PMath 464/764 – Homework 1 solutions

1. List all the points in the algebraic set $V(Y - X^2, X - Y^2) \subset \mathbb{A}^2$.

Solution: We're just looking for all the points where $Y - X^2 = X - Y^2 = 0$. This gives $Y = Y^4$, giving $Y = 0$, $Y = 1$, or $Y = (-1 \pm \sqrt{-3})/2$. Once we know Y, we can deduce X via $X = Y^2$, so we have four points:

$$(0,0),\ (1,1),\ (\frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}),\ (\frac{-1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2})$$

♣

2. Show that $\{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in \mathbb{C}\}$ is an algebraic set.

Solution: To show that this set (which we'll call A) is an algebraic set, we must find a set S of polynomials such that $A = V(S)$. Constructing S is a tricky business, so let's try to guess at some polynomials which might vanish on our A. To do this, let's set $X = t$, $Y = t^2$, and $Z = t^3$, and see what relations we can find between X, Y, and Z.

Well, notice that $t^2 = (t)^2$, so $Y - X^2$ vanishes on A, and similarly $Z - X^3$ also vanishes on A. We claim that $A = V(Y - X^2, Z - X^3)$.

We've already shown that A is a subset of $V(Y - X^2, Z - X^3)$, since both polynomials vanish on A – all we need to do is show the reverse inclusion. Thus, assume that $P = (x, y, z) \in \mathbb{A}^3(k)$ is an element of $V(Y - X^2, Z - X^3)$ – we want to show that $P \in A$.

Since $P \in V(Y - X^2, Z - X^3)$, it follows that $y - x^2 = 0$ and $z - x^3 = 0$. But that means that $P = (x, x^2, x^3)$, so $P \in A$ by definition! Thus, $A = V(Y - X^2, Z - X^3)$, and therefore A is an algebraic set. ♣

3. Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^2$, $L \not\subset C$. Suppose $C = V(F)$, $F \in \mathbb{C}[X, Y]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points.

Solution: First off, let's examine the condition $L \not\subset C$. This means that $I(C) \not\subset I(L)$, and $I(C) = (F)$ and $I(L) = (G)$, where G is some linear polynomial in X and Y. The condition $(F) = I(C) \not\subset I(L) = (G)$ simply means that F is not a multiple of G.

There are two cases. First off, L could be a vertical line: that is, L could be the line $X = c$ for some $c \in \mathbb{C}$. The set $L \cap C$ consists of all points $P \in \mathbb{A}^2$

such that $G(P) = F(P) = 0$. Let's solve these two equations simultaneously and see how many solutions we find.

If $P = (x, y)$, then $G(P) = 0$ means precisely that $x = c$. By the first paragraph, we know that $X - c$ is not a factor of F, so when we substitute $X = c$ in F, we don't get the zero polynomial. That means we must get a polynomial $p(Y)$ in Y of degree at most n, which has at most n roots. Since $F(P) = 0$, we get $F(x, y) = F(c, y) = 0$ and hence y is a root of $p(Y)$. Thus, we have one choice for P's x-coordinate and at most n choices for its y coordinate (the roots of $p(Y)$), and hence at most n choices for P, as desired.

The other case is more complicated, but is essentially the same. Assume that L is not a vertical line. Then we can write $G = Y - (mX + b)$ for some elements m and b of $\mathbb{C}$. If $P = (x, y)$ is a point on $L \cap C$, then we have $G(P) = F(P) = 0$ again, so $y = mx + b$ and $F(x, y) = 0$. Let's again try to solve these equations simultaneously.

By the first paragraph, we know that F is not a multiple of G, so when we substitute $Y = mX + b$ into F, we won't get the zero polynomial. Instead, we have to get a polynomial $p(X)$ in X of degree at most n. Thus, we get $p(x) = 0$, and so x must be a root of $p(X)$ of which there are at most n. Thus, there are at most n choices for the x-coordinate of P.

But once you know the x-coordinate of P, you can plug it into $y = mx+b$ to uniquely determine the y-coordinate as well! So there are at most n choices for P, and hence $L \cap C$ has at most n points. ♣

4. Show that $V(Y - X^2) \subset \mathbb{A}^2$ is irreducible, and that $I(V(Y - X^2)) = (Y - X^2)$.

Solution: Let's take the quotient of $\mathbb{C}[X, Y]$ by the ideal $(Y - X^2)$, and check that we end up with a domain. Define a homomorphism $\phi\colon \mathbb{C}[X, Y] \to \mathbb{C}[X]$ by $\phi(F(X, Y)) = F(X, X^2)$. It is surjective with kernel $(Y - X^2)$, and $\mathbb{C}[X]$ is a domain, so $(Y - X^2)$ must be a prime ideal. This means that $Y - X^2$ is irreducible, as desired.

The fact that $I(V(Y - X^2)) = (Y - X^2)$ is immediate from the Nullstellensatz and the fact that $(Y - X^2)$ is prime, and therefore radical. ♣

5. Let D be the affine algebraic set $V(Y^2 - X^3 - X^2, X)$ in the affine plane $\mathbb{A}^2$. Show that $I(D) \neq (Y^2 - X^3 - X^2, X)$, and that $(Y^2 - X^3 - X^2, X)$ is not a radical ideal.

Solution: Let $J = (Y^2 - X^3 - X^2, X)$. By the Nullstellensatz, we know that $I(D)$ is a radical ideal, and that it contains J. If we can find an polynomial

F such that $F^n \in J$ but $F \notin J$, then we'll know that J is not radical, and hence that it's not equal to $I(D)$. Indeed, F will be a polynomial which is an element of $I(D)$ but not J.

If we reduce everything modulo J, we find that such a polynomial F satisfies $F^n = 0 \pmod{J}$ but $F \neq 0 \pmod{J}$ – that is, F is nilpotent in $\mathbb{C}[X,Y]/J$. So let's examine the ring $\mathbb{C}[X,Y]/J$ and try to find nilpotent elements.

Write $R = \mathbb{C}[X,Y]/J$. In R, we have $Y^2 = X^3 + X^2$ and $X = 0$. It's easy to deduce from these that $Y^2 = 0$. We claim that Y is a nilpotent element of R.

Certainly $Y^2 = 0$ in R, from the previous equation. All we have to do is show that $Y \neq 0 \pmod{J}$, which is to say, we just have to show that $Y \notin J$. Thus, assume $Y \in J$. Then for some polynomials $G(X,Y)$ and $H(X,Y)$, we can write:

$$Y = (Y^2 - X^3 - X^2)G(X,Y) + XH(X,Y)$$

(Remember now that we're working with plain old polynomials in $\mathbb{C}[X,Y]$, not R.) Since there's a linear Y term on the left side, there must be a linear Y term on the right. Where can it come from? Not from $(Y^2 - X^3 - X^2)G(X,Y)$, since every term in that product has degree at least 2. And not from $XH(X,Y)$ either, since every term in that polynomial has a factor of X in it. So the above equality is impossible! Thus, $Y \notin J$, and hence J is not radical, and can therefore not equal $I(D)$. ♣

6. Let I be an ideal in a commutative ring R with $I \neq R$ and $1 \in R$, and let $\pi\colon R \to R/I$ be the natural homomorphism.

(a) For every ideal J' of R/I, define the set $J = \pi^{-1}(J')$. Show that J is an ideal of R containing I, and that for every ideal J of R containing I, the set $J' = \pi(J)$ is an ideal of R/I. This sets up a natural one-to-one correspondence between $\{\text{ideals of } R/I\}$ and $\{\text{ideals of } R \text{ which contain } I\}$.

(b) Show that J' is a radical ideal if and only if J is a radical ideal. Do the same for prime and maximal ideals.

(c) Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian, and that in particular every ring of the form $\mathbb{C}[X_1, \ldots, X_n]/I$ is Noetherian.

[A point of notation: $\pi^{-1}J'$ denotes the set $\{x \in R | \pi(x) \in J'\}$. It does not imply that π is injective; it just represents the set of all elements of R

which end up in J' when you reduce modulo I.]

Solution: (a) Let J' be an ideal of R/I, and let $J = \pi^{-1}J'$. To show that J is an ideal, we need to check that 0 is in J, and that J is closed under addition and under multiplication by elements of R.

Certainly $O \in J$, since $\pi(0) = 0 \in J'$. If a and b are in J, then $\pi(a) \in J'$ and $\pi(b) \in J'$, so $\pi(a+b) = \pi(a) + \pi(b) \in J'$, and hence $a + b \in J$. Finally, if $a \in J$ and $r \in R$, then $\pi(ar) = \pi(r)\pi(a) \in J'$, so $ar \in J$, as desired. Thus, J is an ideal. It contains I because $\ker \pi = I$, and hence if $x \in I$, then $\pi(x) = 0 \in J'$ and hence $x \in J$.

Now assume that J is an ideal of R with $I \subset J$ (the hypothesis $I \subset J$ is actually completely unnecessary). Let's check that $J' = \pi(J) = \{x \in R/I | x = \pi(a) \text{ for some } a \in J\}$ is an ideal of R/I. Certainly $0 \in J'$, since $0 = \pi(0)$ with $0 \in J$. If x and y are elements of J', then $x = \pi(a)$ and $y = \pi(b)$ for some a and b in J, so $x + y = \pi(a + b)$ with $a + b \in J$, since J is an ideal. Finally, if $x \in J'$ and $z \in R/I$, then $x = \pi(a)$ for some $a \in J$ and $z = \pi(r)$ for some $r \in R$ (since π is surjective), and hence $xz = \pi(ar)$ with $ar \in J$ because J is an ideal. ♣

(b) Say J is not radical. Then there is some $a \in R$ with $a^n \in J$ and $a \notin J$, so $\pi(a)^n \in J'$ and $\pi(a) \notin J'$, so J' is not radical either. Conversely, if $x^n \in J'$ but $x \notin J'$, then find $r \in R$ with $\pi(r) = x$ (this is possible because π is surjective). Then $r \notin J$ but $r^n \in J$, so J isn't radical.

Say J is not prime. Then there are a and b in R such that $ab \in J$ but neither a nor b are in J. Then $\pi(a)\pi(b) \in J'$ but $\pi(a)$ and $\pi(b)$ are not in J', so J' isn't prime either. Conversely, if J' is not prime, then there are x and y in R such that $xy \in J'$ but neither x nor y are in J'. If we find a and b in R such that $\pi(a) = x$ and $\pi(b) = y$, then neither a nor b are in J, but $ab \in J$, so J isn't prime either.

Finally, say J isn't maximal. Then there is some proper ideal M of R such that $J \subset M$ but $M \neq J$, so $\pi(M)$ is a proper ideal containing J'. All we need to do is show that $\pi(M) \neq J' = \pi(J)$. Thus, choose some element $m \in M$ with $m \notin J$. Then $\pi(m) \in \pi(M)$, but $\pi(m) \notin J'$, and hence $\pi(M) \neq J'$, as desired. Conversely, if J' is not maximal, then there is some proper ideal M' of R/I such that $J' \subset M'$ but $J' \neq M'$. We know from part (a) that $\pi^{-1}(M)$ is an ideal of R, and it certainly contains J – all we need to do is show that it is not equal to J. Thus, choose any $x \in M'$ with $x \notin J'$, and find $a \in M$ such that $\pi(a) = x$. Then $a \in M$, but $a \notin J$, so M is a proper ideal with $J \subset M$ but $J \neq M$, and hence J is not maximal either. ♣

(c) If $J = (r_1, \ldots, r_i)$ is finitely generated, then for any $r \in J$ we can write $r = f_1 r_1 + \ldots + f_i r_i$, so $\pi(r) = \pi(f_1)\pi(r_1) + \ldots + \pi(f_i)\pi(r_i)$ for any $\pi(r) \in J'$. Thus, $J' = (\pi(r_1), \ldots, \pi(r_i))$ is also finitely generated, as desired.

The last two statements are trivial consequences of the first: if R is Noetherian, then every ideal is finitely generated, so by the previous paragraph (and part (a)) every ideal of R/I is finitely generated, so R/I is Noetherian. The last sentence is just plugging in $R = k[X_1, \ldots, X_n]$ and using the Hilbert Basis Theorem. $\clubsuit$