- Rings
  - Basic properties:
    - Additive and multiplicative closure (if $a, b \in R$, then $ab, a + b \in R$).
    - Additive and multiplicative associativity (if $a, b, c \in R$, then $(ab)c = a(bc)$ and $(a + b) + c = a + (b + c)$).
    - Additive commutativity (if $a, b \in R$, then $a + b = b + a$).
    - Additive identity (there is an element $0 \in R$ such that if $a \in R$, then $a + 0 = a$).
    - Additive inverses (if $a \in R$, then there is an element $(-a) \in R$ such that $a+(-a) = 0$).
    - Left and right distributivity (if $a, b, c \in R$, then $(a+b)c = ac+bc$ and $a(b+c) = ab+ac$.
  - Subrings need only be tested for *closure* and *additive inverses*; all other properties are inherited from the superring.
  - Common additional properties:
    - A *commutative ring* has multiplicative commutativity (if $a, b \in R$, then $ab = ba$).
    - A *ring with identity* or *ring with unity* has multiplicative identity (there is an element $1 \in R$ such that if $a \in R$, then $1a = a1 = a$).
  - Any element of a ring with a multiplicative inverse is called a *unit*.
  - The *characteristic* of a ring is the least positive integer n such that $na = 0$ for every $a \in R$, or 0 if no such n exists.
- Integral domains
  - Basic properties:
    - Are commutative rings with identity.
    - For $a, b \in D$, $ab = 0$ if and only if $a = 0$ or $b = 0$.
  - Notable results:
    - Cancellation property: if $ab = ac$ in an integral domain and $a \neq 0$, then $b = c$.
    - Any subring of an integral domain is an integral domain.
    - Every finite integral domain is a field.
    - Integral domains have prime or zero characteristic.
- Ideals
  - A subring I of a ring R with the *absorption* property: if $r \in R$ and $a \in I$ then $ar, ra \in I$.
  - We almost always are working in commutative rings, so that the distinction between ar and ra above is irrelevant.
  - Ideals need only be tested for *closure*, *absorption*, and *additive inverses*; all other properties are inherited from the ring.
  - "Ideals are to rings as normal subgroups are to groups."
  - They induce *quotient rings*: R/I is the set $\{r + I : r \in R\}$ of *additive cosets* of I.
  - Principal ideals: $\langle a \rangle = \{ra : r \in R\}$.
  - Prime ideals

    - ∗ A proper ideal I of a ring R is prime if for $a, b \in R$, $ab \in I$ implies that either $a \in I$ or $b \in I$.
    - ∗ I is prime iff R/I is an integral domain.
  - Maximal ideals
    - ∗ A proper ideal I of a ring R is maximal if there is no ideal J of R such that $I \subsetneq J \subsetneq R$.
    - ∗ Every maximal ideal is prime.
    - ∗ I is maximal iff R/I is a field.

- Ring homomorphisms
  - $\varphi : R \to R'$ is a *ring homomorphism* if $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$.
  - Highly analogous to group homomorphisms.
    - ∗ Kernels are ideals of R.
    - ∗ Every ideal is a kernel of some homomorphism.
    - ∗ First isomorphism theorem: $R/\ker\varphi \cong \varphi(R)$.

- Polynomial rings
  - For a commutative ring R, $R[x]$ is the ring of polynomials with coefficients in R.
  - If D is an integral domain, then $D[x]$ is an integral domain.
  - If F is a field, then there is a division algorithm in $F[x]$.
  - If F is a field, then $F[x]$ is a principal ideal domain.

- Special elements of integral domains
  - p is an *irreducible* element of D if $p = ab$ implies that either a or b is a unit.
  - p is a *prime* element of D if $p \mid ab$ implies that either $p \mid a$ or $p \mid b$.
  - Every prime is irreducible.
  - If D is a principal ideal domain, every irreducible is prime.
  - If $p(x)$ is an irreducible element of $D[x]$, we may also say $p(x)$ is *irreducible over* D.

- Special types of integral domains
  - A *principal ideal domain (PID)* is an integral domain where every ideal $I = \langle a \rangle$ for some a.
  - A *unique factorization domain (UFD)* is an integral domain where every nonzero element uniquely (up to order and multiplication by units) factors into irreducibles.
  - A *Noetherian domain* is an integral domain where every strictly increasing chain of ideals is finite in length.
  - A *Euclidean domain* is an integral domain with a "degree" function mapping its elements to the natural numbers such that there is a division algorithm where the degree of the remainder is less than the degree of the divisor.
  - Notable connections:
    - ∗ Every PID is a UFD.

    - Every Euclidean domain is a PID, and thus a UFD.
    - Every PID is Noetherian.
    - Every Noetherian ring has factorization (possibly non-unique) into irreducibles.
    - $\mathbb{Z}[x]$ is a UFD even though it is not a PID.

- Fields
  - Commutative rings with identity and such that *every nonzero element* has a multiplicative inverse.
  - Are integral domains.
  - Contain only two ideals: $\{0\}$ and the whole ring.
  - Are trivially PIDs, UFDs, and Euclidean domains.
  - $F[x]$ is also a PID, UFD, and Euclidean domain.

- Vector spaces
  - A *vector space* V over a field F is an algebra with addition among elements of V (called *vectors*, and multiplication of elements of V by elements of F, called *scalars*.
    - V is an Abelian group under addition.
    - For $a \in R$ and $u, v \in V$, $a(u+v) = au + av$.
    - For $a, b \in R$ and $u \in V$, $(a+b)u = au + bu$, and $a(bu) = (ab)u$.
    - For $u \in V$, $1u = u$.
  - A set of vectors is *linearly independent* if for any finite subset $\{v_1, \ldots, v_n\}$, the sum $c_1v_1 + c_2v_2 + c_3v_3 + \cdots + c_nv_n$ for scalars c_i equals zero only if every c_i is zero.
  - A set of vectors *spans* V if for any $w \in V$, there is a finite subset $\{v_1, \ldots, v_n\}$ and choice of scalars $c_1, \ldots, c_n$ such that $c_1v_1 + c_2v_2 + c_3v_3 + \cdots + c_nv_n = w$.
  - A set which both spans V and is linearly independent is a *basis of* V.
  - If V has a finite basis, every basis has the same size, called the *dimension* of V.

- Field extensions
  - A field extension of F is a field which contains F as a subfield.
  - If a polynomial in $F[x]$ is a product of linear factors from $E[x]$, we say that it *splits* in E. Alternatively, if all of its roots are in E, it splits in E.
  - If $f(x) \in F[x]$ splits in E with zeroes $a_1, \ldots, a_n$, then the field $F(a_1, a_2, \ldots, a_n)$ is called the *splitting field* of $f(x)$ over F
  - The splitting field of a polynomial is the minimal field extension which splits it.
  - Every polynomial has a splitting field, and the splitting field is unique up to isomorphism.
  - If $f(x)$ is irreducible over F, and a and b are elements of a field extension such that $f(a) = f(b) = 0$, then $F(a) \cong F(b)$.
  - Multiplicity of zeroes:
    - An irreducible polynomial has the same multiplicity at each of its zeroes.

* An irreducible polynomial $f(x)$ in $F[x]$ either has multiplicity 1 at every zero, or can be rewritten in the form $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$, where p is the characteristic of F.
* A *perfect field* is a field F with either characteristic 0 or one with characteristic p in which for every $a \in F$, there is a $b \in F$ such that $b^p = a$.
* An irreducible polynomial $f(x)$ in $F[x]$ either has multiplicity 1 at every zero if F is perfect.
* Every finite field is perfect.