Commutative Algebra

* Rings and homomorphisms

- - A commutative ring is a set, in which one can add and substract. A multiplication exists but is not in general invertable.
  - An additive identity 0 exists, and a multiplicative identity 1 exists.
  - The distribution law $a(b+c) = ab + ac$ is assumed, and the multiplication is commutative $ab = ba$.
- Examples of rings: the set of all integers, the set of all complex numbers, the set of all square diagonal matrices of a fixed size, the set of polynomials, etc.
- Given two rings A and B, we require that the map obeys the ring structure of the rings $f : A \to B$ is a homomorphism if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$
  - The image of a homomorphism f is the subset of B written as $f(A)$ defined by $\{f(a) \mid a \in A\}$.
  - The kernel of a homomorphism f is the subset of A written as $\ker f$ defined by $\{a \in A \mid f(a) = 0\}$.
  - An endomorphism is a map from a ring into itself. An isomorphism is a map between two rings with a unique inverse. An automorphism is an isomorphism that is an endomorphism.

* Ideals and modules

- The kernel I of a map f between rings $R \to S$ has the following property:

$$\forall r \in R, \forall x \in I : rx \in I$$

When a subset I of a ring R is closed under the multiplication and addition, and satisfies the above property, we call I to be an ideal of R.

Note I : An ideal is the kernel of a ring homomorphism.

Note II : The map $R \to R/I$ is called canonical map or quotient map.

- Example : Consider a polynomial ring $\mathbb{Q}[x]$, the set of polynomials of finitely many terms in x with coefficients in the rational numbers.

Suppose x must equal to $\frac{1}{2}$. In other words, we decide that $x-\frac{1}{2}$ must be "zero" in $\mathbb{Q}[x]/I$. We can define $I = \{f(x)(x-\frac{1}{2}) \mid f(x) \in \mathbb{Q}[x]\}$ as our ideal.

Computing in $\mathbb{Q}[x]/I$ is the same as computing in $\mathbb{Q}[x]$ and evaluate the polynomial at $x=\frac{1}{2}$.

- In general, if we write an ideal I of R as (a,b,c), then we mean

$$I = \{ax + by + cz \mid x, y, z \in R\}.$$

I is said to be generated by a, b, c.

* Prime, maximal

A prime ideal p of R is an ideal not equal to (1) such that

$$ab \in p \text{ implies } a \in p \text{ or } b \in p \text{ for any } a, b \in R$$

- In $\mathbb{Z}$ the zero ideal is prime.
- In $\mathbb{Q}[x]$ the zero ideal is prime.
- If any nonzero elements of a nonzero ring R has a multiplicative inverse, in which case R is called a $\boxed{\text{field}}$
- The ring in which (0) is prime has a special name, (integral) domain. And it's easy to verify R/p is an integral domain.
- Let $f: A \to B$ be a map between two rings. If $p \subseteq B$ is a prime ideal, then $I = f^{-1}(p) \subseteq A$ is prime.

* Modules

Let M be an abelian group with a bilinear operation $\cdot$ such that

$$\forall r \in R, \forall m \in M : r \cdot m \in M.$$

We call M an R-module or a module over R.

- An ideal is a subset of R such that it is a module over R.
- R itself is R-module and $R \oplus R$ is also R-module.

For R-module M if there exist finitely many elements $m_1, \cdots m_n \in M$ such that

$$M = \{r_1 m_1 + \cdots + r_n m_n \mid r_1 \cdots r_n \in R\},$$

then we say M is finitely generated.

- Suppose we are given a ring map $A \to B$. We say B is a finitely generated A-algebra if there exists finitely many elements $b_1 \cdots b_n \in B$ such that any element of b can be written as a polynomial in $b_1 \cdots b_n$ with coefficients in the image of A. In this case, B is sometimes written as $B = A[b_1, \cdots, b_n]$.
- Given two modules M and N over R, we define an R-linear map or R-module homomorphism $f: M \to N$ to satisfy

  $f(m+m') = f(m) + f(m')$ and $f(r \cdot m) = r f(m)$ for any $r \in R, m, m' \in M$

* Free

- An R-module isomorphic to $\oplus_\alpha R$ is called a free module.
- An un-redundant set of generators of a free module is called a basis. The cardinality of basis is called rank.
- Only free modules can we speak of bases.