MATH338 Algebra IIIB

Assignment S1 Solutions

1. In the ring $\mathbf{Q}[x,y]$, each element can be written as $a = \sum_{p,q} a_{pq} x^p y^q$ where $a_{pq} \in \mathbf{Q}$.

(a) Take A to be the set of such a with zero constant term; that is, $a_{00} = 0$. Let $a' = \sum_{p,q} a'_{pq} x^p y^q$ also be in $\mathbf{Q}[x,y]$. The constant term in $a + a'$ is $a_{00} + a'_{00}$; so, if a and a' are in A, so is $a + a'$. The constant term in $a a'$ is $a_{00} a'_{00}$; so, if a is in A, so too is $a a'$. So A is an ideal.

(b) Take B to be the set of a in $\mathbf{Q}[x,y]$ which do not involve x. This is not an ideal since the constant polynomial 1 is in B yet $x\,1$ is not in B.

(c) Let C be the set of a in $\mathbf{Q}[x,y]$ with $a_{pq} = 0$ for all $p + q = 2$. Then x is in C while $x\,x$ is not in C.

2. (a) First we note a general principle: for any ring morphism $f : R \longrightarrow S$, each ideal A in S determines an ideal $f^{-1}A = \{r \in R \mid f(r) \in A\}$ in R. We can apply this to the ring morphism $f : \mathbf{Z} \longrightarrow \mathbf{Z}_6$ defined by $f(k) = k + 6\mathbf{Z}$: every ideal A of $\mathbf{Z}_6$ determines an ideal $f^{-1}A$ of $\mathbf{Z}$. We know all the ideals of $\mathbf{Z}$: so $f^{-1}A = m\mathbf{Z}$ for some $m \geq 0$. So $A = f f^{-1}A = f(m\mathbf{Z}) = \{mk + 6\mathbf{Z} \mid k \in \mathbf{Z}\} = m\mathbf{Z}_6$. Since $m\mathbf{Z} = m'\mathbf{Z}$ whenever $m \pm m'$ is divisible by 6, the complete list of ideals of $\mathbf{Z}_6$ is:

$$0 \,,\, 2\mathbf{Z}_6 \,,\, 3\mathbf{Z}_6 \,,\, \mathbf{Z}_6 .$$

(b) If $f : \mathbf{Z}_6 \longrightarrow R$ is a surjective ring morphism, by the First Isomorphism Theorem, R is isomorphic to $\mathbf{Z}_6 / A$ where A is the kernel of f. Since A is an ideal of $\mathbf{Z}_6$, it must be one of the 4 ideals listed in part (a). It is easily seen that $\mathbf{Z}_6 / 0 \cong \mathbf{Z}_6$, $\mathbf{Z}_6 / 2\mathbf{Z}_6 \cong \mathbf{Z}_2$, $\mathbf{Z}_6 / 3\mathbf{Z}_6 \cong \mathbf{Z}_3$, $\mathbf{Z}_6 / \mathbf{Z}_6 \cong \mathbf{Z}_1 = 0$ (these are cases of the Third Isomorphism Theorem; here Lagrange's Theorem tells you that the cardinalities are correct). So the possible values for n are $1, 2, 3, 6$.

3. Again we begin with a general principle: for commutative rings R and S, the only ideals of the product ring $R \times S$ are those of the form $A \times B$ where A is an ideal of R and B is an ideal of S. To prove this, suppose C is an ideal of $R \times S$. Clearly $A = \{a \in R \mid (a,0) \in C\}$ is an ideal of R and $B = \{b \in S \mid (0,b) \in C\}$ is an ideal of S. We need to see that $A \times B = C$. If $(a,b) \in A \times B$ then $(a,0) \in C$ and $(0,b) \in C$ so $(a,b) = (a,0) + (0,b) \in C$. Conversely, if $(a,b) \in C$ then

$$(a,0) = (1,0)(a,b) \in C \quad \text{and} \quad (0,b) = (0,1)(a,b) \in C;$$

so a is in A and b is in B; so $(a,b) \in A \times B$.

(a) Since fields have no proper ideals, it follows that, if F and K are fields, the only ideals of $F \times K$ are of the form $A \times B$ where $A = 0$ or F and $B = 0$ or K. So the ideals of $F \times K$ are 0×0, $F \times 0$, $0 \times K$, $F \times K$.

(b) Since the only ideals of $\mathbf{Z}$ are of the form $n\mathbf{Z}$, the only ideals of $\mathbf{Z} \times \mathbf{Z}$ are of the form $n_1\mathbf{Z} \times n_2\mathbf{Z}$ for natural numbers n_1 and n_2.

4. (a) $x\,x \in (x^2)$ yet $x \notin (x^2)$; so (x^2) is not prime.

(b) Put $M = (x-2, y-3)$ as an ideal of $\mathbf{Q}[x,y]$. Each $a \in \mathbf{Q}[x,y]$ can be written in the form $a = \alpha + b(x-2) + c(y-3)$ where α is in $\mathbf{Q}$. and b and c are in $\mathbf{Q}[x,y]$. Suppose $M < A$ for some ideal A of $\mathbf{Q}[x,y]$. Then there is some a in A that is not in M. In the notation above, this means $\alpha \neq 0$. Since A contains M, the polynomial $b(x-2) + c(y-3)$ is in A; so α is in A. So $1 = \alpha^{-1}\alpha$ is in A. So $A = \mathbf{Q}[x,y]$. So M is maximal.

(c) Put $P = (y-3)$. Each $a \in \mathbf{Q}[x,y]$ can be written in the form $a = b + c(y-3)$ where b is in $\mathbf{Q}[x]$ and c is in $\mathbf{Q}[x,y]$. Suppose we simmilarly have $a' = b' + c'(y-3)$ with $aa' \in P$. Then

$$aa' = (b + c(y-3))(b' + c'(y-3)) = b\,b' + d(y-3)$$

implies $b\,b' \in P$. But $b\,b' \in \mathbf{Q}[x]$; so the only multiple of $y-3$ it can be is the zero multiple. So $b\,b' = 0$. Since $\mathbf{Q}[x]$ is a division ring, either $b = 0$ or $b' = 0$. So $a \in P$ or $a' \in P$. So P is prime. However P is not maximal since it is contained in the M of part (b).

(d) Put $C = (x^2 + 1)$. Each $a \in \mathbf{Q}[x,y]$ can be written in the form $a = b_0 + b_1 x + c(x^2+1)$ where b_0 and $b_1 \in \mathbf{Q}[y]$ and c is in $\mathbf{Q}[x,y]$. If $aa' \in C$ then $aa' = b_0 b_0' + (b_0 b_1' + b_1 b_0')x + b_1 b_1' x^2 + d(x^2+1)$ implies $b_0 b_0' = 0$, $b_0 b_1' + b_1 b_0' = 0$ and $b_1 b_1' = 0$. Since $\mathbf{Q}[y]$ is a division ring, either $b_0 = 0$ or $b_0' = 0$, and either $b_1 = 0$ or $b_1' = 0$. If $b_0 = 0$ and $b_1 \neq 0$ then $b_1' = 0$ so $b_0 b_1' + b_1 b_0' = 0$ implies $b_0' = 0$; so $a' \in C$. If $b_0 = b_1 = 0$ then $a \in C$. So C is prime. It is not maximal since it is contained in the ideal (x^2+1, y) which does not contain x.

(e) $(x-1)(x+1) \in (x^2-1)$ yet $(x-1) \notin (x^2-1)$ and $(x+1) \notin (x^2-1)$. So (x^2-1) is not prime.

(f) Put $D = (x^2+1, y-3)$. Each $a \in \mathbf{Q}[x,y]$ can be written in the form $a = \alpha + \beta x + c(x^2+1) + d(y-3)$ where α and β are in $\mathbf{Q}$ and c and d are in

$\mathbf{Q}[x,y]$. Assume $D < A$ for some ideal A of $\mathbf{Q}[x,y]$. Take a in A that is not in D. Since $c(x^2+1)+d(y-3)$ is in D and so in A, we see that $\alpha+\beta x$ is in A. Assume $\alpha \neq 0$. Then we have $1+\gamma x \in A$ for some γ in $\mathbf{Q}$ (by multiplying $\alpha+\beta x$ by α^{-1}). So $(x-\gamma)+\gamma(x^2+1) = x+\gamma x^2 = x(1+\gamma x) \in A$. So $x-\gamma \in A$. Also $\gamma+\gamma^2 x = \gamma(1+\gamma x) \in A$. So $(1+\gamma^2)x = (x-\gamma)+(\gamma+\gamma^2 x) \in A$. Since γ is rational, $1+\gamma^2$ is invertible. So $x \in A$. Then $1+\gamma x \in A$ implies $1 \in A$. So $A = \mathbf{Q}[x,y]$. On the other hand, assume $\alpha = 0$. Then $\beta \neq 0$ and $\beta x \in A$; so $x \in A$. Then $1-(1+x^2) = (-x)x \in A$. So $1 \in A$. So $A = \mathbf{Q}[x,y]$. It follows that D is maximal.