1. Ideals

From the "Algebraic Structures" class you already know the basic constructions and properties concerning ideals and their quotient rings [G1, Chapter 8]. For our purposes however we have to study ideals in much more detail — so this will be our goal for this and the next chapter. Let us start with some general constructions to obtain new ideals from old ones. The ideal generated by a subset M of a ring [G1, Definition 8.5] will be written as (M).

Construction 1.1 (Operations on ideals)**.** Let I and J be ideals in a ring R.

(a) The **sum** of the two given ideals is defined as usual by

$$I+J := \{a+b : a \in I \text{ and } b \in J\}.$$

It is easy to check that this is an ideal — in fact, it is just the ideal generated by $I \cup J$.

(b) It is also obvious that the **intersection** $I \cap J$ is again an ideal of R.

(c) We define the **product** of I and J as the ideal generated by all products of elements of I and J, i. e.

$$I \cdot J := (\{ab : a \in I \text{ and } b \in J\}).$$

Note that just the set of products of elements of I and J would in general not be an ideal: if we take $R = \mathbb{R}[x,y]$ and $I = J = (x,y)$, then obviously x^2 and y^2 are products of an element of I with an element of J, but their sum x^2+y^2 is not.

(d) The **quotient** of I by J is defined to be

$$I:J := \{a \in R : aJ \subset I\}.$$

Again, it is easy to see that this is an ideal.

(e) We call

$$\sqrt{I} := \{a \in R : a^n \in I \text{ for some } n \in \mathbb{N}\}$$

the **radical** of I. Let us check that this an ideal of R:

- We have $0 \in \sqrt{I}$, since $0 \in I$.
- If $a, b \in \sqrt{I}$, i. e. $a^n \in I$ and $b^m \in I$ for some $n, m \in \mathbb{N}$, then

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}$$

is again an element of I, since in each summand we must have that the power of a is at least n (in which case $a^k \in I$) or the power of b is at least m (in which case $b^{n+m-k} \in I$). Hence $a+b \in \sqrt{I}$.

- If $r \in R$ and $a \in \sqrt{I}$, i. e. $a^n \in I$ for some $n \in \mathbb{N}$, then $(ra)^n = r^n a^n \in I$, and hence $ra \in \sqrt{I}$.

Note that we certainly have $\sqrt{I} \supset I$. We call I a **radical ideal** if $\sqrt{I} = I$, i. e. if for all $a \in R$ and $n \in \mathbb{N}$ with $a^n \in I$ it follows that $a \in I$. This is a natural definition since the radical $\sqrt{I}$ of an arbitrary ideal I is in fact a radical ideal in this sense: if $a^n \in \sqrt{I}$ for some n, so $a^{nm} \in I$ for some m, then this obviously implies $a \in \sqrt{I}$. 01

Whether an ideal I is radical can also easily be seen from its quotient ring R/I as follows.

Definition 1.2 (Nilradical, nilpotent elements, and reduced rings)**.** Let R be a ring. The ideal

$$\sqrt{(0)} = \{a \in R : a^n = 0 \text{ for some } n \in \mathbb{N}\}$$

is called the **nilradical** of R; its elements are called **nilpotent**. If R has no nilpotent elements except 0, i. e. if the zero ideal is radical, then R is called **reduced**.

Lemma 1.3. *An ideal $I \trianglelefteq R$ is radical if and only if R/I is reduced.*

Proof. By Construction 1.1 (e), the ideal I is radical if and only if for all $a \in R$ and $n \in \mathbb{N}$ with $a^n \in I$ it follows that $a \in I$. Passing to the quotient ring R/I, this is obviously equivalent to saying that $\overline{a}^n = \overline{0}$ implies $\overline{a} = \overline{0}$, i. e. that R/I has no nilpotent elements except $\overline{0}$. □

Example 1.4 (Operations on ideals in principal ideal domains)**.** Recall that a *principal ideal domain* (or short: *PID*) is an integral domain in which every ideal is *principal*, i. e. can be generated by one element [G1, Definition 10.11]. The most prominent examples of such rings are probably *Euclidean domains*, i. e. integral domains admitting a division with remainder [G1, Definition 10.17 and Proposition 10.22], such as $\mathbb{Z}$ or $K[x]$ for a field K [G1, Example 10.18 and Proposition 10.19].

We know that any principal ideal domain R admits a unique prime factorization of its elements [G1, Proposition 11.9] — a concept that we will discuss in more detail in Chapter 8. As a consequence, all operations of Construction 1.1 can then be computed easily: if I and J are not the zero ideal we can write $I = (a)$ and $J = (b)$ for $a = p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$ and $b = p_1^{b_1} \cdot \dots \cdot p_n^{b_n}$ with distinct prime elements $p_1, \dots, p_n$ and $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{N}$. Then we obtain:

(a) $I + J = (p_1^{c_1} \cdot \dots \cdot p_n^{c_n})$ with $c_i = \min(a_i, b_i)$ for $i = 1, \dots, n$: another (principal) ideal contains I (resp. J) if and only if it is of the form $(p_1^{c_1} \cdot \dots \cdot p_n^{c_n})$ with $c_i \leq a_i$ (resp. $c_i \leq b_i$) for all i, so the smallest ideal $I + J$ containing I and J is obtained for $c_i = \min(a_i, b_i)$;

(b) $I \cap J = (p_1^{c_1} \cdot \dots \cdot p_n^{c_n})$ with $c_i = \max(a_i, b_i)$;

(c) $I \cdot J = (ab) = (p_1^{c_1} \cdot \dots \cdot p_n^{c_n})$ with $c_i = a_i + b_i$;

(d) $I : J = (p_1^{c_1} \cdot \dots \cdot p_n^{c_n})$ with $c_i = \max(a_i - b_i, 0)$;

(e) $\sqrt{I} = (p_1^{c_1} \cdot \dots \cdot p_n^{c_n})$ with $c_i = \min(a_i, 1)$.

In particular, we have $I + J = (1) = R$ if and only if a and b have no common prime factor, i. e. if a and b are coprime. We use this observation to define the notion of coprime ideals in general rings:

Definition 1.5 (Coprime ideals)**.** Two ideals I and J in a ring R are called **coprime** if $I + J = R$.

Example 1.6 (Operations on ideals in polynomial rings with SINGULAR)**.** In more general rings, the explicit computation of the operations of Construction 1.1 is quite complicated and requires advanced algorithmic methods that you can learn about in the "Computer Algebra" class. We will not need this here, but if you want to compute some examples in polynomial rings you can use e. g. the computer algebra system SINGULAR [S]. For example, for the ideals $I = (x^2y, xy^3)$ and $J = (x + y)$ in $\mathbb{Q}[x, y]$ the following SINGULAR code computes that $I : J = (x^2y, xy^2)$ and $\sqrt{I \cdot J} = \sqrt{I \cap J} = (x^2y + xy^2)$, and checks that $y^3 \in I + J$:

```
> LIB "primdec.lib"; // library needed for the radical
> ring R=0,(x,y),dp; // set up polynomial ring Q[x,y]
> ideal I=x2y,xy3; // means I=(x^2*y,x*y^3)
> ideal J=x+y;
> quotient(I,J); // compute (generators of) I:J
_[1]=xy2
_[2]=x2y
> radical(I*J); // compute radical of I*J
_[1]=x2y+xy2
> radical(intersect(I,J)); // compute radical of intersection
_[1]=x2y+xy2
> reduce(y3,std(I+J)); // gives 0 if and only if y^3 in I+J
0
```

In this example it turned out that $\sqrt{I \cdot J} = \sqrt{I \cap J}$. In fact, this is not a coincidence — the following lemma and exercise show that the product and the intersection of ideals are very closely related.

Lemma 1.7 (Product and intersection of ideals)**.** *For any two ideals I and J in a ring R we have*

(a) $I \cdot J \subset I \cap J$;

(b) $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Proof.

(a) It suffices to check that all generators of $I \cdot J$ lie in $I \cap J$. But for $a \in I$ and $b \in J$ it is obvious that $ab \in I \cap J$, so the result follows.

(b) We show a circular inclusion, with $\sqrt{I \cdot J} \subset \sqrt{I \cap J}$ following from (a).

If $a \in \sqrt{I \cap J}$ then $a^n \in I \cap J$ for some $n \in \mathbb{N}$, so $a^n \in I$ and $a^n \in J$, and hence $a \in \sqrt{I} \cap \sqrt{J}$. Finally, if $a \in \sqrt{I} \cap \sqrt{J}$ then $a^m \in I$ and $a^n \in J$ for some $m, n \in \mathbb{N}$, therefore $a^{m+n} \in I \cdot J$ and thus $a \in \sqrt{I \cdot J}$. □

Exercise 1.8. Let $I_1, \ldots, I_n$ be pairwise coprime ideals in a ring R. Prove that $I_1 \cdot \cdots \cdot I_n = I_1 \cap \cdots \cap I_n$.

Exercise 1.9. Show that the ideal $(x_1, \ldots, x_n) \trianglelefteq K[x_1, \ldots, x_n]$ cannot be generated by fewer than n elements. Hence in particular, the polynomial ring $K[x_1, \ldots, x_n]$ is not a principal ideal domain for $n \geq 2$.

We will see however in Remark 8.6 that these polynomial rings still admit unique prime factorizations of its elements, so that the results of Example 1.4 continue to hold for principal ideals in these rings.

Remark 1.10 (Ideals of subvarieties = radical ideals)**.** Radical ideals play an important role in geometry: if Y is a subvariety of a variety X and $f \in A(X)$ with $f^n \in I(Y)$, then $(f(x))^n = 0$ for all $x \in Y$ — but this obviously implies $f(x) = 0$ for all $x \in Y$, and hence $f \in I(Y)$. So ideals of subvarieties are always radical.

In fact, if the ground field K is *algebraically closed*, i. e. if every non-constant polynomial over K has a zero (as e. g. for $K = \mathbb{C}$), we will see in Corollary 10.14 that it is *exactly* the radical ideals in $A(X)$ that are ideals of subvarieties. So in this case there is a one-to-one correspondence

$$\begin{array}{rcl} \{\text{subvarieties of } X\} & \overset{1:1}{\longleftrightarrow} & \{\text{radical ideals in } A(X)\} \\ Y & \longmapsto & I(Y) \\ V(I) & \longmapsfrom & I. \end{array}$$

In other words, we have $V(I(Y)) = Y$ for every subvariety Y of X (which we have already seen in Lemma 0.9 (c)), and $I(V(I)) = I$ for every radical ideal $I \trianglelefteq A(X)$. In order to simplify our geometric interpretations we will therefore usually assume from now on in our geometric examples that the ground field is algebraically closed and the above one-to-one correspondence holds. Note that this will not lead to circular reasoning as we will never use these geometric examples to prove anything.

Exercise 1.11.

(a) Give a rigorous proof of the one-to-one correspondence of Remark 1.10 in the case of the ambient variety $\mathbb{A}^1_{\mathbb{C}}$, i. e. between subvarieties of $\mathbb{A}^1_{\mathbb{C}}$ and radical ideals in $A(\mathbb{A}^1_{\mathbb{C}}) = \mathbb{C}[x]$.

(b) Show that this one-to-one correspondence does not hold in the case of the ground field $\mathbb{R}$, i. e. between subvarieties of $\mathbb{A}^1_{\mathbb{R}}$ and radical ideals in $A(\mathbb{A}^1_{\mathbb{R}}) = \mathbb{R}[x]$.

Remark 1.12 (Geometric interpretation of operations on ideals)**.** Let X be a variety over an algebraically closed field, and let $A(X)$ be its coordinate ring. Assuming the one-to-one correspondence of Remark 1.10 between subvarieties of X and radical ideals in $A(X)$ we can now give a geometric interpretation of the operations of Construction 1.1:

(a) As $I + J$ is the ideal generated by $I \cup J$, we have for any two (radical) ideals $I, J \trianglelefteq A(X)$

$$\begin{aligned} V(I+J) &= \{x \in X : f(x) = 0 \text{ for all } f \in I \cup J\} \\ &= \{x \in X : f(x) = 0 \text{ for all } f \in I\} \cap \{x \in X : f(x) = 0 \text{ for all } f \in J\} \\ &= V(I) \cap V(J). \end{aligned}$$

So the intersection of subvarieties corresponds to the sum of ideals. (Note however that the sum of two radical ideals may not be radical, so strictly speaking the algebraic operation corresponding to the intersection of subvarieties is taking the sum of the ideals and then its radical.)

Moreover, as the whole space X and the empty set $\emptyset$ obviously correspond to the zero ideal (0) resp. the whole ring $(1) = A(X)$, the condition $I + J = A(X)$ that I and J are coprime translates into the intersection of $V(I)$ and $V(J)$ being empty.

(b) For any two subvarieties Y, Z of X

$$\begin{aligned} I(Y \cup Z) &= \{f \in A(X) : f(x) = 0 \text{ for all } x \in Y \cup Z\} \\ &= \{f \in A(X) : f(x) = 0 \text{ for all } x \in Y\} \cap \{f \in A(X) : f(x) = 0 \text{ for all } x \in Z\} \\ &= I(Y) \cap I(Z), \end{aligned}$$

and thus the union of subvarieties corresponds to the intersection of ideals. As the product of ideals has the same radical as the intersection by Lemma 1.7 (b), the union of subvarieties also corresponds to taking the product of the ideals (and then its radical).

(c) Again for two subvarieties Y, Z of X we have

$$\begin{aligned} I(Y \backslash Z) &= \{f \in A(X) : f(x) = 0 \text{ for all } x \in Y \backslash Z\} \\ &= \{f \in A(X) : f(x) \cdot g(x) = 0 \text{ for all } x \in Y \text{ and } g \in I(Z)\} \\ &= \{f \in A(X) : f \cdot I(Z) \subset I(Y)\} \\ &= I(Y) : I(Z), \end{aligned}$$

so taking the set-theoretic difference $Y \backslash Z$ corresponds to quotient ideals. (Strictly speaking, the difference $Y \backslash Z$ is in general not a variety, so the exact geometric operation corresponding to quotient ideals is taking the smallest subvariety containing $Y \backslash Z$.)

Summarizing, we obtain the following translation between geometric and algebraic terms:

SUBVARIETIES	$\longleftrightarrow$	IDEALS
full space		*(0)*
empty set		*(1)*
intersection		*sum*
union		*product / intersection*
difference		*quotient*
disjoint subvarieties		*coprime ideals*

Exercise 1.13. Show that the equation of ideals

$$(x^3 - x^2, x^2 y - x^2, xy - y, y^2 - y) = (x^2, y) \cap (x - 1, y - 1)$$

holds in the polynomial ring $\mathbb{C}[x, y]$. Is this a radical ideal? What is its zero locus in $\mathbb{A}^2_{\mathbb{C}}$?

As an example that links the concepts introduced so far, let us now consider the Chinese Remainder Theorem that you already know for the integers [G1, Proposition 11.22] and generalize it to arbitrary rings.

Proposition 1.14 (Chinese Remainder Theorem)**.** *Let $I_1, \ldots, I_n$ be ideals in a ring R, and consider the ring homomorphism*

$$\varphi : R \to R/I_1 \times \cdots \times R/I_n, \quad a \mapsto (\overline{a}, \ldots, \overline{a}).$$

(a) *φ is injective if and only if $I_1 \cap \cdots \cap I_n = (0)$.*

(b) *φ is surjective if and only if $I_1, \ldots, I_n$ are pairwise coprime.*

Proof.

(a) This follows immediately from $\ker \varphi = I_1 \cap \cdots \cap I_n$.

(b) "$\Rightarrow$" If φ is surjective then $(1,0,\ldots,0) \in \operatorname{im}\varphi$. In particular, there is an element $a \in R$ with $a = 1 \mod I_1$ and $a = 0 \mod I_2$. But then $1 = (1-a) + a \in I_1 + I_2$, and hence $I_1 + I_2 = R$. In the same way we see $I_i + I_j = R$ for all $i \neq j$.

"$\Leftarrow$" Let $I_i + I_j = R$ for all $i \neq j$. In particular, for $i = 2,\ldots,n$ there are $a_i \in I_1$ and $b_i \in I_i$ with $a_i + b_i = 1$, so that $b_i = 1 - a_i = 1 \mod I_1$ and $b_i = 0 \mod I_i$. If we then set $b := b_2 \cdot \cdots \cdot b_n$ we get $b = 1 \mod I_1$ and $b = 0 \mod I_i$ for all $i = 2,\ldots,n$. So $(1,0,\ldots,0) = \varphi(b) \in \operatorname{im}\varphi$. In the same way we see that the other unit generators are in the image of φ, and hence φ is surjective. □

Example 1.15.

(a) Consider the case $R = \mathbb{Z}$, and let $a_1,\ldots,a_n \in \mathbb{Z}$ be pairwise coprime. Then the residue class map

$$\varphi : \mathbb{Z} \to \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_n},\ x \mapsto (\bar{x},\ldots,\bar{x})$$

is surjective by Proposition 1.14 (b). Its kernel is $(a_1) \cap \cdots \cap (a_n) = (a)$ with $a := a_1 \cdot \cdots \cdot a_n$ by Exercise 1.8, and so by the homomorphism theorem [G1, Proposition 8.12] we obtain an isomorphism

$$\mathbb{Z}_a \to \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_n},\ \bar{x} \mapsto (\bar{x},\ldots,\bar{x}),$$

which is the well-known form of the Chinese Remainder Theorem for the integers [G1, Proposition 11.22].

(b) Let X be a variety, and let $Y_1,\ldots,Y_n$ be subvarieties of X. Recall from Remark 0.13 that for $i = 1,\ldots,n$ we have isomorphisms $A(X)/I(Y_i) \cong A(Y_i)$ by restricting functions from X to Y_i. Using the translations from Remark 1.12, Proposition 1.14 therefore states that the combined restriction map $\varphi : A(X) \to A(Y_1) \times \cdots \times A(Y_n)$ to all given subvarieties is ...

- injective if and only if the subvarieties $Y_1,\ldots,Y_n$ cover all of X;
- surjective if and only if the subvarieties $Y_1,\ldots,Y_n$ are disjoint.

In particular, if X is the disjoint union of the subvarieties $Y_1,\ldots,Y_n$, then the Chinese Remainder Theorem says that φ is an isomorphism, i. e. that giving a function on X is the same as giving a function on each of the subvarieties — which seems obvious from geometry.

In our study of ideals, let us now consider their behavior under ring homomorphisms.

Definition 1.16 (Contraction and extension)**.** Let $\varphi : R \to R'$ be a ring homomorphism.

(a) For any ideal $I \trianglelefteq R'$ the inverse image $\varphi^{-1}(I)$ is an ideal of R. We call it the **inverse image ideal** or **contraction** of I by φ, sometimes denoted I^c if it is clear from the context which morphism we consider.

(b) For $I \trianglelefteq R$ the ideal generated by the image $\varphi(I)$ is called the **image ideal** or **extension** of I by φ. It is written as $\varphi(I) \cdot R'$, or I^e if the morphism is clear from the context.

Remark 1.17.

(a) Note that for the construction of the image ideal of an ideal $I \trianglelefteq R$ under a ring homomorphism $\varphi : R \to R'$ we have to take the ideal generated by $\varphi(I)$, since $\varphi(I)$ itself is in general not yet an ideal: take e. g. $\varphi : \mathbb{Z} \to \mathbb{Z}[x]$ to be the inclusion and $I = \mathbb{Z}$. But if φ is surjective then $\varphi(I)$ is already an ideal and thus $I^e = \varphi(I)$:

- for $b_1, b_2 \in \varphi(I)$ we have $a_1, a_2 \in I$ with $b_1 = \varphi(a_1)$ and $b_2 = \varphi(a_2)$, and so $b_1 + b_2 = \varphi(a_1 + a_2) \in \varphi(I)$;
- for $b \in \varphi(I)$ and $s \in R'$ we have $a \in I$ and $r \in R$ with $\varphi(a) = b$ and $\varphi(r) = s$, and thus $sb = \varphi(ra) \in \varphi(I)$.

(b) If R is a field and $R' \neq \{0\}$ then any ring homomorphism $\varphi : R \to R'$ is injective: its kernel is 0 since an element $a \in R \backslash \{0\}$ with $\varphi(a) = 0$ would lead to the contradiction

$$1 = \varphi(1) = \varphi(a^{-1}a) = \varphi(a^{-1}) \cdot \varphi(a) = 0.$$

This is the origin of the names "contraction" and "extension", since in this case these two operations really make the ideal "smaller" and "bigger", respectively.

Remark 1.18 (Geometric interpretation of contraction and extension)**.** As in Construction 0.11, let $f : X \to Y$ be a morphism of varieties, and let $\varphi : A(Y) \to A(X), \ g \mapsto g \circ f$ be the associated map between the coordinate rings.

(a) For any subvariety $Z \subset X$ we have

$$\begin{aligned} I(f(Z)) &= \{g \in A(Y) : g(f(x)) = 0 \text{ for all } x \in Z\} \\ &= \{g \in A(Y) : \varphi(g) \in I(Z)\} \\ &= \varphi^{-1}(I(Z)), \end{aligned}$$

so taking images of varieties corresponds to the contraction of ideals.

(b) For a subvariety $Z \subset Y$ the zero locus of the extension $I(Z)^e$ by φ is

$$\begin{aligned} V(\varphi(I(Z))) &= \{x \in X : g(f(x)) = 0 \text{ for all } g \in I(Z)\} \\ &= f^{-1}(\{y \in Y : g(y) = 0 \text{ for all } g \in I(Z)\}) \\ &= f^{-1}(V(I(Z))) \\ &= f^{-1}(Z) \end{aligned}$$

by Lemma 0.9 (c). Hence, taking inverse images of subvarieties corresponds to the extension of ideals.

So we can add the following two entries to our dictionary between geometry and algebra:

SUBVARIETIES	$\longleftrightarrow$	IDEALS
image		*contraction*
inverse image		*extension*

Exercise 1.19. Let $\varphi : R \to R'$ a ring homomorphism. Prove:

(a) $I \subset (I^e)^c$ for all $I \trianglelefteq R$;

(b) $I \supset (I^c)^e$ for all $I \trianglelefteq R'$;

(c) $(IJ)^e = I^e J^e$ for all $I, J \trianglelefteq R$;

(d) $(I \cap J)^c = I^c \cap J^c$ for all $I, J \trianglelefteq R'$.

Exercise 1.20. Let $f : X \to Y$ be a morphism of varieties, and let Z and W be subvarieties of X. The geometric statements below are then obvious. Find and prove corresponding algebraic statements for ideals in rings.

(a) $f(Z \cup W) = f(Z) \cup f(W)$;

(b) $f(Z \cap W) \subset f(Z) \cap f(W)$;

(c) $f(Z \backslash W) \supset f(Z) \backslash f(W)$.

An important application of contraction and extension is that it allows an easy explicit description of ideals in quotient rings.

Lemma 1.21 (Ideals in quotient rings)**.** *Let I be an ideal in a ring R. Then contraction and extension by the quotient map $\varphi : R \to R/I$ give a one-to-one correspondence*

$$\begin{array}{ccc} \{\text{ideals in } R/I\} & \overset{1:1}{\longleftrightarrow} & \{\text{ideals } J \text{ in } R \text{ with } J \supset I\} \\ J & \longmapsto & J^c \\ J^e & \longleftarrow\!\shortmid & J. \end{array}$$

Proof. As the quotient map φ is surjective, we know by Remark 1.17 (a) that contraction and extension are just the inverse image and image of an ideal, respectively. Moreover, it is clear that the contraction of an ideal in R/I yields an ideal of R that contains I, and that the extension of an ideal in R gives an ideal in R/I. So we just have to show that contraction and extension are inverse to each other on the sets of ideals given in the lemma. But this is easy to check:

- For any ideal $J \trianglelefteq R/I$ we have $(J^c)^e = \varphi(\varphi^{-1}(J)) = J$ since φ is surjective.
- For any ideal $J \trianglelefteq R$ with $J \supset I$ we get
$$(J^e)^c = \varphi^{-1}(\varphi(J)) = \{a \in R : \varphi(a) \in \varphi(J)\} = J + I = J.$$ □

Exercise 1.22. Let $I \subset J$ be ideals in a ring R. By Lemma 1.21, the extension J/I of J by the quotient map $R \to R/I$ is an ideal in R/I. Prove that

$$(R/I) \,/\, (J/I) \cong R/J.$$

02

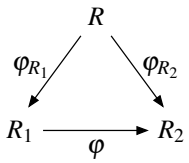
At the end of this chapter, let us now consider ring homomorphisms from a slightly different point of view that will also tell us which rings "come from geometry", i. e. can be written as coordinate rings of varieties.

Definition 1.23 (Algebras and algebra homomorphisms)**.** Let R be a ring.

(a) An **R-algebra** is a ring R' together with a ring homomorphism $\varphi_{R'} : R \to R'$.

(b) Let R_1 and R_2 be R-algebras with corresponding ring homomorphisms $\varphi_{R_1} : R \to R_1$ and $\varphi_{R_2} : R \to R_2$. A **morphism** or **$R$-algebra homomorphism** from R_1 to R_2 is a ring homomorphism $\varphi : R_1 \to R_2$ with $\varphi \circ \varphi_{R_1} = \varphi_{R_2}$.

It is often helpful to draw these maps in a diagram as shown on the right. Then the condition $\varphi \circ \varphi_{R_1} = \varphi_{R_2}$ just states that this diagram *commutes*, i. e. that any two ways along the arrows in the diagram having the same source and target — in this case the two ways to go from R to R_2 — will give the same map.



(c) Let R' be an R-algebra with corresponding ring homomorphism $\varphi_{R'} : R \to R'$. An **R-subalgebra** of R' is a subring $\tilde{R}$ of R' containing the image of φ. Note that $\tilde{R}$ is then an R-algebra using the ring homomorphism $\varphi_{\tilde{R}} : R \to \tilde{R}$ given by $\varphi_{R'}$ with the target restricted to $\tilde{R}$. Moreover, the inclusion $\tilde{R} \to R'$ is an R-algebra homomorphism in the sense of (b).

In most of our applications, the ring homomorphism $\varphi_{R'} : R \to R'$ needed to define an R-algebra R' will be clear from the context, and we will write the R-algebra simply as R'. In fact, in many cases it will even be injective. In this case we usually consider R as a subring of R', drop the homomorphism $\varphi_{R'}$ in the notation completely, and say that $R \subset R'$ is a *ring extension*. We will consider these ring extensions in detail in Chapter 9.

Remark 1.24. The ring homomorphism $\varphi_{R'} : R \to R'$ associated to an R-algebra R' can be used to define a "scalar multiplication" of R on R' by

$$R \times R' \to R', \;\; (a,c) \mapsto a \cdot c := \varphi_{R'}(a) \cdot c.$$

Note that by setting $c = 1$ this scalar multiplication determines $\varphi_{R'}$ back. So one can also think of an R-algebra as a ring together with a scalar multiplication with elements of R that has the expected compatibility properties. In fact, one could also define R-algebras in this way.

Example 1.25.

(a) Without doubt the most important example of an algebra over a ring R is the polynomial ring $R[x_1,\dots,x_n]$, together with the obvious injective ring homomorphism $R \to R[x_1,\dots,x_n]$ that embeds R into the polynomial ring as constant polynomials. In the same way, any quotient $R[x_1,\dots,x_n]/I$ of the polynomial ring by an ideal I is an R-algebra as well.

(b) Let $X \subset \mathbb{A}^n_K$ be a variety over a field K. Then its coordinate ring $A(X) = K[x_1,\dots,x_n]/I(X)$ is a K-algebra by (a), with K mapping to $A(X)$ as the constant functions. Moreover, the ring homomorphism $A(Y) \to A(X)$ of Construction 0.11 corresponding to a morphism $f : X \to Y$ to another variety Y is a K-algebra homomorphism, since composing a constant function with f gives again a constant function. In fact, one can show that these are precisely the maps between the coordinate rings coming from morphisms of varieties, i. e. that Construction 0.11 gives a one-to-one correspondence

$$\{\text{morphisms } X \to Y\} \overset{1:1}{\longleftrightarrow} \{K\text{-algebra homomorphisms } A(Y) \to A(X)\}.$$

Definition 1.26 (Generated subalgebras)**.** Let R' be an R-algebra.

(a) For any subset $M \subset R'$ let

$$R[M] := \bigcap_{\substack{T \supset M \\ R\text{-subalgebra of } R'}} T$$

be the smallest R-subalgebra of R' that contains M. We call it the R-subalgebra **generated by** M. If $M = \{c_1,\dots,c_n\}$ is finite, we write $R[M] = R[\{c_1,\dots,c_n\}]$ also as $R[c_1,\dots,c_n]$.

(b) We say that R' is a **finitely generated** R-algebra if there are finitely many $c_1,\dots,c_n$ with $R[c_1,\dots,c_n] = R'$.

Remark 1.27. Note that the square bracket notation in Definition 1.26 is ambiguous: $R[x_1,\dots,x_n]$ can either mean the polynomial ring over R as in Definition 0.2 (if $x_1,\dots,x_n$ are formal variables), or the subalgebra of an R-algebra R' generated by $x_1,\dots,x_n$ (if $x_1,\dots,x_n$ are elements of R'). Unfortunately, the usage of the notation $R[x_1,\dots,x_n]$ for both concepts is well-established in the literature, so we will adopt it here as well. Its origin lies in the following lemma, which shows that the elements of an R-subalgebra generated by a set M are just the polynomial expressions in elements of M with coefficients in R.

Lemma 1.28 (Explicit description of $R[M]$)**.** *Let M be a subset of an R-algebra R'. Then*

$$R[M] = \left\{ \sum_{i_1,\dots,i_n \in \mathbb{N}} a_{i_1,\dots,i_n}\, c_1^{i_1} \cdot \dots \cdot c_n^{i_n} : a_{i_1,\dots,i_n} \in R,\, c_1,\dots,c_n \in M, \text{ only finitely many } a_{i_1,\dots,i_n} \neq 0 \right\},$$

where multiplication in R' with elements of R is defined as in Remark 1.24.

Proof. It is obvious that this set of polynomial expressions is an R-subalgebra of R'. Conversely, every R-subalgebra of R' containing M must also contain these polynomial expressions, so the result follows. □

Example 1.29. In the field $\mathbb{C}$ of complex numbers the $\mathbb{Z}$-algebra generated by the imaginary unit i is

$$\mathbb{Z}[i] = \{f(i) : f \in \mathbb{Z}[x]\} = \{a + b\,i : a,b \in \mathbb{Z}\} \quad \subset \mathbb{C}$$

by Lemma 1.28. (Note again the double use of the square bracket notation: $\mathbb{Z}[x]$ is the polynomial ring over $\mathbb{Z}$, whereas $\mathbb{Z}[i]$ is the $\mathbb{Z}$-subalgebra of $\mathbb{C}$ generated by i.)

Lemma 1.30 (Finitely generated R-algebras)**.** *An algebra R' over a ring R is finitely generated if and only if $R' \cong R[x_1,\dots,x_n]/I$ for some $n \in \mathbb{N}$ and an ideal I in the polynomial ring $R[x_1,\dots,x_n]$.*

Proof. Certainly, $R[x_1,\dots,x_n]/I$ is a finitely generated R-algebra since it is generated by the classes of $x_1,\dots,x_n$. Conversely, let R' be an R-algebra generated by $c_1,\dots,c_n \in S$. Then

$$\varphi : R[x_1,\dots,x_n] \to R',\ \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n}\, x_1^{i_1} \cdot \dots \cdot x_n^{i_n} \mapsto \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n}\, c_1^{i_1} \cdot \dots \cdot c_n^{i_n}$$

is a ring homomorphism, and its image is precisely $R[c_1,\dots,c_n] = R'$ by Lemma 1.28. So by the homomorphism theorem [G1, Proposition 8.12] φ induces a ring isomorphism $R[x_1,\dots,x_n]/\ker\varphi \cong R'$, which by construction is also an R-algebra isomorphism. □

Remark 1.31 (Coordinate rings = reduced finitely generated K-algebras)**.** Let K be an algebraically closed field. Then by Remark 1.10 the coordinate rings of varieties over K are exactly the rings of the form $K[x_1,\dots,x_n]/I$ for a radical ideal $I \trianglelefteq K[x_1,\dots,x_n]$, so by Lemma 1.3 and Lemma 1.30 precisely the reduced finitely generated K-algebras.