1) Let

$$f = 3x^5 + 4x^4 + x^3 + x^2 + 3x + 2,$$
$$g = 4x^3 + 2,$$

be polynomials in $\mathbb{F}_5[x]$. Find $\gcd(f, g)$.

[**Note:** There is *no need* to express the GCD as linear combination of f and g.]

Solution. With long divisions, we get:

$$f = g \cdot (2x^2 + x + 4) + (2x^2 + x + 4)$$
$$g = (2x^2 + x + 4) \cdot (2x + 4) + (3x + 1)$$
$$(2x^2 + x + 4) = (3x + 1) \cdot (4x + 4) + 0.$$

Hence, $\gcd(f, g)$ is the *monic associate* of $3x + 1$, i.e., $\gcd(f, g) = 2 \cdot (3x + 1) = x + 2$. □

2) Let R be a commutative ring. Prove that $R[x]$ is a domain if and only if R is a domain.

[**Note:** This was done in class.]

Proof. [⇐] Suppose that R is a domain and $f, g \in R[x] \setminus \{0\}$ with $f \cdot g = 0$. Since R is a domain, taking degrees we have:

$$-\infty = \deg(0) = \deg(f \cdot g) = \deg(f) + \deg(g).$$

Since $\deg(f), \deg(g) \in \mathbb{Z}_{\geq 0} \cup \{-\infty\}$, we must have that either $\deg(f) = -\infty$ or $\deg(g) = -\infty$, i.e., either $f = 0$ or $g = 0$, a contradiction.

Hence, $R[x]$ has no non-zero zero divisor, and hence $R[x]$ is a domain.

[⇒] Suppose that R is not a domain. Then, there are $a, b \in R \setminus \{0\}$ such that $a \cdot b = 0$. Since also $a, b \in R[x] \setminus \{0\}$, we have that a [and b] are non-zero zero divisors of $R[x]$, and hence $R[x]$ is also not a domain. □

3) Let F be a field, $f \in F[x]$, and $a_1, a_2, \ldots, a_k \in F$ be distinct roots of f, i.e., $f(a_i) = 0$ for $i = 1, 2, \ldots, k$. Prove that there is $g \in F[x]$ such that

$$f = g \cdot (x - a_1)(x - a_2) \cdots (x - a_k).$$

[**Hint:** We have proved the case when $k = 1$ in class and you *can* use that.]

Proof. We prove it by induction on k.

The case $k = 1$ was done in class.

Now, suppose that the statement is true for $k - 1$ roots, and assume $\{a_1, \ldots, a_k\}$ are roots. Then, by the induction hypothesis we have that there is $g \in F[x]$ such that

$$f = g \cdot (x - a_1) \cdots (x - a_{k-1}).$$

Hence,

$$0 = f(a_k) = g(a_k) \cdot (a_k - a_1) \cdots (a_k - a_{k-1}).$$

Since F is a field [and hence a domain] and all factors on the left of the equation above as in F, we must have that at least one of them is 0. But since $a_1, \ldots, a_k$ are *distinct*, we have that $(a_k - a_1), \ldots (a_k - a_{k-1}) \neq 0$. Thus $g(a_k) = 0$. By the induction hypothesis again, we have that there exists $h \in F[x]$ such that $g = h \cdot (x - a_k)$. Together with the factorization of f above, we obtain:

$$f = h \cdot (x - a_k) \cdot (x - a_1) \cdots (x - a_{k-1}) = h \cdot (x - a_1) \cdots (x - a_k).$$

□

4) Let R be a commutative ring, $a \in R$, $f \in R[x]$, and suppose that $(x-a) \mid f$. Prove that $(x-a)^2 \mid f$ if and only if $(x-a) \mid f'$ [where f' is the derivative of f].

[**Note:** This was a HW problem. You can use the formulas for the derivative from Calculus and the *Basic Lemma* for polynomial rings.]

Proof. Since $(x-a) \mid f(x)$, we can write $f(x) = (x-a)g(x)$ for some $g(x) \in R[x]$. Then, $f'(x) = g(x) + (x-a)g'(x)$. So, if $(x-a) \mid f'(x)$, then $(x-a) \mid g(x)$ by the Basic Lemma. Now, since $(x-a) \mid g(x)$, we have that $g(x) = (x-a)h(x)$ for some $h(x) \in R[x]$, and so $f(x) = (x-a)g(x) = (x-a)^2 h(x)$, i.e., $(x-a)^2 \mid f(x)$.

Suppose now that $(x-a)^2 \mid f(x)$. Thus, we can write $f(x) = (x-a)^2 h(x)$ for some $h(x) \in R[x]$. Then, [using the product rule] we have $f'(x) = 2(x-a)h(x) + (x-a)^2 g'(x) = (x-a)(2h(x) + (x-a)g'(x))$, and $(x-a) \mid f'(x)$. $\square$