1) [20 points] If u is a unit in a *commutative* ring, prove that it's inverse is unique: if $ua = 1$ and $ub = 1$, then $a = b$. *Justify every step with an axiom! (Don't skip steps!)* [The axioms are listed in the last page.]

Proof. We have:

$$\begin{aligned}
ua = 1 &\implies (ua)b = 1 \cdot b && \text{[multiply by } b\text{]} \\
&\implies u(ab) = b && \text{[axioms 6 and 7]} \\
&\implies u(ba) = b && \text{[axiom 5]} \\
&\implies (ub)a = b && \text{[axioms 6]} \\
&\implies 1 \cdot a = b && \text{[by hypothesis]} \\
&\implies a = b && \text{[axioms 7].}
\end{aligned}$$

□

2) Prove or disprove [i.e., if the statement is true, prove it, if not, show why the statement is false].

(a) [15 points] $R = \{f \in \mathbb{Z}[x] \mid f \text{ is monic}\}$ is a domain.

Solution. It's *not* a domain, or even a ring, as it is not closed under addition: $x \in R$ [as it's monic], but $x + x = 2x$ is not [as it is not monic].

[Alternatively, not that R does not have 0 in it, since 0 is not monic. But note that 1 *is* a monic polynomial!] □

(b) [15 points] $R = \{a + x^2 f \mid a \in \mathbb{Z} \text{ and } f \in \mathbb{Z}[x]\}$ is a domain.

Proof. It suffices to prove that it is a subring of $\mathbb{Z}[x]$. Since $\mathbb{Z}$ is a domain, we have that $\mathbb{Z}[x]$ is a domain, and since subrings of domains are domains, we get that a subring of $\mathbb{Z}[x]$ is also a domain.

We have that $1 \in R$ as $1 = 1 + x^2 \cdot 0$ [with $1 \in \mathbb{Z}$ and $0 \in \mathbb{Z}[x]$].

Let now $f, g \in R$. Then, $f = a + x^2 f_1$ and $g = b + x^2 g_1$ for some $a, b \in \mathbb{Z}$ and $f_1, g_1 \in \mathbb{Z}[x]$. Then $f - g = (a - b) + x^2(f_1 - g_1)$. Since $a - b \in \mathbb{Z}$ and $f_1 - g_1 \in \mathbb{Z}[x]$, we have that $f - g \in R$.

Also, $f \cdot g = (a + x^2 f_1)(b + x^2 g_1) = ab + ax^2 g_1 + bx^2 f_1 + x^4 f_1 g_1 = ab + x^2(ag_1 + bf_1 + x^2 f_1 g_1)$. Since $ab \in \mathbb{Z}$ and $(ag_1 + bf_1 + x^2 f_1 g_1) \in \mathbb{Z}[x]$, we have that $f \cdot g \in R$. $\square$

3) Examples of rings (no justifications needed):

(a) [15 points] Give an example of a infinite, *non-commutative* ring R such that $2 \cdot a = 0$ for all $a \in R$.

Solution. $M_2(\mathbb{F}_2(x))$ [2×2 matrices with entries in $\mathbb{F}_2(x)$]. $\square$

(b) [15 points] Give an example of a ring R that is not a field, but *contains* an *infinite* field and such that $25 \cdot a = 0$ for all $a \in R$.

Solution. $\mathbb{F}_5(x)[y]$ [polynomials in y with coefficients in $\mathbb{F}_5(x)$]. $\square$

4) [20 points] Prove that if $f = x^p - x \in \mathbb{F}_p[x]$, then $f(a) = 0$ for all $a \in \mathbb{F}_p$.
[**Hint:** $f = x(x^{p-1} - 1)$. Also, of course, you need facts about congruences modulo p.]

Proof. By *Fermat's Little Theorem*, for all $a \in \mathbb{Z}$ we have that $a^p \equiv a \pmod{p}$. So, for all $a \in \mathbb{F}_p$, we have that $f(a) = a^p - a = a - a = 0$. $\square$

Commutative Ring Axioms: A [non-empty] set with two operations, $+$ and $\cdot$, is a commutative ring if:

0. For all $a, b \in R$ we have that $a + b \in R$ and $a \cdot b \in R$.

1. For all $a, b \in R$ we have that $a + b = b + a$.

2. For all $a, b, c \in R$ we have that $(a + b) + c = a + (b + c)$.

3. There exists $0 \in R$ such that for all $a \in R$ we have $a + 0 = a$.

4. For all $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$.

5. For all $a, b \in R$ we have that $a \cdot b = b \cdot a$.

6. For all $a, b, c \in R$ we have that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

7. There is $1 \in R$ such that for all $a \in R$ we have that $1 \cdot a = a$

8. For all $a, b, c \in R$ we have that $a \cdot (b + c) = a \cdot b + a \cdot c$