Homework III Solutions

2) Let X be an affine variety such that X is a finite set. Let $I = \mathcal{I}(X)$. Show that the Hilbert polynomial $HP_I(t)$ is constant and equal to $|X|$.

$\triangleright$ Let $x = (a_1, a_2, \dots, a_n) \in k^n$. Then $\mathcal{I}(x)$ is the maximal ideal $\mathfrak{m}_x = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n) \in k[X_1, \dots, X_n]$. Indeed, $X_i - a_i$ vanishes on x. Conversely, if $f \in k[X_1, \dots, X_n]$ then applying division with remainder we can write $f = g_1(X_1 - a_1) + \dots + g_n(X_n - a_n) + r$ with $r \in k$. Now, if $f(x) = 0$, it follows that $r = 0$.

We deduce that if X is a finite union of points, then we have $\mathcal{I}(X) = \bigcap_{x \in X} \mathfrak{m}_x$. Therefore, by the Sunzi remainder theorem, since maximal ideals are pairwise coprime, we have

$$k[X_1, X_2, \dots X_n]/\mathcal{I}(X) = \prod_{x \in X} k[X_1, \dots, X_n]/\mathfrak{m}_x = \prod_{x \in X} k$$

Thus, we conclude that Hilbert polynimial of $\mathcal{I}(X)$ is constant and equal to $|X|$.

<u>Extra</u>: Suppose $X = \{x_1, \dots, x_m\}$ with $x_i = (x_i^{(1)}, x_i^{(2)}, \dots, x_i^{(n)}) \in k^n$. It is possible to give the above isomorphism more explicitly by finding polnomials $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ such that $f_i(x_i) = 1$ and $f_i(x_j) = 0$ for $i \neq j$. One way of defining such polynomials is as follows: For each distinct pair $i, j \in \{1, \dots, m\}$ find k_{ij} such that $x_i^{(k_{ij})} \neq x_j^{(k_{ij})}$. Such k_{ij} has to exist as x_i and x_j are different points. Now define

$$f_i = \prod_{\substack{j=1,\\ j \neq i}}^{m} \frac{X_{k_{ij}} - x_j^{(k_{ij})}}{x_i^{(k_{ij})} - x_j^{(k_{ij})}}$$

5) Find the normalisation of $\mathbb{Z}[\sqrt{d}]$ for d a square-free integer.

$\triangleright$ We first note that the field of fractions of $\mathbb{Z}[\sqrt{d}]$ is $K = \mathbb{Q}(\sqrt{d})$. This follows easily from the observation that $\mathbb{Q}(\sqrt{d})$ is the smallest field that contains $\mathbb{Z}[\sqrt{d}]$. Or alternatively, one can write an explicit isomorphism using

$$\frac{x + y\sqrt{d}}{z + w\sqrt{d}} = \frac{(x + y\sqrt{d})(z - w\sqrt{d})}{z^2 - dw^2} = \frac{xz - ywd}{z^2 - dw^2} + \frac{(yz - xw)}{z^2 - dw^2}\sqrt{d} \text{ for } x, y, z, w \in \mathbb{Z},\ (z, w) \neq (0, 0).$$

Next, we observe that any element of K that is integral over $\mathbb{Z}[\sqrt{d}]$ is in fact integral over $\mathbb{Z}$. This holds because $\mathbb{Z}[\sqrt{d}]$ is an integral extension of $\mathbb{Z}$ since $\sqrt{d}$ is the root of the monic polynomial $X^2 - d$ with integer coefficients. Therefore, the normalisation of $\mathbb{Z}[\sqrt{d}]$ coincides with the algebraic integers $\mathcal{O}_K$, that is the integral closure of $\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{d})$.

Let $\alpha = u + v\sqrt{d} \in \mathcal{O}_K$, then α is a zero of the polynomial

$$X^2 - 2uX + u^2 - dv^2$$

so, by Gauss lemma, the rational numbers $2u$ and $u^2 - dv^2$ must in fact be integers. We have $4u^2 - 4dv^2$ and d is square-free, hence $2v$ must be an integer as well. Next, we observe that if d is congruent to 2 or 3 modulo 4, then since $4u^2 - 4dv^2 \equiv 0 \pmod 4$ and a square is congruent to 0 or 1 (mod 4), we see that $2u$ and $2v$ must be even, which implies u and v are integers. In this case, we conclude that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. On the other hand, if d is congruent to 1 modulo 4, then $2u \equiv 2v \pmod 4$, hence $u - v$ is an integer. Hence, we get that elements of $\mathcal{O}_K$ must be of the form $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$. Finally, we note that $\frac{1+\sqrt{d}}{2}$ is indeed in $\mathcal{O}_K$ since setting $u = v = 1/2$ gives $2u \in \mathbb{Z}$ and $u^2 - dv^2 \in \mathbb{Z}$. We conclude that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

7) Consider a 2-by-2 matrix M with entries X, Y, Z, W. If we then want to solve $M^2 = 0$, we get four equations and let's make that into an ideal $I = (X^2+YZ, XY+YW, XZ+WZ, W^2+YZ) \in k[X, Y, Z, W]$. Is I a radical ideal? Show that $\sqrt{I} = (X + W, XW - YZ)$.

Let us first give a proof under the assumption $k = \overline{k}$ algebraically closed. Recall that the characteristic polynomial of a 2-by-2 matrix M is given by

$$\chi_M(t) = t^2 - (\mathrm{tr}M)t + \det M$$

Now, since $M^2 = 0$ and $\chi_M(M) = 0$ (Cayley-Hamilton theorem), the minimal polynomial of M has to divide both t^2 and $\chi_M(t)$. This implies that $\chi_M(t) = t^2$, hence $M^2 = 0$ implies that $\mathrm{tr}M = X + W = 0$ and $\det M = XW - YZ = 0$.

Thus, it follows from Nullstellensatz (using the fact that k is algebraically closed) that $X + W, XW - YZ \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. Or equivalently,

$$J := (X + W, XW - YZ) \subset \sqrt{I}$$

Conversely, to prove that $\sqrt{I} \subset J$ it suffices to show that $I \subset J$ and J is prime. It is easy to see that $I \subset J$ because $X^2 + YZ = (X + W)X - (XW - YZ)$, $XY + YW = (X + W)Y$, $XZ + WZ = (X + W)Z$, $W^2 + YZ = (X + W)W - (XW - YZ)$. (Alternatively, observe that if $\mathrm{tr}M = 0 = \det M$, then from $\chi_M(M) = 0$, we conclude that $M^2 = 0$. Hence, $I \subset \sqrt{J}$ by Nullstellensatz, which implies $I \subset J = \sqrt{J}$ if we show that J is prime.)

It remains to show $J = (X + W, XW - YZ)$ is prime. Showing this is equivalent to proving that $k[X, Y, Z, W]/(X + W, XW - YZ)$ is an integral domain. Let us first observe the ring isomorphism

$$k[X, Y, Z, W]/(X + W, XW - YZ) \simeq k[X, Y, Z]/(X^2 + YZ)$$

given by sending $(\overline{X}, \overline{Y}, \overline{Z}, \overline{W}) \to (\overline{X}, \overline{Y}, \overline{Z}, -\overline{X})$. We observe that this sends $(X+W, XW-YZ)$ to $(X^2 + YZ)$. It is obviously surjective. To see that it is injective, by using the relation $X+W = 0$, any element of $k[X, Y, Z, W]/(X+W, XW-YZ)$ can be represented by $f(\overline{X}, \overline{Y}, \overline{Z})$ for some $f \in k[X, Y, Z]$. This element goes to zero in $k[X, Y, Z]/(X^2 + YZ)$ if and only if $f(X, Y, Z)$ is divisible by $X^2 + YZ$ but then it is also zero $k[X, Y, Z, W]/(X + W, XW - YZ)$ since $X^2+YZ = X(X+W) - (XW-YZ) \in (X+W, XW-YZ)$. Thus, it suffices to see that $k[X, Y, Z]/(X^2 + YZ)$ is an integral domain, or that $(X^2 + YZ) \subset k[X, Y, Z]$ is prime but this holds because $k[X, Y, Z]$ is a UFD and $f = X^2+YZ$ is irreducible. (To see that f is irreducible, you can observe that it doesn't factor into linear components).

We now give a proof that works in general (without assuming k is algebraically closed). The only place where we used k is algebraically closed was when we argued that $X + W$ and $XW - YZ$ are in $\sqrt{I}$. Indeed, we can verify this directly as follows:

$$(X + W)^3 = (X + 3W)(X^2 + YZ) + (W + 3X)(W^2 + YZ) - 4Z(XY + YW)$$
$$(XW - YZ)^2 = (X^2 + YZ)(W^2 + YZ) - XZ(XY + YW) - YW(XZ + WZ)$$

Alternatively, once we see that $X + W \in \sqrt{I}$ from the first equation, we can write $XW - YZ = (X + W)W - (W^2 + YZ)$ to conclude that it too is in $\sqrt{I}$.

8) Show that if $f : R \to S$ is a ring homomorphism between finitely generated k-algebras R and S, then $f^{-1}(\mathfrak{m})$ is a maximal ideal of R for all maximal ideals $\mathfrak{m}$ of S.

Because S is a finitely generated k-algebra, its quotient $S/\mathfrak{m}$ by a maximal ideal $\mathfrak{m}$ is a finite field extension of k by Zariski's lemma. Therefore, the image of R in $S/\mathfrak{m}$ under the composition of ring homomorphisms $R \to S \to S/\mathfrak{m}$ is an integral domain which is an integral extension of k, hence is a field (see Corollary 4.22 in the lecture notes). But, the kernel of the map $R \to S/\mathfrak{m}$ is $f^{-1}(\mathfrak{m})$ hence the image is isomorphic to $R/f^{-1}(\mathfrak{m})$ which we have shown is a field, therefore $f^{-1}(\mathfrak{m})$ is a maximal ideal.