EXAMPLE: The following are rings.

(1) Rings of numbers, like $\mathbb{Z}$ and $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$.

(2) Given a starting ring A, the polynomial ring in one indeterminate
$$A[X] := \{a_d X^d + \cdots + a_1 X + a_0 \mid d \geq 0, a_i \in A\},$$
or in a (finite or infinite![1]) set of indeterminates $A[X_1, \ldots, X_n]$, $A[X_\lambda \mid \lambda \in \Lambda]$.

(3) Given a starting ring A, the power series ring in one indeterminate
$$A[\![X]\!] := \left\{ \sum_{i \geq 0} a_i X^i \mid a_i \in A \right\},$$
or in a set of indeterminates $A[\![X_1, \ldots, X_n]\!]$.

(4) For a set X, $\mathrm{Fun}(X, \mathbb{R}) := \{\text{all functions } f : [0,1] \to \mathbb{R}\}$ with pointwise $+$ and $\times$.

(5) $\mathcal{C}([0,1]) := \{\text{continuous functions } f : [0,1] \to \mathbb{R}\}$ with pointwise $+$ and $\times$.

(6) $\mathcal{C}^\infty([0,1]) := \{\text{infinitely differentiable functions } f : [0,1] \to \mathbb{R}\}$ with pointwise $+$ and $\times$.

($\div$) Quotient rings: given a starting ring A and an ideal I, $R = A/I$.

($\times$) Product rings: given rings R and S, $R \times S = \{(r, s) \mid r \in R, s \in S\}$.

DEFINITION: An element x in a ring R is called a

- **unit** if x has an **inverse** $y \in R$ (i.e., $xy = 1$).
- **zerodivisor** if there is some $y \neq 0$ in R such that $xy = 0$.
- **nilpotent** if there is some $e \geq 0$ such that $x^e = 0$.
- **idempotent** if $x^2 = x$.

We also use the terms **nonunit, nonzerodivisor, nonnilpotent, nonidempotent** for the negations of the above. We say that a ring is **reduced** if it has no nonzero nilpotents.

(1) Warmup with units, zerodivisors, nilpotents, and idempotents.

(a) What are the implications between nilpotent, nonunit, and zerodivisor?

(b) What are the implications between reduced, field, and domain?

(c) What two elements of a ring are always idempotents? We call an idempotent **nontrivial** to mean that it is neither of these.

(d) If e is an idempotent, show that $e' := 1 - e$ is an idempotent[2] and $ee' = 0$.

(a) nilpotent $\Rightarrow$ zerodivisor $\Rightarrow$ nonunit

(b) reduced $\Leftarrow$ domain $\Leftarrow$ field

(c) 0 and 1

(d) $e'^2 = (1-e)(1-e) = 1 - 2e + e^2 = 1 - e = e'$ and $ee' = e(1-e) = e - e^2 = 0$.

(2) Elements in polynomial rings: Let $R = A[X_1, \ldots, X_n]$ a polynomial ring over a *domain* A.

(a) If $n = 1$, and $f, g \in R = A[X]$, briefly explain why the top degree[3] of fg equals the top degree of f plus the top degree of g. What if A is not a domain?

[1] Note: Even if the index set is infinite, by definition the elements of $A[X_\lambda \mid \lambda \in \Lambda]$ are finite sums of monomials (with coefficients in A) that each involve finitely many variables.

[2] We call e' the **complementary idempotent** to e.

[3] The **top degree** of $f = \sum a_i X^i$ is $\max\{k \mid a_k \neq 0\}$; we say **top coefficient** for a_k. We use the term top degree instead of degree for reasons that will come up later.

(b) Again if $n = 1$, briefly explain why $R = A[X]$ is a domain, and identify all of the units in R.
(c) Now for general n, show that R is a domain, and identify all of the units in R.

> **(a)** If $f = a_m X_m +$ lower terms and $g = b_n X_n +$ lower terms , then $fg = \sum a_m b_n X^{m+n} +$ lower terms. If A is a domain, then $a_m, b_n \neq 0$ implies $a_m b_n \neq 0$, but if A is not a domain, the top degree may drop.
> **(b)** By looking at the top degree terms as above, we see that the product of nonzero polynomials is nonzero. The units in R are just the units in A viewed as polynomials with no higher degree terms. Indeed, such elements are definitely units; on the other hand, if $fg = 1$ in R, then the top degree of f and g are both zero, so f and g are constant, which means f and g are in A, so a unit in R is a unit in A.
> (c) The claim that R is a domain follows by induction on n, since $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$. The units in R are again the units in A. This also follows by induction on n: a unit in $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$ is a unit in $A[X_1, \ldots, X_{n-1}]$, which by the induction hypothesis is constant.

(3) Elements in power series rings: Let A be a ring.
(a) Explain why the set of formal sums $\{\sum_{i \in \mathbb{Z}} a_i X_i \mid a_i \in A\}$ with arbitrary positive and negative exponents is *not* clearly a ring in the same way as $A[\![X]\!]$.
(b) Given series $f, g \in A[\![X]\!]$, how much of f, g do you need to know to compute the X^3-coefficient of $f + g$? What about the X^3-coefficient of fg?
(c) Find the first three coefficients for the inverse[4] of $f = 1 + 3X + 7X^2 + \cdots$ in $\mathbb{R}[\![X]\!]$.
(d) Does "top degree" make sense in $A[\![X]\!]$? What about "bottom degree"?
(e) Explain why[5] for a domain A, the power series ring $A[\![X_1, \ldots, X_n]\!]$ is also a domain.
(f) Show[6] that $f \in A[\![X_1, \ldots, X_n]\!]$ is a unit if and only if the constant term of f is a unit.

> **(a)** To multiply two such formal sums, you would have to take an infinite sum in A to compute the coefficient of any X^i.
> **(b)** To compute the X^3-coefficient of $f + g$, you just need to know the X^3-coefficients of f and g. To compute the X^3-coefficient of fg, you need to know the $1, X, X^2, X^3$ coefficients of f and g.
> **(c)** $g = 1 - 3X + 2X^2 + \cdots$.
> **(d)** No; yes.
> **(e)** For $n = 1$, look at the bottom degree terms. The bottom degree term of the product is the product of the bottom degree terms; if A is a domain, this product is nonzero. The statement just follows by induction on n.
> **(f)** If f is a unit, then the constant term is a unit, since the constant term of fg is the constant term of f times that of g.
> For the other direction, first, take $n = 1$. Given $f = \sum_i a_i X^i$, construct $g = \sum_i b_i X^i$ by defining b_m recursively $b_0 = 1/a_0$ and that the X^m-coefficient of $(\sum_{i=0}^m a_i X^i)(\sum_{i=0}^m b_i X_i)$ is 0 for $m > 0$: we can do this since, given $b_0, \ldots, b_m$ that work in the mth step, in the next step we can the formula for the X^{m+1} coefficient is $a_0 b_{m+1} + a_1 b_m + \cdots + a_{m+1} b_0$, since a_0 is a unit, we can solve for b_{m+1} to make this equal

[4] It doesn't matter what the $\cdots$ are!
[5] You might want to start with the case $n = 1$.
[6] Hint: For $n = 1$, given $f = \sum_i a_i X^i$, construct $g = \sum_i b_i X^i$ by defining b_m recursively $b_0 = 1/a_0$ and that the X^m-coefficient of $(\sum_{i=0}^m a_i X^i)(\sum_{i=0}^m b_i X_i)$ is 0 for $m > 0$.

zero without changing the lower coefficients. Continuing this way, take $g = \sum_i b_i X^i$. Then for any k, the X^k-coefficient only depends on the $a_0, \ldots, a_k$ and $b_0, \ldots, b_k$ coefficients, and by construction, this coefficient is zero for $k \geq 1$. Thus, any such f has an inverse.
The general claim follows by induction on n: if $f \in A[\![X_1, \ldots, X_n]\!]$ has a unit constant term considered as a power series in $A[\![X_1, \ldots, X_n]\!]$, then its constant term in $(A[\![X_1, \ldots, X_{n-1}]\!])[\![X_n]\!]$ has a unit constant term, hence is a unit in $A[\![X_1, \ldots, X_{n-1}]\!]$, so f is a unit in $(A[\![X_1, \ldots, X_{n-1}]\!])[\![X_n]\!] = A[\![X_1, \ldots, X_n]\!]$.

(4) Elements in function rings.
  (a) For $R = \mathrm{Fun}([0,1], \mathbb{R})$,
    (i) What are the nilpotents in R?
    (ii) What are the units in R?
    (iii) What are the idempotents in R?
    (iv) What are the zerodivisors in R?
  (b) For $R = \mathcal{C}([0,1], \mathbb{R})$, $R = \mathcal{C}^\infty([0,1], \mathbb{R})$ same questions as above. When are there any/none?

(a) For $R = \mathrm{Fun}([0,1], \mathbb{R})$,
  (i) There are no nilpotents, since for any $\alpha \in [0,1]$, $f(\alpha)^n = 0$ means that $f(\alpha) = 0$.
  (ii) The units are the functions that are never zero, since the function $g(x) = 1/f(x)$ is then defined (and conversely).
  (iii) $f(x)$ is idempotent if $f(\alpha) \in \{0,1\}$ for all $\alpha \in [0,1]$.
  (iv) Any function that is zero at some point is a zerodivisor: if $S = \{\alpha \in [0,1] \mid f(\alpha) = 0\}$ is nonempty, then let g be a nonzero function that vanishes on $[0,1] \smallsetminus S$, then $fg = 0$.
(b) For $R = \mathcal{C}([0,1])$ or $R = \mathcal{C}^\infty([0,1])$,
  (i) Same
  (ii) Same
  (iii) There are no nontrivial idempotents: the same condition as above applies, but by continuity, f must either be identically 0 or identically 1.
  (iv) The difference is that now there may not be a nonzero function that vanishes on $[0,1] \smallsetminus S$, e.g., if f vanishes at a single point. To be a zerodivisor, the set $[0,1] \smallsetminus S$ as above must be not be dense.

(5) Product rings and idempotents.
  (a) Let R and S be rings, and $T = R \times S$. Show that $(1,0)$ and $(0,1)$ are nontrivial complementary idempotents in T.
  (b) Let T be a ring, and $e \in T$ a nontrivial idempotent, with $e' = 1 - e$. Explain why $Te = \{te \mid t \in T\}$ and Te' are rings with the same addition and multiplication as T. Why didn't I say "subring"?
  (c) Let T be a ring, and $e \in T$ a nontrivial idempotent, with $e' = 1 - e$. Show that $T \cong Te \times Te'$. Conclude that R has nontrivial idempotents if and only if R decomposes as a product.

(a) $(1,0)^2 = (1,0)$, $(0,1)^2 = (0,1)$, and $(1,0) + (0,1) = (1,1)$ is the "1" of $R \times S$.
(b) $re + se = (r+s)e$ and $(re)(se) = rse^2 = rse$. Same with e'.
(c) Define $\phi : T \to Te \times Te'$ by $\phi(t) = (te, te')$. The verification that this is a ring homomorphism essentially the content of (b). If $\phi(t) = (0,0)$, then $te = 0$ and $0 = te' = t(1-e) = t - te$, so $t = 0$, hence ϕ is injective. Given $(re, se') \in Te \times Te'$, we have $\phi(re + se') = ((re+se')e, (re+se')e') = (re, se')$, hence ϕ is surjective, as well.

(6) Elements in quotient rings:
   (a) Let K be a field, and $R = K[X,Y]/(X^2, XY)$. Find
      - a nonzero nilpotent in R
      - a zerodivisor in R that is not a nilpotent
      - a unit in R that is not equivalent to a constant polynomial
   (b) Find $n \in \mathbb{Z}$ such that
      - $[4] \in \mathbb{Z}/(n)$ is a unit
      - $[4] \in \mathbb{Z}/(n)$ is a nonzero nilpotent
      - $[4] \in \mathbb{Z}/(n)$ is a nonnilp. zerodivisor
      - $[4] \in \mathbb{Z}/(n)$ is a nontrivial idempotent

This solution is embargoed.

(7) More about elements.
   (a) Prove that a nilpotent plus a unit is always a unit.
   (b) Let A be an arbitrary ring, and $R = A[X]$. Characterize, in terms of their coefficients, which elements of R are units, and which elements are nilpotents.
   (c) Let A be an arbitrary ring, and $R = A[\![X]\!]$. Characterize, in terms of their coefficients, which elements of R are nilpotents.