Chaper 11: Rings

11.1: Definition of a Ring

- **Ring**: A *ring* R is a set with two laws of composition $+$ and $\times$, called addition and multiplication, that satisfy these axioms:
  (a) With the law of composition $+$, R is an abelian group that we denote by R^+; its identity is denoted by 0.
  (b) Multiplication is commutative and associative, and has an identity denoted by 1.
  (c) *Distributive law*: For all a, b and c in R, $(a+b)c = ac + bc$.
  - **Subring**: Subset which is closed under addition, subtraction, multiplication and which contains 1.
  - **Noncommutative Ring**: Satisfies al of the above axioms, except for the commutative law for multiplication.
- **Gauss integers**: The complex numbers of the form $a + bi$ where a and b are integers form a subring of $\mathbb{C}$ that we denote by $\mathbb{Z}[\mathrm{i}] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Its elements are points of a square lattice in the complex plane.
  - $\mathbb{Z}[\alpha]$ **subring**: Ccontains every complex number $\beta = a_n\alpha^n + ... + a_1\alpha + a_0$ where a_i are in $\mathbb{Z}$ and α is a complex number.
    * Analogous to the ring of Gauss integers.
    * Subring generated by α
    * Usually not represented as a lattice in the complex plane
- A complex number α is **algebraic** if it is a root of a (nonzero) polynomial with integer coefficients (i.e. if some expression of the form $a_n\alpha^n + ... + a_1\alpha + a_0$ evaluates to 0)
  - When α is algebraic there will be many polynomial expressions that represent the same complex number.
- If there is no polynomial with integer coefficients having α as a root, α is **transcendental**
  - When α is transcendental, two distinct polynomial expressions represent distinct complex numbers, and the elements of the ring $\mathbb{Z}[\alpha]$ correspond bijectively to polynomials $p(x)$ with integer coefficients.
- A polynomial in x with coefficients in a ring R is an expression of the form $a_nx^n + ... + a_1x + a_0$ with a_i in R.
- **Zero Ring**: A ring containing only the element 0.

  - A ring R in which the elements 1 and 0 are equal is the zero ring.
- **Unit**: A *unit* of a ring is an element that has a multiplicative inverse (if it exists, it is unique)
  - Units in the ring of integers are 1 and -1
  - Units in the ring of Gauss integers are ± 1 and $\pm$i
  - Units in the ring $\mathbb{R}[x]$ of real polynomials are the nonzero constant polynomials
  - The identity element 1 of a ring is always a unit

11.2: Polynomial Rings

- **Formal Polynomial**: A polynomial with coefficients in a ring R is a (finite) linear combination of powers of the variable: $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ where the coefficients a_i are elements of R.