Prime, Primary and Primal submodules

Definition A proper ideal $P$ of a ring $R$ is a prime ideal if for any $a, b \in R$, $ab \not\in P$ implies that either $a \in P$ or $b \in P$.

Example Let $p$ be a prime number. Then, in the ring of integers $\mathbb{Z}$, the ideal $p\mathbb{Z}$ is prime.

Proposition A proper ideal $P$ of a ring $R$ is prime if and only if for any ideals $A, B$ in $R$, $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.

Proof.

Corollary Let $P$ be a prime ideal of a ring $R$ and suppose that $A, B$ are ideals in $R$. If $A \cap B \subseteq P$, then either $A \subseteq P$ or $B \subseteq P$.

Proof.
Definition. Let \( I \) be an ideal in a ring \( R \). The radical of \( I \), denoted \( \sqrt{I} \), is the ideal \( \sqrt{I} = \bigcap P \), where the intersection runs over all prime ideals of \( R \) containing \( I \).

Proposition If \( I \) is an ideal in a ring \( R \), then

\[
\sqrt{I} = \{ r \in R \mid r^n \in I, \text{ for some integer } n > 0 \}.
\]

Example Let \( X \) be a set and \( R \) be the ring \( (P(X), \Delta, \cap) \), where \( P(X) \) is the power set of \( X \) and the operation \( \Delta \) is defined by \( A \Delta B = (A - B) \cup (B - A) \). Since for every \( r \in R \) and every positive integer \( n \), \( r^n = r \), then \( \sqrt{I} = I \) for every ideal \( I \) of \( R \).

Definition A proper ideal \( Q \) of a ring \( R \) is a primary ideal if for any \( a, b \in R, ab \in Q \) and \( a \notin Q \) implies that \( b^n \in Q \) for some positive integer \( n \).
It is clear directly from the definitions that every prime ideal is primary, but the following example shows that the converse is false.

Example  In the ring of integers $\mathbb{Z}$, the ideal $4\mathbb{Z}$ is primary but it is not prime.

Proposition  If $Q$ is a primary ideal in a ring $R$. Then $\sqrt{Q}$ is a prime ideal.

Proof. Since $Q$ is a proper ideal in $R$, then $1 \notin Q$ and hence $1 \notin \sqrt{Q}$ showing $\sqrt{Q}$ is proper ideal in $R$. Let $ab \in \sqrt{Q}$ and $a \notin \sqrt{Q}$, then $(ab)^n \in Q$ for some positive integer $n$, and hence $a^n b^n \in Q$. Since $a \notin \sqrt{Q}$, $a^n \notin Q$. Since $Q$ is primary, there is a positive integer $k$ such that $(b^n)^k \in Q$, whence $b \in \sqrt{Q}$. Therefore $\sqrt{Q}$ is a prime ideal.
Definition. Let $M$ be an $R$–module. A proper submodule $N$ of $M$ is said to be a prime submodule if $rm \in N$ for $r \in R$ and $m \in M$ implies that either $m \in N$ or $rM \subseteq N$.

Definition. Let $M$ be an $R$–module. A proper submodule $N$ of $M$ is said to be a primary submodule if $rm \in N$ for $r \in R$ and $m \in M$ implies that either $m \in N$ or $r^n M \subseteq N$ for some positive integer $n$.

Remark. Consider the ring $R$ as an $R$–module and let $Q$ be a primary ideal (and hence a submodule) of $R$. If $rm \in Q$ with $r \in R$ and $m \notin Q$, then $r^n \in Q$ for some a positive integer $n$. Since $Q$ is an ideal, this implies $r^n R \subseteq Q$. Hence $Q$ is primary submodule of the module $R$. Conversely every primary submodule of $R$ is a primary ideal.
Similarly, an ideal $P$ of the ring $R$ is prime ideal if and only it is prime submodule of the module $R$.

It is clear directly from the definitions that every prime submodule is primary, but the converse is false.

**Definition**  
Let $N$ be a submodule of an $R$–module $M$. The residual of $N$ by $M$, denoted $(N : M)$, is the ideal $(N : M) = \{ r \in R \mid rM \subseteq N \}$.

**Proposition**  
If $L$ and $N$ are submodules of an $R$–module $M$, then $(L \cap N : M) = (L : M) \cap (N : M)$.

**Proposition**  
If $N$ is a prime submodule of an $R$–module $M$, then $(N : M)$ is prime ideal in $R$.

*Proof.* $(N : M)$ is a proper ideal, since $1 \notin (N : M)$. Let $ab \in (N : M)$, and $b \notin (N : M)$. Then $bM \nsubseteq N$, that is there exists $m \in M$ with $bm \notin N$. But $a(bm) = (ab)m \in N$ and $N$ is prime, therefore $aM \subseteq N$, thus $a \in (N : M)$. 
Proposition. If $N$ is a primary submodule of an $R$–module $M$, then $(N : M)$ is primary ideal in $R$, and hence $\sqrt{(N : M)}$ is prime ideal in $R$.

Definition. Let $M$ be an $R$–module and $N$ a submodule of $M$. For any $a \in R$, the submodule $\{m \in M \mid am \in N\}$ is denoted by $a^{-1}N$. Analogously for a subset $A$ of $R$, $A^{-1}N = \{m \in M \mid Am \subseteq N\}$.

Remark. (i) $N \subseteq a^{-1}N$.

(ii) The notation $a^{-1}N$ does not mean that $a$ has an inverse in $R$, however if $a$ has an inverse in $R$, then the submodules $(a^{-1})N = \{a^{-1}m \mid m \in N\}$ and $a^{-1}N = \{m \in M \mid am \in N\}$ are the same.
Proof. (i) follows from definition of $a^{-1}N$. (ii) Let $m \in a^{-1}N$, then $am \in N$, hence $m = a^{-1}(am) \in (a^{-1})N$, therefore $a^{-1}N \subseteq (a^{-1})N$. On other hand if $m \in (a^{-1})N$, then $m = a^{-1}n$ for some $n \in N$. Now $am = a(a^{-1}n) = n \in N$, so $m \in a^{-1}N$, therefore $(a^{-1})N \subseteq a^{-1}N$.

Definition. Let $M$ be an $R$–module and $N$ a submodule of $M$. The element $a \in R$ is (left) prime to $N$ if $a^{-1}N = N$, i.e. if $am \in N$ ($m \in M$) implies $m \in N$.

A is not (left) prime to $N$ if $a^{-1}N \neq N$, i.e. there exists an element $m \in M - N$ with $am \in N$.

A subset $A$ of $R$ is not prime to $N$ if for any $a \in A$, $a$ is not prime to $N$. In this case we say that $A$ is pointwise not prime to $N$.

The subset $A$ of $R$ is uniformly not prime to $N$, if there exists an element $u \in M - N$ with $Au \subseteq N$, i.e. $A$ is uniformly not prime to $N$ if and only if $A^{-1}N \neq N$. 
Example. Consider the submodule $6\mathbb{Z}$ in the $\mathbb{Z}$-module $\mathbb{Z}$. $5$ is prime to $6\mathbb{Z}$ while $2$ is not prime to $6\mathbb{Z}$, the set $\{2, 3\}$ is pointwise not prime to $6\mathbb{Z}$, and the set $\{2, 4, 6, \ldots\}$ is uniformly not prime to $6\mathbb{Z}$.

Proposition. Let $N$ be a proper submodule of an $R$-module $M$. Then the ideal $(N : M)$ is uniformly not prime to $N$.

Proof. By the definition of $(N : M)$, we have $(N : M)M \subseteq N$, and hence $(N : M)u \subseteq N$ for any $u \in M - N$.

Definition. Let $M$ be an $R$-module and $N$ a submodule of $M$. The adjoint of $N$ is the set of all elements of $R$ that are not prime to $N$ and denoted by $\text{adj}(N)$.

On other words, $\text{adj}(N) = \{r \in R \mid rm \in N \text{ for some } m \in M - N\}$. 
Example \quad In \ Z\textendash \text{module } \mathbb{Z}, \text{ adj}(6\mathbb{Z}) \text{ is the set } 2\mathbb{Z} \cup 3\mathbb{Z} \text{ and } \text{adj}(4\mathbb{Z}) \text{ is the ideal } 2\mathbb{Z}.

Proposition \quad Let \ N be a proper submodule of an \ R\textendash \text{module } \ M, \text{ then }

\[ (N : M) \subseteq \sqrt{(N : M)} \subseteq \text{adj}(N) \]

Proof. \ (N : M) \subseteq \sqrt{(N : M)} \text{ follows from Definition }, \text{ so the proof reduces to proving that } \sqrt{(N : M)} \subseteq \text{adj}(N). \text{ Let } r \in \sqrt{(N : M)}, \text{ then } r^nM \subseteq N \text{ for some positive integer } n. \text{ Pick } m \in M \setminus N, \text{ then } r^n m \in N. \text{ If we choose } n_0 \text{ be the smallest positive integer with } r^{n_0} m \in N, \text{ we have } r(r^{n_0-1} m) \in N \text{ while } r^{n_0-1} m \notin N, \text{ Thus } r \in \text{adj}(N).

Definition \quad Let \ M be an \ R\textendash \text{module. A proper submodule } \ N \text{ of } \ M \text{ is said to be primal if } \text{adj}(N) \text{ forms an ideal of } R. \text{ In this case the adjoint of } \ N \text{ will also be called the adjoint ideal of } \ N.
Remark. Consider the ring $R$ as an $R$–module. An ideal $I$ of $R$ is a primal ideal if and only if it is a primal submodule of $R$.

Example. In the ring $\mathbb{Z}$, the ideal $4\mathbb{Z}$ is primal, and the ideal $6\mathbb{Z}$ is not primal.

Proposition. Let $M$ be an $R$–module. If $N$ is a primal submodule of $M$, then $\text{adj}(N)$ is a prime ideal of $R$.

Proof. Since $1 \notin \text{adj}(N)$, $\text{adj}(N)$ is a proper ideal. Let $ab \in \text{adj}(N)$ with $a \notin \text{adj}(N)$, there exists $m \in M - N$ with $abm \in N$, so $bm \in N$ implies that $b \in \text{adj}(N)$.

Remark. Let $N$ be a submodule of an $R$–module $M$. If $r \in R$ and $a \in \text{adj}(N)$, then there exists $m \in M - N$ with $am \in N$, and hence $ram \in N$ while $m \notin N$ and, as a consequence, $ra \in \text{adj}(N)$. Thus to prove $\text{adj}(N)$ is an ideal we only prove $\text{adj}(N)$ is closed under the addition.
Proposition. Let $N$ be a submodule of an $R$–module $M$. If $\text{adj}(N)$ is uniformly not prime to $N$, then $\text{adj}(N)$ is an ideal of $R$, and as a consequence, $N$ is primal.

Proof. Let $a, b \in \text{adj}(N)$, since $\text{adj}(N)$ is uniformly not prime to $N$, then there exists an element $u \in M - N$ with $\text{adj}(N)u \subseteq N$. Thus $au$ and $bu$ are in $N$, and hence $(a + b)u \in N$ showing $a + b \in \text{adj}(N)$.

Definition. Let $M$ be an $R$–module. A proper submodule $N$ of $M$ is said to be uniformly primal if $\text{adj}(N)$ is uniformly not prime to $N$.

Definition. Let $R$ be a ring. An ideal $I$ of $R$ is uniformly primal ideal if it is uniformly primal submodule of the $R$–module $R$.

Proposition. Let $N$ be a proper submodule of an $R$–module $M$. If $\text{adj}(N)$ is a principle ideal of $R$ generated by $a$, then $N$ is uniformly primal.
Proof. By assumption $\text{adj}(N) = Ra$, then $a$ is not prime to $N$, so there exists an element $u \in M - N$ with $au \in N$, thus $\text{adj}(N)u = Rau \subseteq N$, and as a consequence, $\text{adj}(N)$ is uniformly not prime to $N$, and $N$ is uniformly primal.

Corollary Let $R$ be a principal ideal ring, and $M$ an $R$–module. Then every primal submodule is uniformly primal.

Example Consider the ring $\mathbb{Z}$, the ideal $4\mathbb{Z}$ is uniformly primal ideal, since $\text{adj}(4\mathbb{Z}) = 2\mathbb{Z}$ is principle ideal of $\mathbb{Z}$.

Definition Let $M$ be an $R$–module. A proper submodule $N$ of $M$ is said to be irreducible if $N$ is not the intersection of two submodules of $M$ that properly contain it.
Definition. Let $M$ be an $R$–module. A proper submodule $N$ of $M$ is said to be completely irreducible (or strongly irreducible) if for any family $\{N_\alpha\}_{\alpha \in \Delta}$ of submodules of $M$ with $N = \bigcap_{\alpha \in \Delta} N_\alpha$, $N = N_\beta$ for some $\beta \in \Delta$. On other words, $N$ is not the intersection of any collection of submodules of $M$ each properly containing $N$.

Clearly completely irreducible submodules of $M$ are irreducible, but not conversely: the zero ideal of the ring $\mathbb{Z}$ is irreducible but not completely irreducible.

Proposition. (Irreducible $\Rightarrow$ Primal)

Let $M$ be an $R$–module. If $N$ is an irreducible submodule of $M$, then $N$ is primal.

Proof. Let $a, b \in \text{adj}(N)$, then there exists $m_1$ and $m_2$ in $M - N$ such that $am_1 \in N$ and $bm_2 \in N$. Since each of $N + Rm_1$ and $N + Rm_2$ properly contains $N$, and $N$ is...
irreducible, then \( N \subsetneq (N + Rm_1) \cap (N + Rm_2) \), thus there is \( m \in (N + Rm_1) \cap (N + Rm_2) \) with \( m \notin N \). However \( am \in a(N + Rm_1) = aN + aRm_1 = aN + Ram_1 \subseteq N \), similarly \( bm \in N \). So that \( (a + b)m = am + bm \in N \) while \( m \notin N \). Thus \( a + b \in \text{adj}(N) \).

The next example shows that a primal submodule need not be irreducible.

**Example** Consider the ring \( \mathbb{Z}[x] \), the ring of polynomials with coefficients in \( \mathbb{Z} \), the ideal \( \langle 4, 2x, x^2 \rangle \) is primal with \( \langle 2, x \rangle \) as adjoint ideal, but it is not irreducible, since \( \langle 4, 2x, x^2 \rangle = \langle 4, x \rangle \cap \langle 2, x^2 \rangle \).

**Proposition** (Completely Irreducible \( \Rightarrow \) Uniformly Primal)

Let \( M \) be an \( R \)-module. If \( N \) is a completely irreducible submodule of \( M \), then \( N \) is uniformly primal.
Remark. The previous example shows that a uniformly primal submodule need not be completely irreducible.

**Proposition (**)** Let $N$ be a proper submodule of an $R$-module $M$. Then $N$ is a prime submodule of $M$ if and only if $\text{adj}(N) = (N : M)$.

**Proof.** Suppose $N$ is a prime submodule of $M$. Since $(N : M) \subseteq \sqrt{(N : M)} \subseteq \text{adj}(N)$

it suffices to show that $\text{adj}(N) \subseteq (N : M)$. Let $r \in \text{adj}(N)$, then there exists $m \in M - N$ with $rm \in N$, since $N$ is prime, then $rM \subseteq N$, and hence $r \in (N : M)$. 

Conversely, assume \( \operatorname{adj}(N) = (N : M) \), and let \( rm \in N \) where \( r \in R \) and \( m \in M - N \). Then \( r \) is not prime to \( N \), therefore \( r \in \operatorname{adj}(N) = (N : M) \). Thus \( rM \subseteq N \), and \( N \) is prime.

**Corollary** \((\text{Prime} \Rightarrow \text{Uniformly Primal})\)

Let \( M \) be an \( R \)-module. If \( N \) is a prime submodule of \( M \), then \( N \) is uniformly primal.

**Proof:** By Propositions (\( \ast \)) and (\( \ast \ast \))

**Proposition** \( N \) be a proper submodule of an \( R \)-module \( M \). Then \( N \) is a primary submodule of \( M \) if and only if \( \operatorname{adj}(N) = \sqrt{(N : M)} \).
Proof. Suppose $N$ is a primary submodule of $M$. It is sufficient to show that $\text{adj}(N) \subseteq \sqrt{(N : M)}$. Let $r \in \text{adj}(N)$, then there exists $m \in M - N$ with $rm \in N$, since $N$ is primary, then $r^n M \subseteq N$ for some positive integer $n$, and hence $r \in \sqrt{(N : M)}$.

Conversely, assume $\text{adj}(N) = \sqrt{(N : M)}$, and let $rm \in N$ where $r \in R$ and $m \in M - N$. Then $r$ is not prime to $N$, therefore $r \in \text{adj}(N) = \sqrt{(N : M)}$. Thus $r^k M \subseteq N$ for some positive integer $k$, and $N$ is primary.

Corollary (Primary $\Rightarrow$ Primal)

Let $M$ be an $R$–module. If $N$ is a primary submodule of $M$, then $N$ is primal.

Proof. If $N$ is a primary submodule of $M$, then by the previous proposition, $\text{adj}(N) = \sqrt{(N : M)}$ is an ideal in $R$, hence $N$ is primal.

The next example shows: a primal submodule of a module $M$ is not necessarily primary.

Example Consider the ring $F[x,y]$, the ring of polynomials in $x$ and $y$ over a field $F$. The ideal $(x^2,xy)$ of $F[x,y]$ is primal with $(x,y)$ as adjoint prime.
ideal, but it is not primary, for \( xy \in \langle x^2, xy \rangle \) and neither \( x \) nor any power of \( y \) belongs to \( \langle x^2, xy \rangle \).

Summary of
Relation between Submodules

- Completely Irreducible
- Irreducible
- Uniformly Primal
- Primal
- Prime
- Primary
Over Boolean rings we prove the following new result: prime, primary and primal submodules are the same.

First we give the definition of a Boolean ring.

**Definition** A Boolean ring is a ring $R$ in which every element is idempotent, that is, $x^2 = x$ for all $x \in R$.

**Proposition** Let $R$ be a Boolean ring and $M$ be an $R$-module. Then every primal submodule of $M$ is prime.

**Proof.** Let $N$ be a primal submodule of $M$. It suffices to show that $adj(N) \subseteq (N : M)$. Let $a \in adj(N)$, then $1 - a \notin adj(N)$, for otherwise, $1 = (1 - a) + a \in adj(N)$ which is a contradiction. That is $1 - a$ is prime to $N$, hence for all $m \in M$, $(1 - a)am = 0 \in N$ implies $am \in N$. Therefore $a \in (N : M)$. 

Corollary. Let $R$ be a Boolean ring and $M$ be an $R$-module. Then every primary submodule of $M$ is prime.

Corollary. Every primal ideal of a Boolean ring is prime.

Corollary. Every primary ideal of a Boolean ring is prime.