Ultraproducts

David Pierce

August 6, 2012

Mimar Sinan Güzel Sanatlar Üniversitesi
Matematik Bölümü
http://mat.msgsu.edu.tr/~dpierce/

Ultraproducts

Mathematics Department
Mimar Sinan Fine Arts University
Istanbul, Turkey
`http://mat.msgsu.edu.tr/~dpierce/`
`dpierce@msgsu.edu.tr`

1 Preface

These notes are for a course called Ultraproducts and Their Consequences, to be given at the Nesin Mathematics Village in Şirince, Selçuk, İzmir, Turkey, in August, 2012. The notes are mainly for my use; they do not constitute a textbook, although parts of them may have been written in textbook style. The notes have not been thoroughly checked for correctness; writing the notes has been my own way of learning some topics.

The notes have grown like a balloon, at all points: I have added things here and there as I have seen that they are needed or useful. I have also rearranged sections. There is too much material here for a week-long course. Some of the material is background necessary for thorough consideration of some topics; this background may be covered in a simultaneous course in Şirince.

The catalogue listing for the course[1](with abstract as submitted by me on January 27, 2012) is as follows.

Title of course: Ultraproducts and their consequences
Instructor: Assoc. Prof. David Pierce
Institution: Mimar Sinan GSÜ
Dates: 13–19 Ağustos 2012
Prerequisites: Some knowledge of algebra, including the theorem that a quotient of a ring by an ideal is a field if and only if the ideal is maximal.
Level: Advanced undergraduate and graduate
Abstract: An ultraproduct is a kind of average of infinitely many structures. The construction is usually traced to a 1955 paper of Jerzy Los; however, the idea of an ultraproduct can be found in Kurt

[1] From http://matematikkoyu.org/etkinlikler/2012-tmd-lisans-lisansustu/ultra_pierce.pdf, to which there is a link on http://matematikkoyu.org/etkinlikler/2012-tmd-lisans-lisansustu/ as of August 6, 2012.

> Goedel's 1930 proof (from his doctoral dissertation) of the Completeness Theorem for first-order logic. Non-standard analysis, developed in the 1960s by Abraham Robinson, can be seen as taking place in an ultraproduct of the ordered field of real numbers: more precisely, in an ultrapower. Indeed, for each integer, the 'average' real number is greater than that integer; therefore an ultrapower of the ordered field of real numbers is an ordered field with infinite elements and therefore infinitesimal elements. Perhaps the first textbook of model theory is Bell and Slomson's *Models and Ultraproducts* of 1969: the title suggests the usefulness of ultraproducts in the development various model-theoretic ideas. Our course will investigate ultraproducts, starting from one of the simplest interesting examples: the quotient of the cartesian product of an infinite collection of fields by a maximal ideal that has nontrivial projection onto each coordinate. No particular knowledge of logic is assumed.

Such was the abstract that I submitted in January. I have written the following notes since then, by way of working out for myself some of the ideas that might be presented in the course. I have tried to emphasize examples. In some cases, I may have sacrificed generality for concreteness. A theorem that I might have covered, but have not, is the theorem of Keisler and Shelah that elementary equivalence is the same thing as isomorphism of ultrapowers.

Contents

List of Figures

0 Notation

The set-theorist's natural numbers compose the set $\mathrm{\omega}$:

$$\mathrm{\omega} = \{0, 1, 2, \dots\}.$$

In these notes, this set is used:

1) as an index-set for countably infinite sequences $(a_k : k \in \mathrm{\omega})$;
2) as the cardinal number of each countably infinite set.[1]

The set-theoretic feature of $\mathrm{\omega}$ is that if $n \in \mathrm{\omega}$, then

$$n = \{0, \dots, n-1\}.$$

In particular

$$0 = \varnothing, \qquad 1 = \{0\}, \qquad 2 = \{0, 1\}.$$

If A and B are sets, we let

$$A^B = \{\text{functions from } B \text{ to } A\}.$$

In particular, if $n \in \mathrm{\omega}$, then

$$A^n = \{\text{functions from } n \text{ to } A\}.$$

An element of A^n may be written as either of

$$(b_0, \dots, b_{n-1}), \qquad (b^0, \dots, b^{n-1}),$$

and this can be abbreviated by

$$\boldsymbol{b},$$

[1]The $\mathrm{\omega}$ here is printed in an upright, 'roman' font, since it has a constant meaning. This means the sloping, 'italic' ω is available for use as a variable; but in fact it will not be used here.

in boldface: it is an n-**tuple** of elements of A. The superscripts in $(b^0, \dots, b^{n-1})$ are *not* exponents, but just (upper) indices; we may use them, because we shall occasionally use *lower* indices at the same time, as for example in consideration of sequences $(\boldsymbol{b}_k : k \in \omega)$, where $\boldsymbol{b}_k \in A^n$, so that

$$\boldsymbol{b}_k = (b^0_k, \dots, b^{n-1}_k).$$

Note that

$$A^0 = \{0\} = 1.$$

The ring of (rational) integers is $\mathbb{Z}$, which is a sub-ring of $\mathbb{Q}$, the field of rational numbers; this in turn is a subfield of $\mathbb{R}$, the field of real numbers. The set of *positive* integers can be denoted by $\mathbb{N}$. Thus

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

One could write this also as $\omega \smallsetminus \{0\}$. Some people also put 0 in $\mathbb{N}$, and that is fine. However, in these notes, I attempt to distinguish notationally the two roles of natural numbers: (1) as indices and (2) as rational numbers. In the former role, the natural numbers compose ω; in the latter, $\mathbb{N}$. It is also just useful to have distinct simple symbols for the two sets $\{0, 1, 2, \dots\}$ and $\{1, 2, 3, \dots\}$.

1 Introduction

1.1 Products of fields

Suppose $\mathscr{K}$ is an indexed family $(K_0, K_1, K_2, \dots)$ or $(K_i \colon i \in \omega)$, where each K_i is a *field.*[1] For example, each K_i might be $\mathbb{R}$, or each K_i might be a different finite field. We can form the **Cartesian product** of the family $\mathscr{K}$. This product is denoted by one of the expressions

$$\prod_{i\in\omega} K_i, \qquad\qquad \prod \mathscr{K}.$$

If a belongs to this product, this means

$$a = (a_i \colon i \in \omega),$$

where $a_i \in K_i$ in each case. Here a is simply a function on ω that, at every element i of this domain, takes a value in K_i; we write this value as a_i, though it could be written also[2] as $a(i)$ or a^i.

The product $\prod \mathscr{K}$ is a ring in the obvious way, with respect to the termwise operations:

$$\begin{aligned}
a + b &= (a_i + b_i \colon i \in \omega),\\
-a &= (-a_i \colon i \in \omega),\\
0 &= (0 \colon i \in \omega) = (0, 0, 0, \dots),\\
a \cdot b &= (a_i \cdot b_i \colon i \in \omega),\\
1 &= (1 \colon i \in \omega) = (1, 1, 1, \dots).
\end{aligned}$$

[1] The basic of rings and fields are reviewed, for completeness, in Chapter 8; but it is assumed that the reader is already somewhat familiar with them. In the present section, we could work with an arbitrary index set Ω in place of ω. Later (§3.2) we shall do this; but there is no obvious need to do so *now.*

[2] Even the notation i^a might be used. Indeed, a^σ is used below (p. 97, §8.4) for the image under an automorphism σ of an element a of a given field.

Suppose M is a *maximal ideal* of the ring $\prod \mathscr{K}$. Then the quotient $\prod \mathscr{K}/M$ is a field, called an **ultraproduct** of the family $\mathscr{K}$. We want to understand this ultraproduct.

There is a trivial case. There may be some j in ω such that

$$M = \{x \in \prod \mathscr{K} : x_j = 0\}.$$

Then M is a *principal ideal*: it is generated by an element

$$(1, \dots, 1, 0, 1, \dots),$$

where every entry is 1, except the entry 0 with index j. For, if this element of M is c, then for every a in M we have $a = a \cdot c$. In this case

$$x + M = y + M \iff x_j = y_j.$$

Thus $\prod \mathscr{K}/M \cong K_j$ under the map $x \mapsto x_j$. This isomorphism constitutes a proof that the ideal (c) generated by c is indeed maximal (since the quotient of a ring by an ideal is a field if and only if the ideal is maximal[3]). By contrast, if I is an ideal generated by an element

$$(1, \dots, 1, 0, 1, \dots, 1, 0, 1, \dots),$$

with two zero entries, indexed by j and ℓ respectively, then $\prod \mathscr{K}/I \cong K_j \times K_\ell$. Since then $K_j \times K_\ell$ is not a field—since for example the nonzero elements $(1, 0)$ and $(0, 1)$ are not invertible—, I must not be maximal.

If M is a nonprincipal maximal ideal of $\prod \mathscr{K}$, then the ultraproduct $\prod \mathscr{K}/M$ will be seen to be a kind of 'average' of the fields K_j. But this must be properly understood. More precisely, if $a \in \prod \mathscr{K}$, then $a + M$ will be a kind of average of the individual elements a_i of the factors K_i. We consider a particular example in the next section.

1.2 Ultrapowers of the field of real numbers

If each K_i is $\mathbb{R}$, then the product $\prod_{i \in \omega} K_i$ is the power $\mathbb{R}^\omega$. If M is a maximal ideal of this ring, then the quotient $\mathbb{R}^\omega/M$ is called an

[3] This is written out and proved below as Theorem 16 on page 86; but the reader should already be familiar with it.

ultrapower of $\mathbb{R}$. The field $\mathbb{R}$ embeds in $\mathbb{R}^\omega/M$ under the **diagonal map,**

$$x \mapsto (x, x, x, \dots) + M.$$

The diagonal map is so called, presumably because of the similarity of its definition to that of the map $x \mapsto (x, x)$ from $\mathbb{R}$ to $\mathbb{R}^2$, whose range is called a 'diagonal' line.[4] Perhaps we are likely to consider points $(x, x, x, \dots)$ of R^ω themselves as *horizontal* lines, as in Figure 1.1. It

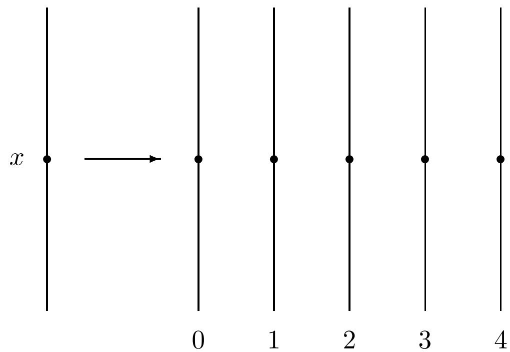

Figure 1.1: The diagonal map

should be clear that the diagonal map is an embedding of $\mathbb{R}$ in $\mathbb{R}^\omega/M$: it is a monomorphism, with trivial kernel. For, if $x \neq 0$, then for every element a of $\mathbb{R}^\omega$ we have

$$a = \left(\frac{a_0}{x}, \frac{a_1}{x}, \frac{a_2}{x}, \dots\right) \cdot (x, x, x, \dots) = \left(\frac{a_i}{x} \colon i \in \omega\right) \cdot (x \colon i \in \omega).$$

Thus, if it were possible that $x \neq 0$, but $(x, x, x, \dots) \in M$, then M would be the improper ideal $\mathbb{R}^\omega$.

If M is a non-principal maximal ideal of $\mathbb{R}^\omega$, then the diagonal embedding of $\mathbb{R}$ in $\mathbb{R}^\omega/M$ is not surjective: it is not an epimorphism. For, the element $(1, 2, 3, \dots) + M$ of the quotient is not in its range. See Figure 1.2. Indeed, suppose if possible

$$(1, 2, 3, \dots) + M = (x, x, x, \dots) + M,$$

[4]Etymologically speaking, a diagonal line is a line joining two angles of a polygon.

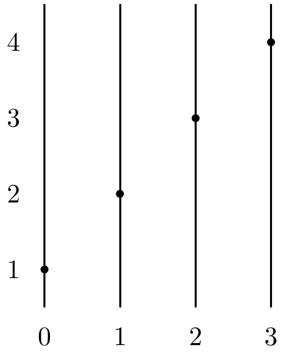

Figure 1.2: An infinite element of $\mathbb{R}^\omega/M$

so that $(1-x, 2-x, 3-x, \dots) \in M$. If $x \notin \mathbb{N}$, then for every a in $\mathbb{R}^\omega$ we have

$$a = \left(\frac{a_0}{1-x}, \frac{a_1}{2-x}, \frac{a_2}{3-x}, \dots\right) \cdot (1-x, 2-x, 3-x, \dots),$$

which must be in M; and this contradicts that M is proper. If $x \in \mathbb{N}$, so that $1-x$ is a non-positive element n of $\mathbb{Z}$, then M contains $(n, n+1, \dots, -1, 0, 1, 2, \dots)$, and therefore M also contains $(1, \dots, 1, 0, 1, \dots)$, because this is

$$(n, n+1, \dots, -1, 0, 1, 2, \dots) \cdot \left(\frac{1}{n}, \frac{1}{n+1}, \dots, \frac{1}{-1}, 0, \frac{1}{1}, \frac{1}{2}, \dots\right).$$

Thus M includes a principal maximal ideal as before, so M itself is either principal or improper.

On the assumption that M is a nonprincipal maximal ideal of $\mathbb{R}^\omega$, we have shown that the element $(1, 2, 3, \dots) + M$ of the quotient $\mathbb{R}^\omega/M$ is not in the image of $\mathbb{R}$ under the diagonal map. But this element will be seen as a kind of average of the elements of $\mathbb{N}$. Indeed, for every m in $\mathbb{N}$, all but finitely many elements of $\mathbb{N}$ are greater than m. So the 'average' element of $\mathbb{N}$ is greater than m. And we shall see that

$$(1, 2, 3, \dots) + M > (m, m, m, \dots) + M.$$

Since this will be true for all m in $\mathbb{N}$, the element $(1, 2, 3, \dots) + M$ of $\mathbb{R}^\omega/M$ will be *infinite.*

But so far, all we know is that $\mathbb{R}^\omega/M$ is a field. We now want to show that it has a (linear) ordering that makes it into an ordered field.

1.3 Ordered rings

In these notes, a **ring** is always a commutative unital ring. Then an **ordered ring** (or more precisely a *partially ordered ring*) is a pair (R, R^+), where R is a ring in our sense, and R^+ is a subset of R that is closed under addition and multiplication and that, for all x in R, contains both x and $-x$ if and only if $x = 0$. That is,

$$x \in R \;\&\; y \in R \implies x + y \in R \;\&\; xy \in R,$$
$$x \in R \;\&\; -x \in R \implies x = 0,$$
$$0 \in R.$$

In this case, we can define

$$x \leqslant y \iff y - x \in R^+.$$

Then

$$R^+ = \{x \in R \colon 0 \leqslant x\}.$$

The set R^+ is the **positive cone** of $\leqslant$. However, only the elements of $R^+ \smallsetminus \{0\}$ should be called positive.[5] It follows that

(1) the relation $\leqslant$ is reflexive, that is,

$$x \leqslant x,$$

since $x - x \in R^+$;

[5] The Wikipedia article 'Ordered ring' defines this as what, for present purposes, should be called a linearly or totally ordered ring: it meets the additional condition that at least one of x and $-x$ is always in R^+. Then what for us is an ordered ring is what, for the Wikipedia article, should be called a partially ordered ring; but the article defines no such thing. At least this is the situation as of July 22, 2012. The notation R^+ and the term *positive cone* are used only in another Wikipedia article, 'Partially ordered group'. The notation and term are unfortunate, since the positive cone in the present sense contains 0, but the real number 0 is not normally considered positive. We could define ordered rings in terms of the set $\{x \colon x > 0\}$; but then the possibility of positive zero-divisors would have to be dealt with; also, there would be a complication in the definition of the product order.

(2) the relation $\leqslant$ is anti-symmetric, that is,

$$x \leqslant y \ \ \& \ \ y \leqslant x \implies x = y,$$

since if $y - x$ and $x - y$ are in R^+, then they must be 0;

(3) the relation $\leqslant$ is transitive, that is,

$$x \leqslant y \ \ \& \ \ y \leqslant z \implies x \leqslant z,$$

since if $y - x$ and $z - y$ are in R^+, so is their sum, $z - x$.

The relation $\leqslant$ is thus a (partial) ordering of R, induced by R^+. Moreover,

(4) this ordering is translation-invariant, that is,

$$x \leqslant y \implies x + z \leqslant y + z,$$

since if $y - x$ is in R^+, so is $(y + z) - (x + z)$. Finally,

(5) multiplication by positive elements preserves the ordering, that is,

$$x \leqslant y \ \ \& \ \ 0 < z \implies xz \leqslant yz,$$

since if $y - x$ and z are in R^+, so is their product, $zy - zx$.

Conversely, these properties of $\leqslant$ imply that the set $\{x \in R \colon 0 \leqslant x\}$ is a positive cone that induces the ordering $\leqslant$. So we can write (R, R^+) also as $(R, \leqslant)$.

Suppose $((R_i, R_i^+) \colon i \in I)$ is an indexed family of ordered rings. Then easily the product

$$\Bigl(\prod_{i \in I} R_i, \prod_{i \in I} R_i^+\Bigr)$$

is an ordered ring. For example, the 'Cartesian plane' $\mathbb{R}^2$ (that is, $\mathbb{R} \times \mathbb{R}$) is an ordered ring whose positive cone is the first quadrant. See Figure 1.3. However, this quadrant is not the positive cone of an ordering of $\mathbb{C}$, since it is not closed under complex multiplication. The complex field does however have an ordering, whose positive cone consists of the non-negative real numbers (as in Figure 1.3). In this ordering, $a + b\mathrm{i} \leqslant x + y\mathrm{i}$

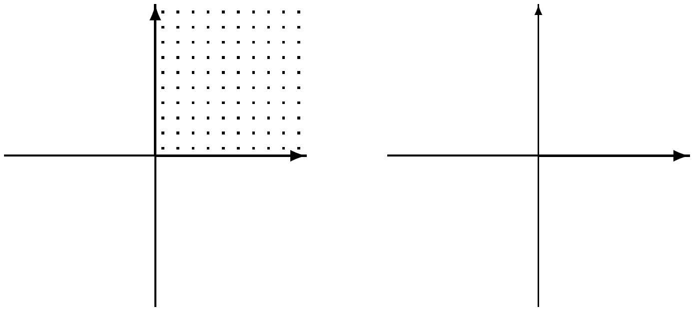

Figure 1.3: The positive cones of $\mathbb{R}^2$ and $\mathbb{C}$

if and only if $a \leqslant x$ and $b = y$. The product-ordering of the power $\mathbb{R}^\omega$ is given by the rule

$$0 \leqslant x \iff 0 \leqslant x_0 \;\&\; 0 \leqslant x_1 \;\&\; 0 \leqslant x_2 \;\&\; \dots \iff \bigwedge_{i \in \omega} 0 \leqslant x_i.$$

Suppose again (R, R^+) is an arbitrary ordered ring, and I is an ideal of R. We let

$$R^+/I = \{x + I \in R/I \colon x \in I\}.$$

It is possible that $x + I \in R^+/I$ although $x \notin R^+$. The set R^+/I is closed under addition and multiplication. So it is the positive cone of an ordering of R/I if and only if

$$x + I \in R^+/I \;\&\; -x + I \in R^+/I \implies x + I = I,$$

that is (since $-x + I \in R^+/I$ means $x + y \in I$ for some y in R^+),

$$x \in R^+ \;\&\; y \in R^+ \;\&\; x + y \in I \implies x \in I.$$

(By symmetry, $y \in I$ can also be concluded.) For example, the only proper, non-trivial ideals of the product ring $\mathbb{R}^2$ are the principal ideals generated respectively by $(1, 0)$ and $(0, 1)$. These ideals meet the desired condition with respect to the product ordering, and the quotient (in either case) is an ordered ring that is order-isomorphic to $\mathbb{R}$.

The same is true for ideals I of $\mathbb{R}^\omega$. Indeed, suppose x and y in $\mathbb{R}^\omega$ are positive or zero (that is, $x_i \geqslant 0$ and $y_i \geqslant 0$ in each case), and $x+y \in I$. Since

$$x_i + y_i = 0 \implies x_i = 0,$$

it follows that $x \in I$. Indeed, under the hypothesis, $x = (x+y)z$, where

$$z_i = \begin{cases} x_i/(x_i+y_i), & \text{if } x_i + y_i \neq 0, \\ 0, & \text{if } x_i + y_i = 0. \end{cases}$$

Thus $\mathbb{R}^\omega/I$ is ordered.

Now let M be a maximal ideal of $\mathbb{R}^\omega$. We want to show that the ordering of $\mathbb{R}^\omega/M$ is *linear.* For every a in $\mathbb{R}^\omega$, we have $a + M \geqslant 0$ if and only if there is b in M such that $a + b \geqslant 0$, that is, $a_i + b_i \geqslant 0$ in each case. If there is such an element b of M, it meets the condition

$$b_i = 0 \implies a_i \geqslant 0.$$

In this case, replacing b with an appropriate product bc, we may assume

$$b_i = 0 \iff a_i \geqslant 0. \tag{$*$}$$

Moreover, this condition on an element b of M is sufficient—not to ensure that $a + b \geqslant 0$, but to ensure that $a + d \geqslant 0$ for *some* d in M. This d could be $e \cdot b$, where, if $b_i \neq 0$, so that $a_i < 0$, then

$$e_i = \frac{-2a_i}{b_i}.$$

We can see now that the following are equivalent:

- $a + M \geqslant 0$.
- M has an element b such that $(*)$ holds.
- M contains every element b of $\mathbb{R}^\omega$ such that $(*)$ holds.

Suppose one of these conditions fails. Then there is some b in $\mathbb{R}^\omega \smallsetminus M$ such that $(*)$ holds. In this case, since M is maximal,

$$M + (b) = \mathbb{R}^\omega.$$

In particular, $(1,1,1,\dots) \in M + (b)$. Hence M has an element c such that

$$b_i = 0 \implies c_i \neq 0,$$

that is,

$$a_i \geqslant 0 \implies c_i \neq 0.$$

As before, by replacing c with a multiple of it, so that $c_i = 0$ when $a_i < 0$, we may assume

$$a_i \geqslant 0 \iff c_i \neq 0;$$

indeed, M contains *every* such element c of $\mathbb{R}^\omega$. Then not only does M contain c such that $a_i + c_i \neq 0$ for all i in ω, but it contains c such that $a_i + c_i < 0$ for all i in ω. Consequently $a + M < 0$, under the assumption that $a + M$ is not positive. Thus the ordering of $\mathbb{R}^\omega/M$ is linear.

1.4 Non-standard analysis

Suppose now M is a *non-principal* maximal ideal of $\mathbb{R}^\omega$. If $m \in \mathbb{N}$, we want to show finally

$$(1,2,3,\dots) + M > (m,m,m,\dots) + M,$$

that is,

$$(1-m, 2-m, 3-m, \dots, -1, 0, 1, 2, 3, \dots) + M > 0.$$

It is enough to show that M has an element a such that

$$i < m \implies a_i \neq 0. \tag{†}$$

Again, M is maximal, but not principal. In particular, it is not included in the principal maximal ideal generated by an element $(1,\dots,1,0,1,\dots)$. Then for all j in ω, M has an element that is nonzero at j. Therefore M contains δ^j, where

$$\delta^j_i = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Then M contains $\delta^0 + \dots + \delta^{m-1}$, which is an element a as desired in (†).

We may assume that $\mathbb{Q}$ is included in every ordered field. An element of an ordered field that is greater than every element of $\mathbb{Q}$ is **infinite;** an element whose absolute value is less than every positive element of $\mathbb{Q}$ is **infinitesimal.** We have now shown that $\mathbb{R}^\omega/M$ has infinite elements. Therefore it also has nonzero infinitesimal elements (namely the reciprocals of the infinite elements). Thus the possibility is opened up of saying that a function f from $\mathbb{R}$ to $\mathbb{R}$ is *continuous* at a if $f(a) - f(x)$ is infinitesimal whenever $a - x$ is infinitesimal.

However, $\mathbb{R}$ itself contains no infinitesimals; so if $a \in \mathbb{R}$, but $a - x$ is infinitesimal, then $x \notin \mathbb{R}$. However, x might be in $\mathbb{R}^\omega/M$. So we want to extend f to a function ${}^*f$ on $\mathbb{R}^\omega/M$. It is obvious how to do this: If $a \in \mathbb{R}^\omega$, then we should define

$$^*f(a + M) = (f(a_i) \colon i \in \omega) + M.$$

However, we must check that such a function ${}^*f$ exists: we must show

$$a + M = b + M \implies (f(a_i) \colon i \in \omega) + M = (f(b_i) \colon i \in \omega) + M,$$

or rather

$$a - b \in M \implies (f(a_i) - f(b_i) \colon i \in \omega) \in M.$$

But this is true since

$$a_i - b_i = 0 \implies f(a_i) - f(b_i) = 0,$$

so that, as before, $(f(a_i) - f(b_i) \colon i \in \omega)$ is a multiple of $a - b$.

We have been using implicitly (or proving special cases of) the lemma that if

$$a_i = 0 \implies b_i = 0$$

and $a \in M$, then $b \in M$. For an arbitrary element a of $\mathbb{R}^\omega$, we define

$$\operatorname{supp}(a) = \{i \in \omega \colon a_i \neq 0\}.$$

Let us now write $\mathfrak{m}$ for $\operatorname{supp}[M]$; that is,

$$\mathfrak{m} = \{\operatorname{supp}(x) \colon x \in M\}.$$

Then M is determined by $\mathfrak{m}$, and moreover

$$M = \{x \in \mathbb{R}^\omega \colon \operatorname{supp}(x) \in \mathfrak{m}\}.$$

The subset $\mathfrak{m}$ of $\mathscr{P}(\omega)$ has the following properties:

$$\varnothing \in \mathfrak{m},$$
$$X \subseteq Y \;\;\&\;\; Y \in \mathfrak{m} \implies X \in \mathfrak{m},$$
$$X \in \mathfrak{m} \;\;\&\;\; Y \in \mathfrak{m} \implies X \cup Y \in \mathfrak{m}.$$

Indeed, the first of these properties follows because $0 \in M$. The second is by the lemma just mentioned. For the third, if $\operatorname{supp}(a) = X$ and $\operatorname{supp}(b) = Y$, then $\operatorname{supp}(c \cdot b) = Y \smallsetminus X$ for some c, and then

$$\operatorname{supp}(a + c \cdot b) = X \cup Y.$$

Let us write $\mathfrak{u}$ for $\mathscr{P}(\omega) \smallsetminus \mathfrak{m}$. Then we have

$$\omega \in \mathfrak{u},$$
$$X \subseteq Y \;\;\&\;\; X \in \mathfrak{u} \implies Y \in \mathfrak{u},$$
$$X \in \mathfrak{u} \;\;\&\;\; Y \in \mathfrak{u} \implies X \cap Y \in \mathfrak{u}.$$

Finally,

$$X \in \mathfrak{m} \iff X \notin \mathfrak{u}.$$

Elements of $\mathfrak{m}$ will be called **small;** elements of $\mathfrak{u}$, **large.** If $a+M = b+M$, that is, $a-b \in M$, this means $\operatorname{supp}(a-b) \in \mathfrak{m}$, that is, a and b differ on a small subset of ω, but they agree on a large subset of ω. Then the same is true of $(f(a_i) \colon i \in \omega)$ and $(g(a_i) \colon i \in \omega)$. Thus there is a well-defined function ${}^*f$ as above.

Much more now follows. For example, $\mathbb{R}^\omega/M$ is **real-closed,** that is, it satisfies the Intermediate Value Theorem for polynomial functions. Indeed, suppose p is a polynomial (in one variable) with coefficients from $\mathbb{R}^\omega/M$ such that, for some a and b in $\mathbb{R}^\omega/M$, we have $p(a) < 0$ and $p(b) > 0$. We may assume $a < b$. It follows that

$$\{i \colon a_i < b_i\} \in \mathfrak{u}.$$

The value $p(a)$ of p at a can be written as $(p_i(a_i) \colon i \in \omega)$, where p_i is obtained from p by replacing its coefficients with their values at i. Then the sets $\{i \colon p_i(a_i) < 0\}$ and $\{i \colon p_i(b_i) > 0\}$ are large, and therefore their intersection is large, and therefore (by the usual Intermediate Value

Theorem for $\mathbb{R}$) there are c_i between a_i and b_i for a large set of i such that $p_i(c_i) = 0$. Choosing c_i for the other i arbitrarily, we have $a < c < b$, and $p(c) = 0$.

In model-theoretic terms, $\mathbb{R}^{\omega}/M$ is an *elementary extension* of $\mathbb{R}$. This is a special case of a general theorem, Łoś's Theorem, which is fairly easy to prove, once one understands what it is all about. The theorem itself is Theorem 4 on page 43 below; the pages before then are preparation for it. First we shall generalize the fields of the present chapter to arbitrary *structures*.

2 Model theory

2.1 Theories and models

If $n \in \omega$, then on a set A, an **n-ary relation** on A is just a subset of A^n; an **n-ary operation** on A is a function from A^n to A. Since $A^0 = \{0\}$, so that a function on A^0 takes only one value, a 0-ary or *nullary* operation on A can be considered as an element of A. Much of mathematics is a study of operations and relations on sets. Group-theory is a study of binary operations with certain properties; field-theory, *two* binary operations; lattice-theory, a binary relation.[1] A particular nonempty set,[2] considered together with certain operations and relations on it, is called a **structure.** If the set is A, B, or C, then the structure might be denoted respectively by $\mathfrak{A}$, $\mathfrak{B}$, or $\mathfrak{C}$. The distinguished operations and relations of $\mathfrak{A}$ are denoted by certain symbols, which constitute the **signature** of $\mathfrak{A}$. The **universe** of $\mathfrak{A}$ is just the set A.

More than one structure can share the same signature. For example, the signature of fields is $\{0, 1, -, +, \cdot\}$; of ordered fields, $\{0, 1, -, +, \cdot, <\}$ (or $\{0, 1, -, +, \cdot, \leqslant\}$). In general, if $\mathscr{S}$ is a signature, then the class of all structures with this signature can be denoted by

$$\mathrm{Mod}(\mathscr{S}).$$

If $\mathfrak{A} \in \mathrm{Mod}(\mathscr{S})$, and $s \in \mathscr{S}$, then, to avoid ambiguity, the operation or relation on A that is denoted in $\mathfrak{A}$ by s can also be denoted by

$$s^{\mathfrak{A}}.$$

[1] This is (nearly?) all that I shall say about *examples* in this chapter, despite the intention stated in the Preface to emphasize examples. Perhaps model-theory as a branch of mathematics can be characterized as *not* being about particular examples, but being an abstraction from them. In any case, the subject of these notes is not model-theory as such, but ultraproducts.

[2] It simplifies things to require the set to be nonempty, although one can certainly define empty structures if one wishes, and sometimes this is useful.

A symbol in a signature is more precisely

- an n**-ary predicate,** if it denotes an n-ary relation, or
- an n**-ary operation-symbol.**

The symbol for a nullary operation (that is, element) can be called a **constant.** The same symbol will never denote, say, an element of one set, but a binary relation on another set.

If $\mathscr{S}$ is a signature, then the *terms* of $\mathscr{S}$ are built up from the operation-symbols in $\mathscr{S}$, along with *(individual) variables.* The *formulas* of $\mathscr{S}$ are then built up from the terms and predicates of $\mathscr{S}$, along with logical symbols such as $\neg$, $\wedge$, and $\exists$ (and brackets, if needed). A term is merely a recipe for obtaining new operations through composition of some given operations. (The coordinate projections are always understood as given.) Then a formula is a recipe for obtaining new relations through set-theoretic manipulations of given operations and relations. We shall review the formal definition of terms and formulas in the next section.

An occurrence of a variable in a formula of $\mathscr{S}$ will be either *free* or *bound.* If precisely the variables x_0, ..., x_{n-1} occur freely in a formula φ of $\mathscr{S}$, then φ can be written as $\varphi(x_0, \dots, x_{n-1})$ or $\varphi(\boldsymbol{x})$. If $\mathfrak{A} \in \operatorname{Mod}(\mathscr{S})$, and $\boldsymbol{a} \in A^n$, then $\varphi(\boldsymbol{a})$ is the result of replacing each free occurrence of x_i in φ with a_i, for each i in n. This new formula $\varphi(\boldsymbol{a})$ may not be a formula of $\mathscr{S}$; but it is a formula of $\mathscr{S}(A)$, which is just $\mathscr{S}$ along with a constant for each element of A. Such constants are often called **parameters.** The new formula $\varphi(\boldsymbol{a})$ is a **sentence,** because it has no free variables. This sentence will be either true or false in $\mathfrak{A}$; if it is true, then we shall write

$$\mathfrak{A} \vDash \varphi(\boldsymbol{a}).$$

The symbol $\vDash$ thus stands for a relation in a more general sense: it is not a binary relation on a set, but it is a relation between certain structures and certain sentences. We might call this the **satisfaction** relation. (However, if $\mathfrak{A} \vDash \varphi(\boldsymbol{a})$, it might be said that $\boldsymbol{a}$ *satisfies* φ in $\mathfrak{A}$.)

The set of all sentences of $\mathscr{S}$ can be denoted by

$$\operatorname{Sn}(\mathscr{S}).$$

If $\Gamma \subseteq \operatorname{Sn}(\mathscr{S})$, and every sentence in Γ is true in $\mathfrak{A}$, then we write

$$\mathfrak{A} \vDash \Gamma;$$

in this case, $\mathfrak{A}$ is a **model** of Γ. We can define

$$\operatorname{Mod}(\Gamma) = \{\mathfrak{A} \in \operatorname{Mod}(\mathscr{S}) \colon \mathfrak{A} \vDash \Gamma\} = \bigcap_{\sigma\in\Gamma} \{\mathfrak{A} \in \operatorname{Mod}(\mathscr{S}) \colon \mathfrak{A} \vDash \sigma\}; \qquad (*)$$

a class of structures of this form is called an **elementary class.** If $\mathcal{K} \subseteq \operatorname{Mod}(\mathscr{S})$, then we define

$$\operatorname{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A}\in\mathcal{K}} \{\sigma \in \operatorname{Sn}(\mathscr{S}) \colon \mathfrak{A} \vDash \sigma\}; \qquad (\dagger)$$

a set of sentences of this form is called a **theory.** Both theories and elementary classes are defined in the same way, as intersections of sets defined in terms of the satisfaction relation $\vDash$. Therefore it turns out that there is a one-to-one correspondence between elementary classes and theories. This is a kind of *Galois correspondence*; see §8.4 (and before that, (†) on page 91).

If $\mathcal{K} = \{\mathfrak{A}\}$, then $\operatorname{Th}(\mathcal{K})$ can be written as

$$\operatorname{Th}(\mathfrak{A}).$$

Such a theory is a **complete theory,** namely a theory that, for every sentence σ if its signature, contains either σ or its negation $\neg\sigma$, but not both. For an arbitrary subclass $\mathcal{K}$ of $\operatorname{Mod}(\mathscr{S})$, if $\operatorname{Th}(\mathcal{K})$ contains both σ and $\neg\sigma$, then $\mathcal{K}$ must be empty, so

$$\operatorname{Th}(\mathcal{K}) = \operatorname{Sn}(\mathscr{S}).$$

Suppose now $\operatorname{Th}(\mathcal{K})$ is complete. Then $\mathcal{K}$ contains some $\mathfrak{A}$, and then, since

$$\operatorname{Th}(\mathcal{K}) \subseteq \operatorname{Th}(\mathfrak{A}) \subset \operatorname{Sn}(\mathscr{S}),$$

the first inclusion must be an equation. Thus the complete theories are precisely the theories of individual structures. However, there are proper classes[3] of structures whose theories are complete. For example, the theory of algebraically closed fields of characteristic 0 is complete (Theorem 9 on page 49).

[3]That is, classes that are not sets, because they are 'too large'.

If $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$, then $\mathfrak{A}$ and $\mathfrak{B}$ are said to be **elementarily equivalent,** and we write

$$\mathfrak{A} \equiv \mathfrak{B}.$$

If $\mathfrak{A}$ and $\mathfrak{B}$ are *isomorphic* in the familiar sense, then (trivially) they are elementarily equivalent. However, by what we have just observed about complete theories, the converse fails: non-isomorphic structures can be elementarily equivalent. This is easily shown with the Compactness Theorem, which we shall prove as Theorem 6 by using ultraproducts. Also, a non-principal ultrapower of an infinite structure is elementarily equivalent, but not isomorphic, to that structure. See also §4.4.

2.2 Definable relations

We are usually interested in $\mathrm{Mod}(T)$ for particular theories T of a signature $\mathscr{S}$. One way to study this is to study the *definable relations* in elements of $\mathrm{Mod}(T)$. Suppose $\mathfrak{A}$ is one of these elements, and φ is an n-ary formula of $\mathscr{S}$. Then φ defines the subset

$$\{\boldsymbol{a} \in A^n \colon \mathfrak{A} \vDash \varphi(\boldsymbol{a})\}$$

of A^n. This subset, denoted by one of

$$\varphi^{\mathfrak{A}}, \qquad\qquad \varphi(\mathfrak{A}),$$

is more precisely a **0-definable relation** of $\mathfrak{A}$. If $B \subseteq A$, and φ is a formula of $\mathscr{S}(B)$, then $\varphi^{\mathfrak{A}}$ is a B**-definable relation** of $\mathfrak{A}$.

2.2.1 Terms

The **terms** of $\mathscr{S}$ are defined recursively as follows.

1. Every variable is a term: we use variables x_i, where $i \in \omega$. These variables are more precisely called **individual variables,** because they stand for individual elements of sets.

2. For all n in ω, if F is an n-ary operation-symbol of $\mathscr{S}$, and $t_0, \dots, t_{n-1}$ are terms of $\mathscr{S}$, then the string
$$Ft_0 \cdots t_{n-1}$$
is a term of $\mathscr{S}$. In particular, if $n = 0$, so that F is a constant, then, standing by itself, it is a term.

This recursive definition allows theorems about all terms to be proved by *induction.* A trivial example is that every term that is not a variable begins with an operation-symbol (possibly a constant); slightly less trivial is that every term ends with a variable or a constant.

We also want to be able to define functions recursively on the set of terms (of a given signature). This requires knowing that every term is **uniquely readable:** it can be constructed in only one way. For example, we want to have that, if $\mathfrak{A} \in \mathrm{Mod}(\mathscr{S})$, then the terms t of $\mathscr{S}$ that use only variables from the set $\{x_i : i < n\}$ can be understood as n-ary operations $t^{\mathfrak{A}}$ on A as follows:
$$\begin{aligned} {x_i}^{\mathfrak{A}}(\boldsymbol{a}) &= a_i, \\ Ft_0 \cdots {t_{n-1}}^{\mathfrak{A}}(\boldsymbol{a}) &= F^{\mathfrak{A}}({t_0}^{\mathfrak{A}}(\boldsymbol{a}), \dots, {t_{n-1}}^{\mathfrak{A}}(\boldsymbol{a})). \end{aligned}$$
This is a valid definition, only if we know that $Ft_0 \dots t_{n-1}$ cannot also be analyzed as $Fu_0 \dots u_{n-1}$ for some terms u_i, where in at least one case u_i is not t_i. But this is true: $Ft_0 \dots t_{n-1}$ cannot be otherwise analyzed. Perhaps the simplest way to prove it is by means of a lemma, proved by induction: every term neither *is* a proper initial segment of another term, nor *has* a proper initial segment that is a term.

2.2.2 Formulas

The **atomic formulas** of $\mathscr{S}$ are of two kinds: **equations,** which take the form
$$t = u,$$
where t and u are terms of $\mathscr{S}$; and expressions of the form
$$Rt_0 \cdots t_{n-1},$$

where $n \in \omega$, R is an n-ary predicate in $\mathscr{S}$, and the t_i are terms of $\mathscr{S}$. Then the **formulas** of $\mathscr{S}$ in general are defined recursively:

1. Atomic formulas are formulas.
2. If φ and ψ are formulas, then so are $\neg\varphi$ and $(\varphi \wedge \psi)$.
3. If φ is a formula and x is a variable, then $\exists x\ \varphi$ is a formula.

Because this definition (like that of terms) is recursive, induction can be used to prove that certain sets of formulas of $\mathscr{S}$ contain *all* formulas of $\mathscr{S}$. For example, induction will be used to establish the lemma called the Tarski–Vaught Test on page 31 below. However, that lemma also involves *truth,* which can be understood formally as a function defined recursively on the set of all formulas of $\mathscr{S}$. (See the next subsection.) As with terms, for such a definition to be valid, unique readability of formulas must be established: every formula is built up from its **subformulas,** but this can happen in only one way.

An occurrence of a variable x in a formula is **free,** unless this occurrence is in a subformula of the form $\exists x\ \varphi$: then the occurrrence is **bound.** This definition would be possible without unique readability, but it would not then be particularly useful.

There are some standard abbreviations:

$$(\varphi \vee \psi) \text{ means } \neg(\neg\varphi \wedge \neg\psi);$$
$$(\varphi \to \psi) \text{ means } (\neg\varphi \vee \psi);$$
$$(\varphi \leftrightarrow \psi) \text{ means } ((\varphi \to \psi) \wedge (\psi \to \varphi));$$
$$\forall x\ \varphi \text{ means } \neg\exists x\ \neg\varphi.$$

It is possible to remove some parentheses from formulas without ambiguity, if it is understood for example that $\wedge$ and $\vee$ take precedence over $\to$ and $\leftrightarrow$, and of two instances of $\to$, the one on the right takes precedence. Also outer parentheses can be removed.

2.2.3 Truth

Now *sentences* are defined as before (p. 23), as formulas with no free variables; and we can now define truth of sentences in structures. Assuming

t, u, and the t_i are terms with no variables, and σ and τ are sentences, but φ is formula with the unique free variable x, we have

$$\begin{aligned}
\mathfrak{A} \models t = u &\iff t^{\mathfrak{A}} = u^{\mathfrak{A}}, \\
\mathfrak{A} \models R t_0 \cdots t_{n-1} &\iff ({t_0}^{\mathfrak{A}}, \dots, {t_{n-1}}^{\mathfrak{A}}) \in R^{\mathfrak{A}}, \\
\mathfrak{A} \models \neg\sigma &\iff \mathfrak{A} \nvDash \sigma, \\
\mathfrak{A} \models \sigma \land \tau &\iff \mathfrak{A} \models \sigma \;\;\&\;\; \mathfrak{A} \models \tau, \\
\mathfrak{A} \models \exists x\, \varphi(x) &\iff \text{for some } b \text{ in } A,\, \mathfrak{A} \models \varphi(b).
\end{aligned}$$

Note here that the expressions $\&$ and $\iff$ are not parts of formulas; they are abbreviations of the English *and* and *if and only if.* We can understand our definition as follows. Given the structure $\mathfrak{A}$ in $\mathrm{Mod}(\mathscr{S})$, we have now recursively defined, on the set of formulas of $\mathscr{S}(A)$, the function $\varphi \mapsto \varphi^{\mathfrak{A}}$, where, if φ is n-ary, we have

$$\varphi^{\mathfrak{A}} = \{\boldsymbol{a} \in A^n : \mathfrak{A} \models \varphi(\boldsymbol{a})\}.$$

It is worthwhile to note that as φ varies here, $\varphi^{\mathfrak{A}}$ ranges over a subset of A^n with some natural closure properties; and as n varies as well, there are still some good closure properties. Section 7.1 is an investigation of these. Before that (as well as later), it is useful to have the notion of *substructure,* developed in the next section.

2.3 Substructures

$\mathfrak{B} \in \mathrm{Mod}(\mathscr{S})$, and $A \subseteq B$, and A is closed under the operations of $\mathfrak{B}$, then A is the universe of a **substructure** of $\mathfrak{B}$. This substructure is $\mathfrak{A}$, where

$$\begin{aligned}
R^{\mathfrak{A}} &= A^n \cap R^{\mathfrak{B}}, \\
F^{\mathfrak{A}} &= F^{\mathfrak{B}} \restriction A^n
\end{aligned}$$

for all n-ary predicates R and operation-symbols F of $\mathscr{S}$, for all n in ω. In this case, we write

$$\mathfrak{A} \subseteq \mathfrak{B}.$$

It follows that, if $\mathfrak{A}$ and $\mathfrak{B}$ are two structures with the same signature $\mathscr{S}$, and $A \subseteq B$, then $\mathfrak{A} \subseteq \mathfrak{B}$ if and only if, for all n in ω, for all n-ary quantifier-free formulas φ of $\mathscr{S}$, for all $\boldsymbol{a}$ in A^n,

$$\mathfrak{A} \models \varphi(\boldsymbol{a}) \iff \mathfrak{B} \models \varphi(\boldsymbol{a}). \tag{‡}$$

Suppose now there is just a function h from A to B. Then h is an **embedding** of $\mathfrak{A}$ in $\mathfrak{B}$ if h is an isomorphism from $\mathfrak{A}$ to a substructure of $\mathfrak{B}$. In any case, the **diagram** of $\mathfrak{A}$, denoted by

$$\operatorname{diag}(\mathfrak{A}),$$

is the set of *quantifier-free* sentences of $\mathscr{S}(A)$ that are true in $\mathfrak{A}$. When we consider $\mathfrak{A}$ as having signature $\mathscr{S}(A)$, we may write the structure as

$$\mathfrak{A}_A.$$

This is an **expansion** of $\mathfrak{A}$ to $\mathscr{S}(A)$; and $\mathfrak{A}$ is then the **reduct** of $\mathfrak{A}_A$ to $\mathscr{S}$. Now $\mathfrak{B}_{h[A]}$ can also be understood as having signature $\mathscr{S}(A)$. In this case, the map h above is an embedding if and only if

$$\mathfrak{B}_{h[A]} \models \operatorname{diag}(\mathfrak{A}).$$

Thus the structures in which $\mathfrak{A}$ embeds are precisely (the reducts to $\mathscr{S}$ of) the models of $\operatorname{diag}(\mathfrak{A})$.

A theory T of $\mathscr{S}$ is **axiomatized** by a subset Γ of $\operatorname{Sn}(\mathscr{S})$ if

$$T = \operatorname{Th}(\operatorname{Mod}(\Gamma)),$$

equivalently, every model of Γ is a model of T.

A **universal** formula is a formula of the form $\forall \boldsymbol{x}\ \varphi$, where φ is quantifier-free. If T is a theory, then we denote by

$$T_\forall$$

the theory axiomatized by the universal sentences in T.

Lemma. *$T_\forall$ is included in the theory of substructures of models of T, that is,*

$$\mathfrak{A} \subseteq \mathfrak{B} \ \& \ \mathfrak{B} \models T \implies \mathfrak{A} \models T_\forall.$$

Proof. Suppose φ is quantifier-free, and $\forall \boldsymbol{x}\ \varphi$ is in T. If $\boldsymbol{a} \in A^n$, then $\boldsymbol{a} \in B^n$, so $\mathfrak{B} \models \varphi(\boldsymbol{a})$ and therefore, by (‡), $\mathfrak{A} \models \varphi(\boldsymbol{a})$. Thus $\mathfrak{A} \models \forall \boldsymbol{x}\ \varphi$. □

The converse is given in Theorem 11 on page 50 below.

If (‡) holds for *all* formulas φ of $\mathscr{S}$, then $\mathfrak{A}$ is called an **elementary substructure** of $\mathfrak{B}$, and we write

$$\mathfrak{A} \preccurlyeq \mathfrak{B}.$$

A map h from A to B is an **elementary embedding** of $\mathfrak{A}$ in $\mathfrak{B}$ if h is an isomorphism from $\mathfrak{A}$ to an elementary substructure of $\mathfrak{B}$. Thus the structures in which $\mathfrak{A}$ embeds elementarily are precisely (the reducts to $\mathscr{S}$ of) the models of $\mathrm{Th}(\mathfrak{A}_A)$.

A theory T of a signature $\mathscr{S}$ is called **model-complete** if for all models $\mathfrak{A}$ of T, the theory of $\mathscr{S}(A)$ axiomatized by $T \cup \mathrm{diag}(\mathfrak{A})$ is complete.

Theorem 1. *A theory is model-complete if and only if, for all of its models $\mathfrak{A}$ and $\mathfrak{B}$,*

$$\mathfrak{A} \subseteq \mathfrak{B} \implies \mathfrak{A} \preccurlyeq \mathfrak{B}.$$

Proof. Each condition is equivalent to the condition that, for all models $\mathfrak{A}$ of T, $T \cup \mathrm{diag}(\mathfrak{A})$ axiomatizes $\mathrm{Th}(\mathfrak{A}_A)$. □

The theorem below is a generalization of the theorem published by Löwenheim in 1915 [20] and improved by Skolem in 1920 [22]: a sentence with a model has a countable model. Skolem's argument uses what we shall call the *Skolem normal form* of the given sentence; we shall discuss this in §5.4. Meanwhile, an example is $\forall x\ \exists y\ Rxy$. If this has a model $\mathfrak{A}$, then there is a singulary operation $x \mapsto x^*$ on A such that

$$\mathfrak{A} \models \forall x\ Rxx^*.$$

If $b \in A$, we can define $(b_k \colon k \in \omega)$ recursively by

$$b_0 = b, \qquad\qquad b_{k+1} = {b_k}^*.$$

Then $\{b_k \colon k \in \omega\}$ is countable and is the universe of a substructure of $\mathfrak{A}$ in which $\forall x\ \exists y\ Rxy$ is true. Our own proof of the general theorem will follow the lines of Skolem's idea; the following lemma will allow us to work in the general situation.

Lemma (Tarski–Vaught Test)**.** *Suppose* $\mathfrak{A} \subseteq \mathfrak{B}$*, both having signature* $\mathscr{S}$*. Then* $\mathfrak{A} \preccurlyeq \mathfrak{B}$*, provided that, for all singulary formulas* φ *of* $\mathscr{S}(A)$*,*

$$\mathfrak{B} \vDash \exists x\ \varphi(x) \implies \text{for some } c \text{ in } A,\ \mathfrak{B} \vDash \varphi(c),$$

that is,

$$\varphi^{\mathfrak{B}} \neq \varnothing \implies \varphi^{\mathfrak{B}} \cap A \neq \varnothing.$$

Proof. Under the given condition, we show by induction that for all formulas φ of $\mathscr{S}$, if φ is n-ary and $\boldsymbol{a} \in A^n$, then

$$\mathfrak{A} \vDash \varphi(\boldsymbol{a}) \iff \mathfrak{B} \vDash \varphi(\boldsymbol{a}).$$

This is given to be the case when φ is atomic (or more generally quantifier-free), and it is easily preserved under negation and conjunction. Suppose it holds when φ is an $(m+1)$-ary formula ψ. By hypothesis, for all $\boldsymbol{a}$ in A^n, the following are equivalent:

$$\begin{gathered}
\mathfrak{B} \vDash \exists y\ \varphi(\boldsymbol{a}, y),\\
\text{for some } b \text{ in } B,\ \mathfrak{B} \vDash \varphi(\boldsymbol{a}, b),\\
\text{for some } b \text{ in } A,\ \mathfrak{B} \vDash \varphi(\boldsymbol{a}, b),\\
\text{for some } b \text{ in } A,\ \mathfrak{A} \vDash \varphi(\boldsymbol{a}, b),\\
\mathfrak{A} \vDash \exists y\ \varphi(\boldsymbol{a}, y).
\end{gathered}$$

This completes the induction. □

Theorem 2 (Downward Löwenheim–Skolem–Tarski)**.** *If* $\mathfrak{B} \in \mathrm{Mod}(\mathscr{S})$*,* $\max(|\mathscr{S}|, \omega) \leqslant |B|$*, and* $X \subseteq B$*, there is a structure* $\mathfrak{A}$ *such that*

$$\mathfrak{A} \preccurlyeq \mathfrak{B}, \qquad X \subseteq A, \qquad |A| \leqslant \kappa,$$

where $\kappa = \max(|X|, |\mathscr{S}|, \omega)$*.*

Proof. There is a subset X' of B of cardinality no greater than κ such that, for every singulary formula φ of $\mathscr{S}(X)$, if $\varphi^{\mathfrak{B}}$ is non-empty, then it has an element in X'. By considering formulas $a = x$, where $a \in X$, we see $X \subseteq X'$. Now we can form X'', and so forth; and we can let

$$A = X \cup X' \cup X'' \cup \dots$$

By considering formulas $F\boldsymbol{x} = y$, we see that A is the universe of a substructure $\mathfrak{A}$ of $\mathfrak{B}$. It is of the required cardinality, and by the Tarski–Vaught Test, it is an elementary substructure of $\mathfrak{B}$. $\square$

3 Ultraproducts and Łoś's Theorem

3.1 Ideals and filters

For every set Ω, the power-set $\mathscr{P}(\Omega)$ is a *ring* in which

- sums are symmetric differences: $+$ is $\triangle$;
- products are intersections: $\cdot$ is $\cap$;
- the additive identity is the empty set: 0 is $\varnothing$;
- every element is its own additive inverse: $-X$ is just X;
- the multiplicative identity is the whole set: 1 is Ω.

It is easy to check this. We note first:

$$X \triangle Y = Y \triangle X, \qquad X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z,$$

(see Figure 3.1) and

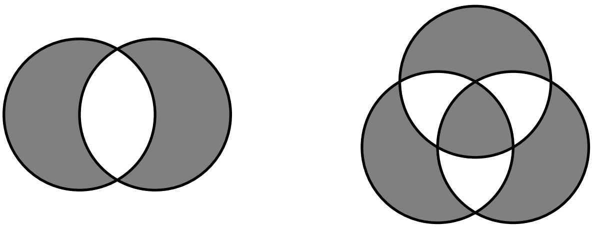

Figure 3.1: Symmetric differences of two sets and three sets

$$X \triangle \varnothing = X, \qquad X \triangle X = \varnothing.$$

So $(\mathscr{P}(\Omega), \triangle, \varnothing)$ is an abelian group in which every element is its own inverse. (That is, it is an abelian group of exponent 2. It is a standard exercise to show that every group of exponent 2 is abelian.) As for multiplication, we have

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$
$$X \cap Y = Y \cap X,$$
$$X \cap \Omega = X,$$
$$X \cap (Y \mathbin{\triangle} Z) = X \cap Y \mathbin{\triangle} X \cap Z,$$

where multiplication $\cap$ takes notational precedence over addition $\triangle$ in the line; see Figure 3.2. So $(\mathscr{P}(\Omega), \triangle, \cap, \varnothing, \Omega)$ is a ring (commutative

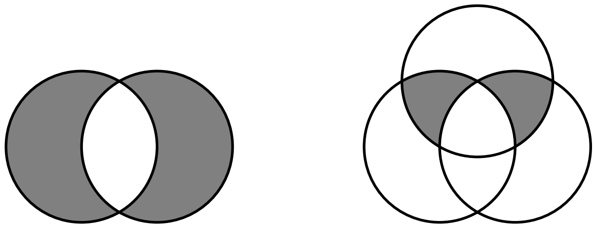

Figure 3.2: Distribution in Boolean rings

and unital, as always in these notes). We have in this ring also

$$X \cap X = X.$$

That is, in the more usual notation of ring-theory, $\mathscr{P}(\Omega)$ is a ring in which

$$x^2 = x. \tag{$*$}$$

Therefore $\mathscr{P}(\Omega)$ is called a **Boolean ring.** We shall see in Chapter 6 that all of the algebraic properties of $\mathscr{P}(\Omega)$ and its sub-rings follow from their being Boolean rings: the class of Boolean rings is precisely the class of rings that embed in rings of the form $\mathscr{P}(\Omega)$.

This ring $\mathscr{P}(\Omega)$ has ideals in the usual sense: a subset I of $\mathscr{P}(\Omega)$ in ideal if and only if

$$\varnothing \in I,$$
$$Y \in I \implies X \cap Y \in I, \tag{$\dagger$}$$
$$X \in I \ \&\ Y \in I \implies X \mathbin{\triangle} Y \in I. \tag{$\ddagger$}$$

However, since

$$X \cap Y \subseteq Y,$$
$$X \subseteq Y \iff X \cap Y = X,$$

the condition (†) is equivalent to

$$X \subseteq Y \ \& \ Y \in I \implies X \in I.$$

Since also

$$X \cup Y = X \mathbin{\triangle} Y \mathbin{\triangle} X \cap Y,$$
$$X \mathbin{\triangle} Y \subseteq X \cup Y,$$

we can replace the condition (‡) with

$$X \in I \ \& \ Y \in I \implies X \cup Y \in I.$$

That is, a subset I of $\mathscr{P}(\Omega)$ is an ideal if and only if

$$\varnothing \in I,$$
$$X \subseteq Y \ \& \ Y \in I \implies X \in I,$$
$$X \in I \ \& \ Y \in I \implies X \cup Y \in I.$$

Thus ideals of $\mathscr{P}(\Omega)$ are just those subsets that are

- downwardly closed,
- closed under finite unions.

Indeed, taken strictly, the last condition implies non-emptiness, since $\varnothing$ is the finite union $\bigcup \varnothing$. See Figure 3.3. Our observations in §1.4 generalize to show that if $(K_i \colon i \in \Omega)$ is an indexed family of fields, and J is an ideal of $\prod_{i\in\Omega} K_i$, then $\operatorname{supp}[J]$ is an ideal of $\mathscr{P}(\Omega)$. Moreover, every ideal I of $\mathscr{P}(\Omega)$ is $\operatorname{supp}[J]$, where

$$J = \{x \in \prod_{i\in\Omega} K_i \colon \operatorname{supp}(x) \in I\};$$

and this is an ideal of $\prod_{i\in\Omega} K_i$, in fact the only ideal whose image under $J \mapsto \operatorname{supp}[J]$ is I. So this map establishes a one-to-one correspondence between the (set of) ideals of $\prod_{i\in\Omega} K_i$ and the (set of) ideals of $\mathscr{P}(\Omega)$.

There are two standard examples of ideals of $\mathscr{P}(\Omega)$.

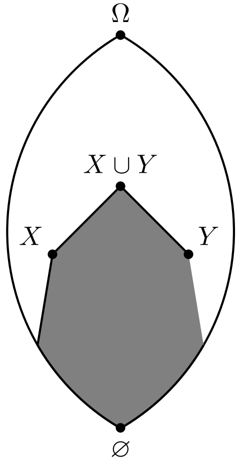

Figure 3.3: An ideal of a Boolean ring

1. If $A \subseteq \Omega$, then $\mathscr{P}(A)$ is the principal ideal of $\mathscr{P}(\Omega)$ generated by A. It corresponds to the ideal $\prod_{i \in A} K_i$ of $\prod_{i \in \Omega} K_i$.
2. The set $\mathscr{P}_\omega(\Omega)$ of finite subsets of Ω is an ideal of $\mathscr{P}(\Omega)$, called the **Fréchet ideal** of $\mathscr{P}(\Omega)$, corresponding to the ideal $\sum_{i \in \Omega} K_i$ of $\prod_{i \in \Omega} K_i$.

There is a notion that is 'dual' to the notion of an ideal: A subset F of $\mathscr{P}(\Omega)$ is a **filter** if $\{X^{\mathrm{c}} \colon X \in F\}$ is an ideal, that is,

$$\Omega \in F,$$
$$X \in F \ \& \ X \subseteq Y \implies Y \in F,$$
$$X \in F \ \& \ Y \in F \implies X \cap Y \in F.$$

See Figure 3.4. Intuitively, elements of an ideal are 'small' subsets of Ω; elements of a filter are 'large' subsets of Ω.

Since filters easily correspond to ideals, we need not introduce the concept of a filter. Alternatively, once we have filters, we can forget about ideals. I prefer not to forget about ideals, since they are familiar from ring-theory. And yet sometimes it will be useful to think in terms of filters as well.

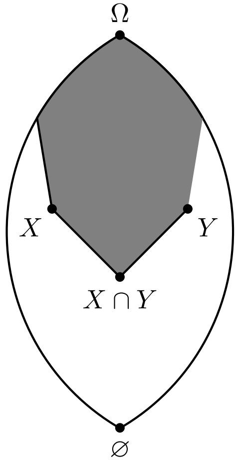

Figure 3.4: A filter of a Boolean ring

A filter *of* $\mathscr{P}(\Omega)$ is also called a filter **on** Ω itself.

Suppose P is a prime ideal of $\mathscr{P}(\Omega)$, that is, P is an ideal such that

$$X \cap Y \in P \ \& \ X \notin P \implies Y \in P.$$

The quotient $\mathscr{P}(\Omega)/P$ is then an integral domain. But it is an integral domain in which $(*)$ holds, that is, for all elements x,

$$x^2 = x, \qquad\qquad 0 = x^2 - x = x \cdot (x - 1).$$

In every integral domain, these equation is solved by 0 and 1, but by no other elements. So $\mathscr{P}(\Omega)/P$ has only two elements, namely P and $\Omega + P$. A two-element integral domain (even a two-element ring) is a field. So $\mathscr{P}(\Omega)/P$ is a field, and therefore P is a maximal ideal. Thus all prime ideals of $\mathscr{P}(\Omega)$ are maximal. Since in $\mathscr{P}(\Omega)$ we have

$$X \mathbin{\triangle} \Omega = X^{\mathrm{c}},$$

we have that X and X^{c} are always in different cosets of P, that is,

$$X \in P \iff X^{\mathrm{c}} \notin P.$$

The filter $\{X^{\mathrm{c}} \colon X \in P\}$ that is dual to P is called an **ultrafilter.** As a filter, it is the set of complements (in Ω) of elements of P; as an ultrafilter, it is the complement (in $\mathscr{P}(\Omega)$) of P.

3.2 Reduced products

Suppose $(\mathfrak{A}_i \colon i \in \Omega)$ is an indexed family of structures with a common signature $\mathscr{S}$. An element of the Cartesian product $\prod_{i\in\Omega} A_i$ is a tuple $(a_i \colon i \in \Omega)$, where $a_i \in A_i$; we may write this tuple simply as a. Let the product $\prod_{i\in\Omega} A_i$ be called also B. This is the universe of a structure

$$\prod_{i\in\Omega} \mathfrak{A}_i$$

or $\mathfrak{B}$ of $\mathscr{S}$, where for all n in ω, for all n-ary operation-symbols F and predicates R of $\mathscr{S}$,

$$F^{\mathfrak{B}}(\boldsymbol{a}) = (F^{\mathfrak{A}_i}(\boldsymbol{a}_i) \colon i \in \Omega), \qquad R^{\mathfrak{B}} = \prod_{i\in\Omega} R^{\mathfrak{A}_i}.$$

Here notation is as in §0, so that $\boldsymbol{a} \in B^n$, which means $\boldsymbol{a} = (a^0, \dots, a^{n-1})$, where $a^k = (a^k_i \colon i \in \Omega)$; and $\boldsymbol{a}_i = (a^0_i, \dots, a^{n-1}_i)$. See Figure 3.5. Note

$$\begin{array}{ccccccc}
\boldsymbol{a} & & \boldsymbol{a}_0 & \boldsymbol{a}_1 & \boldsymbol{a}_2 & \dots \\
\shortparallel & & \shortparallel & \shortparallel & \shortparallel & \\
a^0 & = & a^0_0 & a^0_1 & a^0_2 & \dots \\
\vdots & & \vdots & \vdots & \vdots & \\
a^{n-1} & = & a^{n-1}_0 & a^{n-1}_1 & a^{n-1}_2 & \dots
\end{array}$$

Figure 3.5: Notation for sequences of tuples

that, if $R^{\mathfrak{A}_i} = \varnothing$ for even one index i, then $R^{\mathfrak{B}} = \varnothing$.

Now let I be an ideal of $\mathscr{P}(\Omega)$. We shall define a quotient

$$\prod_{i\in\Omega} \mathfrak{A}_i / I$$

or $\mathfrak{B}/I$. First, we define two elements of B to be **congruent** *modulo* I if they disagree only on a *small* set of indices, that is, a set belonging to I:

$$\{i \in \Omega\colon a_i \neq b_i\} \in I \iff a \equiv b \pmod{I}.$$

Equivalently, if F is the dual filter of I (that is, $F = \{X^{\mathrm{c}}\colon X \in I\}$, then two elements of B are congruent if and only if they agree on a *large* set of indices, that is, a set belonging to F:

$$\{i \in \Omega\colon a_i = b_i\} \in F \iff a \equiv b \pmod{I}.$$

We may write:

- a/I for the congruence-class $\{b\colon a \equiv b \pmod{I}\}$,
- B/I for the set of these congruence-classes,
- $\boldsymbol{a}/I$ for $(a^0/I, \dots, a^{n-1}/I)$.

(Or one could write F for I here.) We want to define a structure $\mathfrak{B}/I$ of $\mathscr{S}$ with universe B/I. Then for all n-ary operation-symbols F of $\mathscr{S}$, we should define

$$F^{\mathfrak{B}/I}(\boldsymbol{a}/I) = F^{\mathfrak{B}}(\boldsymbol{a})/I.$$

However, we must check that this is a valid definition. We shall do this presently; meanwhile, for an n-ary predicate R of $\mathscr{S}$, what should $R^{\mathfrak{B}/I}$ be? By one generalization of the definition in §1.3 of the ordering of $\mathbb{R}^{\omega}/I$, we should define $R^{\mathfrak{B}/I}$ as

$$\{\boldsymbol{a}/I\colon \boldsymbol{a} \in R^{\mathfrak{B}}\}.$$

However, by what we noted above, this relation is empty if $R^{\mathfrak{A}_i} = \varnothing$ for even one index i. The empty relation is still a relation, but it is not what we want here. The 'correct' definition of $R^{\mathfrak{B}/I}$ is given as follows.

Theorem 3. *For all indexed families $(\mathfrak{A}_i\colon i \in \Omega)$ of structures with common signature $\mathscr{S}$, there is a structure $\mathfrak{B}/I$ in $\mathrm{Mod}(\mathscr{S})$, with universe $\prod_{i\in\Omega} A_i/I$, such that all n in ω, for all n-ary operation-symbols F and predicates R of $\mathscr{S}$,*

$$F^{\mathfrak{B}/I}(\boldsymbol{a}/I) = F^{\mathfrak{B}}(\boldsymbol{a})/I, \qquad R^{\mathfrak{B}/I} = \bigl\{\boldsymbol{a}/I\colon \{i\colon \boldsymbol{a}_i \notin R^{\mathfrak{A}_i}\} \in I\bigr\}.$$

If $R^{\mathfrak{A}_i} \neq \varnothing$ for each i in Ω, then

$$R^{\mathfrak{B}/I} = \{\boldsymbol{a}/I\colon \boldsymbol{a} \in R^{\mathfrak{B}}\}.$$

Proof. We need only check that the definition of $F^{\mathfrak{B}/I}$ is valid. Suppose

$$\boldsymbol{a} \equiv \boldsymbol{b} \pmod{I},$$

that is, $\boldsymbol{a}/I = \boldsymbol{b}/I$, that is, $a^k/I = b^k/I$ for each k in n. This means $\{i\colon a_i^k \neq b_i^k\} \in I$ for each k in n. But then

$$\bigcup_{k\in n}\{i\colon a_i^k \neq b_i^k\} \in I.$$

We have also

$$\{i\colon F^{\mathfrak{A}_i}(\boldsymbol{a}_i) \neq F^{\mathfrak{A}_i}(\boldsymbol{b}_i\} \subseteq \bigcup_{k\in n}\{i\colon a_i^k \neq b_i^k\},$$

so $\{i\colon F^{\mathfrak{A}_i}(\boldsymbol{a}_i) \neq F^{\mathfrak{A}_i}(\boldsymbol{b}_i)\} \in I$ and therefore

$$F^{\mathfrak{B}}(\boldsymbol{a}) \equiv F^{\mathfrak{B}}(\boldsymbol{b}) \pmod{I}. \qquad \square$$

The structure $\mathfrak{B}/I$ is a **reduced product** of the family $(\mathfrak{A}_i\colon i \in \Omega)$.

We can understand each element a of $\prod_{i\in\Omega} A_i$ as a new constant, to be interpreted in each $\mathfrak{A}_i$ as a_i, and in $\mathfrak{B}$ as a/I. Then the definition

$$R^{\mathfrak{B}/I} = \bigl\{\boldsymbol{a}/I\colon \{i\colon \boldsymbol{a}_i \notin R^{\mathfrak{A}_i}\} \in I\bigr\}$$

in the theorem just means

$$\mathfrak{B}/I \vDash R\boldsymbol{a} \iff \{i\colon \mathfrak{A}_i \vDash \neg R\boldsymbol{a}\} \in I,$$

and the definition

$$F^{\mathfrak{B}/I}(\boldsymbol{a}/I) = F^{\mathfrak{B}}(\boldsymbol{a})/I$$

has the meaning of

$$\mathfrak{B}/I \vDash F\boldsymbol{a} = b \iff \{i\colon \mathfrak{A}_i \vDash \neg(F\boldsymbol{a} = b)\} \in I.$$

The formulas $R\boldsymbol{x}$ and $F\boldsymbol{x} = y$ here are *unnested* atomic formulas. (So is $x = y$.) Our equivalences have the form

$$\mathfrak{B}/I \vDash \sigma \iff \{i\colon \mathfrak{A}_i \vDash \neg\sigma\} \in I, \tag{§}$$

which can be written also as

$$\mathfrak{B}/I \vDash \sigma \iff \{i \colon \mathfrak{A}_i \vDash \sigma\} \in F.$$

So this is true by definition when σ is an unnested atomic sentence (in the expanded signature $\mathscr{S}(B)$). For which other σ is it true?

Lemma. *The equivalence* (§), *that is,*

$$\mathfrak{B}/I \vDash \sigma \iff \{i \colon \mathfrak{A}_i \vDash \neg\sigma\} \in I,$$

considered as a function of σ, is preserved under conjunction: if it holds when σ is τ or ρ, then it holds when σ is $\tau \land \rho$.

Proof. From the definition of an ideal, we have

$$X \subseteq Y \ \& \ Y \in I \implies X \in I,$$
$$X \in I \ \& \ Y \in I \implies X \cup Y \in I.$$

Together these imply the converse of the latter; so we have

$$X \in I \ \& \ Y \in I \iff X \cup Y \in I.$$

If now (§) holds when σ is τ or ρ, then the following are equivalent:

$$\begin{gathered}
\mathfrak{B}/I \vDash \tau \land \rho, \\
\mathfrak{B}/I \vDash \tau \ \& \ \mathfrak{M} \vDash \rho, \\
\{i \colon \mathfrak{A}_i \vDash \neg\tau\} \in I \ \& \ \{i \colon \mathfrak{A}_i \vDash \neg\rho\} \in I, \\
\{i \colon \mathfrak{A}_i \vDash \neg\tau\} \cup \{i \colon \mathfrak{A}_i \vDash \neg\rho\} \in I, \\
\{i \colon \mathfrak{A}_i \vDash \neg\tau \lor \neg\rho\} \in I, \\
\{i \colon \mathfrak{A}_i \vDash \neg(\tau \land \rho)\} \in I.
\end{gathered}$$ □

Lemma. *The equivalence* (§), *that is,*

$$\mathfrak{B}/I \vDash \sigma \iff \{i \colon \mathfrak{A}_i \vDash \neg\sigma\} \in I,$$

considered as a function of σ, is preserved under quantification:

if *it holds when σ is $\psi(a)$, for all parameters a, for some singular formula ψ (possibly with parameters),*

then *it holds when* σ *is* $\exists x\ \psi(x)$.

Proof. Under the given hypothesis, the following are equivalent:

$$\begin{gathered}\mathfrak{B}/I \models \exists x\ \psi(x),\\ \mathfrak{B}/I \models \psi(a) \text{ for some } a \text{ in } B,\\ \{i \colon \mathfrak{A}_i \models \neg\psi(a_i)\} \in I \text{ for some } a \text{ in } B.\end{gathered}$$

For all a in B, we have

$$\{i \colon \mathfrak{A}_i \models \neg\psi(a_i)\} \supseteq \{i \colon \mathfrak{A}_i \models \neg\exists x\ \psi(x)\}.$$

Moreover, for some choice of a, this inclusion is an equality. This yields the result. □

3.3 Ultraproducts

Suppose P is a prime ideal (hence a maximal ideal) of $\mathscr{P}(\Omega)$. Then the reduced product $\mathfrak{B}/P$ is called more precisely an **ultraproduct** of $(\mathfrak{A}_i \colon i \in \Omega)$. There is a trivial example: For some j in Ω, let P be the *principal* ideal $(\Omega \smallsetminus \{j\})$ of $\mathscr{P}(\Omega)$, that is, $P = \{X \subseteq \Omega \colon j \notin \Omega\}$. Then

$$\prod_{i\in\Omega} \mathfrak{A}_i/P \cong \mathfrak{A}_j.$$

All ultraproducts are thus if Ω is finite; but if Ω is infinite, then the Fréchet ideal of $\mathscr{P}(\Omega)$ (that is, the ideal consisting of all finite subsets of Ω) is a proper ideal, so it may be included in P, which is therefore not principal.[1] Immediately we have:

Lemma. *If* P *is a prime ideal of* $\mathscr{P}(\Omega)$*, then the equivalence*

$$\mathfrak{B}/P \models \sigma \iff \{i \colon \mathfrak{A}_i \models \neg\sigma\} \in P,$$

as a function of σ*, is preserved under negation.*

[1]So we are assuming the Prime Ideal Theorem, that every proper ideal of a ring is included in a prime ideal. This is apparently weaker than the Maximal Ideal Theorem, that every proper ideal of a ring is included in a maximal ideal; this is equivalent to the Axiom of Choice. Some discussion and references are found in [15, §6.2, pp. 272–3].

The three lemmas of this chapter together yield:

Theorem 4 (Łoś[2])**.** *If P is a maximal ideal of $\mathscr{P}(\Omega)$, then*

$$\mathfrak{B}/P \vDash \sigma \iff \{i\colon \mathfrak{A}_i \vDash \neg\sigma\} \in P$$

holds for all σ (with parameters).

As a special case, if each $\mathfrak{A}_i$ is the same structure $\mathfrak{A}$, so that in particular $\prod_{i\in\Omega} A_i$ is the Cartesian power A^Ω, then the ultraproduct $\mathfrak{B}/I$ (that is $\mathfrak{A}^\Omega/P$) is an **ultrapower** of $\mathfrak{A}$. The diagonal embedding $a \mapsto (a\colon i \in \Omega)$ of $\mathfrak{A}$ in $\mathfrak{B}/I$ is now an *elementary embedding,* that is, for all sentences σ with parameters from A (or more precisely from the image of A in A^Ω),

$$\mathfrak{B}/I \vDash \sigma \iff \mathfrak{A} \vDash \sigma.$$

Considering the embedding as an inclusion (that is, identifying $\mathfrak{A}$ with its image in $\mathfrak{B}/I$), we may write then

$$\mathfrak{A} \preccurlyeq \mathfrak{B}/I.$$

3.4 Cardinality

By the theorem below, a non-principal ultrapower $\mathfrak{C}$ of a countably infinite structure $\mathfrak{A}$ is uncountable. By the Downward Löwenheim–Skolem–Tarski Theorem, in a countable signature, there will then be a countable structure $\mathfrak{B}$ such that

$$\mathfrak{A} \prec \mathfrak{B} \prec C.$$

Indeed, $\mathfrak{B}$ may be chosen to include $A\cup\{x\}$ for some x in $C \smallsetminus A$. However, even though $\mathfrak{A}$ is then a proper substructure of $\mathfrak{B}$, these two may be isomorphic. However, this is not the case when $\mathfrak{A}$ is $(\mathbb{N}, +, \cdot)$. Thus *countable non-standard models of arithmetic* exist. A more illuminating construction of such models is given in §4.4 below.

The following is a special case of [15, Thm 9.5.4(a)] (and is said to be found in Frayne, Morel, and Scott [10][3]).

[2] The usual reference is [19] although the theorem is not given clearly there.

[3] I have a printout of this article, but have not sorted through all of its many basic results to find this one. It should be noted that the article has a 'correction' [11], which merely refines the account of Tarski's contribution to the subject (as well as taking some of the credit away from Frayne).

Theorem 5. *For all signatures $\mathscr{S}$, for all $\mathfrak{A}$ in $\operatorname{Mod}(\mathscr{S})$, for all singulary formulas φ of $\mathscr{S}(A)$, for all non-principal prime ideals P of $\mathscr{P}(\omega)$,*

$$\omega \leqslant |\varphi(\mathfrak{A})| \implies |\varphi(\mathfrak{A}^\omega/P)| = |\varphi(\mathfrak{A})|^\omega.$$

In particular, if $\mathfrak{A}$ is countable, then all infinite definable relations of $\mathfrak{A}^\omega/P$ have the cardinality of the continuum.

Proof. For all a in A^ω, if $a/P \in \varphi(\mathfrak{A}^\omega/P)$, then by Łoś's Theorem

$$\{i \in \omega \colon a_i \notin \varphi(\mathfrak{A})\} \in P.$$

Then we may assume this set $\{i \in \omega \colon a_i \notin \varphi(\mathfrak{A})\}$ is actually empty. More precisely, there is a' in $\varphi(\mathfrak{A})^\omega$ such that $a/P = a'/P$. More precisely still, there is an injection $a/P \mapsto a'$ from $\varphi(\mathfrak{A}^\omega/P)$ to $\varphi(\mathfrak{A})^\omega$. This shows

$$|\varphi(\mathfrak{A}^\omega/P)| \leqslant |\varphi(\mathfrak{A})|^\omega.$$

For the reverse inequality, it is enough to find a function $x \mapsto x^*$ from $\varphi(\mathfrak{A}^\omega)$ to itself such that

$$x \neq y \implies x^*/P \neq y^*/P,$$

that is,

$$x \neq y \implies \{i \colon x^*_i \neq y^*_i\} \notin P.$$

Now $x \neq y$ means $x_i \neq y_i$ for some i in ω. If

$$\{j \colon x^*_j \neq y^*_j\} \supseteq \omega \smallsetminus i, \tag{¶}$$

that is, if $\{j \colon x^*_j = y^*_j\} \subseteq i$, then since $i \in P$, we have $\{j \colon x^*_j \neq y^*_j\} \notin P$. So it is enough that

$$x_i \neq y_i \ \&\ i \leqslant j \implies x^*_j \neq y^*_j. \tag{‖}$$

We can achieve this by letting x^*_j be an injective function of $(x_0, \dots, x_j)$, for each j in ω. We can do *this,* if $\varphi(\mathfrak{A})$ is infinite. Indeed, for each i in ω, let μ_i be an injection from $\varphi(\mathfrak{A})^{i+1}$ to $\varphi(\mathfrak{A})$. Now we can define

$$x^*_i = \mu_i(x_0, \dots, x_i). \qquad \square$$

Let us try to generalize this argument, replacing ω with an arbitrary infinite index-set Ω. In the condition (¶), the element $\omega \smallsetminus i$ of the dual filter F of P will be replaced by some element X_i of the dual filter. Then (‖) becomes

$$x_i \neq x_j \ \& \ j \in X_i \implies x_j^* \neq y_j^*.$$

So x_j^* should be an injective function of $(x_i \colon j \in X_i)$, for each j in Ω. For this, it is enough if the sets

$$\{i \in \Omega \colon j \in X_i\}$$

are finite. An ultrafilter F on Ω (that is, an ultrafilter of $\mathscr{P}(\Omega)$ is called **regular** if it has such elements X_i for all i in Ω.

It is easy to show that there are regular ultrafilters on $\mathscr{P}_\omega(\Omega)$ (that is, regular ultrafilters of $\mathscr{P}(\mathscr{P}_\omega(\Omega))$. For, if $i \in \mathscr{P}_\omega(\Omega)$, we need only define

$$X_i = \{j \in \mathscr{P}_\omega(\Omega) \colon i \subseteq j\}.$$

Since $X_i \cap X_j = X_{i \cup j}$, the X_i do generate a filter on $\mathscr{P}_\omega(\Omega)$. The filter is proper, since $i \in X_i$, so none of the X_i is empty. Moreover,

$$\{i \in \mathscr{P}_\omega(\Omega) \colon j \in X_i\} = \{i \in \mathscr{P}_\omega(\Omega) \colon i \subseteq j\} = \mathscr{P}(j),$$

which is finite. So there are regular proper filters, and hence regular ultrafilters, on $\mathscr{P}_\omega(\Omega)$. Since $\mathscr{P}_\omega(\Omega)$ has the same cardinality as Ω (assuming this is infinite), there are regular ultrafilters on Ω.

We shall use an index-set of the form $\mathscr{P}_\omega(\Omega)$ in proving the Compactness Theorem (Theorem 6) on page 47 below.

4 Simple applications

4.1 Arrow's Theorem

This section is inspired by Sasha Borovik's article [4]. We consider an index-set Ω as a set of *voters.* Each voter i in Ω is called on to assign a linear ordering $<_i$ to a set A of *candidates.* These orderings are to be used to assign a linear ordering $<$ to A. This ordering $<$ should be a kind of average of the orderings $<_i$. This suggests that we should take an ultraproduct of the structures $(A, <_i)$. We shall see that, on some reasonable assumptions, we *must* do this.

We want to determine $<$ by first selecting a subset D of $\mathscr{P}(\Omega)$ such that, for all x and y in A, we shall be able to require

$$\{i\colon x <_i y\} \in D \implies x < y.$$

So D will be, so to speak, a collection of 'winning coalitions'. If $X \in D$, then the members of X can determine how the candidates in A shall be ordered (if all members of X agree). Then we must have, first of all,

$$D \neq \varnothing,$$
$$X \in D \implies X^{\mathrm{c}} \notin D.$$

We also require that additional votes for a particular ordering can only help that ordering:

$$X \in D \ \&\ X \subseteq Y \subseteq \Omega \implies Y \in D.$$

Hence in particular $\Omega \in D$. We require voting to be decisive:

$$X \notin D \implies X^{\mathrm{c}} \in D.$$

If A consists of just two candidates, this is all we need. Then D is not necessarily an ultrafilter on Ω; for it need not be closed under intersections. Indeed, in the 'democratic' case, if Ω has a finite number $2n - 1$

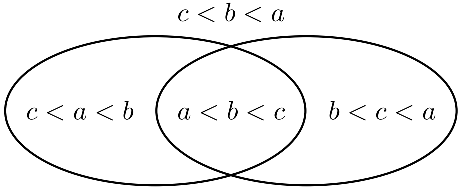

Figure 4.1: An election with three candidates

of members, then D will be $\{X \in \mathscr{P}(\Omega) \colon |X| \geqslant n\}$; this is definitely not closed under intersections unless $n = 1$.

But now suppose A contains three distinct candidates, a, b, and c; and let

$$\{i \colon a <_i b\} = A, \qquad\qquad \{i \colon b <_i c\} = B.$$

Suppose both A and B are in D. Then we must conclude $a < b$ and $b < c$ and therefore $a < c$. We have now

$$A \cap B \subseteq \{i \colon a <_i c\}, \qquad\qquad \{i \colon a <_i c\} \in D.$$

However, possibly

$$A \cap B = \{i \colon a <_i c\};$$

this is the case when—as is possible—

$$\begin{aligned}
\{i \colon c <_i a <_i b\} &= A \smallsetminus B,\\
\{i \colon b <_i c <_i a\} &= B \smallsetminus A,\\
\{i \colon c <_i b <_i a\} &= (A \cup B)^{\mathrm{c}}.
\end{aligned}$$

See Figure 4.1. Thus we must have $A \cap B \in D$. Therefore D is an ultrafilter on Ω. If Ω is finite, then D must be a principal ultrafilter: that is, one voter decides everything, and the system is a dictatorship.

4.2 Compactness

Theorem 6 (Compactness). *Suppose* $\Gamma \subseteq \mathrm{Sn}(\mathscr{S})$, *and every finite subset of* Γ *has a model. Then* Γ *itself has a model.*

Proof. Assuming $\mathfrak{A}_\Delta \vDash \Delta$ for each Δ in $\mathscr{P}_\omega(\Gamma)$, we shall find an ultrafilter F on $\mathscr{P}_\omega(\Gamma)$ such that

$$\prod_{\Delta \in \mathscr{P}_\omega(\Gamma)} \mathfrak{A}_\Delta / F \vDash \Gamma. \tag{$*$}$$

This just means, by Łoś's Theorem, that for each σ in Γ,

$$\{\Delta \in \mathscr{P}_\omega(\Gamma) \colon \mathfrak{A}_\Delta \vDash \sigma\} \in F.$$

But we have

$$\{\Delta \in \mathscr{P}_\omega(\Gamma) \colon \sigma \in \Delta\} \subseteq \{\Delta \in \mathscr{P}_\omega(\Gamma) \colon \mathfrak{A}_\Delta \vDash \sigma\}.$$

Let the former set be denoted by $[\sigma]$; more generally, if $\Delta \in \mathscr{P}_\omega(\Gamma)$, let

$$[\Delta] = \{\Theta \in \mathscr{P}_\omega(\Gamma) \colon \Delta \subseteq \Theta\}.$$

Then

$$\Delta \in [\Delta], \qquad\qquad [\Delta] \cap [\Theta] = [\Delta \cup \Theta].$$

Consequently the sets $[\Delta]$ generate a filter on $\mathscr{P}(\mathscr{P}_\omega(\Gamma))$. Let it be included in the ultrafilter F, and let $\mathfrak{B}$ be the ultraproduct of $(\mathfrak{A}_\Delta \colon \Delta \in \mathscr{P}_\omega(\Gamma))$ with respect to F. For every σ in Γ, we have $[\sigma] \in F$, and for every Δ in $[\sigma]$, we have $\mathfrak{A}_\Delta \vDash \sigma$. Then by Łoś's Theorem, we have $(*)$. □

Now we can establish a complement to Theorem 2 (p. 31):

Theorem 7 (Upward Löwenheim–Skolem–Tarski)**.** *If $\mathfrak{A}$ is an infinite structure with signature $\mathscr{S}$, and* $\max(|A|, |\sigma|) \leqslant \kappa$, *then there is a structure $\mathfrak{B}$ such that*

$$\mathfrak{A} \preccurlyeq \mathfrak{B}, \qquad\qquad |B| = \kappa.$$

Proof. Let C be a set $\{c_\alpha \colon \alpha < \kappa\}$ be a set of new constants, all distinct. By Compactness, the set

$$\mathrm{Th}(\mathfrak{A}_A) \cup \{c_\alpha \neq c_\beta \colon \alpha < \beta < \kappa\}$$

of sentences has a model $\mathfrak{D}_{A\cup C}$. By construction, this model has cardinality at least κ. By the downward version of the theorem, $\mathfrak{D}$ has an elementary substructure $\mathfrak{B}$ of size κ such that $A \subseteq B$. Since also $\mathfrak{A} \preccurlyeq \mathfrak{D}$, the structure $\mathfrak{B}$ is as desired. $\square$

This theorem yields an easy test for completeness of theories. For an infinite cardinal κ, a theory is **κ-categorical** if all of its models of size κ are isomorphic to one another.

Theorem 8 (Łoś–Vaught Test)**.** *If a theory T of a signature $\mathscr{S}$ has models, but no finite models; $|\mathscr{S}| \leqslant \kappa$; and T is κ-categorical; then T is complete.*

Proof. If T contains neither σ nor $\neg\sigma$, then both $T \cup \{\neg\sigma\}$ and $T \cup \{\sigma\}$ have models, which must be infinite. Then by the Löwenheim–Skolem–Tarski theorems (both upward and downward forms may be needed), each of the two sets has a model of cardinality κ; but these two models cannot be isomorphic to one another. $\square$

Theorem 9.

- *The theory of algebraically closed fields of characteristic* 0 *is complete.*
- *For all primes p, the theory of algebraically closed fields of characteristic p is complete.*

Proof. None of these theories has no finite models. Every algebraically closed field is determined up to isomorphism by its characteristic and its transcendence-degree. If κ is uncountable, then a field with transcendence-degree κ has cardinality κ. Now the Łoś–Vaught Test applies. $\square$

Similarly we have the following (see page 30 above):

Theorem 10. *The theory of algebraically closed fields is model-complete.*

Proof. If T is this theory, $K \vDash T$, and $|K| < \kappa$, then $T \cup \operatorname{diag}(K)$ is κ-categorical, but has no finite models. $\square$

We can also now prove the converse of the lemma on page 29 above.

Theorem 11. *For all theories T, the models of $T_\forall$ are precisely the substructures of models of T.*

Proof. Assuming $\mathfrak{A} \models T_\forall$, we want to show $T \cup \operatorname{diag}(\mathfrak{A})$ has a model. By Compactness, and since $\operatorname{diag}(\mathfrak{A})$ is closed under conjunction, it is enough to show $T \cup \{\vartheta(\boldsymbol{a})\}$ has a model whenever ϑ is a quantifier-free formula of $\mathscr{S}$ and $\mathfrak{A} \models \vartheta(\boldsymbol{a})$. If it has no model, then $T \vdash \neg\vartheta(\boldsymbol{a})$, so (since no entry of $\boldsymbol{a}$ is in $\mathscr{S}$) $T \vdash \forall \boldsymbol{x}\ \neg\vartheta(\boldsymbol{x})$, and therefore $\mathfrak{A} \models \forall \boldsymbol{x}\ \neg\vartheta(\boldsymbol{x})$, which is absurd. $\square$

In particular, when T is just field-theory, then $T_\forall$ is the theory of integral domains: see page 88 below.

4.3 Elementary classes

In [19] Łoś defined ultraproducts (but not by that name) in order to state the following algebraic test for being an elementary class of structures.

Theorem 12. *A subclass of* $\operatorname{Mod}(\mathscr{S})$ *is elementary if and only if it contains:*

- *every structure that is elementarily equivalent to a member, and*
- *every ultraproduct of members.*

Proof. The 'only if' direction is the easier. An elementary class is the class of models of some theory T. If the class is $\mathcal{K}$, and $\mathfrak{A} \in \mathcal{K}$, and $\mathfrak{A} \equiv \mathfrak{B}$, then $\mathfrak{B} \models T$, so $\mathfrak{B} \in \mathcal{K}$. If $\{\mathfrak{A}_i : i \in \Omega\} \subseteq \mathcal{K}$, then $\mathfrak{A}_i \models T$ in each case, so every ultraproduct of the $\mathfrak{A}_i$ is a model of T, by Łoś's Theorem.

The more difficult direction is 'if'. Suppose $\mathcal{K}$ is a non-elementary subclass of $\operatorname{Mod}(\mathscr{S})$. Then there is a model $\mathfrak{B}$ of $\operatorname{Th}(\mathcal{K})$ that does not belong to $\mathcal{K}$. However, every element σ of $\operatorname{Th}(\mathfrak{B})$ has a model in $\mathcal{K}$, since otherwise $\neg\sigma$ would be in $\operatorname{Th}(\mathcal{K})$. Therefore every finite subset Δ of $\operatorname{Th}(\mathfrak{B})$ has a model $\mathfrak{A}_\Delta$ in $\mathcal{K}$ (since otherwise the negation of the conjunction of the members of Δ would be in $\operatorname{Th}(\mathcal{K})$). By (the proof of) the Compactness

Theorem, some ultraproduct of $(\mathfrak{A}_\Delta \colon \Delta \in \mathscr{P}_\omega(\mathrm{Th}(\mathfrak{B})))$ is elementarily equivalent to $\mathfrak{B}$. □

4.4 A countable non-standard model of arithmetic

By **arithmetic** we mean the theory of $(\omega, +, \cdot)$ or of $(\omega, +, \cdot, 0, 1, \leqslant)$; it makes little difference, since

1) $\leqslant$ is definable in $(\omega, +, \cdot)$ by the formula $\exists z\ x + z = y$,
2) $\{0\}$ is definable by $\forall y\ y + x = y$,
3) $\{1\}$ is definable by $0 < x \land \forall y\ (0 = y \lor x \leqslant y)$.

Similarly $\{n\}$ is definable in $(\omega, +, \cdot)$ for all n in ω.

Every ultrapower of $(\omega, +, \cdot)$ is a model of arithmetic. Every *non-principal* ultrapower $\mathfrak{B}$ (determined by a non-principal ultrafilter F on ω) is a *non-standard* model of arithmetic, in the sense that it is not isomorphic to $(\omega, +, \cdot)$, but contains an infinite element c. However, $\mathfrak{B}$ here must be uncountable by Theorem 5. As we noted before this theorem, by the Downward Löwenheim–Skolem–Tarski Theorem (Theorem 2), we can obtain a countable elementary substructure $\mathfrak{A}$ of $\mathfrak{B}$ that includes $\omega \cup \{c\}$, and then $\mathfrak{A}$ will be an elementary extension of $(\omega, +, \cdot)$.

We can construct such a structure $\mathfrak{A}$ more directly as follows. Let A be the set of 0-*definable* singulary operations of $(\omega, +, \cdot)$. This means $f \in A$ if and only if the relation $\{(x, f(x)) \colon x \in \omega\}$ is 0-definable (that is, definable without parameters). We can consider A as a subset of ω^ω. Then a constant sequence $(x, x, x, \dots)$ should be understood as the constant function $\{(n, x) \colon n \in \omega\}$ or $n \mapsto x$, which is in A. Thus the diagonal map embeds ω in A. Also A is closed under $+$ and $\cdot$. Therefore A is the universe of a substructure $\mathfrak{A}$ of $\mathfrak{B}$. Also, if $n \in \omega$, and φ is an $(n+1)$-ary formula, and $\boldsymbol{f}$ is an element $(f^0, \dots, f^{n-1})$ of A^n, then A has an element g such that for all i in ω,

$$(\omega, +, \cdot) \vDash \exists y\ \varphi(\boldsymbol{f}(i), y) \iff (\omega, +, \cdot) \vDash \varphi(\boldsymbol{f}(i), g(i)).$$

Indeed, g can be such that $g(i)$ is the *least* b such that $(\omega, +, \cdot) \vDash \varphi(\boldsymbol{f}(i), b)$, if such b exist; and otherwise $g(i) = 0$. Then g is defined by the formula

$$(\varphi(\boldsymbol{f}(x), y) \land (\forall z\ (\varphi(\boldsymbol{f}(x), z) \to y \leqslant z))) \lor (\forall z\ \neg\varphi(\boldsymbol{f}(x), z) \land y = 0).$$

It follows by the Tarski–Vaught Test (page 31) that

$$\mathfrak{A} \preccurlyeq \mathfrak{B};$$

therefore, since $(\omega, +, \cdot) \subseteq \mathfrak{A}$, we have

$$(\omega, +, \cdot) \prec \mathfrak{A}.$$

Indeed, we now have that the following are equivalent:

$$\begin{gathered}
\mathfrak{B} \vDash \exists y\ \varphi(\boldsymbol{f}, y),\\
\{i \colon (\omega, +, \cdot) \vDash \exists y\ \varphi(\boldsymbol{f}(i), y)\} \in F,\\
\{i \colon (\omega, +, \cdot) \vDash \varphi(\boldsymbol{f}(i), g(i))\} \in F,\\
\mathfrak{B} \vDash \varphi(\boldsymbol{f}, g).
\end{gathered}$$

Now the Tarski–Vaught Test applies. This construction of $\mathfrak{A}$ is apparently due to Skolem.[1]

[1] I take it from Bell and Slomson [3, Ch. 12, §2].

5 Gödel's Completeness Theorem

A sentence that is true in all structures of its signature can be called **valid** sentence or a **validity.** It is easy in principle to show that a sentence is *not* valid: just exhibit a model of its negation. But if a sentence *is* valid, how can this be shown? We cannot simply verify the sentence in all structures of its signature, since there will be infinitely many of these structures. The method of *formal proof* is a finitary alternative. We shall show by means of ultraproducts that this method always works in principle. This result is *Gödel's Incompleteness Theorem.*

5.1 Formal proofs

A **formal proof** is just a (finite) list of sentences such that each sentence on the list is either

1) an *axiom,* or
2) derivable from sentences earlier in the list by means of a *rule of inference.*

We choose the axioms and rules of inference to serve our needs; taken all together, they constitute a **proof-system.** In his doctoral dissertation of 1930, Gödel [13] gave a particular proof-system, obtained from the *Principia Mathematica* [24] of Russell and Whitehead. The first four of Gödel's axioms, or rather *schemes* of axioms, are found on page 13, Chapter 1, of the *Principia Mathematica.*[1] Recall that, by our convention

[1] As Gödel notes, there was a fifth axiom, $\varphi \lor (\psi \lor \chi) \to \psi \lor (\varphi \lor \chi)$, but apparently Bernays showed it to be redundant. For us, each of the four formulas given here represents infinitely many axioms, since φ, ψ, and χ can be any formulas. It should be noted that Russell and Whitehead were involved in *creating* formal logic; our way of understanding formulas was not yet fully developed. For an amusing fictionalized account of Russell's interactions with Gödel, see [8].

on symbolic precedence given on page 27, $\lor$ takes precedence over $\to$, and of two instances of $\to$, the one on the right takes precedence.

1) $\varphi \lor \varphi \to \varphi$,

2) $\varphi \to \varphi \lor \psi$,

3) $\varphi \lor \psi \to \psi \lor \varphi$,

4) $(\varphi \to \psi) \to \chi \lor \varphi \to \chi \lor \psi$.

The primitive Boolean connectives here are actually $\lor$ and $\neg$; so $\varphi \to \psi$ should be understood as an abbreviation of $\neg\varphi \lor \psi$. In Chapter 9 of the *Principia* (at $*9.2$ and $*9.25$, pp. 138–40) are found Gödel's next two axioms:[2]

5) $\forall x\ \varphi \to \varphi^x_y$,

6) $\forall x\ (\vartheta \lor \varphi) \to \vartheta \lor \forall x\ \varphi$.

In the former scheme, φ^x_y is the result of replacing every free occurrence of x in φ with y. In the latter scheme, x must not occur freely in ϑ. The primitive quantifier can be taken as $\forall$, so that $\exists x\ \psi$ will be an abbreviation of $\neg\forall x\ \neg\psi$. Finally, equality is treated in two axioms, found in Chapter 13 of the *Principia* (at $*13.15$ and $*13.101$, pp. 177–8):

7) $x = x$,

8) $x = y \to \varphi \to \varphi^x_y$.

Here y should not occur in φ, or at least there should be no subformula $\forall y\ \psi$ in which there is an occurrence of x that is free as an occurrence in φ.

The rules of inference are three:[3]

[2] See the previous note. For Gödel, there were just six axioms in all, using *propositional variables* where I have put φ, ψ, and χ; and using a *functional variable* where I have put ϑ. Then in addition to the three rules of inference given below, there was a fourth, allowing propositional and functional variables to be replaced by *formulas* in our sense.

[3] See the previous note on Gödel's fourth rule of inference (which was actually third on his list). Gödel notes, 'Although Whitehead and Russell use these rules throughout their derivations, they do not formulate all of them explicitly.'

Detachment: From φ and $\varphi \to \psi$ may be[4] inferred ψ.
Generalization: From ϑ may be inferred $\forall x\, \vartheta$.
Change of variables: 'Individual variables (free or bound) may be replaced by others, so long as this does not cause overlapping of the scopes of variables denoted by the same sign' [13, p. 584].

Again, a *formal proof* is a finite list of formulas such that each formula on the list is an axiom or else is derived from previous formulas on the list by means of a rule of inference. The last formula on the list is then said to be *provable.* If φ is provable, we may express this by

$$\vdash \varphi.$$

Note that in fact *every* formula in a formal proof is provable, because every initial segment of a formal proof is still a formal proof.

A **generalization** of a formula φ is a formula $\forall \boldsymbol{x}\, \varphi$, where all free variables of φ occur in $\boldsymbol{x}$. Then we can generalize the notion of validity by saying that an arbitrary formula is **valid** if some (and hence every) generalization of it is true in every structure of its signature.

It should be clear that every provable formula is valid. Gödel proves the converse: this is his Completeness Theorem.

Before Gödel, a completeness theorem for *propositional logic* was known.[5] **Propositional formulas** are, strictly, not formulas as defined in §2.2.2 above; but they can be understood as formulas in which:

1) the place of atomic formulas is taken by **propositional variables;**
2) no quantifier $\exists$ or $\forall$ is used.

In particular, there are no *individual* variables in a propositional formula, but only *propositional* variables. A *structure* for propositional logic assigns a truth-value to each of these propositional variables. Then a propositional formula is true or false in the structure, according to the relevant

[4] Detachment is not Gödel's name for this rule; he (or more precisely his translator) calls it the Inferential Schema.

[5] Gödel's reference for this is Bernays from 1926; but the theorem can be found in Post's 1921 article [21].

parts of the definition of truth of sentences (on page 28), namely:

$$\mathfrak{A} \models \neg\sigma \iff \mathfrak{A} \nvDash \sigma,$$
$$\mathfrak{A} \models \sigma \wedge \tau \iff \mathfrak{A} \models \sigma \ \ \& \ \ \mathfrak{A} \models \tau.$$

Strictly, since $\vee$ is now primitive instead of $\wedge$, we should replace the latter rule with

$$\mathfrak{A} \models \sigma \vee \tau \iff \mathfrak{A} \models \sigma \ \text{ or } \ \mathfrak{A} \models \tau.$$

We may treat the truth-value *true* as 1, and *false* as 0. Then a propositional formula F in an n-tuple $(P_0, \dots, P_{n-1})$ of propositional variables determines an n-ary operation $\hat{F}$ on 2, where if $\boldsymbol{e} \in 2^n$, then $\hat{F}(\boldsymbol{e})$ is the truth-value of F in any propositional structure that assigns the value e_i to P_i when $i < n$. This operation $\hat{F}$ can be described completely in a *truth-table.* If the operation is identically 1, then F is a **(propositional) tautology.** The first four axiom-schemes above, along with the inference-rule of Detachment, constitute a proof-system for propositional logic in which every tautology is provable. This is possibly not an exciting theorem, since there is already an algorithm for determining whether a formula is a tautology: just write out its truth-table.

A **tautology** in general can be understood as resulting from a propositional tautology by replacing each occurrence of a propositional variable with the same formula of some signature $\mathscr{S}$, for all propositional variables occurring in the propositional tautology. Evidently tautologies in this broader sense are valid. They are therefore provable, by the completeness theorem of propositional logic. If we do not want to bother to prove this completeness theorem, we can just introduce, as new axioms, all tautologies, since again there is an algorithm for determining which formulas these are.

If φ is a formula, we may define a formal proof **from** φ as a formal proof in the earlier sense, but with φ treated as an axiom, and with generalization of free variables in φ not allowed.[6] If ψ is provable from φ in this sense, we may write

$$\varphi \vdash \psi;$$

[6]The restriction is to ensure that, if ψ is provable from φ, then the formula $\varphi \to \psi$ is valid, while the converse is still true.

to give it a name, we may call this a **sequent.** For example, by Detachment, the axiom $\forall x\ \varphi \to \varphi^x_y$ gives us the sequent

$$\forall x\ \varphi \vdash \varphi^x_y, \tag{$*$}$$

because the sequence

$$\forall x\ \varphi,\ \forall x\ \varphi \to \varphi^x_y,\ \varphi^x_y.$$

is a formal proof from $\forall x\ \varphi$. Likewise, the axiom $\forall x\ (\vartheta \lor \varphi) \to \vartheta \lor \forall x\ \varphi$ gives us

$$\forall x\ (\vartheta \lor \varphi) \vdash \vartheta \lor \forall x\ \varphi. \tag{$\dagger$}$$

(Recall that x must not be free in ϑ.)

5.2 Completeness by ultraproducts

Suppose σ is an arbitrary sentence. We want to show that either σ is provable, or else its negation has a model, in fact a countable model.[7]

We make several simplifying assumptions:

1. No operation-symbols occur in σ.
2. The sign $=$ of equality does not occur in σ.
3. For some positive integers p and q, for some quantifier-free $(p+q)$-ary formula φ, σ is the sentence

$$\exists \boldsymbol{x}\ \forall \boldsymbol{y}\ \varphi(\boldsymbol{x}, \boldsymbol{y}),$$

where $\boldsymbol{x}$ and $\boldsymbol{y}$ are respectively a p-tuple and a q-tuple of variables.

The justification of these assumptions does not involve ultraproducts, so it is relegated to a later section, §5.4.

Let V be a countably infinite set $\{v_k \colon k \in \omega\}$ of individual variables. The power V^p is countable, so we may assume

$$V^p = \{\boldsymbol{x}_k \colon k \in \omega\}.$$

[7] The ensuing argument is based mainly on that of Bell and Slomson [3, Ch. 12, §1]. These writers cite J.N. Crossley for the suggestion of introducing ultraproducts to Gödel's original argument. Church [7, §44] explicates Gödel's original argument more faithfully.

Now we may suppose

$$\{\boldsymbol{y}_k \colon k \in \omega\} \subseteq V^q,$$

where if $k < \ell$, then $\boldsymbol{y}_k$ and $\boldsymbol{y}_\ell$ have no entries in common, and if $j \leqslant k$, then $\boldsymbol{x}_j$ and $\boldsymbol{y}_k$ have no entries in common. We now denote

$$\begin{gathered}
\varphi(\boldsymbol{x}_k, \boldsymbol{y}_k) \text{ by } \varphi_k,\\
\varphi_0 \text{ by } \vartheta_0,\\
\varphi_{k+1} \lor \vartheta_k \text{ by } \vartheta_{k+1},\\
\forall \boldsymbol{x}_0 \,\cdots \forall \boldsymbol{y}_k\ \vartheta_k \text{ by } \sigma_k.
\end{gathered}$$

That is, ϑ_k is defined recursively in k as shown; and σ_k is a generalization of ϑ_k. We shall prove that, for all k in ω,

$$\sigma_k \vdash \sigma.$$

To this end, we note first that since no entry of $\boldsymbol{y}_{k+1}$ appears in ϑ_k, we have, as a special case of the sequent (†),

$$\forall \boldsymbol{y}_{k+1}\ (\vartheta_k \lor \varphi_{k+1}) \vdash \vartheta_k \lor \forall \boldsymbol{y}_{k+1}\ \varphi_{k+1},$$

that is (by definition of ϑ_{k+1}),

$$\forall \boldsymbol{y}_{k+1}\ \vartheta_{k+1} \vdash \vartheta_k \lor \forall \boldsymbol{y}_{k+1}\ \varphi_{k+1}.$$

By the sequent $(*)$ (used repeatedly), we have

$$\sigma_{k+1} \vdash \forall \boldsymbol{y}_{k+1}\ \vartheta_{k+1}.$$

Therefore, by stringing together the (short) proofs of the last two sequents, we have

$$\sigma_{k+1} \vdash \vartheta_k \lor \forall \boldsymbol{y}_{k+1}\ \varphi_{k+1}. \tag{‡}$$

By repeated use of the axiom allowing removal of universal quantifiers, we have

$$\vdash \forall \boldsymbol{x}\ \neg\forall \boldsymbol{y}\ \varphi(\boldsymbol{x}, \boldsymbol{y}) \to \neg\forall \boldsymbol{y}_{k+1}\ \varphi_{k+1};$$

therefore, by contraposition (justified by completeness for propositional logic),

$$\vdash \forall \boldsymbol{y}_{k+1}\ \varphi_{k+1} \to \exists \boldsymbol{x}\ \forall \boldsymbol{y}\ \varphi(\boldsymbol{x}, \boldsymbol{y}),$$

that is,

$$\vdash \forall \boldsymbol{y}_{k+1}\ \varphi_{k+1} \to \sigma.$$

Combining this with (‡) gives

$$\sigma_{k+1} \vdash \vartheta_k \lor \sigma$$

and therefore (by Generalization mainly)

$$\sigma_{k+1} \vdash \sigma_k \lor \sigma.$$

Thus if $\sigma_k \vdash \sigma$, then $\sigma_{k+1} \vdash \sigma$. Since by change of variables we have

$$\sigma_k \vdash \sigma$$

when $k = 0$, by induction we now have this for all k in ω.

Now we can show that either σ is provable, or $\neg\sigma$ has a model. to do so, we consider two cases. The first one is easy to dispose of: If some σ_k is provable, then so is σ itself, and we are done.

So now let us suppose that no σ_k is provable. Then no ϑ_k is provable; so it must not be a tautology.

Since ϑ_k is quantifier-free, but not a tautology, there must be a truth-assignment to its atomic subformulas that makes ϑ_k false. We can extend this to a truth-assignment F to *all* atomic formulas in variables from V (that is, in the variables v_i) with predicates occurring in φ. Since none of those predicates is $=$, the truth-assignment F determines a structure $\mathfrak{A}_k$ whose universe is ω such that, for each n in ω, for each n-ary predicate R occurring in φ,

$$R^{\mathfrak{A}_k} = \{(i(0), \dots, i(n-1)) \in \omega^n \colon F(Rv_{i(0)} \cdots v_{i(n-1)}) = 1\}.$$

If we now treat each variable v_i as a constant whose interpretation in $\mathfrak{A}_k$ is i, then we have

$$\mathfrak{A}_k \models Rv_{i(0)} \cdots v_{i(n-1)} \iff F(Rv_{i(0)} \cdots v_{i(n-1)}) = 1.$$

Then by construction

$$\mathfrak{A}_k \models \neg\vartheta_k.$$

Suppose $k \leqslant \ell$. Then

$$\vartheta_k \vdash \vartheta_\ell,$$

so that also $\neg\vartheta_\ell \vdash \neg\vartheta_k$, and hence

$$\mathfrak{A}_\ell \vDash \neg\vartheta_k.$$

Thus for all j in ω,

$$\{i \in \omega \colon \mathfrak{A}_i \vDash \vartheta_j\} \subseteq j.$$

Now let $\mathfrak{C}$ be a non-principal ultraproduct of the $\mathfrak{A}_i$. It follows that, for all j in ω,

$$\mathfrak{C} \vDash \neg\vartheta_j.$$

(Here v_i is interpreted as the image of i under the diagonal map.) Hence the conjuncts of the $\neg\vartheta_j$ are true in $\mathfrak{C}$:

$$\mathfrak{C} \vDash \neg\varphi(\boldsymbol{x}_j, \boldsymbol{y}_j).$$

Since we have no operation-symbols in our signature, every subset of C is the universe of a substructure of $\mathfrak{C}$. Let B be the image of ω under the diagonal map in C. Since φ is quantifier-free, and the interpretations of all of the variables are now in B, we have

$$\mathfrak{B} \vDash \neg\varphi(\boldsymbol{x}_j, \boldsymbol{y}_j),$$
$$\mathfrak{B} \vDash \exists \boldsymbol{y}\ \neg\varphi(\boldsymbol{x}_j, \boldsymbol{y}).$$

But we have arranged things so that every element of B^p is the interpretation of some $\boldsymbol{x}_j$. Therefore

$$\mathfrak{B} \vDash \forall \boldsymbol{x}\ \exists \boldsymbol{y}\ \neg\varphi(\boldsymbol{x}, \boldsymbol{y}),$$

that is, σ is false in $\mathfrak{B}$.

5.3 Completeness by König's Lemma

Gödel himself does not use an ultraproduct explicitly in his argument, but he can be understood to create the structure $\mathfrak{B}$ (with universe ω) as follows.[8] Let $(\alpha_k \colon k \in \omega)$ be a list of all of the atomic formulas appearing

[8] I am guided by Church's version of Gödel's argument here. See below.

in the formulas φ_ℓ. We define $\mathfrak{B}$ by determining in each case whether α_k is to be true in $\mathfrak{B}$ (again with variable v_i understood as i). This determination can be made recursively as follows. First, we let

$$\mathfrak{B} \vDash \alpha_0 \iff |\{i\colon \mathfrak{A}_i \vDash \alpha_0\}| = \omega$$

(that is, α_0 is true in $\mathfrak{B}$ if and only if the set of i such that α_0 is true in $\mathfrak{A}_i$ is infinite), and then

$$\mathfrak{B} \vDash \alpha_1 \iff |\{i\colon {\alpha_0}^{\mathfrak{A}_i} = {\alpha_0}^{\mathfrak{B}} \;\&\; \mathfrak{A}_i \vDash \alpha_1\}| = \omega,$$
$$\mathfrak{B} \vDash \alpha_2 \iff |\{i\colon {\alpha_0}^{\mathfrak{A}_i} = {\alpha_0}^{\mathfrak{B}} \;\&\; {\alpha_1}^{\mathfrak{A}_i} = {\alpha_1}^{\mathfrak{B}} \;\&\; \mathfrak{A}_i \vDash \alpha_2\}| = \omega,$$

and so on, where ${\alpha_j}^{\mathfrak{A}_i} = {\alpha_j}^{\mathfrak{B}}$ means simply that α_j is alike true or false in $\mathfrak{A}_i$ and $\mathfrak{B}$. Strictly the definition is by strong or well-ordered recursion, requiring only the single condition

$$\mathfrak{B} \vDash \alpha_k \iff |\{i\colon \bigwedge_{j<k} {\alpha_j}^{\mathfrak{A}_i} = {\alpha_j}^{\mathfrak{B}} \;\&\; \mathfrak{A}_i \vDash \alpha_k\}| = \omega.$$

It follows by induction that, at each step,

$$|\{i\colon \bigwedge_{j<k} {\alpha_j}^{\mathfrak{A}_i} = {\alpha_j}^{\mathfrak{B}}\}| = \omega. \tag{§}$$

The construction ensures $\mathfrak{B} \vDash \neg\vartheta_j$ as before. Indeed, suppose if possible $\mathfrak{B} \vDash \vartheta_j$. Then the atomic subformulas of ϑ_j belong to a finite set $\{\alpha_i\colon i < k\}$, so

$$\{i\colon \bigwedge_{j<k} {\alpha_j}^{\mathfrak{A}_i} = {\alpha_j}^{\mathfrak{B}}\} \subseteq \{i \in \omega\colon \mathfrak{A}_i \vDash \vartheta_j\}.$$

However, as before we have also

$$\{i \in \omega\colon \mathfrak{A}_i \vDash \vartheta_j\} \subseteq j.$$

These two inclusions together contradict (§).

There is some arbitrariness in this definition of $\mathfrak{B}$. If the truth of α_j in $\mathfrak{B}$ has been determined when $j < k$ so that (§) holds, then we shall want

$$|\{i\colon \bigwedge_{j<k} {\alpha_j}^{\mathfrak{A}_i} = {\alpha_j}^{\mathfrak{B}} \;\&\; \mathfrak{A}_i \vDash \neg\alpha_k\}| < \omega \implies \mathfrak{B} \vDash \alpha_k,$$
$$|\{i\colon \bigwedge_{j<k} {\alpha_j}^{\mathfrak{A}_i} = {\alpha_j}^{\mathfrak{B}} \;\&\; \mathfrak{A}_i \vDash \alpha_k\}| < \omega \implies \mathfrak{B} \vDash \neg\alpha_k.$$

If both of these sets are infinite, then the question of whether $\mathfrak{B} \vDash \alpha_k$ can be decided arbitrarily. We decided above that α_k would be true in $\mathfrak{B}$ in this case. However, if at the beginning we had chosen an ultrafilter D on ω, then we could just define

$$\mathfrak{B} \vDash \alpha_k \iff \{i \colon \mathfrak{A}_i \vDash \alpha_k\} \in D.$$

Gödel himself is not explicit about how he obtains $\mathfrak{B}$. His editor van Heijenoort detects an allusion to König's Lemma. There are more than one theorem called by this name, but probably what is meant is the following [17, Lemma II.5.7, p. 69].

A **tree** is a (partially) ordered set such that, for every element a, the subset $\{x \colon x < a\}$ is well-ordered. The ordinal that is isomorphic to this set is then the **height** of a. If this height is β, then a **successor** of a is an element b of the tree with height $\beta + 1$ such that $a < b$. A **branch** of a tree is a maximal linearly ordered subset.

An **ω-tree** is a tree whose every element has finite height and finitely many successors. One version of König's Lemma is that every infinite ω-tree has an infinite branch. To prove this, we select an infinite branch recursively by first letting a_0 be an element at height 0 such that $\{x \colon a_0 < x\}$ is infinite; then, assuming $\{x \colon a_k < x\}$ is infinite, we let a_{k+1} be a successor of a_k such that $\{x \colon a_{k+1} < x\}$ is infinite.

This lemma applies to the present situation as follows. We start with the complete binary tree $2^{<\omega}$, that is, $\bigcup_{n\in\omega} 2^n$, ordered by inclusion, so that $\boldsymbol{a} \leqslant \boldsymbol{b}$ if and only if $\boldsymbol{a}$ is an initial segment of $\boldsymbol{b}$. See Figure 5.1. This has a sub-tree consisting of those $(e_0, \dots, e_{n-1})$ such that the set

$$\{i \colon \bigwedge_{j<n} {\alpha_j}^{\mathfrak{A}_i} = e_j\}$$

is infinite. This sub-tree is infinite, because it has elements at each finite height. By König's Lemma, the sub-tree has an infinite branch, whose union is a sequence $(e_k \colon k \in \omega)$; we can then define

$$\mathfrak{B} \vDash \alpha_k \iff e_k = 1.$$

As before, $\mathfrak{B} \vDash \neg\sigma$.

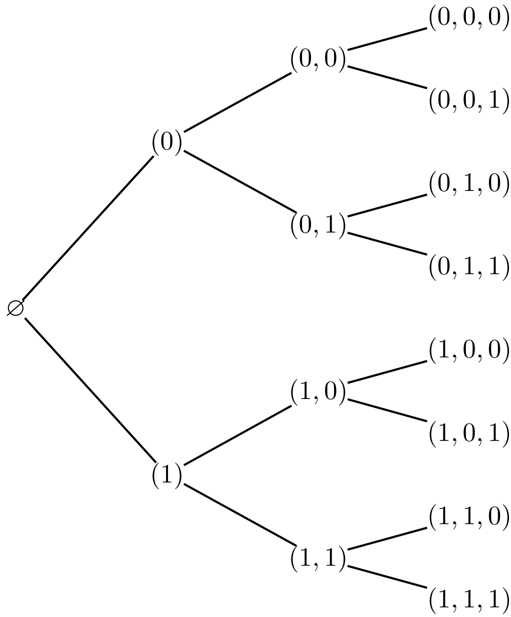

Figure 5.1: A complete binary tree

5.4 Arbitrary formulas

We have to justify the assumptions about σ made at the beginning of §5.2.

5.4.1 Operation-symbols

What we call relations, Gödel calls functions; but he has no symbols for what we call operations. However, even if we do use them, we can dispose of them as follows. Suppose, for some n-ary operation-symbol F, there were an atomic subformula α of σ featuring a term $Ft_0 \cdots t_{n-1}$. Introducing a new $(n+1)$-ary predicate R_F, we could replace the term $Ft_0 \cdots t_{n-1}$ in α with a new variable x, obtaining an atomic formula α'.

We could then replace α in σ with the formula

$$\exists x\ (\alpha' \wedge R_F t_0 \cdots t_{n-1} x),$$

obtaining σ'. Then σ would be logically equivalent to

$$\sigma' \wedge \forall \boldsymbol{x}\ \exists y\ \forall z\ (R\boldsymbol{x}y \wedge (R\boldsymbol{x}z \to y = z)).$$

We should show that σ is provable from this equivalent sentence.

5.4.2 Equality

Suppose no operation-symbol occurs in σ, but the sign $=$ of equality does occur. We have to deal with the requirement that this sign is interpreted in every structure as equality itself (and not merely an equivalence-relation). We introduce a new binary predicate $\equiv$, and we replace each occurrence of $=$ in σ with this new predicate $\equiv$, obtaining a new sentence σ. Now let $(R_0, \dots, R_m)$ be a list of all predicates (including $\equiv$) occurring in σ', and let σ'' be the sentence

$$\sigma' \wedge \forall \boldsymbol{x}\ \forall \boldsymbol{y}\ \Big(\boldsymbol{x} \equiv \boldsymbol{y} \to \bigwedge_{j \leqslant m} (R_j \boldsymbol{x}_j \to R_j \boldsymbol{y}_j)\Big).$$

(Here $\boldsymbol{x}_j$ and $\boldsymbol{y}_j$ are initial segments, of appropriate length, of $\boldsymbol{x}$ and $\boldsymbol{y}$ respectively; and $\boldsymbol{x}$ and $\boldsymbol{y}$ are long enough to make this possible.) One shows that σ is provable from σ''. Also, if $\mathfrak{A} \vDash \sigma''$, then $\equiv^{\mathfrak{A}}$ is an equivalence-relation on A, and the set of equivalence-classes is the universe of a model of σ.

5.4.3 Skolem normal form

Every formula φ is equivalent to a formula $\hat{\varphi}$ of the same signature in **prenex normal form,** that is, with all quantifiers in front. For example, if x is not free in ϑ, then

$$\forall x\ \varphi \wedge \vartheta \sim \forall x\ (\varphi \wedge \vartheta), \qquad \forall x\ \varphi \vee \vartheta \sim \forall x\ (\varphi \vee \vartheta).$$

We shall show that, for every formula φ, there is a *sentence* $\tilde{\varphi}$, possibly with new predicates, with the following two properties.

1. $\tilde{\varphi}$ has the form $\exists \boldsymbol{x}\, \forall \boldsymbol{y}\, \vartheta$, where ϑ is quantifier-free.
2. If $\tilde{\varphi}$ is valid, then so is φ; but if $\neg\tilde{\varphi}$ has a model, then $\neg\varphi$ will be satisfied in that model (that is, it will define a nonempty subset of that model).

The sentence $\tilde{\varphi}$ is a **Skolem normal form** for φ. We can obtain it as follows. First, write out a generalization of φ in prenex normal form, as

$$\exists \boldsymbol{x}\, \forall y\, \mathsf{Q}\, \vartheta,$$

where Q is a string of quantifiers, and ϑ is quantifier-free. Introduce a new predicate R and form the sentence

$$\exists \boldsymbol{x}\, (\forall y\, (\mathsf{Q}\, \vartheta \to R\boldsymbol{x}y) \to \forall y\, R\boldsymbol{x}y).$$

This has the second of the desired properties. It is also equivalent to

$$\begin{gathered}
\exists \boldsymbol{x}\, (\exists y\, (\mathsf{Q}\, \vartheta \land \neg R\boldsymbol{x}y) \lor \forall y\, R\boldsymbol{x}y),\\
\exists \boldsymbol{x}\, \exists y\, ((\mathsf{Q}\, \vartheta \land \neg R\boldsymbol{x}y) \lor \forall z\, R\boldsymbol{x}z),\\
\exists \boldsymbol{x}\, \exists y\, (\mathsf{Q}\, (\vartheta \land \neg R\boldsymbol{x}y) \lor \forall z\, R\boldsymbol{x}z),\\
\exists \boldsymbol{x}\, \exists y\, \mathsf{Q}\, ((\vartheta \land \neg R\boldsymbol{x}y) \lor \forall z\, R\boldsymbol{x}z),\\
\exists \boldsymbol{x}\, \exists y\, \mathsf{Q}\, \forall z((\vartheta \land \neg R\boldsymbol{x}y) \lor R\boldsymbol{x}z),
\end{gathered}$$

This last sentence is in prenex normal form, though perhaps not be in Skolem normal form. Still, the number of universal quantifiers that precede existential quantifiers has decreased. So the process terminates in a sentence that must be in Skolem normal form.

6 Boolean rings and Stone spaces

6.1 Boolean rings

In the ring $(\mathscr{P}(\Omega), \triangle, \cap)$, every element is its own square. As we said in §3.1 on page 34, an arbitrary ring with this property is called a **Boolean ring.** We now establish the promised *Stone Representation Theorem* [23], that for every Boolean ring R the set $\operatorname{Spec}(R)$ of prime ideals of R is such that R embeds (as a ring) in $(\mathscr{P}(\operatorname{Spec}(R)), \triangle, \cap)$. This result is comparable to the so-called Cayley Theorem, that every group G embeds in the group $(\operatorname{Sym}(G), \circ, {}^{-1}, \mathrm{id}_G)$ under $g \mapsto (x \mapsto gx)$.

So let R be a Boolean ring, namely a ring that satisfies the identity

$$x^2 = x.$$

We assume that R has a unit (like all other rings in these notes), but we need not assume that R is commutative, we shall prove it. First, R has characteristic 2, since

$$2x = (2x)^2 = 4x^2 = 4x, \qquad 0 = 2x, \qquad -x = x.$$

It follows that R must be commutative, since now

$$\begin{gathered} x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y, \\ 0 = xy + yx, \\ yx = -xy = xy. \end{gathered}$$

There are Boolean rings-without-units, for example $\mathscr{P}_\omega(\omega)$ (the set of finite subsets of ω, defined on page 36); but again, we shall not consider these as Boolean rings.

We can rewrite the defining identity $x^2 = x$ for Boolean rings as

$$0 = x^2 - x = x \cdot (x - 1) = x \cdot (x + 1).$$

Hence if $\mathfrak{p}$ is a prime ideal of R, then since $0 \in \mathfrak{p}$, for all x in R we have either $x \in \mathfrak{p}$ or $x - 1 \in \mathfrak{p}$ (that is, $x + 1 \in \mathfrak{p}$). Thus $\mathfrak{p}$ has just two cosets: itself and $1 + \mathfrak{p}$. Therefore $R/\mathfrak{p} \cong \mathbb{F}_2$, a field, so $\mathfrak{p}$ must be maximal. (We showed this for $\mathscr{P}(\Omega)$ on page 37.) Also,

$$x \in \mathfrak{p} \iff x + 1 \notin \mathfrak{p}.$$

As above, we let $\mathrm{Spec}(R)$ be the set of prime ideals of R, and if $x \in R$, we let $[x]$ be the set of prime ideals of R that do *not* contain x. If $\mathfrak{p} \in \mathrm{Spec}(R)$, we have

$$xy \in \mathfrak{p} \iff x \in \mathfrak{p} \lor y \in \mathfrak{p},$$

hence

$$xy \notin \mathfrak{p} \iff x \notin \mathfrak{p} \ \ \& \ \ y \notin \mathfrak{p}.$$

Thus,

$$[xy] = [x] \cap [y].$$

Because R has characteristic 2, the sum of any two elements of $\{x, y, x+y\}$ is the third. Since

$$xy(x + y) = x^2 + xy^2 = xy + xy = 0,$$

$\mathfrak{p}$ must contain at least one of x, y, and $x + y$. Then $\mathfrak{p}$ contains exactly one of these, or all:

$$x + y \notin \mathfrak{p} \iff (x \in \mathfrak{p} \ \ \& \ \ y \notin \mathfrak{p}) \lor (x \notin \mathfrak{p} \ \ \& \ \ y \in \mathfrak{p}).$$

Thus

$$[x + y] = [x] \mathbin{\triangle} [y].$$

Since finally $[1] = \mathrm{Spec}(R)$, we have now that $x \mapsto [x]$ is a homomorphism (of rings) from R to $\mathscr{P}(R)$. It is injective too, since if $x \neq 0$, then $x + 1 \neq 1$, so $x + 1$ generates a proper ideal that does not contain x, and this ideal is included in a prime ideal, which must be in $[x]$, so $[x] \neq \varnothing$.

6.2 Ultrafilters

It follows now that an arbitrary Boolean ring R has all of the operations and relations that can be defined on a Boolean ring $\mathscr{P}(\Omega)$ and its subrings. For example, R is (partially) ordered by $\leqslant$ corresponding to $\subseteq$, where

$$x \leqslant y \iff xy = x.$$

Also R has operations $\neg$ and $\wedge$, corresponding respectively to ${}^{\mathrm{c}}$ and $\cap$, so that

$$\neg x = x + 1, \qquad\qquad x \wedge y = xy.$$

Then

$$0 = x \wedge \neg x, \qquad\qquad 1 = \neg 0,$$

and the operation $\vee$ corresponding to $\cup$ can be given by

$$x \vee y = \neg(\neg x \wedge \neg y). \tag{$*$}$$

The structure $(R, \neg, \wedge)$ is called a **Boolean algebra.** Usually the signature of Boolean algebras is considered to be $\{0, 1, \neg, \wedge, \vee\}$; but again the additional operations can be defined from $\neg$ and $\wedge$.

There is an equivalent axiomatic definition, which for the record can be given as follows. A structure $(R, \neg, \wedge)$ is a Boolean algebra if and only if R has at least two elements, and the following equations are identities in the structure:

$$\begin{gathered}
x \wedge y = y \wedge x, \\
x \wedge (y \wedge z) = (x \wedge y) \wedge z, \\
x \wedge x = x, \\
\neg\neg x = x, \\
(x \wedge \neg x) \wedge y = x \wedge \neg x, \\
\neg(x \wedge \neg(y \wedge z)) = \neg(x \wedge \neg y) \wedge \neg(x \wedge \neg z).
\end{gathered}$$

The last identity is equivalent to

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

when $\vee$ is defined as in $(*)$. The Boolean ring $(R, +, \cdot, 0, 1)$ can be recovered from the algebra by the rules

$$x + y = (x \wedge \neg y) \vee (\neg x \wedge y), \qquad\qquad xy = x \wedge y.$$

Now we have the characterization of ideals on page 35, as well as the definition of filters: A subset I of R is an ideal if and only if

$$\begin{gathered} 0 \in I, \\ x \leqslant y \;\; \& \;\; y \in I \implies x \in I, \\ x \in I \;\; \& \;\; y \in I \implies x \vee y \in I, \end{gathered}$$

and a subset F is a **filter** if and only if $\{x + 1 \colon x \in F\}$ is an ideal, or equivalently

$$\begin{gathered} 1 \in F, \\ x \in F \;\; \& \;\; x \leqslant y \implies y \in F, \\ x \in F \;\; \& \;\; y \in F \implies x \wedge y \in F. \end{gathered}$$

Then F is an **ultrafilter** if and only if $\{x + 1 \colon x \in F\}$ is a prime ideal, and in this case F is the complement in R of the prime ideal.

6.3 Stone spaces

Given a Boolean ring R, we denote the set of its ultrafilters by

$$\mathrm{S}(R).$$

We have a bijection $\mathfrak{p} \mapsto \mathfrak{p}^{\mathrm{c}}$ from $\operatorname{Spec}(R)$ to $\mathrm{S}(R)$; this induces an isomorphism from $\mathscr{P}(\operatorname{Spec}(R))$ to $\mathscr{P}(\mathrm{S}(R))$. In particular, if $x \in R$, we may now define

$$[x] = \{\mathfrak{f} \in \mathrm{S}(R) \colon x \in f\},$$

so that $x \mapsto [x]$ is an embedding of R in $\mathscr{P}(\mathrm{S}(R))$.

A reason for working with $\mathrm{S}(R)$ rather than $\operatorname{Spec}(R)$ is that, as we shall discuss in §7.3 below, logical theories can be understood as filters, and then theories that are ultrafilters will be called *complete theories.* Also, in a *topological space* X, the set of *neighborhoods* of a point is a filter of $\mathscr{P}(X)$.

The set $\mathrm{S}(R)$ is called the **Stone space** of R. Indeed, since (as we saw)

$$[x] \cap [y] = [xy], \qquad [1] = \mathrm{S}(R),$$

the subsets $[x]$ of $\mathrm{S}(R)$ compose a *basis* for a topology on $\mathrm{S}(R)$ called the **Stone topology.** Every union of sets $[x]$ is called is *open* in this topology, and it follows that:

1) if $\mathcal{U}$ is a finite collection of open sets, then $\bigcap \mathcal{U}$ is also open—here we may by convention allow $\bigcap \varnothing = \mathrm{S}(R)$;
2) if $\mathcal{U}$ is a collection of open sets, then $\bigcup \mathcal{U}$ is open—in particular, $\bigcup \varnothing = \varnothing$, so this is understood to be open.

The complement of an open set is *closed.* Since

$$[x]^{\mathrm{c}} = [x+1],$$

the basic open sets $[x]$ are also closed.

Suppose $\mathfrak{f}$ and $\mathfrak{g}$ are distinct elements of $\mathrm{S}(R)$. Then we may assume $\mathfrak{f} \smallsetminus \mathfrak{g}$ has an element x. In this case

$$\mathfrak{f} \in [x], \qquad \mathfrak{g} \in [x+1], \qquad [x] \cap [x+1] = \varnothing.$$

Thus the Stone topology is *Hausdorff:* it separates points.

Suppose $\bigcup_{x \in A}[x] = \mathrm{S}(R)$ for some subset A of R. Then every ultrafilter of R contains some element of A. Then no prime ideal of R includes A (since otherwise its complement would be an ultrafilter disjoint from A). Therefore the ideal (A) of R generated by A must the improper ideal R. In particular, this ideal contains 1. But then (A_0) must contain 1 for some finite subset A_0 of A. In this case no prime ideal of R includes A_0, so every ultrafilter contains an element of A_0, which means

$$\bigcup_{x \in A_0} [x] = \mathrm{S}(R).$$

This shows the Stone topology is *compact.*

Another way to prove this topology compact is the following. We have $\mathrm{S}(R) \subseteq \mathscr{P}(R)$, and we may identify the power 2^R with $\mathscr{P}(R)$ under the map

$$(x_i \colon i \in R) \mapsto \{i \in R \colon x_i = 1\}$$

from 2^R to $\mathscr{P}(R)$. (This map can be understood as $x \mapsto x^{-1}(1)$.) If we give the set 2 the discrete topology, then 2^R can be given the corresponding *product topology,* which is the weakest topology in which all of the maps $x \mapsto x_i$ (where $i \in R$) are continuous. Since the factors 2 are finite, this means the topology has a basis comprising, for each finite subset R_0 of R, for each $(a_i \colon i \in R_0)$ in 2^{R_0}, the set $\{x \in 2^R \colon (x_i \colon i \in R_0) = (a_i \colon i \in R_0)\}$. This set is both open and closed. Then $\mathrm{S}(R)$ has the subspace topology and is moreover a closed subset of 2^R, being the intersection of all closed sets of the forms

$$\begin{gathered}\{x \in 2^R \colon x_1 = 1\},\\ \{x \in 2^R \colon x_{ab} = 0 \lor x_b = 1\},\\ \{x \in 2^R \colon x_a = 0 \lor x_b = 0 \lor x_{ab} = 1\},\\ \{x \in 2^R \colon x_a = 0 \iff x_{a+1} = 1\}.\end{gathered}$$

As 2^R is compact by the *Tychonoff Theorem,* so must $\mathrm{S}(R)$ be compact.

Note that this case of the Tychonoff Theorem is easy to prove (and the general theorem is not much harder). Suppose $\mathcal{F}$ is a collection of closed subsets of 2^R with the *finite-intersection property,* that is, for every finite subset $\mathcal{F}_0$ of $\mathcal{F}$, the intersection $\bigcap \mathcal{F}_0$ is nonempty. We want to show that $\bigcap \mathcal{F}$ itself is nonempty. We may assume that the elements of $\mathcal{F}$ are *basic* closed sets; and then we may assume that each element of $\mathcal{F}$ has the form $\{x \in 2^R \colon x_i = e\}$ for some i in R and e in 2. By the finite intersection property, there is no i in R such that $\mathcal{F}$ contains both $\{x \colon x_i = 0\}$ and $\{x \colon x_i = 1\}$. Then $\bigcap \mathcal{F}$ contains a, where

$$a_i = \begin{cases} e, & \text{if } \{x \colon x_i = e\} \in \mathcal{F},\\ 0, & \text{otherwise.}\end{cases}$$

We can compute

$$\begin{aligned}[x] \cup [y] &= ([x]^{\mathrm{c}} \cap [y]^{\mathrm{c}})^{\mathrm{c}} \\ &= ([x+1] \cap [y+1])^{\mathrm{c}} \\ &= [(x+1)(y+1)]^{\mathrm{c}} \\ &= [xy+x+y+1]^{\mathrm{c}} \\ &= [xy+x+y] \\ &= [x \vee y].\end{aligned}$$

Consequently, the only open sets that are also closed are the basic open sets, that is, the sets $[x]$. For if the open set $\bigcup_{x\in A}[x]$ is also closed, then (since closed subsets of compact spaces are compact), we have

$$\bigcup_{x\in A}[x] = [x_0] \cup \cdots \cup [x_{n-1}] = [x_0 \vee \cdots \vee x_{n-1}]$$

for some x_i in A. Thus the subsets of $\mathrm{S}(R)$ that are both closed and open—*clopen*—compose a Boolean algebra or ring, which is the isomorphic image of R under $x \mapsto [x]$.

An arbitrary compact Hausdorff space with a basis of clopen sets can be called a **Stone space** simply. Suppose S is one of these, and let $\mathrm{B}(S)$ be the set of clopen subsets of S. Then $\mathrm{B}(S)$ is a Boolean sub-ring of $\mathscr{P}(S)$. In the special case where $S = \mathrm{S}(R)$, we have just noted

$$R \cong \mathrm{B}(\mathrm{S}(R)).$$

In the general case, for every point P in S, the set $\{U \in \mathrm{B}(S)\colon P \in U\}$ of basic neighborhoods of P is a filter and in fact an ultrafilter of $\mathrm{B}(S)$. Thus we have a map

$$P \mapsto \{U \in \mathrm{B}(S)\colon P \in U\} \tag{\dagger}$$

from S to $\mathrm{S}(\mathrm{B}(S))$. Since S is Hausdorff, the map is injective. Suppose $\mathfrak{f} \in \mathrm{S}(\mathrm{B}(S))$. The intersection of every finite subset of $\mathfrak{f}$ is an element of $\mathfrak{f}$; in particular, it is a nonempty subset of S. Thus $\mathfrak{f}$ has the finite intersection property. Since S is compact, $\bigcap \mathfrak{f}$ itself must be a nonempty subset of S. Since also again S is Hausdorff, $\bigcap \mathfrak{f}$ must consist of a single point, P; and then we must have

$$\mathfrak{f} = \{U \in \mathrm{B}(S)\colon P \in U\}.$$

So the map in (†) is a bijection from S to $\mathrm{S}(\mathrm{B}(S))$. In fact it is a homeomorphism. For, it takes every clopen subset V of S (that is, every element V of $\mathrm{B}(S)$) to the subset

$$\big\{\{U \in \mathrm{B}(S)\colon P \in U\}\colon P \in V\big\}$$

of $\mathrm{S}(\mathrm{B}(S))$; and this subset is $[V]$, namely $\{\mathfrak{f} \in \mathrm{S}(\mathrm{B}(S))\colon V \in \mathfrak{f}\}$, since

$$V \in \{U \in \mathrm{B}(S)\colon P \in U\} \iff P \in V.$$

6.4 Boolean operations

We observed in §6.2 that Boolean rings and Boolean algebras are 'interdefinable': every Boolean ring is also a Boolean algebra whose basic operations are the interpretations in the ring of certain terms; and then the Boolean ring can be obtained from the algebra in the same way.

A **Boolean operation** on a power-set $\mathscr{P}(\Omega)$ is just an operation on $\mathscr{P}(\Omega)$ that is the interpretation of a term in the signature of rings or Boolean algebras. We should like to verify that every operation on $\mathscr{P}(\Omega)$ that can be defined without reference to Ω itself is a Boolean operation. One way of doing this is as follows.

Suppose we have n subsets $X^0, \dots, X^{n-1}$ of Ω. For each element σ of 2^n, there is a subset X_σ of Ω given by

$$X_\sigma = X^0_\sigma \cap \dots \cap X^{n-1}_\sigma,$$

where

$$X^i_\sigma = \begin{cases} X^i, & \text{if } \sigma(i) = 1,\\ (X^i)^{\mathrm{c}}, & \text{if } \sigma(i) = 0.\end{cases}$$

See Figure 6.1 for the cases $n = 2$ and $n = 3$ (here each set X_σ is labelled with σ). In case $n = 0$, the set 2^n has the unique element 0 (the empty function), and then X_σ should be understood as Ω. In any case, the sets X_σ partition Ω into at most 2^n subsets—or $|2^n|$ subsets, if we still consider 2^n as the set of functions from n to 2. For every subset S of 2^n in this sense, the subset $\bigcup_{\sigma\in S} X_\sigma$ of Ω is a Boolean combination of the sets X^i; and every Boolean combination of these sets is of this form.

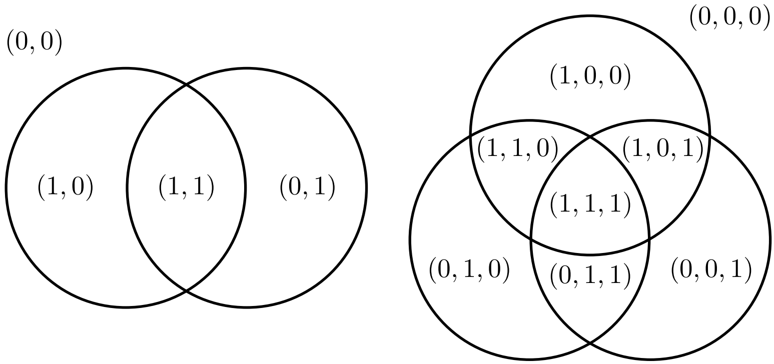

Figure 6.1: Boolean combinations

Thus the number of Boolean combinations of the X^i is at most 2^{2^n}. (It is less, if one of them is included in the union of the others.)

7 More model theory

7.1 The structure of definable relations

The structures that we have worked with so far are more precisely called **one-sorted structures.** By contrast, a vector-space is a two-sorted structure, with a sort for the vectors and a sort for the scalars. It is difficult to use a general notation for structures of arbitrarily many sorts; so we just describe the general situation for one-sorted structures, and then we point out that things can be adapted to many-sorted structures as needed.

The definable relations of a (one-sorted structure) $\mathfrak{A}$ are themselves elements of a many-sorted structure, with a sort for each finite subset I of ω: this sort corresponds to the set $\{x_i : i \in I\}$ of variables.

The n-ary relations on A compose the set $\mathscr{P}(A^n)$. Suppose $B \subseteq A$. The set of n-ary B-definable relations of $\mathfrak{A}$ can be denoted by

$$\mathrm{Def}^n_B(\mathfrak{A}).$$

This is a subset of $\mathscr{P}(A^n)$, and moreover it closed under the Boolean operations; that is, $\mathrm{Def}^n_B(\mathfrak{A})$ is (the universe of) a Boolean sub-algebra of $\mathscr{P}(A^n)$. To check this, we need only note:

$$(\varphi^{\mathfrak{A}})^{\mathrm{c}} = (\neg\varphi)^{\mathfrak{A}}, \qquad \varphi^{\mathfrak{A}} \cap \psi^{\mathfrak{A}} = (\varphi \wedge \psi)^{\mathfrak{A}}, \tag{$*$}$$

and also

$$\varnothing = \Big(\bigvee_{i<n} x^i \neq x^i\Big)^{\mathfrak{A}},$$

so that $\mathrm{Def}^n_B(\mathfrak{A})$ has the two distinct elements $\varnothing$ and its complement A^n.

On the set $\mathscr{P}(A^n)$, if $n > 1$, additional operations besides the Boolean operations are possible. Indeed, if σ is a permutation of n, then there is a function σ^* from A^n to A^n, given by

$$\sigma^*(x^0, \dots, x^{n-1}) = (x^{\sigma(0)}, \dots, x^{\sigma(n-1)}).$$

Now the singulary operation $X \mapsto \sigma^*[X]$ on $\mathscr{P}(A^n)$ is induced.

The same idea gives us functions from $\mathscr{P}(A^n)$ to $\mathscr{P}(A^m)$. Indeed, suppose now σ is a function from m to n, where $n > 0$ or $m = 0$. For example, if $m < n$, then σ could be the inclusion of m in n. Or if $m = n + 1$, then σ could be given by

$$\sigma(i) = \begin{cases} i, & \text{if } i < n, \\ n-1, & \text{if } i = n. \end{cases} \tag{†}$$

In any case, a function σ^* from A^n to A^m is induced, given by

$$\sigma^*(x^0, \dots, x^{n-1}) = (x^{\sigma(0)}, \dots, x^{\sigma(m-1)}).$$

Then we have the function $X \mapsto \sigma^*[X]$ from $\mathscr{P}(A^n)$ to $\mathscr{P}(A^m)$; here

$$\sigma^*[X] = \{(x^{\sigma(0)}, \dots, x^{\sigma(m-1)})\colon (x^0, \dots, x^{n-1}) \in X\}.$$

For example, if $n = m + 1$, and σ is the inclusion of m in n, then

$$\sigma^*[X] = \{(x^0, \dots, x^{m-1})\colon (x^0, \dots, x^m) \in X\};$$

but since the appearance of x^m here may seem peculiar, we can also write

$$\sigma^*[X] = \{(x^0, \dots, x^{m-1})\colon (x^0, \dots, x^m) \in X \text{ for some } x^m\}.$$

For another example, if $m = 2$ and $n = 1$, so that σ must be the constant function $x \mapsto 0$ on 2, then

$$\sigma^*[X] = \{(x, x)\colon x \in X\}.$$

In the general situation, we also have $X \mapsto \sigma_*[X]$ from $\mathscr{P}(A^m)$ to $\mathscr{P}(A^n)$, where

$$\sigma_*[X] = (\sigma^*)^{-1}[X] = \{(x^0, \dots, x^{n-1}) \in A^n\colon (x^{\sigma(0)}, \dots, x^{\sigma(m-1)}) \in X\}.$$

For example, if σ is the inclusion of m in n, then $\sigma_*[X]$ can be understood as $X \times A^{n-m}$; while if $\sigma\colon 2 \to 1$, then

$$\sigma_*[X] = \{x \in A\colon (x,x) \in X\}.$$

Note that, in general, every function σ from m to n is a composition of:

1. permutations of some k,
2. inclusions of some k in $k+1$;
3. maps from some $k+1$ to k as in (†).

It should be clear that $X \mapsto \sigma^*[X]$ takes $\operatorname{Def}^m_B(\mathfrak{A})$ to $\operatorname{Def}^n_B(\mathfrak{A})$, and $X \mapsto \sigma_*[X]$ takes $\operatorname{Def}^n_B(\mathfrak{A})$ to $\operatorname{Def}^m_B(\mathfrak{A})$.

The elements of ω are also finite subsets of ω. We could work with arbitrary finite subsets of ω. A formula whose free variables compose the set $\{x_i\colon i \in I\}$ then defines in $\mathfrak{A}$ a subset of A^I; and then we have the subsets $\operatorname{Def}^I_B(\mathfrak{A})$ of $\mathscr{P}(A^I)$.

Consider the collection of all indexed families $(P_I\colon I \in \mathscr{P}_\omega(\omega))$, where $P_I \subseteq \mathscr{P}(A^I)$, and

- each P_I is closed under the Boolean operations,
- if $\sigma\colon I \to J$, the function $X \mapsto \sigma^*[X]$ takes P_J to P_I, and $X \mapsto \sigma_*[X]$ takes P_I to P_J,
- for each n in ω, for each n-ary predicate R in $\mathscr{S}$, P_n contains $R^{\mathfrak{A}}$,
- for each n in ω, for each n-ary operation-symbol F in $\mathscr{S}$, P_{n+1} contains $\{(\boldsymbol{a}, b) \in A^{n+1}\colon F^{\mathfrak{A}}(\boldsymbol{a}) = b\}$ (that is, $(F\boldsymbol{x} = x^n)^{\mathfrak{A}}$).
- for each c in B, P_1 contains $\{c\}$.

The indexed family $(\operatorname{Def}^I_B(\mathfrak{A})\colon I \in \mathscr{P}_\omega(\omega))$ is a minimum among these families.

7.2 Lindenbaum–Tarski algebras

For any signature $\mathscr{S}$ and n in ω, let us denote by

$$\operatorname{Sn}^n(\mathscr{S})$$

the set of n-ary formulas of $\mathscr{S}$. Two elements φ and ψ of $\mathrm{Sn}^n(\mathscr{S})$ are said to be **logically equivalent** if the formula $\varphi \leftrightarrow \psi$ is a validity in the sense of Chapter 5, that is, for every structure $\mathfrak{A}$ of $\mathscr{S}$,

$$\varphi^{\mathfrak{A}} = \psi^{\mathfrak{A}},$$

or equivalently the sentence

$$\forall \boldsymbol{x}\ (\varphi(\boldsymbol{x}) \leftrightarrow \psi(\boldsymbol{x}))$$

is true in all structures in $\mathrm{Mod}(\mathscr{S})$. The set of logical equivalence-classes of elements of $\mathrm{Sn}^n(\mathscr{S})$ is denoted by

$$\mathrm{B}_n(\mathscr{S}).$$

This is the nth **Lindenbaum–Tarski algebra** of $\mathscr{S}$, and it is a Boolean algebra in a fairly obvious way. The rest of this section is devoted to spelling this out.

The set $\mathrm{Sn}^n(\mathscr{S})$ can be understood as a structure equipped with the operations $\neg$ and $\wedge$. A structure without relations, but only operations, is called an **algebra.** So we have an algebra $(\mathrm{Sn}^n(\mathscr{S}), \neg, \wedge)$. This algebra is *not* a Boolean algebra, simply because, for example, $\neg\neg\varphi$ is never the same formula as φ.

Still, if $\mathfrak{A} \in \mathrm{Mod}(\mathscr{S})$ and $B \subseteq A$, the function $\varphi \mapsto \varphi^{\mathfrak{A}}$ is an epimorphism from $(\mathrm{Sn}^n(\mathscr{S}(B)), \neg, \wedge)$ to $(\mathrm{Def}^n_B(\mathfrak{A}), {}^{\mathrm{c}}, \cap)$: it is a surjection that respects the operations, as in $(*)$ on page 75.

For an arbitrary homomorphism h from an algebra $\mathfrak{M}$ to $\mathfrak{N}$, the **(generalized) kernel** of h is the binary relation $\{(x, y) \colon h(x) = h(y)\}$ on M. If the structures are rings, then the connection between the usual kernel and the generalized kernel is shown by the equivalence

$$h(x) = h(y) \iff h(x - y) = 0.$$

Such an equivalence is not always available for arbitrary algebras. Still, the generalized kernel is an equivalence-relation; and then a quotient $\mathfrak{M}/\ker(h)$ can be defined, which is isomorphic to the image of $\mathfrak{M}$ under h.

In particular then, there is a quotient of $(\mathrm{Sn}^n(\mathscr{S}(B)), \neg, \wedge)$ that is a Boolean algebra, namely the quotient by the kernel of $\varphi \mapsto \varphi^{\mathfrak{A}}$: this quotient is isomorphic to $\mathrm{Def}^n_B(\mathfrak{A})$.

The kernel of a homomorphism on the arbitrary algebra $\mathfrak{M}$ is an example of a **congruence-relation:** an equivalence-relation $\sim$ on M that respects the algebraic structure of $\mathfrak{M}$ in the sense that, for every n in ω, for every basic n-ary operation of $\mathfrak{M}$,

$$x^0 \sim y^0 \ \& \ \cdots \ \& \ x^{n-1} \sim y^{n-1} \implies F(\boldsymbol{x}) \sim F(\boldsymbol{y}).$$

In this case there is a well-defined quotient $\mathfrak{M}/{\sim}$, and there is a quotient-map from $\mathfrak{M}$ to $\mathfrak{M}/{\sim}$ whose kernel is of course $\sim$.

We have seen the one-to-one correspondence between ideals and filters of a Boolean algebra. There is also a one-to-one correspondence between ideals and congruence-relations of a Boolean algebra, namely

$$I \mapsto \{(x, y) \colon x + I = y + I\},$$

with inverse ${\sim} \mapsto \{x \colon x \sim 0\}$.

The set of congruence-relations on $(\mathrm{Sn}(\mathscr{S})\mathscr{S}, \neg, \wedge)$ (or on any algebra) is closed under arbitrary intersections. The intersection of the set of kernels of all homomorphisms $\varphi \mapsto \varphi^{\mathfrak{A}}$, where $\mathfrak{A} \in \mathrm{Mod}(\mathscr{S})$, is just the relation of logical equivalence defined above, and $\mathrm{B}_n(\mathscr{S})$ is the quotient of $\mathrm{Sn}^n(\mathscr{S})$ by this relation. We shall henceforth each formula with its logical equivalence-class, that is, confuse each element of $\mathrm{Sn}^n(\mathscr{S})$ with its image in $\mathrm{B}_n(\mathscr{S})$.

7·3 Theories and type-spaces

By Gödel's Completeness Theorem, the relation $\vdash$ can be considered as a binary relation on $\mathrm{B}_n(\mathscr{S})$; indeed, it is the ordering induced by the algebraic structure. That is, $\varphi \vdash \psi$ means that the formula $\varphi \to \psi$ is a validity. With respect to the ordering, the greatest and least elements of the algebra (that is, the 1 and the 0) can be denoted respectively by

$$\top, \qquad\qquad \bot.$$

Every theory of $\mathscr{S}$ can be understood as a filter of $\mathrm{B}_0(\mathscr{S})$. That is, if $\mathcal{K} \subseteq \mathrm{Mod}(\mathscr{S})$, then $\mathrm{Th}(\mathcal{K})$ has the closure properties required of a filter:

1) it contains $\top$;
2) if it contains σ and τ, then it contains $\sigma \wedge \tau$;
3) if it contains σ, and if $\sigma \vdash \tau$, then it contains τ.

Suppose $\Gamma \subseteq \mathrm{B}_0(\mathscr{S})$. Then the set

$$\mathrm{Th}(\mathrm{Mod}(\Gamma))$$

is a filter of $\mathrm{B}_0(\mathscr{S})$. This filter is the set of all elements of $\mathrm{B}_0(\mathscr{S})$ that are true in all models of Γ. But there is also a filter generated by Γ, namely the set of all σ such that $\bigwedge \Gamma_0 \vdash \sigma$ for some finite subset Γ_0 of Γ. By the Compactness Theorem (Theorem 6, page 47), these two filters are the same. If σ is a member, we may write

$$\Gamma \vdash \sigma.$$

By the Compactness Theorem then, every proper filter of $\mathrm{B}_0(\mathscr{S})$ has a model.

The sameness of the two foregoing filters is not trivial, because the Compactness Theorem is not trivial. The Compactness Theorem does not follow merely from the compactness of Stone spaces. For example, the *second-order* theory of $(\omega, 0, x \mapsto x + 1)$ is axiomatized by

$$\begin{gathered}\forall x\; x + 1 \neq 0,\\ \forall x\, \forall y\; (x + 1 = y + 1 \rightarrow x = y),\\ \forall X\; (0 \in X \wedge \forall y\; (y \in X \rightarrow y + 1 \in X) \rightarrow \forall y\; y \in X).\end{gathered}$$

All models of these axioms are isomorphic to one another. In particular, there is no model that is also a model of each of the sentences $c \neq 0$, $c \neq 1$, $c \neq 2$, and so on, where c is a new constant. However, every finite set of these sentences has a model, if the interpretation of c is large enough.

If T is a theory of $\mathscr{S}$, then two formulas φ and ψ are **equivalent *modulo*** T if

$$T \vdash \forall \boldsymbol{x}\; (\varphi(\boldsymbol{x}) \leftrightarrow \psi(\boldsymbol{x})).$$

The equivalence-classes with respect to this relation compose the Boolean algebra

$$\mathrm{B}_n(T).$$

Then $\mathrm{B}_n(\mathscr{S})$ is $\mathrm{B}_n(\varnothing)$ or $\mathrm{B}_n(\top)$. The Stone space of $\mathrm{B}_n(T)$ can be denoted by

$$\mathrm{S}_n(T).$$

The elements of this space are called ***n*-types** of T—or one may call them **complete *n*-types** of T, if one wants to use the word *type* more generally for arbitrary filters of $\mathrm{B}_n(T)$ or just arbitrary collections of n-ary formulas. In any case, an element of $\mathrm{S}_0(\mathscr{S})$ is called a **complete theory.**

Suppose $\Phi \in \mathrm{S}_n(T)$. If Φ_0 is a finite subset of Φ, then $\bigwedge \Phi_0$ is *not* equivalent to $\bot$ *modulo* T. In this case $T \cup \left\{\exists \boldsymbol{x} \ \bigwedge \Phi_0(\boldsymbol{x})\right\}$ has a model.

Suppose also $\mathfrak{A} \vDash T$. An element $\boldsymbol{a}$ of A^n **realizes** Φ if, for all φ in Φ,

$$\mathfrak{A} \vDash \varphi(\boldsymbol{a}).$$

In this case, we may say also that $\mathfrak{A}$ itself **realizes** Φ. By Compactness, some model of T realizes Φ. Indeed, $\mathfrak{A}$ has an elementary extension that realizes Φ.

7.4 Saturation

We are often concerned with the *parameters* used in formulas and types. If $\mathfrak{M} \in \mathrm{Mod}(\mathscr{S})$, and A is a subset of M, then by $\mathfrak{M}_A$ we mean $\mathfrak{M}$, considered as having signature $\mathscr{S}(A)$. We may then denote $\mathrm{S}_n(\mathrm{Th}(\mathfrak{M}_A))$ simply by

$$\mathrm{S}_n(A);$$

an element of this can be called a type **over** A. For every infinite cardinal κ, a structure is called **κ-saturated** if it realizes every type that has fewer than κ-many parameters. In particular, a structure is **ω_1-saturated** or **$\aleph_1$-saturated** if it realizes all types in countably many parameters.

Theorem 13. *For every structure $\mathfrak{A}$ with a countable signature, every non-principal ultrapower $\mathfrak{A}^\omega/P$ of $\mathfrak{A}$ is ω_1-saturated.*

Proof. If Φ is a type in countably many parameters, then Φ itself is countable, so we can write it as $\{\varphi_n : n \in \omega\}$. Let $\boldsymbol{a}_n$ satisfy $\varphi_0 \wedge \cdots \wedge \varphi_n$ in $\mathfrak{A}$. Then

$$k \leqslant n \implies \mathfrak{A} \vDash \varphi_k(\boldsymbol{a}_n).$$

Therefore, if P is a non-principal prime ideal of $\mathscr{P}(\omega)$, then $(\boldsymbol{a}_n : n \in \omega)/P$ realizes Φ in $\mathfrak{A}^\omega/P$. $\square$

There is a version [5, Thm 6.1.1, p. 384] of the foregoing for uncountable index-sets (or exponents) Ω; but then P must have a countable subset whose union is Ω (so one should show that such prime ideals can be found).

8 Rings

8.1 Ideals

In this chapter, as throughout these notes, the word **ring** will always mean a commutative unital ring. The letter R will always denote a ring in this sense. We have spent time with Boolean rings; now we work more generally (and also review some of the basic facts about integral domains and fields that we have already used). The main point is to develop some of the algebraic geometry that will be used in the examples of ultraproducts in the remaining two chapters.

The following are equivalent conditions on the ring R:

- $1 = 0$ in R.
- R has only one element.

A ring meeting either of these conditions will be called **trivial.**

Let the variables x and y range over R. If $x \neq 0$ and $y \neq 0$ (that is, if $x \in R \smallsetminus \{0\}$ and $y \in R \smallsetminus \{0\}$), but

$$xy = 0,$$

then x and y are called **zero-divisors.** An **integral domain** is a non-trivial ring with no zero-divisors.[1] Equivalently, R is an integral domain if and only if

$$xy = 0 \wedge x \neq 0 \implies y = 0.$$

For example, the ring $\mathbb{Z}$ of rational integers is an integral domain. So are the polynomial rings $K[X]$, $K[X,Y]$, and so forth, where K is a field.

[1] Lang [18, pp. 91–92] recommends *entire* as the adjective form of *integral domain,* observing that *integral* would have been better, had it not already been taken for other purposes.

However, suppose n is a positive integer. Then $\mathbb{Z}/n\mathbb{Z}$ (namely the ring of integers *modulo* n) is an integral domain if and only if n is prime.

Here $n\mathbb{Z}$ is the ideal $\{nx\colon x \in \mathbb{Z}\}$ of $\mathbb{Z}$. In general, an **ideal** of R is an additive subgroup I such that the quotient group R/I is also a ring with respect to the multiplication given by

$$(x + I) \cdot (y + I) = xy + I.$$

That is, for I to be an ideal, we need

$$(x + I) \cdot I = I$$

(since I is the zero of R/I); this means

$$y \in I \implies xy \in I;$$

and this is enough.

Every ideal contains 0 at least; if it contains nothing else, it is the **trivial ideal** or **zero-ideal.**

A **proper** ideal of R is an ideal different from R itself: equivalently, it is an ideal that does not contain 1.

A proper ideal I of R is called **prime** if

$$xy \in I \ \& \ x \notin I \implies y \in I.$$

Compare this with the definition of integral domains:

Theorem 14. *A ring is an integral domain if and only if the trivial ideal is prime.*

For another example, $\{0\} \cup \{\text{zero-divisors}\}$ is a prime ideal, which we shall denote by

$$I_0.$$

So R is an integral domain if and only if $I_0 = \{0\}$. A positive integer n is prime if and only if $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

Theorem 15. *Let I be an ideal of R. Then R/I is an integral domain if and only if I is prime.*

Proof. We have that R/I is nontrivial if and only if I is proper. Assuming I is proper we have that the following are equivalent.

- R/I is an integral domain.
- $(x+I)\cdot(y+I) = I \;\;\&\;\; x+I \neq I \implies y+I = I.$
- $xy \in I \;\;\&\;\; x \notin I \implies y \in I.$
- I is prime. □

A **unit** of a ring is a divisor of 1. That is, if

$$xy = 1,$$

then both x and y are units. The units of R compose a multiplicative subgroup of R, denoted by

$$R^\times.$$

In a trivial ring, 0 is a unit. but zero-divisors are never units or 0; that is, if R has any zero-divisors, they belong to $R \smallsetminus (R^\times \cup \{0\})$. We can also write

$$1 \neq 0 \implies I_0 \cap R^\times = \varnothing.$$

A ring is a **field** if all nonzero elements are units. That is, R is a field if and only if $R = R^\times \cup \{0\}$. In particular, fields have no zero-divisors, so they are integral domains.

The standard examples of fields are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Moreover, if p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is (not only an integral domain, but) a field.

A **maximal ideal** is a proper ideal that is maximal as such. An ideal I of R is maximal if I is a proper ideal and, for all ideals J of R,

$$I \subseteq J \;\;\&\;\; I \neq J \implies J = R.$$

If $A \subseteq R$, then by

$$(A)$$

is meant the smallest ideal of R that includes A. Then (A) is the set of sums

$$a^0x_0 + \cdots + a^{n-1}x_{n-1},$$

where $a^i \in A$ and $x_i \in R$ and $n \in \omega$. In particular, n can be 0, and in this case the sum above is 0. Thus $(\varnothing) = \{0\}$, the trivial ideal.

When $A = \{a_0, a_1, \dots\}$, we may write (A) as $(a_0, a_1, \dots)$. In particular, $R = (1)$. Also the trivial ideal is (0), where 0 is the ring element, not the empty set; but then this notation is redundant: strictly we should be able to write the zero-ideal as $(\ )$.

A proper ideal I of R is maximal if and only if, for all x in $R \smallsetminus I$, we have

$$(I \cup \{x\}) = R,$$

that is,

$$1 \in (I \cup \{x\}),$$

that is, for some y in R,

$$1 \in xy + I.$$

Theorem 16. *Let I be an ideal of R. Then R/I is a field if and only if I is maximal.*

Proof. Again, R/I is nontrivial if and only if I is proper. Assuming I is proper we have that the following are equivalent.

- R/I is a field.
- If $x + I \neq I$, then for some y, $(x + I)(y + I) = 1 + I$.
- If $x \notin I$, then for some y, $1 \in xy + I$.
- I is maximal. □

Corollary. *Maximal ideals are prime.*

The converse is true in $\mathbb{Z}$.

8.2 Localizations

Throughout this section, the ring R will be nontrivial. It will then have a *quotient field* (or *field of fractions*) constructed as $\mathbb{Q}$ is constructed from $\mathbb{Z}$.

A **multiplicative subset** of a ring is just a subset that is closed under multiplication. More precisely, if S is a multiplicative subset of R, this means that for all finite subsets $\{a^k : k < n\}$ of S, the product $\prod_{k<n} a^k$

is also in S. In particular, $1 \in S$, since $\prod_{k<n} a^k$ is 1 when $n = 0$ (that is, the empty product is multiplicatively neutral element 1, just as the empty sum is 0).

For example, the set $R \smallsetminus I_0$ of non-zero non-zero-divisors of R is a multiplicative subset of R; more generally, so is the complement of any prime ideal; and so are $\{1\}$ and $R^\times$.

Lemma. *If S is a multiplicative subset of R, there is an equivalence-relation $\sim$ on $R \times S$ given by*

$$(a, b) \sim (x, y) \iff (ay - bx) \cdot s = 0 \text{ for some } s \text{ in } S. \tag{$*$}$$

If R is an integral domain and $0 \notin S$, or more generally if $S \cap I_0 = \varnothing$, then the equivalence-relation of the lemma is given by

$$(a, b) \sim (x, y) \iff ay - bx = 0;$$

but we shall be interested in the more general situation, especially in Chapter 10.5, and then a broader condition as in $(*)$ is needed.

The $\sim$-class of (a, b) is denoted by

$$\frac{a}{b}$$

or a/b. The set of these classes is denoted by

$$S^{-1}R;$$

it can be called the **localization** of R at S.

Theorem 17. *Let S be a multiplicative subset of R. The localization $S^{-1}R$ is a ring with respect to the usual operations:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad\qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

There is a homomorphism $x \mapsto x/1$ from R to $S^{-1}R$. This homomorphism is injective if and only if $S \cap I_0 = \varnothing$.

For the homomomorphism of the theorem, the condition of injectivity is not always met. It *is* met when $0 \notin S$ and also R is an integral domain (that is, I_0 is trivial). In particular, we have

Theorem 18. *A ring is an integral domain if and only if it a sub-ring of a field.*

Proof. For sufficiency, note that a zero-divisor of a sub-ring is a zero-divisor of the original ring.

To show necessity, we note that an integral domain R embeds in the ring $(R \smallsetminus \{0\})^{-1}R$, which is a field. $\square$

The field $(R \smallsetminus \{0\})^{-1}R$ in the proof is the **quotient field** (or **field of fractions**) of R (assuming R is a integral domain; otherwise this field is $(R \smallsetminus I_0)^{-1}R$).

Every substructure of a field is a ring. Therefore, by Theorem 11 on page 50, if T is field-theory, then $T_\forall$ is the theory of integral domains. The following is obvious, but should be noted:

Theorem 19. *If an integral domain embeds in a field, then the embedding factors through the fraction field of the integral domain. That is, if R is an integral domain embedding under ι in its fraction-field K, and R embeds in a field L under φ, then K embeds in L under a map ψ such that $\psi \circ \iota = \varphi$.* $\square$

See Figure 8.1. Suppose now K is a field, and L is a field of which K is

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\iota"'] & L \\ K \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

Figure 8.1: The universal property of the quotient field

a subfield, that is, $K \subseteq L$. In short, L/K is a field-extension. If $n \in \omega$, we may let $\boldsymbol{X}$ be an n-tuple $(X^0, \dots, X^{n-1})$ of indeterminates, so that we can form the **ring of polynomials** in $\boldsymbol{X}$ over K, denoted by

$$K[\boldsymbol{X}].$$

The fraction-field of this ring is denoted by

$$K(\boldsymbol{X});$$

it is the **field of rational functions** in $\boldsymbol{X}$ over K. Suppose now $\boldsymbol{a} \in L^n$. Then there is a function $f \mapsto f(\boldsymbol{a})$ (or $X^i \mapsto a^i$) from $K[\boldsymbol{X}]$ to L. The range of this function is denoted by

$$K[\boldsymbol{a}],$$

and the fraction-field of this ring is denoted by

$$K(\boldsymbol{a});$$

by the last theorem, we may consider this field as a subfield of L. In other words,

- $K[\boldsymbol{a}]$ is the smallest sub-ring of L that includes $K \cup \{a_0, \dots, a_{n-1}\}$;
- $K(\boldsymbol{a})$ is the smallest subfield of L that includes $K \cup \{a_0, \dots, a_{n-1}\}$.

Note well that the function $f \mapsto f(\boldsymbol{a})$ is not generally defined on all of $K(\boldsymbol{X})$, though it may be defined on a sub-ring of this field that strictly includes $K[\boldsymbol{X}]$. We shall consider this situation presently. Meanwhile, the kernel of the homomorphism $f \mapsto f(\boldsymbol{a})$ on $K[\boldsymbol{X}]$ is a prime ideal $\mathfrak{p}$, and then

$$K[\boldsymbol{a}] \cong K[\boldsymbol{X}]/\mathfrak{p}.$$

If that ideal is nontrivial, then $\boldsymbol{a}$ is said to be **algebraically dependent** over K, or simply **algebraic** over K in case $n = 1$.

Theorem 20. *If a is algebraic over K, then*

$$K[a] = K(a).$$

Thus prime ideals of $K[X]$ are maximal.

Proof. If $b_0 + b_1 \cdot a + \dots + b_n \cdot a^n = 0$, then

$$\frac{1}{a} = -\Bigl(\frac{b_1}{b_0} + \frac{b_2}{b_0} \cdot a + \dots + \frac{b_n}{b_0} \cdot a^{n-1}\Bigr). \qquad \square$$

Recall that Boolean rings also have the property that prime ideals are maximal (pages 37 and 67). This is not generally true for $K[\boldsymbol{X}]$. For example $K[X,Y]/(X-Y) \cong K[X]$, an integral domain that is not a field; so $(X-Y)$ is a non-maximal prime ideal of $K[X,Y]$.

In general, if S is a multiplicative subset of R, then, using the notation above, we can denote the localization $S^{-1}R$ also by

$$R[S^{-1}].$$

In case S is the complement of a prime ideal $\mathfrak{p}$ of R, then this localization is denoted also by

$$R_{\mathfrak{p}}.$$

Confusingly, this may called the **localization** of R at $\mathfrak{p}$, although in the earlier terminology it is the localization of R at the *complement* of $\mathfrak{p}$. If R is an integral domain, then its fraction-field is the localization $R_{\{0\}}$.

Suppose again L/K is a field-extension and $\boldsymbol{a} \in L^n$. If $\mathfrak{p}$ is the prime ideal of $K[\boldsymbol{X}]$ that is the kernel of $f \mapsto f(\boldsymbol{a})$, then $K[\boldsymbol{X}]_{\mathfrak{p}}$ is the largest sub-ring of $K(\boldsymbol{X})$ on which the homomorphism $f \mapsto f(\boldsymbol{a})$ is defined.

In general, as we noted, if $\mathfrak{p}$ is a prime ideal of R, then $R \setminus \mathfrak{p}$ is multiplicative. The converse is true, and more, in the following sense:

Theorem 21. *Let I be a proper ideal of R.*

1. *$R \setminus I$ is multiplicative if and only if I is prime.*
2. *$R \setminus I = R^{\times}$ if and only if I is the unique maximal ideal of R.* $\square$

A ring with a unique maximal ideal is called a **local ring.**

Theorem 22. *The localization of a ring at (the complement of) a prime ideal is a local ring, whose maximal ideal is generated by the image of that prime ideal.* $\square$

We can now refer to $R_{\mathfrak{p}}$ (where $\mathfrak{p}$ is prime) as the local ring of R at $\mathfrak{p}$. A reason for the terminology can be seen in algebraic geometry, to which we now turn.

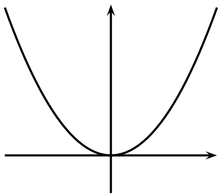

Figure 8.2: The zero-locus of $y - x^2$ in $\mathbb{R}$

8.3 Algebraic geometry

Again suppose K and L are fields such that $K \subseteq L$. For example, K might be $\mathbb{Q}$, and then L might be $\mathbb{C}$. Let $\boldsymbol{X}$ be $(X^0, \dots, X^{n-1})$ for some n in ω. Given a point $\boldsymbol{x}$ of L^n, we have looked at the homomorphism $f \mapsto f(\boldsymbol{x})$ from $K[\boldsymbol{X}]$ to L. 'Dually', an element f of $K[\boldsymbol{X}]$ determines a function $\boldsymbol{x} \mapsto f(\boldsymbol{x})$ from L^n to L. Often we are interested in the solution-set of the equation

$$f(\boldsymbol{x}) = 0.$$

Such equations are studied in school, at least when $L = \mathbb{R}$ and $n = 1$. We define

$$\mathrm{Z}_L(f) = \{\boldsymbol{x} \in L^n \colon f(\boldsymbol{x}) = 0\};$$

this is the **zero-locus** of f in L. See Figure 8.2. We may also want to look at more than one equation simultaneously, as for example in defining a straight line in $\mathbb{R}^3$. Accordingly, if $A \subseteq K[\boldsymbol{X}]$, we define

$$\mathrm{Z}_L(A) = \bigcap_{f \in A} \mathrm{Z}_L(f),$$

that is,

$$\mathrm{Z}_L(A) = \bigcap_{f \in A} \{\boldsymbol{x} \in L^n \colon f(\boldsymbol{x}) = 0\}; \tag{†}$$

this is the **zero-locus** of A in L. See Figure 8.3. (The definition should be compared with (∗) and (†) on page 24.) The function $A \mapsto \mathrm{Z}_L(A)$ is the **zero-locus map.** A course in 'analytic geometry' is a study of

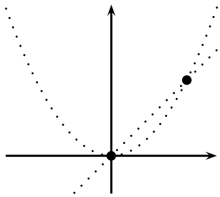

Figure 8.3: The zero-locus of $\{y - x^2, y - x\}$ in $\mathbb{R}$

zero-loci in $\mathbb{R}$, in case n is 2 or 3, where $K[\boldsymbol{X}]$ can be written as $K[X, Y]$ or $K[X, Y, Z]$.

If I is an ideal of an arbitrary ring R, we define

$$\sqrt{I} = \bigcup_{n \in \omega} \{x \in R \colon x^n \in I\};$$

this is the **radical** of I. (Note that the radical is indeed an ideal: if $f^n \in I$ and $g^m \in I$, then $(f + g)^{n+m-1} \in I$.) An ideal is a **radical ideal** if it is equal to its own radical.

Theorem 23. *For all subsets A of $K[\boldsymbol{X}]$,*

$$\mathrm{Z}_L(A) = \mathrm{Z}_L((A)) = \mathrm{Z}_L(\sqrt{(A)}).$$

Thus all zero-loci are zero-loci of radical ideals.

The zero-loci of the various subsets (or just ideals, or just radical ideals) of $K[\boldsymbol{X}]$ are also called **algebraic sets.** As the notation is supposed to recall, the definition of $\mathrm{Z}_L(A)$ depends on L. We intend to overcome this dependence. Meanwhile, we have the following.

Theorem 24. *The algebraic sets in L are the closed sets of a topology on L^n.*

Proof. What this means, and what we shall show, is that (1) the intersection of an arbitrary collection of algebraic sets is an algebraic set, and (2) the union of a finite collection of algebraic sets is an algebraic set. (In particular, since $\varnothing = \bigcup \varnothing$, this will be shown to be an algebraic set;

also, $\bigcap\varnothing$ is to be understood as L^n, so this too will be an algebraic set. See also page 70.)

The first point is obvious from the definition. Indeed, if $\mathcal{A}$ is a collection of ideals of $K[\boldsymbol{X}]$, then

$$\bigcap_{\mathfrak{a}\in\mathcal{A}} \mathrm{Z}_L(\mathfrak{a}) = \mathrm{Z}_L(\textstyle\sum\mathcal{A}),$$

where $\sum\mathcal{A}$ is the ideal generated by $\bigcup\mathcal{A}$. (So the ideal is $(\bigcup\mathcal{A})$; but it consists of finite sums of elements of $\bigcup\mathcal{A}$, and the notation $\sum\mathcal{A}$ is more suggestive of this.) In particular, as a special case we have

$$L^n = \mathrm{Z}_L(\{0\}).$$

For the second point, let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $K[\boldsymbol{X}]$. Then

$$\mathfrak{a}\subseteq\mathfrak{b} \implies \mathrm{Z}_L(\mathfrak{a})\supseteq\mathrm{Z}_L(\mathfrak{b}).$$

Consequently

$$\mathrm{Z}_L(\mathfrak{a}\cap\mathfrak{b})\supseteq\mathrm{Z}_L(\mathfrak{a})\cup\mathrm{Z}_L(\mathfrak{b}).$$

Conversely, suppose $\boldsymbol{x}\in\mathrm{Z}_L(\mathfrak{a}\cap\mathfrak{b})\smallsetminus\mathrm{Z}_L(\mathfrak{a})$. Then for some f in $\mathfrak{a}$ we have $f(\boldsymbol{x})\neq 0$. But then for all g in $\mathfrak{b}$ we have $f\cdot g\in\mathfrak{a}\cap\mathfrak{b}$, so $f(\boldsymbol{x})\cdot g(\boldsymbol{x})=0$, and hence $g(\boldsymbol{x})=0$ (since L is an integral domain). Thus $\boldsymbol{x}\in\mathrm{Z}_L(\mathfrak{b})$. Therefore

$$\mathrm{Z}_L(\mathfrak{a}\cap\mathfrak{b})=\mathrm{Z}_L(\mathfrak{a})\cup\mathrm{Z}_L(\mathfrak{b}). \tag{‡}$$

Finally

$$\mathrm{Z}_L((1))=\varnothing.$$

Thus finite unions of algebraic sets are algebraic. □

The zero-locus of an *arbitrary* intersection of radical ideals need not be the union of the zero-loci of the ideals. For example, if $K=\mathbb{Q}$ and

$$\mathfrak{a}_k=\Bigl(\prod_{i=1}^{k}(X-i)\Bigr)=\bigl((X-1)\cdots(X-k)\bigr),$$

then $Z_L(\mathfrak{a}_k) = \{1, \dots, k\}$, but $\bigcap_{k \in \mathbb{N}} \mathfrak{a}_k = \{0\}$, so

$$\bigcup_{k \in \mathbb{N}} Z_L(\mathfrak{a}_k) = \mathbb{N} \subset L = Z_L(\{0\}) = Z_L(\bigcap_{k \in \mathbb{N}} \mathfrak{a}_k).$$

The topology on L^n given by the theorem is called the **Zariski topology over** K. Then algebraic sets may be called **Zariski-closed over** K, or perhaps K**-closed.** All intersections of such sets are finite intersections, because of the following:

Theorem 25 (Hilbert Basis Theorem)**.** *For every n in ω, every ideal of the polynomial ring $K[X^0, \dots, X^{n-1}]$ is finitely generated.*

Proof. The claim implies, and is therefore equivalent to, an apparently stronger claim, namely that every ideal (A) of $K[X^0, \dots, X^{n-1}]$ is (A_0) for some finite subset A_0 of A. For, if $(A) = (f_0, \dots, f_{m-1})$, then each f_k is in (A^k) for some finite subset A^k of A; and then we can let $A_0 = \bigcup_{k<m} A^k$.

The claim as also equivalent to the claim that every sequence $(\mathfrak{a}_k : k \in \omega)$ of ideals such that

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$

—that is, every increasing chain of ideals (indexed by ω)—is eventually constant. For, the union of such a chain is an ideal $\mathfrak{b}$, and if this ideal is finitely generated, then it has a generating set whose elements all lie in some $\mathfrak{a}_\ell$, and then this ideal is $\mathfrak{b}$. Conversely (or inversely), if $\mathfrak{a}$ were not finitely generated, then for all subsets $\{f_k : k < \ell\}$ of $\mathfrak{a}$ we could find f_ℓ in $\mathfrak{a} \smallsetminus (f_k : k < \ell)$; thus we could form a strictly increasing chain $((f_k : k < \ell) : \ell \in \omega)$.

There is now also a fourth form of our claim: every *countably* generated ideal is finitely generated. We turn to proving the claim, in any convenient form.

The claim is trivially true when $n = 0$, since a field has only two ideals: the trivial ideal and the improper ideal (1).

The claim is still easy when $n = 1$, because $K[X]$ is a Euclidean domain. In particular, if f and g are in $K[X]$, we have an algorithm (the Euclidean algorithm) for finding their greatest common divisor—say h; and then $(f, g) = (h)$. Hence if $\mathfrak{a} = (f_k \colon k \in \omega)$, for each k in ω we can find g_k so that

$$(f_0, \dots, f_k) = (g_k).$$

In particular, g_{k+1} divides g_k. Then $\min\{\deg(g_k) \colon k \in \omega\} = \deg(g_\ell)$ for some ℓ, and consequently $\mathfrak{a} = (g_\ell)$.

When $n \geqslant 2$, we have not got the Euclidean algorithm; but we can come close enough if we use induction. Suppose then that the claim is true when $n = m$. Let $\mathfrak{a}$ be an ideal of $K[X^0, \dots, X^m]$. We form a sequence $(f_0, f_1, \dots)$ of elements of $\mathfrak{a}$ by recursion: Given $(f_k \colon k < \ell)$, we let f_ℓ, if it exists, be an element of $\mathfrak{a} \smallsetminus (f_k \colon k < \ell)$ of minimal degree as a polynomial in X^m over $K[X^0, \dots, X^{m-1}]$. Then these degrees form an increasing sequence:

$$\deg_{X^m}(f_0) \leqslant \deg_{X^m}(f_1) \leqslant \deg_{X^m}(f_2) \leqslant \dots$$

Let g_k be the leading coefficient of f_k (as a polynomial in X^m over $K[X^0, \dots, X^{m-1}]$; so $g_k \in K[X^0, \dots, X^{m-1}]$). By inductive hypothesis, for some ℓ,

$$(g_k \colon k \in \omega) = (g_k \colon k < \ell).$$

Then in particular

$$g_\ell \in (g_k \colon k < \ell).$$

Therefore $(f_k \colon k < \ell)$ has an element h whose leading coefficient (as a polynomial in X^m over $K[X^0, \dots, X^{m-1}]$) is g_ℓ; and the degree of this element can have any value that is at least the degree of $f_{\ell-1}$. In particular we may assume h has the degree of f_ℓ. But then $f_\ell - h$ has lower degree and belongs to $\mathfrak{a} \smallsetminus (f_k \colon k < \ell)$; that is, f_ℓ did not have minimal degree. Thus there *is* no f_ℓ; that is, $\mathfrak{a} = (f_k \colon k < \ell)$. □

A *singly* generated ideal is called **principal.** Then part of our proof of the theorem gives the following:

Porism. *Every ideal of $K[X]$ is principal.* □

Hence, although in the example above $\mathbb{N}$ is the union of zero-loci, it cannot itself be a zero-locus; for, every zero-locus of polynomials in one variable is the zero-locus of a single polynomial, so it is either the whole field L or a finite subset of this.

The theorem itself has the following:

Corollary. *Every decreasing chain of closed subsets of L^n is eventually constant.* □

It is not obvious that the corollary implies the theorem, since it is not obvious that $\mathfrak{a} \subset \mathfrak{b}$ implies $\mathrm{Z}_L(\mathfrak{a}) \supset \mathrm{Z}_L(\mathfrak{b})$, even if $\mathfrak{a}$ and $\mathfrak{b}$ are radical ideals. In fact, this can be *false.* For example, when $L = \mathbb{R}$, then (X^2+1) is a radical ideal whose zero-locus is the same as the zero-locus of (1), namely empty.

8.4 A Galois correspondence

For a 'dual' to the definition of zero-loci, if $A \subseteq L^n$, we define

$$\mathrm{I}_K(A) = \bigcap_{\boldsymbol{x} \in A} \{f \in K[\boldsymbol{X}] \colon f(\boldsymbol{x}) = 0\};$$

this is a radical ideal of $K[\boldsymbol{X}]$, and we may call it the **ideal of A over K.** The function $A \mapsto \mathrm{I}_K(A)$ is the **ideal map.** The definition does not involve the field L as such, but it does involve K, as the notation indicates.

Every subset A of L^n has a **Zariski closure** over K, namely the smallest K-closed subset of L^n that includes A. We can denote this closure by

$$\overline{A}^K.$$

Then we have easily:

Theorem 26. *For all subsets A of L^n,*

$$\overline{A}^K = \mathrm{Z}_L(\mathrm{I}_K(A)), \qquad \mathrm{I}_K(A) = \mathrm{I}_K(\overline{A}^K).$$

In the proof of Theorem 24 we used that the zero-locus map is inclusion-reversing. This is by the form of the definition. Since the definition of the ideal map has the same form, this function too is inclusion-reversing.

The last theorem theorem is entirely formal in this way. Indeed, the form of the definitions of the zero-locus and ideal maps is just the form used in establishing the original **Galois correspondence** in field theory. In that context, L is a normal and separable finite extension of K. We let G be the group of automorphisms of L over K, that is, $G = \mathrm{Aut}(L/K)$. For subgroups H of G, we define

$$\mathrm{Fix}(H) = \bigcap_{\sigma \in H} \{x \in L \colon x^{\sigma} = x\};$$

for intermediate extensions F of L/K, we have

$$\mathrm{Aut}(L/F) = \bigcap_{x \in F} \{\sigma \in G \colon x^{\sigma} = x\}.$$

If we abbreviate $\mathrm{Fix}(H)$ as H', and $\mathrm{Aut}(L/F)$ as F', then we always have

$$X \subseteq Y \implies X' \supseteq Y', \qquad\qquad X \subseteq X'',$$

so that (as a special case of the latter) $X' \subseteq X'''$, but also $X' \supseteq X'''$. Thus

$$X''' = X'.$$

Therefore we have a one-to-one correspondence $X \mapsto X'$ between the fields $\mathrm{Fix}(H)$ and the groups $\mathrm{Aut}(L/F)$; and this is entirely by the general form of the definitions. What makes the correspondence useful is the special features of the situation: that $|G| = [L : K]$, simply because L/K is normal, separable, and finite; and then $|\mathrm{Aut}(L/F)| = [L : F]$ for all intermediate extensions F of L/K; and therefore *every* intermediate field of L/K is $\mathrm{Fix}(H)$ for some H, and every subgroup of G is $\mathrm{Aut}(L/F)$ for some intermediate field F of L/K.

We return to the algebraic-geometric situation. For the formal reasons just discussed, we have a one-to-one **Galois correspondence** between the K-closed subsets of L^n and certain radical ideals of $K[\boldsymbol{X}]$, namely those of the form $\mathrm{I}_K(F)$ for some K-closed set F. See Figure 8.4. We

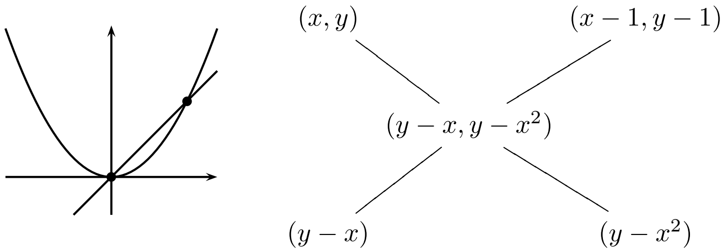

Figure 8.4: Algebraic-geometric Galois correspondence

may refer to those ideals as being themselves **L-closed.** Is this Galois correspondence of any use?

The L-closed ideals of $K[\boldsymbol{X}]$ are just those of the form $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$ for some radical ideal $\mathfrak{a}$ of $K[\boldsymbol{X}]$; and then

$$\mathfrak{a} \subseteq \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})). \tag{§}$$

This is an equation if and only if $\mathfrak{a}$ is L-closed. We noted in effect that if $L = \mathbb{R}$ then the radical ideal (X^2+1) is not L-closed:

$$(X^2+1) \subset (1) = \mathrm{I}_K(\mathrm{Z}_{\mathbb{R}}((X^2+1))).$$

However, as L grows larger, so does $\mathrm{Z}_L(\mathfrak{a})$; but then $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$ becomes smaller. In fact

$$(X^2+1) = \mathrm{I}_K(\mathrm{Z}_{\mathbb{C}}((X^2+1))).$$

We now are faced with the following:

Question 1. *For every radical ideal $\mathfrak{a}$ of $K[\boldsymbol{X}]$, is there an extension L of K large enough that*

$$\mathfrak{a} = \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))?$$

Question 2. *Is there an extension L of K large enough that for all ideals $\mathfrak{a}$ of $K[\boldsymbol{X}]$ and all extensions M of K,*

$$\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) \subseteq \mathrm{I}_K(\mathrm{Z}_M(\mathfrak{a}))?$$

Note well that $\mathfrak{a}$ and L are quantified in different orders in the two questions, as $\forall\mathfrak{a}\ \exists L$ and $\exists L\ \forall\mathfrak{a}$ respectively. This means a positive answer to Question 1 does not immediately give a positive answer to Question 2. We would first have to show that the different fields L corresponding to the different ideals $\mathfrak{a}$ are all included in one large field. This is true however, since the class of fields has the **joint embedding property:** If f_0 embeds K in L_0, and f_1 embeds K in L_1, then there is a field M, and there are embeddings g_i of the L_i (respectively) in M, such that $g_0 \circ f_0 = g_1 \circ f_1$. See Figure 8.5.

$$\begin{tikzcd}
 & M & \\
L_0 \arrow[ur, dash, "g_0"] & & L_1 \arrow[ul, dash, "g_1"'] \\
 & K \arrow[ul, dash, "f_0"] \arrow[ur, dash, "f_1"'] &
\end{tikzcd}$$

Figure 8.5: Joint embedding property of fields

By contrast, even if Question 2 has a positive answer, it is not at all clear that the answer to Question 1 must be positive. We settle Question 1 first in a special case.

Lemma. *For all* maximal *ideals* $\mathfrak{m}$ *of* $K[\boldsymbol{X}]$*, for all extensions* L *of* K *in which* $K[\boldsymbol{X}]/\mathfrak{m}$ *embeds over* K*,*

$$\mathfrak{m} = \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{m})).$$

Proof. As formulated here, the lemma almost proves itself. We just have to show $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{m}))$ is a proper ideal. But the image of $\boldsymbol{X}$ in $K[\boldsymbol{X}]/\mathfrak{m}$ is in the zero-locus of $\mathfrak{m}$. In particular, if L includes this field, then $\mathrm{Z}_L(\mathfrak{m})$ is not empty, so $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{m}))$ cannot be all of $K[\boldsymbol{X}]$. $\square$

This gives us another special case:

Theorem 27. *If $K[\boldsymbol{X}]^{\mathrm{alg}} \subseteq L$, for all ideals $\mathfrak{a}$ of $K[\boldsymbol{X}]$ such that $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$ is the improper ideal,*

$$\mathfrak{a} = \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})).$$

Proof. The claim is

$$\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) = (1) \implies \mathfrak{a} = (1).$$

We prove the contrapositive. If $\mathfrak{a}$ is a proper ideal of $K[\boldsymbol{X}]$, then it is included in some maximal ideal $\mathfrak{m}$. The field $K[\boldsymbol{X}]/\mathfrak{m}$ can be understood as an algebraic extension of $K(X^i\colon i \in I)$ for some subset I of n, so it embeds in $K(\boldsymbol{X})^{\mathrm{alg}}$. By the lemma then, since $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{m}))$ is a proper ideal, so is $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$. □

Note that if $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) \neq (1)$, then $\mathrm{Z}_L(\mathfrak{a}) \neq \varnothing$. Thus every proper ideal has non-empty zero-locus in a large-enough field. *Nullstellensatz* means zero-locus theorem:

Theorem 28 (Nullstellensatz)**.** *If $K[\boldsymbol{X}, Y]^{\mathrm{alg}} \subseteq L$, for all radical ideals $\mathfrak{a}$ of $K[\boldsymbol{X}]$,*

$$\mathfrak{a} = \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})).$$

Proof. Say $f \in \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$. If $\boldsymbol{x} \in \mathrm{Z}_L(\mathfrak{a})$, then $f(\boldsymbol{x}) = 0$. This shows $\mathrm{Z}_L(\mathfrak{a} \cup \{f - 1\}) = \varnothing$, so

$$\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a} \cup \{f - 1\})) = (1).$$

By the last theorem, $\mathfrak{a} \cup \{f - 1\}$ too must generate the improper ideal of $K[\boldsymbol{X}]$. We want to be able to conclude $f \in \mathfrak{a}$. To do so, we modify the argument so far. We have $f \cdot Y \in \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$, if we consider $\mathfrak{a}$ now as a subset of $K[\boldsymbol{X}, Y]$. As before, $\mathfrak{a} \cup \{f \cdot Y - 1\}$ must generate the improper ideal of $K[\boldsymbol{X}, Y]$. Now, by itself, $\mathfrak{a}$ generates the ideal of $K[\boldsymbol{X}, Y]$ whose elements are polynomials in Y with coefficients from $\mathfrak{a}$. Hence there is some such polynomial g, and there is some h in $K[\boldsymbol{X}, Y]$, such that

$$g + h \cdot (f \cdot Y - 1) = 1.$$

Substituting $1/f$ for Y, we get $g(1/f) = 1$; that is,

$$g_0 + g_1 \cdot \frac{1}{f} + \dots g_m \cdot \frac{1}{f^m} = 1$$

for some g_i in $\mathfrak{a}$, and hence

$$g_0 \cdot f^m + g_1 \cdot f^{m-1} + \dots + g_m = f^m.$$

This means $f^m \in \mathfrak{a}$. Assuming $\mathfrak{a}$ is radical, we have $f \in \mathfrak{a}$. Thus $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) \subseteq \mathfrak{a}$ and therefore $\mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) = \mathfrak{a}$. $\square$

We have now settled both Questions 1 and 2. This suggests that understanding algebraic sets can somehow be reduced to understanding radical ideals of $K[\boldsymbol{X}]$. Indeed, there is *some* extension L of K large enough that we have a Galois correspondence between the K-closed subsets of L^n and the radical ideals of $K[\boldsymbol{X}]$. It is not particularly important for what follows that this field L can be chosen as K^{alg}. Nonetheless, it is true:

Theorem 29 (Hilbert's Nullstellensatz, weak form)**.** *Every proper ideal of $K[\boldsymbol{X}]$ has a non-empty zero-locus in every extension of K^{alg}.*

Proof. In the lemma, by the Hilbert Basis Theorem, $\mathfrak{m}$ has the form $(f_0, \dots, f_\ell)$ for some f_i in $K[\boldsymbol{X}]$. Thus the formula

$$f_0 = 0 \wedge \dots \wedge f_\ell = 0$$

has a solution in $K[\boldsymbol{X}]/\mathfrak{m}$ and *a fortiori* in $(K[\boldsymbol{X}]/\mathfrak{m})^{\mathrm{alg}}$. The latter field is an *elementary* extension of K^{alg}, by the model-completeness of the theory of algebraically closed fields (Theorem 10 on page 49). Therefore the formula has a solution here too. Thus as long as $K^{\mathrm{alg}} \subseteq L$, we have $\mathrm{Z}_L(\mathfrak{m}) \neq 0$. $\square$

Now the proof of Theorem 28 gives:

Corollary (Hilbert's Nullstellensatz, strong form)**.** *For all radical ideals $\mathfrak{a}$ of $K[\boldsymbol{X}]$,*

$$\mathrm{I}_K(\mathrm{Z}_{K^{\mathrm{alg}}}(\mathfrak{a})) = \mathfrak{a}.$$

9 Finite fields

9.1 Ultraproducts of finite structures

Suppose a theory T has arbitrarily large finite models. Then there is a sequence $(\mathfrak{A}_m : m \in \omega)$ of finite models of T such that $|A_m| > m$ in each case. Consequently, the sentence

$$\exists(x_0, \dots, x_m) \bigwedge_{i<j<m} x_i \neq x_j$$

is true in each $\mathfrak{A}_n$ such that $m \leqslant n$. By Łoś's Theorem then, the sentence is true in every non-principal ultraproduct of the structures $\mathfrak{A}_i$. In particular, this ultraproduct is infinite. Moreover, every sentence that is true in each $\mathfrak{A}_i$ is true in the ultraproduct; that is, the ultraproduct is a model of the theory of the structures $\mathfrak{A}_i$. Thus the ultraproduct is an infinite model of the theory of finite models of T. Such a structure might be called a **pseudo-finite** model of T. We shall consider the case where T is the theory of fields.

9.2 Finite fields

Let us review the basic theorems about finite fields. Suppose K is a field. There is a homomorphism $1 \mapsto 1$ (or $k \mapsto k \cdot 1$) from $\mathbb{Z}$ to K. The kernel of this homomorphism is $n\mathbb{Z}$ for some *positive* n, called the **characteristic** of K, $\operatorname{char}(K)$. Since $\mathbb{Z}/n\mathbb{Z}$ must be an integral domain (by Theorem 18, p. 88), n is either 0 or prime. If $\operatorname{char}(K) = 0$, we may consider $\mathbb{Q}$ as a subfield of K; if $\operatorname{char}(K)$ is a prime p, we consider $\mathbb{Z}/p\mathbb{Z}$, denoted by $\mathbb{F}_p$, as a subfield of K. Respectively, $\mathbb{Q}$ or $\mathbb{F}_p$ is the **prime field** of K.

Let K be a finite field of characteristic p. Then K is a vector-space over $\mathbb{F}_p$ of some finite dimension m, so K has order p^m. The group $K^\times$ of units of K has order $p^m - 1$, so its every element is a root of $x^{p^m-1} - 1$. Then *every* element of K is a root of the polynomial

$$x^{p^m} - x.$$

Since the formal derivative of this is -1, it has no repeated roots. Thus its roots (in an algebraic closure ${\mathbb{F}_p}^{\mathrm{alg}}$ of $\mathbb{F}_p$ that includes K) are precisely the elements of K: we have

$$K = \{x \in {\mathbb{F}_p}^{\mathrm{alg}} \colon x^{p^m} = x\}.$$

Conversely, for all m in $\mathbb{N}$, since the map $x \mapsto x^{p^m}$ is an automorphism of ${\mathbb{F}_p}^{\mathrm{alg}}$, the set $\{x \in {\mathbb{F}_p}^{\mathrm{alg}} \colon x^{p^m} = x\}$ (namely the fixed field of the automorphism) is a subfield having order p^m. This then is the *unique* subfield of ${\mathbb{F}_p}^{\mathrm{alg}}$ of this order, and we can denote it by

$$\mathbb{F}_{p^m}.$$

The group ${\mathbb{F}_{p^m}}^{\times}$ of units of this field is cyclic. For again, it is a finite abelian group of order $p^m - 1$ and is therefore a direct product

$$\prod_{\ell \mid p^m-1} G_\ell,$$

where each G_ℓ is an ℓ-group (a group whose elements have orders that are powers of ℓ; here and elsewhere in this chapter, ℓ is, like p, a prime number). Since G_ℓ is finite, for some positive integer n, every element of G_ℓ is a solution of

$$x^{\ell^n} = 1.$$

But in a field, this equation has no more than ℓ^n solutions. Therefore, if n is minimal, G_ℓ must be cyclic of order ℓ^n. Then the product ${\mathbb{F}_{p^m}}^{\times}$ is itself cyclic, of order $p^m - 1$.

The collection of finite subfields of ${\mathbb{F}_p}^{\mathrm{alg}}$, ordered by inclusion, is isomorphic, under the map $\mathbb{F}_{p^m} \mapsto m$, to $\mathbb{N}$ as ordered by dividing. That is,

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n.$$

See Figure 9.1. Indeed, if $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is a vector-space over $\mathbb{F}_{p^m}$,

$$
\begin{tikzcd}[column sep=small]
\mathbb{F}_{p^8} \arrow[dr, dash] & & \mathbb{F}_{p^{12}} \arrow[dr, dash] & & \mathbb{F}_{p^{18}} \arrow[dr, dash] & & \mathbb{F}_{p^{27}} \\
& \mathbb{F}_{p^4} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{F}_{p^6} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{F}_{p^9} \arrow[ur, dash] & \\
& & \mathbb{F}_{p^2} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{F}_{p^3} \arrow[ur, dash] & & \\
& & & \mathbb{F}_p \arrow[ur, dash] & & &
\end{tikzcd}
$$

Figure 9.1: The lattice of finite fields of characteristic p

so its order is $(p^m)^k$ for some k, and then $n = mk$, so $m \mid n$. Conversely, if $m \mid n$, then

$$p^m - 1 \mid p^n - 1,$$

and therefore

$$x^{p^m-1} - 1 \mid x^{p^n-1} - 1,$$

so $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

Finally,

$$\mathbb{F}_p{}^{\mathrm{alg}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n} \tag{$*$}$$

(since every extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is certainly algebraic, while every finite algebraic extension of $\mathbb{F}_p$ is a finite field).

9.3 Galois groups

We have shown that for each prime p, for each m in $\mathbb{N}$, there is a subfield $\mathbb{F}_{p^m}$ of $\mathbb{F}_p{}^{\mathrm{alg}}$, and this subfield is generated by (in fact it consists of) the roots of the polynomial $x^{p^m} - x$, which is separable. Therefore the finite field-extension $\mathbb{F}_{p^m}/\mathbb{F}_p$ is normal and separable, that is, Galois.

The order of its group of automorphisms is $[\mathbb{F}_{p^m} : \mathbb{F}_p]$, that is, m. But the **Frobenius automorphism** of ${\mathbb{F}_p}^{\mathrm{alg}}$, namely $x \mapsto x^p$ or

$$\mathrm{Frob},$$

restricts to an automorphism of $\mathbb{F}_{p^m}$ of order m, since we have shown in effect

$$\mathrm{Fix}(\mathrm{Frob}^k) = \mathbb{F}_{p^k}.$$

Thus

$$\mathrm{Aut}(\mathbb{F}_{p^m}/\mathbb{F}_p) = \langle \mathrm{Frob} \restriction \mathbb{F}_{p^m} \rangle \cong \mathbb{Z}/m\mathbb{Z}.$$

For any field K, let us write

$$\mathrm{Gal}(K) = \mathrm{Aut}(K^{\mathrm{sep}}/K),$$

the *absolute Galois group* of K. We want to determine $\mathrm{Gal}(\mathbb{F}_p)$. Suppose $\sigma \in \mathrm{Gal}(\mathbb{F}_p)$. For every n in $\mathbb{N}$, we have

$$\sigma \restriction \mathbb{F}_{p^n} \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p),$$

and hence for some $\sigma(n)$ in $\mathbb{Z}$

$$\sigma \restriction \mathbb{F}_{p^n} = (\mathrm{Frob} \restriction \mathbb{F}_{p^n})^{\sigma(n)}.$$

All that matters here is the congruence-class of $\sigma(n)$ *modulo* n. Thus we have an injective map

$$\sigma \mapsto (\sigma(n) \colon n \in \mathbb{N})$$

from $\mathrm{Gal}(\mathbb{F}_p)$ to $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$. The map is not surjective, but if $m \mid n$, then since $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ we must have

$$\sigma(n) \equiv \sigma(m) \pmod{m}.$$

However, suppose an element $(\sigma(n) \colon n \in \mathbb{N})$ of $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ meets this condition. For any x in ${\mathbb{F}_p}^{\mathrm{alg}}$ we can define an element σ of $\mathrm{Gal}(\mathbb{F}_p)$ by

$$x^\sigma = x^{p^{\sigma(m)}},$$

where $x \in \mathbb{F}_{p^m}$. (Here x^σ is of course the image of x under σ.) This definition of x^σ is independent of the choice of m, since if also $x \in \mathbb{F}_{p^n}$, then

$$x \in \mathbb{F}_{p^{\gcd(m,n)}},$$

so

$$\sigma(m) \equiv \sigma(\gcd(m,n)) \equiv \sigma(n) \pmod{\gcd(m,n)}$$

and therefore

$$x^{p^{\sigma(m)}} = x^{p^{\sigma(\gcd(m,n))}} = x^{p^{\sigma(n)}}.$$

Thus

$$\mathrm{Gal}(\mathbb{F}_p) \cong \{(\sigma(n)\colon n \in \mathbb{N}) \in \prod_{i\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}\colon \bigwedge_{m|n} \pi^n_m(\sigma(n)) = \sigma(m)\}$$

where π^n_m is the quotient-map $x + n\mathbb{Z} \mapsto x + m\mathbb{Z}$ from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$.

In particular, $\mathrm{Gal}(\mathbb{F}_p)$ has a certain 'universal property' with respect to the system of groups $\mathbb{Z}/n\mathbb{Z}$ and homomorphisms π^n_m:

1. $\mathrm{Gal}(\mathbb{F}_p)$ is a group G from which there is a homomorphism h^G_n to $\mathbb{Z}/n\mathbb{Z}$ for every n in $\mathbb{N}$ such that, if $m \mid n$, then
$$\pi^n_m \circ h^G_n = h^G_m.$$
2. For every such group G, there is a unique homomorphism h from G to $\mathrm{Gal}(\mathbb{F}_p)$ such that, for each n in $\mathbb{N}$,
$$h^G_n = h^{\mathrm{Gal}(\mathbb{F}_p)}_n \circ h.$$

See Figure 9.2. Therefore $\mathrm{Gal}(\mathbb{F}_p)$ is called a **limit** of the given system of

$$\begin{tikzcd}
 & \mathrm{Gal}(\mathbb{F}_p) \arrow[ddl, "h^{\mathrm{Gal}(\mathbb{F}_p)}_n"'] \arrow[ddr, "h^{\mathrm{Gal}(\mathbb{F}_p)}_m"] & \\
 & G \arrow[u, "h"] \arrow[dl, "h^G_n"] \arrow[dr, "h^G_m"'] & \\
\mathbb{Z}/n\mathbb{Z} \arrow[rr, "\pi^n_m"'] & & \mathbb{Z}/m\mathbb{Z}
\end{tikzcd}$$

Figure 9.2: The universal property of $\mathrm{Gal}(\mathbb{F}_p)$

groups and homomorphisms. This is the category-theoretic sense of *limit* as given in, say, [9, p. 705] or [2]. Every set of groups, equipped with some homomorphisms, has a limit in this sense, though the limit might be empty.

The group $\mathrm{Gal}(\mathbb{F}_p)$ is called more precisely a **projective limit** or an **inverse limit** of the system of groups $\mathbb{Z}/n\mathbb{Z}$ with the quotient-maps, because any two of these groups are quotients of a third. This condition is not required for the existence of the limit.

We give the finite groups $\mathbb{Z}/n\mathbb{Z}$ the discrete topology, and their product the product topology. This product is compact by the Tychonoff Theorem (mentioned above on page 71). The image of $\mathrm{Gal}(\mathbb{F}_p)$ in this group is closed, so it too is compact: it is called a **pro-finite completion** of the system of finite cyclic groups.[1]

9.4 Pseudo-finite fields

Two examples of infinite models of the theory of finite fields are:

$$\prod_{p \text{ prime}} \mathbb{F}_p/M, \qquad\qquad \prod_{n\in\mathbb{N}} \mathbb{F}_{p^n}/M, \tag{†}$$

where in each case M is some non-principal maximal ideal. The first example has characteristic 0; the second, characteristic p.

By the 'Riemann Hypothesis for curves' as proved by Weil,[2] for every prime power q, for every curve C of genus g over $\mathbb{F}_q$, the number of $\mathbb{F}_q$-rational points of C is at least

$$1 + q - 2g\sqrt{q}.$$

In particular, if q is large enough, then C does have an $\mathbb{F}_q$-rational point.

A field K is called **pseudo-algebraically-closed** or **PAC** if every plane curve defined over K has a K-rational point. This condition entails that every absolutely irreducible variety over K has a K-rational point.[3]

[1] Perhaps one should talk about convergent sequences here. . .
[2] See for example [14, Ex. V.1.10, p. 368] or [12, Thm 3.14, p. 35].
[3] See [12, ch. 10, pp. 129–131].

The following are now true of every infinite model of the theory of finite fields:

1. It is perfect.
2. It has exactly one extension of each degree (in some algebraic closure).
3. It is pseudo-algebraically-closed.

This is not obvious, even given the results stated above; one must show that these conditions are *first-order,* that is, the structures that satisfy them make up an elementary class. By the definition of Ax [1], a field with the first two of these properties is **quasi-finite;** with all three of these properties, **pseudo-finite.** So every infinite model of the theory of finite fields is (quasi-finite and) pseudo-finite. Ax proves the converse. In particular, Ax proves that every pseudo-finite field is elementarily equivalent to a non-principal ultraproduct of finite fields, and indeed to one of the ultraproducts given above in (†). The method is as follows; here I use Ax [1] and also Chatzidakis [6].

For every field K, the field $\mathrm{Abs}(K)$ of **absolute numbers** of K consists of the algebraic elements of K (here algebraic means algebraic over the prime field). The following is [1, Prop. 7′, §10, p. 261].

Lemma. *For every field K of prime characteristic p, there is a maximal ideal M of $\prod_{n\in\mathbb{N}}\mathbb{F}_{p^n}$ such that*

$$\mathrm{Abs}(K)\cong\mathrm{Abs}(\prod_{n\in\mathbb{N}}\mathbb{F}_{p^n}/M).$$

Proof. Because ${\mathbb{F}_p}^{\mathrm{alg}}=\bigcup_{n\in\mathbb{N}}\mathbb{F}_{p^n}$ as in (∗) on page 104, we need only choose M so that, for all m in $\mathbb{N}$,

$$\mathbb{F}_{p^m}\subseteq K\iff\mathbb{F}_{p^m}\subseteq\prod_{n\in\mathbb{N}}\mathbb{F}_{p^n}/M.$$

For each m in $\mathbb{N}$, let f_m be an irreducible element of $\mathbb{F}_p[X]$ of degree m. Then each zero of f_m generates $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. So we want M to be such that

$$\mathbb{F}_{p^m}\subseteq K\iff f_m\text{ has a zero in }\prod_{n\in\mathbb{N}}\mathbb{F}_{p^n}/M.$$

Let F be the ultrafilter on $\mathbb{N}$ corresponding to M, that is,

$$F = \{\mathbb{N} \smallsetminus \operatorname{supp}(f) \colon f \in M\} = \bigl\{\{n \colon f_n = 0\} \colon f \in M\bigr\}.$$

Then

$$f_m \text{ has a zero in } \prod_{n\in\mathbb{N}} \mathbb{F}_{p^n}/M \iff \bigl\{n \colon f_m \text{ has a zero in } \mathbb{F}_{p^n}\bigr\} \in F.$$

Moreover,

$$f_m \text{ has a zero in } \mathbb{F}_{p^n} \iff m \mid n.$$

So, combining all of our equivalences, we want to choose F on $\mathbb{N}$ such that

$$\mathbb{F}_{p^m} \subseteq K \iff \{n \colon m \mid n\} \in F.$$

For each m in $\mathbb{N}$, the subset

$$\{k \colon k \mid m \ \ \& \ \ \mathbb{F}_{p^k} \subseteq K\}$$

of $\mathbb{N}$ is a sublattice of the lattice of factors of m with respect to divisibility: in particular, it contains the least common multiple of any two members. It also contains 1.[4] Therefore it has a maximum element, say $g(m)$. The arithmetic function g is multiplicative:

$$\gcd(m, n) = 1 \implies g(mn) = g(m) \cdot g(n).$$

Now let

$$b_m = \{x \colon \gcd(m, x) = g(m)\}.$$

Then the function $m \mapsto b_m$ is also multiplicative, in the sense that

$$\gcd(m, n) = 1 \implies b_{mn} = b_m \cap b_n. \tag{‡}$$

Indeed, suppose $\gcd(m, n) = 1$. Then or all x in $\mathbb{N}$,

$$\gcd(mn, x) = \gcd(m, x) \cdot \gcd(n, x),$$

and these factors are co-prime, being respectively factors of m and n. But also $g(mn) = g(m) \cdot g(n)$, and these factors are co-prime, being respectively factors of m and n. Therefore

$$\gcd(mn, x) = g(mn) \iff \gcd(m, x) = g(m) \ \ \& \ \ \gcd(n, x) = g(n).$$

[4] Thus it contains the least common multiple of every (finite) set of members, including the empty set.

So we have (‡). Moreover, we have also

$$m \leqslant n \implies b_{\ell^n} \subseteq b_{\ell^m}. \tag{§}$$

For, we have

$$b_{\ell^n} = \begin{cases} \{g(\ell^n) \cdot y \colon \ell \nmid y\}, & \text{if } g(\ell^n) < \ell^n, \\ \{\ell^n y \colon y \in \mathbb{N}\}, & \text{if } g(\ell^n) = \ell^n, \end{cases}$$

and also

$$m \leqslant n \implies g(\ell^m) = \min\bigl(\ell^m, g(\ell^n)\bigr).$$

Now we can just check that (§) holds in each of the three cases

$$g(\ell^n) = \ell^n, \qquad \ell^m < g(\ell^n) < \ell^n, \qquad g(\ell^n) < \ell^m.$$

So we have finally

$$b_m \cap b_n = b_{\operatorname{lcm}(m,n)}.$$

Thus, since each b_m is nonempty, the set of these generates a proper filter on $\mathbb{N}$. Let F be an ultrafilter on $\mathbb{N}$ that contains all of the sets b_m. We claim that this F is as desired. Indeed,

- if $\mathbb{F}_{p^m} \subseteq K$, so $g(m) = m$, then $b_m = \{mx \colon x \in \mathbb{N}\}$;
- if $\mathbb{F}_{p^m} \nsubseteq K$, so $g(m) < m$, then $b_m \cap \{mx \colon x \in \mathbb{N}\} = \varnothing$.

Consequently the following are equivalent:

$$\mathbb{F}_{p^m} \subseteq K,$$
$$\{mx \colon x \in \mathbb{N}\} \in F,$$
$$f_m \text{ has a root in } \prod_{n \in \mathbb{N}} \mathbb{F}_{p^n}/M,$$
$$\mathbb{F}_{p^m} \subseteq \prod_{n \in \mathbb{N}} \mathbb{F}_{p^n}/M. \qquad \square$$

The lemma has a companion [1, Prop. 7], namely that for every quasi-finite field K of characteristic 0, there is a maximal ideal M of $\prod_p \mathbb{F}_p$ such that

$$\operatorname{Abs}(K) = \operatorname{Abs}(\prod_p \mathbb{F}_p/M),$$

but the proof is more difficult. Since all fields of characteristic 0 are perfect, quasi-finiteness in this case just means having exactly one extension of each degree. In this case the field of absolute numbers has *at most* one extension of each degree. This is because, if α is algebraic over $\mathrm{Abs}(K)$, then α has the same degree over K that it has over $\mathrm{Abs}(K)$. For, the minimal polynomial of α over $\mathrm{Abs}(K)$ is a product

$$\prod_{i<n}(X-\alpha_i),$$

the α_i being the conjugates of α over $\mathrm{Abs}(K)$. The minimal polynomial over K is a factor of this; so its coefficients are polynomial functions of (some of) the conjugates of α over $\mathrm{Abs}(K)$. So the coefficients are algebraic (over $\mathrm{Abs}(K)$); therefore the already belong to $\mathrm{Abs}(K)$, by its definition.

We now want to prove [1, Thm 4, §8, p. 255], that if F and F' are pseudo-finite fields, then

$$\mathrm{Abs}(F) \cong \mathrm{Abs}(F') \implies F \equiv F'. \qquad (¶)$$

With this and the foregoing lemma, we shall have that every pseudo-finite field (at least in positive characteristic) is elementarily equivalent to an ultraproduct of finite fields.

To establish (¶), since $\mathrm{Abs}(F)$ is determined by $\mathrm{Th}(F)$, we can replace F and F' (respectively) by elementarily equivalent fields. In particular, we can replace them with ultrapowers with exponent ω; these ultrapowers are ω_1-saturated by Theorem 13 on page 81. Now take a countable elementary substructure F_0 of F; this exists by the downward Löwenheim–Skolem–Tarski Theorem, Theorem 2. One shows [6, 5.10, Lemme de plongement] that this embeds in F' under a monomorphism φ_0. Then F' has an elementary substructure F_0' that includes the image of F_0; and F_0' embeds in F under a monomorphism φ_0' that extends ${\varphi_0}^{-1}$. Continuing, we obtain isomorphic elementary substructures F_ω and F'_ω of F and F' respectively. See Figure 9.3. This establishes (¶).

$$
\begin{tikzcd}
F \arrow[d, dash] & F' \arrow[d, dash] \\
F_\omega \arrow[r, "\bigcup_{n\in\omega}\varphi_n"] \arrow[d, dash, dotted] & F'_\omega \arrow[d, dash, dotted] \\
F_1 \arrow[r, "\varphi_1"] \arrow[d, dash] & \varphi_1[F_1] \arrow[d, dash] \\
\varphi'_0[F'_0] \arrow[d, dash] & F'_0 \arrow[l, "\varphi'_0"'] \arrow[d, dash] \\
F_0 \arrow[r, "\varphi_0"] & \varphi_0[F_0]
\end{tikzcd}
$$

Figure 9.3: Isomorphisms of pseudo-finite fields

10 Schemes

Sources for the algebraic geometry of this chapter include Coombes [16] and Hartshorne [14]. The main point is to look at the *ultraproduct scheme* at the end; this work is based on the first of the three MSRI/Evans Hall Lectures, given at the University of California at Berkeley in the spring of 1998 by Angus Macintyre.[1]

10.1 The spectrum of a polynomial ring

In §8.4, letting f range over $K[\boldsymbol{X}]$ where $\boldsymbol{X} = (X^0, \dots, X^{n-1})$, and letting $\boldsymbol{x}$ range over L^n where $K \subseteq L$, we used the equation $f(\boldsymbol{x}) = 0$ to establish a Galois correspondence between the K-closed subsets of L^n and certain radical ideals of $K[\boldsymbol{X}]$. If L is large enough (by Theorem 28 on page 100)—more precisely, if L includes K^{alg} (by Theorem 29 and its corollary)—, then the Galois correspondence is between the K-closed subsets of L^n and (all of) the radical ideals of $K[\boldsymbol{X}]$. In particular, the correspondence is inclusion-reversing. Thus the set of radical ideals of $K[\boldsymbol{X}]$ encodes the topological structure of L^n for sufficiently large L, even for L including K^{alg}.

Suppose indeed $K^{\mathrm{alg}} \subseteq L$. We want more than the Galois correspondence. Suppose we are given a particular f in $K[\boldsymbol{X}]$. We are interested in its zero-locus, the K-closed set $\mathrm{Z}_L(f)$; and this now corresponds to $\mathrm{I}_K(\mathrm{Z}_L(f))$, which is $\sqrt{(f)}$. We should should like to have a way of picking out this ideal among all of the radical ideals of $K[\boldsymbol{X}]$, without having to refer to L^n. One way of doing this is simply to observe that $\sqrt{(f)}$ is the intersection of all radical ideals of $K[\boldsymbol{X}]$ that contain f. We shall develop an alternative that is in some ways more satisfying.

[1] These lectures used to be preserved on the MSRI website; but I could not find them there, the last time I looked.

If $\boldsymbol{a} \in L^n$, let us write $\mathrm{I}_K(\boldsymbol{a})$ for $\mathrm{I}_K(\{\boldsymbol{a}\})$. That is,

$$\mathrm{I}_K(\boldsymbol{a}) = \{f \in K[\boldsymbol{X}] \colon f(\boldsymbol{a}) = 0\}.$$

This is always a prime ideal. In particular, it is radical. Moreover, for every subset A of L^n,

$$\mathrm{I}_K(A) = \bigcap_{\boldsymbol{x} \in A} \mathrm{I}_K(\boldsymbol{x}).$$

In particular,

$$\mathrm{I}_K(\mathrm{Z}_L(f)) = \bigcap_{\boldsymbol{x} \in \mathrm{Z}_L(f)} \mathrm{I}_K(\boldsymbol{x}).$$

Thus $\mathrm{I}_K(\mathrm{Z}_L(f))$ is the intersection of *some* prime ideals of $K[\boldsymbol{X}]$ that include it. Therefore it is the intersection of *all* prime ideals of $K[\boldsymbol{X}]$ that include it.

Let us henceforth denote $K[\boldsymbol{X}]$ simply by R. Then the set of all prime ideals of $K[\boldsymbol{X}]$ is denoted by

$$\mathrm{Spec}(R).$$

(This will later be understood as part of the *spectrum* of R.) Usually $\mathfrak{p}$ will be understood as ranging over this set. We have the following.

Theorem 30. *For all radical ideals $\mathfrak{a}$ of R,*

$$\mathfrak{a} = \bigcap \{\mathfrak{p} \in \mathrm{Spec}(R) \colon \mathfrak{a} \subseteq \mathfrak{p}\}.$$

In particular, for all f in R,

$$\sqrt{(f)} = \bigcap \{\mathfrak{p} \in \mathrm{Spec}(R) \colon f \in \mathfrak{p}\}.$$

Proof. If L is large enough, then we now have

$$\mathfrak{a} = \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) = \bigcap \{\mathfrak{p} \colon \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a})) \subseteq \mathfrak{p}\} = \bigcap \{\mathfrak{p} \colon \mathfrak{a} \subseteq \mathfrak{p}\}.$$

Also, for all $\mathfrak{p}$ in $\mathrm{Spec}(R)$,

$$\sqrt{(f)} \subseteq \mathfrak{p} \iff f \in \mathfrak{p}. \qquad \square$$

This theorem is true for arbitrary rings R (see Theorem 34 below); but in the present case the work of proving it has already been done for the Nullstellensatz (Theorem 28).

In the theorem, the condition that $f \in \mathfrak{p}$ is equivalent to the condition that $f + \mathfrak{p} = 0$ in $R/\mathfrak{p}$. Moreover:

Theorem 31. *The homomorphism*

$$f \mapsto (f + \mathfrak{p} \colon \mathfrak{p} \in \operatorname{Spec}(R))$$

from R into the product

$$\prod_{\mathfrak{p} \in \operatorname{Spec}(R)} R/\mathfrak{p}$$

is an embedding.

Proof. The kernel of this map is $\bigcap \operatorname{Spec}(R)$, which is the trivial ideal since this ideal is prime. □

So if L is large enough, that is $L \supseteq K^{\mathrm{alg}}$, we have a one-to-one correspondence between:

- closed subsets $\mathrm{Z}_L(\mathfrak{a})$ of L^n;
- radical ideals $\mathfrak{a}$ of R;
- subsets $\{\mathfrak{p} \in \operatorname{Spec}(R) \colon \mathfrak{a} \subseteq \mathfrak{p}\}$ of $\operatorname{Spec}(R)$.

Moreover, suppose we write

$$(f_{\mathfrak{p}} \colon \mathfrak{p} \in \operatorname{Spec}(R)) = (f + \mathfrak{p} \colon \mathfrak{p} \in \operatorname{Spec}(R)).$$

That is, we consider this as a function $\mathfrak{p} \mapsto f_{\mathfrak{p}}$ on $\operatorname{Spec}(R)$, where $f_{\mathfrak{p}} \in R/\mathfrak{p}$. If $A \subseteq R$, then

$$\begin{aligned}\{\mathfrak{p} \in \operatorname{Spec}(R) \colon A \subseteq \mathfrak{p}\} &= \bigcap_{f \in A} \{\mathfrak{p} \in \operatorname{Spec}(R) \colon f \in \mathfrak{p}\} \\ &= \bigcap_{f \in A} \{\mathfrak{p} \in \operatorname{Spec}(R) \colon f_{\mathfrak{p}} = 0\}.\end{aligned}$$

This is a kind of zero-locus. If $f \in R$, we can define

$$\mathrm{Z}(f) = \{\mathfrak{p} \in \operatorname{Spec}(R) \colon f_{\mathfrak{p}} = 0\}$$

(with no subscript on the Z this time), and if $A \subseteq R$, we define

$$\mathrm{Z}(A) = \bigcap_{f \in A} \mathrm{Z}(f).$$

Just as in §8.3, by the same proofs, we have

$$\mathrm{Z}(A) = \mathrm{Z}(\surd(A)),$$

and these sets are the closed sets of a topology on $\mathrm{Spec}(R)$. In particular, to establish

$$\mathrm{Z}(\mathfrak{a}) \cup \mathrm{Z}(\mathfrak{b}) = \mathrm{Z}(\mathfrak{a} \cap \mathfrak{b})$$

corresponding to (‡) on page 93, we need that the functions $\mathfrak{p} \mapsto f_{\mathfrak{p}}$ on $\mathrm{Spec}(R)$ take values in integral domains; and this is the case, since $f_{\mathfrak{p}} \in R/\mathfrak{p}$.

The inverse image of the basic closed set $\mathrm{Z}(f)$ under $\boldsymbol{x} \mapsto \mathrm{I}_K(\boldsymbol{x})$ is just $\mathrm{Z}_L(f)$, since

$$\begin{aligned}\{\boldsymbol{x} \in L^n \colon \mathrm{I}_K(\boldsymbol{x}) \in \mathrm{Z}(f)\} &= \{\boldsymbol{x} \in L^n \colon f \in \mathrm{I}_K(\boldsymbol{x})\} \\ &= \{\boldsymbol{x} \in L^n \colon f(x) = 0\} \\ &= \mathrm{Z}_L(f).\end{aligned}$$

Thus the function $\boldsymbol{x} \mapsto \mathrm{I}_K(\boldsymbol{x})$ from L^n to $\mathrm{Spec}(R)$ is continuous, and moreover, every closed subset of L^n is the inverse image of a closed subset of $\mathrm{Spec}(R)$. The argument here uses nothing about L (except $L \supseteq K$, as always).

The function $\boldsymbol{x} \mapsto \mathrm{I}_K(\boldsymbol{x})$ injective on K^n, since if $\boldsymbol{a} \in K^n$ then

$$\mathrm{I}_K(\boldsymbol{a}) = (X^0 - a^0, \dots, X^{n-1} - a^{n-1}).$$

The map is not generally injective: if $n = 2$, $K = \mathbb{Q}$, and L is $\mathbb{R}$ or $\mathbb{C}$, then

$$\mathrm{I}_K((\pi, \pi)) = (X - Y) = \mathrm{I}_K((\mathrm{e}, \mathrm{e})).$$

The map is not generally surjective, even if L is large enough to ensure $\mathfrak{a} = \mathrm{I}_K(\mathrm{Z}_L(\mathfrak{a}))$ for radical $\mathfrak{a}$: If $L = \mathbb{Q}^{\mathrm{alg}}$, then $(X - Y)$ is not in the range. But still the map is surjective when L is large enough, not just ‘algebraically’, but also ‘transcendentally’:

Lemma. *If $K(\boldsymbol{X})^{\mathrm{alg}} \subseteq L$, then every prime ideal of $K[\boldsymbol{X}]$ is $\mathrm{I}_K(\boldsymbol{a})$ for some $\boldsymbol{a}$ in L^n.*

Proof. Suppose $\mathfrak{p}$ is a prime ideal of $K[\boldsymbol{X}]$. We can embed $K[\boldsymbol{X}]/\mathfrak{p}$ in L over K. Let a^i be the image of $X^i + \mathfrak{p}$ under this embedding. Then for all f in $K[\boldsymbol{X}]$ we have that $f(\boldsymbol{a})$ is the image of $f + \mathfrak{p}$. Therefore $\mathrm{I}_K(\boldsymbol{a}) = \mathfrak{p}$. □

Theorem 32. *If $K(\boldsymbol{X})^{\mathrm{alg}} \subseteq L$, then the map $\boldsymbol{x} \mapsto \mathrm{I}_K(\boldsymbol{x})$ from L^n to* $\mathrm{Spec}(R)$ *is surjective, continuous, closed, and open.*

Proof. The lemma gives surjectivity. Before that, we proved continuity. We also proved that closed subsets of L^n are inverse images of closed subsets of $\mathrm{Spec}(R)$. Taking complements, we have that open sets are inverse images of open sets. By surjectivity, a set is the inverse image only of its own image; so $\boldsymbol{x} \mapsto \mathrm{I}_K(\boldsymbol{x})$ must be closed and open. □

Thus, if $K(\boldsymbol{X})^{\mathrm{alg}}$, then L^n is nearly indistinguishable from $\mathrm{Spec}(R)$. However, as we observed with (π, π) and (e, e), the former space can contain distinct, but topologically indistinguishable, points: distinct points $\boldsymbol{a}$ and $\boldsymbol{b}$ such that every open set containing one of them contains the other. This just means $\mathrm{I}_K(\boldsymbol{a}) = \mathrm{I}_K(\boldsymbol{b})$, that is, the two points are sent to the same point of $\mathrm{Spec}(R)$. The $\mathrm{Spec}(R)$ itself is not Hausdorff, but it is 'T_0': if $\mathfrak{p}$ and $\mathfrak{q}$ are distinct points of $\mathrm{Spec}(R)$, then there is f belonging to $\mathfrak{p} \bigtriangleup \mathfrak{q}$, and this means $\mathrm{Z}(f)$ contains only one of the points.

It will be useful to have a notation for the *open* subsets of $\mathrm{Spec}(R)$. If $f \in R$, let us write

$$\mathrm{U}_f = \mathrm{Z}(f)^{\mathrm{c}} = \{\mathfrak{p} \in \mathrm{Spec}(R) \colon f \notin \mathfrak{p}\}.$$

If $A \subseteq R$, we let

$$\mathrm{U}_A = \mathrm{Z}(A)^{\mathrm{c}} = \bigcup_{f \in A} \mathrm{U}_f = \{\mathfrak{p} \in \mathrm{Spec}(R) \colon A \nsubseteq \mathfrak{p}\}.$$

These are the open subsets of $\mathrm{Spec}(R)$, and each of them is $\mathrm{U}_{\mathfrak{a}}$ for some radical ideal $\mathfrak{a}$ of R.

10.2 Regular functions

At the beginning of the last section, we considered the equation $f(\boldsymbol{x}) = 0$, where $f \in K[\boldsymbol{X}]$ and $\boldsymbol{x} \in L^n$. We have generally $f(\boldsymbol{x}) \in L$, that is, f is a function from L^n to L. There can be other such functions. An arbitrary function h from a subset S of L^n to L is **regular** (or more precisely *K-regular*) *at* a point $\boldsymbol{a}$ of S if there is a neighborhood U of $\boldsymbol{a}$ (in the Zariski topology over K, restricted to S) and there are elements f and g of $K[\boldsymbol{X}]$ such that, for all $\boldsymbol{x}$ in U,

$$h(\boldsymbol{x}) = \frac{f(\boldsymbol{x})}{g(\boldsymbol{x})}.$$

The function is **regular,** simply, if it is regular at all points of its domain. The only regular functions on L^n itself are the elements of $K[\boldsymbol{X}]$. However, let

$$S_0 = \mathrm{Z}_L(Y^2 - X^3) \smallsetminus \mathrm{Z}_L(X), \qquad S_1 = \mathrm{Z}_L(Y^2 - X^3) \smallsetminus \mathrm{Z}_L(Y).$$

These are open subsets of their union. On S_0 and S_1 respectively there are regular functions h_0 and h_1 given by

$$h_0(x, y) = \frac{y}{x^2}, \qquad h_1(x, y) = \frac{x}{y}.$$

These two functions agree on $S_0 \cap S_1$, since $y^2 = x^3$ for all (x, y) in that set (and even in $S_0 \cup S_1$). Thus $h_0 \cup h_1$ is a regular function h on $S_0 \cup S_1$. However, there are no f and g in $K[X, Y]$ such that, for all (x, y) in $S_0 \cup S_1$, $h(x, y) = f(x, y)/g(x, y)$.

In the example, $S_0 \cup S_1$ is an open subset of the closed subset $\mathrm{Z}_L(Y^2 - X^3)$ of L^2. For now, we shall look just at open subsets of the powers L^n themselves.

If $\mathfrak{p}$ is a prime ideal of $K[\boldsymbol{X}]$, and f and g in $K[\boldsymbol{X}]$ are such that $\boldsymbol{x} \mapsto f(\boldsymbol{x})/g(\boldsymbol{x})$ is well-defined (and therefore regular) on $L^n \smallsetminus \mathrm{Z}_L(\mathfrak{p})$, this means f/g is a well-defined element of the local ring $K[\boldsymbol{X}]_{\mathfrak{p}}$.

Now write $R = K[\boldsymbol{X}]$ as before, and let $\mathfrak{a}$ be an arbitrary radical ideal of R, so that $\mathrm{U}_{\mathfrak{a}}$ is an open subset of $\operatorname{Spec}(R)$. We define shall define a sub-ring, to be denoted by

$$\mathscr{O}(\mathrm{U}_{\mathfrak{a}}),$$

of the product[2]

$$\prod_{\mathfrak{p}\in \mathrm{U}_{\mathfrak{a}}} R_{\mathfrak{p}}.$$

See Figure 10.1. Elements of this product are functions on $\mathrm{U}_{\mathfrak{a}}$; so as

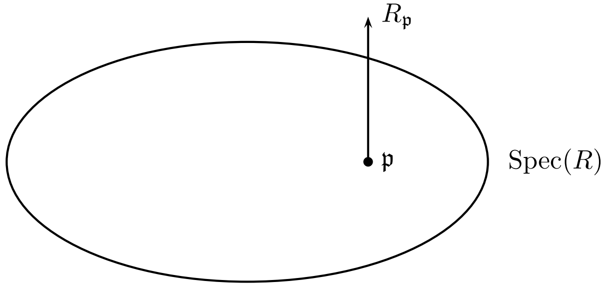

Figure 10.1: A stalk of a sheaf (see p. 121)

before we have a notion of being *regular:* An element h of the product is **regular** at a point $\mathfrak{p}$ of $\mathrm{U}_{\mathfrak{a}}$ if, for some open subset V of $\mathrm{U}_{\mathfrak{a}}$ that contains $\mathfrak{p}$, there are f and g in R such that, for all $\mathfrak{q}$ in V,

$$h_{\mathfrak{q}} = \frac{f}{g}.$$

Note that this requires $g \notin \mathfrak{q}$. The ring $\mathscr{O}(\mathrm{U}_{\mathfrak{a}})$ consists of the elements of $\prod_{\mathfrak{p}\in \mathrm{U}_{\mathfrak{a}}} R_{\mathfrak{p}}$ that are regular at all points of $\mathrm{U}_{\mathfrak{a}}$.

There is a simpler definition when $\mathfrak{a}$ is a principal ideal (g). In this case, one shows

$$\mathscr{O}(\mathrm{U}_{(g)}) \cong \{g^k \colon k \in \omega\}^{-1}R,$$

because the map $x/g^n \mapsto (x/g^n \colon \mathfrak{p} \in \mathrm{U}_{(g)})$ from this ring to $\mathscr{O}(\mathrm{U}_{(g)})$ is injective and surjective. See Hartshorne [14, Prop. II.2.2, p. 71].

[2]Note well that the factors of the product are the localizations $R_{\mathfrak{p}}$, rather than, say, the quotient-fields of the quotients $R/\mathfrak{p}$. However, in the other case that we shall be interested in, where R is itself a product of fields, then the integral domains $R/\mathfrak{p}$ will already be fields, which are isomorphic to the localizations $R_{\mathfrak{p}}$. See §10.5 below.

If U and V are open subsets of R such that $U \supseteq V$, then the restriction-map from $\prod_{\mathfrak{p}\in U} R_{\mathfrak{p}}$ to $\prod_{\mathfrak{p}\in V} R_{\mathfrak{p}}$ itself restricts to a map ρ_V^U from $\mathscr{O}(U)$ to $\mathscr{O}(V)$. If $h \in \mathscr{O}(U)$, we then write

$$\rho_V^U(h) = h \upharpoonright V.$$

The function $U \mapsto \mathscr{O}(U)$ on the collection of open subsets of R, together with these homomorphisms ρ_{UV}, is called a **pre-sheaf** of rings on $\operatorname{Spec}(R)$ because:

$$\mathscr{O}(\varnothing) = \{0\}, \qquad \rho_U^U = \mathrm{id}_U, \qquad \rho_W^U = \rho_W^V \circ \rho_V^U.$$

(The notation ρ_V^U implies $U \supseteq V$; so for the last equation we have $U \supseteq V \supseteq W$.) We now have a situation that is 'dual' (because the arrows are reversed) to that of the Galois group $\operatorname{Gal}(\mathbb{F}_p)$: see page 106. For all $\mathfrak{p}$ in $\operatorname{Spec}(R)$, $R_{\mathfrak{p}}$ has a certain 'universal property' with respect to the system of rings $\mathscr{O}(U)$ such that $\mathfrak{p} \in U$:

1. $R_{\mathfrak{p}}$ is a ring A to which there is a homomorphism h_A^U from $\mathscr{O}(U)$ for such that, if $U \supseteq V$, then

$$h_A^V \circ \rho_V^U = h_A^U.$$

2. For every such ring A, there is a unique homomorphism h to A from $R_{\mathfrak{p}}$ such that

$$h_A^U = h \circ h_{R_{\mathfrak{p}}}^U.$$

See Figure 10.2. Therefore $R_{\mathfrak{p}}$ is called a **co-limit** or **direct limit** of the given system of rings. This limit can be obtained as a quotient of the sum $\sum_{\mathfrak{p}\in U} \mathscr{O}(U)$ by the smallest ideal that contains, for each pair U and V such that $U \supset V$, every element x such that $x_V = \rho_V^U(x_U)$, and $x_W = 0$ if W is not U or V.

The pre-sheaf $U \mapsto \mathscr{O}(U)$ is further a **sheaf** of rings because it has two additional properties:

1. If $h \in \mathscr{O}(U)$, and $h \upharpoonright V = 0$ for all V in an open covering of U, then $h = 0$.
2. If there is h_V in $\mathscr{O}(V)$ for every V in an open covering of U, and

$$h_V \upharpoonright (V \cap W) = h_W \upharpoonright (V \cap W)$$

$$\begin{tikzcd}
 & R_{\mathfrak{p}} \arrow[d, "h"] & \\
 & A & \\
\mathscr{O}(V) \arrow[uur, "h^V_{R_{\mathfrak{p}}}"] \arrow[ur, "h^V_A"'] & & \mathscr{O}(U) \arrow[uul, "h^U_{R_{\mathfrak{p}}}"'] \arrow[ul, "h^U_A"] \arrow[ll, "\rho^U_V"]
\end{tikzcd}$$

Figure 10.2: The universal property of $R_{\mathfrak{p}}$

for all V and W in this open covering, then for some h in $\mathscr{O}(U)$, for each V in the open covering,

$$h_V = h \upharpoonright V.$$

The local ring $R_{\mathfrak{p}}$ is the **stalk** of the sheaf at $\mathfrak{p}$. In the fullest sense, the **spectrum** of R is $\mathrm{Spec}(R)$ as a topological space equipped with this sheaf. The sheaf is then the **structure sheaf** of the spectrum of R.

10.3 Generic points and irreducibility

This section is here for completeness, but will not be used later. Every point $\boldsymbol{a}$ of L^n is called a **generic point** of $\mathrm{Z}_L(\mathrm{I}_K(\boldsymbol{a}))$; more precisely, $\boldsymbol{a}$ is a generic point *over* K of $\mathrm{Z}_L(\mathrm{I}_K(\boldsymbol{a}))$. In the example on page 116, (π, π) and (e, e) are generic points of $\mathrm{Z}_L(X - Y)$ over $\mathbb{Q}$.

In any case, if for some radical ideal $\mathfrak{a}$, the algebraic set $\mathrm{Z}_L(\mathfrak{a})$ has a generic point, then $\mathfrak{a}$ must be prime. The converse may fail. For example, $\mathrm{Z}_L((X - Y))$ has no generic point if $L \subseteq \mathbb{Q}^{\mathrm{alg}}$. However, to Theorem 32, we have the following

Corollary. *If $K(\boldsymbol{X})^{\mathrm{alg}} \subseteq L$, then the zero-locus in L of every prime ideal has a generic point.*

A closed subset of L^n is called **irreducible** if it cannot be written as the union of two closed subsets, neither of which includes the other.

Theorem 33. *For all radical ideals $\mathfrak{a}$ of $K[\boldsymbol{X}]$, if $K^{\mathrm{alg}} \subseteq L$,*

$$\mathfrak{a} \textit{ is prime} \iff \mathrm{Z}_L(\mathfrak{a}) \textit{ is irreducible.}$$

Proof. If $\mathfrak{p}$ is prime, and $\mathrm{Z}_L(\mathfrak{p}) = \mathrm{Z}_L(\mathfrak{a}) \cup \mathrm{Z}_L(\mathfrak{b})$ for some radical ideals $\mathfrak{a}$ and $\mathfrak{b}$, then (by Hilbert's Nullstellensatz)

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

so we may assume $\mathfrak{p} = \mathfrak{a}$ and therefore $\mathrm{Z}_L(\mathfrak{a}) \supseteq \mathrm{Z}_L(\mathfrak{b})$.

Suppose conversely $\mathrm{Z}_L(\mathfrak{a})$ is irreducible, and $fg \in \mathfrak{a}$. Then

$$\mathrm{Z}_L(\mathfrak{a}) = \mathrm{Z}_L(\mathfrak{a} \cup \{f\}) \cup \mathrm{Z}_L(\mathfrak{a} \cup \{g\}),$$

so we may assume $\mathrm{Z}_L(\mathfrak{a}) = \mathrm{Z}_L(\mathfrak{a} \cup \{f\})$ and therefore (again by Hilbert's Nullstellensatz) $f \in \mathfrak{a}$. □

For example, L^n itself is irreducible, since the zero-ideal of $K[\boldsymbol{X}]$ is prime. Therefore the closure of every open subset is the whole space L^n. In any case, every closed set is the union of only finitely many irreducible closed sets: this is by the corollary to the Hilbert Basis Theorem (Theorem 25 on page 94). Hence every radical ideal of $K[\boldsymbol{X}]$ is the intersection of just finitely many elements of $\mathrm{Spec}(K[\boldsymbol{X}])$.

10.4 Affine schemes

The construction of the spectrum of $K[\boldsymbol{X}]$ can be carried out for any ring (that is, commutative unital ring). For an arbitrary ring R, we can still let $\mathrm{Spec}(R)$ be the set of prime ideals of R. Then every element f of R determines a function $\mathfrak{p} \mapsto f_{\mathfrak{p}}$ on $\mathrm{Spec}(R)$, where $f_{\mathfrak{p}}$ is the element $f + \mathfrak{p}$ of $R/\mathfrak{p}$. However, the corresponding map

$$f \mapsto (f_{\mathfrak{p}} \colon \mathfrak{p} \in \mathrm{Spec}(R)) \tag{$*$}$$

from R to $\prod_{\mathfrak{p} \in \mathrm{Spec}(R)} R/\mathfrak{p}$ need not be injective. For example, the kernel of this map contains $X + (X^2)$ when $R = K[X]/(X^2)$.

We do have the generalization of Theorem 30 on page 114:

Theorem 34. *For all subsets A of R,*

$$\sqrt{(A)} = \bigcap\{\mathfrak{p} \in \operatorname{Spec}(R) \colon A \subseteq \mathfrak{p}\}.$$

Proof. It is clear that the intersection includes $\sqrt{(A)}$. Now suppose $x \in R \smallsetminus \sqrt{(A)}$. Let $\mathfrak{b}$ be an ideal of R that is maximal with respect to including $\sqrt{(A)}$, but not containing any power of x. Say y and z are not in $\mathfrak{b}$. By maximality,

$$x \in \mathfrak{b} + (y), \qquad\qquad x \in \mathfrak{b} + (z),$$

and therefore

$$x^2 \in \mathfrak{b} + (yz),$$

so $yz \notin \mathfrak{b}$ (since $x^2 \notin \mathfrak{b}$). Thus $\mathfrak{b}$ is prime. □

Corollary. $\bigcap \operatorname{Spec}(R) = \sqrt{\{0\}}$.

In particular, the kernel of $f \mapsto (f_{\mathfrak{p}} \colon \mathfrak{p} \in \operatorname{Spec}(R))$ is $\sqrt{\{0\}}$. (Again this is non-trivial if, for example, $R = K[X]/(X^2)$.)

As before, we still obtain a Galois correspondence between certain subsets of R and of $\operatorname{Spec}(R)$. If $A \subseteq R$ and $B \subseteq \operatorname{Spec}(R)$, we define

$$\mathrm{Z}(A) = \bigcap_{f \in A}\{\mathfrak{p} \in \operatorname{Spec}(R) \colon f_{\mathfrak{p}} = 0\} = \{\mathfrak{p} \in \operatorname{Spec}(R) \colon A \subseteq \mathfrak{p}\},$$

$$\mathrm{I}(B) = \bigcap_{\mathfrak{p} \in B}\{f \in R \colon f_{\mathfrak{p}} = 0\} = \bigcap B.$$

As before,

$$\mathrm{Z}(A) = \mathrm{Z}(\sqrt{(A)}).$$

So the sets $\mathrm{Z}(A)$ (where $A \subseteq R$) are just the sets $\mathrm{Z}(\mathfrak{a})$ (where $\mathfrak{a}$ is a radical ideal of R). Moreover, by the last theorem, if $\mathfrak{a}$ and $\mathfrak{b}$ are distinct radical ideals, then $\mathrm{Z}(\mathfrak{a}) \neq \mathrm{Z}(\mathfrak{b})$. Thus we have:

Theorem 35 (Nullstellensatz)**.** *The functions $V \mapsto \mathrm{I}(V)$ and $\mathfrak{a} \mapsto \mathrm{Z}(\mathfrak{a})$ establish a one-to-one order-reversing correspondence between the radical ideals of R and certain subsets of* $\operatorname{Spec}(R)$*.* □

If $A \subseteq R$, we define

$$\mathrm{U}_A = \mathrm{Z}(A)^{\mathrm{c}} = \{\mathfrak{p} \in \operatorname{Spec}(R)\colon A \nsubseteq \mathfrak{p}\}.$$

Theorem 36. *The subsets* $\mathrm{U}_{\mathfrak{a}}$ *of* $\operatorname{Spec}(R)$ *are the open sets of a topology on* $\operatorname{Spec}(R)$.

Proof. Since the elements $\mathfrak{p}$ of $\operatorname{Spec}(R)$ are prime, we have

$$\mathfrak{ab} \subseteq \mathfrak{p} \iff \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p}$$

or rather

$$\mathfrak{ab} \nsubseteq \mathfrak{p} \iff \mathfrak{a} \nsubseteq \mathfrak{p} \ \& \ \mathfrak{b} \nsubseteq \mathfrak{p}.$$

Therefore

$$\mathrm{U}_{\mathfrak{a}} \cap \mathrm{U}_{\mathfrak{b}} = \mathrm{U}_{\mathfrak{ab}}\,.$$

Also, $\operatorname{Spec}(R) = \mathrm{U}_{(1)}$. Finally, if $\mathcal{A}$ is a collection of ideals of $\operatorname{Spec}(R)$, then

$$\bigcup_{\mathfrak{a} \in \mathcal{A}} \mathrm{U}_{\mathfrak{a}} = \mathrm{U}_{\sum \mathcal{A}}\,.$$

(As a special case, $\varnothing = \mathrm{U}_{\{0\}}$.) □

The topology just given is of course the **Zariski topology.** Just as before, we obtain the sheaf $U \mapsto \mathscr{O}(U)$ of rings on $\operatorname{Spec}(R)$, with stalks $R_{\mathfrak{p}}$. Continuing the example on page 118, we may let

$$R = K[X, Y]/(Y^2 - X^3).$$

Let x and y be the images of X and Y respectively in R. Then

$$\mathrm{U}_{(x,y)} = \mathrm{U}_x \cup \mathrm{U}_y,$$

and

$$\mathfrak{p} \in \mathrm{U}_x \implies \frac{y}{x^2} \in R_{\mathfrak{p}}, \qquad \mathfrak{p} \in \mathrm{U}_y \implies \frac{x}{y} \in R_{\mathfrak{p}},$$

and if $\mathfrak{p} \in \mathrm{U}_x \cap \mathrm{U}_y$, then y/x^2 and x/y are the same element of $R_{\mathfrak{p}}$. Thus we obtain an element of $\mathscr{O}(\mathrm{U}_{(x,y)})$.

The spectrum of a ring is called an **affine scheme.** One point of introducing this terminology is that a *scheme,* simply, is a topological space with a sheaf of rings such that such that every point of the space has a neighborhood that, with the restriction of the sheaf to it, is an affine scheme. However, we shall not look at schemes in general. In fact we shall look at just one affine scheme whose underlying ring is not a polynomial ring.

10.5 Regular rings (in the sense of von Neumann)

Again R is an arbitrary ring (commutive and unital as always), and $\mathfrak{p}$ is a prime ideal. We have worked with both the quotient $R/\mathfrak{p}$ and the localization $R_\mathfrak{p}$. Are these two rings ever isomorphic? More precisely, is there ever a well-defined isomorphism

$$x + \mathfrak{p} \mapsto \frac{x}{1}$$

from $R/\mathfrak{p}$ to $R_\mathfrak{p}$?

- There is, if R is already a field.
- There is not, if R is an integral domain that is not a field; for in this case the homomorphism from R to $R_\mathfrak{p}$ is a proper embedding.

The homomorphism $x + \mathfrak{p} \mapsto x/1$ is well-defined if and only if

$$x \in \mathfrak{p} \implies \frac{x}{1} = 0,$$

that is, if $x \in \mathfrak{p}$, then $x \cdot s = 0$ for some s in $R \smallsetminus \mathfrak{p}$. In particular, we must have $\mathfrak{p} \subseteq I_0$ (the set $\{0\} \cup \{\text{zero-divisors}\}$, defined on page 84).

The homomorphism $x + \mathfrak{p} \mapsto x/1$ is injective if and only if

$$\frac{x}{1} = 0 \implies x \in \mathfrak{p},$$

that is, if $x \cdot s = 0$ for some s in $R \smallsetminus \mathfrak{p}$, then $x \in \mathfrak{p}$. Since $\mathfrak{p}$ contains 0 and is prime, the homomorphism is automatically injective (if it is well-defined).

The homomorphism is surjective if and only if, for all x/y in $R_{\mathfrak{p}}$, there is z in R and there is s in $R \smallsetminus \mathfrak{p}$ such that $(x - yz) \cdot s = 0$, that is,

$$xs = yzs.$$

It is enough if, for some z,

$$xy = yzy.$$

It is then enough if z has the form xy^* for some y^*. Then it is enough if

$$y = yy^*y.$$

A ring in which for every element y there is y^* with this property is called a **regular ring** (in the sense of von Neumann).[3]

A Boolean ring is a regular ring: just let x^* be 1 or x (or anything in between). We have shown in effect that every such ring embeds in a power ${\mathbb{F}_2}^{\Omega}$ of the two-element field. More generally, if $(K_i : i \in \Omega)$ is an indexed family of arbitrary fields, then the product

$$\prod_{i\in\Omega} K_i$$

is a regular ring. Indeed, if $x \in R$, we can define x^* by

$$x^*{}_i = \begin{cases} {x_i}^{-1}, & \text{if } x_i \neq 0, \\ 0, & \text{if } x_i = 0. \end{cases}$$

Then indeed $xx^*x = x$. We shall see presently that all regular rings embed in such products.

Theorem 37. *Let R be a regular ring, and let $\mathfrak{p}$ be a prime ideal, then the map*

$$x + \mathfrak{p} \mapsto \frac{x}{1}$$

is a well-defined isomorphism from $R/\mathfrak{p}$ to $R_{\mathfrak{p}}$. Moreover, each of these rings is a field. Thus $\mathfrak{p}$ is maximal.

[3]The definition applies to non-commutative rings as well.

Proof. For all x in R, we have $x = xx^*x$, that is,

$$x \cdot (1 - xx^*) = 0.$$

Since $\mathfrak{p}$ is a proper ideal, we have

$$x \in \mathfrak{p} \iff 1 - xx^* \in R \smallsetminus \mathfrak{p}.$$

Thus, as above, the homomorphism is well-defined. It is then injective and surjective, as we said. In particular, in $\mathbb{R}_{\mathfrak{p}}$,

$$\frac{x}{1} \neq 0 \iff x \in R \smallsetminus \mathfrak{p} \iff \frac{1}{x} \text{ is well-defined;}$$

so $R_{\mathfrak{p}}$ is a field. □

The map in $(*)$ on page 122 is now an embedding into a product of fields:

Corollary. *Every regular ring R embeds in the product*

$$\prod_{\mathfrak{p} \in \operatorname{Spec}(R)} R/\mathfrak{p}$$

(which is a product of fields) under the map

$$f \mapsto (f + \mathfrak{p} : p \in \operatorname{Spec}(R)).$$

Proof. We need only note that the given map is injective, which it is because all ideals of R are radical, so that

$$\bigcap \operatorname{Spec}(R) = \sqrt{\{0\}} = \{0\}.$$ □

10.6 The ultraproduct scheme

Now let R be the product $\prod_{i \in \Omega} K_i$ of fields as above. As $\mathfrak{p}$ ranges over $\operatorname{Spec}(R)$, the quotients $R/\mathfrak{p}$ are just the possible ultraproducts of the fields K_i. We want to investigate how these arise from the structure sheaf of the spectrum of R. So, letting $\mathfrak{a}$ be an ideal of R, we want to understand $\mathscr{O}(\mathrm{U}_{\mathfrak{a}})$.

We can identify $\operatorname{Spec}(R)$ with $\operatorname{Spec}(\mathscr{P}(\Omega))$, and more generally, we can identify ideals of R with ideals of $\mathscr{P}(\Omega)$. Because $R_{\mathfrak{p}} \cong R/\mathfrak{p}$, we may assume
$$\mathscr{O}(\mathrm{U}_{\mathfrak{a}}) \subseteq \prod_{\mathfrak{p}\in\mathrm{U}_{\mathfrak{a}}} R/\mathfrak{p}.$$
Here we may treat $\mathfrak{a}$ as an ideal of $\mathscr{P}(\Omega)$, so $\mathrm{U}_{\mathfrak{a}}$ can be thought of as an open subset of $\operatorname{Spec}(\mathscr{P}(\Omega))$. Then, in the product $\prod_{\mathfrak{p}\in\mathrm{U}_{\mathfrak{a}}} R/\mathfrak{p}$, the index $\mathfrak{p}$ ranges over this open subset, but in the quotient $R/\mathfrak{p}$, the index returns to being the corresponding ideal of R.

Let $s \in \prod_{\mathfrak{p}\in\mathrm{U}_{\mathfrak{a}}} R/\mathfrak{p}$. Every *principal* ideal in $\mathrm{U}_{\mathfrak{a}}$ is $(\Omega \smallsetminus \{i\})$ for some i in Ω. In this case we have $\mathfrak{a} \nsubseteq (\Omega \smallsetminus \{i\})$, that is,
$$i \in \bigcup \mathfrak{a}.$$
Let us denote $(\Omega \smallsetminus \{i\})$ by $\mathfrak{p}(i)$. There is only one prime ideal of $\mathscr{P}(\Omega)$ that does not contain $\{i\}$, namely $\mathfrak{p}(i)$. Thus
$$\mathrm{U}_{\{i\}} = \{\mathfrak{p}(i)\}.$$
In particular, s is automatically regular at $\mathfrak{p}(i)$. We want to understand when s is regular at not-principal ideals.

Still considering also the principal ideals, we have
$$R/\mathfrak{p}(i) \cong K_i.$$
Let $s_{\mathfrak{p}(i)}$ be sent to s_i under this isomorphism, so whenever x in R is such that $x_i = s_i$, we have
$$s_{\mathfrak{p}(i)} = x + \mathfrak{p}(i).$$
By definition, we have $s \in \mathscr{O}(\mathrm{U}_{\mathfrak{a}})$ if and only if, for all $\mathfrak{p}$ in $\mathrm{U}_{\mathfrak{a}}$, for some subset $\mathrm{U}_{\mathfrak{b}}$ of $\mathfrak{a}$ such that $\mathfrak{b} \nsubseteq \mathfrak{p}$, for some x in R, for all $\mathfrak{q}$ in $\mathrm{U}_{\mathfrak{b}}$,
$$s_{\mathfrak{q}} = x + \mathfrak{q}.$$
We may assume $\mathfrak{b}$ is a principal ideal (A), where $A \in \mathfrak{a} \smallsetminus \mathfrak{p}$. If $\mathfrak{q}$ in U_A here is the principal ideal $\mathfrak{p}(j)$, so that $j \in A$, we must have $x_j = s_j$.

More generally, $\mathfrak{q} \in \mathrm{U}_A$ means $A \notin \mathfrak{q}$, so A is $\mathfrak{q}$-large, and hence for all x in R, $x + \mathfrak{q}$ is determined by $(x_i : i \in A)$. Thus we may assume

$$x = (s_i : i \in \Omega).$$

This establishes that $\mathscr{O}(\mathrm{U}_\mathfrak{a})$ is the image of R in $\prod_{\mathfrak{p} \in \mathrm{U}_\mathfrak{a}} R/\mathfrak{p}$:

$$\mathscr{O}(\mathrm{U}_\mathfrak{a}) = \{(x + \mathfrak{p} : \mathfrak{p} \in \mathrm{U}_\mathfrak{a}) : x \in R\}.$$

In particular, $\mathscr{O}(\mathrm{U}_\mathfrak{a})$ is a quotient of R, that is, a reduced product of the K_i. More precisely,

$$\mathscr{O}(\mathrm{U}_\mathfrak{a}) \cong R/\mathfrak{b},$$

where

$$\mathfrak{b} = \bigcap_{\mathfrak{p} \in \mathrm{U}_\mathfrak{a}} \mathfrak{p} = \bigcap_{\mathfrak{a} \nsubseteq \mathfrak{p}} \mathfrak{p}.$$

It follows that

$$\mathscr{O}(\mathrm{U}_\mathfrak{a}) \cong \prod_{i \in \bigcup \mathfrak{a}} K_i. \tag{$\dagger$}$$

We can see this in two ways. For example, if $\mathfrak{p} \in \mathrm{U}_\mathfrak{a}$, so that $\mathfrak{a} \nsubseteq \mathfrak{p}$, then $\bigcup \mathfrak{a} \notin \mathfrak{p}$, that is, $\bigcup \mathfrak{a}$ is $\mathfrak{p}$-large. Therefore the image of x in $\mathscr{O}(\mathrm{U}_\mathfrak{a})$ depends only on $(x_i : i \in \bigcup \mathfrak{a})$. This shows that $\mathscr{O}(\mathrm{U}_\mathfrak{a})$ is a quotient of $\prod_{i \in \bigcup \mathfrak{a}} K_i$.

It is moreover the quotient by the trivial ideal. For, if $i \in \bigcup \mathfrak{a}$, then $\mathfrak{p}(i) \in \mathrm{U}_\mathfrak{a}$, so that $x + \mathfrak{p}(i)$ depends only on x_i, that is,

$$x + \mathfrak{p}(i) = 0 \iff x_i = 0.$$

This gives us ($\dagger$).

Note that possibly $\bigcup \mathfrak{a} \notin \mathfrak{p}$, although $\mathfrak{a} \subseteq \mathfrak{p}$. Such is the case when $\mathfrak{p}$ is non-principal, but $\mathfrak{a}$ is the ideal of finite sets. However, we always have

$$\bigcup \mathfrak{a} \notin \mathfrak{p} \implies (\bigcup \mathfrak{a}) \nsubseteq \mathfrak{p}.$$

Another way to establish ($\dagger$) is to show

$$\bigcap_{\mathfrak{a} \nsubseteq \mathfrak{p}} \mathfrak{p} = (\Omega \smallsetminus \bigcup \mathfrak{a}).$$

If $X \subseteq \Omega \smallsetminus \bigcup \mathfrak{a}$, and $\mathfrak{a} \nsubseteq \mathfrak{p}$, then $\bigcup \mathfrak{a} \notin \mathfrak{p}$, so $\Omega \smallsetminus \bigcup \mathfrak{a} \in \mathfrak{p}$, and therefore $X \in \mathfrak{p}$. Inversely, if $X \nsubseteq \Omega \smallsetminus \bigcup \mathfrak{a}$, then $X \cap \bigcup \mathfrak{a}$ has an element i, so that $X \notin \mathfrak{p}(i)$ and $\mathfrak{a} \nsubseteq \mathfrak{p}(i)$.

Because the stalk $R_{\mathfrak{p}}$ is always a direct limit of those $\mathscr{O}(U)$ such that $\mathfrak{p} \in U$, we have in the present situation that the ultraproduct $\prod_{i \in \Omega} K_i/\mathfrak{p}$ is a direct limit of those products $\prod_{i \in A} K_i$ such that $A \notin \mathfrak{p}$. Symbolically,

$$\prod_{i \in \Omega} K_i/\mathfrak{p} = \varinjlim \Bigl\{ \prod_{i \in A} K_i \colon A \notin \mathfrak{p} \Bigr\}.$$

Equivalently, the ultraproduct is the direct limit of those $R/\mathfrak{a}$ such that $\mathfrak{a}$ is a principal ideal included in $\mathfrak{p}$:

$$\prod_{i \in \Omega} K_i/\mathfrak{p} = \varinjlim \Bigl\{ \prod_{i \in \Omega} K_i/(B) \colon B \in \mathfrak{p} \Bigr\}.$$

Bibliography

[1] James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR MR0229613 (37 #5187)

[2] Michael Barr and Charles Wells, *Category theory for computing science*, Prentice Hall International Series in Computer Science, Prentice Hall International, New York, 1990. MR MR1094561 (92g:18001)

[3] J. L. Bell and A. B. Slomson, *Models and ultraproducts: An introduction*, North-Holland Publishing Co., Amsterdam, 1969, reissued by Dover, 2006. MR MR0269486 (42 #4381)

[4] Alexandre Borovik and Mikhael Katz, *Inevitability of infinitesimals*, `http://manchester.academia.edu/AlexandreBorovik/Papers/305871/Inevitability_of_infinitesimals`, accessed July 18, 2012.

[5] C. C. Chang and H. J. Keisler, *Model theory*, third ed., Studies in Logic and the Foundations of Mathematics, vol. 73, North-Holland Publishing Co., Amsterdam, 1990. MR 91c:03026

[6] Zoé Chatzidakis, *Théorie de modèles des corps finis et pseudo-finis*, Prépublications de l'Equipe de Logique, Université Paris VII, Octobre 1996, `http://www.logique.jussieu.fr/~zoe/`.

[7] Alonzo Church, *Introduction to mathematical logic. Vol. I*, Princeton University Press, Princeton, N. J., 1956. MR 18,631a

[8] Apostolos Doxiadis and Christos H. Papadimitriou, *Logicomix*, Bloomsbury, London, 2009.

[9] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 97a:13001

[10] T. Frayne, A. C. Morel, and D. S. Scott, *Reduced direct products*, Fund. Math. **51** (1962/1963), 195–228. MR 0142459 (26 #28)

[11] ______, *Correction to the paper "Reduced direct products"*, Fund. Math. **53** (1963), 117. MR 0154807 (27 #4751)

[12] Michael D. Fried and Moshe Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 11, Springer-Verlag, Berlin, 1986. MR 89b:12010

[13] Kurt Gödel, *The completeness of the axioms of the functional calculus of logic (1930a)*, From Frege to Gödel (Jean van Heijenoort, ed.), Harvard University Press, 1976, pp. 582–91.

[14] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR MR0463157 (57 #3116)

[15] Wilfrid Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications, vol. 42, Cambridge University Press, Cambridge, 1993. MR 94e:03002

[16] howpublished=`http://odin.mdacc.tmc.edu/~krcoombes/agathos/contents.html` note=accessed August 6, 2012 Kevin R. Coombes, title=AGATHOS: Algebraic Geometry: A Total Hypertext Online System.

[17] Kenneth Kunen, *Set theory*, Studies in Logic and the Foundations of Mathematics, vol. 102, North-Holland Publishing Co., Amsterdam, 1983, An introduction to independence proofs, Reprint of the 1980 original. MR 85e:03003

[18] Serge Lang, *Algebra*, third ed., Addison-Wesley, Reading, Massachusetts, 1993, reprinted with corrections, 1997.

[19] Jerzy Łoś, *Quelques remarques, théorèmes et problèmes sur les classes définissables d'algèbres*, Mathematical interpretation of formal systems, North-Holland Publishing Co., Amsterdam, 1955, pp. 98–113. MR MR0075156 (17,700d)

[20] Leopold Löwenheim, *On possibilities in the calculus of relatives (1915)*, From Frege to Gödel (Jean van Heijenoort, ed.), Harvard University Press, 1976, pp. 228–251.

[21] Emil L. Post, *Introduction to a general theory of elementary propositions*, Amer. J. Math. **43** (1921), no. 3, 163–185.

[22] Thoralf Skolem, *Logico-combinatorial investigations in the satisfiability or provability of mathematical propositions: A simplified proof of a theorem by L. Löwenheim and generalizations of the theorem (1920)*, From Frege to Gödel (Jean van Heijenoort, ed.), Harvard University Press, 1976, pp. 252–63.

[23] M. H. Stone, *The theory of representations for Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), no. 1, 37–111. MR MR1501865

[24] Alfred North Whitehead and Bertrand Russell, *Principia mathematica*, vol. I, University Press, Cambridge, 1910.

A a	B b	C c	D d	E e	F f	G g
A a	B b	C c	D d	E e	F f	G g
H h	I i	J j	K k	L l	M m	N n
H h	I i	J j	K k	L l	M m	N n
O o	P p	Q q	R r	S s	T t	U u
O o	P p	Q q	R r	S ſ s	T t	U ŭ
	V v	W w	X x	Y y	Z z	
	V v	W w	X x	Y y	Z z	