Math 724: Solutions 3

1. Let X be a subset of $\mathbb{A}^n$ over an algebraically closed field. Is $I(X)$ radical? Prove your answer.

2. Let $\mathbb{A}^n$ be affine space over an algebraically closed field. Give an example of a subset $X \subset \mathbb{A}^n$ such that $Z(I(X)) \neq X$. What condition would ensure equality? Prove your answer. You may use Hilbert Nullstellensatz, i.e. that
$$I(Z(I)) = rad\, I$$
but you may not use the fact that this gives a 1-1 bijection between algebraic sets and radical ideals unless you prove it.

   Solution. An example where equality does not hold is the disk $X = \{x \in \mathbb{C} : ||x||^2 < 1\}$ in $\mathbb{C}^1$. In this case, $I(X) = \{0\}$ since no nonzero polynomials vanish on this disk. Then $Z(I(X)) = \mathbb{C}^1 \neq X$. We can ensure that we get equality if X is algebraic. X is algebraic implies $X = Z(I)$ for some ideal I. We may choose I radical (by Nullstellensatz). Then $I(X) = I(Z(I)) = I$ implies that $Z(I(X)) = Z(I) = X$.

3. Let k be an algebraically closed field. Show that all nonzero prime ideals in $k[x]$ are maximal. What does this mean about algebraic sets on $\mathbb{A}^1$? Would this be true if k were not algebraically closed? Assuming k is algebraically closed, find a nonzero prime ideal in $k[x_1, x_2]$ that is not maximal. What algebraic set does this correspond to?

   Solution. We showed that for an algebraically closed field, all nonzero maximal ideals of $k[x]$ are of the form
$$\mathfrak{m}_p = \{x - a\}.$$
   Let $I \subset k[x]$ be prime. Then I is generated by a finite number of functions $f_1, \ldots f_l$. Each one of these functions f_i factors into a product of linear terms over an algebraically closed field. Since I is prime, one of these linear terms must also be in I. This implies that $\mathfrak{m}_p \subset I$, where p is obtained by one such linear term. But since $\mathfrak{m}_p$ is maximal, we have that $I = \mathfrak{m}_p$. (By the way, this also implies that I is generated by just one, linear function). This implies that the only algebraic sets on $\mathbb{A}^1$ are points (and $\mathbb{A}^1$ and $\emptyset$).

   When k is not algebraically closed, this is still true for $k[x]$. Let $P \subset k[x]$ be a prime ideal. Choose $f \in P$ of minimal degree. Since P is prime, f cannot be factored into smaller-degree polynomials (for if it could, then one of factors would be in P, contradicting the assumption that P is prime). If $(f) \subset P$ is maximal, then $(f) = P$ and we're done. Otherwise, assume (f) is not maximal. Let g be such that (f, g) properly contains (f) (you may choose $g \in P$ but you don't have to). We show that $(f, g) = k[x]$, implying that (f) has to be maximal, and therefore $(f) = P$ is maximal.

   Use the Euclidean algorithm. Write
$$f = q_0 g + r_1,$$

with $\deg(r_1) < \deg(g)$ (here $\deg(g)$ is the degree as a polynomial). This implies $r_1 \in (f, g)$.

Since f can't be factored, you get $r_1 \neq 0$. Continue:

$$f = q_1 r_1 + r_2,$$

and $\deg(r_2) < \deg(r_1)$ and $r_2 \neq 0$ since f can't be factored. This implies $r_2 \in (f, g)$.

Continue inductively to obtain $f = q_m r_m + r_{m+1}$ where $\deg(r_{m+1}) = 0$ but $r_{m+1} \neq 0$, which means it's a field element. Thus $r_{m+1} \in (f, g)$ which implies it's the whole ring.

More generally, in a PID every nonzero prime ideal is maximal. Proving that fact is good preparation for the preliminary exam!

An example of an prime ideal that's not maximal in $k[x_1, x_2]$ is $I = (x_1^2 - x_2)$ on $\mathbb{C}^2$. There are more solutions than distinct points, which implies that the ideal is not maximal. However, it is prime since $k[x_1, x_2]/I \cong k[x_1]$, which is an integral domain.

4. 2.2 p. 79

Solution. We show that $R[U^{-1}] \cong R[\{x_u\}_{u \in U} / (\{ux_u - 1\}_{u \in U})$.

Let $\phi : R[U^{-1}] \to R[\{x_u\}_{u \in U} / (\{ux_u - 1\}_{u \in U})$ be given by $\phi(r, u) = rx_u$. We need to show this is a well-defined isomorphism of R-modules. Let $(r', u') \sim (r, u)$. Then there is some $v \in U$ such that $vr'u = vru'$. Then

$$\begin{aligned}
\phi(r', u') &= r' x_{u'} \\
&= r' uv x_u x_v x_{u'} \quad \text{since } vx_v = ux_u = 1 \text{ in the target ring} \\
&= ru' v x_u x_v x_{u'} \\
&= r x_u \quad \text{since } vx_v = u' x_{u'} = 1 \\
&= \phi(r, u).
\end{aligned}$$

We now show it's an isomorphism. It's clearly surjective, for any polynomials is a sum of monomials, and any monomial $r x_{u_1}^{k_1} \cdots x_{u_r}^{k_r}$ is the image of $(r, u_1^{k_1} \cdots u_r^{k_r})$. Lastly, the map ϕ is injective: any polynomial in this ring can be rewritten as rx_u for some $r \in R, u \in U$, since

$$x_{u_1}^{k_1} \cdots x_{u_r}^{k_r} = x_{u_1^{k_1} \cdots u_r^{k_r}}$$

and

$$x_u + x_v = (u + v) x_{uv}$$

(these follow from the well-defined-ness of ϕ, since $(1, u) \cdot (1, u') = (1, uu')$ and $(r, u) + (r', v) \sim (ru + r'v, uv)$in $R[U^{-1}]$.). Then a monomial rx_u is zero if and only if $r = 0$, which in turn implies its preimage is $(0, u) \sim 0$ in $R[U^{-1}]$.

5. Describe as explicitly as possible the $\mathbb{Z}$-module $Hom_{\mathbb{Z}}(\mathbb{Z}_p, \mathbb{Z}_m)$ where p is a prime number.

Solution.

A homomorphism is determined by where it sends 1. But since $1 + \cdots 1 (p \text{ times}) = 0$ in $\mathbb{Z}_p$, 1 must map to something in $\mathbb{Z}_m$ which, when summed p times is 0, i.e whose order is p in $\mathbb{Z}_m$. If p does not divide m,

no elements of $\mathbb{Z}_m$ have order p, and thus there is only the 0-homomorphism. If p divides m, then 1 can go to $\frac{m}{p}$ or any multiple of it in $\mathbb{Z}_m$. There are p such numbers, and they form a cyclic subgroup of $\mathbb{Z}_m$. We define a map

$$\Phi : \hom_{\mathbb{Z}}(\mathbb{Z}_p, \mathbb{Z}_m) \longrightarrow \mathbb{Z}_p$$

as follows. Let $\phi \in \hom(IZ_p, \mathbb{Z}_m)$. Then $\phi(1) = k_\phi \frac{m}{p}$, by the discussion above, where $k_\phi \in \{0, 1, \ldots, p-1\}$. Let $\Phi(\phi) := k_\phi \in \mathbb{Z}_p$. It is easy to check that Φ is a homomorphism of $\mathbb{Z}$-modules, since $k_\phi \frac{m}{p} + k_\psi \frac{m}{p} = (k_\phi + k_\psi \mod p)\frac{m}{p}$ implies $\Phi(\phi + \psi) = k_{\phi+\psi} = k_\phi + k_\psi \mod p$. To show that Φ is an isomorphism we simply note that it's clearly surjective (injectivity follows from the cardinality). You could also prove injectivity directly.

6. Describe as explicitly as possible $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_m$ where p is a prime number.

   If p does not divide m, then the tensor product is 0, since there exist $a, b \in \mathbb{Z}$ such that $1 = ap + bm$, which in turn implies that

   $$1 \otimes 1 \sim (ap + bm)(1 \otimes 1) = (ap + bm) \otimes 1 = bm \otimes 1 = b \otimes m = 0.$$

   If $1 \otimes 1 = 0$, then there cannot be any other nontrivial elements, since any $r \otimes r' = rr'(1 \otimes 1)$.

   On the other hand, if p does divide m, then $1 \otimes r \sim 0$ if r is a multiple of p, since $1 \otimes pr' \sim p \otimes r' \sim 0 \otimes r' = 0$. We claim that

   $$\mathbb{Z}_p \otimes \mathbb{Z}_m \cong \mathbb{Z}_p,$$

   with isomorphism given by $\Phi : 1 \otimes r \to r \mod p$. The map is a well-defined homomorphism, because

   $$\begin{aligned}\Phi(1 \otimes r + 1 \otimes r') &= \Phi\left(1 \otimes (r + r' \mod m)\right) \\ &= [(r + r') \mod m] \mod p \quad = r + r' \mod p \quad \text{(this is where we use } p \text{ divides } m\text{)} \\ &= \Phi\left(1 \otimes r\right)) + \Phi\left(1 \otimes r'\right)\end{aligned}$$

   The map is clearly onto, since $r \in \mathbb{Z}_m$ covers every element in $\mathbb{Z}_p$. It is one-to-one because if $r \mod p = r' \mod p$, then $r - r' = ap$ for some $a \in \mathbb{Z}$. This implies $1 \otimes (r - r') = p \otimes a = 0$ in $\mathbb{Z}_p \otimes \mathbb{Z}_m$. But then $1 \otimes r = 1 \otimes r'$.

7. (Extra Credit) 2.4 p. 79