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

Proof. We have:

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

□

2) Let R be a commutative ring and $U(R)$ be the set of units of a ring, i.e.,

$$U(R) = \{a \in R \ : \ \exists b \in R \text{ such that } ab = 1\}.$$

[We denote this b, such that $ab = 1$, by a^{-1}.]
[**Hint:** To show $x \in U(R)$ we need to find $y \in R$ such that $xy = 1$.]

(a) [15 points] Show that if $x \in U(R)$, then $x^{-1} \in U(R)$.

Proof. We have that $x \cdot x^{-1} = 1$, so, since R is commutative, we have that $x^{-1} \cdot x = 1$ [and $x \in R$]. Hence, by definition, we have that $x^{-1} \in U(R)$. □

(b) [15 points] Show that if $x, y \in U(R)$, then $xy \in U(R)$.

Proof. Since $x, y \in U(R)$, there $x^{-1}, y^{-1} \in R$ such that $xx^{-1} = 1$, $yy^{-1} = 1$. Also, since R is a ring $x^{-1} \cdot y^{-1} \in R$. Then,

$$(xy) \cdot (x^{-1}y^{-1}) = (xx^{-1})(yy^{-1}) = 1 \cdot 1 = 1.$$

So, $xy \in U(R)$. □

3) [20 points] Let F be a field and suppose that $\mathbb{F}_3$ is a subfield of F. Prove that the prime field of F is $\mathbb{F}_3$. [I proved this in class (in more generality), but you can't use it here, of course. It's a very simple proof though!]

Proof. Let E be the prime field of F. So, by its minimality, we have that $E \subseteq \mathbb{F}_3$.
On the other hand, since E is a subfield, we have that $1_F \in E$. Since $\mathbb{F}_3$ is a subfield of F, we have that $1_F = 1_{\mathbb{F}_3} = [1]$, and hence $[1] \in E$.
Now, since E is a field, it's closed under addition, and hence $[1] + [1] = [2] \in E$ and $[2] + [1] = [3] = [0] \in E$. So, $\mathbb{F}_3 = \{[0], [1], [2]\} \subseteq E$.
Therefore, $E = \mathbb{F}_3$. $\square$

4) Let R be a ring with $\mathbb{F}_2 = \{[0],[1]\}$ [also denoted $\mathbb{I}_2$ or $\mathbb{Z}/2\mathbb{Z}$] as a subring, and having exactly four elements, say $R = \{[0],[1],a,b\}$. [So, no two among $[0]$, $[1]$, a, and b are equal! Hence, $a \neq b$, $a \neq [1]$, $b \neq [0]$, etc.]

(a) [15 points] Prove that since R contains $\mathbb{F}_2$, we have that $2x = 0$ [or $x + x = 0$] for all $x \in R$. [**Hint:** Use the ring axioms [and the fact that $\mathbb{F}_2$ is a subring, of course]. The axioms are given in the last page.]

Proof. First observe that since $\mathbb{F}_2$ is a subring of R, we have $1_R = 1_{\mathbb{F}_2} = [1]$, and $0_R = 0_{\mathbb{F}_2} = [0]$.

We have:

$$\begin{aligned} 2x &= x + x \\ &= x \cdot (1_R + 1_R) \\ &= x \cdot ([1] + [1]) \\ &= x \cdot [0] \\ &= x \cdot 0_R \\ &= 0_R. \end{aligned}$$

□

(b) [15 points] Prove that $a + [1] = b$. [**Hint:** Prove that $a + [1] \neq [0]$, $a + [1] \neq [1]$, and $a + [1] \neq a$.]

Proof. Since R is a ring, it's closed under addition. Then, $a + [1] \in R$. So, we have that $a + [1]$ is either $[0]$, $[1]$, a or b.

If $a + [1] = [0]$, then, adding $[1]$ we get $a = [1]$, a contradiction.

If $a + [1] = [1]$, then, adding $[1]$ we get $a = [0]$, a contradiction.

If $a + [1] = a$, then $a + [1] = a + [0]$, and by the additive cancellation law [i.e., adding $-a$ to both sides], we have $[1] = [0]$, a contradiction.

So, the only possibility is that $a + [1] = b$. □

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 $a \cdot (b + c) = a \cdot b + a \cdot c$