Proof Object: *Nakayama's Lemma*

Statement and Relevant Definitions

Definition 0.1 (Group)**.** A **group** is a set G with a binary operation $*$ on G such that the following properties hold.

1. **Associativity.** For all $a, b, c, \in G$, $(a * b) * c = a * (b * c)$.
2. **Identity.** There exists an element $e \in G$ such that for all $a \in G$, $a * e = a$ and $e * a = a$.
3. **Inverses.** For every $a \in G$ there exists some $b \in G$ for which $a * b = e$ and $b * a = e$.

A group G is called **abelian** if $a * b = b * a$ for all $a, b \in G$.

Definition 0.2 (Ring)**.** A **ring** is a set R with two binary operations, denoted $+$ and $\cdot$, for which the following hold.

1. **Abelian group under addition.** R is an abelian group under $+$ with identity denoted "0."
2. **Associativity of multiplication.** $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ for all $r, s, t \in R$.
3. **Multiplicative identity.** There is an element denoted "1" in R for which $r \cdot 1 = r$ and $1 \cdot r = r$ for every $r \in R$.
4. **Distributivity.** $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(r + s) \cdot t = r \cdot t + s \cdot t$ for all $r, s, t \in R$.

A ring R is called **commutative** if $r \cdot s = s \cdot r$ for all $r, s \in R$.

Definition 0.3 (Ideal of a commutative ring)**.** An **ideal** of a commutative ring R is a subset $I \subseteq R$ for which the following hold.

1. **Abelian group under addition.** R is an abelian group under $+$ with identity denoted "0."
2. **Absorption.** $ra \in I$ for all $r \in R$ and $a \in I$.

An ideal $\mathfrak{m}$ of a ring R is called **maximal** if it is a proper ideal, i.e., $\mathfrak{m} \subsetneq R$, and there is no other proper ideal strictly containing $\mathfrak{m}$, i.e., if $\mathfrak{m} \subseteq J \subsetneq R$ for some ideal J of R, then $J = \mathfrak{m}$.

Definition 0.4. A **local ring** is a ring that has a unique maximal ideal.

Remark 0.5. Assuming the axiom of choice, every ring has at least one maximal ideal since given ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots R$$

one can check that the union $\bigcup_{i=1}^{\infty} I_i$ is again an ideal of R, so the existence of a maximal ideal follows by Zorn's lemma. In fact, any *unit* of R–element with no multiplicative inverse–is contained in a maximal ideal.

Definition 0.6 (Module over a ring)**.** A **module** over a ring R is an abelian group M under a binary operation $+$, and a function $\cdot : R \times M \to M$, satisfying the following properties for all $r, s \in R$ and $u, v \in M$.

1. $r \cdot (u + v) = r \cdot u + r \cdot v$.
2. $(r + s) \cdot u = r \cdot u + s \cdot u$.
3. $(rs) \cdot u = r \cdot (s \cdot u)$.
4. $1 \cdot u = u$ for all $u \in M$.

A module is called **finitely generated** if there exist a fixed finite list $u_1, \ldots, u_n \in M$ such that any $w \in M$ can be written as $w = r_1 u_1 + r_1 u_2 + \cdots + r_n u_n$ for some $r_1, \ldots, r_n \in R$.

Though the following has long been traditionally called a "lemma," it is a fundamental theorem in the field of commutative algebra, and could arguably called the "Fundamental Theorem of Commutative Algebra."

Definition 0.7. Suppose that R is a commmutative ring, I is an ideal of R, than M is an R-module. Then IM is the set of elements of the form $a_1 u_1 + a_2 u_2 + \cdots + a_k u_k$, where $a_1, \ldots, a_2$. Due to the absorption property of ideals, IM is an R-module contained in M.

Theorem 0.8 (Nakayama's Lemma). *Let M be a finitely generated module over a local ring R that has maximal ideal $\mathfrak{m}$. If $M = \mathfrak{m}M$, then $M = 0$.*

Informal Proof. We apply induction on the number of generators n of M. For the base case $n = 1$, suppose that u generates M. Then every element of M has the form ru for some $r \in R$, and hence every element of $\mathfrak{m}M$ has the form $a(ru) = (ar)u = (ra)u$ for some $a \in \mathfrak{m}$. By the absorption property of ideals, $ra \in \mathfrak{m}$, and we conclude that every element of $\mathfrak{m}M$ has the form xu for some $x \in \mathfrak{m}$.

Suppose that $M = \mathfrak{m}M$. Then since $u \in M$, $u = xu$ for some $x \in \mathfrak{m}$. Hence $(1 - x)u = 0$. We claim that $1 - x$ has a multiplicative inverse. If not, then it is contained in $\mathfrak{m}$, but then since $x \in m$, we have that $1 = (1 - x) + x \in \mathfrak{m}$, contradicting the fact that $\mathfrak{m}$ is a proper ideal of R. Hence $1 - x$ has a multiplicative inverse y, and so

$$0 = y \cdot 0 = y((1 - x)u) = (y(1 - x))u = 1 \cdot u = u.$$

This forces $M = 0$, and the statement holds.

Now, inductively, for some $n \geq 1$, assume that M is generated by $u_1, \ldots, u_n \in M$. Let Ru_1 denote the R-module generated by u_1, and let if $N = M/Ru_1$ be the R-module consisting of equivalence classes of elements of M with respect to the equivalence relation given by $w \sim w'$ if and only if $w - w' \in Ru_1$. Then N is generated by the equivalence classes of $u_2, \ldots, u_n$, $(n-1)$-many element of N, and $\mathfrak{m}N = N$ still holds. So by the inductive hypothesis, $N = 0$, which says that $M = Ru_1$. But we have already done the case where $n = 1$. $\square$