10. *Primary ideals and the radical.*

*** *Multiplicatively closed setes.* ***

10.1 Definition. A non-empty subset S of a commutative ring R is called **multiplicatively closed** if s, $t \in S$ implies $st \in S$.

A multiplicatively closed set S is called **saturated** if it contains every divisor of each of its elements, i.e., if $s = ab \in S$ implies $a \in S$.

Examples of multiplicatively closed sets (1–3 are saturated):

1) $R \setminus P$, where P is a prime ideal of R,
2) $R \setminus \bigcup_{\alpha \in A} P_\alpha$, where all P_α are prime ideals of R
3) the set of all non-zero-divisors in R
4) the set of powers of a fixed element $\{r^n \mid n \in \mathbb{N}_0\}$.

10.2 Lemma. Let S be a multiplicatively closed subset of R and I an ideal of R with $I \cap S = \emptyset$. Then there exists a prime ideal P of R with $I \subseteq P$ and $P \cap S = \emptyset$.

Proof. Apply Zorn's Lemma to $\mathcal{J} = \{J \trianglelefteq R \mid I \subseteq J \text{ and } S \cap J = \emptyset\}$. Since $I \in \mathcal{J}$, $\mathcal{J} \neq \emptyset$. Every chain of ideals in $\mathcal{J}$ has an upper bound in $\mathcal{J}$: its union is in $\mathcal{J}$. Let P be a maximal element of $\mathcal{J}$. We will show that P is prime. $S \neq \emptyset$ implies $P \neq R$. Suppose $ab \in P$, $a \notin P$ and $b \notin P$. By maximailty of P there exists $s \in S \cap (P + Ra)$ and $t \in S \cap (P + Rb)$. But then $st \in S \cap P$, a contradiction. □

10.3 Definition. If $S \subseteq R$ is a multiplicatively closed set then its **saturation** $\bar{S}$ is the set of all divisors of elements of S: $\bar{S} = \{t \in R \mid \exists s \in S \;\, t \bigm| s\}$.

It is easy to see that the saturation of a multiplicatively closed set S is a saturated multiplicatively closed set that contains S.

10.4 Corollary. Let S be a saturated multiplicatively closed subset of R. Then $S = R \setminus \bigcup_{P \in \mathcal{P}} P$, where $\mathcal{P}$ is the set of all prime ideals P of R with $S \cap P = \emptyset$.

Proof. Clearly, $S \subseteq R \setminus \bigcup_{P \in \mathcal{P}} P$. For the reverse inclusion, we show that for every $u \notin S$ there exists some prime ideal P with $S \cap P = \emptyset$ and $u \in P$. By the saturation of S, $u \notin S$ implies $Ru \cap S = \emptyset$. By Lemma 10.2 there exists a prime ideal P with $Ru \subseteq P$ and $S \cap P = \emptyset$. □

10.5 Lemma. Let I be an ideal of R and P a prime ideal containing I. Then there exists a minimal prime P' of I with $I \subseteq P' \subseteq P$.

Proof. Let $S = R \setminus P$ and consider the set $\mathcal{S}$ of multiplicatively closed sets T with $S \subseteq T$ and $T \cap I = \emptyset$. Then $\mathcal{S}$ is non-empty because $S \in \mathcal{S}$ and every chain of elements of $\mathcal{S}$ has an upper bound in $\mathcal{S}$ (its union). Let S_0 be a maximal element of $\mathcal{S}$ (which exists by Zorn's Lemma), and set $U = R \setminus S_0$. By Lemma 10.2, there exists a prime ideal P' containing I and disjoint from S_0, i.e., $I \subseteq P' \subseteq U$. It follows that $P' = U$ and P' is a minimal prime of I, since for any prime ideal Q with $I \subseteq Q \subsetneqq U$, its complement $R \setminus Q$ would be an element of $\mathcal{S}$ stricltly containing S_0. $\square$

$* * *$ *The radical.* $* * *$

10.6 Definition. Let I be an ideal of R. The **radical of** I is defined by

$$\sqrt{I} = \{r \in R \mid \exists n \in \mathbb{N}\ \ r^n \in I\}.$$

Convince yourself of the following easy facts:

10.7 Remark.

(1) $I \subseteq \sqrt{I}$

(2) $\sqrt{\sqrt{I}} = \sqrt{I}$

(3) $\sqrt{I} = R \iff I = R$

(4) If Q is an intersection of prime ideals then $\sqrt{Q} = Q$.

10.8 Proposition.

$$\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ I \subseteq P}} P.$$

Proof. Clearly, $\sqrt{I}$ is contained in all prime ideals containing I. Conversely, if $r \notin \sqrt{I}$, then $S = \{r^n \mid n \in \mathbb{N}\}$ is a multiplicatively closed set with $S \cap I = \emptyset$ and by Lemma 10.2, there exists a prime ideal P with $I \subseteq P$ and $r \notin P$. $\square$

Recall that an element $r \in R$ is called **nilpotent** if there exists a natural number n with $r^n = 0$.

10.9 Definition. The radical of (0), consisting of all nilpotent elements of R, is called the **nilradical** of R:

$$\mathrm{Nil}(R) = \{r \in R \mid \exists n \in \mathbb{N}\ \ r^n = 0\}.$$

10.10 Corollary of 10.8. The nilradical of R is the intersection of all prime ideals of R.

10.11 Lemma. Some rules of arithmetic for radicals:
(1) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
(2) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$
(3) $\sqrt{I} + \sqrt{J} = R \iff I + J = R$

Proof. Exercise. $\square$

10.12 Lemma. Let P be a prime ideal of R and I an ideal of R.
(i) $P^n \subseteq I \subseteq P$ for some $n \in \mathbb{N}$ implies $\sqrt{I} = P$.
(ii) If R is Noetherian, then $\sqrt{I} = P$ implies for some n $P^n \subseteq I \subseteq P$.

Proof. (i) is easy. Ad (ii), $P = (p_1, \ldots, p_m) = \sqrt{I}$ implies for some $k \in \mathbb{N}$, $p_1^k, \ldots, p_m^k \in I$. Every element q of P is an R-linear combination of the p_i. By the multinomial theorem, $(r_1p_1 + \ldots + r_mp_m)^m k$ is a sum of terms each of which is divisible by p^k for some i, therefore $q^n \in I$ for every $q \in P$, $n = km$. $\square$

*** *Primary ideals* ***

10.13 Definition. An ideal Q of R is called **primary** iff $Q \neq R$ and for all a, $b \in R$ with $ab \in Q$ either $a \in Q$ or $\exists n \in \mathbb{N}\ \ b^n \in Q$.

The definition of primary tends to be confusing at first. Note that for a primary ideal Q, $ab \in Q$ implies $a \in Q$ or $b \in \sqrt{Q}$ as well as $b \in Q$ or $a \in \sqrt{Q}$. (R is commutative after all). Therefore, for an ideal $Q \neq R$, being primary is equivalent to $ab \in Q$ implies $a \in Q$ or $b \in Q$ or, if neither a nor b is in Q then a and b are both in $\sqrt{Q}$.

10.14 Lemma. If Q is a primary ideal then $\sqrt{Q}$ is a prime ideal.

Proof. Easy. $\square$

10.15 Definition. A primary ideal Q with $\sqrt{Q} = P$ is called **P-primary**.

Not every ideal whose radical is prime is primary, however. For instance, $\sqrt{P^n} = P$ for every prime ideal P and $n \in \mathbb{N}$, but not every power of a prime ideal is primary. In a more positive vein, we have the following facts:

10.16 Lemma. Let M be a maximal ideal of R and Q an ideal with $\sqrt{Q} = M$. Then Q is M-primary.

Proof. Suppose $ab \in Q$ and $a \notin M$; we must show $b \in Q$. We have $M + aR = R$, i.e., $\sqrt{Q} + aR = R$. This implies $Q + aR = R$, so $1 = q + ar$ for some $q \in Q$ and $r \in R$, and finally $b = qb + abr \in Q$. $\square$

10.17 Corollary. Let M be a maximal ideal of R and $I \neq R$ an ideal with $M^n \subseteq I$ for some $n \in \mathbb{N}$. Then I is M-primary.

Proof. I is not contained in any prime ideal P other than M: if $I \subseteq P$ then for every $m \in M$, $m^n \in I \subseteq P$ implies $m \in P$, hence $M = P$. Since $I \neq R$, this shows $\sqrt{I} = M$ and we are done. $\square$

Just like prime ideals, primary ideals behave nicely with respect to ring homomorphisms, particularly surjective ones:

10.18 Lemma. Let $f\colon R \to T$ be a ring homomorphism (with $f(1) = 1$, as always) and I, Q ideals of T. Then

(1) $f^{-1}(\sqrt{I}) = \sqrt{f^{-1}(I)}$.

(2) If Q is primary then $f^{-1}(Q)$ is primary.

Again, like prime ideals, primary ideals can be characterized by a property of their quotient ring.

10.19 Proposition. An ideal Q is primary if and only if R/Q is a non-zero ring in which every zero-divisor is nilpotent.

Proof. Easy. $\square$

Together with the previous lemma this implies that a canonical projection induces a bijection between primary ideals containing the kernel and primary ideals in the quotient ring. (Note that everything we show for canonical projections holds mutatis mutandis for any surjective ring homomorphism $f\colon R \to T$, since f is just the canonical projection $\pi\colon R \to R/\mathrm{Ker} f$ followed by the isomorphism $\bar{f}\colon R/\mathrm{Ker} f \to T$.)

10.20 Proposition. Let I be an ideal of R and $\pi\colon R \to R/I$ the canonical projection. Then a bijection between all primary ideals Q of R with $I \subseteq Q$ and all primary ideals of R/I is given by $Q \mapsto \pi(Q)$. Its inverse is $\tilde{Q} \mapsto \pi^{-1}(\tilde{Q})$ (for $\tilde{Q} \trianglelefteq R/I$).

Primary ideals also behave just like prime ideals with respect to the canonical homomorphism into a ring of fractions $f_S\colon R \to S^{-1}R$ and with respect to the canonical projection onto a residue class ring:

10.21 Proposition. Let $S^{-1}R$ be a ring of fractions of R and $f_S\colon R \to S^{-1}R$ the canonical homomorphism.

(1) If $Q \trianglelefteq R$ is primary and $\frac{r}{s} \in S^{-1}Q$ then $r \in Q$.

(2) A bijection between the primary ideals Q of R with $S \cap Q = \emptyset$ and all primary ideals of $S^{-1}R$ is given by $Q \mapsto S^{-1}Q$ (for Q a primary ideal of R). Its inverse is $\tilde{Q} \mapsto f_S^{-1}\tilde{Q}$ (for $\tilde{Q}$ a primary ideal of $S^{-1}R$).

This is shown just like the analogous statement for prime ideals. (Note that $Q \cap S = \emptyset$ implies $\sqrt{Q} \cap S = \emptyset$.)

$* * *$ *Symbolic powers* $* * *$

10.22 Definition. Let P be a prime ideal of R. The n-th symbolic power of P is defined by $P^{(n)} = R \cap P^n R_P$.

The n-th symbolic power of P is the contraction back to R of the extension of P^n into R_P and thus contains P^n.

10.23 Proposition. Let P be a prime ideal of R and $n \in \mathbb{N}$.

(1) $P^{(n)}$ is P-primary.

(2) If Q is a primary ideal then $P^n \subseteq Q \implies P^{(n)} \subseteq Q$.

(3) $P^{(n)} = P^n \iff P^n$ is primary.

10.24 Corollary. If M is a maximal ideal of R then $M^{(n)} = M^n$ for all $n \in \mathbb{N}$.

$* * *$ *Primary decompostion of ideals in Noetherian rings* $* * *$

10.25 Definition. An ideal $I \neq R$ of a commutative ring R is called **irreducible** if there do not exist ideals A, B of R, each properly containing I, such that $I = A \cap B$.

Note that prime ideals are certainly irreducible: Suppose $P = A \cap B$. If P is prime, then $AB \subseteq A \cap B \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.

It is easy to see that $I \neq R$ being irreducible is equivalent to: there do not exist finitely many ideals A_i with $A_i \supset I$ and $I = A_1 \cap \ldots \cap A_n$. It is however possible for an irreducible ideal to be the intersection of an infinite collection of ideals each properly containing it (just consider (0) in $\mathbb{Z}$).

10.26 Lemma. Let R be a Noetherian ring. Then every proper ideal of R can be expressed as a finite intersection of irreducible ideals.

Proof. Let S be the set of proper ideals of R that are not finite intersections of irreducible ideals. If $S \neq$ then S contains a maximal ideal I. As I is certainly not irreducible, there exist ideals A, B, each properly containing I with $I = A \cap B$. By maximalty of I, $A, B \notin S$. Therfore A and B are each expressible as a finite intersection of irreducible ideals, and so is I, a contradiction. $\square$

10.27 Lemma. Let R be a Noetherian ring. Then every irreducible ideal of R is primary.

Proof. Let I be irreducible and $ab \in R$. To show: $b \in I$ or there exists $n \in \mathbb{N}$ with $a^n \in I$.

Consider the ascending chain of ideals of R:

$$I \subseteq (I :_R a) \subseteq (I :_R a^2) \subseteq \ldots \subseteq (I :_R a^n) \subseteq (I :_R a^{n+1}) \subseteq \ldots,$$

Let $N \in \mathbb{N}$ be such that $(I :_R a^n) = (I :_R a^N)$ for all $n \geq N$. We will show that $I = (I + (b)) \cap (I + (a^N))$. Once this is established, we are done, because irreducibility of I then implies either $I + (b) = I$ (and hence $b \in I$) or $I = I + (a^N)$ (and hence $a^N \in I$).

Clearly, $I \subseteq (I + (b)) \cap (I + (a^N))$. Now let $r \in (I + (b)) \cap (I + (a^N))$. Then $r = i + sb = j + ta^N$ for some $i, j \in I$ and $s, t \in R$. Multiplying by a we get $ai - aj + sab = ta^{N+1}$. The left hand side is in I, therefore $t \in (I : a^{N+1})$. By the choice of N, $(I : a^{N=1}) = (I : a^N)$, and so $ta^N \in I$. This implies $r = j + ta^N \in I$. $\square$

10.28 Corollary. Let R be a Noetherian ring. Then every proper ideal of R can be expressed as a finite intersection of primary ideals.

10.29 Definition. Let I be an ideal. A finite list of primary ideals $Q_1, \ldots, Q_m$ such that $I = Q_1 \cap \ldots \cap Q_m$ is called a **primary decomposition** of I.

A primary decomposition of I is called **reduced** if

(1) there doesn't exist j such that $Q_j \supseteq \bigcap_{i \neq j} Q_i$ and

(2) $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$.

10.30 Lemma. If Q_1 and Q_2 are P-primary ideals then $Q_1 \cap Q_2$ is again P-primary.

Proof. Exercise. $\square$

10.31 Corollary. Any ideal that has a primary decomposition has a reduced primary decomposition.

Proof. Given a primary decomposition $I = Q_1 \cap \ldots \cap Q_m$ we can create a reduced primary decomposition by grouping together primary ideals with the same radical and taking their intersection (applying 10.30) and then deleting one by one those primary ideals that contain the intersection of the remaining ones (as long as any such redundant primary ideals are left). Since our list of Q_i is finite, this process terminates with a reduced decomposition. $\square$

10.32 Remark. By 10.26, 10.27 and 10.31, every proper ideal in a Noetherian ring has a reduced primary decomposition. This is in general no longer a decomposition into irreducible ideals. (We have taken the intersections of irreducible components sharing the same radical.)

10.33 Lemma. Let Q be a P-primary ideal of R, and $r \in R$.

(1) If $r \notin Q$ then $(Q : r)$ is P-primary.

(2) If $r \notin P$ then $(Q : r) = Q$.

Proof. Easy. $\square$

10.34 Lemma. Suppose $I = Q_1 \cap \ldots \cap Q_m$ is a reduced primary decompostion with $\sqrt{Q_i} = P_i$ for $1 \leq i \leq m$.

For any prime ideal P of R, the following are equivalent

(1) $P = P_i$ for some i.

(2) There exists $r \in R$ such that $(I : r)$ is P-primary.

(3) There exists $r \in R$ such that $\sqrt{(I : r)} = P$.

Furthermore, if R is Noetherian, then the following is equivalent to the previous three conditions:

(4) There exists $r \in R$ such that $(I : r) = P$.

Proof. $(1 \Rightarrow 2)$ Suppose $P = P_i$ and let $a_i \in (\bigcap_{j \neq i} Q_i) \setminus Q_i$ (which exists because the primary decomposition is reduced). Then

$$(I : a_i) = \left(\bigcap_{j=1}^{m} Q_j : a_j \right) = \bigcap_{j=1}^{m} (Q_j : a_j) = (Q_i : a_i),$$

which is P_i-primary, i.e. P-primary, by 10.33.

$(2 \Rightarrow 3)$ is trivial;

$(3 \Rightarrow 1)$

$$P = \sqrt{(I : r)} = \bigcap_{j=1}^{m} \sqrt{(Q_j : r)} = \bigcap_{\substack{j \\ a \notin Q_j}} P_j$$

P is equal to a finite intersection of prime ideals (necessarily there exists some j such that $a \notin Q_j$, otherwise $P = R$), therefore P coincides with one of the P_j.

$(4 \Rightarrow 2)$ is trivial; for Noetherian R we show $(2 \Rightarrow 4)$: The set of P-primary ideals of the form $(I : r)$ contains a maximal element $(I : s)$. We claim that $(I : s) = P$. It suffices to show that $(I : s)$ is prime. Let $ab \in (I : s)$, and suppose $a, b \notin (I : s)$. Then $(I : s)$ is properly contained in $(I : as)$ (witness b), and $(I : as)$ is a proper ideal of R (witness a).

The radical of $(I : as)$ is P: if $c^n \in (I : as)$ then $ac^n \in (I : s)$ while $a \notin (I : s)$ implies $c^n \in P$, and further $c \in P$. Therefore $\sqrt{(I : as)} \subseteq P$ and the reverse inclusion follows from $(I : s) \subseteq (I : as)$.

Let $cd \in (I : as)$, $c \notin (I : as)$. Then $cda \in (I : s)$, while $ca \notin (I : s)$ implies $d \in \sqrt{(I : s)} = P = \sqrt{(I : as)}$. Therefore $(I : as)$ is P-primary, a contradiction to the maximality of $(I : s)$. $\square$

10.35 Theorem. Suppose $I = Q_1 \cap \ldots \cap Q_m$ is a reduced primary decompostion, and $P_i = \sqrt{Q_i}$, for $1 \leq i \leq m$. Then for every reduced primary decomposition of I, the same set of prime ideals $\{P_1, \ldots, P_m\}$ occurs as the set of radicals of the primary components.

Proof. By 10.34, the criterion for P to occur among the radicals of the Q_i does not depend on the primary decomposition but only on I. $\square$

10.36 Theorem. Suppose $I = Q_1 \cap \ldots \cap Q_m$ is a reduced primary decompostion, and $P_i = \sqrt{Q_i}$, where $P_1, \ldots, P_k$ are the isolated primes and $P_{k+1}, \ldots, P_m$ the embedded primes of I. Given any other reduced primary decompostion $I = Q'_1 \cap \ldots \cap Q'_m$ with $P_i = \sqrt{Q'_i}$, then $Q'_i = Q_i$ for $1 \leq i \leq k$.

Proof. Given an isolated prime P_i, let $r \in (\bigcap_{j \neq i} P_j) \setminus P_i$. Such an r exists, for, if P_i contained $\bigcap_{j \neq i} P_j$, it would contain some P_j with $j \neq i$, contrary to assumption. Let $n \in \mathbb{N}$ such that $r^n \in \bigcap_{j \neq i} Q_j$ as well as $r^n \in \bigcap_{j \neq i} Q'_j$. By 10.33,

$$(I : r^n) = \bigcap_{j=1}^{m} (Q_j : r^n) = (Q_i : r^n) = Q_i$$

and by the same token, $(I : r^n) = Q'_i$. $\square$