Midterm Solutions

Math 412

Fall 2016

(1) $a \mid (b+c) \Rightarrow \exists k \in \mathbb{Z}$ s.t. $ak = b+c$

$\gcd(b,c) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ s.t. $1 = bu + cv$

since $ak = b+c$, $c = ak - b$

so $1 = bu + cv$

$= bu + (ak-b)v$

$= b(u-v) + ak$

hence $\gcd(a,b) = 1$

similarly, $\gcd(a,c) = 1$ QED

(2) Suppose $e^2 = e$. Then $e^2 - e = 0$

so $e(e-1) = 0$

since $e \neq 0$ & $e-1 \neq 0$ by assumption

we see that e is a zero-divisor. QED

(3)(a) A general element of S_d looks like $f = \sum_{k=0}^{\infty} a_{dk} x^{dk}$.

(i) let $f(x), g(x) \in S_d$. show $f - g \in S_d$.

Write $g = \sum_{k=0}^{\infty} b_{dk} x^{dk}$. Then $f - g = \sum_{k=0}^{\infty} (a_{dk} - b_{dk}) x^{dk} \in S_d$

(ii) let $f, g \in S_d$. Show $fg \in S_d$

$f \cdot g = \sum_{k=0}^{\infty} c_k x^k$ with $c_k = \sum_{\substack{0 \le i,j \le k \\ i+j=k}} a_i b_j$. If $d \nmid k$ & $i+j=k$ & $d \mid i$, then $d \nmid j$. Similarly if $d \mid j$ then $d \nmid i$.

hence $\forall\, 0 \le i, j \le k$ with $i+j=k$ at least one of a_i or b_j is 0, so $c_k = \sum_{\substack{0 \le i,j \le k \\ i+j=k}} a_i b_j = 0$. so $f \cdot g \in S_d$

(iii) $1 \in R[x]$ is $1 + 0x^1 + 0x^2 + \cdots$. Since $d \mid 0$, $\forall\, k$ with $d \nmid k$, the coeff of x^k in 1 is 0. Hence $1 \in S_d$. So $S_d \le R[x]$ QED

(3)(b) $S_2 = \{\sum_{k=0}^{\infty} a_{2k} x^{2k} \in R[x]\}$, $S_3 = \{\sum_{k=0}^{\infty} a_{3k} x^{3k} \in R[x]\}$

$x^2 \in S_2$, $x^3 \in S_3$ so $x^2, x^3 \in S$, but $x^2 + x^3 \notin S_2$ & $\notin S_3$

so $x^2 + x^3 \notin S$

so S is not closed under addition & hence S is <u>not</u> a subring of $R[x]$.

(Technically, if $R = 0$, the zero ring, then $S = R[x] = 0$, too, so in this case $S \in R[x]$)

(4)(a) The elements of S are exactly the matrices of the form $M = \begin{pmatrix} a & b \\ 3c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}$

Let $M' = \begin{pmatrix} a' & b' \\ 3c' & d' \end{pmatrix}$ $a', b', c', d' \in \mathbb{Z}$

(i) Show $M - M' \in S$: $M - M' = \begin{pmatrix} a-a' & b-b' \\ 3(c-c') & d-d' \end{pmatrix}$ so the $(2,1)$-entry is divisible by 3 & all entries are integers

so $M - M' \in S$ ✓

(ii) Show $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3\cdot 0 & 1 \end{pmatrix} \in S$ ✓

(iii) Show $M \cdot M' \in S$: $M \cdot M' = \begin{pmatrix} a & b \\ 3c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ 3c' & d' \end{pmatrix} = \begin{pmatrix} aa' + 3bc' & ab' + bd' \\ 3a'c + 3c'd & 3b'c + dd' \end{pmatrix}$ ($aa' + 3bc' \in \mathbb{Z}$, $ab' + bd' \in \mathbb{Z}$, $3b'c + dd' \in \mathbb{Z}$)

$3a'c + 3c'd = 3(a'c + c'd) \in 3\mathbb{Z}$

so $M \cdot M' \in S$ ✓

Since (i), (ii), (iii) hold, $S \leq M_2(\mathbb{Z})$ QED

(b) (i) $\varphi(I) = [1]$ so $1_S \mapsto 1_{\mathbb{Z}/3\mathbb{Z}}$ ✓

(ii) $\varphi(M + M') = d + d'$ ✓

$\varphi(M) + \varphi(M') = d + d'$

(iii) $\varphi(M \cdot M') = \varphi\begin{pmatrix} a & \\ & \end{pmatrix} = [3b'c + dd'] = [d \cdot d']$ ✓ (because $[3 \cdot b'c] = [0]$)

$\varphi(M) \cdot \varphi(M') = [d] \cdot [d'] = [d \cdot d']$

hence φ is a homomorphism QED

(5) $ax_1 \equiv b \pmod n$ & $ax_2 \equiv b \pmod n$ so $ax_1 - ax_2 \equiv 0 \pmod n$

$a(x_1 - x_2)$.

Thus, $\exists k \in \mathbb{Z}$ s.t. $a(x_1 - x_2) = nk$. For $g = \gcd(a, n)$, $\exists a', n' \in \mathbb{Z}$ s.t. $a = ga'$ & $n = gn'$

$$a'g(x_1 - x_2) = n'gk$$

so $a'(x_1 - x_2) \equiv 0 \pmod{n'}$

so $a'x_1 \equiv a'x_2 \pmod{n'}$

Since $a' = \frac{a}{g}$ & $n' = \frac{n}{g}$ & $g = \gcd(a, n)$

we have that $\gcd(a', n') = 1$.

Thus $\exists u \in \mathbb{Z}$ with $a'u \equiv 1 \pmod{n'}$

so $ua'x_1 = ua'x_2 \pmod{n'}$

($ua'x_1 = x_1$, $ua'x_2 = x_2$)

so $x_1 \equiv x_2 \pmod{\frac{n}{g}}$ QED

Alternatively from here: so $n' \mid a'(x_1 - x_2)$.

Since $\gcd(a', n') = 1$ (as above), $n' \mid (x_1 - x_2)$

so $x_1 \equiv x_2 \pmod{\frac{n}{g}}$ QED