Assignment-1

Algebraic Geometry

TRISHAN MONDAL, SOUMYA DASGUPTA, AARATRICK BASU

Problem 1.1. *Let, $J = (XY, XZ, YZ)$ be an ideal of $k[X, Y, Z]$; find $V(J)$; is it irreducible ? Is it true that, $I(V(J)) = J$? Prove that J can't be generated by 2 elements. Now let, $J' = (XY, (X - Y)Z)$; find $V(J')$ and calculate $\mathbf{rad}J'$.*

Solution. Let $p = (x, y, z) \in \mathbb{A}^3$. $p \in V(J)$ if and only if $xy = yz = zx = 0$. Clearly this can happen iff at most one coordinate is non-zero. Hence,

$$V(J) = \{(x, 0, 0) \mid x \in k\} \cup \{(0, y, 0) \mid y \in k\} \cup \{(0, 0, z) \mid z \in k\}.$$

Note that we have

$$\{(x, 0, 0) \mid x \in k\} = V(Y + Z, Y - Z)$$

and similarly for the other subsets appearing in the union on the right. Hence, as $V(J)$ is a union of proper algebraic subsets, we get $V(J)$ is not irreducible.

$*$ Suppose $f(X, Y, Z) = \sum f_{\alpha,\beta,\gamma} X^\alpha Y^\beta Z^\gamma$ is in $I(V(J))$, i.e, it vanishes on $V(J)$. But we have

$$f(x, 0, 0) = \sum f_{\alpha,0,0} X^\alpha$$

and similarly for $f(0, y, 0), f(0, 0, z)$. These one-variable polynomials vanish identically (and the field k is infinite) and hence, their coefficients are all zero. Therefore,

$$f \in I(V(J)) \implies f(X, Y, Z) = \sum_{(\alpha,\beta,\gamma)\in S} f_{\alpha,\beta,\gamma} X^\alpha Y^\beta Z^\gamma$$

where S is the subset of indices such that at most one of the three indices is zero. But then, each monomial appearing in f is in fact an element of $J = (XY, XZ, YZ)$, and hence so is f. As $I(V(J)) \supset J$ for any ideal J, we get

$$I(V(J)) = J$$

in this case.

Suppose $J = (f, g)$ for some $f, g \in k[X, Y, Z]$. We know $J \subset \mathfrak{m}$, where $\mathfrak{m} = (X, Y, Z)$ is a maximal ideal in $k[X, Y, Z]$. Then, $J/\mathfrak{m}J$ is a $k-$vector space and as we have assumed J is generated by two generators, it has dimension at most 2 over k. Therefore, if u, v, w denote the images of XY, XZ, YZ here, we must have $\{u, v, w\}$ is a linearly dependent set. This exactly means $au + bv + cw = 0$ in $J/\mathfrak{m}J$ for some $(a, b, c) \neq (0, 0, 0) \in k^3$, in other words, $aXY + bYZ + cZX \in \mathfrak{m}J$. But no non-zero element of $\mathfrak{m}J = (X^2Y, X^2Z, Y^2X, Y^2Z, Z^2X, Z^2Y)$ has degree less than 3, because all the products of the generators are cubics. Hence, $aXY + bYz + cZX \in \mathfrak{m}J$ implies that all of a, b, c are 0, which is a contradiction and therefore, proves that J cannot be generated by two elements. ■

$**$ Let $p = (x, y, z) \in \mathbb{A}^3$. $p \in V(J')$ if and only if $xy = 0$ and $(x - y)z = 0$. If $z \neq 0$, $x = y = 0$. Otherwise, if $z = 0$, at least one of x, y is zero because $xy = 0$. Hence,

$$V(J') = \{(x, 0, 0) \mid x \in k\} \cup \{(0, y, 0) \mid y \in k\} \cup \{(0, 0, z) \mid z \in k\}.$$

We assume for the last part that k is algebraically closed. Then, by the Nullstellensatz,

$$\operatorname{rad} J' = I(V(J')).$$

But as $V(J) = V(J')$ and we have already shown $I(V(J)) = J$, we get $\operatorname{rad} J' = J$.

Without Assuming k is algebraically closed - In order to do this we will use the following lemma (claim).

> **Claim—** $\mathbf{rad}(a, bc) = \mathbf{rad}(a, b) \cap \mathbf{rad}(a, c)$.

Proof. If, $f \in \mathbf{rad}(a, bc)$ then, $f^n \in (a, bc)$ i.e. $f^n = ax + ybc$ so, $f^n \in (a, b)$ and $f^n \in (a, c)$. So, $\mathbf{rad}(a, bc) \subseteq \mathbf{rad}(a, b) \cap \mathbf{rad}(a, c)$. If, $f \in \mathbf{rad}(a, b) \cap \mathbf{rad}(a, c)$, for some m, n we can say, $f^n \in (a, b)$ and $f^m \in (a, c)$ and hence,

$$\begin{aligned} f^n &= xa + yb \\ f^m &= ta + uc \\ \Rightarrow (f^n - ax)(f^m - at) &= yubc \end{aligned}$$

Thus we can see, $f^{m+n} \in (a, bc)$, and hence $f \in \mathbf{rad}(a, bc)$. Thus we have, $\mathbf{rad}(a, b) \cap \mathbf{rad}(a, c) \subseteq \mathbf{rad}(a, bc)$ and hence our proof is complete. ■

Using the above claim we can say, $\mathbf{rad}(XY, (X - Y)Z) = \mathbf{rad}(XY, X - Y) \cap \mathbf{rad}(XY, Z) = \mathbf{rad}(X, Y) \cap \mathbf{rad}(X, Z) \cap \mathbf{rad}(Y, Z)$. Since these are prime ideal we can say, $\mathbf{rad}J' = (XY) \cap (YZ) \cap (ZX) = (XY, YZ, ZX)$.

REMARK: $*$ This proof works if we assume the field is infinite. In general the book deals with infinite field that's why we have taken that assumptions moreover professor told us to do whatever we like.

$**$ Again we have taken the assumption k is algebraically closed after asking professor.

Problem 1.2. *Let, $J = (x^2 + y^2 - 1, y - 1)$. Find $f \in I(V(J)) \setminus J$.*

Solution. Note that, $V(J) = \{(x, y) \in \mathbb{A}^2 : x^2 + y^2 - 1 = 0, y - 1 = 0\} = \{(0, 1)\}$. $I(V(J))$ will be the maximal ideal $(x, y - 1)$. Now we claim that $x \notin J$. Note that $J = (x^2 + y^2 - 1, y - 1) = (x^2, y - 1)$. If $x \in J$ then for some polynomials $f, g \in k[x, y]$ we must have

$$x = f.(x^2) + g.(y - 1)$$

Just by looking at the degree (and coefficients) of In the above equation put $y = 1$ to get $x = f(x, 1)x^2$. Now just by looking at the degree on both side we can say it's not possible. ■

Problem 1.3. *Prove that the irreducible components of an algebraic set are unique (this was stated without proof in (3.7, b)). That is, given two decompositions $V = \cup_{i \in I} V_i = \cup_{j \in J} W_j$ of V as a union of irreducibles, assumed to be irredundant, prove that V_i are renumbering of the W_j.*

Solution. Note that, $V_i = V \cap V_i$. Now we have,

$$V_i = \left(\bigcup_{i \in J} W_j \right) \cap V_i = \bigcup_{j \in J} (V_i \cap W_j)$$

Since, V_i is irreducible we can say, $V_i = W_j \cap V_i$ for some $j \in J$. So we have $V_i \subseteq W_j$. Now use the fact, $W_j = V \cap W_j$. By similar computation we have, $W_j = V_{i'} \cap W_j$ and $W_j \subseteq V_{i'}$. So, $V_i \subseteq V_{i'}$ but by the decompositions we have $V_i \cap V_k = \emptyset$ for any pair $i, k \in I$. Thus we must have $i' = i$, $W_j \subseteq V_i$ and hence $V_i = W_j$. We will continue doing the same thing on $V \setminus V_i = V \setminus W_j$. Thus we will have, $I = J$ and W_i are renumbering of V_j. ■

Problem 1.4. *If $J = (uw - v^2, w^3 - u^5)$, show that $V(J)$ has two irreducible components, one of which is the curve C of (3.11,b).*

Prove that the same curve C can be defined by two equations, $uw = v^2$ and $u^5 - 2u^2vw + w^3 = 0$. The point here is that the second equation, restricted to the quadric cone ($uw = v^2$), is trying to be a square.

Solution. Let $p = (x, y, z) \in V(J)$, so that $xz = y^2$ and $z^3 = x^5$. Then, $x = 0$ implies both $y, z = 0$. Similarly, if $y = 0$ then both $x, z = 0$ and if $z = 0$, both $x, y = 0$. Hence, $(0, 0, 0)$ is a point of $V(J)$ and all other points have all coordinates non-zero.

Assume $(x, y, z) \in V(J)$ is a point with no coordinates 0. Let $t = \frac{y}{x}$. Then,

$$xz = y^2 \implies xz = x^2t^2 \implies z = xt^2.$$

Further,

$$z^3 = x^5 \implies x^3t^6 = x^5 \implies x^2 = t^6 \implies x = \pm t^3$$

So, we get that the variety $V(J) = X_1 \cup X_2$ where X_1 is the image of the map $t \mapsto (t^3, t^4, t^5)$ and X_2 is the image of the map $t \mapsto (-t^3, -t^4, -t^5)$. These are the irreducible components of $V(J)$ as they are polynomial images of $\mathbb{A}^1$, and X_1 is the curve C.

We need to show that $C = X$, where $X = V(uw - v^2, u^5 - 2u^2vw + w^3)$. Clearly, $C \subset X$ as putting $x = t^3, y = t^4, z = t^5$ gives $xz = y^2$ and

$$x^5 = z^3 \implies x^5 - 2x^2yz + z^3 = 0$$

Now let $(x, y, z) \in X$. Now,

$$x^5 - 2x^2yz + z^3 = 0 \implies x^5 + z^3 = 2xy^3 \implies x^{10} + z^6 + 2x^5z^3 = 4z^2y^6 = 4x^5z^3 \implies (x^5 - z^3)^2 = 0$$

which then gives $x^5 = z^3$ and so, $X \subset C \cup X_2$. As $(-t^3, -t^4, -t^5) \in X \implies t = 0$, we get $X \subset C$ and hence, $X = C$.

Problem 1.5. (i) *Prove that for any field k, an algebraic set in $\mathbb{A}^1_k$ is either finite or the whole of $\mathbb{A}^1_k$. Deduce that the Zariski topology is the cofinite topology.*

(ii) *Let k be any field, and $f, g \in k[X, Y]$ irreducible elements, not multiples of one another. Prove that $V(f, g)$ is finite.*

(iii) *Prove that any algebraic set $V \subset \mathbb{A}^2_k$ is a finite union of points and curves.*

Solution. **(i)** Any algebraic set of V is given by the zero set of an ideal $I \subset k[x]$, i.e. $V = \{P \in \mathbb{A}^1_k : f(P) = 0, f \in I\}$. Since, $k[x]$ is P.I.D, I can be generated by a polynomial g. Clearly, $V = \{P \in \mathbb{A}^1_k : g(P) = 0\}$. This is the finite set unless g is the 0 polynomial. If g is 0 polynomial, $V = \mathbb{A}^1_k$. So, the closed set are either the whole set of a finite set. Thus it has a **cofinite topology**.

(ii) Let, $K = k(x)$ and we can treat f, g as elements of $K[y]$. f and g are irreducible and they are not multiple of each-other. There must exist $p, q \in K[y]$ such that $pf + qg = 1$. There exist, $a, b \in K[X, Y]$ and $h \in K[x]$ so that, $h(x) = af + bg$. Hence, there are finitely many possible values of x. Corresponding to x there are also finitely many values of y. So, $V(f, g)$ is finite.

(iii) Since, $k[x, y]$ is Noetherian V can contain at-most finite number of irreducible components. Let, $X_0 \subset V$ is an irreducible component of V. If X_0 is finite point's then we are fine. If X_0 is not finite points then, we consider $I(X_0)$, which is prime in $k[x, y]$ as X_0 is irreducible. If this case if $f \in I(X_0)$ it must have an irreducible factor $g \in I(X_0)$. Let, $h \in I(x_0) \setminus (g)$. Then, $X \subseteq V(g, h)$ where h and g don't have any common factor. Thus by the previous part we can say, $X_0 \subseteq \{\text{a finite set}\}$. But we are considering the case when, X_0 is not finite. In this case, $I(X_0) = (g)$ and hence, $X_0 = V(g)$, which is curve. Thus irreducible components of V is finite points or curves and since there are finite irreducible component of V we can say, V is union of finite points and curves.

Problem 1.6.

(a) *Let k be an infinite field and $f \in k[X_1, \ldots, X_n]$; suppose that f is nonconstant, that is, $f \notin k$. Prove that $V(f) \neq \mathbb{A}^n_k$.*

(b) *Now suppose that k is algebraically closed, and let f be as in (a). Suppose that f has degree m in X_n, and that its leading term is $a_m(X_1, \dots, X_{n-1})X_n^m$; show that wherever $a_m \neq 0$, there is a finite nonempty set of points of $V(f)$ corresponding to every value of $(X_1, \dots, X_{n-1})$. Deduce in particular that if $n \geq 2$ then $V(f)$ is infinite.*

(c) *Put together the results of (b) and Exercise 3.12(iii) to deduce that if the field k is algebraically closed, then distinct irreducible polynomials $f \in k[X, Y]$ define distinct hypersurfaces of $\mathbb{A}_k^2$.*

(d) *Generalise the result of (c) to $\mathbb{A}_k^n$.*

Solution. **Part (a).** For $n = 1$, the result is obviously true, because if $f \in k[X] \setminus k$, then f can have at most $\deg f$ many roots. Thus $V(f) \subsetneq \mathbb{A}_k^1$. Suppose the result is true for all nonconstant polynomials $f \in k[X_1, \dots, X_{n-1}]$, that is, if $f \in k[X_1, \dots, X_{n-1}] \setminus k$ then $V(f) \neq \mathbb{A}_k^{n-1}$. We need to show that if $f \in k[X_1, \dots, X_n] \setminus k$, then $V(f) \neq \mathbb{A}_k^n$.

If f does not involve X_n, then we can consider the polynomial $g(X_1, \dots, X_{n-1}) = f(X_1, \dots, X_{n-1}, 0)$. Then $V(f) = V(g) \times \mathbb{A}_k^1$, but by induction hypothesis $V(g) \neq \mathbb{A}_k^{n-1}$, and thus $V(f) \neq \mathbb{A}_k^n$. So we can assume that f involves the indeterminate X_n, for the sake of contradiction suppose that $V(f) = \mathbb{A}_k^n$, and write $f(X_1, \dots, X_n) = \sum_{i=1}^m a_i(X_1, \dots, X_{n-1})X_n^i$ with $a_m \neq 0$. Then for any $\mathbf{c} = (c_1, \dots, c_{n-1}) \in \mathbb{A}_k^{n-1}$, we get that $g_{\mathbf{c}}(X_n) = f(c_1, \dots, c_{n-1}, X_n) = \sum_{i=1}^m a_1(c_1, \dots, c_{n-1})X_n^i$ is the zero polynomial, but then we get that $a_m(c_1, \dots, c_{n-1}) = 0$, but $\mathbf{c}$ was chosen arbitrarily, thus we get that $V(a_m) = \mathbb{A}_k^{n-1}$, contradicting our induction hypothesis, since a_m is non-constant polynomial thus we must have $V(a_m) \neq \mathbb{A}_k^{n-1}$. Hence we get that $V(f) \neq \mathbb{A}_k^n$.

Part (b). Let $\mathbf{c} = (c_1, \dots, c_{n-1})$ be such that $a_m(c_1, \dots, c_{n-1}) \neq 0$ (such points exists by part (a)). Then $g(X_n) = f(c_1, \dots, c_{n-1}, X_n) \in k[X_n]$ is a polynomial of degree m. Now since k is algebraically closed, g has exactly m roots in k. Thus we have shown that wherever $a_m \neq 0$, there is a finite non-empty set of points of $V(f)$ corresponding to every value of $(X_1, \dots, X_{n-1})$. This is particular tells us that $V(f)$ is infinite for $n \geq 2$. Let $\mathbf{c} = (c_1, \dots, c_{n-1}) \in \mathbb{A}_k^{n-1}$, and let $g(X_n) = f(c_1, \dots, c_{n-1}, X_n) \in k[X_n]$ has at least one root, thus we get that

$$V(f) = \bigcup_{\mathbf{c} \in \mathbb{A}_k^{n-1}} \{\mathbf{c}\} \times V(g_{\mathbf{c}}),$$

where $V(g_{\mathbf{c}})(\neq \emptyset) \subseteq \mathbb{A}_k^1$ (since k is algebraically closed). Thus in particular we get that $V(f)$ is infinite.

Part (c). In **Problem 3.12** we have proved that if f and g are distinct irreducible polynomials in $k[X, Y]$, then $V(f, g)$ is finite. But then we know that $V(f)$ and $V(g)$ are infinite sets (by part (b)), and hence since $V(f, g) = V(f) \cap V(g)$, we get that $V(f)$ and $V(g)$ have only finitely many points in common, hence they can not define the same hypersurface.

Part (d). We can generalise the above result as follows:
Let f, g in $k[X_1, \dots, X_n]$ be irreducible polynomials which are not multiple of one another, further assume that $n \geq 2$ and k algebraically closed, then the hypersurfaces $V(f)$ and $V(g)$ defined by them are distinct.

We can easily proof this using Nullstellensatz theorem, for the sake of contradiction assume that $V(f) = V(g)$. But then we get that

$$(f) = \mathbf{rad}(f) = I(V(f)) = I(V(g)) = \mathbf{rad}(g) = (g)$$

since (f) and (g) are prime ideals and k is algebraically closed, thus we get that $f = \lambda g$ (contradiction!). Therefore we must have $V(f) \neq V(g)$. ■

Problem 1.7. *Give an example to show that the proof of Noether normalisation given in (3.13) fails over a finite field k.*

Solution. For simplicity let, $k = \mathbb{F}_q$. Let, $q > d$. Take the Ideal $I = (f) \subset k[X, Y]$, where $f(X, Y) = X^q Y^{d-q} - XY^d$. Now,

$$f(X + \alpha Y, Y) = (X^q + \alpha^q Y^q)Y^{d-q} - (X + \alpha Y)Y^{d-1} = (\alpha^q - \alpha)Y^d + (\cdots)$$

Note that, $F(\alpha, 1) = \alpha^q - \alpha$ is zero for all $\alpha \in k$. Thus we can't prove Noether Normalization in the same way.

Problem 1.8. *Let, A be a ring and $A \subset B$ is a finite A-algebra. Prove that if $\mathfrak{m}$ is a maximal ideal of A then $mB \neq B$.*

Solution. Since B is a finite A algebra we can assume, $a_1, \cdots, a_m$ be generates B (as a module of A). If $mB = B$ then we can write,

$$a_j = \sum_i b_{ij} a_i$$

where i runs over $1, \cdots, m$ and b_{ij} are elements of $\mathfrak{m}$. Thus, we have

$$B(a_1 \cdots a_m)^T = 0$$

where $B_{ij} = b_{ij}$ for $i \neq j$ and $B_{ij} = b_{ij} - 1$ for $i = j$. From here, it's not hard to see $\det B(a_1 \cdots a_m)^T = 0$ (just by multiplying **adj** B with the above equation). So, $\det B.a_i = 0$ for all i. And hence, $\det B.1_B = 0$. This means $1 \in \mathfrak{m}$. Which is not possible by definition of 'maximal ideal'. ■

Problem 1.9. *Let, $A = k[a_1, \cdots, a_n]$ be as in the statement of Noether Normalization. Let, I be the kernal of the natural map, $k[X_1, \cdots, X_n] \to k[a_1, \cdots, a_n]$. Consider, $V = V(I)$ in $\mathbb{A}_k^n$ (for simplicity assume I is prime ideal). Let, $Y_1, \cdots Y_m$ be the general linear forms in $k[X_1, \cdots, X_n]$. Let, $\pi : \mathbb{A}_k^n \to \mathbb{A}_k^m$ and $p : \pi|_V : V \to \mathbb{A}_k^m$. Prove that, for every $P \in \mathbb{A}_k^m$, $p^{-1}(P)$ is non-empty and finite if k is algebraically closed.*

Solution. Before proving the statement we would like to describe the map p explicitly. Let, ρ^* be the map from $k[X_1, \cdots, X_n]$ to $A = k[a_1, \cdots, a_n] \simeq k[X_1, \cdots, X_n]/I$. A is a finite k-algebra. By **Noether Normalization** we can say, $k[a_1, \cdots, a_n]$ is finite and integral over $k[t_1, \cdots, t_m]$, Where, $\{t_i\}$ are algebraically independent. From the constructive proof of **Noether Normalization**, we can assume t_i to be linear over a_i. Thus,

$$t_i = \sum_{j=1}^{n} A_{ij} a_j$$

If we set, $\pi^* : k[Y_1, \cdots, Y_m] \to k[X_1, \cdots, X_n]$ where, $Y_i \mapsto \sum A_{ij} X_i$, the following diagram commutes:

$$\begin{tikzcd}
k[X_1, \cdots, X_n] \arrow[r, "\rho^*"] & A = k[a_1, \cdots, a_n] \simeq k[X_1, \cdots, X_n]/I \\
k[Y_1, \cdots, Y_m] \arrow[u, "\pi^*"] \arrow[r, "y_i \mapsto t_i"'] & k[t_1, \cdots, t_m] \arrow[u, hook, "\subseteq"']
\end{tikzcd}$$

Now, If we treat the above commutative diagram as a 'diagram of co-ordinate rings', there is a commutative diagram corresponding to the algebraic sets as follows :

$$\begin{tikzcd}
\mathbb{A}_k^n \arrow[d, "\pi"'] & V(I) \arrow[l, "\rho"'] \arrow[d, "p"] \\
\mathbb{A}_k^m & \mathbb{A}_k^m \arrow[l, "\text{id}"']
\end{tikzcd}$$

Here, ρ is the inclusion of $V(I)$ in $\mathbb{A}_k^n$, the π map is given by, $(x_1, \cdots, x_n) \mapsto (\sum A_{1j} x_1, \cdots, A_{mj} x_m)$. If we restrict π to $V(I)$ we will get p, thus the above diagram also commutes (as $p = \pi \circ \rho = \pi|_V$). We will first show, p is **surjective**. Let, $P = (b_1, \cdots, b_m)$ be a point in $\mathbb{A}_k^m$. Let, $\mathfrak{m}_P$ be the corresponding maximal ideal (by Nullstelensatz) in $k[Y_1, \cdots, Y_m]$. Consider the ideal $b_P := I + (\pi^*(Y_1) - b_1, \cdots, \pi^*(Y_m) - b_m)$ in $k[X_1, \cdots, X_n]$. We claim that, $b_P \neq (1)$. Otherwise we must had,

$$1 = f + f_1(\pi^*(Y_1) - b_1) + \cdots + f_m(\pi^*(Y_m) - b_m)$$

where $f \in I$ and $f_i \in k[x_1, \cdots x_n]$. Look at it's image under the map ρ^*. It will give us

$$1 = \bar{f}_1(t_1 - b_1) + \cdots + \bar{f}_m(t_m - b_m)$$

Here, I have used the fact $\rho^* \circ \pi^*(Y_i) = t_i$. Using the weak nullstelensatz we know $(t_1 - b_1, \cdots, t_m - b_m)$ is a maximal ideal in $k[t_1, \cdots, t_m]$ (as k is algebraically closed). But this maximal ideal contains 1, Which is not possible. Thus $b_P \neq (1)$ and hence $V(b_P) = V(I) \cap V(\pi^*(Y_1) - b_1, \cdots, \pi^*(Y_m) - b_m) \neq \emptyset$. There is a point $Q \in V(I)$ such that $f(Q) = 0$ for all $f \in b_P$. So, $\pi \circ p(Q) = P$, and hence by commutativity of the above square we can say, $p(Q) = P$. So, p is surjective.

Now, form the commutativity of the diagram of co-ordinate rings we can say, every X_i is given by a monic relation in $k[Y_1, \cdots, Y_m]$ which in contained in I. Thus, $p^{-1}(P)$ is **finite**. ■