3 Minimal primary decomposition.

3.1 Radical of an ideal.

Definition 3.1. *Let R be a ring, let $\mathfrak{a} \lhd R$. The* ***radical*** *of the ideal $\mathfrak{a}$ is defined to be*

$$\operatorname{rad} \mathfrak{a} = \{r \in R \mid \exists n \in \mathbb{N}\, r^n \in \mathfrak{a}\}.$$

Remark 3.2. Let R be a ring, let $\mathfrak{a} \lhd R$. Then $\operatorname{rad} \mathfrak{a}$ is an ideal.

Proof. Fix $a, b \in \operatorname{rad} \mathfrak{a}$. Then $a^n \in \mathfrak{a}$ and $b^m \in \mathfrak{a}$, for some $n, m \in \mathbb{N}$. But then

$$\begin{aligned}(a-b)^{n+m-1} &= a^n a^{m-1} + \binom{n+m-1}{1} a^n a^{m-1} b + \ldots + \binom{n+m-1}{m-1} a^n b^{m-1} \\ &+ \binom{n+m-1}{m} a^{n-1} b^m + \binom{n+m-1}{m+1} a^{n-2} b^m b + \ldots + b^{n-1} b^m \in \mathfrak{a},\end{aligned}$$

which means $a - b \in \operatorname{rad} \mathfrak{a}$. Moreover, if $r \in R$, then

$$(ra)^n = r^n a^n \in \mathfrak{a},$$

that is $ra \in \operatorname{rad} \mathfrak{a}$. □

Remark 3.3. Let R be a ring, let $\mathfrak{a}, \mathfrak{b} \lhd R$.

1. $\mathfrak{a} \subseteq \operatorname{rad} \mathfrak{a}$,
2. $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \operatorname{rad} \mathfrak{a} \subseteq \operatorname{rad} \mathfrak{b}$,
3. $\operatorname{rad}(\operatorname{rad} \mathfrak{a}) = \operatorname{rad} \mathfrak{a}$,
4. $\operatorname{rad} \mathfrak{a} \cdot \mathfrak{b} = \operatorname{rad} \mathfrak{a} \cap \mathfrak{b}$,
5. $\operatorname{rad} \mathfrak{a} \cap \mathfrak{b} = \operatorname{rad} \mathfrak{a} \cap \operatorname{rad} \mathfrak{b}$,
6. $\operatorname{rad} \mathfrak{a} = (1) \Leftrightarrow \mathfrak{a} = (1)$,
7. $\operatorname{rad} \mathfrak{a} + \mathfrak{b} = \operatorname{rad}(\operatorname{rad} \mathfrak{a} + \operatorname{rad} \mathfrak{b})$,
8. $\mathfrak{a} + \mathfrak{b} = (1) \Leftrightarrow \operatorname{rad} \mathfrak{a} + \operatorname{rad} \mathfrak{b} = (1)$.

Proof. 1. and 2. follow directly from the definiton of a radical.

For the proof of 3., fix $a \in \operatorname{rad}(\operatorname{rad} \mathfrak{a})$. Then $a^n \in \operatorname{rad} \mathfrak{a}$, for some $n \in \mathbb{N}$. But then $a^{nm} = (a^n)^m \in \mathfrak{a}$, for some $m \in \mathbb{N}$, that is $a \in \operatorname{rad} \mathfrak{a}$.

In order to prove 4., as $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, in view of 2. also $\operatorname{rad} \mathfrak{a} \cdot \mathfrak{b} \subseteq \operatorname{rad} \mathfrak{a} \cap \operatorname{rad} \mathfrak{b}$ and it suffices to show the other inclusion. Fix $a \in \operatorname{rad} \mathfrak{a} \cap \mathfrak{b}$. Thus $a^n \in \mathfrak{a} \cap \mathfrak{b}$, for some $n \in \mathbb{N}$, and, consequently, $a^{2n} = a^n a^n \in \mathfrak{a} \cdot \mathfrak{b}$.

To show 5., since $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ and $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{b}$, by 2. $\operatorname{rad} \mathfrak{a} \cap \mathfrak{b} \subseteq \operatorname{rad} \mathfrak{a}$ and $\operatorname{rad} \mathfrak{a} \cap \mathfrak{b} \subseteq \operatorname{rad} \mathfrak{b}$, so it suffices to show the other inclusion. Fix $a \in \operatorname{rad} \mathfrak{a} \cap \operatorname{rad} \mathfrak{b}$. Then $a^n \in \mathfrak{a}$ and $a^m \in \mathfrak{b}$, for some $n, m \in \mathbb{N}$. Hence $a^{n+m} = a^n a^m \in \mathfrak{a} \cap \mathfrak{b}$, so that $a \in \operatorname{rad} \mathfrak{a} \cap \mathfrak{b}$.

6. is clear, since $1 \in \operatorname{rad} \mathfrak{a} \Leftrightarrow 1 = 1^n \in \mathfrak{a}$.

To show 6. notice that, as $\mathfrak{a}+\mathfrak{b}=(\mathfrak{a}\cup\mathfrak{b})\subseteq(\operatorname{rad}\mathfrak{a}\cup\operatorname{rad}\mathfrak{b})=\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b}$, one inclusion follows from 2., and it suffices to justify the other one. Fix $a\in\operatorname{rad}(\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b})$. Then $a^n\in\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b}$, for some $n\in\mathbb{N}$. Hence $a^n=b+c$ with $b\in\operatorname{rad}\mathfrak{a}$ and $c\in\operatorname{rad}\mathfrak{b}$, that is $b^k\in\mathfrak{a}$ and $c^l\in\mathfrak{b}$, for some $k,l\in\mathbb{N}$. Therefore $a^{n(k+l)}=(a^n)^{k+l}=(b+c)^{k+l}=b^kx+c^ly$, for some $x,y\in R$, that is $a^{n(k+l)}\in\mathfrak{a}+\mathfrak{b}$ and, as a result, $a\in\operatorname{rad}(\mathfrak{a}+\mathfrak{b})$.

Finally, for the proof of 7. firstly observe, that if $1\in\mathfrak{a}+\mathfrak{b}$ then, by 1. also $1\in\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b}$. Conversely, if $1\in\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b}$ then, by 1. and 7., $1\in\operatorname{rad}(\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b})=\operatorname{rad}\mathfrak{a}+\operatorname{rad}\mathfrak{b}$. Therefore, by 6., $1\in\mathfrak{a}+\mathfrak{b}$. □

Remark 3.4. Let R be a ring, let $\mathfrak{p}\lhd R$ be a prime ideal, let $m\in\mathbb{N}$. Then $\operatorname{rad}\mathfrak{p}^m=\mathfrak{p}$.

Proof. Fix $a\in\operatorname{rad}\mathfrak{p}^m$. Then $a^n\in\mathfrak{p}^m$, for some $n\in\mathbb{N}$, and since $\mathfrak{p}\supseteq\mathfrak{p}^2\supseteq\ldots\supseteq\mathfrak{p}^m$ it follows that $a^n\in\mathfrak{p}$. But as $\mathfrak{p}$ is a prime ideal, this implies $a\in\mathfrak{p}$.

Conversely, fix $a\in\mathfrak{p}$. Then $a^m\in\mathfrak{p}^m$, so that $a\in\operatorname{rad}\mathfrak{p}$. □

Definition 3.5. *Let R be a ring. The set of all nilpotent elements of R:*

$$\operatorname{Nil}R=\{a\in R|\,\exists n\in\mathbb{N}\,a^n=0\}$$

is called the ***nilradical*** *of R.*

Remark 3.6. Let R be a ring. Then $\operatorname{Nil}R\lhd R$.

Proof. Let $a,b\in\operatorname{Nil}R$. Then $a^n=0$ and $b^m=0$, for some $n,m\in\mathbb{N}$. Consequently

$$\begin{aligned}(a+b)^{n+m} &= a^na^m+\binom{n+m}{1}a^na^{m-1}b+\ldots+\binom{n+m}{m}a^nb^m\\ &+ \binom{n+m}{m+1}a^{n-1}b^mb+\ldots+b^nb^m\\ &= 0,\end{aligned}$$

so that $a+b\in\operatorname{Nil}R$. Clearly, for $r\in R$, also $(ra)^n=r^na^n=0$, hence $ra\in\operatorname{Nil}R$. □

Proposition 3.7. *Let R be a ring. Then*

$$\operatorname{Nil}R=\bigcap\{\mathfrak{p}|\,\mathfrak{p}\in\operatorname{Spec}R\}.$$

Proof. Denote $A=\bigcap\{\mathfrak{p}|\,\mathfrak{p}\in\operatorname{Spec}R\}$. Fix $a\in\operatorname{Nil}R$, and in order to show that $a\in A$, fix a prime ideal $\mathfrak{p}\lhd R$. As $a^n=0$, for some $n\in\mathbb{N}$, this implies that $a^n=a^{n-1}a=0\in\mathfrak{p}$. Since $\mathfrak{p}$ is prime, either $a\in\mathfrak{p}$, or $a^{n-1}\in\mathfrak{p}$ – in the latter case a simple inductive argument follows.

For the other inclusion fix $a\in R$ and assume $a\notin\operatorname{Nil}R$. Thus $a^n\neq 0$, for all $n\in\mathbb{N}$. Let

$$\mathcal{R}=\{\mathfrak{a}\lhd R|\,a^n\notin\mathfrak{a},\ \text{for all } n\in\mathbb{N}\}.$$

By our assumption, $(0)\in\mathcal{R}$. One also easily verifies that if $\mathcal{L}$ is a chain of ideals from $\mathcal{L}$, then also $\bigcup\mathcal{L}\in\mathcal{R}$. Thus, by Zorn's Lemma, the family $\mathcal{R}$ has a maximal element $\mathfrak{p}$.

We shall show that $\mathfrak{p}$ is a prime ideal. Fix $x,y\in R$ and assume that both $x\notin\mathfrak{p}$ and $y\notin\mathfrak{p}$. Then

$$\mathfrak{p}\subsetneq\mathfrak{p}+(x)\qquad\text{and}\qquad\mathfrak{p}\subsetneq\mathfrak{p}+(y),$$

which, by the maximality of $\mathfrak{p}$, means that $\mathfrak{p}+(x), \mathfrak{p}+(y) \notin \mathcal{R}$, that is, for some $n, m \in \mathbb{N}$:

$$a^n \in \mathfrak{p}+(x) \qquad \text{and} \qquad a^m \in \mathfrak{p}+(y).$$

But then

$$a^{n+m} \in (\mathfrak{p}+(x))\cdot(\mathfrak{p}+(y)) = \mathfrak{p}^2 + \mathfrak{p}\cdot(x) + \mathfrak{p}\cdot(y) + (xy).$$

Since $\mathfrak{p}^2 + \mathfrak{p}\cdot(x) + \mathfrak{p}\cdot(y) \subseteq \mathfrak{p}$ this means $a^{n+m} \in \mathfrak{p}+(xy)$. Therefore $\mathfrak{p}+(xy) \notin \mathcal{R}$, and, in particular, $xy \notin \mathfrak{p}$ (for otherwise $\mathfrak{p}+(xy) = \mathfrak{p} \in \mathcal{R}$). This proves that $\mathfrak{p}$ is prime.

Now, $a^n \notin \mathfrak{p}$, for all $n \in \mathbb{N}$, and, in particular, $a \notin \mathfrak{p}$. This means $a \notin A$. □

Remark 3.8. Let R be a ring, let $\mathfrak{a} \lhd R$. If $\operatorname{rad} \mathfrak{a}$ is a maximal ideal, then $\mathfrak{a}$ is primary.

Proof. Let $\mathfrak{m} = \operatorname{rad} \mathfrak{a}$ be a maximal ideal and let $\kappa: R \to R / \mathfrak{a}$ be the canonical epimorphism. Then, for $a \in R$ and $n \in \mathbb{N}$:

$$(a+\mathfrak{a})^n = \bar{0} \in R / \mathfrak{a} \Leftrightarrow a^n \in \mathfrak{a} \Leftrightarrow a \in \mathfrak{m},$$

that is $\kappa(\mathfrak{m})$ equals the nilradical of $R / \mathfrak{a}$. Since $\operatorname{Nil} R / \mathfrak{a} = \bigcap \{\mathfrak{P} | \ \mathfrak{P} \in \operatorname{Spec} R / \mathfrak{a}\}$, it follows that $\kappa^{-1}(\mathfrak{P}) \lhd R$ and $\mathfrak{m} \subseteq \kappa^{-1}(\mathfrak{P})$, for $\mathfrak{P} \in \operatorname{Spec} R / \mathfrak{a}$. But, as $\mathfrak{m}$ is maximal, this, in fact, means $\mathfrak{m} = \kappa^{-1}(\mathfrak{P})$, for $\mathfrak{P} \in \operatorname{Spec} R / \mathfrak{a}$. Hence $R / \mathfrak{a}$ contains exactly one prime ideal, which is equal to $\operatorname{Nil} R / \mathfrak{a}$. Consequently, $R / \mathfrak{a}$ contains only one maximal ideal, namely $R / \mathfrak{a}$. Therefore every element of $R / \mathfrak{a}$ outside $\operatorname{Nil} R / \mathfrak{a}$ is a unit, for otherwise it would be contained in one of the maximal ideals of $R / \mathfrak{a}$. Thus every zero divisor of $R / \mathfrak{a}$ has to be nilpotent, and by Lemma 2.4.ii the ideal $\mathfrak{a}$ is primary. □

Lemma 3.9. *Let R be a ring, let $\mathfrak{q} \lhd R$ be a primary ideal. Then $\operatorname{rad} \mathfrak{q}$ is prime.*

Proof. Let $a, b \in R$ and assume that $ab \in \operatorname{rad} \mathfrak{q}$. Thus $a^n b^n = (ab)^n \in \mathfrak{q}$. If $a^n \in \mathfrak{q}$ then $a \in \operatorname{rad} \mathfrak{q}$. If $a^n \notin \mathfrak{q}$, then, as $\mathfrak{q}$ is primary, $b^{nm} = (b^n)^m \in \mathfrak{q}$, for some $m \in \mathbb{N}$. But then $b \in \operatorname{rad} \mathfrak{q}$. □

Definition 3.10. *Let R be a ring, let $\mathfrak{q} \lhd R$ be a primary ideal and let $\mathfrak{p} = \operatorname{rad} \mathfrak{q}$. Then $\mathfrak{q}$ is called* ***$\mathfrak{p}$-primary****.*

Remark 3.11. Let R be a ring, let $\mathfrak{m} \lhd R$ be a maximal ideal, let $m \in \mathbb{N}$. Then $\mathfrak{m}^m$ is $\mathfrak{m}$-primary.

Proof. Let $\mathfrak{m} \lhd R$ be a maximal ideal and let $m \in \mathbb{N}$. Then $\mathfrak{m}$ is also prime, and by Remark 3.4 $\operatorname{rad} \mathfrak{m}^m = \mathfrak{m}$ is a maximal ideal. But then, by Remark 3.8, it is primary. □

Lemma 3.12. *Let R be a ring, let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary. Then $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is $\mathfrak{p}$-primary.*

Proof. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary and denote $\mathfrak{q} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$. By Remark 3.3.5

$$\operatorname{rad} \mathfrak{q} = \operatorname{rad} \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \operatorname{rad} \mathfrak{q}_1 \cap \ldots \cap \operatorname{rad} \mathfrak{q}_n = \mathfrak{p} \cap \ldots \cap \mathfrak{p} = \mathfrak{p},$$

and it remains to show that $\mathfrak{q}$ is primary. Let $a, b \in R$ and assume $ab \in \mathfrak{q}$ with $b \notin \mathfrak{q}$. In particular, $b \notin \mathfrak{q}_{i_0}$ for some $i_0 \in \{1, \ldots, n\}$. At the same time, $ab \in \mathfrak{q}_{i_0}$ and $\mathfrak{q}_{i_0}$ is primary, so that $a^k \in \mathfrak{q}_{i_0}$, for some $k \in \mathbb{N}$. Thus $a \in \operatorname{rad} \mathfrak{q}_{i_0} = \mathfrak{p}$. But we have already shown that $\mathfrak{p} = \operatorname{rad} \mathfrak{q}$, so that $a^m \in \mathfrak{q}$ for some $m \in \mathbb{N}$. This proves that $\mathfrak{q}$ is primary. □

3.2 Minimal primary decomposition.

Definition 3.13. *Let R be a ring, let $\mathfrak{a} \lhd R$ be a proper ideal and let*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$$

be a primary decomposition of $\mathfrak{a}$. If

$$\mathfrak{q}_j \not\supseteq \bigcap_{i \neq j} \mathfrak{q}_i$$

and

$$\operatorname{rad} \mathfrak{q}_i \neq \operatorname{rad} \mathfrak{q}_j \text{ for } i \neq j,$$

then the primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is called ***minimal****.*

Theorem 3.14. (Noether-Lasker) *Let R be a Noetherian ring, let $\mathfrak{a} \lhd R$ be a proper ideal. Then $\mathfrak{q}$ has a minimal primary decomposition and the prime ideals $\mathfrak{p}_i = \operatorname{rad} \mathfrak{q}_i$ are uniquely determined up to the order.*