8. Prime Factorization and Primary Decompositions

When it comes to actual computations, Euclidean domains (or more generally principal ideal domains) are probably the "nicest" rings that are not fields. One of the main reasons for this is that their elements admit a unique prime factorization [G1, Proposition 11.9]. This allows for an easy computation of many concepts in commutative algebra, such as e. g. the operations on ideals in Example 1.4.

Unfortunately however, such rings are rather rare in practice, with the integers $\mathbb{Z}$ and the polynomial ring $K[x]$ over a field K being the most prominent examples. So we now want to study in this chapter if there are more general rings that allow a prime factorization of their elements, and what we can use as a substitute in rings that do not admit such a factorization.

More precisely, given an element $a \neq 0$ in an integral domain R which is not a unit we ask if we can write $a = p_1 \cdot \cdots \cdot p_n$ for some $n \in \mathbb{N}_{>0}$ and $p_1, \ldots, p_n \in R$ such that:

- The p_i for $i = 1, \ldots, n$ are *irreducible* or *prime* — recall that in a principal ideal domain these two notions are equivalent, but in a general integral domain we only know that every prime element is irreducible [G1, Lemma 11.3 and Proposition 11.5].
- The decomposition is unique up to permutation and multiplication with units, i. e. if we also have $a = q_1 \cdot \cdots \cdot q_m$ with $q_1, \ldots, q_m$ irreducible resp. prime, then $m = n$ and there are units $c_1, \ldots, c_n \in R$ and a permutation $\sigma \in S_n$ such that $q_i = c_i\, p_{\sigma(i)}$ for all $i = 1, \ldots, n$.

Let us first discuss the precise relation between the different variants of these conditions.

Proposition and Definition 8.1 (Unique factorization domains)**.** *For an integral domain R the following statements are equivalent:*

(a) *Every non-zero non-unit of R is a product of prime elements.*

(b) *Every non-zero non-unit of R is a product of irreducible elements, and this decomposition is unique up to permutation and multiplication with units.*

(c) *Every non-zero non-unit of R is a product of irreducible elements, and every irreducible element is prime.*

If these conditions hold, R is called ***factorial*** *or a* ***unique factorization domain*** *(short:* ***UFD****).*

13

Proof.

(a) $\Rightarrow$ (b): Let $a \in R$ be a non-zero non-unit. By assumption we know that $a = p_1 \cdot \cdots \cdot p_n$ for some prime elements $p_1, \ldots, p_n$. As prime elements are irreducible [G1, Lemma 11.3], we therefore also have a decomposition into irreducible elements.

Moreover, let $a = q_1 \cdot \cdots \cdot q_m$ be another decomposition into irreducible elements. Then p_1 divides $a = q_1 \cdot \cdots \cdot q_m$, and as p_1 is prime this means that p_1 divides one of these factors, without loss of generality $p_1 \,|\, q_1$. Hence $q_1 = c\, p_1$ for some $c \in R$. But q_1 is irreducible and p_1 is not a unit, so c must be a unit. This means that p_1 and q_1 agree up to multiplication with a unit. Canceling p_1 in the equation $p_1 \cdot \cdots \cdot p_n = q_1 \cdot \cdots \cdot q_m$ by p_1 now yields $p_2 \cdot \cdots \cdot p_n = c \cdot q_2 \cdot \cdots \cdot q_m$, and continuing with this equation in the same way for $p_2, \ldots, p_n$ gives the desired uniqueness statement.

(b) $\Rightarrow$ (c): Let $p \in R$ be irreducible, we have to show that p is prime. So let $p \,|\, ab$, i. e. $ab = pc$ for some $c \in R$. By assumption we can write all these four elements as products of irreducible elements and thus obtain an equation

$$a_1 \cdot \cdots \cdot a_n \cdot b_1 \cdot \cdots \cdot b_m = p \cdot c_1 \cdot \cdots \cdot c_r.$$

But by the uniqueness assumption, the factor p on the right must up to a unit be one of the $a_1,\dots,a_n$ or $b_1,\dots,b_m$, which implies that $p \mid a$ or $p \mid b$.

(c) $\Rightarrow$ (a) is trivial. □

Remark 8.2. In Proposition 8.1, the assumption in (b) and (c) that every non-zero non-unit can be written as a product of irreducible elements is a very weak one: it is satisfied e. g. in every Noetherian domain by Exercise 7.22 (a). The other conditions are much stronger, as we will see in Examples 8.3 (b) and 8.7.

Example 8.3. The following two examples are already known from the "Algebraic Structures" class:

(a) As mentioned above, principal ideal domains (so in particular $\mathbb{Z}$ and univariate polynomial rings over a field) are unique factorization domains [G1, Proposition 11.9].

(b) In the ring $R = \mathbb{Z}[\sqrt{5}i] \subset \mathbb{C}$ the element 2 obviously divides $6 = (1+\sqrt{5}i)(1-\sqrt{5}i)$, but neither $1+\sqrt{5}i$ nor $1-\sqrt{5}i$. Hence 2 is not prime. But one can show that 2 is irreducible in R, and thus R is not a unique factorization domain [G1, Example 11.4]. In fact, $2 \cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$ are two decompositions of the same number 6 that do not agree up to permutation and units.

It follows by (a) that R cannot be a principal ideal domain. One can also check this directly: the ideal $(2, 1+\sqrt{5}i)$ is not principal [G1, Exercise 10.38]. In fact, we will see in Example 13.28 that up to multiplication with a constant this is the only non-principal ideal in R.

We will see in Example 13.8 however that R admits a "unique prime factorization" for ideals (instead of for elements) — a property that holds more generally in so-called Dedekind domains that we will study in Chapter 13.

Remark 8.4. The most important feature of the unique factorization property is that it is preserved when passing from a domain R to the polynomial ring $R[x]$. Often this is already shown in the "Introduction to Algebra" class, and so we will only sketch the proof of this statement here. It relies on the well-known *Lemma of Gauß* stating that an irreducible polynomial over $\mathbb{Z}$ (or more generally over a unique factorization domain R) remains irreducible when considered as a polynomial over $\mathbb{Q}$ (resp. the quotient field $K = \operatorname{Quot} R$). More precisely, if $f \in R[x]$ is reducible in $K[x]$ and factors as $f = gh$ with non-constant $g, h \in K[x]$, then there is an element $c \in K \setminus \{0\}$ such that cg and $\frac{h}{c}$ lie in $R[x]$, and so $f = (cg) \cdot \frac{h}{c}$ is already reducible in $R[x]$ [G3, Proposition 3.2 and Remark 3.3].

Proposition 8.5. *If R is a unique factorization domain, then so is $R[x]$.*

Proof sketch. We will check condition (c) of Definition 8.1 for $R[x]$.

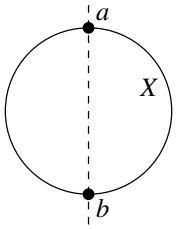
Let $f \in R[x]$, and let c be a greatest common divisor of all coefficients of f. Then $f = cf'$ for some polynomial $f' \in R[x]$ with coefficients whose greatest common divisor is 1, so that no constant polynomial which is not a unit can divide f'. Now split f' into factors until all of them are irreducible — this process has to stop for degree reasons as we have just seen that the degree of each factor must be at least 1. But c can also be written as a product of irreducible elements since R is a unique factorization domain, and so $f = cf'$ is a product of irreducible elements as well.

Next assume that f is irreducible, in particular we may assume that $c = 1$. We have to show that f is also prime. So let f divide gh for some $g, h \in R[x]$. If we denote by K the quotient field of R, then f is also irreducible in $K[x]$ by Remark 8.4, hence prime in $K[x]$ by Example 8.3 (a), and so without loss of generality $f \mid g$ in $K[x]$. This means that $g = fk$ for some $k \in K[x]$. But now by Remark 8.4 we can find $\frac{a}{b} \in K$ (with a and b coprime) such that $\frac{a}{b} f$ and $\frac{b}{a} k$ are in $R[x]$. Since the greatest common divisor of the coefficients of f is 1 this is only possible if b is a unit. But then $k = ab^{-1}(\frac{b}{a}k) \in R[x]$, and so $f \mid g$ in $R[x]$. □

Remark 8.6. Of course, Proposition 8.5 implies by induction that $R[x_1,\dots,x_n] = R[x_1][x_2]\cdots[x_n]$ is a unique factorization domain if R is. In particular, the polynomial ring $K[x_1,\dots,x_n]$ over a field K is a unique factorization domain. This also shows that there are more unique factorization domains than principal ideal domains: as the ideal $(x_1,\dots,x_n)$ in $K[x_1,\dots,x_n]$ cannot be generated by fewer than n elements by Exercise 1.9, this polynomial ring is a principal ideal domain only for $n = 1$.

Example 8.7 (Geometric interpretation of prime and irreducible elements)**.** Consider the coordinate ring $R = \mathbb{R}[x,y]/(x^2+y^2-1)$ of the unit circle $X = V(x^2+y^2-1) \subset \mathbb{A}^2_{\mathbb{R}}$. Note that x^2+y^2-1 is obviously irreducible (it cannot be written as a product of two linear polynomials since otherwise X would have to be a union of two lines), and hence prime by Proposition 8.1 since $\mathbb{R}[x,y]$ is a unique factorization domain by Remark 8.6. So (x^2+y^2-1) is a prime ideal by Example 2.6 (a), and consequently R is an integral domain by Lemma 2.3 (a).

We are going to show that R is not a unique factorization domain. In fact, we will prove — and interpret geometrically — that $\bar{x} \in R$ is irreducible, but not prime. Note that the zero locus $V(\bar{x})$ of $\bar{x}$ in X consists of the two points $a = (0,1)$ and $b = (0,-1)$ shown in the picture on the right. In particular, $\bar{x}$ is neither 0 in R (otherwise $V(\bar{x})$ would be X) nor a unit (otherwise $V(\bar{x})$ would be empty).



(a) $\bar{x}$ is not prime: Geometrically, by Remark 2.7 (b) this is just the statement that $V(\bar{x})$ is not an irreducible variety since it consists of two points.

Algebraically, $\bar{x}$ divides $\bar{x}^2 = (1+\bar{y})(1-\bar{y})$ in R, but it does not divide $1 \pm \bar{y}$: if e. g. we had $\bar{x} \mid 1+\bar{y}$ this would mean $1+y = gx + h(x^2+y^2-1)$ for some $g,h \in \mathbb{R}[x,y]$, but plugging in the point a would then give the contradiction $2 = 0$.

(b) $\bar{x}$ is irreducible: otherwise we would have $\bar{x} = \overline{f}\,\overline{g}$ for two non-units $\overline{f}$ and $\overline{g}$ in R.

Intuitively, as the function $\bar{x}$ vanishes on X exactly at the two points a and b with multiplicity 1, this would mean that one of the two factors, say $\overline{f}$, would have to vanish exactly at a with multiplicity 1, and the other $\overline{g}$ exactly at b. But this would mean that the curve $V(f)$ in $\mathbb{A}^2_{\mathbb{R}}$ meets the circle X exactly at one point a with multiplicity 1. This seems geometrically impossible since the circle X has an outside and an inside, so if $V(f)$ crosses the circle and goes from the outside to the inside, it has to cross it again somewhere (as the dashed line in the picture above) since it cannot end in the interior of the circle.

To give an exact argument for this requires a bit more work. Note that every element $\overline{h} \in R$ has a unique representative of the form $h_0 + x h_1 \in \mathbb{R}[x,y]$ with $h_0, h_1 \in \mathbb{R}[y]$. We define a "norm" map

$$N : R \to \mathbb{R}[y],\ \ \overline{h} \mapsto h_0^2 + (y^2-1)\,h_1^2$$

which can also be thought of as taking the unique representative of $h(x,y) \cdot h(-x,y)$ not containing x. In particular, N is multiplicative (which can of course also be checked directly). Hence we have

$$(y+1)(y-1) = N(\bar{x}) = N(\overline{f})\,N(\overline{g}).$$

As $\mathbb{R}[y]$ is a unique factorization domain, there are now two possibilities (up to symmetry in $\overline{f}$ and $\overline{g}$):

- $N(\overline{f})$ is constant: Then $f_0^2 + (y^2-1)\,f_1^2$ is constant. But the leading coefficients of both f_0^2 and $(y^2-1)\,f_1^2$ are non-negative and thus cannot cancel in the sum, and hence we must have that f_0 is constant and $f_1 = 0$. But then $\overline{f}$ is a unit in R, which we excluded.
- $N(\overline{f}) = a\,(y-1)$ for some $a \in \mathbb{R}\setminus\{0\}$: Then $f_0^2 + (y^2-1)\,f_1^2 = a\,(y-1)$, and so we have $y-1 \mid f_0$. So we can write $f_0 = (y-1)\,f_0'$ for some polynomial $f_0' \in \mathbb{R}[y]$ and obtain $(y-1)\,f_0'^2 + (y+1)\,f_1^2 = a$. This is again a contradiction, since the left hand side must have a positive non-constant leading term.

Altogether, this contradiction shows that $\bar{x}$ is in fact irreducible.

Exercise 8.8. In contrast to Example 8.7, show that the following rings are unique factorization domains:

(a) the coordinate rings $\mathbb{R}[x,y]/(y-x^2)$ and $\mathbb{R}[x,y]/(xy-1)$ of the standard parabola and hyperbola in $\mathbb{A}^2_{\mathbb{R}}$, respectively;

(b) $\mathbb{C}[x,y]/(x^2+y^2-1)$.

We will also see in Proposition 12.14 "(e) $\Rightarrow$ (c)" that the localization of $\mathbb{R}[x,y]/(x^2+y^2-1)$ at the maximal ideal corresponding to one of the points a and b in Example 8.7 is a unique factorization domain. For the moment however we just note that the unique factorization property easily breaks down, and in addition is only defined for integral domains — so let us now study how the concept of prime factorization can be generalized to a bigger class of rings.

To see the idea how this can be done, let us consider Example 8.7 again. The function $\bar{x} \in R$ was not prime since its zero locus $V(\bar{x})$ was a union of two points. We could not decompose $\bar{x}$ as a product of two functions vanishing at only one of the points each, but we can certainly decompose the *ideal* $(\bar{x})$ into two maximal (and hence prime) ideals as

$$(\bar{x}) = I(a) \cap I(b) = (\bar{x}, \bar{y}-1) \cap (\bar{x}, \bar{y}+1),$$

which by Remark 1.12 is just the algebraic version of saying that $V(\bar{x})$ is the union of the two points a and b. So instead of elements we should rather decompose ideals of R, in the sense that we write them as intersections of "easier" ideals. (Note that in the above example we could also have taken the product of the two ideals instead of the intersection, but for general rings intersections turn out to be better-behaved, in particular under the presence of zero-divisors. Decompositions into products of maximal or prime ideals will be studied in Chapter 13, see e. g. Proposition 13.7 (b) and Example 13.12.)

To see what these "easier" ideals should be, consider the simple case of a principal ideal domain R: any non-zero ideal $I \trianglelefteq R$ can be written as $I = (p_1^{k_1} \cdot \dots \cdot p_n^{k_n})$ for some distinct prime elements $p_1, \dots, p_n \in R$ and $k_1, \dots, k_n \in \mathbb{N}_{>0}$ by Example 8.3 (a), and the "best possible" decomposition of this ideal as an intersection of easier ideals is

$$I = (p_1)^{k_1} \cap \dots \cap (p_n)^{k_n}.$$

So it seems that we are looking for decompositions of ideals as intersections of powers of prime ideals. Actually, whereas this is the correct notion for principal ideal domains, we need a slight variant of prime powers for the case of general rings:

Definition 8.9 (Primary ideals)**.** Let R be a ring. An ideal $Q \trianglelefteq R$ with $Q \neq R$ is called **primary** if for all $a, b \in R$ with $ab \in Q$ we have $a \in Q$ or $b^n \in Q$ for some $n \in \mathbb{N}$ (which is obviously equivalent to $a \in Q$ or $b \in \sqrt{Q}$).

Example 8.10 (Primary ideals = powers of prime ideals in principal ideal domains)**.** In a principal ideal domain R, the primary ideals are in fact exactly the ideals of the form (p^n) for a prime element $p \in R$ and $n \in \mathbb{N}_{>0}$:

- The ideal (p^n) is primary: if $ab \in (p^n)$ then $ab = cp^n$ for some $c \in R$. But now the n factors of p are either all contained in a (in which case $a \in (p^n)$), or at least one of them is contained in b (in which case $b^n \in (p^n)$).
- Conversely, let $I = (p_1^{k_1} \cdot \dots \cdot p_n^{k_n})$ be any primary ideal, where $p_1, \dots, p_n$ are distinct primes and $k_1, \dots, k_n \in \mathbb{N}_{>0}$. Then we must have $n = 1$, since otherwise $p_1^{k_1} \cdot (p_2^{k_2} \cdot \dots \cdot p_n^{k_n}) \in I$, but neither $p_1^{k_1}$ nor any power of $p_2^{k_2} \cdot \dots \cdot p_n^{k_n}$ are in I.

Note that if R is only a unique factorization domain the same argument still works for principal ideals — but not for arbitrary ideals as we will see in Example 8.13 (a).

Remark 8.11. Let R be a ring.

(a) Obviously, every prime ideal in R is primary, but the converse does not hold by Example 8.10.

(b) However, if $Q \trianglelefteq R$ is primary then $P = \sqrt{Q}$ is prime: if $ab \in P$ then $(ab)^n \in Q$ for some $n \in \mathbb{N}$. Hence $a^n \in Q$ or $b^n \in \sqrt{Q}$, which means that a or b lie in $\sqrt{Q} = P$. In fact, P is then the smallest prime ideal containing Q by Lemma 2.21.

If we want to specify the underlying prime ideal $P = \sqrt{Q}$ of a primary ideal Q we often say that Q is **P-primary**.

(c) The condition of an ideal $Q \trianglelefteq R$ with $Q \neq R$ being primary can also be expressed in terms of the quotient ring R/Q: obviously, Definition 8.9 translates into the requirement that $\overline{a}\,\overline{b} = 0$ implies $\overline{a} = 0$ or $\overline{b}^n = 0$ for some $n \in \mathbb{N}$. This means for every element $\overline{b}$ that $\overline{b}^n = 0$ for some $n \in \mathbb{N}$ if there is an $\overline{a} \neq 0$ with $\overline{a}\,\overline{b} = 0$. So Q is primary if and only if every zero-divisor of R/Q is nilpotent.

As in Corollary 2.4 this means that primary ideals are preserved under taking quotients, i. e. for an ideal $I \subset Q$ we have that Q is primary in R if and only if Q/I is primary in R/I.

To obtain more examples of primary ideals, we need the following lemma. It gives a particularly easy criterion to detect a primary ideal Q if its underlying prime ideal $\sqrt{Q}$ is maximal.

Lemma 8.12 (Primary ideals over maximal ideals)**.** *Let P be a maximal ideal in a ring R. If an ideal $Q \trianglelefteq R$ satisfies one of the following conditions:*

(a) $\sqrt{Q} = P$;

(b) $P^n \subset Q \subset P$ *for some* $n \in \mathbb{N}_{>0}$;

then Q is P-primary.

Proof.

(a) The given condition means that in R/Q the nilradical $\sqrt{(0)}$ is equal to P/Q, hence maximal by Corollary 2.4. Exercise 2.25 then implies that every element of R/Q is either a unit or nilpotent. Therefore every zero-divisor of R/Q (which is never a unit) is nilpotent, and so Q is primary by Remark 8.11 (c).

(b) Taking radicals in the given inclusions yields $\sqrt{P} = \sqrt{P^n} \subset \sqrt{Q} \subset \sqrt{P}$, and hence we get $\sqrt{Q} = \sqrt{P} = P$. So the result then follows from (a). □

Example 8.13 (Primary ideals $\neq$ powers of prime ideals)**.** In general, primary ideals and powers of prime ideals are different objects:

(a) Primary ideals need not be powers of prime ideals: let $Q = (x^2, y)$ and $P = (x, y)$ in $\mathbb{R}[x, y]$. Then $\sqrt{Q} = P$ is maximal by Example 2.6 (c), and so Q is P-primary by Lemma 8.12 (a). However, $(x^2, xy, y^2) = P^2 \subsetneq Q \subsetneq P = (x, y)$, hence Q is not a power of P.

(b) Powers of prime ideals need not be primary: Let $R = \mathbb{R}[x, y, z]/(xy - z^2)$ and $P = (\overline{x}, \overline{z}) \trianglelefteq R$. Then P is prime by Lemma 2.3 (a) since $R/P \cong \mathbb{R}[y]$ is an integral domain. But the power $P^2 = (\overline{x}^2, \overline{x}\,\overline{z}, \overline{z}^2)$ is not primary as $\overline{x}\,\overline{y} = \overline{z}^2 \in P^2$, but neither is $\overline{x}$ in P^2 nor any power of $\overline{y}$.

However, if R is Noetherian and Q primary with $\sqrt{Q} = P$, then Q always *contains* a power of the prime ideal P by Exercise 7.22 (b).

Remark 8.14. Note that the condition of Definition 8.9 for a primary ideal Q is not symmetric in the two factors a and b, i. e. it does not say that $ab \in Q$ implies that one of the two factors a and b lie in $\sqrt{Q}$. In fact, Example 8.13 (b) shows that this latter condition is not equivalent to Q being primary as it is always satisfied by powers of prime ideals: if P is prime and $ab \in P^n$ for some $n \in \mathbb{N}_{>0}$ then we also have $ab \in P$, hence $a \in P$ or $b \in P$, and so a or b lie in $P = \sqrt{P} = \sqrt{P^n}$.

Let us now prove that every ideal in a Noetherian ring can be decomposed as an intersection of primary ideals.

Definition 8.15 (Primary decompositions)**.** Let I be an ideal in a ring R. A **primary decomposition** of I is a finite collection $\{Q_1, \ldots, Q_n\}$ of primary ideals such that $I = Q_1 \cap \cdots \cap Q_n$.

Proposition 8.16 (Existence of primary decompositions)**.** *In a Noetherian ring every ideal has a primary decomposition.*

Proof. Assume for a contradiction that R is a Noetherian ring that has an ideal without primary decomposition. By Lemma 7.4 (a) there is then an ideal $I \trianglelefteq R$ which is maximal among all ideals in R without a primary decomposition. In the quotient ring $S := R/I$ the zero ideal I/I is then the only one without a primary decomposition, since by Remark 8.11 (c) contraction and extension by the quotient map give a one-to-one correspondence between primary decompositions of an ideal $J \supset I$ in R and primary decompositions of J/I in R/I.

In particular, the zero ideal $(0) \trianglelefteq S$ is not primary itself, and so there are $a, b \in S$ with $ab = 0$, but $a \neq 0$ and $b^n \neq 0$ for all $n \in \mathbb{N}$. Now as R is Noetherian, so is S by Remark 7.8 (b), and hence the chain of ideals

$$\operatorname{ann}(b) \subset \operatorname{ann}(b^2) \subset \operatorname{ann}(b^3) \subset \cdots$$

becomes stationary, i. e. there is an $n \in \mathbb{N}$ such that $\operatorname{ann}(b^n) = \operatorname{ann}(b^{n+1})$.

Note that $(a) \neq 0$ and $(b^n) \neq 0$ by our choice of a and b. In particular, these two ideals have a primary decomposition. Taking the primary ideals of these two decompositions together, we then obtain a primary decomposition of $(a) \cap (b^n)$ as well. But $(a) \cap (b^n) = 0$: if $x \in (a) \cap (b^n)$ then $x = ca$ and $x = db^n$ for some $c, d \in S$. As $ab = 0$ we then have $0 = cab = xb = db^{n+1}$, hence $d \in \operatorname{ann}(b^{n+1}) = \operatorname{ann}(b^n)$, which means that $x = db^n = 0$. This is a contradiction, since the zero ideal in S does not have a primary decomposition by assumption. □

14

Example 8.17.

(a) In a unique factorization domain R every principal ideal $I = (p_1^{k_1} \cdot \cdots \cdot p_n^{k_n})$ has a primary decomposition

$$I = (p_1)^{k_1} \cap \cdots \cap (p_n)^{k_n}$$

by Example 8.10 (where $p_1, \ldots, p_n$ are distinct prime elements and $k_1, \ldots, k_n \in \mathbb{N}_{>0}$).

(b) Geometrically, if $I = Q_1 \cap \cdots \cap Q_n$ is a primary decomposition of an ideal I in the coordinate ring of a variety X, we have

$$V(I) = V(Q_1) \cup \cdots \cup V(Q_n) = V(P_1) \cup \cdots \cup V(P_n)$$

by Remark 1.12, where $P_i = \sqrt{Q_i}$ for $i = 1, \ldots, n$. So by Remark 2.7 we have decomposed the subvariety $Y = V(I)$ as a union of irreducible subvarieties $V(P_i)$. As coordinate rings of varieties are always Noetherian by Remark 7.15, Proposition 8.16 asserts that such a decomposition of a (sub-)variety into finitely many irreducible subvarieties is always possible.

However, the primary decomposition of an ideal $I \trianglelefteq A(X)$ contains more information that is not captured in its zero locus $V(I)$ alone: we do not only get subvarieties whose union is $V(I)$, but also (primary) ideals whose zero loci are these subvarieties. These primary ideals can be thought of as containing additional "multiplicity information": for example, the zero locus of the ideal $I = ((x-a_1)^{k_1} \cdot \cdots \cdot (x-a_n)^{k_n})$ in $\mathbb{R}[x]$ is the subset $\{a_1, \ldots, a_n\}$ of $\mathbb{R}$ — but the ideal also associates to each point a_i a multiplicity k_i, and the primary decomposition

$$I = ((x-a_1)^{k_1}) \cap \cdots \cap ((x-a_n)^{k_n})$$

as in (a) remembers these multiplicities.

In fact, in higher dimensions the additional information at each subvariety is more complicated than just a multiplicity. We will not study this here in detail, however we will see an instance of this in Example 8.23.

Having proven that primary decompositions always exist in Noetherian rings, we now want to see in the rest of this chapter to what extent these decompositions are unique. However, with our current definitions it is quite obvious that they are far from being unique, since they can be changed in two simple ways:

Example 8.18 (Non-uniqueness of primary decompositions)**.**

(a) We can always add "superfluous ideals" to a primary decomposition, i. e. primary ideals that are already contained in the intersection of the others. For example, (x^2) and $(x) \cap (x^2)$ in $\mathbb{R}[x]$ are two primary decompositions of the same ideal (x^2) by Example 8.10.

(b) In a given primary decomposition we might have several primary ideals with the same underlying radical, such as in

$$(x^2, xy, y^2) = (x^2, y) \cap (x, y^2) \qquad (*)$$

in $\mathbb{R}[x,y]$. Note that this equation holds since the ideals (x^2,y), (x,y^2), and (x^2,xy,y^2) contain exactly the polynomials without the monomials 1 and x, 1 and y, and without any constant or linear terms, respectively. Moreover, all three ideals have the radical $P = (x,y)$, and hence they are all P-primary by Lemma 8.12 (a). So $(*)$ are two different primary decompositions of the same ideal, in which none of the ideals is superfluous as in (a).

By a slight refinement of the definitions it is actually easy to remove these two ambiguities from primary decompositions. To do this, we need a lemma first.

Lemma 8.19 (Intersections of primary ideals)**.** *Let P be a prime ideal in a ring R. If Q_1 and Q_2 are two P-primary ideals in R, then $Q_1 \cap Q_2$ is P-primary as well.*

Proof. First of all, by Lemma 1.7 (b) we have $\sqrt{Q_1 \cap Q_2} = \sqrt{Q_1} \cap \sqrt{Q_2} = P \cap P = P$. Now let $ab \in Q_1 \cap Q_2$, i. e. $ab \in Q_1$ and $ab \in Q_2$. As Q_1 and Q_2 are P-primary we know that $a \in Q_1$ or $b \in P$, as well as $a \in Q_2$ or $b \in P$. This is the same as $a \in Q_1 \cap Q_2$ or $b \in P = \sqrt{Q_1 \cap Q_2}$. Hence $Q_1 \cap Q_2$ is P-primary. □

Definition 8.20 (Minimal primary decompositions)**.** Let $\{Q_1, \dots, Q_n\}$ be a primary decomposition of an ideal I in a ring R, and let $P_i = \sqrt{Q_i}$ for $i = 1, \dots, n$. Then the decomposition is called **minimal** if

(a) none of the ideals is superfluous in the intersection, i. e. $\bigcap_{j \neq i} Q_j \not\subset Q_i$ for all i;

(b) $P_i \neq P_j$ for all i, j with $i \neq j$.

Corollary 8.21 (Existence of minimal primary decompositions)**.** *If an ideal in a ring has a primary decomposition, it also has a minimal one.*

In particular, in a Noetherian ring every ideal has a minimal primary decomposition.

Proof. Starting from any primary decomposition, leave out superfluous ideals, and replace ideals with the same radical by their intersection, which is again primary with the same radical by Lemma 8.19.

The additional statement follows in combination with Proposition 8.16. □

Exercise 8.22. Find a minimal primary decomposition of ...

(a) the ideal $I = (\overline{x}^2)$ in the ring $R = \mathbb{R}[x,y]/(x^2+y^2-1)$ (see Example 8.7);

(b) the ideal $I = (6)$ in the ring $R = \mathbb{Z}[\sqrt{5}\,i]$ (see Example 8.3 (b));

(c) the ideal $I = (x,y) \cdot (y,z)$ in the ring $\mathbb{R}[x,y,z]$.

As a consequence of Corollary 8.21, one is usually only interested in minimal primary decompositions. However, even then the decompositions will in general not be unique, as the following example shows.

Example 8.23 (Non-uniqueness of minimal primary decompositions)**.** Let us consider the ideal $I = (y) \cdot (x,y) = (xy, y^2)$ in $\mathbb{R}[x,y]$. Geometrically, the zero locus of this ideal is just the horizontal axis $V(I) = V(y)$, which is already irreducible. However, I is not primary since $yx \in I$, but $y \notin I$ and $x^n \notin I$ for all $n \in \mathbb{N}$. Hence, I is not its own minimal primary decomposition. However, we claim that

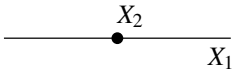
$$I = Q_1 \cap Q_2 = (y) \cap (x^2, xy, y^2) \quad \text{and} \quad I = Q_1 \cap Q_2' = (y) \cap (x, y^2)$$

are two different minimal primary decompositions of I. In fact, both equations can be checked in the same way as in Example 8.18 (b) (the ideal I contains exactly the polynomials with no monomial 1, y, or x^n for $n \in \mathbb{N}$). Moreover, Q_1 is primary since it is prime, and Q_2 and Q_2' are primary by Lemma 8.12 (a) since both of them have the same maximal radical $P_2 = (x,y)$. Finally, it is clear that

in both decompositions none of the ideals is superfluous, and that the radicals of the two ideals are different — namely $P_1 = (y)$ with zero locus $X_1 = V(P_1) = \mathbb{R} \times \{0\}$ and $P_2 = (x,y)$ with zero locus $X_2 = V(P_2) = \{(0,0)\}$, respectively.

So geometrically, even our minimal primary decompositions contain a so-called *embedded* component, i. e. a subvariety X_2 contained in another subvariety X_1 of the decomposition, so that it is not visible in the zero locus of I. The other component X_1 is usually called an *isolated* component. The corresponding algebraic statement is that P_2 contains another prime ideal P_1 occurring as a radical in the decomposition; we will also say that P_2 is an embedded and P_1 an isolated prime ideal (see Definition 8.25 and Example 8.28).

The intuitive reason why this embedded component occurs is that X_2 has a higher "multiplicity" in I than X_1 (in a sense that we do not want to make precise here). We can indicate this as in the picture on the right by a "fat point" X_2 on a "thin line" X_1.



In any case, we conclude that even minimal primary decompositions of an ideal are not unique. However, this non-uniqueness is very subtle: we will now show that it can only occur in the primary ideals of embedded components. More precisely, we will prove that in a minimal primary decomposition:

(a) the underlying prime ideals of all primary ideals are uniquely determined (see Proposition 8.27); and

(b) the primary ideals corresponding to all isolated components are uniquely determined (see Proposition 8.34).

So in our example above, P_1, P_2, and Q_1 are uniquely determined, and only the primary ideal corresponding to P_2 can depend on the decomposition.

To prove the first statement (a), we give an alternative way to reconstruct all underlying prime ideals of a minimal primary decomposition (the so-called *associated prime ideals*) without knowing the decomposition at all.

Lemma 8.24. *Let Q be a P-primary ideal in a ring R. Then for any $a \in R$ we have*

$$\sqrt{Q:a} = \begin{cases} R & \text{if } a \in Q, \\ P & \text{if } a \notin Q. \end{cases}$$

Proof. If $a \in Q$ then clearly $Q:a = R$, and thus $\sqrt{Q:a} = R$ as well.

Now let $a \notin Q$. Then for any $b \in Q:a$ we have $ab \in Q$, and so $b \in P$ since Q is P-primary. Hence $Q \subset Q:a \subset P$, and by taking radicals we obtain $P \subset \sqrt{Q:a} \subset P$ as desired. □

Definition 8.25 (Associated, isolated, and embedded prime ideals)**.** Let I be an ideal in a ring R.

(a) An **associated prime ideal** of I is a prime ideal that can be written as $\sqrt{I:a}$ for some $a \in R$. We denote the set of these associated primes by $\operatorname{Ass}(I)$.

(b) The minimal elements of $\operatorname{Ass}(I)$ are called **isolated prime ideals** of I, the other ones **embedded prime ideals** of I.

Remark 8.26. For an ideal I of a ring R, note that not every ideal that can be written as $\sqrt{I:a}$ for some $a \in R$ is prime. By definition, $\operatorname{Ass}(I)$ contains only the prime ideals of this form.

Proposition 8.27 (**First Uniqueness Theorem** for primary decompositions)**.** *Let $Q_1, \dots, Q_n$ form a minimal primary decomposition for an ideal I in a ring R, and let $P_i = \sqrt{Q_i}$ for $i = 1, \dots, n$.*

Then $\{P_1, \dots, P_n\} = \operatorname{Ass}(I)$. In particular, the number of components in a minimal primary decomposition and their radicals do not depend on the chosen decomposition.

Proof.

"$\subset$": Let $i \in \{1,\dots,n\}$, we will show that $P_i \in \operatorname{Ass}(I)$. As the given decomposition is minimal, we can find $a \in \bigcap_{j\neq i} Q_j$ with $a \notin Q_i$. Then

$$\begin{aligned}\sqrt{I:a} &= \sqrt{Q_1:a \cap \dots \cap Q_n:a} \\ &= \sqrt{Q_1:a} \cap \dots \cap \sqrt{Q_n:a} && \text{(Lemma 1.7 (b))} \\ &= P_i && \text{(Lemma 8.24),}\end{aligned}$$

and so $P_i \in \operatorname{Ass}(I)$.

"$\supset$": Let $P \in \operatorname{Ass}(I)$, so $P = \sqrt{I:a}$ for some $a \in R$. Then as above we have

$$P = \sqrt{I:a} = \sqrt{Q_1:a} \cap \dots \cap \sqrt{Q_n:a},$$

and thus $P \supset \sqrt{Q_i:a}$ for some i by Exercise 2.10 (a) since P is prime. But of course the above equation also implies $P \subset \sqrt{Q_i:a}$, and so $P = \sqrt{Q_i:a}$. Now by Lemma 8.24 this radical can only be P_i or R, and since P is prime we conclude that we must have $P = P_i$. □

Example 8.28. In the situation of Example 8.23, Proposition 8.27 states that the associated prime ideals of I are P_1 and P_2 since we have found a minimal primary decomposition of I with these underlying prime ideals. It is then obvious by Definition 8.25 that P_1 is an isolated and P_2 an embedded prime of I.

Exercise 8.29. Let I be an ideal in a ring R. In Definition 8.25 we have introduced $\operatorname{Ass}(I)$ as the set of prime ideals that are of the form $\sqrt{I:a}$ for some $a \in R$. If R is Noetherian, prove that we do not have to take radicals, i. e. that $\operatorname{Ass}(I)$ is also equal to the set of all prime ideals that are of the form $I:a$ for some $a \in R$.

Corollary 8.30 (Isolated prime ideals = minimal prime ideals)**.** *Let I be an ideal in a Noetherian ring R. Then the isolated prime ideals of I are exactly the minimal prime ideals over I as in Exercise 2.23, i. e. the prime ideals $P \supset I$ such that there is no prime ideal Q with $I \subset Q \subsetneq P$.*

In particular, in a Noetherian ring there are only finitely many minimal prime ideals over any given ideal.

Proof. As R is Noetherian, there is a minimal primary decomposition $I = Q_1 \cap \dots \cap Q_n$ of I by Corollary 8.21. As usual we set $P_i = \sqrt{Q_i}$ for all i, so that $\operatorname{Ass}(I) = \{P_1,\dots,P_n\}$ by Proposition 8.27.

Note that if $P \supset I$ is any prime ideal, then $P \supset Q_1 \cap \dots \cap Q_n$, hence $P \supset Q_i$ for some i by Exercise 2.10 (a), and so by taking radicals $P \supset \sqrt{Q_i} = P_i$. With this we now show both implications stated in the corollary:

- Let $P_i \in \operatorname{Ass}(I)$ be an isolated prime ideal of I. If P is any prime ideal with $I \subset P \subset P_i$ then by what we have just said $P_j \subset P \subset P_i$ for some j. But as P_i is isolated we must have equality, and so $P = P_i$. Hence P_i is minimal over I.
- Now let P be a minimal prime over I. By the above $I \subset Q_i \subset P_i \subset P$ for some i. As P is minimal over I this means that $P = P_i$ is an associated prime, and hence also an isolated prime of I. □

Remark 8.31. In particular, Corollary 8.30 states that the isolated prime ideals of an ideal I in a coordinate ring of a variety $A(X)$ correspond exactly to the maximal subvarieties, i. e. to the irreducible components of $V(I)$ — as already motivated in Example 8.23.

Exercise 8.32. Let R be a Noetherian integral domain. Show:

(a) R is a unique factorization domain if and only if every minimal prime ideal over a principal ideal is itself principal.

(b) If R is a unique factorization domain then every minimal non-zero prime ideal of R is principal.

Finally, to prove the second uniqueness statement (b) of Example 8.23 the idea is to use localization at an isolated prime ideal to remove from I all components that do not belong to this prime ideal.

Lemma 8.33. *Let S be a multiplicatively closed subset in a ring R, and let Q be a P-primary ideal in R. Then with respect to the ring homomorphism $\varphi : R \to S^{-1}R$, $a \mapsto \frac{a}{1}$ we have*

$$(Q^e)^c = \begin{cases} R & \text{if } S \cap P \neq \emptyset, \\ Q & \text{if } S \cap P = \emptyset. \end{cases}$$

Proof. If $S \cap P \neq \emptyset$ there is an element $s \in S$ with $s \in P = \sqrt{Q}$, and thus $s^n \in Q$ for some $n \in \mathbb{N}$. So $\frac{1}{1} = \frac{s^n}{s^n} \in S^{-1}Q = Q^e$ by Example 6.18. Hence $Q^e = S^{-1}R$, and therefore $(Q^e)^c = R$.

On the other hand, assume now that $S \cap P = \emptyset$. By Exercise 1.19 (a) it suffices so prove $(Q^e)^c \subset Q$. If $a \in (Q^e)^c$ we have $\frac{a}{1} \in Q^e$, and so $\frac{a}{1} = \frac{q}{s}$ for some $q \in Q$ and $s \in S$ by Proposition 6.7 (a). Hence $u(q - as) = 0$ for some $u \in S$, which implies that $a \cdot us = uq \in Q$. As Q is P-primary it follows that $a \in Q$ or $us \in P$. But $us \in S$, so $us \notin P$ since $S \cap P = \emptyset$, and we conclude that $a \in Q$. □

Proposition 8.34 (**Second Uniqueness Theorem** for primary decompositions)**.** *Let $Q_1, \dots, Q_n$ form a minimal primary decomposition for an ideal I in a ring R, and let $P_i = \sqrt{Q_i}$ for $i = 1, \dots, n$.*

If $i \in \{1, \dots, n\}$ such that P_i is minimal over I, then $(I^e)^c = Q_i$, where contraction and extension are taken with respect to the canonical localization map $R \to R_{P_i}$. In particular, in a minimal primary decomposition the primary components corresponding to minimal prime ideals do not depend on the chosen decomposition.

Proof. Localizing the equation $I = Q_1 \cap \dots \cap Q_n$ at S gives $S^{-1}I = S^{-1}Q_1 \cap \dots \cap S^{-1}Q_n$ by Exercise 6.24 (b), hence $I^e = Q_1^e \cap \dots \cap Q_n^e$ by Example 6.18, and so $(I^e)^c = (Q_1^e)^c \cap \dots \cap (Q_n^e)^c$ by Exercise 1.19 (d).

Now let P_i be minimal over I, and set $S = R \backslash P_i$. Then $S \cap P_i = \emptyset$, whereas $S \cap P_j \neq \emptyset$ for all $j \neq i$ since $P_j \not\subset P_i$. So applying Lemma 8.33 gives $(I^e)^c = (Q_i^e)^c = Q_i$ as desired. □

15