1. Let $F_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. How many elements are there in $F_2^2$, i.e. how many functions are there from $F_2$ to $F_2$? Show that every function from $F_2$ to $F_2$ is of the form $E(f)$ for a unique polynomial $f$ of the form $ax + b$ (i.e. either $\deg f \leq 1$ or $f = 0$).

2. (i) Let $R$ be a ring. Show that, if $r$ and $s$ are not divisors of zero, then $rs$ is not a divisor of zero. In particular, if $r$ is not a divisor of zero, then $r^n$ is not a divisor of zero for every $n > 0$.

(ii) Show that, if $R$ is a finite ring, then every element of $R$ is either a zero divisor or a unit. In particular, the set of divisors of zero in $\mathbb{Z}/n\mathbb{Z}$ is $\mathbb{Z}/n\mathbb{Z} - (\mathbb{Z}/n\mathbb{Z})^*$.

3. Let $X$ be a set and let $R$ be a ring. Show that, if $X$ has at least two elements, then $R^X$ is not an integral domain.

4. Recall that an element $r$ of a ring $R$ is nilpotent if there exists a positive integer $N$ such that $r^N = 0$. (The possibility that $r = 0$, i.e. that $N = 1$, is allowed.)

(a) What are all of the nilpotent elements in $\mathbb{Z}/6\mathbb{Z}$? In $\mathbb{Z}/8\mathbb{Z}$? In $\mathbb{Z}/24\mathbb{Z}$? Describe more generally all of the nilpotent elements in $\mathbb{Z}/n\mathbb{Z}$.

(b) Show that, if $r$ is nilpotent and $s \in R$, then $sr$ is nilpotent.

(c) Show that, if $r, s \in R$ and $r$ and $s$ are both nilpotent, then $r + s$ is also nilpotent (i.e. the sum of two nilpotent elements is again nilpotent. (Use the binomial theorem.) (Note: this does not necessarily hold in a non-commutative ring, for example, in $M_2(\mathbb{R})$ both $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent, but their sum is invertible.) Is it true that the set of all nilpotent elements of $R$ is a subring of $R$?

(d) Show that, if $r$ is nilpotent, then $1 + r$ is a unit. (Hint: geometric series, and first show that $1 - r$ is a unit.) More generally, if $u$ is a unit in $R$ and $r$ is nilpotent, then $u + r$ is a unit.

(e) If $r$ is a nilpotent element of $R$, then the polynomial $1 + rx$ is a unit in $R[x]$. Hence, if $R$ is not an integral domain, then it is possible for $(R[x])^*$ to be larger than $R^*$.
5. Let $p$ be a prime number.

(a) If $k$ is an integer with $1 \leq k \leq p - 1$, show that $p$ divides the binomial coefficient $\binom{p}{k}$.

(b) Let $R$ be an integral domain of characteristic $p$, or more generally a ring such that $p \cdot r = 0$ for all $r \in R$. Show that, for all $r, s \in R$, $(r + s)^p = r^p + s^p$. (Use the binomial theorem and part (a).)

(c) If $R$ is a ring such that $p \cdot r = 0$ for all $r \in R$, show that the function $F : R \to R$ defined by $F(r) = r^p$ is a (ring) homomorphism (the Frobenius homomorphism). If $R$ is an integral domain, show that $F$ is injective.

(d) Let $R = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Show that $F(1) = 1$ and conclude that $F : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the identity. (This gives another proof of Fermat’s Little Theorem, a standard number theory fact proved in Modern Algebra I.)

(e) Let $R = (\mathbb{Z}/p\mathbb{Z})[x] = \mathbb{F}_p[x]$. What is $F(\sum a_i x^i)$? Show that $F : R \to R$ is injective but not surjective and describe the image of $F$.

The Frobenius homomorphism is very important in the study of finite fields, and it will reappear later on in the course.

6. Let $a, b, c \in \mathbb{Q}$, not all zero. We would like to show that $\mathbb{Q}(\sqrt[3]{2})$ is a field by rationalizing the denominator in an expression of the form $\frac{1}{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2}$. Show that this can be done by multiplying by

$$1 = \frac{(a^2 - 2bc) + (-ab + 2c^2)\sqrt[3]{2} + (b^2 - ac)(\sqrt[3]{2})^2}{(a^2 - 2bc) + (-ab + 2c^2)\sqrt[3]{2} + (b^2 - ac)(\sqrt[3]{2})^2},$$

by checking that

$$(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2)((a^2 - 2bc) + (-ab + 2c^2)\sqrt[3]{2} + (b^2 - ac)(\sqrt[3]{2})^2))$$

is the rational number $a^3 + 2b^3 + 4c^3 - 6abc$, which is nonzero if not all of $a, b, c$ are zero (you do not need to prove that this expression is nonzero). We will see a few different ways to explain how to find this rationalizing factor over the course of the semester.