2 Primary decomposition.

2.1 Primary decomposition.

Remark 2.1. Consider the ring $\mathbb{Z}$ and an element $n \in \mathbb{Z}$. Then there exist uniquely determined prime numbers $p_1, \ldots, p_m$ and exponents $k_1, \ldots, k_m \in \mathbb{N}$ such that

$$n = \pm p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$$

or, equivalently:

$$(n) = (p_1^{k_1}) \cdot \ldots \cdot (p_m^{k_m}) = (p_1^{k_1}) \cap \ldots \cap (p_m^{k_m}).$$

Definition 2.2. *Let R be any ring. An ideal $\mathfrak{q} \lhd R$ is called **primary**, if $\mathfrak{q} \neq R$ and for all $a, b \in R$*

$$a b \in \mathfrak{q} \wedge b \notin \mathfrak{q} \Rightarrow \exists n \in \mathbb{N} \quad a^n \in \mathfrak{q}.$$

Example 2.3.

1. Every prime ideal is primary.

2. An ideal in $\mathbb{Z}$ generated by a power of a prime number is primary.

3. Let R be a principal ideal domain. Then $\mathfrak{q}$ is primary if and only if $\mathfrak{q} = \mathfrak{p}^n$, for a prime ideal $\mathfrak{p}$.

Proof. 1. and 2. are obvious. In order to show 3., assume that $\mathfrak{q} = \mathfrak{p}^n$. As R is a PID, it follows that $\mathfrak{p} = (p)$, for some prime element $p \in R$. Consequently, $\mathfrak{q} = (p)^n = (p^n)$. Say $a \cdot b \in \mathfrak{q} = (p^n)$ with $b \notin \mathfrak{q} = (p^n)$, for some $a, b \in R$. Then $p^n | a \cdot b$ and $p^n \nmid b$. As a PID, R is a unique factorization domain, so that it follows $p | a$, and, consequently, $p^n | a$, that is $a^n \in \mathfrak{q}$.

Conversely, assume that $\mathfrak{q}$ is primary. Let $\mathfrak{q} = (c)$, for some $c \in R$. Suppose that $c \neq u \cdot p^n$, for all units $u \in U(R)$, all prime elements $p \in R$, and all $n \in \mathbb{N}$. Then, by unique factorization, c is divisible by two different prime elements, say p and q. Let $c = a \cdot b$ with $p | a$ and $q | b$. Then $c | a \cdot b$ and $c \nmid b$, but also $c \nmid a^n$, for all $n \in \mathbb{N}$, which means that $\mathfrak{q} = (c)$ is not primary – a contradiction. □

Lemma 2.4. *Let R be a ring, let $\mathfrak{q} \lhd R$ be a proper ideal in R. The following conditions are equivalent:*

i. $\mathfrak{q}$ *is primary,*

ii. every zero divisor in $R/\mathfrak{q}$ is nilpotent,

iii. the zero ideal in $R/\mathfrak{q}$ is primary.

Proof. It suffices to notice that $\mathfrak{q}$ being primary is equivalent to the following condition in $R/\mathfrak{q}$:

$$(a + \mathfrak{q}) \cdot (b + \mathfrak{q}) = \mathfrak{q} \wedge a + \mathfrak{q} \neq \mathfrak{q} \Rightarrow \exists n \in \mathbb{N}\ (a + \mathfrak{q})^n = \mathfrak{q}.$$ □

Example 2.5. The ideal $(x, y^2) \lhd k[x, y]$, where k is any field, is primary, but is not a power of a prime ideal.

Proof. Observe that every polynomial $f(x,y)\in k[x,y]$ can be written as

$$f(x,y)=x\cdot g(x,y)+h(y)=x\cdot g(x,y)+y^2\cdot h_1(y)+a\cdot y+b,$$

with $g(x,y)\in k[x,y]$, $h(y),h_1(y)\in k[y]$ and $a,b\in k$. It then follows that the map

$$k[x,y]/\mathfrak{q}\to k[y]/(y^2),\qquad f(x,y)+\mathfrak{q}\mapsto a\cdot y+b+(y^2)$$

is a well-defined ring isomorphism, so that $k[x,y]/\mathfrak{q}\cong k[y]/(y^2)$.

In order to show that $\mathfrak{q}$ is primary, we note that $k[y]$ is a PID, and y is a prime element of $k[y]$, so that, by Example 2.3.3 the ideal (y^2) is primary. Thus, by Lemma 2.4.iii, the zero ideal in the ring $k[y]/(y^2)$ is primary, and so is the zero ideal in the isomorphic ring $k[x,y]/\mathfrak{q}$, leading to $\mathfrak{q}$ being primary.

We proceed to show that $\mathfrak{q}$ is not a power of a prime ideal. Firstly, $\mathfrak{q}$ is not prime itself, as the ring $k[x,\ y]/\mathfrak{q}$ is not a domain: the isomorphic ring $k[y]/(y^2)$ has zero divisors, for example $(y+(y^2))^2=(y^2)$. Secondly, suppose that $\mathfrak{q}=\mathfrak{p}^n$, for some prime ideal $\mathfrak{p}\lhd k[x,y]$. Since

$$(x,y^2)=\mathfrak{q}=\mathfrak{p}^n\subseteq\mathfrak{p},$$

it follows that $x,y^2\in\mathfrak{p}$. As $\mathfrak{p}$ is prime, also $y\in\mathfrak{p}$. Consequently, $(x,y)\subseteq\mathfrak{p}$, but as (x,y) is maximal, it follows $(x,y)=\mathfrak{p}$. Thus $\mathfrak{q}=\mathfrak{p}^n=(x,y)^n$. On the other hand

$$(x,y)^2\subsetneq\mathfrak{q}\subsetneq(x,y),$$

which yields a contradiction. $\square$

Definition 2.6. *Let R be a ring. An ideal $\mathfrak{n}\lhd R$, $0\neq\mathfrak{n}$ is* ***irreducible*** *if, for all $\mathfrak{a},\mathfrak{b}\lhd R$*

$$\mathfrak{n}=\mathfrak{a}\cap\mathfrak{b}\Rightarrow\mathfrak{n}=\mathfrak{a}\vee\mathfrak{n}=\mathfrak{b}.$$

Example 2.7.

1. Every maximal ideal is irreducible.
2. Every prime ideal is irreducible.
3. An ideal $\mathfrak{n}\lhd R$ is irreducible if and only if the zero ideal in $R/\mathfrak{n}$ is irreducible.

Proof. 1. is obvious. For the proof of 2., suppose that $\mathfrak{p}$ is a prime ideal of a ring R such that $\mathfrak{p}=\mathfrak{a}\cap\mathfrak{b}$, for some $\mathfrak{a},\mathfrak{b}\lhd R$, with $\mathfrak{p}\subsetneq\mathfrak{a}$ and $\mathfrak{p}\subsetneq\mathfrak{b}$. Then there exist $a\in\mathfrak{a}\setminus\mathfrak{p}$ and $b\in\mathfrak{b}\setminus\mathfrak{p}$. Clearly $a\cdot b\in\mathfrak{p}$ implying $a\in\mathfrak{a}$ or $b\in\mathfrak{p}$, which yields a contradiction.

In order to show 3., assume that $\mathfrak{n}$ is an irreducible ideal of a ring R. Let

$$(\mathfrak{n})=\mathfrak{A}\cap\mathfrak{B},$$

for some ideals $\mathfrak{A}$, $\mathfrak{B}\lhd R/\mathfrak{n}$. Let $\mathfrak{a}=\kappa^{-1}(\mathfrak{A})$ and $\mathfrak{b}=\kappa^{-1}(\mathfrak{B})$, where κ denotes the canonical epimorphism $\kappa\colon R\to R/\mathfrak{n}$, $a\overset{\kappa}{\longmapsto}a+\mathfrak{n}$. Then

$$\mathfrak{n}=\kappa^{-1}((\mathfrak{n}))=\kappa^{-1}(\mathfrak{A})\cap\kappa^{-1}(\mathfrak{B})=\mathfrak{a}\cap\mathfrak{b}.$$

As $\mathfrak{n}$ is irreducible, either $\mathfrak{n}=\mathfrak{a}$ or $\mathfrak{n}=\mathfrak{b}$, which leads to $(\mathfrak{n})=\mathfrak{A}$ or $(\mathfrak{n})=\mathfrak{B}$.

Conversely, assume that $(\mathfrak{n})$ is an irreducible ideal in $R/\mathfrak{n}$. Let

$$\mathfrak{n}=\mathfrak{a}\cap\mathfrak{b},$$

for some ideals $\mathfrak{a},\mathfrak{b}\lhd R$. Let $\mathfrak{A}=\kappa(\mathfrak{a})$ and $\mathfrak{B}=\kappa(\mathfrak{b})$. Then

$$(\mathfrak{n})=\kappa(\mathfrak{n})=\kappa(\mathfrak{a}\cap\mathfrak{b})=\kappa(\mathfrak{a})\cap\kappa(\mathfrak{b})=\mathfrak{A}\cap\mathfrak{B};$$

indeed, clearly $\kappa(\mathfrak{a}\cap\mathfrak{b})\subset\kappa(\mathfrak{a})\cap\kappa(\mathfrak{b})$, and for the other inclusion fix $\overline{y}\in\kappa(\mathfrak{a})\cap\kappa(\mathfrak{b})$. Thus $\overline{y}=\kappa(a)$, for some $a\in\mathfrak{a}$, and $\overline{y}=\kappa(b)$, for some $b\in\mathfrak{b}$. Hence $a-b\in\ker\kappa=\mathfrak{n}$, so that $a=b+n$, for some $n\in\mathfrak{n}$, but as $\mathfrak{n}\subseteq\mathfrak{b}$, this yields $a\in\mathfrak{b}$ and, consequently, $a\in\mathfrak{a}\cap\mathfrak{b}$.

Now, by irreducibility of $(\mathfrak{n})$, we either get $(\mathfrak{n})=\mathfrak{A}$, leading to $\mathfrak{n}=\mathfrak{a}$, or $(\mathfrak{n})=\mathfrak{B}$, leading to $\mathfrak{n}=\mathfrak{b}$. $\square$

Lemma 2.8. *Let R be Noetherian. Every irreducible ideal in R is primary.*

Proof. Let $\mathfrak{n}$ be an irreducible ideal in a Noetherian ring R. By Lemma 2.4.2 it suffices to show that in the ring $A/\mathfrak{n}$ every zero divisor is nilpotent. Let $\bar{x},\bar{y}\in R/\mathfrak{n}$ be such that $\bar{x}\bar{y}=\bar{0}$ with $\bar{y}\neq\bar{0}$. For $\bar{t}\in R/\mathfrak{n}$ let

$$\operatorname{Ann}\bar{t}=\{\bar{z}\in R/\mathfrak{n}|\ \bar{z}\bar{t}=0\}.$$

One easily checks that $\operatorname{Ann}\bar{t}\lhd R/\mathfrak{n}$, and thus

$$\operatorname{Ann}\bar{x}\subseteq\operatorname{Ann}\bar{x}^2\subseteq\ldots\subseteq\operatorname{Ann}\bar{x}^n\subseteq\ldots$$

is an ascending chain of ideals. Since R is Noetherian, so is $R/\mathfrak{n}$, and hence there exists $n\in\mathbb{N}$ such that

$$\operatorname{Ann}\bar{x}^n=\operatorname{Ann}\bar{x}^{n+1}=\ldots.$$

We claim that $(\bar{x}^n)\cap(\bar{y})=(\bar{0})$. Indeed, let $\bar{a}\in(\bar{x}^n)\cap(\bar{y})$. Then $\bar{a}=\bar{b}\,\bar{x}^n$ and $\bar{a}=\bar{c}\,\bar{y}$, for some $\bar{b}$, $\bar{c}\in R/\mathfrak{n}$. Hence

$$\bar{b}\bar{x}^{n+1}=\bar{b}\bar{x}^n\bar{x}=\bar{a}\bar{x}=\bar{c}\bar{y}\bar{x}=\bar{c}\bar{0}=\bar{0},$$

so that $\bar{b}\in\operatorname{Ann}\bar{x}^{n+1}=\operatorname{Ann}\bar{x}^n$ and, consequently, $\bar{a}=\bar{b}\bar{x}^n=\bar{0}$. This proves the claim.

By Example 2.7.3 the zero ideal of $R/\mathfrak{n}$ is irreducible. Thus, by the above claim, $(\bar{x}^n)=(\bar{0})$, as $\bar{y}\in(\bar{y})$ and $\bar{y}\neq\bar{0}$. Therefore $\bar{x}^n=\bar{0}$, that is $\bar{x}$ is nilpotent. $\square$

Lemma 2.9. *Let R be Noetherian, let $\mathfrak{a}\lhd R$ be a proper ideal. Then $\mathfrak{a}$ is an intersection of a finite number of irreducible ideals.*

Proof. Suppose that there exists a nonempty family $\mathcal{R}$ of proper ideals that are not intersections of finite numbers of irreducible ideals. Since R is Noetherian, the family $\mathcal{R}$ contains a maximal element $\mathfrak{c}$. In particular, $\mathfrak{c}$ is not irreducible. Let $a,b\in R$ with $a,b\notin\mathfrak{c}$ and let $\mathfrak{a}=\mathfrak{c}+(a)$ and $\mathfrak{b}=\mathfrak{c}+(b)$. Then

$$\mathfrak{c}=\mathfrak{a}\cap\mathfrak{b},\qquad\mathfrak{c}\subsetneq\mathfrak{a},\qquad\mathfrak{c}\subsetneq\mathfrak{b},$$

which means that $\mathfrak{a}$, $\mathfrak{b}\notin\mathcal{R}$. Thus both $\mathfrak{a}$ and $\mathfrak{b}$ are intersections of finite numbers of irreducible ideals, and so is $\mathfrak{c}$ – a contradiction. $\square$

Theorem 2.10. *Let R be Noetherian, let $\mathfrak{a}\lhd R$ be a proper ideal. Then $\mathfrak{a}$ is an intersection of a finite number of primary ideals.*

Proof. By Lemma 2.9 every ideal is an intersection of a finite number of irreducible ideals, and by Lemma 2.8 every irreducible ideal in R is primary. $\square$

2.2 Radical of an ideal.

Definition 2.11. *Let R be a ring, let $\mathfrak{a}\lhd R$. The **radical** of the ideal $\mathfrak{a}$ is defined to be*

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

Remark 2.12. Let R be a ring, let $\mathfrak{a}\lhd R$. Then $\mathrm{rad}\,\mathfrak{a}$ is an ideal.

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

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

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

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

that is $ra\in\mathrm{rad}\,\mathfrak{a}$. $\square$

Remark 2.13. Let R be a ring, let $\mathfrak{a},\mathfrak{b}\lhd R$.

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

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

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

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

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

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

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 2.14. 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 2.15. *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 2.16. 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 2.17. *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 $a^n\neq0$, 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 2.18. 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 2.19. *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 2.20. *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 2.21. 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 2.14 $\operatorname{rad} \mathfrak{m}^m = \mathfrak{m}$ is a maximal ideal. But then, by Remark 2.18, it is primary. □

Lemma 2.22. *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 2.13.5

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

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. □

Definition 2.23. *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

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

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

Theorem 2.24. (Noether-Lasker) *Let R be a Noetherian ring, let $\mathfrak{a} \triangleleft R$ 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.*