MTH 4104 Example Sheet III Solutions Shu SASAKI

III-1. S is a ring but not a field. The additive identity is $0 = 0/1$ (recall $\gcd(0,1) = 1$). It is not a field because even though $2 = 2/1$ is an element of S, it has no multiplicative inverse. Indeed, the multiplicative inverse *has to be* $1/2$ but this is not an element of S.

On the other hand, T is not even a ring. In fact, it is not closed in addition. While $1/2$ is an element of T, $1/2 + 1/2 = 1$ is not. Since it is not a ring, it certainly is not a field (recall a field is a ring).

III-2. (a) $\mathbb{Q}$. (b) The set $\mathbb{Q}(\sqrt{2})$ of real numbers of the form $r + r_2\sqrt{2}$ where r and r_2 range over the field $\mathbb{Q}$ of rational numbers. (c) The set $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$ of real numbers of the form $r + r_2\sqrt{2} + r_3\sqrt{3} + r_6\sqrt{6}$ where r, r_2, r_3, r_6 range over $\mathbb{Q}$. The set $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is not closed under multiplication!

III-3. For example, to check (R+×), i.e. if a, b, c are complex numbers, then $(a+b)c = ac + ab$. For $* \in \{a, b, c\}$, let $* = \mathrm{Re}(*) + \mathrm{Im}(*)\sqrt{-1}$. Then

$$a(b+c) = (\mathrm{Re}(a) + \mathrm{Im}(a)\sqrt{-1})\left((\mathrm{Re}(b) + \mathrm{Re}(c)) + (\mathrm{Im}(b) + \mathrm{Im}(c))\sqrt{-1}\right)$$

equals, by the definition of $\times$ on $\mathbb{C}$,

$$[\mathrm{Re}(a)(\mathrm{Re}(b) + \mathrm{Re}(b)) - \mathrm{Im}(a)(\mathrm{Im}(b) + \mathrm{Im}(c))] + [\mathrm{Re}(a)(\mathrm{Im}(b) + \mathrm{Im}(c)) + \mathrm{Im}(a)(\mathrm{Re}(b) + \mathrm{Re}(c))]\sqrt{-1}.$$

On the other hand,

$$ab = (\mathrm{Re}(a) + \mathrm{Im}(a)\sqrt{-1})(\mathrm{Re}(b) + \mathrm{Im}(b)\sqrt{-1})$$

is

$$[(\mathrm{Re}(a)\mathrm{Re}(b) - \mathrm{Im}(a)\mathrm{Im}(b)] + [\mathrm{Re}(a)\mathrm{Im}(b) + \mathrm{Re}(b)\mathrm{Im}(a)]\sqrt{-1},$$

while

$$ac = (\mathrm{Re}(a) + \mathrm{Im}(a)\sqrt{-1})(\mathrm{Re}(c) + \mathrm{Im}(c)\sqrt{-1})$$

is

$$[(\mathrm{Re}(a)\mathrm{Re}(c) - \mathrm{Im}(a)\mathrm{Im}(c)] + [\mathrm{Re}(a)\mathrm{Im}(c) + \mathrm{Re}(c)\mathrm{Im}(a)]\sqrt{-1}.$$

Combining, $ab + ac$ is

$$[\mathrm{Re}(a)(\mathrm{Re}(b) + \mathrm{Re}(b)) - \mathrm{Im}(a)(\mathrm{Im}(b) + \mathrm{Im}(c))] + [\mathrm{Re}(a)(\mathrm{Im}(b) + \mathrm{Im}(c)) + \mathrm{Im}(a)(\mathrm{Re}(b) + \mathrm{Re}(c))]\sqrt{-1}$$

which is exactly what we get for $a(b+c)$.

The computation for (R+×) is similar.

III-4. It fails to satisfy (R×+). For example, let g and γ be the identity function (sending x to x), while f sends x to x^2. Then $f(g+\gamma)$ sends x to $(f(g+\gamma))(x) = f((g+\gamma)(x)) = f(g(x)+\gamma(x)) = f(x+x) = f(2x) = 4x^2$, while $fg + f\gamma$ sends x to $(fg + f\gamma)(x) = (fg)(x) + (f\gamma)(x) = f(g(x)) + f(\gamma(x)) = f(x) + f(x) = x^2 + x^2 = 2x^2$.

III-5. $R = \mathbb{Z}_4$. The element $[2]_4$ is non-zero and $[2]_4^2 = [2^2]_4 = [4]_4 = [0]_4$.

III-6. (a) Yes. $[4]$ is the multiplicative identity and $[4][4] = [16] = [4]$, $[4][2] = [2] = [2][4]$ and $[4][0] = [0] = [4][0]$. (b)R is a field.

III-7. By definition, $([a]+[b])+[c] = [a+b]+[c] = [a+b+c] = [a]+[b+c] = [a]+([b]+[c])$.

III-8. By definition, $a + (-a) = 0$. Multiplying b from left, the RHS becomes $0b = 0$ (see lecture notes), while the LHS becomes $(a + (-a))b \overset{(\mathrm{R}+\times)}{=} ab + (-a)b$. We therefore have $ab + (-a)b = 0$. Since ab is an element of R, it has additive inverse $-ab$. Adding this onto both side, we have $-ab+(ab+(-a)b) = -ab+0$. By (R+1), the LHS becomes $(-ab+ab)+(-a)b = 0 + (-a)b = (-a)b$ by (R+2), while the RHS becomes $-ab$. To put them together, we have $(-a)b = -ab$ as desired.

III-9. (a) $f + g = [4]X^2 + ([2] + [6])X + ([3] + [3]) = [4]X^2 + [6]$. (b) $fg = ([2][4])X^3 + ([3][4] + [2][6])X^2 + ([3][6] + [3][2])X + [3][3] = [8]X^2 + [24]X^2 + [24]X + [9] = [1]$.

III-10. (a) Let $f = c_m(f)X^m + c_{m-1}(f)X^{m-1} + \cdots c_1(f)X + c(f) \in R[X]$ and $g = c_n(g)X^n + c_{n-1}X^{n-1} + \cdots + c_1(g)X + c(g) \in R[X]$ and assume that $c_m(f)$ and $c_n(g)$ are non-zero, in which case $\deg(f) = m$ and $\deg(g) = n$. We see that

$$fg = c_m(f)c_n(g)X^{m+n} + (c_m(f)c_{n-1}(g) + c_{m-1}(f)c_n(g))X^{m+n-1} + \cdots .$$

We claim that $c_m(f)c_n(f)$ is non-zero (because F is assumed to be a field). If $c_m(f)c_n(g) = 0$, then multiplying both sides by $c_m(f)^{-1}$ (which exists in F since F is a field and $c_m(f)$ is a non-zero element of F) we get $c_m(f)^{-1}c_m(f)c_n(g) = c_m(f)^{-1}0$, i.e. $c_n(g) = 0$. This contradicts the assumption that $c_n(g)$ is non-zero. Therefore, $c_m(f)c_n(g)$ is non-zero. Granted, $\deg(fg) = \deg(f)+\deg(g)$. (b) If (and only when) $\deg(f)$ is distinct from $\deg(g)$, then $\deg(f+g) = \max(\deg(f), \deg(g))$ holds. Otherwise, there is nothing conclusive we can say about $\deg(f+g)$. (c) $\deg(fg) = \deg(f)+\deg(g)$ no longer holds if the coefficients are defined only over a ring. For example, $[2]X+[1]$ and $[3]X+[1]$ are both degree 1 polynomials in $\mathbb{Z}_6$, but their product is $([2][3])X^2+([2]+[3])X+[1] = [5]X+[1]$ of degree 1.

III-10. See the typed-up lecture notes.

III-11. For example, let $R = \mathbb{Z}_4$ and define f to be the one that sends x to $[1]_4$ if $x = [0]_4$ and to $[0]_4$ otherwise.