# 2. Prime and Maximal Ideals

There are two special kinds of ideals that are of particular importance, both algebraically and geometrically: the so-called prime and maximal ideals. Let us start by defining these concepts.

**Definition 2.1** (Prime and maximal ideals)**.** Let $I$ be an ideal in a ring $R$ with $I \neq R$.

(a) $I$ is called a **prime ideal** if for all $a, b \in R$ with $ab \in I$ we have $a \in I$ or $b \in I$. By induction, this is obviously the same as saying that for all $a_1, \dots, a_n \in R$ with $a_1 \cdot \dots \cdot a_n \in I$ one of the $a_i$ must be in $I$.

(b) $I$ is called a **maximal ideal** if there is no ideal $J$ with $I \subsetneq J \subsetneq R$.

(c) The set of all prime ideals of $R$ is called the **spectrum**, the set of all maximal ideals the **maximal spectrum** of $R$. We denote these sets by $\operatorname{Spec} R$ and $\operatorname{mSpec} R$, respectively.

**Remark 2.2.** Let $R \neq \{0\}$ be a ring. Note that its two trivial ideals $R$ and $(0)$ are treated differently in Definition 2.1:

(a) The whole ring $R$ is by definition never a prime or maximal ideal. In fact, maximal ideals are just defined to be the inclusion-maximal ones among all ideals that are not equal to $R$.

(b) The zero ideal $(0)$ may be prime or maximal if the corresponding conditions are satisfied. More precisely, by definition $(0)$ is a prime ideal if and only if $R$ is an integral domain [G1, Definition 7.6 (d)], and it is maximal if and only if there are no ideals except $(0)$ and $R$, i. e. if $R$ is a field [G1, Example 8.8 (c)].

In fact, there is a similar criterion for arbitrary ideals if one passes to quotient rings:

**Lemma 2.3.** *Let $I$ be an ideal in a ring $R$ with $I \neq R$.*

(a) *$I$ is a prime ideal if and only if $R/I$ is an integral domain.*

(b) *$I$ is a maximal ideal if and only if $R/I$ is a field.*

*Proof.*

(a) Passing to the quotient ring $R/I$, the condition of Definition 2.1 (a) says that $I$ is prime if and only if for all $\overline{a}, \overline{b} \in R/I$ with $\overline{a}\,\overline{b} = \overline{0}$ we have $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, i. e. if and only if $R/I$ is an integral domain.

(b) By Lemma 1.21, the condition of Definition 2.1 (b) means exactly that the ring $R/I$ has only the trivial ideals $I/I$ and $R/I$, which is equivalent to $R/I$ being a field [G1, Example 8.8 (c)]. □

We can view this lemma as being analogous to Lemma 1.3, which asserted that $I$ is a radical ideal if and only if $R/I$ is reduced. The fact that these properties of ideals are reflected in their quotient rings has the immediate consequence that they are preserved under taking quotients as in Lemma 1.21:

**Corollary 2.4.** *Let $I \subset J$ be ideals in a ring $R$. Then $J$ is radical / prime / maximal in $R$ if and only if $J/I$ is radical / prime / maximal in $R/I$.*

*Proof.* By Lemma 1.3, the ideal $J$ is radical in $R$ if and only if $R/J$ is reduced, and $J/I$ is radical in $R/I$ if and only if $(R/I)/(J/I)$ is reduced. But these two rings are isomorphic by Exercise 1.22, so the result follows.

The statement about prime and maximal ideals follows in the same way, using Lemma 2.3 instead of Lemma 1.3. □

**Corollary 2.5.** *Every maximal ideal in a ring is prime, and every prime ideal is radical.*

*Proof.* Passing to the quotient ring, this follows immediately from Lemma 1.3 and Lemma 2.3 since a field is an integral domain and an integral domain is reduced. □

**Example 2.6.**

(a) Let $R$ be an integral domain, and let $p \in R\backslash\{0\}$ not be a *unit*, i. e. it does not have a multiplicative inverse in $R$ [G1, Definition 7.6 (a)]. Then by definition the ideal $(p)$ is prime if and only if for all $a, b \in R$ with $p \mid ab$ we have $p \mid a$ or $p \mid b$, i. e. by definition if and only if $p$ is a *prime element* of $R$ [G1, Definition 11.1 (b)]. Of course, this is the origin of the name "prime ideal".

(b) We claim that for non-zero ideals in a principal ideal domain $R$ the notions of prime and maximal ideals agree. To see this, is suffices by Corollary 2.5 to show that every non-zero prime ideal is maximal. So let $I \trianglelefteq R$ be prime. Of course, we have $I = (p)$ for some $p \in R$ as $R$ is a principal ideal domain, and since $I \neq R$ by definition and $I \neq 0$ by assumption we know by (a) that $p$ is prime. Now if $J \supset I$ is another ideal we must have $J = (q)$ for some $q \mid p$. But $p$ is prime and thus *irreducible*, i. e. it cannot be written as a product of two non-units in $R$ [G1, Definition 11.1 (a) and Lemma 11.3]. So up to a unit $q$ must be 1 or $p$. But then $J = R$ or $J = I$, respectively, which means that $I$ must have been maximal.

(c) Let $K$ be a field, and consider the ideal $I(a) = (x_1 - a_1, \ldots, x_n - a_n) \trianglelefteq K[x_1, \ldots, x_n]$ of $a$ for a given point $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$ as in Example 0.7. Then the ring homomorphism

$$K[x_1, \ldots, x_n]/I(a) \to K, \ \overline{f} \mapsto f(a)$$

is obviously an isomorphism, since $f \in I(a)$ is by definition equivalent to $f(a) = 0$. So $K[x_1, \ldots, x_n]/I(a) \cong K$ is a field, and thus by Lemma 2.3 (b) the ideal $I(a)$ is maximal.

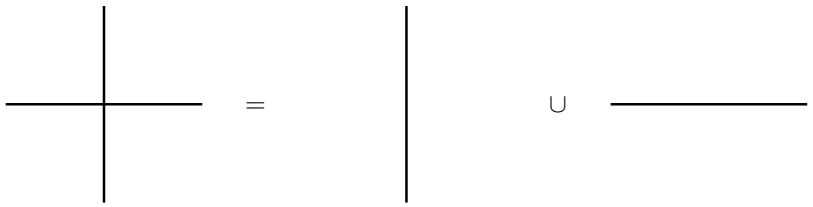
For general fields, not all maximal ideals of $K[x_1, \ldots, x_n]$ have to be of this form. For example, the ideal $(x^2 + 1) \trianglelefteq \mathbb{R}[x]$ is also maximal by (a) and (b), since the real polynomial $x^2 + 1$ is irreducible and thus prime in $\mathbb{R}[x]$ [G1, Proposition 11.5]. But if $K$ is algebraically closed, we will see in Corollary 10.10 that the ideals considered above are the only maximal ideals in the polynomial ring. In fact, it is easy to see that we would expect this if we look at the following geometric interpretation of maximal ideals.

**Remark 2.7** (Geometric interpretation of prime and maximal ideals)**.** Let $X$ be a variety over an algebraically closed field $K$, so that we have a one-to-one correspondence between subvarieties of $X$ and radical ideals in $A(X)$ by Remark 1.10.

(a) As the correspondence between subvarieties and ideals reverses inclusions, the maximal ideals of $A(X)$ correspond to minimal subvarieties of $X$, i. e. to points of $X$. For example, we have just seen in Example 2.6 (c) that the maximal ideal $(x_1 - a_1, \ldots, x_n - a_n) \trianglelefteq K[x_1, \ldots, x_n]$ is the ideal $I(a)$ of the point $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$.

(b) Let $Y$ be a non-empty subvariety of $X$, corresponding to a proper ideal $I(Y) \trianglelefteq A(X)$.

If $I(Y)$ is *not* prime then there are functions $f_1, f_2 \in A(X)$ such that $f_1 \cdot f_2$ vanishes on $Y$, but $f_1$ and $f_2$ do not. Hence the zero loci $Y_1 := V_Y(f_1)$ and $Y_2 := V_Y(f_2)$ of $f_1$ and $f_2$ on $Y$ are not all of $Y$, but their union is $Y_1 \cup Y_2 = V_Y(f_1 f_2) = Y$. So we can write $Y$ as a non-trivial union of two subvarieties. If a variety has this property we call it *reducible*, otherwise *irreducible*. As shown in the picture below, the union $Y = V(x_1 x_2)$ of the two coordinate axes in $\mathbb{A}^2_{\mathbb{R}}$ is a typical example of a reducible variety, with $f_1 = x_1$ and $f_2 = x_2$ in the notation above.




$Y = V(x_1 x_2)$ $Y_1 = V(x_1)$ $Y_2 = V(x_2)$

Conversely, if $Y$ is reducible with $Y = Y_1 \cup Y_2$ for two proper subvarieties $Y_1$ and $Y_2$, we can find $f_1 \in I(Y_1) \backslash I(Y)$ and $f_2 \in I(Y_2) \backslash I(Y)$. Then $f_1 f_2 \in A(X)$ vanishes on $Y$ although $f_1$ and $f_2$ do not, and thus $I(Y)$ is not a prime ideal.

Summarizing, we get the following correspondence:

| SUBVARIETIES | $\longleftrightarrow$ | IDEALS |
|---|---|---|
| *irreducible* | | *prime ideal* |
| *point* | | *maximal ideal* |

**Exercise 2.8.** Which of the following ideals are prime, which ones are maximal in $\mathbb{Z}[x]$?

$$I = (5, x^3 + 2x + 3) \qquad J = (4, x^2 + x + 1, x^2 + x - 1)$$

**Exercise 2.9.** Let $\varphi : R \to S$ be a ring homomorphism, and let $I \trianglelefteq S$. Show that:

(a) If $I$ is radical, then so is $\varphi^{-1}(I)$.

(b) If $I$ is prime, then so is $\varphi^{-1}(I)$.

(c) If $I$ is maximal, then $\varphi^{-1}(I)$ need not be maximal.

**Exercise 2.10.** Let $R$ be a ring.

(a) Let $I_1, \dots, I_n \trianglelefteq R$, and let $P \trianglelefteq R$ be a prime ideal. If $P \supset I_1 \cap \dots \cap I_n$, prove that $P \supset I_k$ for some $k = 1, \dots, n$.

(b) Let $I \trianglelefteq R$, and let $P_1, \dots, P_n \trianglelefteq R$ be prime ideals. If $I \subset P_1 \cup \dots \cup P_n$, prove that $I \subset P_k$ for some $k = 1, \dots, n$.

(c) Show that the statement of (b) still holds if $P_1$ is not necessarily prime (but $P_2, \dots, P_n$ still are).

Can you give a geometric interpretation of these statements?

**Exercise 2.11.** Let $R$ be the ring of all continuous real-valued functions on the unit interval $[0,1]$. Similarly to Definition 0.3 (c), for any subset $S$ of $R$ we denote by

$$V(S) := \{a \in [0,1] : f(a) = 0 \text{ for all } f \in S\} \quad \subset [0,1]$$

the zero locus of $S$. Prove:

(a) For all $a \in [0,1]$ the ideal $I_a := \{f \in R : f(a) = 0\}$ is maximal.

(b) If $f_1, \dots, f_n \in R$ with $V(f_1, \dots, f_n) = \emptyset$, then $f_1^2 + \dots + f_n^2$ is invertible in $R$.

(c) For any ideal $I \trianglelefteq R$ with $I \neq R$ we have $V(I) \neq \emptyset$.

(d) The assignment $[0,1] \to \operatorname{mSpec} R$, $a \mapsto I_a$ gives a one-to-one correspondence between points in the unit interval and maximal ideals of $R$ (compare this to Remark 2.7 (a)).

**Exercise 2.12.** Let $R$ be a ring such that for all $a \in R$ there is a natural number $n > 1$ with $a^n = a$.

(a) Show that every prime ideal of $R$ is maximal.

(b) Give an example of such a ring which is neither a field nor the zero ring.

We have now studied prime and maximal ideals in some detail, but left out one important question: whether such ideals actually always exist. More precisely, if $I$ is an ideal in a ring $R$ with $I \neq R$, is it guaranteed that there is a maximal (and hence also prime) ideal that contains $I$? In particular, taking $I = (0)$, is it clear that there is any maximal ideal in $R$ at all? From a geometric point of view this seems to be trivial: using the translations of Remark 2.7 (a) we are just asking whether a non-empty variety always contains a point — which is of course true. But we know already that not every ring is the coordinate ring of a variety, so for general rings we have to find an algebraic argument that ensures the existence of maximal ideals. It turns out that this is rather tricky, so let us start by giving the idea how such maximal ideals could be found.

**Remark 2.13** (Naive strategy to find maximal ideals)**.** Let $I$ be an ideal in a ring $R$ with $I \neq R$; we want to find a maximal ideal that contains $I$. Set $I_0 := I$. Of course, there is nothing to be done if $I_0$ is already maximal, so let us assume that it is not. Then there is an ideal $I_1$ with $I_0 \subsetneq I_1 \subsetneq R$. Now if $I_1$ is maximal we are done, otherwise we find an ideal $I_2$ with $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq R$. Continuing this process, we either find a maximal ideal containing $I$ after a finite number of steps, or arrive at an infinite strictly increasing chain

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

of ideals in $R$.

Is it possible that such an infinite chain of ideals exists? In general, the answer to this question is yes (see e. g. Example 7.2 (c)). There is a special and very important class of rings however — the *Noetherian rings* that we will discuss in Chapter 7 — that do not admit such infinite increasing chains of ideals. In these rings the above process must terminate, and so we can easily find a maximal ideal containing $I$. In fact, all coordinate rings of varieties turn out to be Noetherian (see Remark 7.15), which is why our geometric picture above suggested that the existence of maximal ideals might be trivial. 03

But what can we do if the chain above does not terminate? The main observation is that we can then form a "limit"

$$I_\infty := \bigcup_{n \in \mathbb{N}} I_n$$

over all previous ideals (it is easy to see that this is in fact an ideal which is not equal to $R$; we will check this in the proof of Corollary 2.17). Of course, $I_\infty$ is strictly bigger than every $I_n$. So it is an ideal that we have not seen before in the chain, and consequently we can continue the above process with this limit ideal: if it is maximal we are finished, otherwise choose a bigger one which we might call $I_{\infty+1}$, and so on. Unless we find a maximal ideal at some point, we can thus construct another infinite increasing chain starting with $I_\infty$, take the limit over this chain again, repeat the whole process of constructing a chain and taking its limit infinitely many times, take the limit over all these infinitely many limit ideals, and so on. Intuitively speaking, we obtain an increasing "chain" of ideals in this way that is *really* long, certainly not indexed any more by the natural numbers, and not even countable. Continuing our sloppy wording, we could hope that eventually we would have to obtain even more ideals in this way than there are subsets of $R$ at all. This would of course be a contradiction, suggesting that the process must stop at some point and give us a maximal ideal.

In fact, we will now make this argument precise. The key step in the proof is *Zorn's Lemma*, which abstracts from the above situation of rings and ideals and roughly states that in any sort of structure where you can compare objects and the above "limiting process over chains" works to get something bigger than what you had before, you will find a maximal object. To be able to formulate this rigorously we need some definitions regarding orders on sets.

**Definition 2.14** (Orders)**.** Let $\leq$ be a relation on a set $M$.

(a) We call $\leq$ a **partial order** on $M$ if:
  (i) $a \leq a$ for all $a \in M$ (we say $\leq$ is *reflexive*);
  (ii) for all $a, b, c \in M$ with $a \leq b$ and $b \leq c$ we have $a \leq c$ (we say $\leq$ is *transitive*);
  (iii) for all $a, b \in M$ with $a \leq b$ and $b \leq a$ we have $a = b$ (we say $\leq$ is *antisymmetric*).

(b) If in addition $a \leq b$ or $b \leq a$ for all $a, b \in M$, then $\leq$ is called a **total order** on $M$.

(c) An element $b \in M$ is an **upper bound** for a subset $A \subset M$ if $a \leq b$ for all $a \in A$.

(d) An element $a \in M$ is called **maximal** if for all $b \in M$ with $a \leq b$ we have $b = a$.

For a partial order $\leq$ we write $a < b$ if $a \leq b$ and $a \neq b$. A set $M$ together with a partial or total order is called a **partially** or **totally ordered set**, respectively.

**Example 2.15.**

(a) The sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ with their standard order are all totally ordered sets.

(b) Certainly the most important example of a partial order (in fact, probably our only example) is the set-theoretic inclusion, where $M$ is any family of sets. Note that this is in general not a total order since for two sets $A, B \in M$ it might of course happen that neither $A \subset B$ nor $B \subset A$ holds. But if we have a chain $A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots$ of sets (or even a "longer chain" as in Remark 2.13) then the family $\{A_0, A_1, A_2, \dots\}$ of all sets in this chain is totally ordered by inclusion. So totally ordered sets will be our generalization of chains to families that are not necessarily indexed by the natural numbers.

(c) If $M$ is the set of all ideals $I \neq R$ in a ring $R$, partially ordered by inclusion as in (b), then the maximal elements of $M$ are by definition exactly the maximal ideals of $R$.

(d) In contrast to the case of total orders, a maximal element $a$ in a partially ordered set $M$ need not be an upper bound for $M$, because $a$ might not be comparable to some of the elements of $M$.

With this notation we can thus translate our informal condition in Remark 2.13 that "the limiting process works" into the rigorous requirement that every totally ordered set should have an upper bound. If this condition is met, Zorn's Lemma guarantees the existence of a maximal element and thus makes the intuitive argument of Remark 2.13 precise:

**Proposition 2.16** (Zorn's Lemma)**.** *Let $M$ be a partially ordered set in which every totally ordered subset has an upper bound. Then $M$ has a maximal element.*

Before we prove Zorn's Lemma, let us first apply it to the case of ideals in rings to see that it really solves our existence problem for maximal ideals.

**Corollary 2.17** (Existence of maximal ideals)**.** *Let $I$ be an ideal in a ring $R$ with $I \neq R$. Then $I$ is contained in a maximal ideal of $R$.*

*In particular, every ring $R \neq 0$ has a maximal ideal.*

*Proof.* Let $M$ be the set of all ideals $J \trianglelefteq R$ with $J \supset I$ and $J \neq R$. By Example 2.15 (c), the maximal ideals of $R$ containing $I$ are exactly the maximal elements of $M$, and hence by Zorn's Lemma it suffices to show that every totally ordered subset of $M$ has an upper bound.

So let $A \subset M$ be a totally ordered subset, i. e. a family of proper ideals of $R$ containing $I$ such that, for any two of these ideals, one is contained in the other. If $A = \emptyset$ then we can just take $I \in M$ as an upper bound for $A$. Otherwise, let

$$J' := \bigcup_{J \in A} J$$

be the union of all ideals in $A$. We claim that this is an ideal:

- $0 \in J'$, since 0 is contained in each $J \in A$, and $A$ is non-empty.
- If $a_1, a_2 \in J'$, then $a_1 \in J_1$ and $a_2 \in J_2$ for some $J_1, J_2 \in A$. But $A$ is totally ordered, so without loss of generality we can assume that $J_1 \subset J_2$. It follows that $a_1 + a_2 \in J_2 \subset J'$.
- If $a \in J'$, i. e. $a \in J$ for some $J \in A$, then $ra \in J \subset J'$ for any $r \in R$.

Moreover, $J'$ certainly contains $I$, and we must have $J' \neq R$ since $1 \notin J$ for all $J \in A$, so that $1 \notin J'$. Hence $J' \in M$, and it is certainly an upper bound for $A$. Thus, by Zorn's Lemma, $M$ has a maximal element, i. e. there is a maximal ideal in $R$ containing $I$. □

So to complete our argument we have to give a proof of Zorn's Lemma. However, as most textbooks using Zorn's Lemma do not prove it but rather say that it is simply an axiom of set theory, let us first explain shortly in what sense we can prove it.

**Remark 2.18** (Zorn's Lemma and the Axiom of Choice)**.** As you know, essentially all of mathematics is built up on the notion of sets. Nevertheless, if you remember your first days at university, you were not given precise definitions of what sets actually are and what sort of operations you can do with them. One usually just uses the informal statement that a set is a "collection of distinct objects" and applies common sense when dealing with them.

Although this approach is good to get you started, it is certainly not satisfactory from a mathematically rigorous point of view. In fact, it is even easy to obtain contradictions (such as Russell's Paradox [G2, Remark 1.14]) if one applies common sense too naively when working with sets. So one needs strict axioms for set theory — the ones used today were set up by Zermelo and Fraenkel around 1930 — that state exactly which operations on sets are allowed. We do not want to list all these axioms here, but as a first approximation one can say that one can always construct new sets from old ones, whereas "circular definitions" (that try e. g. to construct a set that contains itself as an element) are forbidden.

Of course, the idea of these axioms is that they are all "intuitively obvious", so that nobody will have problems to accept them as the foundation for all of mathematics. One of them is the so-called *Axiom of Choice*; it states that if you have a collection of non-empty sets you can simultaneously choose an element from each of them (even if you do not have a specific rule to make your choice). For example, if you want to prove that a surjective map $f : A \to B$ has a right-sided inverse, i. e. a map $g : B \to A$ with $f \circ g = \mathrm{id}_B$, you need to apply the Axiom of Choice since you have to construct $g$ by simultaneously choosing an inverse image of every element of $B$ under $f$. In a similar way you have probably used the Axiom of Choice many times already without knowing about it — simply because it seems intuitively obvious.

Now it happens that Zorn's Lemma is in fact equivalent to the Axiom of Choice. In other words, if we removed the Axiom of Choice from the axioms of set theory we could actually prove it if we took Zorn's Lemma as an axiom instead. But nobody would want to do this since the statement of the Axiom of Choice is intuitively clear, whereas Zorn's Lemma is certainly not. So it seems a bit cheated not to prove Zorn's Lemma because it could be taken as an axiom.

Having said all this, what we want to do now is to assume the Axiom of Choice (which you have done in all your mathematical life anyway) and to prove Zorn's Lemma with it. To do this, we need one more notion concerning orders.

**Definition 2.19** (Well-ordered sets)**.** A totally ordered set $M$ is called **well-ordered** if every non-empty subset $A$ of $M$ has a minimum, i. e. an element $a \in A$ such that $a \leq b$ for all $b \in A$.

**Example 2.20.**

(a) Any finite totally ordered set is well-ordered. Every subset of a well-ordered set is obviously well-ordered, too.

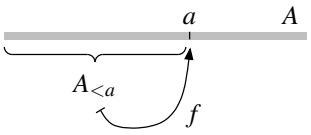
(b) The set $\mathbb{N}$ of natural numbers is well-ordered with its standard order, whereas $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are not. Instead, to construct "bigger" well-ordered sets than $\mathbb{N}$ one has to add "infinite elements": the set $\mathbb{N} \cup \{\infty\}$ (obtained from $\mathbb{N}$ by adding one more element which is defined to be bigger than all the others) is well-ordered. One can go on like this and obtain well-ordered sets $\mathbb{N} \cup \{\infty, \infty + 1\}$, $\mathbb{N} \cup \{\infty, \infty + 1, \infty + 2\}$, and so on.

It can be seen from these examples already that well-ordered sets are quite similar to the chains of ideals constructed in Remark 2.13. In fact, the idea of Remark 2.13 should be clearly visible in the following proof of Zorn's Lemma, in which our chains of ideals correspond to the $f$-sets introduced below, and the choice of a new bigger ideal that extends a previously constructed chain is given by the function $f$.

*Proof of Proposition 2.16 (Zorn's Lemma).* Let $M$ be a partially ordered set in which every *well-ordered* subset has an upper bound (this is all we will need — so we could in fact weaken the assumption of Proposition 2.16 in this way). We will prove Zorn's Lemma by contradiction, so assume that $M$ has no maximal element.

For any well-ordered subset $A \subset M$ there is then an upper bound which cannot be maximal, and so we can find an element of $M$ which is even bigger, and thus *strictly* bigger than all elements of $A$. Choose such an element and call it $f(A)$ — we can thus consider $f$ as a function from the set of all well-ordered subsets of $M$ to $M$. (Actually, this is the point where we apply the Axiom of Choice as explained in Remark 2.18.)

Let us call a subset $A \subset M$ an *$f$-set* (we choose this name to indicate that this notion depends on the choice of $f$ made above) if it is well-ordered and satisfies $a = f(A_{<a})$ for all $a \in A$, where we used the obvious notation $A_{<a} := \{b \in A : b < a\}$. Drawing $A$ symbolically as a line (since it is a totally ordered set after all), one can visualize this condition as in the picture on the right.




Intuitively, an $f$-set is thus determined at each point $a \in A$ by its predecessors in $A$ by applying $f$. For example:

- If an $f$-set $A$ has only finitely many elements $a_1 < \cdots < a_n$, we must have $a_1 = f(\emptyset)$ and $a_i = f(\{a_1, \ldots, a_{i-1}\})$ for $i = 2, \ldots, n$.
- If $A$ is an $f$-set, then $A \cup \{f(A)\}$ is also an $f$-set, obtained by "adding one element at the end" — and this is in fact the only element we could add at the end to obtain a new $f$-set.

In particular, we would expect that, although any two $f$-sets $A$ and $B$ might have different lengths, they should contain the same elements up to the point where one of them ends — so they should look like the picture below on the left, and not like the one on the right. Let us prove this rigorously:


*Claim:* If $A$ and $B$ are two $f$-sets and there is an element $b_0 \in B \backslash A$, then $A \subset B$ and $b_0$ is bigger than all elements of $A$.

To prove this, let $C$ be the union of all subsets of $A \cap B$ with the property that with any element they also contain all smaller elements in $A \cup B$ — let us call such subsets of $A \cap B$ *saturated*. Of course, $C$ is then saturated as well, so it is obviously the biggest saturated set. We can think of it as the part where $A$ and $B$ still coincide, as in the picture above.

By construction, it is clear that $C \subset A$. If we had $C \neq A$, then $A \backslash C$ and $B \backslash C$ would be non-empty (the latter because it contains $b_0$), and so there are $a = \min(A \backslash C)$ and $b = \min(B \backslash C)$ since $A$ and $B$ are well-ordered. Then $A_{<a} = B_{<b} = C$ by construction, and so $a = f(A_{<a}) = f(B_{<b}) = b$ as $A$ and $B$ are $f$-sets. But this means that $C \cup \{a\}$ is a bigger saturated set than $C$, which is a contradiction and shows that we must have $C = A$. So $A = C$ is a subset of $B$, and $b_0$ is bigger than all elements of $C = A$, proving our claim.

Now let $D$ be the union of all $f$-sets. Then every $a \in D$ is contained in an $f$-set $A$, and by our claim all elements of $D \backslash A$ (which must be contained in another $f$-set) are bigger than $a$. Hence $D$ is an $f$-set as well:

- $D$ is totally ordered (an element $a$ of an $f$-set $A$ is smaller than all elements of $D \backslash A$, and can be compared to all other elements of $A$ since $A$ is totally ordered);
- a minimum of any non-empty subset $D' \subset D$ can be found in any $f$-set $A$ with $A \cap D' \neq \emptyset$, since the other elements of $D'$ are bigger anyway — so $D$ is well-ordered;
- for any $a \in D$ in an $f$-set $A$ we have $f(D_{<a}) = f(A_{<a}) = a$.

So $D$ is the biggest $f$-set of $M$. But $D \cup \{f(D)\}$ is an even bigger $f$-set, which is a contradiction. Hence $M$ must have a maximal element. □

As another application of Zorn's lemma, let us prove a formula for the radical of an ideal in terms of prime ideals.

**Lemma 2.21.** *For every ideal $I$ in a ring $R$ we have*

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

*Proof.*

"$\subset$" If $a \in \sqrt{I}$ then $a^n \in I$ for some $n$. But then also $a^n \in P$ for every prime ideal $P \supset I$, which implies $a \in P$ by Definition 2.1 (a).

"$\supset$" Let $a \in R$ with $a \notin \sqrt{I}$, i. e. $a^n \notin I$ for all $n \in \mathbb{N}$. Consider the set

$$M = \{J : J \trianglelefteq R \text{ with } J \supset I \text{ and } a^n \notin J \text{ for all } n \in \mathbb{N}\}.$$

In the same way as in the proof of Corollary 2.17 we see that every totally ordered subset of $M$ has an upper bound (namely $I$ if the subset is empty, and the union of all ideals in the subset otherwise). Hence by Proposition 2.16 there is a maximal element $P$ of $M$. It suffices to prove that $P$ is prime, for then we have found a prime ideal $P \supset I$ with $a \notin P$, so that $a$ does not lie in the right hand side of the equation of the lemma.

So assume that we have $b, c \in R$ with $bc \in P$, but $b \notin P$ and $c \notin P$. Then $P + (b)$ and $P + (c)$ are strictly bigger than $P$, and thus by maximality cannot lie in $M$. This means that there are $n, m \in \mathbb{N}$ such that $a^n \in P + (b)$ and $a^m \in P + (c)$, from which we obtain

$$a^{n+m} \in (P + (b)) \cdot (P + (c)) \subset P + (bc) = P,$$

in contradiction to $P \in M$. Hence $P$ must be prime, which proves the lemma. □

**Remark 2.22.** Let $Y$ be a subvariety of a variety $X$. Then the statement of Lemma 2.21 for the (already radical) ideal $I(Y)$ in the ring $A(X)$ corresponds to the geometrically obvious statement that the variety $Y$ is the union of its irreducible subvarieties (see Remark 2.7).

**Exercise 2.23** (Minimal primes)**.** Let $I$ be an ideal in a ring $R$ with $I \neq R$. We say that a prime ideal $P \trianglelefteq R$ is *minimal over* $I$ if $I \subset P$ and there is no prime ideal $Q$ with $I \subset Q \subsetneq P$.

(a) Prove that there is always a minimal prime ideal over $I$.

(b) Determine all minimal prime ideals over $(x^2y, xy^2)$ in $\mathbb{R}[x, y]$.

If $R$ is the coordinate ring of a variety and $I$ the ideal of a subvariety, what is the geometric interpretation of a prime ideal minimal over $I$?

**Exercise 2.24.** Let $P$ and $Q$ be two distinct maximal ideals in a ring $R$, and let $n, m \in \mathbb{N}$. Show that $P^n$ and $Q^m$ are coprime.

**Exercise 2.25.** Show that for any ring $R$ the following three statements are equivalent:

(a) $R$ has exactly one prime ideal.

(b) Every element of $R$ is either a unit or nilpotent.

(c) $\sqrt{(0)}$ is a maximal ideal.

Give an example for such a ring which is not a field.

**Exercise 2.26.** Let $M$ be an infinite set.

(a) Use Zorn's Lemma to prove that $M$ can be written as a disjoint union of sets that are all countably infinite.

(b) Show that for any non-empty and at most countable set $A$ there is a bijection between $M$ and $M \times A$.

**Exercise 2.27.**

(a) Show that every vector space has a basis (even if it is not finitely generated).

(b) Let $n, m \in \mathbb{N}_{>0}$ with $n \neq m$. Of course, you know that $\mathbb{R}^n$ and $\mathbb{R}^m$ are not isomorphic as $\mathbb{R}$-vector spaces. However, prove now that $\mathbb{R}^n$ and $\mathbb{R}^m$ are isomorphic as groups (with the standard addition).

(Hint: Consider $\mathbb{R}^n$ and $\mathbb{R}^m$ as $\mathbb{Q}$-vector spaces, and use Exercise 2.26 (b).)

04