# Commutative Algebra Cheat Sheet

## Rings

A **ring** $A$ is a set with two binary operations addition and multiplication such that

- $A$ is an abelian group with addition.
- Multiplication is associative and distributive over addition.

Additionally we consider rings with commutativity and existence of multiplicative identity 1.
A function $\varphi : A \to B$ between rings is a **homomorphism** if it preserves addition multiplication and sends 1 to 1.
A **subring** is a subset of a ring that is also a ring with the induced relations.

## Universal mapping property

A universal property is some notion of a construction that uniquely determines it. In particular for some functor $F$ between categories $\mathbf{C}, \mathbf{D}$ an arrow $X \to F$ for $X \in \mathbf{D}$ is said to be universal if there exists some arrow $u$ and $C \in \mathbf{C}$ such that all other arrows $X \to F(C')$ necessarily factor through $u : X \to F(C)$ uniquely.
This will be very useful in characterizing certain constructions later.
For example in the first isomorphism theorem infact the quotient of kernel is universal as all mappings to the image algebra factor through it.

## Ideals

An **ideal** $\mathfrak{a}$ of a ring $A$ is a subset of $A$ which is a additive subgroup group and for $x \in \mathfrak{a}, xA \subseteq \mathfrak{a}$.
The cosets of $\mathfrak{a} \in A$ form a quotient ring $A/\mathfrak{a}$.
**Correspondence theorem for rings:** There is a bijection between ideals of $A$ containing $\mathfrak{a}$ and the ideals of $A/\mathfrak{a}$.

## Zero divisors, units

An element is called a **zero divisor** if its product with a non zero element gives 0.
A commutative ring with the only zero divisor being zero is called an **integral domain**.
An element is called a **unit** if its product with some element gives 1.

- $x \in A$ is a unit $\iff \langle x \rangle = \{ax \mid a \in A\} = A = \langle 1 \rangle$

A ring in which every non zero element is a unit is called a **field**.

- All fields are integral domains.
- All finite integral domains are fields.
- The only ideals in a field $F$ are 0 and $\langle 1 \rangle = F$

## Prime and Maximal ideals

A proper ideal $\mathfrak{p} \in A$ is called **prime** if for $xy \in \mathfrak{a} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ alternatively if $A/\mathfrak{p}$ is an integral domain.
A proper ideal $\mathfrak{m} \in A$ is called **maximal** if it is maximal with respect to inclusion alternatively if $A/\mathfrak{m}$ is a field.

## Local rings

F A ring with exactly one maximal ideal is called a **local** ring. And its subsequent quotient is called the **residue field** of the ring. If number of maximal ideals are finite then it is called **semi local**.

- A ring is local iff its set of non units form an ideal (which is consequently maximal)
- If $M \subset A$ is maximal then if $1 + m$ is a unit for all $m \in M \implies A$ is local.
- A local ring has no idempotents except 0 and 1.

## Ideal operations

For ideals $\mathfrak{a}, \mathfrak{b} \in A$,

- $\mathfrak{a} + \mathfrak{b}$ forms an ideal and is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$.
- Intersection of ideals is an ideal.
- Product of ideals is an ideal.
- Unions are in general not ideals.
- $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq a + b$.
- The distributive laws hold.

The **ideal quotient/colon ideal** is defined as $(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$ and $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
For a ring homomorphism $\varphi : A \to B$ and some ideals $\mathfrak{a} \in A, \mathfrak{b} \in B$ we define the extension of $\mathfrak{a}$ as $\mathfrak{a}^e$ as the ideal generated by $\varphi(\mathfrak{a})$.
And the contraction of $\mathfrak{b}$ just its preimage in $A$ which is always an ideal.

## Radical ideals

For an ideal $\mathfrak{a}$ its radical ideal is denoted as $\sqrt{\mathfrak{a}}$ or $r(\mathfrak{a}) = \{x \in A \mid x^n \in \mathfrak{a}\}$

## Nilradical and Jacobson ideal

The **nilradical** of a ring $A$ is denoted by $N(R)$ and consists of the set of all nilpotent elements of $A$. Equivalently it is the intersection of all prime ideals. This shows that a radical of an ideal is just the intersection of prime ideals containing it.
The **Jacobson** radical of a ring $A$ denoted by $J(R)$ is the intersection of all its maximal ideals. An element $x$ is in the Jacobson radical $\iff 1 - xy$ is a unit in $A, \forall y \in A$.

## Prime avoidance theorem

For ring $A$ consider $\mathfrak{a} \subset A$ that is stable under addition and multiplication and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideals such that $\mathfrak{p}_3, \ldots, \mathfrak{p}_n$ are prime in $A$. If $\mathfrak{a}$ is contained in the union of all $\mathfrak{p}_i$ then $\mathfrak{a} \subset \mathfrak{p}_i$ for some $i$.

## Chinese Remainder Theorem

For a ring $A$, let $I_1, \ldots, I_n$ be ideals of the ring $A$. Consider the map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as $\pi(a) = (a \mod I_1, \ldots, a \mod I_n)$. Then $\ker \pi = I_1 \bigcap \cdots \bigcap I_n$, i.e. it is surjective iff $I_1, \cdots I_n$ are pairwise comaximal. If $\pi$ is a surjection we have,

$$A/\bigcap I_k = A/\prod I_k \cong \prod (A/I_k)$$

## Modules

For ring $A$ we define an $A-$**module** $M$ to be an abelian group with addition along with scalar multiplication $A \times M \to M$ such that the following hold for $a, b \in A, m, n \in M$

- $a(m + n) = am + an$ and $(a + b)m = am + bm$
- $a(bm) = (ab)m$
- $1m = m$

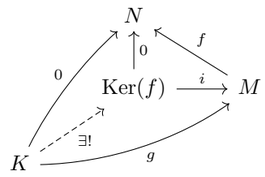
We also define the following notions pertaining to modules,

- A **submodule** $N$ of $M$ is simply a subgroup closed under scalar multiplication.
- For a submodule $N$ of $M$ its quotient module $M/N$ is defined naturally.
- The submodules of a module form a complete lattice w.r.t. inclusion.
- Define an **annihilator** of $m \in M$ to be $\mathrm{Ann}(m) = \{x \in A \mid xm = 0\}$ this extends to the full module as well. They are ideals of $A$. Furthermore $M$ can be seen as a $A/\mathfrak{a}$ module for $\mathfrak{a} \subset \mathrm{Ann}(M)$ naturally.

## Module homomorphisms

For $A-$modules $M, N$ a mapping $f : M \to N$ is a **module homomorphism** if $f(x + y) = f(x) + f(y)$ and $f(ax) = af(x)$ for $a \in A, x, y \in M$

- The set of all homomorphisms between modules, i.e. $\mathrm{Hom}_A(M, N)$ determines another $A-$module naturally.
- $\mathrm{Hom}_A(A, M) \cong M$ where $\varphi(f(x)) = f(1)$ defines the isomorphism.
- For a module homomorphism $f : M \to M$, its kernel and image are submodules.
- We define cokernel and coimages as the categorical dual of kernels and images. Explicitly as follows, for $f : M \to N$ homomorphism between $A-$modules, $\mathrm{Coker}(f) = N/\mathrm{Im}(f)$ and $\mathrm{Coim}(f) = M/\mathrm{Ker}(f)$
- $\mathrm{Ker}(f)$ has the following UMP, for $i$ defined to be the inclusion,




- The module of endomorphisms $\mathrm{Hom}_A(M, M)$ also denoted $\mathrm{End}_A(M)$ is in fact a ring (not necessarily commutative). A module is **faithful** if the map from $A \to \mathrm{End}_A(M)$ is injective equivalently if $\mathrm{Ann}(M) = 0$. Also $\mathrm{End}_R(M) \subset \mathrm{End}_{\mathbb{Z}} R(M)$ as we can consider $M$ as an abelian group hence as a $\mathbb{Z}-$module

We have the following isomorphism theorems in modules, $A-$modules $L \subset N, M \subset N$

- $L + M$ forms a module and $f : L \to L + M \to (L + M)/M$ has kernel $L \cap M$ so we have $L/(L \cap M) \cong (L + M)/M$
- If $L \subset M$ we have $N/M \cong (N/L)/(M/L))$ as $f :\to N \to N/L \to (N/L)/(M/L)$ forms a surjection with kernel $M$.

## Nakayama's Lemma

For $M$ a finitely generated $A$ module then for its Jacobson radical $J(A)$ we have $J(A)M = M \implies M = 0$

## Localization

For a multiplicatively closed subset $S$ of $A$ the **localization** of $A$ at $S$ denoted as $S^{-1}A$ is a ring which consists of tuples $(a, s)$ for $a \in A, s \in S$ and is characterized by the equivalence relation

$$(a, s) \sim (a', s') \iff \exists t \in S, t(as' - sa') = 0$$

.
For representatives of equivalence classes given as $[(a, s)], [(a', s')]$ addition is defined as $[(as' + sa', ss')]$ and multiplication is componentwise.