

Math 552: Homework 1

Sep 2nd, 2020

Professor Kevin Tucker

Anish Chedalavada

This homework was done in collaboration with Neelima Borade.

Exercise 1. Prove the Hilbert Basis Theorem, i.e. if a commutative ring R is Noetherian then the polynomial ring $R[x]$ is Noetherian.

Proof. Suppose $I \subset R[x]$ is an ideal. Define $I' \subset R$ to be the ideal

$$I' := \{a \in R \mid a \text{ is a leading coefficient of some } f \in I\}$$

This is an ideal as if $a, b \in I'$ are associated to some polynomials f, g , say of degree n, m respectively (assume $n \leq m$ w.l.o.g.) we have that $a + b$ is the leading coefficient of $f + gx^{n-m}$, and for any $r \in R$, ra is the leading coefficient of rf . Thus, I' is closed under R -multiplication and addition, and is an ideal as asserted. By Noetherianity, $I' = (a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in I'$, associated to some polynomials $p_1, \dots, p_n \in I$ with p_i of smallest degree witnessing a_i as a leading coefficient, say of degrees $d_1 < \dots < d_n$ (which we can assume again w.l.o.g.). For all $k \leq d$, define I'_k analogous to I' to be the ideal

$$I'_m := \{a \in R \mid a \text{ is a leading coefficient of some } f \in I \text{ of degree } \leq m\}$$

By the same logic as above, this is an ideal, and is finitely generated by Noetherianity, Let $f_1^{(k)}, \dots, f_{n_k}^{(k)}$ be of minimal degree witnessing the generators of I'_k as leading coefficients. Let J be the ideal given by:

$$J := (p_1, \dots, p_n) + \sum_{i=0}^{d_n} (f_1^i, \dots, f_{n_i}^i)$$

J is clearly finitely generated, and we assert that $I = J$. One inclusion is already clear, and proceed to show the other by strong induction. Suppose $g \in I$ is of degree m , and $\forall q \in I$ of degree less than m w.h.t. $q \in J$. Then we have two cases:

Case 1: $m < d_n$ In this case, we have that the leading coefficient of g , say $b \in I'_m$. Let $a_1^{(m)}, \dots, a_{n_m}^{(m)}$ be the generators of this ideal, we have that $b = \sum_{i=1}^{n_m} b_i a_i^{(m)}$. Thus, consider the following expression:

$$h = g - \sum_{i=1}^{n_m} b_i x^{(m - \deg f_i^{(m)})} f_i^{(m)}$$

We have that the right hand side is polynomials of degree m , and the coefficient of $x^m = b - b = \sum_{i=1}^{n_m} b_i a_i^{(m)} = 0$, and so h has degree less than m and thus belongs to J by the inductive hypothesis. Thus, $g \in J$.

Case 2: $m > d_n$ This case is exactly the same as the previous case, except for b the leading coefficient of g , $b \in I'$ and so we get an expression of the form

$$h = g - \sum_{i=1}^n b_i x^{(m - \deg p_i)} p_i$$

Yielding that $g \in J$.

We thus have the claim, by strong induction; i.e. $I = J$ and so I is finitely generated for I an arbitrary ideal in $R[x]$. Thus, $R[x]$ is Noetherian. \square

Exercise 2. For k an algebraically closed field, show that the prime ideals of $k[x, y]$ are precisely:

- 0
- $(f(x, y))$ for f an irreducible polynomial
- $(x - a, y - b)$ for $a, b \in k$

Explain how this completely characterizes the Zariski topology on \mathbb{A}_k^2 .

Proof. It is clear that the ideals mentioned above are prime ideals, either by maximality or by properties of UFDs. Now suppose \mathfrak{p} is a proper prime ideal that is not of the form above. By assumption, it must contain at least two distinct irreducible polynomials, as if it only contains one irreducible polynomial then that polynomial must divide every element of \mathfrak{p} by properties of UFDs. If it contains an expression only comprising of x 's, then it must contain a root of this polynomial of the form $(x - a)$ by algebraic closure, then by the correspondence principle it must be the pullback of a prime ideal in $k[y]$ by the map $k[x, y] \mapsto k[x, y]/(x - a) = k[y]$, in which all prime ideals are of the form $(y - b)$ by algebraic closure, implying that $\mathfrak{p} = (x - a, y - b)$. Symmetric logic applies for if it contains an expression comprising of only y 's. Suppose it contains irreducibles not of this form, i.e. distinct polynomials of positive x -degree and y -degree $f, g \in k[x][y]$. If these polynomials do not contain a common factor in $k[x][y]$, then they do not possess a common factor in $k(x)[y]$ by Gauss's Lemma as they are irreducible and assumed distinct (as $k[x]$ is a UFD). However, $k(x)[y]$ is a PID, and so $\exists p(x), q(x) \in k(x)$ such that $fp + gq = 1$. By clearing denominators in $k(x)$ we get polynomials $p', q' \in k[x]$ such that $fp' + gq' = 1$, a contradiction, as \mathfrak{p} was assumed to be a proper ideal. Thus, there cannot exist two distinct irreducibles in \mathfrak{p} of both positive x and y degree, implying that all prime ideals must be of the form above. \square

Exercise 3. Show that \mathbb{A}_k^2 endowed with the Zariski topology does not have the product topology of the Zariski topologies on $\mathbb{A}_k^1 \times \mathbb{A}_k^1$.

Proof. It suffices to find a closed set in \mathbb{A}_k^2 that cannot come from the product topology on \mathbb{A}_k^1 . Note that for any field k , the Zariski topology on \mathbb{A}_k^1 is not Hausdorff, as the space is irreducible \implies it is not the union of two closed sets $\implies \nexists U_1, U_2$ open $\subset \mathbb{A}_k^1$ s.t. $U_1 \cap U_2 = \emptyset$. Thus, the diagonal set $(x, x) \in \mathbb{A}_k^1 \times \mathbb{A}_k^1$ is not closed, as this is equivalent to \mathbb{A}_k^1 being Hausdorff. However, we have that the diagonal in \mathbb{A}_k^2 is the vanishing of the polynomial $(x - y) \in k[x, y]$, and must be closed. Thus, \mathbb{A}_k^2 does not have the product topology. \square

Exercise 4. Show that the open sets $D(f) = \mathbb{A}_k^n \setminus V(f)$ for $f \in k[x_1, \dots, x_n]$ form a basis for the Zariski topology on affine space, and that this topology is quasicompact.

Proof. First, it is clear that the sets $D(f)$ are open sets, as they are the complements of closed sets. To show they form a basis, it suffices to show that they contain the complement of any basic open set $V(I)$ for $I \subset k[x_1, \dots, x_n]$ an ideal, as all open sets are unions or finite intersections of these open sets (the corresponding dual statement being true for closed sets and $V(I)$ s). Note then that $V(I) = \bigcup_{f \in I} V(f)$ by definition, and thus we have that $\mathbb{A}_k^n \setminus V(I) = \bigcup_{f \in I} \mathbb{A}_k^n \setminus V(f) = \bigcup_{f \in I} D(f)$, yielding the claim. To show quasicompactness, we used the closed set formalization of compactness, i.e. that if an infinite family of closed sets has an empty intersection then we may select a finite subfamily with empty intersection. Suppose that $\{V(I_\alpha)\}_{\alpha \in A}$ is an arbitrary family of closed sets with empty intersection. In particular, we have that

$$\emptyset = \bigcap_{\alpha \in A} V(I_\alpha) = V\left(\sum_{\alpha \in A} I_\alpha\right)$$

Now by Noetherianity of $k[x_1, \dots, x_n]$, we have that each of these ideals is finitely generated, so A must be a countable family (as there is an injection into the infinite disjoint union of finite subsets of $k[x_1, \dots, x_n]$ by taking generators, and this latter set is a subset of countable union of finite products of countable sets, i.e. countable). Thus, pick an enumeration of A , and consider the following ascending chain of ideals:

$$I_1 \subseteq I_1 + I_2 \subseteq \dots \subseteq \sum_{i=1}^n I_i \subseteq \dots$$

By Noetherianity, this ascending chain must terminate at a finite stage, and so we have that the ideal $\sum_{\alpha \in A} I_\alpha = \sum_{i=1}^k I_i$ for some k finite. This in particular implies that

$$\emptyset = V\left(\sum_{\alpha \in A} I_\alpha\right) = V\left(\sum_{i=1}^k I_i\right) = \bigcap_{i=1}^k V(I_i)$$

Yielding the claim. \square

Exercise 5. Identify $\mathbb{A}_k^{m^2}$ with the set of all $m \times m$ matrices. Show that:

a) For all r , the set of matrices with rank $\leq r$ is an algebraic subset of $\mathbb{A}_k^{m^2}$.

b) $SU(2)$ cannot be embedded as an affine algebraic set of $\mathbb{A}_{\mathbb{C}}^4$, but can be embedded as one in $\mathbb{A}_{\mathbb{R}}^8$.

Proof. a) We have that if a matrix A has rank $\leq r$, the determinant of all minors of size $r+1$ must be trivial. Furthermore, if a matrix A has rank $> r$, then we may apply elementary row and column operations to yield an upper triangular matrix with leading 1s in $> r$ many rows, thus yielding an upper triangular matrix with a nonvanishing minor. Thus, we may embed all matrices of rank $\leq r$ in k^{m^2} as the vanishing of all minors, represented as an ideal of polynomials in $k[x_1, \dots, x_{m^2}]$.

b) Assume towards a contradiction that $SU(2)$ can be embedded as such an algebraic subset of $\mathbb{A}_{\mathbb{C}}^4$. In particular, there exists an ideal $I \subset \mathbb{C}[a, b, c, d]$ such that $V(I) = SU(2)$, i.e. it contains all relations between a, b, c, d such that the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is special unitary. Note then that we can study this algebraic set by looking at its intersection with other algebraic subsets of $\mathbb{A}_{\mathbb{C}}^4$. Consider the ideal $J = I + (b, c)$, which characterizes special unitary matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $b = c = 0$. In particular, this contains matrices such that $a = 1/d$ and $|a| = |d| = 1$. In $\mathbb{A}_{\mathbb{C}}^2$, we may consider the vanishing ideal $V(A)$ for $A = J/(b, c) \subset \mathbb{C}[a, b, c, d]/(b, c) = \mathbb{C}[a, d]$. Note that by the previous logic, $ad - 1 \in J/(b, c)$. Thus, we get an ideal $B = J/(b, c, ad - 1) \subset \mathbb{C}[a, d]/(ad - 1) = \mathbb{C}[a, a^{-1}]$, and by assumption B is not empty as it must vanish at all a such that $|a| = 1$, and is not the whole ring. Thus, consider the ideal $\mathbb{C}[a] \cap B \subset \mathbb{C}[a]$, the pullback of B along the inclusion $\mathbb{C}[a] \hookrightarrow \mathbb{C}[a, a^{-1}]$. By clearing denominators, this ideal contains all Laurent polynomials which vanished at $|a| = 1$, and so in the affine line $\mathbb{A}_{\mathbb{C}}^1$, we have that $V(B \cap \mathbb{C}[a]) = \{a \mid |a| = 1\}$. However, $\mathbb{C}[a]$ is a PID, and so every ideal is generated by a single polynomial which vanishes at finitely many points, implying that the affine line has the cofinite topology. The set above is infinite and thus cannot be a closed algebraic set, yielding a contradiction. Thus, $SU(2)$ cannot be embedded as an algebraic subset of $\mathbb{A}_{\mathbb{C}}^4$. We may think of it as an algebraic subset of $\mathbb{A}_{\mathbb{R}}^8$. For $x = a, b, c, d$ the complex matrix entries, let x_1 denote $\operatorname{Re}(x)$ and x_2 denote $\operatorname{Im}(x)$. In $\mathbb{R}[a_1, a_2, \dots, d_1, d_2]$, we may encode the determinant 1 condition as:

$$\{a_1 d_1 - a_2 d_2 - b_1 c_1 + b_2 c_2 = 1, a_1 d_2 + a_2 d_1 - b_1 c_2 - b_2 c_1 = 0\}$$

Which encodes that $\operatorname{Re}(ad - bc) = 1$ and $\operatorname{Im}(ad - bc) = 0$. We may encode the Hermitian condition as:

$$\begin{aligned} &\{a_1^2 + a_2^2 + b_1^2 + b_2^2 = 1, \\ &a_1 c_1 + a_2 c_2 + b_1 d_1 + b_2 d_2 = -a_1 c_2 + a_2 c_1 - b_1 d_2 + b_2 d_1 = 0, \\ &c_1^2 + c_2^2 + d_1^2 + d_2^2 = 1, \\ &a_1 c_1 + a_2 c_2 + b_1 d_1 + b_2 d_2 = a_1 c_2 - a_2 c_1 + b_1 d_2 - b_2 d_1 = 0\} \end{aligned}$$

Which encodes multiplication with the adjoint matrix yielding the identity. \square

Exercise 6. Find $I(X)$ where $X = V(x^2, xy^2) \subset k^2$ and check that it is the radical of (x, xy^2) . Find the irreducible components of X .

Proof. We have that $V(x^2, xy^2) = V(x^2) \cap V(xy^2)$. This is all points along which $x^2 = 0$, which implies $x = 0$ as it is a field, which is contained in the points for which $V(xy^2) = 0$ as these are points for which either $x = 0$ or $y = 0$. Thus, $V(x^2, xy^2)$ is the y -axis, and so $I(X) = (x)$. This is indeed the radical of (x^2, xy^2) as if $r \in k[x, y]$ s.t. $\exists n \in \mathbb{N}$ ($r^n \in (x^2, xy^2)$) then $x \mid r^n \implies x \mid r \implies r \in (x)$, and all elements in (x) can be raised to the 2nd power to obtain an element divisible by (x^2) . $V(x)$ is the only irreducible component of $V(x^2, xy^2)$, irreducible as (x) is prime. \square

Exercise 7. Let Y be the algebraic set in \mathbb{A}_k^3 defined by the polynomials $(x^2 - yz, xz - x)$. Show that Y is the union of three irreducible sets, describe them, and find their associated prime ideals.

Proof. Note firstly that $x - xz = x(z - 1)$. Thus, any minimal prime ideal \mathfrak{p} containing I must contain either x or $z - 1$. Assume it contains x . Then $x^2 - yz \in I \subset \mathfrak{p}$ containing x so \mathfrak{p} contains either y or z . Thus, \mathfrak{p} contains either (x, y) or (x, z) in this case, both of which are prime and contain I . Thus, $\mathfrak{p} \in \{(x, y), (x, z)\}$ if it contains x . Assume \mathfrak{p} instead contains $(z - 1)$. Then $(x^2 - yz, z - 1) \subset \mathfrak{p}$. We may mod out by $(z - 1)$ and consider the ideal $\mathfrak{p}/(z - 1) \subset k[x, y]$. We have that $x^2 - y \in \mathfrak{p}/(z - 1)$ coming from $x^2 - yz + (z - 1)$. This polynomial is irreducible in $k[x, y]$ and thus $(x^2 - y)$ is a minimal prime, implying that $\mathfrak{p}/(z - 1) = (x^2 - y)$ or that $\mathfrak{p} = (x^2 - y, z - 1)$ in this case. Thus, we have three associated minimal primes to this ideal, given by $(x, y), (x, z), (x^2 - y, z - 1)$. We have that the radical of I is the intersection of these prime ideals, (intersection of minimal primes in $k[x, y, z]/I$ is nilradical) and thus $V(I) = V(\sqrt{I}) = V(x - y^2, z - 1) \cup V(x, y) \cup V(x, z)$, which are irreducible sets as desired by primality. \square

Exercise 8. Let k be an arbitrary field.

- Suppose $X \subseteq \mathbb{A}_k^n$ is an algebraic set. Show that X is irreducible iff $I(X)$ is a prime ideal.
- Give an example of an irreducible polynomial $f \in R[x, y]$ whose zero set is not irreducible.

Proof. a) Suppose $I(X)$ is not prime. Then in particular $\sqrt{I(X)}$ is the intersection of finitely many prime ideals by primary decomposition (Noetherianity), implying that X is the union of the closed sets corresponding to the vanishing of these prime ideals: thus, X is not irreducible. Suppose that $I(X)$ is prime. Then if X were not irreducible, we would have closed sets $V(A), V(B) \neq X$ distinct such that $V(A) \cup V(B) = X \implies I(V(A)) \cap I(V(B)) = I(X)$. By primality, this is only possible if $I(X) = I(V(A))$ or $I(V(B))$, a contradiction as $V(B), V(A) \neq X$. Thus, the claim holds.

- One such example of an irreducible polynomial of this form is $(xy)^2 + 1$, which is irreducible as it does not break up into any factors, but which vanishes nowhere, and thus does not have irreducible vanishing set. \square