M3P23, M4P23, M5P23: COMPUTATIONAL ALGEBRA & GEOMETRY

SOLUTIONS 1

(1) We proceed by induction on n. Let $f \in \mathbb{R}[x]$, and assume $f(a) = 0$ for all $a \in \mathbb{R}$. If $f \neq 0$ then f has at most $\deg f$ roots, contradicting the assumption. Hence $f = 0$.

Suppose $f \in \mathbb{R}[x_1, \ldots, x_n, x_{n+1}]$, and $f(a_1, \ldots, a_n, a_{n+1}) = 0$ for all $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{R}^{n+1}$. For any $\alpha \in \mathbb{R}$, define $g_\alpha(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, \alpha)$. Then $g_\alpha \in \mathbb{R}[x_1, \ldots, x_n]$ vanishes for all $(a_1, \ldots, a_n) \in \mathbb{R}^n$, so by the inductive hypothesis $g_\alpha = 0$. Since α was arbitrary, it follows that $f = 0$.

(2) (a) First notice that $0^2 = 0$ and $1^2 = 1$. Thus if either x or y is 0, so $x^2y + y^2x$ vanishes. The only remaining possibility is $x = y = 1$, but then we have $1 \cdot 1 + 1 \cdot 1 = 0$.

(b) $x^2yz + xyz^2$ vanishes at all points in $\mathbb{F}_2^3$. More generally, for $n \geq 2$,

$$(x_1 + x_n) \prod_{i=1}^{n} x_i \in \mathbb{F}_2[x_1, \ldots, x_n]$$

vanishes at all points in $\mathbb{F}_2^n$.

(3) First suppose that $f_1, \ldots, f_m \in I$, and let $g \in (f_1, \ldots, f_m)$. Then

$$g = \sum_{i=1}^{m} h_i f_i, \qquad \text{for some } h_i \in k[x_1, \ldots, x_n].$$

Since $f_i \in I$, so $h_i f_i \in I$, and hence $g \in I$. So $(f_1, \ldots, f_m) \subseteq I$.

Conversely, suppose that $(f_1, \ldots, f_m) \subseteq I$. Then $f_i \in (f_1, \ldots, f_m) \subseteq I$ for each $1 \leq i \leq m$ and we're done.

(4) $\mathbb{V}(x^n, y^m) = \{(a, b) \in k^2 \mid a^n = 0 \text{ and } b^m = 0\}$. But k is an integral domain, so $a^n = 0$ iff $a = 0$, and $b^m = 0$ iff $b = 0$. Hence $\mathbb{V}(x^n, y^m) = \{(0, 0)\} = \mathbb{V}(x, y)$, and so

$$\mathbb{I}(\mathbb{V}(x^n, y^m)) = \mathbb{I}(\mathbb{V}(x, y)) \supseteq (x, y).$$

Conversely, consider any $f \in \mathbb{I}(\mathbb{V}(x, y))$. Then $f(0, 0) = 0$, and so the constant term of f must be zero. Hence either $f = x^l g$ for some $l > 0$, $g \in k[x, y]$, in which case $f \in (x) \subset (x, y)$, or $f = y^{l'} g'$ for some $l' > 0$, $g' \in k[x, y]$, in which case $f \in (y) \subset (x, y)$. In either case $f \in (x, y)$, and so

$$\mathbb{I}(\mathbb{V}(x^n, y^m)) = \mathbb{I}(\mathbb{V}(x, y)) \subseteq (x, y).$$

(5) (a) $x^2 - x = x(x - 1)$. Clearly this vanishes at 0 and at 1. Similarly for $y^2 - y$. Hence $(x^2 - x, y^2 - y) \subseteq I$.

a.m.kasprzyk@imperial.ac.uk

http://magma.maths.usyd.edu.au/∼kasprzyk/.

(b) Let $f \in \mathbb{F}_2[x, y]$. We can write

$$f = \sum_{i \in S} p_i(x) y^i, \qquad \text{where } p_i \in \mathbb{F}_2[x] \text{ are non-zero.}$$

Applying the division algorithm to the p_i, we see

$$p_i = q_i(x^2 - x) + r_i$$

where $r_i = 0$ or $\deg r_i < \deg (x^2 - 2) = 2$. Hence

$$f = (x^2 - x) \sum_{i \in S} q_i(x) y^i + \sum_{i \in S} r_i(x) y^i.$$

Since each r_i is either 0 or $\deg r_i \leq 1$, we can write

$$\sum_{i \in S} r_i(x) y^i = g(y)x + h(y), \qquad \text{for some } g, h \in \mathbb{F}_2[y].$$

Hence

$$f = A(x, y)(x^2 - x) + g(y)x + h(y), \qquad \text{for some } A \in \mathbb{F}_2[x, y].$$

Now we apply the division algorithm to g and h:

$$\begin{aligned} g &= q_1(y^2 - y) + r_1, \text{ where } r_1 = 0 \text{ or } \deg r_1 < 2, \\ h &= q_2(y^2 - y) + r_2, \text{ where } r_2 = 0 \text{ or } \deg r_2 < 2. \end{aligned}$$

Finally, we see that

$$\begin{aligned} f &= A(x^2 - x) + B(y^2 - y) + r_1 x + r_2 \\ &= A(x^2 - x) + B(y^2 - y) + axy + bx + cy + d. \end{aligned}$$

(c) Consider $r(x, y) = axy + bx + cy + d$, and suppose that r vanishes at every point in $\mathbb{F}_2^2$. Then:

$$\begin{aligned} r(0,0) &= d && \Rightarrow d = 0 \\ r(0,1) &= c + d && \Rightarrow c = 0 \\ r(1,0) &= b + d && \Rightarrow b = 0 \\ r(1,1) &= a + b + c + d && \Rightarrow a = 0 \end{aligned}$$

Hence r is the zero polynomial.

(d) Let $f \in I$. Since $f \in \mathbb{F}_2[x, y]$ we can write

$$f = A(x^2 - x) + B(y^2 - y) + axy + bx + cy + d.$$

We have already seen that $x^2 - x, y^2 - y \in I$, hence

$$f - A(x^2 - x) - B(y^2 - y) = axy + bx + cy + d \in I.$$

Since this vanishes at every point in $\mathbb{F}_2^2$, by our previous result we have that $a = b = c = d = 0$. Hence $f = A(x^2 - x) + B(y^2 - y) \in (x^2 - x, y^2 - y)$. It follows that $I = (x^2 - x, y^2 - y)$.

(e) $x^2y + y^2x = y(x^2 - x) + x(y^2 - y)$ since $2xy = 0xy = 0$.

(6) Suppose that $(x, y) = (f)$ for some $f \in k[x, y]$. In particular, $f \mid x$ and so f is either a constant – which implies that $(f) = k[x, y]$ and so is impossible – or $f = cx$ for some $c \in k$. Similarly since $f \mid y$ we see that $f = dy$ for some $d \in k$. It follows that $c = d = 0$ and so $(f) = (0)$, a contradiction.

(7) We proceed by induction on m. When $m = 2$ the result is trivial. Let $h = \gcd\{f_2, \ldots, f_m\}$. Since $h \mid f_i$, $2 \leq i \leq m$, we have that $f_i \in (f_1, h)$ and so $(f_1, h) \supseteq (f_1, \ldots, f_m)$.

Conversely set $h' = \gcd\{f_3, \ldots, f_m\}$. By the inductive hypothesis, $(f_2, h') = (f_2, f_3, \ldots, f_m)$. Since $h = \gcd\{f_2, h'\}$, so $(h) = (f_2, h') = (f_2, \ldots, f_m)$. Now let $f \in (f_1, h)$. Then $f = k_1 f_1 + k_2 h$ for some $k_1, k_2 \in k[x]$. Then – since $(h) = (f_2, \ldots, f_m)$ – there exist $g_i \in k[x]$ such that $f = k_1 f_1 + k_2 g_2 f_2 + \ldots + k_2 g_m f_m$, and so $f \in (f_1, f_2, \ldots, f_m)$ and so $(f_1, h) \subseteq (f_1, \ldots, f_m)$. The result follows.

(8) Use a computer.

(9) Notice that 2 is a root of all three generators:

$$\begin{aligned}
x^3 + x^2 - 4x - 4 &= (x - 2)(x^2 + 3x + 2) \\
x^3 - x^2 - 4x + 4 &= (x - 2)(x^2 + x - 2) \\
x^3 - 2x^2 - x + 2 &= (x - 2)(x^2 - 1) = (x - 2)(x - 1)(x + 1).
\end{aligned}$$

Now 1 is a root of $x^2 + x - 2$ but not of $x^2 + 3x + 2$, and -1 is a root of $x^2 + 3x + 2$ but not of $x^2 + x - 2$. Hence

$$\gcd\{x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2\} = x^2 - 2$$

and so

$$(x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2) = (x - 2).$$

Finally, notice that $x^2 - 4 = (x - 2)(x + 2)$, hence $x^2 - 4 \in (x - 2)$.