Math 6130 Notes. Fall 2002.

1. Two Hilbert Theorems. To get started, we need two theorems of Hilbert on the properties of ideals in the polynomial rings:

$$\mathbf{C}[x_1, ..., x_n]$$

The ideal $I \subseteq \mathbf{C}[x_1, ..., x_n]$ generated by $f_1, ..., f_m$ will be written:

$$\langle f_1, ..., f_m \rangle := \{\sum_{i=1}^{m} g_i f_i \mid g_1, ..., g_m \in \mathbf{C}[x_1, ..., x_n]\}$$

Thinking of ideals as kernels of ring homomorphisms yields bijections:

$\{\text{ideals } I \subseteq \mathbf{C}[x_1, ..., x_n]\} \leftrightarrow \{\text{quotient rings } A = \mathbf{C}[x_1, ..., x_n]/I\}$

$\{\text{prime ideals } P \subset \mathbf{C}[x_1, ..., x_n]\} \leftrightarrow \{\text{quotient domains } D = \mathbf{C}[x_1, ..., x_n]/P\}$

$\{\text{maximal ideals } m \subset \mathbf{C}[x_1, ..., x_n]\} \leftrightarrow \{\text{quotient fields } K = \mathbf{C}[x_1, ..., x_n]/m\}$

It may be hard to find a finite set of generators of a given ideal, but:

Hilbert's Basis Theorem: Every ideal $I \subseteq \mathbf{C}[x_1, ..., x_n]$ can be generated by a finite set of polynomials $f_1, ..., f_m$.

In the case of *maximal* ideals, we can be much more specific:

Hilbert's Nullstellensatz: Every maximal ideal $m \subset \mathbf{C}[x_1, ..., x_n]$ can be generated by polynomials $x_1 - a_1, ..., x_n - a_n$ for constants $a_1, .., a_n \in \mathbf{C}$.

Proof of the Basis Theorem: We prove a more general result.

Definition: A commutative ring A with 1 is *Noetherian* if every ideal $I \subseteq A$ can be generated by finitely many elements of A.

Proposition 1.1: If A is Noetherian, then:

(i) Every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq A$ is eventually stationary (i.e. there is an n such that $I_n = I_{n+1} = ...$) and

(ii) the polynomial ring $A[y]$ is Noetherian.

(The basis theorem follows by induction since $\mathbf{C}$ is obviously Noetherian)

Proof: For (i), notice that $I := \bigcup_{n=1}^{\infty} I_n$ is an ideal, hence by assumption it is finitely generated. If $f_1, ..., f_m$ are generators, then they are all contained in some I_n, and then $I_n = I_{n+1} = ... = I$.

For (ii), let $J \subseteq A[y]$ be any ideal and consider the ideals $I_d \subseteq A$ of leading coefficients of polynomials $f(y) \in J$ of degree d. That is, $a \in I_d$ if and only if there is a polynomial $f(y) = ay^d + a_{d-1}y^{d-1} + ... + a_0 \in J$. The ideals I_d form an ascending chain: $I_0 \subseteq I_1 \subseteq I_2 \subseteq ... \subseteq A$ which must be eventually stationary, say $I_n = I_{n+1} = ...$ by (i). Let $I_d = \langle a_{d,1}, ..., a_{d,m_d} \rangle$ for each $d \leq n$ and for each pair (d,i) choose some $f_{d,i}(y) = a_{d,i}y^d + a_{d-1}y^{d-1} + ... + a_0 \in J$. Then the $f_{d,i}(y)$ together generate J.

Example: If $V \subset \mathbf{C}^2$ is any subset, then we find generators of the ideal:

$$I(V) := \{f(x,y) \in \mathbf{C}[x,y] \mid f(p,q) = 0 \text{ for all } (p,q) \in V\}$$

(in principle) by this method, regarding $\mathbf{C}[x,y] = \mathbf{C}[x][y]$. For example, if

$$V = \{(0,0),(0,1),(1,0)\} \quad \text{then:}$$

$I_0 = \langle x^2 - x \rangle$ (since $a(x) \in I_0 \Leftrightarrow a(0) = a(1) = 0$)

$I_1 = \langle x \rangle$ (since $a_0(x) + a(x)y \in I_1 \Leftrightarrow a(0) = a_0(0) = 0$ and $a_0(1) = 0$) and we can choose $xy \in I(V)$

$I_2 = \langle 1 \rangle$ and we can choose $y^2 - y \in I(V)$

and we stop here because at this point I_2 is a large as it can get. So:

$$I(V) = \langle x^2 - x, xy, y^2 - y \rangle$$

Corollary 1.2: If M is a finitely generated module over a Noetherian ring (e.g. $\mathbf{C}[x_1, ..., x_n]$), then every submodule $S \subseteq M$ is also finitely generated.

Proof: The generators allow us to express M as a quotient $q : A^m \to M$, and then S is the image of $q^{-1}(S)$, which is a submodule of A^m. So it suffices to prove that submodules of A^m (for any m) are finitely generated. When $m = 1$, this is the definition of Noetherian, since submodules are ideals. In general, we proceed by induction on m. If $S \subset A^m$ and:

$$0 \to A^{m-1} \xrightarrow{i} A^m \xrightarrow{p} A \to 0$$

is the projection onto the last factor, then $i^{-1}(S)$ is finitely generated, by the inductive assumption, and $p(S)$ is finitely generated, as it is an ideal. The generators of the former together with arbitrary lifts of the generators of the latter will then generate S.

Proof of the Nullstellensatz: We start with a field theory reminder.

Field Theory I: The *transcendence degree* of an extension $K \subset L$ of fields (denoted $\mathrm{trd}_K(L)$) is the cardinality of (every) subset $\{\alpha_1, ..., \alpha_d\} \subset L$ that is maximal with the property that the α_i have no non-trivial polynomial relations with coefficients in K. Do not confuse this with the *degree* $[L : K]$ of a finite field extension, which is the dimension of L as a K-vector space.

The transcendence degree has the following properties:

- $\mathrm{trd}_K(K(x_1, ..., x_d)) = d$.
- $\mathrm{trd}_K(L) = d - 1$ if L is the field of fractions of $K[x_1, ..., x_d]/f$ and f is any non-constant polynomial in the $x_1, ..., x_d$.
- $\mathrm{trd}_K(L) = 0$ for all finite field extensions $K \subset L$.
- $\mathrm{trd}_K(L) + \mathrm{trd}_L(M) = \mathrm{trd}_K(M)$ if $K \subset L \subset M$.

Reminder: $\mathbf{C}$ is algebraically closed, so every non-trivial field extension $\mathbf{C} \subset K$ has positive transcendence degree.

Next, we prove a very useful lemma:

Noether Normalization Lemma: If $D \cong \mathbf{C}[x_1, ..., x_n]/P$ is a domain whose field of fractions K has transcendence degree d over $\mathbf{C}$, then there are linear combinations:

$$y_i = \sum_{j=1}^{n} a_{ij} x_j; \quad i = 1, ..., d$$

so that $\mathbf{C}[y_1, ..., y_d] \hookrightarrow D$ and D is finitely generated as a $\mathbf{C}[y_1, ..., y_d]$-module.

Proof: If $n = d$, then $P = 0$ is forced by the transcendence degree, and there is nothing to prove. Otherwise, the images $\overline{x}_1, ..., \overline{x}_n$ of $x_1, ..., x_n$ in D satisfy a polynomial relation $f(\overline{x}_1, ..., \overline{x}_n) = 0$. If, as a polynomial in $\overline{x}_n$, $f = a\overline{x}_n^d +$ {lower order in $\overline{x}_n$} for some non-zero constant $a \in \mathbf{C}$, then D is generated by $1, \overline{x}_n, ..., \overline{x}_n^{d-1}$ as a $\mathbf{C}[x_1, ..., x_{n-1}]/P \cap \mathbf{C}[x_1, ..., x_{n-1}]$-module, and we can proceed by induction. In general, f may not have this form, but if we let $y_i = x_i + a_i x_n$ for $i = 1, ..., n-1$, then *as a function of* $\overline{y}_1, \overline{y}_2, ..., \overline{y}_{n-1}, \overline{x}_n$, f always has the form $f = g(a_1, ..., a_{n-1})\overline{x}_n^d +$ {lower order in $\overline{x}_n$} where g is a non-zero polynomial in the a_i. We can choose constants $a_1, ..., a_{n-1}$ so that $g(a_1, ..., a_{n-1}) \neq 0$ and then in terms of the new coordinates $y_1, ..., y_{n-1}, x_n$, f **does** have the desired form. Now proceed by induction.

Back to the Nullstellensatz: Let $m \subset \mathbf{C}[x_1, ..., x_n]$ be a maximal ideal and consider the field extension: $\mathbf{C} \hookrightarrow K = \mathbf{C}[x_1, ..., x_n]/m$.

Since $\mathbf{C}$ is algebraically closed, this is either trivial or else of positive transcendence degree. In the first case, let a_i be the image of x_i in $K = \mathbf{C}$. Then $x_i - a_i \in m$ for all i, hence $m = \langle x_1 - a_1, ..., x_n - a_n \rangle$ as desired.

On the other hand, if $d > 0$ is the transcendence degree of K over $\mathbf{C}$, then applying Noether Normalization to the domain $D = K$ would give us:

$$\mathbf{C} \subset \mathbf{C}[y_1, ..., y_d] \hookrightarrow K$$

with K finitely generated as a $\mathbf{C}[y_1, ..., y_d]$-module. But this is nonsensical. For example, take any $f \in \mathbf{C}[y_1, ..., y_d]$ and consider the ascending chain:

$$\mathbf{C}[y_1, ..., y_d] \subset f^{-1}\mathbf{C}[y_1, ..., y_d] \subset f^{-2}\mathbf{C}[y_1, ..., y_d] \subset ... \subset K$$

of submodules of K. This chain is eventually stationary (Exercise 3(b)). But:

$$f^{-n}\mathbf{C}[y_1, ..., y_d] = f^{-n-1}\mathbf{C}[y_1, ..., y_d]$$

implies $f^{-n-1} = f^{-n}g$ can be solved with $g \in \mathbf{C}[y_1, ..., y_d]$, and then $g = f^{-1}$ which is ridiculous. Nonconstant polynomials don't have inverse polynomials!

Corollary 1.3: Given polynomials $f_1, ..., f_m \in \mathbf{C}[x_1, ..., x_n]$, then either there is a point $(a_1, ..., a_n) \in \mathbf{C}^n$ so that $f_i(a_1, ..., a_n) = 0$ for all i or else:

$$1 = \sum_{i=1}^{m} g_i f_i \text{ can be solved with } g_1, ..., g_m \in \mathbf{C}[x_1, ..., x_n]$$

Proof: If there is no such point, then $f_1, ..., f_m$ do not all belong to any maximal ideal, by the Nullstellensatz, so they must generate $\mathbf{C}[x_1, ..., x_n]$!

Example: The polynomials $x^3 - y^4, x^4 + y^5, x^5 + y^2 - 1 \in \mathbf{C}[x, y]$ have no common zeroes in $\mathbf{C}^2$, so we know there are polynomials $g_1, g_2, g_3 \in \mathbf{C}[x, y]$ such that:

$$1 = g_1(x_3 - y^4) + g_2(x^6 + y^5) + g_3(x^3 + y^2 - 1)$$

but the Nullstellensatz and its Corollary give us no clue about how to find the polynomials g_1, g_2, g_3 or even any sort of upper bound on their degrees.

Corollary 1.4: For ideals $I \subseteq \mathbf{C}[x_1, ..., x_n]$ and subsets $V \subseteq \mathbf{C}^n$, define:

$$V(I) = \{(a_1, ..., a_n) \in \mathbf{C}^n \mid f(a_1, ..., a_n) = 0 \ \forall f \in I\} \text{ and}$$

$$I(V) = \{f \in \mathbf{C}[x_1, ..., x_n] \mid f(a_1, ..., a_n) = 0 \ \forall (a_1, ..., a_n) \in V\}.$$

Then $I(V(I)) = \sqrt{I} := \{f \in \mathbf{C}[x_1, ..., x_n] \mid f^N \in I \text{ for some } N > 0\}$.

(In particular, $I(V(P)) = P$ whenever $P \subset \mathbf{C}[x_1, ..., x_n]$ is a prime ideal.)

Proof: It is clear that $\sqrt{I} \subseteq I(V(I))$. On the other hand, if we choose generators $I = \langle f_1, ..., f_m \rangle$ then for any $f \in I(V(I))$, consider:

$$J = \langle f_1, ..., f_m, 1 - x_{n+1}f \rangle \subset \mathbf{C}[x_1, ..., x_{n+1}]$$

We get $\emptyset = V(J) \subset \mathbf{C}^{n+1}$ by assumption, so by Corollary 1.3, we can solve:

$$1 = \sum_{i=1}^{m} f_i g_i + (1 - x_{n+1}f)g$$

where the g's are polynomials in $x_1, ..., x_{n+1}$. Now subsitute f^{-1} for x_{n+1}:

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

and clear denominators by multiplying by a sufficiently large power of f. This gives $f^N \in \langle f_1, ..., f_m \rangle$, as desired.

Examples: (a) Consider the ideals $\langle xy - a \rangle \subset \mathbf{C}[x, y]$ for $a \in \mathbf{C}$.

$\mathbf{C}[x, y]/\langle xy - a \rangle \to \mathbf{C}[t, t^{-1}]; x \mapsto t, y \mapsto at^{-1}$ is an isomorphism when $a \neq 0$

so in particular, each $\langle xy - a \rangle$ is a prime ideal, but

$\mathbf{C}[x, y]/\langle xy \rangle \hookrightarrow \mathbf{C}[s] \times \mathbf{C}[t]; x \mapsto (s, 0), y \mapsto (0, t)$ and $\langle xy \rangle$ is not prime

You should think of this as the family of hyperbolas $V(xy - a)$ for $a \neq 0$ (which we visualize in $\mathbf{R}^2$ since $\mathbf{C}^2$ is inaccessible to our 3-dimensional minds) degenerating to the union of the x and y axes when $a = 0$. From the point of view of isomorphism types of the quotient rings, this is a constant family (of domains isomorphic to $\mathbf{C}[t, t^{-1}]$) degenerating to a non-domain.

(b) The ideals $I = \langle y^2 - (x^3 - a)\rangle$ for $a \in \mathbf{C}$ have a different flavor. The quotients are domains when $a \neq 0$ as can be seen by Eisenstein's criterion but they are not all isomorphic to each other (though this is far from obvious!) The sets $V(y^2 - (x^3 - a)) \subset \mathbf{C}^2$ are called *plane cubics in Weierstrass form*.

The $a = 0$ case is also different and interesting:

$$\mathbf{C}[x, y]/\langle y^2 - x^3\rangle \hookrightarrow \mathbf{C}[t];\ x \mapsto t^2,\ y \mapsto t^3$$

so $\langle y^2 - x^3\rangle$ is still a prime. Note that $V(y^2 - x^3) = \{(a^3, a^2) \mid a \in \mathbf{C}\} \subset \mathbf{C}^2$ and when you graph this (in $\mathbf{R}^2$ of course), the origin is a "singular" point. This is called the *cuspidal plane cubic*.

And while we are on the subject of cubic polynomials in x, y, consider:

$$\mathbf{C}[x, y]/\langle y^2 - x^2(x + 1)\rangle \hookrightarrow \mathbf{C}[t];\ x \mapsto (t^2 - 1), y \mapsto t(t^2 - 1)$$

which is therefore also a domain, but here $V(y^2 - x^2(x + 1))$ has a different sort of singularity, with two "branches" coming together at the origin. This one is called the *nodal plane cubic*.

(c) Consider the ideals $\langle y^2 - x, x - a\rangle$ for $a \in \mathbf{C}$. Then:

$$\mathbf{C}[x, y]/\langle y^2 - x, x - a\rangle \cong \mathbf{C}[y]/\langle y^2 - a\rangle$$

is never a domain, but $\sqrt{\langle y^2 - x, x - a\rangle} = \langle y^2 - x, x - a\rangle$ when $a \neq 0$ whereas $\sqrt{\langle y^2 - x, x\rangle} = \langle y, x\rangle \neq \langle y^2 - x, x\rangle$. The algebraic sets $V(\langle y^2 - x, x - a\rangle)$ are the intersections of a parabola (lying on its side) with vertical lines. When the line meets the parabola "transversely" in two points $(a, \pm\sqrt{a})$, then the ideal is equal to its "radical" (i.e. $\sqrt{I} = I$), but when the line is the y-axis, tangent to the parabola, then the ideal is not equal to its radical.

Exercises 1.

1. (a) Prove that $\mathbf{C}[x_1, ..., x_n]$ is a UFD. (Hint: Gauss' Lemma)

(b) Prove that $\mathbf{C}[x]$ is a principal ideal domain.

(c) For each $n > 1$, find an ideal $I \subset \mathbf{C}[x, y]$ that needs n generators.

2. Prove that the power series rings $\mathbf{C}[[x_1, ..., x_n]]$ are Noetherian.

3. (a) If all ascending chains of ideals in a commutative ring A with 1 are eventually stationary, conclude that A is Noetherian.

(b) Prove that an ascending chain of submodules of a finitely generated module over a Noetherian ring must be eventually stationary.

4. (a) Prove that $\mathbf{C}[x, y]/\langle xy - 1\rangle$ is not finitely generated as a $\mathbf{C}[x]$-module, but it is finitely generated as a $\mathbf{C}[x + ay]$-module for any non-zero a.

(b) Prove that if k is any infinite field and $g \in k[x_1, ..., x_n]$ is any non-zero polynomial, then there are constants $a_1, ..., a_n \in k$ so that $g(a_1, ..., a_n) \neq 0$. Conclude that Noether Normalization as stated holds over any infinite field.

(c) Find a counterexample to (b) when k is a finite field.

(d) If k is an infinite field, prove that the quotient of $k[x_1, ..., x_n]$ by a maximal ideal is a finite extension of k. (This is also true when k is finite, but Noether Normalization needs to be modified...see Mumford's Red Book).

5. If $f_1, f_2 \in \mathbf{C}[x]$ do not simultaneously vanish at any point $a \in \mathbf{C}$, give an algorithm for producing g_1, g_2 so that:

$$1 = f_1g_1 + f_2g_2 \in \mathbf{C}[x]$$

6. If $A = \mathbf{C}[x_1, ..., x_n]/I$, show that $I(V(I)) = I$ if and only if A has no *nilpotents* (elements $a \in A - 0$ such that $a^m = 0$ for some m).

7. Describe $V(I) \subset \mathbf{C}^3$ (or rather visualize it in $\mathbf{R}^3$) and find the ideal $\sqrt{I} = I(V(I)) \subset \mathbf{C}[x, y, z]$ for each of the following ideals I. In particular, determine whether or not $I = \sqrt{I}$ and whether or not I is prime.

(a) $I = \langle x^3y^2z\rangle$, (b) $I = \langle xz - y^2, xyz\rangle$, (c) $I = \langle x - yz, y - y^2\rangle$

(d) $I = \langle xy, xz, yz\rangle$, (e) $I = \langle x^2, y^2, z^2\rangle$,

(f) $I = \langle x^3 - y^2, y^5 - z^3\rangle$, (g) $I = \langle x^l, y^m, z^n, x + y + z - 1\rangle$,

(h) $I = \langle xy - z^2\rangle$, (i) $I = \langle xy, xz\rangle$