Exercise 13.3. *Show that a commutative ring with cancellation has no zero-divisors.*

Proof. Let R a commutative ring with cancellation. For any element $a\ b \in R$ such that $ab = 0$, if both a and b are zero, then trivial. Suppose $a \neq 0$, then $ab = a0$ implies $b = 0$. □

Exercise 13.5. *Show that every non-zero element in Z_n is either zero-divisor or unit.*

Proof. For any non-zero element $k \in Z_n$, let $d = \gcd(k, n)$.

- If $d \neq 1$, then there is q such that $kq = \operatorname{lcm}(k, n)$, therefore k is a zero-divisor.
- If $d = 1$, then $k \in U(n)$, therefore k is a unit.

□

Exercise 13.7. *Let R be a **finite** commutative ring with unity. Prove that every non-zero element in R is either a zero-divisor or a unit.*

Proof. For any non-zero element $a \in R$, consider the mapping $f(b) = ab : R \to R$. If f is onto, then there is $a^{-1} \in R$ such that $f(a^{-1}) = aa^{-1} = 1$. If f is not onto, then f is not one-to-one (since R is finite), therefore there are distinct b and c such that $f(b) = ab = ac = f(c)$. Then $a(b - c) = 0$ where $b - c \neq 0$, therefore a is a zero-divisor. □

Exercise 13.20. *Show that Z_n has a non-zero nilpotent element iff n is divisible by square of some prime.*

Proof. Newline please!!

- ($\Rightarrow$) Let a be non-zero nilpotent element, therefore $a^2 = 0$. We know n divides a^2 (since $a^2 \cdot 1 = 0$), that is, $nz = a^2$. Let $d = \gcd(a, n)$, then $dx = a$ and $dy = n$ for some $x\ y \in \mathbb{N}$. Then $dyz = d^2x^2 \to yz = dx^2$, note that x is coprime to y since they are come from gcd and z is integer, we know y divides d, that is, $d = yk$. Therefore $dy = y^2k = n$, for any prime factor p of y, p^2 divides n.
- ($\Leftarrow$) Since n is divisible by square of some prime, then $n = p^2q$ where p is prime. Then $(pq)^2 = p^2q^2 = nq$.

□

Exercise 13.34. *Let R be a finite integral domain, then $|R| = p^k$ where p is prime.*

Proof. If p and q divide $|R|$ where p and q are distinct prime, then there are a $b \in R$ such that $|a| = p$ and $|b| = q$. Now, $(q \cdot a)(p \cdot b) = (pq) \cdot (ab) = (p \cdot a)(q \cdot b) = 0$. Note that $q \cdot a$ and $p \cdot b$ are non-zero, since p and q are distinct prime, therefore a is a zero divisor and R is no longer a integral domain. □

Exercise 13.35. *Let F be a field of order p^n where p is prime. Prove that* $\operatorname{char} F = p$.

Proof. Since F is an Abelian group under addition, then there is $a \in F$ such that $|a| = p$, that is, $p \cdot a = 0$. Then $(p \cdot a)a^{-1} = p \cdot (aa^{-1}) = p \cdot 1 = 0$. For any $1 < q < p$, $q \cdot 1 \neq 0$, cause it implies that q divides p, which is unacceptible. Therefore $|1| = p$, and then $\operatorname{char} F = p$. □

Exercise 13.47. *Let R be a commutative ring without zero-divisors. Show that all the non-zero elements of R have the same order under addition.*

Proof. If R has no non-zero element of finite order, then trivial. Now, let $a \in R$ a non-zero element of minimum order, say, $|a| = n$. Then for any non-zero element $b \in R$, we have $(n \cdot a)b = a(n \cdot b) = 0b = 0$. Since a is non-zero, therefore $n \cdot b = 0$, and n is the minimum, so $|b| = n$. □

Exercise 13.48. *Suppose that R is a commutative ring without zero-divisors. Show that* $\operatorname{char} R$ *is* 0 *or some prime.*

Proof. Newline please!!

- If $R = 0$, TODO!
- Let $a \in R$ a non-zero element, by Exercise 13.47, if $|a| = \infty$, then $\operatorname{char} R = 0$. So we suppose $|a| = n$, then all non-zero element of R have order n. If n is not prime and is divisible by some prime p, then $n = pq$, and $(p \cdot a)(q \cdot a) = (pq) \cdot a^2 = n \cdot a^2 = 0$. Note that $p \cdot a$ and $q \cdot a$ are non-zero since $p < |a|$ and $q < |a|$. Therefore, $\operatorname{char} R$ has to be some prime.

□

Exercise 13.64. *Let F a finite field with n element. Prove that $x^{n-1} = 1$ for all non-zero $x \in F$.*

Proof. Since F is a field, all elements except 0 forms a group under multiplication, say, F^*, then $|F^*| = n - 1$. Therefore for any non-zero element in F (which is also in F^*), $x^{n-1} = 1$. $\square$