S occurs as a subring of R and any element $h \in R$ is equivalent modulo the ideal $(y_0 - G_0(x_0, \ldots, x_s), \ldots, y_r - G_r(x_0, \ldots, x_s))$ to an element $\eta \in S \subset R$. But $\phi(\overline{\eta}) = \eta$, so the only element $\overline{\eta}$ in $\ker(\phi)$ is $\overline{0}$. □

Exercise 35.2. If $f : \mathbb{A}^s \to \mathbb{A}^r$ is an algebraic map such that $f^* : \mathbb{C}[\mathbb{A}^r] \to \mathbb{C}[\mathbb{A}^s]$ is surjective, show that $f(\mathbb{A}^s)$ is a Zariski-closed subset of $\mathbb{A}^r$ and f is an isomorphism to its image.

Solution. Let $V = \overline{f(\mathbb{A}^s)}$. Then f induces a mapping $h : \mathbb{A}^s \to V$ of algebraic sets (where $h = f$ except that we restrict the range of h to be V), so by Corollary 14.2 it suffices to show that $h^* : \mathbb{C}[V] \to \mathbb{C}[\mathbb{A}^s]$ is an isomorphism. In particular, this implies that f maps $\mathbb{A}^s$ onto V, hence $f(\mathbb{A}^s) = V$ is closed, and isomorphic to $\mathbb{A}^s$.

Note $\ker(f^*) \subseteq I(V)$, since $g \in \ker(f^*)$ implies $0 = f^*(g) = g \circ f$ so $g(f(b)) = 0$ for all $b \in \mathbb{A}^s$, hence g vanishes on $V = f(\mathbb{A}^s)$, so $g \in I(V)$. Conversely, if $g \in I(V)$, then g vanishes on $V = f(\mathbb{A}^s)$ so $f^*(g) = g \circ f$ is identically 0 on $\mathbb{A}^s$, hence $g \in \ker(f^*)$. Thus h induces the $\mathbb{C}$-homomorphism $\mathbb{C}[V] = \mathbb{C}[\mathbb{A}^r]/I(V) = \mathbb{C}[\mathbb{A}^r]/\ker(f^*) \to \mathbb{C}[\mathbb{A}^s]$, which is an isomorphism as we wanted to show, since f^* is surjective by hypothesis.

This finishes the solution to this exercise, but it may be of interest to have a direct proof that f is bijective to its image. Let $\mathbb{C}[\mathbb{A}^s] = \mathbb{C}[x_1, \ldots, x_s]$. Say $p \neq q$ for $p, q \in \mathbb{A}^s$. Then there is an i such that $x_i(p) \neq x_i(q)$. But f^* is surjective, so there is a polynomial $g \in \mathbb{C}[\mathbb{A}^r]$ such that $f^*(g) = x_i$ and hence $x_i(p) = g(f(p)) \neq g(f(q)) = x_i(q)$, so $f(p) \neq f(q)$. Thus f is injective.

Next, we show that f is surjective to $V = \overline{f(\mathbb{A}^s)}$, and hence $f(\mathbb{A}^s)$ is a Zariski-closed subset of $\mathbb{A}^r$. Let $a \in V \subseteq \mathbb{A}^r$ and let $M_a \subset \mathbb{C}[\mathbb{A}^r] = \mathbb{C}[y_1, \ldots, y_r]$ be the maximal ideal corresponding to the point a. Then $a \in V$ implies $I(V) \subseteq M_a$, so $M_a/\ker(f^*) \subset \mathbb{C}[\mathbb{A}^r]/\ker(f^*)$ is a maximal ideal that maps under the isomorphism $\mathbb{C}[\mathbb{A}^r]/\ker(f^*) \cong \mathbb{C}[\mathbb{A}^s]$ induced by f^* to a maximal ideal M_b where $b \in \mathbb{A}^s$. Thus, if $f(b) = (c_1, \ldots, c_s)$ and $a = (a_1, \ldots, a_r)$, then $y_i - a_i \in M_a$ for all i, so $y_i \circ f - a_i = f^*(y_i - a_i) \in M_b$ vanishes at b, hence $0 = (y_i \circ f - a_i)(b) = c_i - a_i$ for all i, so $c_i = a_i$, hence $f(b) = a$. $\square$

Lecture 36. April 13, 2011

The Plücker Relations. The image $\delta_r(\mathrm{Gr}(r,n)) \subset \mathbb{P}^N$, $N = \binom{n}{r} - 1$, is Zariski-closed, defined by homogeneous polynomial equations known as the Plücker relations. To see that it is closed, it's enough by Exercise 36.1 to find an open cover of $\mathbb{P}^N$ such the intersection of $\delta_r(\mathrm{Gr}(r,n))$ with each open set in the open cover is closed. To define the open cover, let $\mathbb{C}[\mathbb{P}^N] = \mathbb{C}[y_0, \ldots, y_N]$. The open cover we will use is $\{U_{y_0}, \ldots, U_{y_N}\}$.

Consider $\delta_r(\mathrm{Gr}(r,n)) \cap U_{y_i}$ for some i. Recall that each variable y_i corresponds to a choice of r of the n rows of $n \times r$ matrices in the set $\mathcal{M}$ of all $n \times r$ matrices of rank r. We will work through the case $i = 0$ and assume that y_0 corresponds to the top r rows; other cases are treated similarly.

So let $p \in \mathrm{Gr}(r,n)$. Let $p = [M]$ for some $M \in \mathcal{M}$. Then $\delta_r([M]) = [(a_0, \ldots, a_N)] \in U_{y_0}$ if and only if $a_0 \neq 0$. But $a_0 = \det(M_0)$ is the determinant of the top r rows of M. Thus M_0 is an invertible matrix, so for some $g \in \mathrm{GL}_r(\mathbb{C})$ we can write Mg as the block matrix $Mg = \binom{I_r}{B}$, where B is an $(n-r) \times r$ matrix. The transposed matrix $(Mg)^T$ is just the reduced row echelon form of M, and thus has the same column space as does M and so represents the same point of $\mathrm{Gr}(r,n)$; i.e., $[M] = [Mg] \in \mathrm{Gr}(r,n)$. Moreover, by Exercise 36.2, if $\binom{I_r}{B}$ and $\binom{I_r}{C}$ represent the same point of $\mathrm{Gr}(r,n)$, i.e., if $[\binom{I_r}{B}] = [\binom{I_r}{C}]$ or equivalently if $\binom{I_r}{B}$ and $\binom{I_r}{C}$ have the same column space, then $B = C$.

Let $U_{y_0} \xrightarrow{\phi} \mathbb{A}^N$ be the map $\phi([(a_0, a_1, \ldots, a_N)]) = (a_1/a_0, \ldots, a_N/a_0)$; recall ϕ is an isomorphism. Note that if $a_0 = 1$, then ϕ is just truncation (i.e., drop the leftmost coordinate). Also, think of $\mathbb{A}^{(n-r)r} = \mathbb{C}^{(n-r)r}$ as the set of all $(n-r) \times r$ matrices, and let $\psi : \mathbb{A}^{(n-r)r} \to \mathrm{Gr}(r,n) \cap \delta_r^{-1}(U_{y_0})$ be the map $B \mapsto \left[\binom{I_r}{B}\right]$; by our observations of the previous paragraph, ψ is a bijection. We now have a map

$$\lambda_0 : \mathbb{A}^{(n-r)r} \to \mathrm{Gr}(r,n) \cap \delta_r^{-1}(U_{y_0}) \xrightarrow{\delta_r} U_{y_0} \xrightarrow{\phi} \mathbb{A}^N$$

defined by

$$B \mapsto \left[\begin{pmatrix} I_r \\ B \end{pmatrix}\right] \mapsto [(1, a_1, \ldots, a_N)] \mapsto (a_1, \ldots, a_N),$$

and the coordinate functions $B \mapsto a_i$ are given by polynomials in the entries of B (given by taking determinants of $r \times r$ submatrices of $\binom{I_r}{B}$). Thus λ is an algebraic map.

If we show that the induced $\mathbb{C}$-homomorphism $\lambda_0^* : \mathbb{C}[\mathbb{A}^N] \to \mathbb{C}[\mathbb{A}^{(n-r)r}]$ is surjective, then, by Exercise 35.2, $\delta_r(\mathrm{Gr}(r,n)) \cap U_{y_0}$ is closed, as we wanted to show, and we will obtain the Plücker relations by applying Exercise 35.1.

Exercises:

Exercise 36.1. Let $\{U_i\}$ be an open cover of a topological space X. Show that a subset $C \subseteq X$ is closed if and only if $C \cap U_i$ is closed in U_i for all i.

Solution by Melanie DeVries. Let C be closed in X. Then by definition of the subspace topology, $C \cap U_i$ is closed in U_i.

Conversely, let $C \cap U_i$ be closed for each i. Then $U_i \setminus (C \cap U_i)$ is open in each U_i and hence $U_i \setminus (C \cap U_i) = U \cap U_i$ for some open subset U of X, and thus $U_i \setminus (C \cap U_i)$ is open in X. Thus the union $\cup_i (U_i \setminus (C \cap U_i)) = (\cup_i U_i) \setminus C = X \setminus C$ is open, hence C is closed. □

Exercise 36.2. Let B and C be arbitrary $(n-r) \times r$ matrices and let $P = \binom{I_r}{B}$ and $Q + \binom{I_r}{C}$. Show that P and Q have rank r and that P and Q have the same column space if and only if $B = C$.

Solution by Ashley Weatherwax, as retyped (with minor modifications because I hate typing) by moi. Suppose that P does not have rank r. Then there is a column (say column i) of P that is a linear combination of the other columns of P. This means the top r rows of column i is a linear combination of the top r rows of the other columns of P, but this is impossible since the top r rows of P is a matrix of rank r. Similarly, Q has rank r.

Also, note if $B = C$, then $P = Q$ and so P and Q will have the same column space. Suppose that P and Q have the same column space. Let v be the ith column of P, so the top r rows of v just give the ith standard basis vector e_i. Since P and Q have the same column space, v is a linear combination of the columns of Q. Thus the top r rows of v is a linear combination of the top r rows of Q; i.e., e_i is a linear combination of the columns of I_r. The only such linear combination is to have e_i equal to the ith column of I_r, hence v is the ith column of Q. I.e., P and Q have the same columns so $B = C$. □

Lecture 37. April 15, 2011

The Plücker Relations (cont). To show that $\delta_r(\mathrm{Gr}(r,n)) \cap U_{y_i}$ is a closed subset of U_{y_i} for $i = 0$ (and in the same way for any i) and hence that $\delta_r(\mathrm{Gr}(r,n))$ is a closed subset of $\mathbb{P}^N$ it is enough (as mentioned above) to show that $\lambda_0^* : \mathbb{C}[\mathbb{A}^N] \to \mathbb{C}[\mathbb{A}^{(n-r)r}]$ is surjective. Now $\mathbb{C}[\mathbb{A}^N] = \mathbb{C}[y_1/y_0, \ldots, y_N/y_0]$ and $\mathbb{C}[\mathbb{A}^{(n-r)r}] = \mathbb{C}[x_{1,1}, \ldots, x_{n-r,r}]$, where we think of the elements of $\mathbb{A}^{(n-r)r}$ as $(n-r) \times r$ matrices and the variables $x_{i,j}$ correspond to the entries of those matrices. The homomorphism λ_0^* takes y_i/y_0 to the determinant of the ith $r \times r$ submatrix (with respect to some fixed enumeration of the submatrices) of the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ x_{1,1} & x_{1,2} & \cdots & x_{1,r-1} & x_{1,r} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,r-1} & x_{2,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n-r,1} & x_{n-r,2} & \cdots & x_{n-r,r-1} & x_{n-r,r} \end{pmatrix}. \tag{‡}$$

Each of the variables x_j (up to sign) is the determinant of some $r \times r$ submatrix of the matrix (‡). For example, each row of variables of (‡) is of the form $(x_{s,1}, x_{s,2}, \cdots, x_{s,r-1}, x_{s,r})$ for $1 \le s \le n-r$.

Consider

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ x_{s,1} & x_{s,2} & \cdots & x_{s,r-1} & x_{s,r} \end{pmatrix}. \tag{††}$$

Dropping the top row of (††) gives an $r \times r$ submatrix of (‡) with determinant $\pm x_{s,1}$. Dropping the second row gives an $r \times r$ submatrix with determinant $\pm x_{s,2}$, etc. In general, delete row k of the identity matrix I_r to get an $(r-1) \times r$ matrix M' and append row j of the $(n-r) \times r$ matrix whose entries are the variables $x_{s,t}$ to the bottom of M' to get an $r \times r$ matrix M''; then $\det(M'') = (-1)^{r-k} x_{j,k}$. Thus the image of λ_i^* includes all of the variables of $\mathbb{C}[\mathbb{A}^{(n-r)r}]$.

Thus λ_i^* is surjective as claimed for $i = 0$ (and also for any i by the analogous argument), and hence $\delta_r(\mathrm{Gr}(r,n))$ is a closed subset of $\mathbb{P}^N$. There is still the question of writing down homogeneous polynomials which cut out $\delta_r(\mathrm{Gr}(r,n))$ (i.e., whose common zero-locus in $\mathbb{P}^N$ is $\delta_r(\mathrm{Gr}(r,n))$). These polynomials are called the Plücker relations.

To write down the Plücker relations, first write down generators for the kernel of λ_i^* for each i. Say the generators for a given i are $H_{i1}, \ldots, H_{il_i}$, which we can give explicitly by Exercise 35.1. Each H_{ij} is a polynomial in $y_0/y_i, \ldots, y_N/y_i$. If $\deg(H_{ij}) = d$, then $H_{ij}^* = y_i^d H_{ij}$ is homogeneous of degree d in the variables $y_0, \ldots, y_N$, and by Exercise 37.1, the zero-locus of all of the H_{ij}^* is precisely $\delta_r(\mathrm{Gr}(r,n))$.

Example 37.1. Here we find the Plücker relations for $\delta_2(\mathrm{Gr}(2,4)) \subset \mathbb{P}^5$. We first consider the open set U_{y_0}. The corresponding homomorphism $\lambda_0^* : \mathbb{C}[y_1/y_0, \ldots, y_5/y_0] \to \mathbb{C}[x_1, \ldots, x_4]$ has $y_1/y_0 \mapsto G_1 = \det\begin{pmatrix} 1 & 0 \\ x_{1,1} & x_{1,2} \end{pmatrix} = x_{1,2}$, $y_2/y_0 \mapsto G_2 = \det\begin{pmatrix} 1 & 0 \\ x_{2,1} & x_{2,2} \end{pmatrix} = x_{2,2}$, $y_3/y_0 \mapsto G_3 = \det\begin{pmatrix} 0 & 1 \\ x_{1,1} & x_{1,2} \end{pmatrix} = -x_{1,1}$, $y_4/y_0 \mapsto G_4 = \det\begin{pmatrix} 0 & 1 \\ x_{2,1} & x_{2,2} \end{pmatrix} = -x_{2,1}$, $y_5/y_0 \mapsto G_5 = \det\begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} = x_{1,1}x_{2,2} - x_{1,2}x_{2,1}$. We also have $F_1 = -y_3/y_0 \mapsto x_{1,1}$, $F_2 = y_1/y_0 \mapsto x_{1,2}$, $F_3 = -y_4/y_0 \mapsto x_{2,1}$, and $F_4 = y_2/y_0 \mapsto x_{2,2}$. So now by Exercise 35.1 the kernel of λ_0^* is generated by $y_1/y_0 - G_1(F_1, \ldots, F_4) = 0$, $y_2/y_0 - G_2(F_1, \ldots, F_4) = 0$, $y_3/y_0 - G_3(F_1, \ldots, F_4) = 0$, $y_4/y_0 - G_4(F_1, \ldots, F_4) = 0$, and $y_5/y_0 - G_5(F_1, \ldots, F_4) = y_5/y_0 + (y_2/y_0)(y_3/y_0) - (y_1/y_0)(y_4/y_0)$. I.e., the kernel is generated by $y_5/y_0 + (y_2/y_0)(y_3/y_0) - (y_1/y_0)(y_4/y_0)$. Homogenizing gives the single Plücker relation $y_0y_5 + y_2y_3 - y_1y_4$. Repeating the same steps for the other open sets U_{y_i}, $i = 1, 2, 3, 4, 5$ gives in each case the same relation $y_0y_5 + y_2y_3 - y_1y_4$. Thus $\delta_2(\mathrm{Gr}(2,4))$ is the zero locus in $\mathbb{P}^5$ of the single polynomial $y_0y_5 + y_2y_3 - y_1y_4$.

Exercises:

Exercise 37.1. Let $\mathbb{C}[\mathbb{P}^N] = \mathbb{C}[y_0, \ldots, y_N]$, and let $C \subseteq \mathbb{P}^N$ be closed. Assume $H_{i1}, \ldots, H_{il_i} \in \mathbb{C}[y_0/y_i, \ldots, y_N/y_i] = \mathcal{O}_{\mathbb{P}^N}(U_{y_i})$ have zero-locus $C \cap U_{y_i}$, for each i. Let $H_{ij}^* \in \mathbb{C}[y_0, \ldots, y_N]$ be the homogenization of H_{ij}; i.e., $H_{ij}^* = y_i^d H_{ij}$ where $d = \deg(H_{ij})$. Then C is the zero-locus of the homogeneous polynomials $\{H_{ij}^*\}$.

Solution. For a fixed i and j, $Z_{\mathbb{P}^N}(H_{ij}^*) \cap U_{y_i} = Z(H_{ij}) \subset U_{y_i}$ and hence $Z_{\mathbb{P}^N}(\{H_{ij}^* : 1 \le j \le l_i\}) \cap U_{y_i} = U_{y_i} \cap C$. Thus the simultaneous zero-locus $Z_{\mathbb{P}^N}(\{H_{ij}^* : 1 \le j \le l_i, 0 \le i \le N\})$ is C. □

Exercise 37.2. Let $X \subseteq Y$ be topological spaces. If X is irreducible, then show that the closure $\overline{X}$ of X in Y is also irreducible.

Solution. If $\overline{X}$ is not irreducible, then there are nonempty closed subsets $A \subsetneq \overline{X}$ and $B \subsetneq \overline{X}$ with $\overline{X} = A \cup B$. Since $A \subsetneq \overline{X}$, then $X \not\subseteq A$ and likewise $X \not\subseteq B$, so $X \cap A$ and $X \cap B$ are nonempty proper closed subsets of X with union X, hence X is not irreducible. □

Lecture 38. April 18, 2011

Dimension and Smoothness.

38.1. **Dimension.**

Definition 38.1.1. Let X be a topological space. Define $\dim(X)$ to be the supremum of all n such that there exists a chain $\varnothing \subsetneq C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_n \subseteq X$ of closed irreducible subsets.

By Exercise 38.1, $\dim(\mathbb{A}^n) = 0$ if we give $\mathbb{A}^n$ the standard topology. However, if we give $\mathbb{A}^n$ the Zariski topology with $\mathbb{C}[\mathbb{A}^n] = \mathbb{C}[x_1, \ldots, x_n]$, take $C_0 = Z(x_1, \ldots, x_n) \cong \mathbb{A}^0$, $C_1 = Z(x_2, \ldots, x_n) \cong \mathbb{A}^1$, $C_2 = Z(x_3, \ldots, x_n) \cong \mathbb{A}^2$, etc., up to $C_{n-1} = Z(x_n) \cong \mathbb{A}^{n-1}$ and $C_0 = Z(0) = \mathbb{A}^n$. Each C_i is irreducible, since $\mathbb{C}[\mathbb{A}^i]$ is a domain. Thus $\dim(\mathbb{A}^n) \geq n$ now follows, but in fact we have $\dim(\mathbb{A}^n) = n$. This follows from Theorem 38.1.3 below, since $\operatorname{trdeg}_{\mathbb{C}}\mathbb{C}(\mathbb{A}^n) = n$.

Recall for a ring R that the Krull dimension of R, denoted simply $\dim(R)$, is the supremum of all n such that there is a chain of primes ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subseteq R$.

We now have:

Proposition 38.1.2. *Let X be a closed subset of $\mathbb{A}^n$. Then* $\dim(X) = \dim(\mathbb{C}[X])$.

Proof. There is a bijective inclusion reversing correspondence between primes ideals of $\mathbb{C}[X]$ and irreducible closed subsets of X. Thus Krull dimension of $\mathbb{C}[X]$ coincides with topological dimension of X. □

If X is a quasi-projective variety we can say more (see p. 6 of Hartshorne's *Algebraic Geometry*) for a version of the following result):

Theorem 38.1.3. *Let X be a quasi-projective variety and let $U \subseteq X$ be a nonempty open affine subset. Then* $\dim(X) = \dim(U) = \dim(\mathcal{O}_X(U)) = \operatorname{trdeg}(\mathbb{C}(X))$.

Terminology: If $X \subseteq Y$, then $\dim(X) \leq \dim(Y)$ by Exercise 38.3. We refer to $\dim(Y) - \dim(X)$ as the *codimension* of X in Y, written $\operatorname{codim}_Y(X)$.

Codimension is related to height. The *height* of a prime ideal P in a ring R is the supremum of all n such that there is a chain of primes $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$. Thus the Krull dimension of R is just the supremum of the heights of its prime ideals. If R is a domain which is a finitely generated $\mathbb{C}$-algebra, then a fundamental fact for any prime ideal $P \subset R$ is that

$$\operatorname{height}(P) + \dim(R/P) = \dim(R)$$

(see Theorem I.1.8A, p. 6 of Hartshorne's *Algebraic Geometry*). In geometrical terms this says: if $X \subseteq Y \subseteq \mathbb{A}^m$ are closed irreducible subsets, then $\operatorname{height}(I_Y(X)) + \dim(X) = \dim(Y)$ and hence $\operatorname{height}(I_Y(X)) = \operatorname{codim}_Y(X)$.

Krull's Hauptidealsatz is an important and useful result:

Theorem 38.1.4 (Krull's Hauptidealsatz)**.** *Let A be a Noetherian ring, and let $f \in A$ not be a zero-divisor (and thus not be 0) and not be a unit. Then every minimal prime of f has height 1. (I.e., if $P \subset A$ is a prime with $f \in P$ such that any prime $Q \subset A$ with $f \in Q \subseteq P$ has $Q = P$ (so P is a minimal prime of f), then P has height 1.)*

The following result is a corollary of the Hauptidealsatz:

Corollary 38.1.5. *Let $f \in \mathbb{C}[\mathbb{A}^n]$ be a polynomial of positive degree (i.e., not a constant). Let Y be an irreducible closed subset of $\mathbb{A}^n$ and assume that $Y \cap Z(f) \neq \varnothing$. Let X be an irreducible component of $Y \cap Z(f)$. Then* $\operatorname{codim}_Y(X) \leq 1$, *with equality if $X \neq Y$.*

Proof. If $Y \subseteq Z(f)$, then $X = Y$ and $\operatorname{codim}_Y(X) \leq 0$. So say $Y \not\subseteq Z(f)$. Thus the restriction $\overline{f}$ to Y gives an element $\overline{f} \in \mathbb{C}[Y]$ which is not 0, and, by assumption, $Y \cap Z(f) \neq \varnothing$, so $\overline{f}$ is not a unit. Thus the Hauptidealsatz says that any minimal prime $P \subset \mathbb{C}[Y]$ of $\overline{f}$ has height 1. In particular, $I_Y(X)$ is a minimal prime (since X is an irreducible component of $Z_Y(f)$), so in this case we have $1 = \operatorname{height}(I_Y(X)) = \operatorname{codim}_Y(X)$. □

38.2. **Smoothness.** Let $X \subseteq \mathbb{A}^n$ be an affine variety. Let $I(X) = (f_1, \ldots, f_r) \subset \mathbb{C}[\mathbb{A}^n] = \mathbb{C}[x_1, \ldots, x_n]$. The Jacobian matrix $\operatorname{Jac}(f_1, \ldots, f_r)$ is the $r \times n$ matrix J whose entries are $J_{i,j} = \partial f_i / \partial x_j$.

Definition 38.2.1. If $p \in X$ with X as above, we say p is *smooth* if the rank of $\operatorname{Jac}(f_1, \ldots, f_r)(p)$ is the codimension of X in $\mathbb{A}^n$. Otherwise we say p is a *singular* point of X.

Example 38.2.2. If X is a hypersurface (i.e., defined by a single polynomial f), then $p \in X$ is singular if and only if the gradient vanishes at p; i.e., if and only if $\nabla f(p) = (f_{x_1}(p), \ldots, f_{x_n}(p))$.

Exercises:

Exercise 38.1. For the standard topology on $\mathbb{C}^n \cong \mathbf{R}^{2n}$, show that the only irreducible subsets are points. [Hint: if a closed subset contains two points, consider the hyperplane in $\mathbf{R}^{2n}$ which is the perpendicular bisector of the line segment between the two points.]

Solution. Let C be a subset closed in the standard topology. Assume C contains distinct points p and q. Let H be the real hyperplane which is the perpendicular bisector to the real line segment from p to q. Then H is defined by a linear equation $L = 0$. Let A be the set of all points a such that $L(a) \geq 0$ and let B be the set of all points b such that $L(b) \leq 0$. Then $A \cap B = H$ while $A \cup B = \mathbf{R}^{2n}$, and may assume $p \in A$ and $q \in B$, but then $q \notin A$ and $p \notin B$, so $A \cap C$ and $B \cap C$ are nonempty proper closed subsets of C with union C. Thus C is not irreducible. Clearly individua points are irreducible, so they are the only irreducible subsets of $\mathbf{R}^{2n}$. □

Exercise 38.2. Let X be a closed subset of $\mathbb{A}^n$. Let $X_1, \ldots, X_r$ be the irreducible components of X. Show that $\dim(X) = \max_i(\dim(X_i))$.

Solution. Let X_0 be the component of maximum dimension, and say its dimension is d. Then X_0 has a chain $C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_d$ of closed irreducible subsets. These are necessarily also closed irreducible subsets of X, so $\dim X \geq d = \dim X_0$.

Let $D_0 \subsetneq D_1 \subsetneq \cdots \subsetneq D_e$ be any chain of closed irreducible subsets of X. Since D_e is irreducible, there must be a component X_i of X such that $D_e \subseteq X_i$, and hence $e \leq \dim X_i \leq \dim X_0$. Thus $\dim X \leq \dim X_0$. Therefore $\dim X = \dim X_0$. □

Exercise 38.3. Let $X \subseteq Y$ be topological spaces. Show that $\dim(X) \leq \dim(Y)$.

Solution. The closure of an irreducible subset is irreducible by Exercise 37.2, so if $C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_d$ is any chain of closed irreducible subsets of X, then their closures $\overline{C_i}$ in Y give a chain $\overline{C_0} \subsetneq \overline{C_1} \subsetneq \cdots \subsetneq \overline{C_d}$ of closed irreducible subsets of Y. Thus $\dim X \leq \dim Y$. □

Exercise 38.4. Let $X \subseteq Y \subseteq \mathbb{A}^n$ be irreducible closed subsets. Show that $\operatorname{codim}_{\mathbb{A}^n}(X) = \operatorname{codim}_Y(X) + \operatorname{codim}_{\mathbb{A}^n}(Y)$.

Solution. We have $\operatorname{codim}_{\mathbb{A}^n}(X) = \dim \mathbb{A}^n - \dim X = \dim \mathbb{A}^n - \dim Y + \dim Y - \dim X = \operatorname{codim}_{\mathbb{A}^n}(Y) + \operatorname{codim}_Y(X)$. □

Exercise 38.5. Let $f_1, \ldots, f_r \in \mathbb{C}[\mathbb{A}^n]$. Let X be an irreducible component of $Z(f_1, \ldots, f_r)$. Show that $\operatorname{codim}_{\mathbb{A}^n}(X) \leq r$.

Proof. By Corollary 38.1.5, every component of $Z(f_1)$ has codimension at most 1. If Y is a component of $Z(f_1, \ldots, f_{r-1})$, assume by induction that $\operatorname{codim}_{\mathbb{A}^n}(Y) \leq r-1$. Then again by Corollary 38.1.5, each component X of $Z(f_1, \ldots, f_r)$ has $\operatorname{codim}_Y(X) \leq 1$, hence by Exercise 38.4 we have $\operatorname{codim}_{\mathbb{A}^n}(X) = \operatorname{codim}_Y(X) + \operatorname{codim}_{\mathbb{A}^n}(Y) \leq r$. □

Lecture 39. April 20, 2011

Smoothness (cont.). We can extend the definition of smoothness to points of any closed affine subset. Let X be a closed subset of $\mathbb{A}^n$. Let $p \in X$ and let $I(X) = (f_1, \ldots, f_t)$. Let r be the maximum of the dimensions of the irreducible components of X containing p. Then we say that X is smooth at p if $\operatorname{rk}((\operatorname{Jac}(f_1, \ldots, f_t))(p)) = n - r$.

This makes it unclear to what extent smoothness is intrinsic. It seems to depend on n and on the choice of generators f_i. A theorem of Zariski shows that whether or not X is smooth at a point $p \in X$ is independent of the embedding of X in $\mathbb{A}^n$ and of the generators f_i:

Theorem 39.1 (Zariski)**.** *Let X be an affine algebraic set, $p \in X$, and let r be the maximum of the dimensions of the irreducible components of X which contain p. Then X is smooth at p if and only if $I_X(p)/(I_X(p))^2$, as a vector space over the field $\mathbb{C}[X]/I_X(p)$, has dimension r.*

For the proof of a version of this result, see Theorem I.5.1, p. 32 of Hartshorne's *Algebraic Geometry*.

Aside: This result led to the notion of regular local rings. A Neotherian ring R with a unique maximal ideal M is defined to be a *regular local ring* if M/M^2 has dimension $\dim(R)$ as an R/M-vector space.

Example 39.2. Let $X = Z(f) \subset \mathbb{A}^2$ for $f = xy \in \mathbb{C}[\mathbb{A}^2] = \mathbb{C}[x, y]$. To find the singular points we solve $\nabla f = \overline{0}$; i.e., $0 = \partial f/\partial x = y$ and $0 = \partial f/\partial y = x$. Thus the only solution is $x = 0$, $y = 0$, so the origin $(0, 0) \in X$ is the only singular point. Alternatively, using Zariski's criterion, we have $\mathbb{C}[X] = \mathbb{C}[x, y]/(xy)$. This ring consists of all polynomials of the form $g(x) + h(y)$ (i.e., polynomials in x and y with no cross terms). Let p be the origin. The maximal ideal $I_X(p)$ consists of all polynomials of the form $g(x) + h(y)$ such that $h(0) = 0$ and $h(0) = 0$. Thus $(I_X(p))^2$ consists of all polynomials of the form $g(x) + h(y)$ and with all terms of degree at least 2. Thus the images of x and y in $I_X(p)/(I_X(p))^2$ give a basis; i.e., $I_X(p)/(I_X(p))^2$ has dimension 2 but both components of X have dimension 1, so p is singular.

Now let $p = (1, 0)$. The x-axis is the only component of X containing p and it has dimension 1. Now $I_X(p)$ consists of all polynomials of the form $g(x) + h(y)$ such that $g(1) = 0$ and $h(y) = 0$; i.e., all polynomials of the form $(x - 1)l(x) + ym(y)$. Since $y, x - 1 \in I_X(p)$ we see that $-y(x - 1) = y \in (I_X(p))^2$, so $(I_X(p))^2$ consists of all polynomials of the form $(x - 1)^2 l(x) + ym(y)$, hence $x - 1$ maps to a basis of $I_X(p)/(I_X(p))^2$, so $I_X(p)/(I_X(p))^2$ has vector space dimension 1, hence p is a smooth point of X.

Example 39.3. Let $X = Z(f) \subset \mathbb{A}^2$ for $f = y^2 - x^3 \in \mathbb{C}[\mathbb{A}^2] = \mathbb{C}[x, y]$. Thus X is a curve defined parametrically by (t^2, t^3) for $t \in \mathbb{C}$, which gives the isomorphism $\mathbb{C}[X] = \mathbb{C}[t^2, t^3]$. To find the singular points we solve $\nabla f = \overline{0}$; i.e., $0 = \partial f/\partial x = -3x^2$ and $0 = \partial f/\partial y = 2y$. Thus the only solution is $x = 0$, $y = 0$, so the origin $(0, 0) \in X$ is the only singular point. Alternatively, using Zariski's criterion, we have $I_X(p)/(I_X(p))^2 = (t^2, t^3)/(t^2, t^3)^2 = \langle t^2, t^3, \ldots\rangle/\langle t^4, t^5, \ldots\rangle$ hence t^2 and t^3 map to a basis of $I_X(p)/(I_X(p))^2$, so its dimension is 2, versus X which has dimension 1, so p is a singular point of X.

Lecture 40. April 22 and April 25, 2011

Example 40.4. Here we show that $p = (1, 1)$ is a smooth point of $X = Z(f) \subset \mathbb{A}^2$ for $f = y^2 - x^3 \in \mathbb{C}[\mathbb{A}^2] = \mathbb{C}[x, y]$, using Zariski's criterion. We saw above that $(0, 0)$ is the only singular

point of X using the Jacobian criterion, so now we want to do an example using Zariski's criterion. Note that p is indeed a point of X, since $p \in Z(y^2 - x^3)$, and that the dimension of X is 1.

Under the isomorphism $\mathbb{C}[X] = \mathbb{C}[t^2, t^3]$, the ideal $I_X(p)$ is $(t^2 - 1, t^3 - 1)$. Thus we must show that $(t^2 - 1, t^3 - 1)/(t^2 - 1, t^3 - 1)^2$ is a 1 dimensional $\mathbb{C}$-vector space.

Note that we have a homomorphism $\Lambda : \mathbb{C}[t^2, t^3] \to \mathbb{C}[t]/((t-1)^2)$ given by composing the inclusion $\mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$ with the quotient $\mathbb{C}[t] \to \mathbb{C}[t]/((t-1)^2)$. The kernel of Λ contains $(t^2 - 1, t^3 - 1)^2$ since every element of $(t^2 - 1, t^3 - 1)$ is divisible in $\mathbb{C}[t]$ by $t - 1$. Thus Λ induces a $\mathbb{C}$-homomorphism $\lambda : \mathbb{C}[t^2, t^3]/(t^2 - 1, t^3 - 1)^2 \to \mathbb{C}[t]/((t-1)^2)$. For any polynomial $g \in \mathbb{C}[t]$, let $\overline{g}$ denote its image under the quotient $\mathbb{C}[t] \to \mathbb{C}[t]/((t-1)^2)$. Likewise, for any polynomial $f \in \mathbb{C}[t^2, t^3]$, let $\overline{f}$ denote its image in $\mathbb{C}[t^2, t^3]/(t^2 - 1, t^3 - 1)^2$.

We will show that λ is an isomorphism and that it maps $(t^2 - 1, t^3 - 1)/(t^2 - 1, t^3 - 1)^2$ isomorphically to $(t-1)/((t-1)^2)$. But note that $\{1, t-1, (t-1)^2, (t-1)^3, \ldots\}$ is a $\mathbb{C}$-vector space basis for the ring $\mathbb{C}[t]$ (since every polynomial has a unique Taylor series centered at $t = 1$), with $\{t-1, (t-1)^2, (t-1)^3, \ldots\}$ being a basis for $(t-1)$ and $\{(t-1)^2, (t-1)^3, \ldots\}$ being a basis for $((t-1)^2)$. Thus the image of $t - 1$ in $(t-1)/((t-1)^2)$ is a basis vector for $(t-1)/((t-1)^2)$; i.e., $(t-1)/((t-1)^2)$ and hence $(t^2 - 1, t^3 - 1)/(t^2 - 1, t^3 - 1)^2$ is 1 dimensional.

To show that λ is an isomorphism, first we show that λ is surjective. Note that λ is a $\mathbb{C}$-homomorphism, so it's enough to show that $\overline{t}$ is in the image of λ. But

$$\lambda((\overline{t}^2 + 1)/2) = (\overline{t}^2 + 1)/2 = (\overline{t}^2 + 1 - (\overline{t} - 1)^2)/2 = \overline{t},$$

so λ is surjective.

Also note that $\lambda^{-1}((\overline{t} - 1)) = (\overline{t}^2 - 1, \overline{t}^3 - 1)$. To see this it's enough to check that $\Lambda^{-1}((\overline{t} - 1)) = (t^2 - 1, t^3 - 1)$, which itself follows if we show that $(\mathbb{C}[t^2, t^3]) \cap (t - 1) = (t^2 - 1, t^3 - 1)$, where the intersection takes place in $\mathbb{C}[t]$. Clearly, $(t^2 - 1, t^3 - 1) \subseteq (\mathbb{C}[t^2, t^3]) \cap (t - 1)$. To see the reverse containment, let $f \in (\mathbb{C}[t^2, t^3]) \cap (t - 1)$. Writing $f = a_0 + a_1 t + \cdots + a_n t^n$ for constants $a_i \in \mathbb{C}$, having $f \in \mathbb{C}[t^2, t^3]$ means $a_1 = 0$, while $f \in (t - 1)$ means $0 = f(1) = a_0 + a_2 + \cdots + a_n$ and hence $a_0 = -(a_2 + \cdots + a_n)$. Thus

$$f = -(a_2 + \cdots + a_n) + a_2 t^2 + \cdots + a_n t^n = \sum_{i \geq 2} (a_i t^i - a_i) = \sum_{i \geq 2} a_i (t^i - 1). \qquad (*)$$

For $i = 2, 3$ we have $t^i - 1 \in (t^2 - 1, t^3 - 1)$. For $i > 3$ we have $t^i - 1 = (t^i - t^2) + (t^2 - 1) = t^2(t^{i-2} - 1) + (t^2 - 1) \in (t^2 - 1, t^3 - 1)$. Thus each term of f in $(*)$ is in $(t^2 - 1, t^3 - 1)$ so $f \in (t^2 - 1, t^3 - 1)$. Thus λ induces a surjective homomorphism $(t^2 - 1, t^3 - 1)/(t^2 - 1, t^3 - 1)^2 \to (t - 1)/((t - 1)^2)$.

Aside: This shows that $(t^2 - 1, t^3 - 1) = \Lambda^{-1}(\overline{t} - 1)$. We might be tempted at this point to claim that therefore $(t^2 - 1, t^3 - 1)^2$ is the kernel of Λ since $((\overline{t} - 1)^2) = (\overline{0})$, and hence that λ is injective but this is not sound reasoning; see Exercise 40.1.

So we still need to check that λ is injective. But since $\lambda : \mathbb{C}[t^2, t^3]/(t^2 - 1, t^3 - 1)^2 \to \mathbb{C}[t]/((t-1)^2)$ is surjective and $\mathbb{C}[t]/((t-1)^2)$ has $\mathbb{C}$-vector space dimension 2 (with basis given by the images of 1 and $t - 1$), we see that $\mathbb{C}[t^2, t^3]/(t^2 - 1, t^3 - 1)^2$ has $\mathbb{C}$-vector space dimension at least 2. On the other hand, $(t^2 - 1, t^3 - 1)^2 = ((t^2 - 1)^2, (t^2 - 1)(t^3 - 1), (t^3 - 1)^2) = (t^4 - 2t^2 + 1, t^5 - t^3 - t^2 + 1, t^6 - 2t^3 + 1)$. Moreover, $(2 + t^2)(t^4 - 2t^2 + 1) - (t^6 - 2t^3 + 1) = 2t^3 - 3t^2 + 1 \in (t^2 - 1, t^3 - 1)^2$. Thus, modulo $(t^2 - 1, t^3 - 1)^2$, every polynomial in $\mathbb{C}[t^2, t^3]$ can be reduced to a polynomial of degree at most 2 and hence of the form $a + bt^2$. Thus $\mathbb{C}[t^2, t^3]/(t^2 - 1, t^3 - 1)^2$ has $\mathbb{C}$-vector space dimension at most 2, and hence exactly 2.

Thus λ, being surjective, is also injective as a vector space homomorphism, and thus it is injective, as we wanted to show.

Here are a few additional facts about smoothness for a closed subset $X \subseteq \mathbb{A}^n$. Let $p \in X$. Then we have the following facts.

(a) The maximum r of the dimensions of the irreducible components of X containing p is a lower bound on the dimension of the Zariski tangent space of X at p:

$$\dim_{\mathbb{C}} I_X(p)/I_X(p)^2 \geq r.$$

(See Atiyah-Macdonald, Corollary 11.15, p. 121 for a version of this.)

(b) If X is smooth at p, then $\mathbb{C}[X]_{I_X(p)}$ is a domain. (See Theorem I.5.4A of Hartshorne's *Algebraic Geometry.*)

(c) If p lies on more than one component of X, then X is singular at p. (See Exercise 40.2.)

Exercises:

Exercise 40.1. Let $f : A \to B$ be a homomorphism of rings. Let $I \subseteq B$ be an ideal and let $J = f^{-1}(I)$. Show by example that it need not be true that $J^2 = f^{-1}(I^2)$.

Solution. Let $f : \mathbb{C}[x] \to \mathbb{C} = \mathbb{C}[x]/(x)$ be the quotient map. Let $I = (0)$ so $J = \ker(f) = (x)$. Then $I^2 = I = (0)$, so $f^{-1}(I^2) = J = (x) \neq (x^2) = J^2$. □

Exercise 40.2. Consider a closed subset $X \subseteq \mathbb{A}^n$. If p lies on more than one component of X, show that X is singular at p. [Hint: show that $\mathbb{C}[X]_{I_X(p)}$ is not a domain.]

Solution. Let C_p be an irreducible component of X containing p and let D_p be a different irreducible component of X containing p. Let C be the union of C_p with all irreducible components of X except D_p and let D be the union of D_p with all irreducible components of X except C_p. Thus $X = C \cup D$ (and hence $I(X) \subseteq I(C) \cap I(D)$), where $p \in C \cap D$ and where C and D are closed, proper subsets of X. Thus there are elements $f \in I(C) \setminus I(X)$ and $g \in I(D) \setminus I(X)$ such that $fg \in I(X)$. Since $I(C) \subseteq I(p)$ and $I(D) \subseteq I(p)$, we see $f, g \in I(p)$. Modding out by $I(X)$ gives $\overline{0} \neq \overline{f} \in I_X(C)$ and $\overline{0} \neq \overline{g} \in I_X(D)$ but $\overline{f}\overline{g} = \overline{0}$.

Let $^* : \mathbb{C}[X] \to \mathbb{C}[X]_{I_X(p)}$ be the localization homomorphism. Then $\overline{f}^* \neq \overline{0}^*$, for if $\overline{f}^* = \overline{0}^*$, there would be an element $s \in \mathbb{C}[\mathbb{A}^n]$ such that $\overline{s} \notin I_X(p)$ (and hence $s \notin I(p)$) but $\overline{s}\overline{f} = \overline{0}$ in $\mathbb{C}[X]$. Thus sf vanishes on all of X. However, $f \in I(C) \setminus I(X)$ implies that f does not vanish on D_p so s vanishes on D_p, which implies $s(p) \neq 0$ and therefore contradicts $s \notin I(p)$. Similarly, $\overline{g}^* \neq \overline{0}^*$, yet $\overline{f}^*\overline{g}^* = \overline{0}^*$, so $\mathbb{C}[X]_{I_X(p)}$ is not a domain and hence X is not smooth at p. □

Exercise 40.3. Let A be a ring, M a maximal ideal of A and I an M-primary ideal. Let B be the localized ring A_M and $J = IB$ the ideal generated by I in B. Show that the canonical homomorphism $F : A \to B$ (induced by $a \mapsto \frac{a}{1}$) induces an isomorphism $f : A/I \to B/J$. [Note that therefore modding out by I has the effect of inverting all elements not in M.]

Solution. Given $a \in A$, let $\overline{a}$ denote the image of a in A/I, and likewise Given $b \in B$, let $\overline{b}$ denote the image of b in B/J. Let $S = A \setminus M$. Then $\overline{s}$ is a unit in A/I for every $s \in S$. To see this, consider $I + (s)$. Since I is M-primary, $\sqrt{I} = M$, so $\sqrt{I + (s)} = \sqrt{I} + \sqrt{(s)} = M + \sqrt{s}$ contains both M and s hence equals (1). Thus $1^n = 1 \in I + (s)$, so $1 = i + us$ for some $u \in A$ and $i \in I$ and hence $\overline{1} = \overline{us}$, and therefore $\overline{s}$ is a unit as claimed.

Clearly $F(I) \subseteq J$, so F induces a homomorphism $f : A/I \to B/J$. Say $f(\overline{a}) = \overline{0}$. Then $F(a) \in J$, so there is an element $s \in A \setminus M$ and an element $c \in I$ such that $\frac{a}{1} = F(a) = \frac{c}{s}$, hence there is a $t \in A \setminus M$ such that $t(sa - c) = 0$ in A. Thus $\overline{t}\overline{sa} = \overline{t}\overline{c} = \overline{0} \in A/I$, and since $\overline{t}\overline{s}$ is a unit in A/I, we see $\overline{a} = \overline{0}$, so f is injective.

Now consider any $\overline{b} \in B/J$. Then $b = \frac{a}{s}$ for some $a \in A$ and $s \in S$. Let $\overline{u}$ be the inverse of $\overline{s}$. Then $f(\overline{s}^{-1}\overline{a}) = f(\overline{ua}) = \overline{F(au)} = \overline{\frac{a}{1}\frac{u}{1}} = \overline{\frac{a}{s}} = b$, so f is surjective and hence an isomorphism. □

Lecture 41. April 27, 2011

We can extend the definition of smoothness to closed subsets of projective space. Let $p \in X \subseteq \mathbb{P}^N$, where X is closed in $\mathbb{P}^N$. Pick an i such that $p \in U_{x_i}$ and regard $p \in X \cap U_{x_i} \subseteq U_{x_i} \cong \mathbb{A}^N$. If p is a smooth point of $X \cap U_{x_i}$ regarded as a closed subset of $\mathbb{A}^N$, we say p is a smooth point of X.

Consider $X = Z_{\mathbb{P}^N}(F) \subset \mathbb{P}^N$, where $F \in \mathbb{C}[\mathbb{P}^N] = \mathbb{C}[x_0, \ldots, x_N]$ is non-constant and homogeneous. Let $d = \deg(F)$, so $d > 0$. Let $p \in \mathbb{P}^N$. If $\frac{\partial F}{\partial x_i}(p) = 0$ for all i, then $F(p) = (\sum_i x_i \frac{\partial F}{\partial x_i}(p))/d = 0$ so $p \in X$. By Exercise 41.1, p is a singular point of X.

Example 41.5. Let $F = zy^2 - x^3 \in \mathbb{C}[\mathbb{P}^2]$. Consider $X = Z_{\mathbb{P}^2}(F) \subset \mathbb{P}^2$. Then $\nabla(F) = (-3x^2, 2zy, y^2)$. Thus $\nabla(F)(p) = \overline{0}$ if and only if $x = y = 0$, so the singular locus of X consists of a single point, $p = (0, 0, 1)$.

Divisors: Let X be a smooth, irreducible, quasi-projective variety. A *prime divisor* is a closed irreducible subset of X of codimension 1. Define $\mathrm{Div}(X)$ to be the free abelian group on the prime divisors of X.

Each prime divisor $D \subset X$ determines a discrete valuation ν_D. Recall that a *discrete valuation* on a field K is a surjective map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ such that the only element of K mapping to ∞ is $0 \in K$. The map ν must satisfy $\nu(ab) = \nu(a) + \nu(b)$ and $\nu(a + b) \geq \min(\nu(a), \nu(b))$. The set R of all $a \in K$ with $\nu(a) \geq 0$ is a Noetherian ring, called the *valuation ring* of ν, and K is the field of fractions of R. A *discrete valuation ring* (or DVR) is a ring R occurring in this way. (See Atiyah-Macdonald, p. 94, for background on DVRs.)

Before explaining where the discrete valuation associated to a prime divisor comes from in general, we do an example.

Example 41.6. Let $X = \mathbb{A}^1 = \mathbb{C}$, so $\mathbb{C}[X] = \mathbb{C}[x]$. Then the prime divisors on X are just the single points of X. Thus an element of $\mathrm{Div}(X)$ is an expression of the form $\sum_{p \in X} m_p p$, where $m_p \in \mathbb{Z}$ for all $p \in \mathbb{A}^1$, and such that $m_p = 0$ for all but finitely many p. Let $K = \mathbb{C}(X)$ so $K = \mathbb{C}(x)$ is the function field of X. A point $p \in X$ is just an element of $\mathbb{C}$. Given $p \in X$, the associated discrete valuation ν_p is defined as follows. For any $f \in \mathbb{C}[X] = \mathbb{C}[x]$, let $\nu_p(f)$ be the order of vanishing of f at p; i.e., the largest m such that $(x - p)^m$ divides f. If f is the 0 element, we set $\nu_p(f) = \infty$. If $f, g \in \mathbb{C}[x]$ with g not the 0 element, we define $\nu_p(f/g) = \nu_p(f) - \nu_p(g)$; this extends ν_p to all of K. The valuation ring R in this case is the localization $\mathbb{C}[x]_{(x-p)}$ of $\mathbb{C}[x]$ at the maximal ideal $(x - p)$, and for any element $0 \neq f \in R$we can regard $\nu_p(f)$ as the largest m such that $f \in M^m$, where M is the unique maximal ideal of R (i.e., the ideal generated in R by $x - p$). The valuation ν_p specifies the order of zero (or pole) that an element $f/g \in K$ has at p. If $\nu_p(f/g) = -m < 0$, then we can say that f/g has a zero of order $-m$, but it's more common to say that f/g has a *pole* of order m at p.

Since $\mathbb{C}[x]$ is a UFD, it's easy to see that $\nu_p(fg) = \nu_p(f) + \nu_p(g)$ for $f, g \in \mathbb{C}[x]$ and this extends to $\mathbb{C}(x)$. The fact that $\nu_p(f + g) \geq \min(\nu_p(f), \nu_p(g))$ comes from the fact that you can get cancellation when you add, but when you drop terms the order of zero at a point can go up. For example, if $f = (x - p)^5 - 7(x - p)^2$ and $g = (x - p)^8 + 7(x - p)^2$, then $\nu_p(f) = 2$ and $\nu_p(g) = 2$, but $\nu_p(f + g) = 5$. The valuations of f and g come from their terms of least degree (when regarded as polynomials in $x - p$; i.e., as polynomials centered at p), but adding f to g cancels these least degree terms, leading to $f + g$ having an increased valuation. When cancellation doesn't occur, such as for $f = (x - p)^5 - 7(x - p)^2$ and $g = (x - p)^8 + 7(x - p)^3$, the term of f of least degree survives in $f + g$ to become the term of $f + g$ of least degree, and the valuation of $f + g$ comes from this term of least degree, which in this case gives $\nu_p(f + g) = \min(\nu_p(f), \nu_p(g)) = \min(2, 3) = 2$.

Exercises:

Exercise 41.1. Let $F \in \mathbb{C}[\mathbb{P}^N]$ be non-constant and homogeneous. Show that p is a singular point of $Z_{\mathbb{P}^N}(F)$ if and only if $(\nabla F)(p) = \overline{0}$.

Solution. Assume $(\nabla F)(p) = \overline{0}$; then as we saw above $p \in X$. Say F is the polynomial $F(x_0, \ldots, x_N)$, where $\mathbb{C}[\mathbb{P}^N] = \mathbb{C}[x_0, \ldots, x_N]$. For some i we have that $p \in U_{x_i}$. Thus $p \in Z_{\mathbb{P}^N}(F) \cap U_{x_i} = Z_{\mathbb{A}^N}(F(x_0/x_i, \ldots, x_N/x_i))$, and p is singular if $(\partial F/\partial(x_j/x_i))(p) = 0$ for all $j \neq i$. But we have $(\partial F/\partial(x_j/x_i))(p) = 0$ if and only if $(\partial F/\partial x_j)(p) = 0$, hence if $(\nabla F)(p) = \overline{0}$, then p is a singular point of X.

Conversely, if p is a singular point of X, then $p \in X$, so $F(p) = 0$. As before, $p \in U_{x_i}$ and hence $(\partial F/\partial(x_j/x_i))(p) = 0$ for all $j \neq i$, so $(\partial F/\partial x_j)(p) = 0$ for $j \neq i$. But $F(p) = (\sum_l x_l \frac{\partial F}{\partial x_l}(p))/d = 0$ while $x_i(p) \neq 0$ and $\frac{\partial F}{\partial x_l}(p) = 0$ for $l \neq i$, so $\frac{\partial F}{\partial x_i}(p) = 0$, hence $(\nabla F)(p) = \overline{0}$. □

Exercise 41.2. Recall that a valuation ring is a domain R such that for each element r of the field of fractions K of R we have either $x \in R$ or $x^{-1} \in R$ (see Atiyah-Macdonald, p. 65). Show that a DVR is a valuation ring.

Solution. See Atiyah-Macdonald for the proof. □

Lecture 42. April 29, 2011

Given a smooth quasi-projective variety X and a prime divisor $D \subset X$, let $U \subseteq X$ be any open affine subset of X such that $U \cap D \neq \varnothing$. Let $\mathcal{O}_{X,D}$ be the localization of $\mathcal{O}_X(U)$ at the prime ideal $I_U(D)$. Then $\mathcal{O}_{X,D}$ turns out to be a DVR; denote the corresponding valuation on $\mathbb{C}(X)$ by ν_D. Given any $f \in \mathbb{C}(X) \setminus \{0\}$, there are only finitely many prime divisors D such that $\nu_D(f) \neq 0$ (see Hartshorne's *Algebraic Geometry*, Lemma II.6.1, p. 131). Thus the sum $\operatorname{div}(f) = \sum_D \nu_D(f)D$ over all prime divisors D on X is itself a divisor. A divisor coming in this way from a non-trivial rational function f is called a *principal* divisor.

Since $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$, the set of principal divisors is a subgroup $\operatorname{PrDiv}(X)$ of $\operatorname{Div}(X)$. The quotient group $\operatorname{Div}(X)/\operatorname{PrDiv}(X)$ is called the *divisor class group* of X, denoted $\operatorname{Cl}(X)$. If D_1 and D_2 are divisors whose images $[D_i]$ in $\operatorname{Cl}(X)$ are the same (i.e., if there is a rational function f such that $D_1 = D_2 + \operatorname{div}(f)$), we say that D_1 and D_2 are *linearly equivalent*.

Example 42.7. Let $X = \mathbb{A}^N$. Then there is a bijection between the irreducible polynomials in $\mathbb{C}[\mathbb{A}^N]$ (modulo scalar multiples) and prime divisors; given an irreducible $F \in \mathbb{C}[\mathbb{A}^N]$, the corresponding prime divisor is $Z(F)$. Choose such an F for each prime divisor D and denote it F_D. Given any divisor $m_1D_1 + \cdots + m_rD_r$, where each D_i is a prime divisor, $f = \Pi_i F_{D_i}^{m_i} \in \mathbb{C}(X)$ is a rational function with $\operatorname{div}(f) = m_1D_1 + \cdots + m_rD_r$. Thus $\operatorname{PrDiv}(X) = \operatorname{Div}(X)$ and $\operatorname{Cl}(X) = 0$.

Example 42.8. Let $X = \mathbb{P}^N$. Then there is a bijection between the irreducible homogeneous polynomials in $\mathbb{C}[\mathbb{P}^N]$ (modulo scalar multiples) and prime divisors; given an irreducible homogeneous $F \in \mathbb{C}[\mathbb{P}^N]$, the corresponding prime divisor is $Z_{\mathbb{P}^N}(F)$. If we define the degree $\deg(D)$ of D to be the degree of F, we get a homomorphism $\deg : \operatorname{Div}(X) \to \mathbb{Z}$ whose kernel is $\operatorname{PrDiv}(X)$; i.e., $\operatorname{PrDiv}(X)$ is precisely the subgroup of divisors of degree 0. (See Hartshorne's *Algebraic Geometry*, Proposition II.6.4, p. 132.)

Let X be a smooth quasi-projective variety. Let $D = m_1D_1 + \cdots + m_rD_r$ be a divisor where $D_1, \ldots, D_r$ are distinct prime divisors. We say D is *effective* if $m_i \geq 0$ for all i. For any divisor D, effective or not, we write $|D|$ for the set of all effective divisors linearly equivalent to D, and we write $L(D)$ for the set of rational functions f such that either $f = 0$ or $D + \operatorname{div}(f)$ is effective. Since for any prime divisor P we have $\nu_P(f + g) \geq \min(\nu_P(f), \nu_P(g))$, it follows that $L(D)$ is a

$\mathbb{C}$-vector space, and we can regard $|D|$ as the associated projective space (i..e., as the 1-dimensional subspaces of $L(D)$).

A fundamental fact is that if X is a smooth projective variety, $L(D)$ is a finite dimensional vector space (see Hartshorne's *Algebraic Geometry*, Theorem III.5.2, p. 228). Studying the dimension of $L(D)$ for various D is a major issue in algebraic geometry. One of the most important theorems in algebraic geometry is the theorem of Riemann-Roch, which bounds the dimension of $L(D)$ by numerical data related to X and D.

Department of Mathematics, University of Nebraska, Lincoln, NE 68588-0130 USA
E-mail address: bharbour@math.unl.edu