1) [25 points] Let $f = x^5 + x^4 + x^2 + 2x + 1$ and $g = x^4 + 2x$ in $\mathbb{F}_3[x]$. Find $\gcd(f, g)$ and express is as a linear combination of f and g.

Solution. We have:

$$f = g \cdot (x+1) + (2x^2+1),$$

$$g = (2x^2+1) \cdot (2x^2+2) + (2x+1),$$

$$(2x^2+1) = (2x+1) \cdot (x+1) + 0.$$

So, the GCD is the "monic version" of $2x+1$, i.e., $2(2x+1) = x+2$.
Now:

$$\begin{aligned} 2x+1 &= g - (2x^2+1) \cdot (2x^2+2) \\ &= g - [f - g \cdot (x+1)](2x^2+2) \\ &= -(2x^2+2) \cdot f + (1 + (x+1)(2x^2+2)) \cdot g. \end{aligned}$$

Hence:

$$\begin{aligned} x+2 &= 2 \cdot (2x+1) \\ &= 2\left[-(2x^2+2) \cdot f + (1 + (x+1)(2x^2+2)) \cdot g\right] \\ &= -2 \cdot (2x^2+2) \cdot f + 2 \cdot (1 + (x+1)(2x^2+2)) \cdot g. \end{aligned}$$

□

2) [25 points] Let R be a domain. Prove that $f \in R[x]$ is a unit [of $R[x]$] if and only if f is a unit of R [i.e., f is a constant polynomial and this constant is a unit of the ring R].
[**Note:** This was a HW problem.]

Proof. If $f = a \in U(R)$, then there is $b \in R$ such that $ab = 1$. Since $a, b \in R[x]$ and 1 of R is the one of $R[x]$, we have that a is a unit of $R[x]$.
Conversely, if $f \in U(R[x])$, then there is $g \in R[x]$ such that $f \cdot g = 1$. Then, since R is a domain, $\deg(f) + \deg(g) = \deg(f \cdot g) = \deg(1) = 0$. Clearly neither f nor g is zero, as otherwise $f \cdot g = 0 \neq 1$. So, we have $\deg(f), \deg(g) \geq 0$ and since they add up to 0, both have to be 0, i.e., both are in R. Since they multiply to 1, the are in $U(R)$. $\square$

3) [25 points] Prove that if R is a domain, then $R[x]$ is also a domain. [You can assume that $R[x]$ is already a commutative ring, as polynomial rings always are (under the assumption R is commutative).]
[**Note:** This was done in class.]

Proof. Suppose that $f \neq 0$ is a zero divisor. Then, there is $g \in R[x]$, with $g \neq 0$, such that $f \cdot g = 0$. So, as $f, g \neq 0$, we have $\deg(f), \deg(g) \geq 0$.
But, since R is a domain, we have $\deg(f \cdot g) = \deg(f) + \deg(g)$, and thus $-\infty = \deg(0) = \deg(f \cdot g) = \deg(f) + \deg(g) \geq 0$, a contradiction. □

4) [25 points] Let F be a field and $f, g \in F[x]$ such that $f \cdot g = a \cdot x^n$, for some $a \in F$, $a \neq 0$, and $n \in \mathbb{Z}_{>0}$. Prove that $f = b \cdot x^r$, $g = c \cdot x^s$ such that $bc = a$ and $r + s = n$.
[**Hint:** Section 3.6.]

Proof. Note that $f \cdot g = a \cdot x^n$ is the factorization of $f \cdot g$ into irreducibles [since x is irreducible].
So, since $f \mid f \cdot g = ax^n$, by the proposition from class, $f = b \cdot x^r$, for some $r \in \{0, 1, \ldots, n\}$ and $b \neq 0$. Similarly, $g = c \cdot x^s$ for some $s \in \{0, 1, \ldots, n\}$ and $c \neq 0$.
Now, since F is a field [and hence a domain], we have that $n = \deg(f \cdot g) = \deg(f) + \deg(g) = r + s$. Also, since

$$a \cdot x^n = (b \cdot x^r) \cdot (cx^s) = (b \cdot c) \cdot x^{r+s} = (b \cdot c) \cdot x^n,$$

we have $a = b \cdot c$. □