1) [25 points] Let K be a field and $F \subseteq K$. Suppose that F is also a field with the *same addition and product* as K. [We are *not* assuming that $1_k = 1_F$, so, in principle, F might now be a subfield of K.]

(a) Show that $1_F \neq 0_K$. [**Hint:** Remember that since F is a field, $1_F \neq 0_F$.]

Proof. We have that $1_F \cdot 0_F = 0_F$. If $1_F = 0_K$, then $1_F \cdot 0_F = 0_K \cdot 0_F = 0_K = 1_F$ [as any element of K when multiplied by 0_K yield 0_K]. Since $0_F \neq 1_F$, this cannot happen [as we'd have $1_F = 0_F \cdot 1_F = 0_F$].

[Alternatively, one can show that $0_K = 0_F$ and hence $1_F \neq 0_F = 0_K$. This is true as $0_K + 1_F = 1_F = 0_F + 1_F$ and hence we can subtract 1_F [in K] to obtain $0_K = 0_F$.]

□

(b) Show that $1_F = 1_K$. [**Hint:** By part (a), 1_F is invertible in K, and so if $1_F \cdot a = 1_F \cdot b$, for any $a, b \in K$ [or F], we have that $a = b$.]

Proof. We now have $1_F \cdot 1_F = 1_F = 1_F \cdot 1_K$. So, as in the hint $1_F = 1_K$. □

2) [25 points] Let R be a [not necessarily commutative] ring [with one] such that $a^2 = a$ for all $a \in R$.

(a) Show that $1_R = -1_R$. [**Hint:** Consider $(1_R + 1_R)^2$.]

Proof. On the one hand we have that $(1_R + 1_R)^2 = 1_R + 1_R$, by hypothesis. On the other hand, we have $(1_R + 1_R)^2 = (1_R + 1_R)(1_R + 1_R) = 1_R + 1_R + 1_R + 1_R$. Thus, $1_R + 1_R + 1_R + 1_R = 1_R + 1_R$. Subtracting 1_R three times in this equation, we obtain that $1_R = -1_R$.

[Alternatively, we have: $(-1_F)^2 = (-1_F)(-1_F) = 1_F$, where the last equality we have seen in class [$-1_F \cdot a = -a$ and $-(-a) = a$], and since $a^2 = a$, we also have $(-1_F)^2 = -1_F$. Thus, $-1_F = (-1_F)^2 = 1_F$.]

□

(b) Show that R is commutative. [**Hint:** By (a), it suffices to show that for all $a, b \in R$, we have $ab + ba = 0$. Consider $(a + b)^2$, and remember we cannot assume that R is commutative!]

Proof. Let $a, b \in R$. [We need to show $ab = ba$. Since R might not be commutative, we must write $(a + b)^2 = a^2 + ab + ba + b^2$, and by hypothesis, this gives us $(a + b)^2 = a + ab + ba + b$. On the other hand, $(a + b)^2 = a + b$, by hypothesis. Hence, we have $a + b = a + ab + ba + b$, and subtracting $a + b$ from both sides, we obtain $ab + ba = 0$, i.e., $ab = -ba$. Since $1_R = -1_R$, we have $ab = -ba = -1_R \cdot ba = 1_R \cdot ba = ba$, and R must be commutative.

□

3) [25 points] Let p be a prime with $p \geq 3$, and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ [or $\mathbb{F}_p = \mathbb{I}_p$, as in the book]. [Remember that $\mathbb{F}_p$ is a *field*!] Let $U = \mathbb{F}_p^\times$ be the set of units of $\mathbb{F}_p$.

(a) Show that the only elements of $a \in \mathbb{F}_p^\times$ such that $a = a^{-1}$ are $\overline{1}$ and $\overline{p-1}$. [**Hint:** If $a^{-1} = a$, then $a^2 = \overline{1}$. Then, what are all the roots of the polynomial $x^2 - \overline{1}$ in $\mathbb{F}_p$?]

Proof. Since $\mathbb{F}_p$ is a field, we have that $x^2 - \overline{1}$ has at most two roots. But $x = \overline{1}$ and $x = \overline{p-1}$ are roots, and hence *all* the roots. [Note that since $p \neq 2$, $\overline{1}$ and $\overline{p-1}$ are different!] So, these are the only elements that are inverse of themselves.

□

(b) Use (a) to show that $(p-1)! \equiv -1 \pmod{p}$. [**Hint:** That is the same as to say that $\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{p-1}$.]

Proof. In $\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdots \overline{p-1}$, each of the terms distinct from $\overline{1}$ and $\overline{p-1}$ can be paired up with another [different] term yielding $\overline{1}$, i.e., you can pair it with its inverse. [E.g., for $p = 7$, we have $\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} = \overline{1} \cdot (\overline{2} \cdot \overline{4}) \cdot (\overline{3} \cdot \overline{5}) \cdot \overline{6} = \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{6} = \overline{6}$.] So, what is left is $\overline{1}$ and $\overline{p-1}$. Therefore $\overline{(p-1)!} = \overline{1} \cdot \overline{p-1} = \overline{-1}$, and hence $(p-1)! \equiv -1 \pmod{p}$. □

4) [25 points] Let R be an *integral domain*, and suppose that there is some $n \in \mathbb{Z} \setminus \{0\}$ such that $n \cdot 1_R = 0_R$. [Note that n can be negative.]

(a) Show that there exists some prime p such that $p \cdot 1_R = 0_R$. [**Hint:** We have that if $a, b \in \mathbb{Z}$, then $(a \cdot b) \cdot 1_R = (a \cdot 1_R) \cdot (b \cdot 1_R)$. Then, use the *Fundamental Theorem of Arithmetic* and the fact that R is a domain.]

Proof. Suppose that $n \cdot 1_R = 0_R$. Then, if $n < 0$, we have that $0_R = -0_R = -(n \cdot 1_R) = (-n) \cdot 1_R$. Thus, we may assume that $n > 0$. Since $1_R \neq 0_R$, we must have that $n > 1$.

Now, by the *Fundamental Theorem of Arithmetic*, we have that $n = p_1 \cdots p_k$, where the p_i's a prime. Hence, $n \cdot 1_R = (p_1 \cdots p_k) \cdot 1_R = (p_1 \cdot 1_R) \cdots (p_k \cdot 1_R) = 0_R$. Then, since R is a domain, we have that $(p_i \cdot 1_R) = 0_R$ for some i.

□

(b) Show that the prime in (a) is unique. [**Hint:** If $p \neq q$, both primes, then $\gcd(p, q) = 1$. You can use *Bezout's Theorem* [i.e., the *Extended Euclidean Algorithm*]. Also, remember that $1_R \neq 0_R$.]

Proof. Suppose that p, q are distinct primes such that $p \cdot 1_R = q \cdot 1_R = 0_R$. Since $\gcd(p, q) = 1$, there are $r, s \in \mathbb{Z}$ such that $1 = rp + sq$. Then, $1_R = 1 \cdot 1_R = (rp + sq) \cdot 1_R = r(p \cdot 1_R) + s(q \cdot 1_R) = r \cdot 0_R + s \cdot 0_R = 0_R + 0_R = 0_R$. But, in a ring we must have $1_R \neq 0_R$. □