Course Notes for Math 737 (Algebraic Geometry)

12. Varieties. The Nullstellensatz. The Hilbert Nullstellensatz is proved. We will extract some geometric information from the proof, as well as algebraic corollaries of the theorem. We define closed immersions, dominant and finite regular maps of affine varieties, explore some properties of finite maps and prove that every affine variety is a "ramified cover" of an affine space of the same dimension.

Hilbert's Nullstellensatz: If k is an algebraically closed field, then:

(a) The ideals $\langle x_1 - a_1, ..., x_n - a_n\rangle$ for $(a_1, ..., a_n) \in \mathbf{A}_k^n$ are the **only** maximal ideals in $k[x_1, ..., x_n]$.

(b) The radical ideals in $k[x_1, ..., x_n]$ are precisely the geometric ideals. If $I \subset k[x_1, ..., x_n]$ is any ideal, then $I(V(I)) = \text{rad}(I)$.

We will need the following analogue of algebraic dependence of fields:

Definition: Suppose $f : A \to B$ is a homomorphism of commutative rings with 1. Then B is **integrally dependent upon** A if each $b \in B$ is the solution to some monic polynomial:

$$x^n + f(a_{n-1})x^{n-1} + ... + f(a_0) = 0.$$

Proposition 12.1: (a) Suppose B is finitely generated as an A-algebra. Then B is integrally dependent upon A if and only if B is finitely generated as an A-**module**.

(b) Integral dependence is transitive.

Proof: (a) Let $b_1, ..., b_m \in B$ generate B as an A-algebra. If B is integrally dependent upon A, then each b_i satisfies a monic polynomial $x^{n_i} +$ lower order $= 0$, or, to put it differently, each $b_i^{n_i}$ can be rewritten as a linear combination of lower order terms with coefficients in $f(A)$. But this allows us to generate B as an A-**module** by monomials $b_1^{i_1}...b_m^{i_m}$ as i_j vary from 0 to $n_j - 1$. Conversely, suppose B is generated by $b_1, ..., b_m$ as an A-module and consider $b \in B$. Let $f(a_{i,j})$ be a matrix representing the A-linear "multiplication by b". That is, $bb_i = \sum_{j=1}^m f(a_{i,j})b_j$. Then the matrix $M := (bI - f(a_{i,j}))$ annihilites every A-linear combination of the b_i's, hence by Cayley's theorem, $\det(M)$ annihilates every element of B, including 1, so that $\det(M) = 0$. But $\det(M)$ is a monic polynomial in b.

(b) Without loss of generality, suppose $A \subset B \subset C$ and $c \in C$ satisfies a given monic polynomial $c^n + b_{n-1}c^{n-1} + ... + b_0 = 0$. If B is integrally dependent upon A, then the subring $A[b_1, ..., b_{n-1}] \subset B$ must be finitely generated as a module over A by (a), therefore the ring $A[b_1, ..., b_{n-1}, c]$ is also finitely generated as an A-module, hence by (a) again, c satisfies a monic polynomial with coefficients in A, and the Proposition is proved.

We'll use the following lemma for the proof of the Nullstellensatz and in other contexts as well. It is an analogue for integral domains of the existence of a transcendence basis for field extensions:

Noether Normalization Lemma: Suppose A is an integral domain, which is finitely generated as a k-algebra. If the field of fractions of A has transcendence degree n over k, then there is an injective map $f : k[x_1, ..., x_n] \hookrightarrow A$, such that A is integrally dependent upon $k[x_1, ..., x_n]$.

Proof: (Nagata) Suppose $a_1, ..., a_m \in A$ is a framing of A. We will prove the lemma by induction on m. That is, we show that if $m > n$, then there exist $b_1, ..., b_{m-1} \in A$ such that A is integrally dependent upon $k[b_1, ..., b_{m-1}] \subset A$. If $m = n$, then $f : k[x_1, ..., x_n] \to A;\ x_i \mapsto a_i$ must be injective, hence an isomorphism, so the lemma follows.

If $m > n$, then there must be a nonzero polynomial $f(x_1, ..., x_m)$ such that $f(a_1, ..., a_m) = 0$ in A because otherwise, $x_1, ..., x_m$ would be algebraically independent in the field of fractions. Choose integers $r_1, ..., r_{m-1}$ inductively satisfying the constraints:

$$r_i > \deg(f(x_1, x_2 + x_1^{r_1}, ..., x_i + x_1^{r_{i-1}}, x_{i+1}, ..., x_m)),$$

and let $b_i = a_{i+1} - a_1^{r_i}$.

We define a new polynomial $g(x_1, ..., x_m) = f(x_1, x_2 + x_1^{r_1}, ..., x_m + x_1^{r_{m-1}})$, and observe that $g(a_1, b_1, ..., b_{m-1}) = 0$ by construction. Moreover, by the choice of the integers r_i, it follows that the term in $g(x_1, ..., x_m)$ of highest degree is of the form λx_1^N, coming from the monomial $\lambda x_1^{n_1} ... x_m^{n_m}$ in f where the "word" $(n_m, n_{m-1}, ..., n_1)$ is lexicographically as large as possible. But dividing by $\lambda \in k$ gives a monic polynomial satisfied by a_1 with coefficients in the subring generated by the b_i. The other $a_i = b_{i-1} + a_1^{r_i}$ must therefore also be integrally dependent upon this subring, and the lemma is proved.

Now we are ready for the:

Proof of the Nullstellensatz: (a) Suppose k is algebraically closed, and $m \subset k[x_1, ..., x_n]$ is a maximal ideal. Then via the maps:

$$k \hookrightarrow k[x_1, ..., x_n] \to k[x_1, ..., x_n]/m =: K$$

we have an inclusion of fields $k \subset K$. Thus either $k = K$ or else K has transcendence degree $m > 0$ over k. But K is finitely generated as a k-algebra, so by the Lemma, positive transcendence degree would imply that there is a polynomial ring $A := k[y_1, ..., y_m] \subset K$ upon which K is integrally dependent. But if $a \in A$, then $a^{-1} \in K$ is a root of a monic polynomial:

$$x^n + a_1 x^{n-1} + ... + a_n = 0, \quad a_i \in A$$

and evaluating at a^{-1} and multiplying through by a^{n-1}, we get:

$$a^{-1} = -(a_1 + a_2 a + ... + a_n a^{n-1}) \in A.$$

So A is a field(!) A polynomial ring is never a field. So $k = K$.

But in this case, we must have $k + m = k[x_1, ..., x_n]$, and for each x_i, there must be elements $a_i \in k$ such that $x_i - a_i \in m$, so m contains the ideal generated by the $x_i - a_i$, and it must **be** that ideal by maximality.

(b) Suppose we are given $\langle f_1, ..., f_m \rangle \subset k[x_1, ..., x_n]$, and suppose that $g \in I(V(f_1, ..., f_m))$. We will prove that $g^N \in \langle f_1, ..., f_m \rangle$ for some N. Since the converse is obviously true, this tells us that $I(V(I)) = \mathrm{rad}(I)$ for all ideals I, hence in particular, that $I(V(I)) = I$ for all **radical** ideals I, and thus geometric ideals are the same as radical ideals.

Construct a new ideal $I \subset k[x_1, ..., x_{n+1}]$ generated by the polynomials $f_i(x_1, ..., x_n)$ and $1 - x_{n+1} g(x_1, ..., x_n)$. If $(p_1, ..., p_n, p_{n+1}) \in V(I)$, then necessarily $(p_1, ..., p_n) \in V(f_1, ..., f_m)$, which implies that $g(p_1, ..., p_n) = 0$ by assumption, and $1 - x_{n+1} g$ cannot then vanish at $(p_1, ..., p_{n+1})$. So $V(I) = \emptyset$. But by (a), this implies that I is not contained in any maximal ideal. In other words, $1 \in I$.

So there exist polynomials $h_1, ..., h_m$ and $h \in k[x_1, ..., x_{n+1}]$ such that

$$1 = \sum_{i=1}^{m} h_i f_i + h(1 - x_{n+1} g).$$

If we substitute g^{-1} for x_{n+1}, we get:

$$1 = \sum_{i=1}^{m} h(x_1, ..., x_n, g^{-1}(x_1, ..., x_n)) f_i(x_1, ..., x_n),$$

and clearing denominators by multiplying by a sufficiently high power of g, we see that $g^N \in \langle f_1, ..., f_m \rangle$, as desired.

There are numerous corollaries we can draw from the Nullstellensatz.

Corollaries: Suppose k is an algebraically closed field. Then:

(a) If A is an integral domain and a finitely generated k-algebra, then $A \cong k[V]$ for some affine variety V. If K is a field of finite type over k, then $K \cong k(V)$ for some affine variety V.

(b) If A, B are integral domains and finitely generated k-algebras, then $A \otimes_k B$ is also an integral domain. (See §11)

(c) If $f \in k[x_1, ..., x_n]$, then write $f = f_1^{n_1} ... f_m^{n_m}$ as a product of irreducible polynomials. Then $I(V(f)) = \langle \prod f_i \rangle$ and similarly for homogeneous polynomials. Thus, for instance, if $n = 2$ and f is square-free, then $V(f)$ is a plane curve of degree $\deg(f)$ (compare with the hard work we needed in §4 when we couldn't assume k was algebraically closed).

Proof: Prime ideals are radical ideals, hence geometric ideals by the Nullstellensatz. Thus condition (2) preceding Proposition 11.6 is superfluous when k is algebraically closed, and (a) and (b) follow from §11.

In (c), we have $\mathrm{rad}(\langle f \rangle) = \langle \prod f_i \rangle$.

Here's a more involved corollary:

Corollary 12.2: Suppose V is an affine variety over an algebraically closed field and $\phi \in k(V)$. Then ϕ is regular if and only if $V =$ domain(ϕ).

Remark: This is false without the assumption on k. E.g. $\frac{1}{1+x^2} \in k(\mathbf{A}^1_{\mathbf{R}})$.

Proof: Let $\phi = \frac{f}{g}$ and consider the set: $I = \{g' \in k[V] \mid \frac{f'}{g'} \sim \frac{f}{g}\} \cup \{0\}$. This is an ideal in $k[V]$ (the "ideal of denominators of ϕ") because if $\frac{f}{g} \sim \frac{f'}{g'} \sim \frac{f''}{g''}$ and $g' \neq -g''$, then $\frac{f}{g} \sim \frac{f'+f''}{g'+g''}$ and $\frac{f}{g} \sim \frac{af'}{ag'}$ for any nonzero $a \in k[V]$.

Notice that $V(I) = V - \text{domain}(\phi)$. We assume $\text{domain}(\phi) = V$ and aim to prove $\phi \in k[V]$ (the other direction is obvious). Let J be the ideal containing $I(V)$ in $k[x_1, ..., x_n]$ corresponding to I. Then $J = \langle h_1, ..., h_m \rangle$ for some polynomials $h_1, ..., h_m$ by the basis theorem, and $V(J) = V(I) = \emptyset$, so J is not contained in any maximal ideal by the Nullstellensatz(!) and Lemma 3.1 (otherwise we would have $p \in V(J)$ for some p), so $J = k[x_1, ..., x_n]$ and in particular, $1 \in J$. Thus:

$$1 = \sum_{i=1}^{m} u_i h_i \text{ for some polynomials } u_i$$

and taking images in $k[V]$, we get $1 = \sum_{i=1}^{m} \overline{u}_i g_i$ where $g_i \in I$ is the image of $h_i \in J$. But this means $1 \in I$, so that there is an $a \in k[V]$ such that $\frac{f}{g} \sim \frac{a}{1}$. That is, $\phi \in k[V]$.

Remark: You may want to think of this as an algebraic version of the statement: "holomorphic functions are meromorphic functions with no poles".

Now for a projective version of the Nullstellensatz:

Definitions: (a) The homogeneous maximal ideal $m := \langle x_0, ..., x_n \rangle \subset k[\mathbf{P}_k^n]$ is called the **irrelevant maximal ideal**.

(b) The set $C(V) := \{(p_0, ..., p_n) \in \mathbf{A}_k^{n+1} \mid (p_0 : ... : p_n) \in V\} \cup \{(0, ..., 0)\}$ is the **affine cone over** $V \subset \mathbf{P}_k^n$. It is immediate from the definitions (§1) that if $V = V(I) \neq \emptyset$ is a projective algebraic set and k is infinite, then $C(V) = V(I)$, thought of as an algebraic subset of $\mathbf{A}_k^{n+1}$.

Projective Nullstellensatz: If k is algebraically closed, then except for the irrelevant maximal ideal, the homogeneous radical ideals in $k[x_0, ..., x_n]$ are precisely the homogeneous geometric ideals.

Proof: An algebraically closed field is infinite, in particular, so geometric ideals are automatically homogeneous (HW §1). Also, the radical of a homogeneous ideal is homogeneous, as you may check.

Suppose $I \subset k[x_0, ..., x_n]$ is a homogeneous ideal and let $V = V(I) \subset \mathbf{P}_k^n$ be the corresponding projective algebraic subset. By the Nullstellensatz, we know that $I(V(I)) = I(C(V)) = \text{rad}(I) \subset k[\mathbf{A}_k^{n+1}]$, when we perform the operations $V(*)$ and $I(*)$ in the context of $\mathbf{A}_k^{n+1}$.

But from the definitions in §1, it follows that if we perform the operation $I(*)$ in $\mathbf{P}^n_k$, we get $J = I(V)$, which does not agree with the previous $I(C(V))$, but rather with $I(C(V) - (0, ..., 0))$ because the origin is missing in projective space. On the other hand, if $C(V) - (0, ..., 0)$ is dense in $C(V)$ in the Zariski topology, it follows that $J = I(C(V))$, hence $J = \text{rad}(I)$.

But unless $C(V) - (0, ..., 0)$ is empty (which happens exactly in case $I(V(I)) = \text{rad}(I) = m$), $C(V)$ contains an affine line through the origin, and since $\mathbf{A}^1_k - 0$ is obviously dense in $\mathbf{A}^1_k$, it follows that $C(V) - (0, ..., 0)$ is dense in $C(V)$. Thus we have shown that unless $\text{rad}(I) = m$, we have $J = \text{rad}(I)$. But as in the Nullstellensatz, this proves that the rest of the homogeneous radical ideals are precisely the homogeneous geometric ideals.

Remark: In Corollary 12.2, we have used the Nullstellensatz to conclude that if $V(I) = \emptyset$ in affine space, then $1 \in I$. In the context of projective space, we cannot conclude $1 \in I$ but rather that $m \subseteq \text{rad}(I)$.

Definition: A regular map $\Phi : V \to W$ of affine varieties is called:

(a) a **closed immersion** if $\Phi^* : k[W] \to k[V]$ is surjective,

(b) **dominant** if $\Phi^* : k[W] \to k[V]$ is injective, and

(c) **finite** if $k[V]$ is integrally dependent upon $k[W]$ (via Φ^*).

Proposition 12.3: (a) $\Phi : V \to W$ is a closed immersion if and only if the image of Φ is an affine variety $Z \subset W$, and the map to Z is an isomorphism.

(b) Φ is dominant if and only if its image is Zariski dense in W.

(c) Any regular map Φ is a composition $\Phi = \Psi \circ \Gamma$ where Γ is dominant and Ψ is a closed immersion. Moreover, Φ is finite if and only if Γ is finite.

Proof: For (a), we may assume that $W = \mathbf{A}^n_k$, and suppose $V \subset \mathbf{A}^m_k$. Then the content of (a) is the statement that $I := \ker(\Phi^*) \subset k[x_1, ..., x_n]$ is a geometric ideal. Let $Z = V(I)$ (an affine variety since I is prime). Just from the fact that $I \subseteq \ker(\Phi^*)$, it follows that we can factor $\Phi : V \to Z \subset \mathbf{A}^n_k$. But if $f \notin I$, then $\Phi^*(f) \neq 0$, so $\Phi^*(f)$ fails to vanish at some point of V, and it is thus impossible that $f \in I(Z)$. So $I = I(Z)$ is geometric, and $\Phi : V \to Z$ is an isomorphism because $\Phi^* : k[Z] \to k[V]$ is an isomorphism. We've already proved (b) in §11, and (c) is the first isomorphism theorem for rings and the definition of integral dependence.

Examples: (i) A composition of closed immersions is a closed immersion, and similarly for dominant maps and finite maps (by Proposition 12.1).

(ii) The map $\Phi = (x, xy) : \mathbf{A}_k^2 \to \mathbf{A}_k^2$ is dominant, so it has a dense image. But $\Phi(\mathbf{A}_k^2) \subset \mathbf{A}_k^2$ is neither open nor closed. Notice that $y \in k[x, y]$ does not satisfy a monic polynomial with coefficients in $k[x, xy]$, so Φ is not finite.

(iii) The projection $\pi : V(x - y^2) \to \mathbf{A}_k^1$ given by $\pi(x, y) = x$ is finite and dominant, because $k[x, y]/\langle x - y^2\rangle$ is generated as a $k[x]$-module by $1, y$.

Notice that π is surjective and $2:1$ everywhere except at the origin if k is algebraically closed. If $k = \mathbf{R}$, the image is the nonnegative reals, which is dense but not Zariski closed. And if $k = \mathbf{Q}$, then the image is even more peculiar, but still Zariski dense, because it is infinite.

Finite maps are very important. Here are some first properties:

Proposition 12.4: Suppose $\Phi : V \to W$ is a finite map. Then:

(a) $\Phi^{-1}(p)$ is a finite set for all $p \in W$ (hence the term "finite") and

(b) if k is algebraically closed, then Φ is a closed map.

In particular, if Φ is also dominant in (b), then Φ is surjective.

(By the examples above, (b) is certainly not true in general if $k \neq \overline{k}$.)

The proof of the Proposition requires another commutative algebra result:

Cohen-Seidenberg Going Up: Suppose $B \subset A$ are commutative rings with 1 and A is integrally dependent upon B. Then every prime ideal in B is the intersection of B with a prime ideal in A.

Proof: Given a prime ideal $\mathcal{P} \subset B$, let $M = B - \mathcal{P}$. If we localize both A and B with respect to the multiplicative set M (see HW # 2), we get natural maps $i : A \to A_M, j : B \to B_M$ in a commuting diagram:

$$\begin{array}{ccc} A & \stackrel{i}{\to} & A_M \\ \cup & & \cup \\ B & \stackrel{j}{\to} & B_M \end{array}$$

Now B_M is a local ring with maximal ideal m satisfying $\mathcal{P} = j^{-1}(m)$. If we find an ideal $m' \subset A_M$ such that $m' \cap B_{\mathcal{P}} = m$, it follows that $i^{-1}(m') \cap B = j^{-1}(m' \cap B_{\mathcal{P}}) = \mathcal{P}$, and we will have proved the result.

Let $I \subset A_M$ be **any** maximal ideal. Then $B_M/(B_M \cap I) \subset A_M/I$ and A_M/I is integrally dependent upon $B_M/(B_M \cap I)$ (it is easy to see that A_M is integrally dependent upon B_M, and trivial to see that this implies the integral dependence of the quotients). But A_M/I is a field, so as in the proof of the Nullstellensatz, $B_M/(B_M \cap I)$ is a field also, which implies that $B_M \cap I = m$, the **unique** maximal ideal.

Proof of the Proposition: We prove (b) first. Since a closed immersion is a closed map, (this follows from 12.3(a)) and since a composition of closed maps is closed, we can assume Φ is dominant, by 12.3(c). Thus we can assume Φ^* is the inclusion of rings $k[W] \subset k[V]$. Suppose $Y \subset V$ is an algebraic subset and let $I = I(Y)$. By §11 HW # 2, we know that $\overline{\Phi(Y)} = V(I \cap k[W])$. We need to show that equality holds.

Suppose $q \in V(I \cap k[W])$. Let $m_q \supset I \cap k[W]$ be the corresponding maximal ideal. If we find a maximal ideal $m' \subset k[V]$ such that $m' \cap k[W] = m$ and $m' \supset I$, then using the Nullstellensatz(!), we see that $V(m') = p$ for some $p \in Y \subset V$, and by §11 HW # 2 again, it follows that $\Phi(p) = q$. But consider the (integrally dependent) inclusion of commutative rings with 1: $k[W]/(I \cap k[W]) \subset k[V]/I$. Going Up tells us that given the maximal ideal $\overline{m}_q \subset k[W]/(I \cap k[W])$ corresponding to $m_q \subset k[W]$, there is a prime ideal $\mathcal{P} \subset k[V]/I$ such that $\mathcal{P} \cap (k[W]/(I \cap k[W])) = \overline{m}_q$. Then any maximal ideal in $k[W]/I$ containing $\mathcal{P}$ corresponds to a maximal ideal in $k[V]$ with the desired properties.

(a) Suppose $p \in W$, and let $m_p \subset k[W]$ be the associated maximal ideal. Then $\Phi^{-1}(p) = V(I)$, where $I \subset k[V]$ is the ideal generated by the subset $\Phi^*(m_p) \subset k[V]$ by §11 HW # 2. We need to see that $V(I)$ is a finite set.

Either $I = k[V]$, and we are done, because in that case $V(I) = \emptyset$, or else $(\Phi^*)^{-1}(I) = m_p$ (it is an ideal containing m_p, after all), so $k[V]/I$ is integrally dependent upon the subring $k \cong k[W]/m_p$. By Proposition 12.2, $k[V]/I$ is therefore a finite-dimensional vector space over k. But a k-algebra which is a finite-dimensional vector space over k can have only finitely many maximal ideals (see Lemma 12.5 below). So there are only finitely many maximal ideals in $k[V]/I$, hence only finitely many maximal ideals in $k[V]$ containing I, which tells us that $V(I) = \Phi^{-1}(p)$ must consist of only finitely many points.

Lemma 12.5: Suppose A is a commutative ring with 1. If $m_1, ..., m_r \subset A$ are distinct maximal ideals, then the natural map:

$$A/m_1 \cap ... \cap m_r \to \times_{i=1}^r A/m_i$$

is an isomorphism. In particular, if A is a k-algebra of rank r as a vector space over k, then A can have at most r maximal ideals.

Proof: This is the Chinese Remainder Theorem(!) We proceed by induction on r. If $r = 1$, the result is obvious. Suppose the Lemma holds for r distinct maximal ideals. Since there are exactly r maximal ideals in the product of fields: $\times_{i=1}^r A/m_i$ it follows that $m_1, ..., m_r$ must be the only maximal ideals containing $m_1 \cap .. \cap m_r$. Thus if m_{r+1} is a new maximal ideal, then $m_{r+1} + (m_1 \cap ... \cap m_r) = A$, and by the Chinese Remainder Theorem, we get the isomorphism:

$$A/m_1 \cap ... \cap m_r \cap m_{r+1} \xrightarrow{\sim} \times_{i=1}^r A/m_i \times A/m_{r+1}.$$

Example: Consider the projection $\pi : V := V(x - y^2) \to \mathbf{A}^1_{\mathbf{Q}}$ again. Recall from the proof of the Proposition that $\pi^{-1}(p) = V(\langle x - p \rangle) \subset V(x - y^2)$.

(i) If p is not a perfect square, then $k[V]/\langle x-p \rangle \cong \mathbf{Q}[x, y]/\langle x-y^2, x-p \rangle \cong \mathbf{Q}[\sqrt{p}]$. Thus $\langle x - p \rangle$ is a maximal ideal in $k[V]$, but it does not correspond to any point in V.

(ii) If $p \neq 0$ is a perfect square, then $k[V]/\langle x - p \rangle \cong \mathbf{Q} \times \mathbf{Q}$ via the maximal ideals $\langle y \pm \sqrt{p} \rangle$ which intersect in $\langle x - p \rangle$, and which correspond to the two points $(p, \pm\sqrt{p}) = \pi^{-1}(p)$.

(iii) $k[V]/\langle x \rangle \cong \mathbf{Q}[y]/\langle y^2 \rangle =: A$. This has a unique maximal ideal, $\langle y \rangle$, and $A/\langle y \rangle \cong \mathbf{Q}$. This corresponds to the unique point $(0, 0) = \pi^{-1}(0)$.

Definition: A finite dominant map $\Phi : V \to W$ is **ramified** over $q \in W$ if $\langle \Phi^*(m_p) \rangle =: m_q k[V] \subset k[V]$ is not an intersection of maximal ideals.

Thus the map π above is ramified exactly over the origin in $\mathbf{A}^1_{\mathbf{Q}}$. Because of ramification, we see that even over an algebraically closed field, the number of points in $\Phi^{-1}(p)$ may depend upon p, becoming smaller over points where the map is ramified. It is perhaps counterintuitive, but even without ramification it is possible for the number of points in a fiber to vary:

Example: Consider the parametrization $\rho : \mathbf{A}^1_k \to W = V(y^2 - x(x+1))$ from §4 given by $\rho(t) = (t^2 - 1, t(t^2 - 1))$. This is certainly finite, because $k[t]$ is generated by $1, t$ as a module over $k[t^2 - 1, t^3 - t]$. You can check that ρ is not ramified over any point of W, but that $\rho^{-1}(0,0) = \{-1, 1\}$ and the other preimages are unique.

With coverings in topology, we can simply define the degree to be the number of preimages of a point. Obviously in light of the previous examples, we need to be more careful with finite maps:

Proposition 12.6: If $\Phi : V \to W$ is finite and dominant, then $k(V)$ is a finite field extension of $k(W)$. The **degree** of Φ is, by definition, the degree $[k(V) : k(W)]$ of the field extension.

Proof: Suppose $k[V]$ is generated by $b_1, ..., b_m$ as a $k[W]$-module. Then I claim $k(V)$ is generated by $b_1, ..., b_m$ as a field extension of $k(W)$ as well(!) To see this, suppose $\frac{f}{g} \in k(V)$. Then $g \in k[V]$ satisfies a (minimal) monic polynomial over $k[W]$:

$$g^n + a_{n-1}g^{n-1} + ... + a_1 g + a_0 = 0.$$

Since $k[V]$ is an integral domain and $g \neq 0$, it follows that $a_0 \neq 0$. But then $-a_0 = g(g^{n-1} + ... + a_1)$ so it follows that $\frac{f}{g} \sim \frac{h}{a_0}$ where $h = -f(g^{n-1} + ... + a_1)$. In other words, every fraction can be put in a form where the denominator is in $k[W]$. But then it follows immediately that the b_i generate the field extension.

Examples: The degree of π above is 2 because $k(V) \cong \mathbf{Q}(\sqrt{x})$ is a degree two extension of $\mathbf{Q}(x)$. On the other hand, the degree of ρ above is 1 because $k(t^2 - 1, t^3 - t) = k(t)$. The point is that the extra generator t becomes redundant when we are allowed to take fractions, as $t = \frac{t^3 - t}{t^2 - 1}$.

In light of all we now know about finite maps, the following geometric version of Noether Normalization is a significant property of affine varieties:

Geometric Noether Normalization: If V is an affine variety of dimension n, then there is a dominant finite map $\Phi : V \to \mathbf{A}^n_k$.

Proof: By the Noether Normalization Lemma, there is an injective k-algebra homomorphism $\Phi^* : k[x_1, ..., x_n] \hookrightarrow k[V]$, such that $k[V]$ is integrally dependent upon $k[x_1, ..., x_n]$. The map Φ is the associated regular map.

Seventh Homework Assignment

1. A crash course on radical ideals. If A is a commutative ring with 1 and $I \subset A$ is an ideal, then:

$$\mathrm{rad}(I) := \{f \in A \mid f^n \in I \text{ for some } n\}.$$

(a) Prove that $\mathrm{rad}(I)$ is an ideal, and prove that:

(b) $\mathrm{Rad}(0) = \cap \mathcal{P}$, the intersection of all prime ideals of A, more generally,

(c) $\mathrm{Rad}(I) = \cap_{I \subseteq \mathcal{P}} \mathcal{P}$, the intersection of the prime ideals containing I, and finally,

(d) If A is graded and I is homogeneous, then $\mathrm{rad}(I)$ is homogeneous.

2. A crash course on localization. A subset $M \subset A$ of a commutative ring with 1 is **multiplicative** if $1 \in M, 0 \notin M$, and $m, n \in M$ implies $mn \in M$. Given M, one defines:

$$A_M := \{\frac{a}{m} \mid a \in A, m \in M\}/\sim$$

with the usual addition and multiplication of fractions, where $\frac{a}{m} \sim \frac{a'}{m'}$ if $n(am' - a'm) = 0$ for some $n \in M$.

(a) Check that $\sim$ is an equivalence relation, and that addition and multiplication are well-defined. Prove that A_M is a commutative ring with 1, and that the natural map $\iota : A \to A_M; a \mapsto \frac{a}{1}$ is a ring homomorphism which is injective if and only if M contains no zero divisors of A.

(b) If $I \subset A$ is an ideal, let $I_M \subset A_M$ denote the ideal generated by $\iota(I)$. Prove that $I_M = \{\frac{a}{m} \mid a \in I, m \in M\}/\sim$ and prove the following fundamental correspondences for ideals:

(i) $(\iota^{-1}(J))_M = J$ for all ideals $J \subset A_M$ and

(ii) $\iota^{-1}(\mathcal{P}_M) = \mathcal{P}$ for all prime ideals $\mathcal{P} \subset A$ disjoint from M.

Conclude that any localization of a Noetherian ring is again Noetherian.

Prove moreover that $\mathcal{P}_M$ is always prime if $\mathcal{P}$ is a prime ideal disjoint from M, and conclude from (i) and (ii) that $\mathcal{P} \mapsto \mathcal{P}_M$ gives a bijection between prime ideals in A disjoint from M and prime ideals in A_M.

(c) Prove that if $A \subset B$ are commutative rings with 1 and $M \subset A$ is multiplicative (hence also multiplicative in B), then $A_M \subset B_M$ and if B is integrally dependent upon A, then B_M is integrally dependent upon A_M. Find a counterexample for the converse of the last statement.

Some Standard Notation:

If $M = \{1, f, f^2, ...\}$, then A_M is usually written as A_f.

If $M = A - \mathcal{P}$, then A_M is usually written as $A_{\mathcal{P}}$

(d) Suppose A is an integral domain, so $K = A_{A-\{0\}}$ is the field of fractions of A and each A_f and $A_{\mathcal{P}}$ can be thought of as a subset of K. Prove that $A = \cap A_m$, where the intersection is taken over all maximal ideals m. Prove that each $A_f = \cap_{f \notin \mathcal{P}} A_{\mathcal{P}}$ where the intersection is taken over all prime ideals $\mathcal{P}$ which do not contain $f \neq 0$, and that if A happens to be finitely generated as an algebra over some field k, then $A_f = \cap_{f \notin m} A_m$.

Definition: If $A \subset K$ is an integral domain contained in a field, then $\overline{A} \subset K$, the **integral closure of** A **in** K, is the set of elements $\alpha \in K$ which satisfy a monic polynomial with coefficients in A. An integral domain A is said to be **integrally closed** if $\overline{A} = A$ in the field of fractions of A.

3. (a) Prove that $\overline{A}$ is always an integral domain.

(b) Prove that the polynomial rings $k[x_1, ..., x_n]$ are integrally closed.

(c) Find the integral closure of $k[V]$ in $k(V)$ when V is the nodal cubic or the cuspidal cubic.

(d) Prove that A is integrally closed iff A_m is integrally closed for all maximal ideals $m \subset A$.

Definition: A **discrete valuation ring** (or just DVR for short) is a local Noetherian integral domain whose maximal ideal is nonzero and principal.

Examples: (a) The localizations $\mathbf{Z}_{\langle p \rangle}$ for primes p.

(b) The localizations $k[x]_{\langle f(x) \rangle}$ for irreducible nonzero $f(x)$.

(c) The localization $k[x, y]_{\langle x,y \rangle}$ is a local Noetherian domain, but not a DVR. The maximal ideal requires two generators.

4. (a) Let $\langle t \rangle \subset A$ be the maximal ideal in a DVR. Prove that every nonzero element $a \in A$ has a unique expression as $a = t^d u$ where $d \geq 0$ and u is a unit in A. Conclude that a DVR is a PID. Prove that every nonzero $\alpha \in K$ (the field of frations of A) has a unique expression as $\alpha = t^d u$ where $d \in \mathbf{Z}$ and u is a unit in A.

(b) If A is a DVR and k is a field included in A, prove that A cannot be finitely generated as a k-algebra(!)

(c) Prove that a DVR is integrally closed.

(d) Suppose $V = V(y^2 - (x+a)(x+b)(x+c)) \subset \mathbf{A}_k^2$ is a plane cubic, where a, b, c are distinct and k is algebraically closed. Prove that each $k[V]_m$ is a DVR, and conclude that $k[V]$ is integrally closed.

Definition: A **Dedekind domain** is an integral domain A which has the property that each localization A_m at a maximal ideal is a DVR. Although each A_m is a PID (by # 4(a)) it is by no means necessary that A itself is a PID. For example, $k[V]$ above happens not to be a PID.