1) Congruences:

(a) Find all $x \in \mathbb{Z}$ such that

$$4x \equiv 10 \pmod{30}.$$

If there is no such x, simply justify why.

Solution. We have that $(4, 30) = 2 \mid 10$ and hence there are solutions and they are the solutions of

$$2x \equiv 5 \pmod{15}$$

Since $1 = 8 \cdot 2 + (-1) \cdot 15$, we multiply by 8, getting

$$x \equiv 8 \cdot 5 = 40 \equiv 10 \pmod{15}.$$

So, the solutions are $x = 10 + 15k$ for $k \in \mathbb{Z}$. □

(b) Find all $x \in \mathbb{Z}$ satisfying [simultaneously]:

$$\begin{aligned} x &\equiv 2 \pmod{7}, \\ x &\equiv 3 \pmod{11}. \end{aligned}$$

If there is no such x, simply justify why.

Solution. Since $(7, 11) = 1$, there are solutions. The first equation gives us that $x = 2 + 7k$, for $k \in \mathbb{Z}$. Substituting in the second equation we get

$$7k \equiv 1 \pmod{11}.$$

Since $1 = (-3) \cdot 7 + 2 \cdot 11$, we multiply by -3 and get

$$k \equiv -3 \equiv 8 \pmod{11}.$$

So, $k = 8 + 11l$ for $l \in \mathbb{Z}$ and therefore $x = 2 + 7 \cdot (8 + 11l) = 58 + 77l$ for $l \in \mathbb{Z}$. □

2) Let R be a *non-commutative* ring and $a \in R$ such that there are $b, c \in R$ such that $ba = 1$ and $ac = 1$. Prove that $b = c$. *Justify each step!*

Proof. [This was done in the Errata 1.] We have

$$\begin{aligned} b &= b \cdot 1 && \text{[property of 1]} \\ &= b \cdot (ac) && \text{[assumption that } ac = 1\text{]} \\ &= (ba) \cdot c && \text{[associativity]} \\ &= 1 \cdot c && \text{[assumption that } ba = 1\text{]} \\ &= c && \text{[property of 1]} \end{aligned}$$

□

3) Examples:

(a) [10 points] Give an example of an *infinite field* F such that $6 \cdot a = 0$ for all $a \in F$. [**Hint:** Can you find a finite example first?]

Solution. Note that $\mathbb{I}_6$ or $\mathbb{I}_6[x]$ do not work, since $\mathbb{I}_6$ is not a domain. But, in $\mathbb{F}_2 = \mathbb{I}_2$, we have that $2 \cdot a = 0$ for all $a \in \mathbb{F}_2$, and hence $6a = 3 \cdot (2a) = 3 \cdot 0 = 0$ for all $a \in \mathbb{F}_2$. [F_3 would also work.] But, $\mathbb{F}_2$ is finite. To make it infinite, we could take $\mathbb{F}_2[x]$. [Note that in there also every element multiplied by 2 is zero, since it makes all coefficients zero.] But it is not a field. So, we could take $\mathbb{F}_2(x)$ [the field of rational functions with coefficients in $\mathbb{F}_2$]. Since $\mathbb{F}_2[x] \subseteq \mathbb{F}_2(x)$, it is clearly infinite.

[Another example would be $\mathbb{F}_3(x)$.] □

(b) [10 points] Give an example of a ring R that contains $\mathbb{C}[x]$ as a *proper* subring [i.e., $\mathbb{C}[x] \subseteq R$, $\mathbb{C}[x]$ a subring of R, but $\mathbb{C}[x] \neq R$].

Solution. One example [and probably the simplest] would be $(\mathbb{C}[x])[y] = \mathbb{C}[x, y]$ [ring of polynomial in two variables, x and y].

Other examples would be $\mathbb{C}(x)$ or $\mathbb{C}[[x]]$ [the ring of power series], although the latter I've only mentioned it briefly. □

4) Prove that

$$R = \{f \in \mathbb{Z}[x] \ : \ f = a + x^2 f_1 \text{ for some } a \in \mathbb{Z} \text{ and } f_1 \in \mathbb{Z}[x]\}$$

is a domain.

Proof. Since $\mathbb{Z}$ is a domain, we have that $\mathbb{Z}[x]$ is a domain. So, it suffices to show that R is a subring of $\mathbb{Z}[x]$ [as subrings of domains are automatically domains].

Since $1 = 1 + x^2 \cdot 0$, and $1 \in \mathbb{Z}$ and $0 \in \mathbb{Z}[x]$, we have that $1 \in R$.

Let now $f, g \in R$. Then, there are $a, b \in \mathbb{Z}$ and $f_1, g_1 \in \mathbb{Z}[x]$ such that $f = a + x^2 \cdot f_1$ and $g = b + x^2 \cdot g_1$.

Then, $f - g = (a - b) + x^2(f_1 - f_2)$. Since $(a - b) \in \mathbb{Z}$ and $(f_1 - f_2) \in \mathbb{Z}[x]$, we have that $(f - g) \in R$.

Also,

$$\begin{aligned} f \cdot g &= (a + x^2 f_1)(b + x^2 g_1) \\ &= ab + x^2(ag_1) + x^2(bf_1) + x^4 f_1 g_1 \\ &= ab + x^2(bf_1 + ag_1 + x^2 f_1 g_1). \end{aligned}$$

Since $ab \in \mathbb{Z}$ and $(bf_1 + ag_1 + x^2 f_1 g_1) \in \mathbb{Z}[x]$, we have that $f \cdot g \in R$.

Hence, R is a subring of $\mathbb{Z}[x]$ and thus a domain.

□

5) Let R be a commutative ring [but not necessarily a domain] and let $f, g \in R[x] \setminus \{0\}$, with $\deg(f) = \deg(g)$ and $f \mid g$.

(a) Prove that if R is a domain, then there is $a \in R$ such that $g = a \cdot f$.

Proof. Since $f \mid g$, there is $h \in R[x]$ such that $g = f \cdot h$ [by definition of "divides"]. Since R is a domain, we then have that

$$\deg(g) = \deg(f \cdot h) = \deg(f) + \deg(h) = \deg(g) + \deg(h).$$

So, $\deg(h) = 0$ and hence $h = a \in R \setminus \{0\}$ and $g = a \cdot f$.

□

(b) Prove that in $\mathbb{I}_6[x]$, if $f = \bar{2}x + \bar{1}$ and $g = \bar{5}x + \bar{1}$, then $f \mid g$. [So, the statement does not hold for non-domains, as clearly g is not a multiple of f].

Proof. We have that

$$(\bar{2}x + \bar{1})(\bar{3}x + \bar{1}) = \bar{6}x^2 + \bar{5}x + \bar{1} = \bar{5}x + \bar{1}.$$

Hence, $g = f \cdot (\bar{3}x + \bar{1})$, and so $f \mid g$. □