Fields in Mathematical Logic

by

Carl Joachim Svenn

Thesis for the degree of

Master of Science

(Master i Matematikk)

Department of Mathematics
Faculty of Mathematics and Natural Sciences
University of Oslo

November 2011

Contents

Introduction

As a subject for a thesis, I wanted to work with some nice mathematics, which I thought could be found in algebra or mathematical logic. This thesis became the result of topics in mathematical logic suggested by my advisor Dag Normann. It consists of two chapters, "Computable fields" and "Model theory of fields".

In "Computable fields" we use a definition of a computable field which has been used in litterature before. For a computable field, there is an explicit construction of its algebraic closure. We use this construction to show that the algebraic closure of a computable field is computable. We notice that the definition of a computable field alone is too weak, so we add two requirements for computability of fields, where the second requirement is stronger than the first. We show that if a computable field satisfies the first requirement, then its computable algebraic closure also satisfies the first requirement. We show that if a computable field satisfies the second requirement, then its computable algebraic closure also satisfies the second requirement. But even if a field is computable, satisfying our stronger second requirement, there may be properties of the field which are not computable.

In "Model theory of fields" we consider model theory for $(+, \cdot, 0, 1)$–structures satisfying the theory of fields TF. We see that in order to say as much as possible about a field, we must use complete extensions of TF. We show that if T is a complete extension of TF with a finite model, then all models of T are isomorphic. So a finite field has a theory saying everything about its structure. For a complete theory extending TF without a finite model, there are models of any infinite cardinality, by upward Löwenheim–Skolem. Hence we consider the models with the least cardinality, cardinality ω. We show that there is no extension of TF such that all models of cardinality ω are isomorphic. Hence we consider the isomorphism classes of models of cardinality ω for complete theories extending TF without a finite model. We let $\mathsf{n}(T)$ be the number of isomorphism classes of models of cardinality ω for a theory T, and $\mathsf{Th}\, K$ be the complete theory of a field K. Algebraically closed fields are infinite, and we show that $\mathsf{n}(\mathsf{Th}\, K) = \omega$ for an algebraically closed field K. An infinite field has characteristic 0 or prime p. For an infinite field K with characteristic 0 and finite algebraic degree over its prime subfield, we show that $\mathsf{n}(\mathsf{Th}\, K) > \omega$. It is an open question whether the corresponding result holds for infinite fields with characteristic prime p. We discuss the possibility that $\mathsf{n}(\mathsf{Th}\, K) = 0$ if K is finite, $\mathsf{n}(\mathsf{Th}\, K) = \omega$ if K is infinite and algebraically closed, and $\mathsf{n}(\mathsf{Th}\, K) > \omega$ if K is infinite and not algebraically closed. I do not have an answer to this. We end the chapter by considering $(+, \cdot, 0, 1, \leq)$–structures having a field structure, and showing that $\mathbf{Q}$ and $\mathbf{Q}(c)$ are not elementary equivalent.

Did I work with nice mathematics? Nice mathematics for me is a simple and logically clean theory of complex patterns. This was not the case in the first chapter. The definition of a computable field was unnatural, it did not resemble what we were actually looking at. This hid the actual ideas, so that the chapter became difficult to read. I

liked the mathematics in the second chapter better. Here I could play with theory from algebra and model theory.

I would like to thank my advisor Dag Normann for letting me write this thesis. When we have had different interests, he has let me do things the way I wanted. He has also helped me with theory I did not know. I would also like to thank my fellow students for a motivating working environment and their attempts to answer my questions.

Carl Joachim Svenn
Oslo, 15 November 2011

Notation

The natural numbers $\mathbf{N}$ is a set denoting the cardinalities of finite sets. We can compare the sizes of two finite sets, this induces a relation $(\leq) \subseteq \mathbf{N} \times \mathbf{N}$. So we have a structure $(\mathbf{N}, \leq)$. The union of two finite sets is a finite set, this induces a function $(+) : \mathbf{N} \times \mathbf{N} \longrightarrow \mathbf{N}$. So we have a structure $(\mathbf{N}, +)$. The structures have been expanded to give structures $(\mathbf{N}, +, \cdot)$, $(\mathbf{Q}, 0, 1, +, \cdot)$, $(\mathbf{R}, 0, 1, +, \cdot)$, $(\mathbf{Q}, 0, 1, +, \cdot, \leq)$, $(\mathbf{R}, 0, 1, +, \cdot, \leq)$, etc. With abuse of notation, we may consider the set $\mathbf{N}$ as the structure $(\mathbf{N}, +, \cdot)$, the structure $(\mathbf{N}, +, \cdot)$ as the set $\mathbf{N}$, etc. When we enumerate elements using $(\mathbf{N}, \leq)$, we start with the first element 0. We let $x_1 \ldots x_n$ denote n elements, where n can be 0. $\vec{x}$ is shorthand for some $x_1 \ldots x_n$. Arguments of functions are denoted without parentheses, as in $f\, x_1 \ldots x_n$.

If K is a field and A are symbols, let $K[A]$ denote the formal integral domain of polynominals in A over K, let $K(A)$ denote the field of fractions of $K[A]$. If K is a subfield of L and A are elements of L, then $K(A)$ gives a subfield $K(A)$ of L. If $L : K$ is a field extension, we let $[L : K]$ denote the dimension of L as a vector space over K. The algebraic degree of L is the dimension of the algebraic elements of L over K. If a is an algebraic element, then $\mathsf{deg}(a,K)$ is the dimension of the subspace $K(a)$, $\mathsf{deg}(a,K) = [K(a) : K]$. It is known that $\mathsf{deg}(a,K)$ is the degree of the unique irreducible monic polynominal in $K[x]$ corresponding to a. Finite field extension means finite–dimensional field extension, and similar for infinite. We let $\mathbf{F}_{p^n}$ denote the field with p^n elements. The prime subfield of a field K is its least subfield, we typically denote this subfield by $\mathbf{K}$. If K has characteristic 0, its prime subfield is isomorphic to $\mathbf{Q}$, if K has charactertistic prime p, its prime subfield is isomorphic to $\mathbf{F}_p$. A field extension $L : K$ has a transcendence basis, and every two such bases have the same cardinality. The transcendence degree of a field K is the cardinality of a transcendence basis of K over its prime subfield $\mathbf{K}$.

If A is an S–structure, we let $\mathsf{Aut}(A)$ denote the set of S–isomorphisms $A \longrightarrow A$. If A and B are isomorphic S–structures, we write $A \cong B$. We try to make formulas easier to read by ignoring syntactic rules from time to time, as omitting parentheses. The notation x^0 means 1, x^{n+1} means xx^n. With abuse of language, the notation $0 \cdot x$ means 0, $(n+1) \cdot x$ means $x + (n \cdot x)$. The distinctions should be clear.

Chapter 1

Computable fields

1.1 Algebraic background

A field is a $(+, \cdot, 0, 1)$–structure with properties defined by the axioms of fields. A field extension is a triple (i, K, L) such that $i : K \longrightarrow L$ is an injective homomorphism between the fields K and L, and we denote this as $L : K$. The injective homomorphism lets us consider K as a subfield of L. An algebraic element a of a field extension $L : K$ is an element in L for which there exists $f \in K[x]$ such that $f\,a = 0$. If every $a \in L$ is algebraic over K, then $L : K$ is called an algebraic field extension. Every polynominal $f \in K[x]$ has a factorization into $ap_1 \dots p_n$ where a is constant and $p_1 \dots p_n$ are irreducible monic polynominals. This factorization is unique up to the ordering of the factors. If every p_i of this factorization has degree 1, we say that f splits in K. There is a special type of fields where any polynominal splits.

Definition 1.1.1. Algebraically closed field
A field K is algebraically closed if and only if every $f \in K[x]$ splits in K.

There is also a special type of algebraic field extension where the extending field is algebraically closed. If L is an algebraic field extension of K which is algebraically closed, then L is called an *algebraic closure of* K. The structure of an algebraic closure of a field K is unique.

Theorem 1.1.2. *Every field K has an algebraic closure $\overline{K}$. If L_1 and L_2 are algebraic closures of K, then $L_1 \cong L_2$.*

Proof. [3, Theorem 8.2, Theorem 8.4] □

The following result characterizes an algebraic closure of a field.

Theorem 1.1.3. *The following are equivalent for a field extension $L : K$*

1. *$L : K$ algebraic such that L algebraically closed*

2. *$L : K$ algebraic such that every $f \in K[x]$ splits in L*

3. *$L : K$ algebraic such that ($L' : L$ algebraic $\Rightarrow L' = L$)*

Proof. [3, Theorem 8.1] □

The computable function

$$P\,x\,y = \frac{1}{2}((x+y)^2 + 3x + y) \tag{1.1}$$

is a bijection $\mathbf{N} \times \mathbf{N} \longrightarrow \mathbf{N}$. Since P is a computable bijection, we can for every z search for (x, y) such that $P\,x\,y = z$, hence the functions π_0, π_1 such that $P\,(\pi_0\,x)\,(\pi_1\,x) = x$ for all x, are computable.

Let K be a countable field. Define $K_0 = K$. Suppose we have defined the K_n–th field, being countable and an extension of all previous fields. Since K_n is countable, we have an enumeration of the non–constant polynominals in $K_n[x]$. We pick the $(\pi_1\,n)$–th non–constant polynominal f_n in $K_{(\pi_0\,n)}[x]$. Since $\pi_0\,n \leq n$, this makes sense. Let p_n be an irreducible factor of f_n. Define the field $K_{n+1} = K_n[x]/(p_n)$ which is countable and an extension of all previous fields. We then have the fields

$$\begin{aligned} K_0 &= K \\ K_{n+1} &= K_n[x]/(p_n) \end{aligned}$$

each being a field extension of all previous fields. Now consider the field L constructed by "taking the union" of all K_i. If a is an element of L then $a \in K_i$ for some i, and so a is algebraic over K. For each i and each non–constant $f \in K_i[x]$ there is a K_j such that f has a root a. So f has a factor $(x - a)$ in K_j. Continuing this way we see that f splits in L. By Theorem 1.1.3 we know that L is an algebraic closure of K.

1.2 Computable representation

The theory of computability in the natural numbers $\mathbf{N}$ is well established. To define computability in another object O, we can let elements in $\mathbf{N}$ represent structure of O, giving a subset of $\mathbf{N}$. The question of whether a part of O is computable or not reduces to whether a corresponding part in $\mathbf{N}$ is computable or not. We use this consideration in our definition of a computable field. If K is a countable field, we let the elements k of K be represented by disjoint subsets A_k of $\mathbf{N}$. This gives a subset $A = \cup A_k$ of $\mathbf{N}$ representing the set of elements of K. The two functions 0, 1 of K induces two elements in $\{A_k : k \in K\}$. The two functions $(+)$, $(\cdot)$ of K induces two functions in $\{A_k : k \in K\} \times \{A_k : k \in K\} \longrightarrow \{A_k : k \in K\}$. If there are partial computable functions on $\mathbf{N}$ which agree on these induced functions, we are able to compute the induced structure in $\mathbf{N}$.

Definition 1.2.1. Computable representation
A computable representation of a field K on A is a tuple (ϕ, f, g, z, w) such that

- $\phi : A \subseteq \mathbf{N} \longrightarrow K$ surjection
- f : "$\mathbf{N} \times \mathbf{N}$" $\longrightarrow \mathbf{N}$ partial computable such that $(\phi\, x) + (\phi\, y) = \phi\,(f\, x\, y)$ for all $x, y \in A$
- g : "$\mathbf{N} \times \mathbf{N}$" $\longrightarrow \mathbf{N}$ partial computable such that $(\phi\, x) \cdot (\phi\, y) = \phi\,(g\, x\, y)$ for all $x, y \in A$
- $z \in A$ such that $\phi\, z = 0$
- $w \in A$ such that $\phi\, w = 1$

We define a *computable field* K to be a field K for which there exists a computable representation of K on some subset A of $\mathbf{N}$. This definition implies that K is countable. An element k of K corresponds to the subset $A_k = \{x : \phi\, x = k\}$ of A.

1.3 Computable algebraic closure

We now show that if K is a computable field, then the algebraic closure $\overline{K}$ is a computable field, by constructing a representation of $\overline{K}$ from a representation of K. Let K be a computable field. As above, we construct a sequence $\{K_i : i \in \mathbf{N}\}$ of fields such that each field is an extension of all previous fields. Then the field L constructed as "the union" of all K_i is an algebraic closure of K. Let R_0 be a representation of $K_0 = K$ on a subset A_0 of $\mathbf{N}$. For a representation R_n of K_n on A_n, we let A_{n+1} be the subset of $\mathbf{N}$ consisting of the sequence numbers of the finite sequences of A_n. Then each element in $K_n[x]$ can be represented by an element in A_{n+1}. Since the operations on the field $K_n[x]/(p_n)$ are computable with respect to K_n, we have a representation R_{n+1} of K_{n+1} on A_{n+1}. So we have representations for each K_i. Those representations can be used in a representation of L, and thus the algebraic closure $\overline{K}$ is computable.

Proposition 1.3.1. *If K is a computable field, then $\overline{K}$ is a computable field.*

Proof. For each K_i we have a representation R_i on A_i. For each i, define the set

$$B_i = \left\{p_i^{a+1} : a \in A_i\right\}$$

where p_i is the i–th prime. If $i \neq j$ then B_i and B_j are disjoint subsets of $\mathbf{N}$. We lift each representation on A_i to a representation on B_i, so we have representations of the fields K_i on disjoint subsets of $\mathbf{N}$. There is now a representation of L on the set $B = \cup B_i$. Since $L \cong K$, we have an obvious surjection $\phi' : B \longrightarrow \overline{K}$. Let x, y be elements in B, say $x \in B_i$, $y \in B_j$ where $i \leq j$. The injection $K_i \longrightarrow K_j$ as a function $B_i \longrightarrow B_j$ is computable. To compute an operation on (x, y), we put x and y in B_j and perform the operation there. By uniformity, there are computable functions f, g on B such that

$(\phi' x) + (\phi' y) = \phi' (f x y)$ and $(\phi' x) \cdot (\phi' y) = \phi' (g x y)$. We also have elements z, w in B such that $\phi' z = 0$ and $\phi' w = 1$. So we have a representation of $\overline{K}$. □

1.4 Equality

In a computable representation (ϕ, f, g, z, w) of a field K on A, the functions f, g sends representatives of two elements to a representative for the result, in a computable way. They do not necessarily care about the actual element in K of a representative. The equality relation on K corresponds to the equivalence relation

$$x \sim y \iff \phi x = \phi y$$

on A. The elements in K corresponds to the equivalence classes on A induced by this equivalence relation. Without any computional requirement on these equivalence classes, a computable representation is uninteresting, as the following example shows.

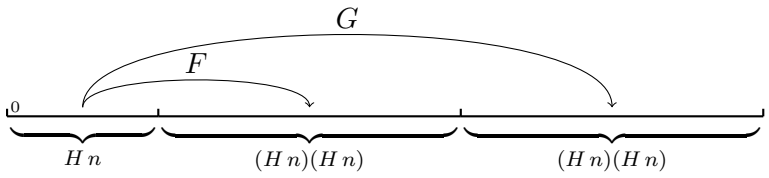
Let K be a countable field. Then there is a set $X \subseteq \mathbf{N}$ with a bijection $X \longrightarrow K$. Define the following disjoint subsets of $\mathbf{N}$

$$P_i = \left\{ p_i^{n+1} \,:\, n \in \mathbf{N} \right\}$$

each being a copy of $\mathbf{N}$. Then $P_0^X = \{p_0^x : x \in X\} \subseteq P_0$. Set $H\,0 = 1$. From $H\,n$ elements we have $(H\,n)(H\,n)$ pairs. Two copies of $(H\,n)(H\,n)$ elements gives $2(H\,n)(H\,n)$ elements. Set $H\,(n+1) = (H\,n) + 2(H\,n)(H\,n)$. There are then computable functions F, G such that for all n

$$\begin{aligned} i < H\,n \text{ and } j < H\,n &\;\Rightarrow\; H\,n \leq F\,i\,j < H\,(n+1) \\ i < H\,n \text{ and } j < H\,n &\;\Rightarrow\; H\,n \leq G\,i\,j < H\,(n+1) \end{aligned}$$

and more important, F, G are injective functions $\mathbf{N} \times \mathbf{N} \longrightarrow \mathbf{N}$ with disjoint images.



This gives partial computable functions

$$\begin{aligned} f\,(p_i^{x+1})\,(p_j^{y+1}) &= p_{F\,i\,j}^{(P\,x\,y)+1} \\ g\,(p_i^{x+1})\,(p_j^{y+1}) &= p_{G\,i\,j}^{(P\,x\,y)+1} \end{aligned}$$

sending an element in $P_i \times P_j$ to an element in $P_{F\,i\,j}$ and $P_{G\,i\,j}$ respectively ($P\,x\,y$ is the computable bijection (1.1), on page 9). Starting with the set P_0^X, these computable functions will give a representation of K on some set $A \subseteq \mathbf{N}$. This type of construction works for structures with a signature consisting of a finite number of function symbols.

1.4.1 Equality computably enumerable

A computable requirement on the equivalence classes may be that the equivalence relation is computably enumerable. We say that K is a *computable field with computably enumerable equality relation* if and only if there exists a computable representation of K with computably enumerable equivalence relation. Below is a characterization of a computably enumerable equivalence relation.

Lemma 1.4.1. *Let (ϕ, f, g, z, w) be a computable representation of a field K on A. The equivalence relation is computably enumerable if and only if A and the set $\{x : \phi\, x = 0\}$ are computably enumerable.*

Proof. Let A and $\{x : \phi\, x = 0\}$ be computably enumerable. There is an element a in A such that $\phi\, a = (-1)$, so we can compute "$x - y$" of two representatives by $f\, x\, (g\, a\, y)$. Since $x \sim y \iff \phi\, x = \phi\, y$, we have $x \sim y \iff \phi\, (f\, x\, (g\, a\, y)) = 0$, so the set of pairs in the equivalence relation is computably enumerable.

Let the set of pairs in the equivalence relation be computably enumerable. Since the equivalence relation $(\sim)$ also is reflexive, that is $x \sim x$ for all x, the set A is computably enumerable. Since $\phi\, z = 0$, we have $\phi\, x = 0 \iff x \sim z$, so the set $\{x : \phi\, x = 0\}$ is computably enumerable. □

1.4.2 Equality computable

A computable requirement on the equivalence classes may be that the equivalence relation is computable. This is a stronger requirement than the previous. We say that K is a *computable field with computable equality relation* if and only if there exists a computable representation of K with computable equivalence relation. Below is a characterization of a computable equivalence relation.

Lemma 1.4.2. *Let (ϕ, f, g, z, w) be a computable representation of a field K on A. The equivalence relation is computable if and only if A and the set $\{x : \phi\, x = 0\}$ are computable.*

Proof. Let A and $\{x : \phi\, x = 0\}$ be computable. There is an element a in A such that $\phi\, a = (-1)$, so we can compute "$x - y$" of two representatives by $f\, x\, (g\, a\, y)$. Since $x \sim y \iff \phi\, x = \phi\, y$, we have $x \sim y \iff \phi\, (f\, x\, (g\, a\, y)) = 0$, so the set of pairs in the equivalence relation is computable.

Let the set of pairs in the equivalence relation be computable. Since the equivalence relation $(\sim)$ also is reflexive, the set A is computable. Since $\phi\, z = 0$, we have $\phi\, x = 0 \iff x \sim z$, so the set $\{x : \phi\, x = 0\}$ is computable. □

We could have defined a computable representation of K on A as a tuple (ϕ, f, g, z, w) such that $\phi : K \longrightarrow A$ is a bijection, $\phi\, (x + y) = f\, (\phi\, x)\, (\phi\, y)$ and $\phi\, (x \cdot y) = g\, (\phi\, x)\, (\phi\, y)$

for all x, y in K with f, g partial computable, $\phi\, 0 = z$ and $\phi\, 1 = w$, and A a computable set. Call this an alternative–representation. Then there is an alternative–representation on A if and only if there is a representation on A with equality relation computable. For if R is a representation on A with equality relation computable, let $\phi' : K \longrightarrow A$ be the bijection sending an element to its representative with lowest value. The functions f', g' are the functions f, g modified to give the representative with lowest value. Since the equality relation is computable, the functions f', g' are computable. Conversely, if R' is an alternative–representation on A we can let $\phi : A \longrightarrow K$ be the inverse of ϕ', and since A is computable the equality relation is trivially computable.

1.5 Algebraic closure with computably enumerable equality

Suppose K is a computable field with computably enumerable equality relation. We can then construct a representation $\overline{K}$ on B from a representation of K on A, as described in Proposition 1.3.1. We show that we can construct the representation of $\overline{K}$ in a way that the equivalence relation on B will be computably enumerable, so if K is a computable field with computably enumerable equality relation, then $\overline{K}$ is a computable field with computably enumerable equality relation.

We will construct representations of K_i on A_i such that A_i and $\{x : \phi_i\, x = 0\}$ are computably enumerable, and then construct a representation of $\overline{K}$ from these. When we construct a representation R_{n+1} of K_{n+1} on A_{n+1}, we need to find a representative in A_{n+1} of a non–constant polynominal in $K_n[x]$. This implies that we need to know whether an element in A_n does not represent 0. By the assumtion that $\{x : \phi_n\, x = 0\}$ is computably enumerable, we can tell if an element in A_n represent 0. But we know that

$$x \neq 0 \iff \exists y \;\; x \cdot y = 1$$

so we can also tell if an element of A_n does not represent 0. Hence we are able to find a representative of a i–th non–constant polynominal in $K_n[x]$ for any i.

Proposition 1.5.1. *If K is a computable field with computably enumerable equality relation, then $\overline{K}$ is a computable field with computably enumerable equality relation.*

Proof. We have a representation R_0 of K_0 on A_0 such that the set A_0 and $\{x : \phi_0\, x = 0\}$ are computably enumerable. Suppose $R_0, \ldots, R_n$ are such that each R_i is representation of K_i on A_i with A_i computably enumerable. Suppose the set $\{x : \phi_n\, x = 0\}$ in A_n is computably enumerable. Since A_n is computably enumerable, the set A_{n+1} is computably enumerable. We now show that the subset $\{x : \phi_{n+1}\, x = 0\}$ of A_{n+1} is computably enumerable.

Since all A_i are computably enumerable, we can pick a representative of the $(\pi_1\, n)$–th non–constant polynominal f_n in $K_{(\pi_0\, n)}[x]$ as an element in A_{n+1}. Starting with $g_0 = f_n$,

we can search for a factorization of g_i into two non–constant factors, and if such found, continue this process with the first factor as g_{i+1}. If g_{i+1} is a factor of g_i and g_{i+2} is a factor of g_{i+1}, then g_{i+2} is a factor of g_i. So this process gives smaller and smaller factors of f_n, eventually giving an irreducible factor p_n of f_n. The set $\{x : \phi_{n+1}\, x = 0\}$ is the set of elements in A_{n+1} representing polynominals with the factor p_n. If x is an element in A_{n+1} representing some polynominal h, we can search for a factorization of h having a factor g_i, by searching after the factors g_i of f_n at the same time. We will find a factor g_i of h if and only if $\phi_{n+1}\, x = 0$.

Let R' be the representation of $\overline{K}$ on B constructed from the representations R_i. By uniformity, the set B is computably enumerable. By uniformity, the set $\{x : \phi'\, x = 0\}$ is computably enumerable. So we have a representation of $\overline{K}$ with computably enumerable equivalence relation, by Lemma 1.4.1. □

1.6 Algebraic closure with computable equality

Suppose K is a computable field with computable equality relation. From Proposition 1.5.1 we have a representation of $\overline{K}$ with computably enumerable equality relation. We show that in fact this equality relation is computable.

Proposition 1.6.1. *If K is a computable field with computable equality relation, then $\overline{K}$ is a computable field with computable equality relation.*

Proof. We have a representation R of K on A. By Lemma 1.4.2, the sets A and $\{x : \phi\, x = 0\}$ are computable. By Lemma 1.4.2, it suffices to show that the sets B and $\{x : \phi'\, x = 0\}$ in the representation of $\overline{K}$ are computable. Since A is computable, the set B is computable by its construction. By Proposition 1.5.1, the set $\{x : \phi'\, x = 0\}$ is computably enumerable, so we only need to show that its complement in $\mathbf{N}$ is computably enumerable.

Let $a \neq 0$ be an element in the field $\overline{K}$. Since $\overline{K}$ is algebraic over K, there is an irreducible f in $K[x]$ such that $f\, a = 0$. Also, $a \neq 0$ so x is not a factor of the polynominal f. Hence $f\, 0 \neq 0$. Conversely, if $f\, a = 0$ and $f\, 0 \neq 0$ for f in $K[x]$, then $a \neq 0$. So for all $a \in \overline{K}$ we have

$$a \neq 0 \iff \text{there is } f \text{ in } K[x] \text{ such that } f\, a = 0 \text{ and } f\, 0 \neq 0$$

Consider an element in the complement of $\{x : \phi'\, x = 0\}$. If the element is not in B we can tell this, since B is computable. Otherwise, let x be an element in B representing an element $a \neq 0$ of the field $\overline{K}$. By the construction of the representation of $\overline{K}$, we can consider the subset B_0 of B as the subfield K of $\overline{K}$. Since the sets B_0 and $\{x : \phi'\, x = 0\}$ are computably enumerable, we can search for elements $b_0 \ldots b_n$ in B_0 such that

$$(\phi'\, x)^{n+1} + (\phi'\, b_n)(\phi'\, x)^n + \cdots + (\phi'\, b_0) = 0$$

And since the set $\{x : \phi_0\, x = 0\}$ of B_0 is computable, we can also verify that $b_0 \ldots b_n$ represent a polynominal f for which $f\, 0 \neq 0$. Thus, the complement of $\{x : \phi'\, x = 0\}$ is computably enumerable, so the equivalence relation is computable. So we have a computable representation of $\overline{K}$ with computable equivalence relation. □

1.7 Non–computable properties

With computability theory, it is pretty easy to show that even if a field is computable by our definition, there are properties of the field which do not need to be computable. Let X be a computably enumerable, non–computable subset of $\mathbf{N}$. By [4, 5.Theorem VI] such a set exists. We show that there is a field K with a property which can not be computed from any representation of K. Let $\{p_i : i \in \mathbf{N}\}$ be the set of primes ordered by value. Let K be the subfield of $\overline{\mathbf{Q}}$ generated by 1 and $q_i^{1/2}$ for each $i \in X$. Then the predicate $(\exists y\ \ y^2 = x)$ on K can not be computable. For if this predicate is computable, there will exist a representation of K on some A such that $\left\{a : \exists y\ \ y^2 = \phi\, a\right\}$ is a computable set, by definition. Suppose R is one such representation. We have a representative of 1, so for each i we can compute a representative for p_i. If $i \in X$ then ${p_i}^{1/2} \in K$. Suppose $i \notin X$ and ${p_i}^{1/2} \in K$. Then ${p_i}^{1/2} \in \mathbf{Q}({q_1}^{1/2} \ldots {q_n}^{1/2})$ for some primes $q_1 \ldots q_n$ corresponding to elements of X, which is a contradiction by the following lemma.

Lemma 1.7.1. *Let $q_1 \ldots q_n$ be integers such that $\mathsf{gcd}(q_i,q_j) = 1$ for all $i \neq j$ and ${q_i}^{1/2} \notin \mathbf{Q}$ for all i.*

$$[\mathbf{Q}({q_1}^{1/2} \ldots {q_n}^{1/2}) : \mathbf{Q}] = 2^n$$

Proof. If $n = 0$ then $[\mathbf{Q} : \mathbf{Q}] = 1 = 2^0$, so the result holds. If $n = 1$ then $[\mathbf{Q}({q_1}^{1/2}) : \mathbf{Q}] = 2 = 2^1$ by assumption, so the result holds. Suppose the result holds for n and $n + 1$. Let $q_1 \ldots q_n q_{n+1} q_{n+2}$ be integers satisfying the assumption. Set $\mathbf{Q}_n = \mathbf{Q}({q_1}^{1/2} \ldots {q_n}^{1/2})$ and $\mathbf{Q}_{n+1} = \mathbf{Q}({q_1}^{1/2} \ldots {q_n}^{1/2} {q_{n+1}}^{1/2})$. Since ${q_{n+2}}^{1/2}$ is a root of $x^2 - q_{n+2}$, $\mathsf{deg}({q_{n+2}}^{1/2},\mathbf{Q}_{n+1}) \leq 2$. Suppose the degree is not 2, then ${q_{n+2}}^{1/2} \in \mathbf{Q}_{n+1}$, so ${q_{n+2}}^{1/2} = a_0 + a_1 {q_{n+1}}^{1/2}$ for a_0, a_1 in $\mathbf{Q}_n$.

Suppose $a_0 = 0$. Then ${q_{n+2}}^{1/2} = a_1 {q_{n+1}}^{1/2}$ is an element in $\mathbf{Q}_{n+1}$. Since also ${q_{n+1}}^{1/2} \in \mathbf{Q}_{n+1}$, ${q_{n+2}}^{1/2} {q_{n+1}}^{1/2} = a_1 {q_{n+1}}^{1/2} {q_{n+1}}^{1/2} = a_1 q_{n+1}$ is an element in $\mathbf{Q}_n$. So $\mathbf{Q}_n$ contains the roots of $x^2 - q_{n+2} q_{n+1}$, and so $[\mathbf{Q}_n((q_{n+2} q_{n+1})^{1/2}) : \mathbf{Q}] = [\mathbf{Q}_n : \mathbf{Q}] = 2^n$. But the $n + 1$ integers $q_1 \ldots q_n (q_{n+2} q_{n+1})$ satisfy the conditions, so the dimension is 2^{n+1} which is a contradiction.

Suppose $a_1 = 0$. Then ${q_{n+2}}^{1/2} = a_0$ is an element in $\mathbf{Q}_n$, so $[\mathbf{Q}_n({q_{n+2}}^{1/2}) : \mathbf{Q}] = [\mathbf{Q}_n : \mathbf{Q}] = 2^n$. But the $n + 1$ integers $q_1 \ldots q_n q_{n+2}$ satisfy the conditions, so the dimension is 2^{n+1}, which is a contradiction.

Suppose $a_0 \neq 0$, $a_1 \neq 0$. Then ${q_{n+2}}^{1/2} = a_0 + a_1 {q_{n+1}}^{1/2}$ is an element in $\mathbf{Q}_{n+1}$, and so also $q_{n+2} = a_0^2 + 2 a_0 a_1 {q_{n+1}}^{1/2} + a_1^2 q_{n+1}$. So ${q_{n+1}}^{1/2} = (2 a_0 a_1)^{-1}(q_{n+2} - a_0^2 - a_1^2 q_{n+1})$

is an element in $\mathbf{Q}_n$, so $[\mathbf{Q}_n({q_{n+1}}^{1/2}) : \mathbf{Q}] = [\mathbf{Q}_n : \mathbf{Q}] = 2^n$. But the $n+1$ integers $q_1 \ldots q_n q_{n+1}$ satisfy the conditions, so the dimension is 2^{n+1}, which is a contradiction.

Then $\mathsf{deg}({q_{n+2}}^{1/2}, \mathbf{Q}_{n+1}) = 2$, so $[\mathbf{Q}_{n+1}({q_{n+2}}^{1/2}) : \mathbf{Q}] = [\mathbf{Q}_{n+1}({q_{n+2}}^{1/2}) : \mathbf{Q}_{n+1}][\mathbf{Q}_{n+1} : \mathbf{Q}] = 2 \cdot 2^{n+1} = 2^{n+2}$. □

Hence $i \in X$ if and only if ${p_i}^{1/2} \in K$. But then the set X is computable, as $\{a : \exists y \;\; y^2 = \phi\, a\}$ is a computable set.

We should also show that there is a representation of K with equivalence relation computable, in order to show that we have a representation of K with our strongest computable requirement on the equivalence classes. Since X is computably enumerable, we have a computable bijection $I : \mathbf{N} \longrightarrow X$. Let q_i be the $(I\, i)$–th prime. Then $i \mapsto q_i$ is a computable function. Define fields

$$K_0 = \mathbf{Q}$$
$$K_{n+1} = K_n({q_n}^{1/2})$$

There is a representation R_0 of K_0 on A_0 with computable equivalence relation. Suppose R_n is a representation of K_n on A_n with computable equivalence relation. By Lemma 1.7.1, the polynominal $x^2 - q_n$ is irreducible over K_n and so $K_{n+1} \cong K_n[x]/(x^2 - q_n)$. Let A_{n+1} be the set of sequence numbers of the finite sequences of A_n. There is a representation of $K_n[x]/(x^2 - q_n)$ on A_{n+1}. Since $x^2 - q_n$ is irreducible over K_n, and the equivalence relation of R_n is computable, and the function $i \mapsto q_i$ is computable, we can use the division algorithm in $K_n[x]$ to compute the subset $\{a : \phi_{n+1}\, a = 0\}$ of A_{n+1}. Hence there is a representation R_{n+1} of K_{n+1} on A_{n+1} with computable equivalence relation. As before we lift the representations R_i to representations of K_i on B_i, to create a representation R' of K on the disjoint union $B = \cup B_i$. By uniformity and the fact that X is computably enumerable, the equivalence relation of R' is computable.

Chapter 2

Model theory of fields

2.1 Model theory

In model theory we are interested in the structures satisfied by theories in first order languages. The signature of a structure is the set of relation symbols and function symbols of the structure. For each signature, there is a corresponding first order language. If A is a structure with signature S and $X \subseteq A$, we can create the structure $(A, a)_{a \in X}$ with signature S', where S' is the disjoint union of the symbols in S and symbols $\underline{a}$ for each $a \in X$. The notation $A \models F\,\vec{\underline{a}}$ means $(A, a)_{a \in A} \models F\,\vec{\underline{a}}$. If T is a consistent theory, then T has a model.

A complete theory T is a consistent theory such that for all sentences F in the language, either $T \vdash F$ or $T \vdash \neg F$. Let T be a complete theory, and let $X_{x_1 \ldots x_n}$ be the set of formulas in the language with free variables among $x_1 \ldots x_n$. A formula F in $X_{x_1 \ldots x_n}$ is said to be consistent with T if $(T \vdash \exists x_1 \ldots \exists x_n \;\; F\,x_1 \ldots x_n)$, a subset M of $X_{x_1 \ldots x_n}$ is said to be consistent with T if any finite conjuction of members in M is consistent with T. A n–type of T is a maximal consistent with T subset of some $X_{x_1 \ldots x_n}$. Let $\mathsf{S}_n(T)$ denote the set of maximal consistent with T subsets of $X_{x_1 \ldots x_n}$. The syntactic notion $\mathsf{S}_n(T)$ can be used in various ways to say something about the models of a complete theory T.

Lemma 2.1.1. *Let T be a complete theory of a countable signature. If T has uncountable many n–types for some n, then T has uncountable many non–isomorphic countable models.*

Proof. Suppose the set of non–isomorphic countable models of T is countable. By the proof of [1, Proposition 2.2.7], we know that every n–type is realized in some countable model of T. Since each countable model of T realizes countable many n–types, the set of n–types is a countable union of countable sets. But then the set of n–types is countable, which is false. □

Let A be a structure with signature S. If $S' \subseteq S$, we can consider A as a structure A' with signature S'. But then we decrease the structural properties, so it is easier for two S'–structures to be isomorphic. In the other direction, if we add more structural properties we will have more possibilities of different structures, so it is more difficult for two structures to be isomorphic. If a new property is already given by the theory, the new property will not give us any more possibilities of different structures, as the following lemma shows.

Lemma 2.1.2. *Let S' be a subset of a signature S. Let T be a theory in the language of S such that for each relation symbol R of S*

$$T \vdash R\,\vec{x} \longleftrightarrow F_R\,\vec{x}$$

for some S'–formula F_R, and for every function symbol f of S

$$T \vdash f\,\vec{x} = y \longleftrightarrow F_f\,\vec{x}\,y$$

for some S'–formula F_f. Let A_0, A_1 be models of T, and let A_0', A_1' be the respective S'–structures. If $\phi : A_0' \longrightarrow A_1'$ is an S'–isomorphism, then $\phi : A_0 \longrightarrow A_1$ is an S–isomorphism.

Proof. Suppose $\phi : A_0' \longrightarrow A_1'$ is an S'–isomorphism. Let R be a relation symbol of S. Then

$$\begin{aligned} A_0 \models R\,\underline{a} &\iff A_0 \models F_R\,\underline{\vec{a}} \\ &\iff A_1 \models F_R\,\underline{\phi\,\vec{a}} \\ &\iff A_1 \models R\,\underline{\phi\,\vec{a}} \end{aligned}$$

for all $\vec{a}$ of A_0. Let f be a function symbol of S. Then

$$\begin{aligned} A_0 \models f\,\underline{a} = \underline{b} &\iff A_0 \models F_f\,\underline{\vec{a}}\,\underline{b} \\ &\iff A_1 \models F_f\,(\underline{\phi\,\vec{a}})\,(\underline{\phi\,b}) \\ &\iff A_1 \models f\,\underline{\phi\,\vec{a}} = \underline{\phi\,b} \end{aligned}$$

for all $\vec{a}$ of A_0, and so $\phi(f\,\vec{a}) = f\,(\phi\,\vec{a})$. □

2.2 Theory of fields

The theory of fields TF is the following theory of $(+, \cdot, 0, 1)$–structures:

$$
\begin{aligned}
&0 \neq 1\\
&\forall x \forall y \;\; x + y = y + x\\
&\forall x \;\; x + 0 = x\\
&\forall x \exists y \;\; x + y = 0\\
&\forall x \forall y \forall z \;\; (x + y) + z = x + (y + z)\\
&\forall x \forall y \;\; x \cdot y = y \cdot x\\
&\forall x \;\; x \cdot 1 = x\\
&\forall x \;\; (x \neq 0 \longrightarrow \exists y \;\; x \cdot y = 1)\\
&\forall x \forall y \forall z \;\; (x \cdot y) \cdot z = x \cdot (y \cdot z)\\
&\forall x \forall y \forall z \;\; x \cdot (y + z) = x \cdot y + x \cdot z
\end{aligned}
$$

We want to use our language to express as much as possible of the structural properties of a given field. One such structural property of fields we are able to express is the characteristic. Let C_i be the sentence

$$C_i = \underbrace{1 + \cdots + 1}_{i} = 0$$

Note that if p is prime, then $K \models C_p$ implies $K \not\models C_i$ for $1 \leq i < p$, so for p prime we have $K \models C_p$ if and only if K has characteristic p. A field with characteristic 0 is a field where C_i is false for all $i \geq 1$. Let $\mathsf{Char_0}$ be the set consisting of $\neg C_i$ for all $i \geq 1$. Let $\mathsf{Char_p}$ be the set consisting of C_p and $\neg C_i$ for all $1 \leq i < p$.

Another structural property we are able to express with our language is that all polynominals of a given degree has a root in the field. This property holds in particular for algebraically closed fields. The theory ACF of algebraically closed fields is TF extended with

$$\forall a_0 \ldots \forall a_n \;\; \exists x \;\; x^{n+1} + a_n x^n + \cdots + a_0 = 0$$

for all n. It is shown that $\mathsf{ACF} \cup \mathsf{Char_x}$ is a complete theory for $x = 0$ or x prime ([7, Corollary 3.2.3]).

If we want to describe the structural properties of a given field, we can add to TF the properties of the field we are able to express in our language. For example, if K is a field where every element has a square root, then $\mathsf{TF} \cup \{\forall x \exists y \; x = y^2\}$ is a theory for K. In order to say as much as possible about the structural properties of a field, we are interested in theories T extending TF.

2.2.1 Categoricity

A categorical theory T is a theory where any two models of T are isomorphic. A categorical theory T is surely complete, for if F is a sentence such that neither $T \vdash F$ nor $T \vdash \neg F$, we can create models A and B such that $A \models T \cup \{F\}$ and $B \models T \cup \{\neg F\}$, and so A and B are non–isomorphic models of T. Given a field K, the theory saying as much as possible about the structural properties of K is the theory of all sentences true in K, $\mathsf{Th}\, K$, which is a complete theory. The following result shows that if T is a complete theory extending TF with a finite model, then any two models of T are isomorphic, and so T is a categorical theory. The result is a special case of the fact that a complete theory from any signature with a finite model is a categorical theory.

Proposition 2.2.1. *Let T be a complete theory extending TF with a finite model.*

$$A \models T \text{ and } B \models T \;\Rightarrow\; A \cong B$$

Proof. Let A be a finite model of T with n elements. Since T is complete we know that $T \vdash F$ if and only if $A \models F$ for all F in the language. Let N be the formula

$$\begin{aligned} N\, x_1 \ldots x_n = x_1 \neq x_2 \wedge \ldots \wedge x_1 \neq x_n \quad & \wedge \\ & \vdots \\ x_n \neq x_1 \wedge \ldots \wedge x_n \neq x_{n-1} \quad & \wedge \\ \forall x \;\; (x = x_1 \vee \ldots \vee x = x_n) & \end{aligned}$$

characterizing n elements. Choose a bijection $\phi : \{x_1 \ldots x_n\} \longrightarrow A$. Let $F_{(+)}$ be the following formula defining the result of $(+)$ for all the n^2 pairs of elements in A:

$$F_{(+)}\, x_1 \ldots x_n = (x_1 + x_1 = x_{(1,1)}) \wedge \ldots \wedge (x_n + x_n = x_{(n,n)})$$

where $x_{(i,j)}$ is the result of $x_i + x_j$ induced from the bijection ϕ. Let $F_{(\cdot)}$ be the following formula defining the result of $(\cdot)$ for all the n^2 pairs of elements in A:

$$F_{(\cdot)}\, x_1 \ldots x_n = (x_1 \cdot x_1 = x_{(1,1)}) \wedge \ldots \wedge (x_n \cdot x_n = x_{(n,n)})$$

where $x_{(i,j)}$ is the result of $x_i \cdot x_j$ induced from the bijection ϕ. The formula

$$\begin{aligned} G = \exists x_1 \ldots \exists x_n & \\ & (N\, x_1 \ldots x_n \wedge F_{(+)}\, x_1 \ldots x_n \wedge F_{(\cdot)}\, x_1 \ldots x_n) \end{aligned}$$

is true in A, so $T \vdash G$. If B is a model of T, then $B \models G$, so B has n elements with its graphs defined by G. Hence $A \cong B$. □

Let T be a complete theory extending TF without a finite model. By upward Löwenheim–Skolem, there is a model of T of any infinite cardinality. Hence T is not categorical. Also, by downward Löwenheim–Skolem, if A is a model of T, there is a model B of T

of cardinality ω. Hence, for a complete theory T extending TF without a finite model, we are interested in the models of T of cardinality ω. An ω–categorical theory T is a theory with a model of cardinality ω and where any two models of T with cardinality ω are isomorphic. Suppose T is an ω–categorical theory of a countable signature. If T is not complete there are non–isomorphic models A and B of T with cardinality ω, which is a contradiction. If T has a finite model then all models of T are finite, which is a contradiction. Hence an ω–categorical theory of a countable signature is a complete theory without a finite model. In the following results, found in [5], we show that there is no extension T of TF such that T is ω–categorical.

Theorem 2.2.2. *Let T be a complete theory of a countable signature without a finite model. The following are equivalent:*

- *T is ω–categorical*
- *$\mathsf{S}_n(T)$ is finite for all n*
- *If A is a countable model of T, then the number of orbits from $\mathsf{Aut}(A)$ on n–tuples of elements in A is finite, for all n*

Proof. This is proven in [5, Theorem 7.3.1]. □

Theorem 2.2.3. *Let T be an ω–categorical theory of a countable signature. Let A be a model of T. If A' is any finitely generated substructure of A, then A' is finite. More specific, for each n there is a least number m such that every substructure of A generated by n elements has size less than or equal to m.*

Proof. Suppose T is ω–categorical. Then T is a complete theory without a finite model. Let $\vec{a}$ be generators for a substructure A', and b, c be different elements in that substructure. We look at the $(n+1)$–types satisfied by $\vec{a}\,b$ and $\vec{a}\,c$:

$$N_b\,\vec{x}\,y = \{F\,\vec{x}\,y \,:\, A \models F\,\vec{a}\,b\}$$
$$N_c\,\vec{x}\,y = \{F\,\vec{x}\,y \,:\, A \models F\,\vec{a}\,c\}$$

We now show that these types are different. Since b and c are generated by $\vec{a}$, there are terms such that $b = t_b\,\vec{a}$ and $c = t_c\,\vec{a}$. Hence

$$(y = t_b\,\vec{x}) \in N_b$$
$$(y = t_c\,\vec{x}) \in N_c$$

Since b and c are different elements we have

$$T \vdash \exists x_1 \ldots \exists x_n \;\; (t_b\,\vec{x} \neq t_c\,\vec{x})$$

and so

$$(y = t_c\,\vec{x}) \notin N_b$$

since N_b is a consistent set by definition. Thus, N_b and N_c are different types. Since A is ω–categorical, the set of $(n+1)$–types is finite (Theorem 2.2.2), and so A' is a finite set. Hence every finitely generated substructure of A is finite.

We now show that for each n, there is a least number m such that every substructure generated by n elements has size less than or equal to m. By Theorem 2.2.2, the set of orbits of $\mathsf{Aut}(A)$ on n–tuples is finite. These orbits are the equivalence classes of the equivalence relation

$$\vec{x} \sim \vec{y} \iff \text{there is an isomorphism in } \mathsf{Aut}(A) \text{ sending } \vec{x} \text{ to } \vec{y}$$

Let $\vec{a_1} \dots \vec{a_r}$ be tuples representing each equivalence class, and let $A'_1 \dots A'_r$ be the substructures generated by $\vec{a_1} \dots \vec{a_r}$ respectively. As proven above, each A'_i is finite, say $|A_i| = m_i$. Let B be any substructure generated by n elements $\vec{b}$. Then $\vec{b}$ is equivalent to some $\vec{a_i}$, so we have an isomorphism $A \longrightarrow A$ sending $\vec{b}$ to $\vec{a_i}$. Thus, the substructure generated by $\vec{b}$ has size m_i. Then $m = \mathsf{max}(m_1 \dots m_r)$ is a least number such that every substructure of A generated by n elements has size less than or equal to m. □

Theorem 2.2.4. *There is no ω–categorical extension of* TF.

Proof. Suppose T is an extension of TF such that T is ω–categorical. Then T is complete. Let A be a countable model of T. By Theorem 2.2.3, every substructure A' of A generated by one element is finite with size less than or equal to m. Let x be a non–zero element of A. Since the substructure generated by x is finite with size less than or equal to m, there are x^i and x^j from the $m+1$ terms $x^1 \dots x^{m+1}$ such that $x^i = x^j$ and $i < j$. Hence $x^{j-i} = 1$ with $j - i \leq m$. This means that every non–zero element of A satisfy $x^{m!} - 1 = 0$. But A is assumed to be infinite, so $x^{m!} - 1$ will then have infinitely many roots, which is not possible. □

2.3 The number of isomorphism classes

We are interested in the models of cardinality ω for a complete theory T extending TF. As two isomorphic structures are "the same" structure, we will consider the isomorphism classes of models of T. A natural question about the isomorphism classes is "how many?". We try to answer this for the case with cardinality ω. We let $\mathsf{n}(T)$ be the number of isomorphism classes of models of cardinality ω of T.

Let T be a complete theory extending TF with a finite model. Then $\mathsf{n}(T) = 0$, since T has no model of cardinality ω. Let T be a complete theory extending TF without a finite model. Since T is complete, there is at least one model of cardinality ω, so $\mathsf{n}(T) \neq 0$. Since T is not ω–categorical, $\mathsf{n}(T) \neq 1$. By a classical proof in model theory, $\mathsf{n}(T) \neq 2$ ([8, Corollary 21.5]). An algebraically closed field is infinite. We can use algebraic arguments to show that if K is an algebraically closed field, then $\mathsf{n}(\mathsf{Th}\, K) = \omega$.

Proposition 2.3.1. *Let K be an algebraically closed field.*

$$\mathsf{n}(\mathsf{Th}\, K) = \omega$$

Proof. Let A and B be algebraically closed fields of the same characteristic. If $A \cong B$ then the transcendence degrees of A and B are equal. Suppose A and B have the same transcendence degree. Let $\mathbf{K}_A$ and $\mathbf{K}_B$ be the prime subfields of A and B respectively. Then X_A and X_B are transcendence bases of A and B respectively, with a bijection $X_A \longrightarrow X_B$. Then

$$\begin{aligned} \mathbf{K}_A &\leq \mathbf{K}_A(X_A) \leq \overline{\mathbf{K}_A(X_A)} \leq A \\ \mathbf{K}_B &\leq \mathbf{K}_B(X_B) \leq \overline{\mathbf{K}_B(X_B)} \leq B \end{aligned}$$

since A and B are algebraically closed (using [3, Corollary 8.1]). By the assumption that $\mathbf{K}_A \cong \mathbf{K}_B$ and $X_A \longrightarrow X_B$ is a bijection, $\overline{\mathbf{K}_A(X_A)} \cong \overline{\mathbf{K}_B(X_B)}$. Since X_A is a transcendence basis for A, A is an algebraic extension of $\overline{\mathbf{K}_A(X_A)}$. Since X_B is a transcendence basis for B, B is an algebraic extension of $\overline{\mathbf{K}_B(X_B)}$. But then $\overline{\mathbf{K}_A(X_A)} = A$ and $\overline{\mathbf{K}_B(X_B)} = B$, since $\overline{\mathbf{K}_A(X_A)}$ and $\overline{\mathbf{K}_B(X_B)}$ are algebraically closed, so $A \cong B$.

A model of $\mathsf{Th}\, K$ of cardinality ω has either finite or countable infinite transcendence degree over its prime subfield $\mathbf{K}$. So the number of isomorphism classes of models of cardinality ω is at most ω. On the other side, $\mathsf{ACF} \cup \mathsf{Char}_{\mathsf{x}}$ is a complete theory for fixed characteristic x, and thus equal to $\mathsf{Th}\, K$ for some x. Then $\overline{\mathbf{K}(x_1 \ldots x_n)}$ is a model of $\mathsf{Th}\, K$ of cardinality ω for each n, so the number of isomorphism classes of models of cardinality ω is at least ω. □

Infinite fields may have characteristic 0 or prime p. If an infinite field K is algebraically closed, then $\mathsf{n}(\mathsf{Th}\, K) = \omega$, regardless of the characteristic. We now consider $\mathsf{n}(\mathsf{Th}\, K)$ for an infinite field K in the two cases characteristic 0 and characteristic prime p.

2.3.1 Characteristic 0

Let K be a field of characteristic 0. Then K is an infinite field. Also, the least substructure of K is isomorphic to $\mathbf{Q}$. For the field $\mathbf{Q}$, the number of isomorphism classes of models of cardinality ω is not countable.

Proposition 2.3.2.

$$\mathsf{n}(\mathsf{Th}\, \mathbf{Q}) > \omega$$

Proof. Let $\{p_i : i \in \mathbf{N}\}$ be the set of primes. Let T be the complete theory of the $(+, \cdot, 0, 1)$–structure $\mathbf{Q}$. We extend the signature $S = (+, \cdot, 0, 1)$ to S' by adding a new constant symbol $\underline{c}$. For each subset $X \subseteq \mathbf{N}$ we show that there is an S'–structure $\mathbf{Q}'_X$

satisfying

$$T \cup \{ \ \ (\exists x \ \ x^{p_i} = \underline{c}) \ : \ i \in X\}$$
$$\cup \{\neg(\exists x \ \ x^{p_i} = \underline{c}) \ : \ i \notin X\}$$

Let

$$(\exists x \ \ x^{q_1} = \underline{c}) \quad \ldots \quad (\exists x \ \ x^{q_m} = \underline{c})$$
$$\neg(\exists x \ \ x^{r_1} = \underline{c}) \quad \ldots \quad \neg(\exists x \ \ x^{r_n} = \underline{c})$$

be a finite subset of these formulas. Define the S'–structure $\mathbf{Q}'$ by setting $\underline{c} = 2^{q_1 \cdots q_m}$ in $\mathbf{Q}$. We then have

$$\mathbf{Q}' \models (\exists x \ \ x^{q_i} = \underline{c})$$

for all q_i. Conversely, if $(a/b)^r = 2^{q_1 \cdots q_m}$ for some prime r and a, b have no common factor, then $a^r = 2^{q_1 \cdots q_m} b^r$, so $b = 1$, and then $a^r = 2^{q_1 \cdots q_m}$. Since 2 is prime we have $a = 2^s$, $2^{sr} = 2^{q_1 \cdots q_m}$, so $r = q_i$ for some i. Hence

$$\mathbf{Q}' \models \neg(\exists x \ \ x^{r_i} = \underline{c})$$

for all r_i. By the compactness theorem there exists such a structure ${\mathbf{Q}'}_X$. Let c be the element $\underline{c}$ of ${\mathbf{Q}'}_X$, and consider ${\mathbf{Q}'}_X$ as a $(+, \cdot, 0, 1)$–structure $\mathbf{Q}_X$. Let N_X be the 1–type of T realized by the element c in $\mathbf{Q}_X$:

$$N_X = \{F\, y \ : \ \mathbf{Q}_X \models F\, \underline{c}\}$$

If $X_0 \neq X_1$, say $i \in X_0$, $i \notin X_1$, then

$$(\exists x \ \ x^{p_i} = y) \in N_{X_0}$$
$$\neg(\exists x \ \ x^{p_i} = y) \in N_{X_1}$$

and so $N_{X_0} \neq N_{X_1}$. Thus, T has uncountable many 1–types, and by Lemma 2.1.1, $\mathsf{n}(\mathsf{Th}\, \mathbf{Q}) > \omega$. □

The proof of Proposition 2.3.2 can actually be generalized such that it holds for fields of characteristic 0 where the algebraic elements over their prime subfields have bounded degree. Let K be a field of characteristic 0 with prime subfield $\mathbf{K}$. If K has finite algebraic degree over $\mathbf{K}$, then the algebraic elements over $\mathbf{K}$ have bounded degree. If K has infinite algebraic degree over $\mathbf{K}$, there are finite–dimensional algebraic extensions L_n of $\mathbf{K}$ inside K of arbitrary high degrees, and since $\mathbf{K}$ has characteristic 0, $L_n = \mathbf{K}(a_n)$ for some $a_n \in K$, by [2, 51.16 Corollary]. Hence the algebraic elements over $\mathbf{K}$ of K do not have bounded degree. So for a field K with characteristic 0 we have that the algebraic elements of K over its prime subfield have bounded degree if and only if K has finite algebraic degree over its prime subfield. Instead of speaking about fields where the algebraic elements over their prime subfields have bounded degree, we speak about fields with finite algebraic degree over their prime subfields. Below we prove that if K is a field of characteristic 0 with finite algebraic degree over its prime subfield, then $\mathsf{n}(\mathsf{Th}\, K) > \omega$. We need the following lemma.

Lemma 2.3.3. *For distinct primes $r, q_1, \ldots, q_n$, the polynominal*

$$x^r - p^{q_1 \cdots q_n}$$

is irreducible over $\mathbf{Q}$ *for any prime* p.

Proof. This is shown in [9, Beispiele. 1., page 81], using a generalization of Eisenstein criterion by *G. Dumas*. □

Proposition 2.3.4. *Let* K *be a field of characteristic* 0 *where the algebraic elements over its prime subfield have bounded degree.*

$$\mathsf{n}(\mathsf{Th}\, K) > \omega$$

Proof. Let L be the subfield of K consisting of the elements algebraic over its prime subfield $\mathbf{K}$, $\mathbf{K} \leq L \leq K$. By assumption, there is a number d such that if a is an element of L, then $\mathsf{deg}(a,\mathbf{K}) \leq d$. Let $\{s_i : i \in \mathbf{N}\}$ be the set of primes strictly greater than d. Let T be the complete theory of the $(+, \cdot, 0, 1)$–structure K. We extend the signature $S = (+, \cdot, 0, 1)$ to S' by adding a constant symbol $\underline{c}$. For each subset $X \subseteq \mathbf{N}$ we show that there is an S'–structure ${K'}_X$ satisfying

$$\begin{aligned} T \cup \{ \ & (\exists x \ \ x^{s_i} = \underline{c}) : i \in X\} \\ \cup \{ & \neg(\exists x \ \ x^{s_i} = \underline{c}) : i \notin X\} \end{aligned}$$

Let

$$\begin{array}{ccc} (\exists x \ \ x^{q_1} = \underline{c}) & \ldots & (\exists x \ \ x^{q_m} = \underline{c}) \\ \neg(\exists x \ \ x^{r_1} = \underline{c}) & \ldots & \neg(\exists x \ \ x^{r_n} = \underline{c}) \end{array}$$

be a finite subset of these formulas. Define the S'–structure K' by setting $\underline{c} = 2^{q_1 \cdots q_m}$ in K. We then have

$$K' \models (\exists x \ \ x^{q_i} = \underline{c})$$

for all q_i. Suppose $y^{r_i} = 2^{q_1 \cdots q_m}$ for some y in K. Then y is algebraic over $\mathbf{K}$, so $y \in L$. By Lemma 2.3.3, $x^{r_i} - 2^{q_1 \cdots q_m}$ is irreducible over $\mathbf{Q}$, so $\mathsf{deg}(y,\mathbf{K}) = r_i$. But this is a contradiction, since $d < r_i$. Hence

$$K' \models \neg(\exists x \ \ x^{r_i} = \underline{c})$$

for all r_i. By the compactness theorem there exists such a structure ${K'}_X$. Let c be the element $\underline{c}$ of ${K'}_X$ and consider ${K'}_X$ as a $(+, \cdot, 0, 1)$–structure K_X. Let N_X be the 1–type of T realized by the element c in K_X:

$$N_X = \{F\, y : K_X \models F\, \underline{c}\}$$

If $X_0 \neq X_1$, say $i \in X_0, i \notin X_1$, then

$$\begin{aligned} (\exists x \ \ x^{s_i} = y) &\in N_{X_0} \\ \neg(\exists x \ \ x^{s_i} = y) &\in N_{X_1} \end{aligned}$$

and so $N_{X_0} \neq N_{X_1}$. Thus, T has uncountable many 1–types, and by Lemma 2.1.1, $\mathsf{n}(\mathsf{Th}\, K) > \omega$. □

2.3.2 Characteristic prime p

Let K be a field of characteristic prime p with prime subfield $\mathbf{K}$. If K has finite algebraic degree over $\mathbf{K}$, then the algebraic elements over $\mathbf{K}$ have bounded degree. If K has infinite algebraic degree over $\mathbf{K}$, there are finite–dimensional algebraic extensions L_n of $\mathbf{K}$ inside K of arbitrary high degrees, and since $\mathbf{K}$ is a finite field, $L_n = \mathbf{K}(a_n)$ for some $a_n \in K$, by [2, 33.6 Corollary]. Hence the algebraic elements over $\mathbf{K}$ of K do not have bounded degree. So for a field K with characteristic prime p we have that the algebraic elements of K over its prime subfield have bounded degree if and only if K has finite algebraic degree over its prime subfield. Instead of speaking about fields where the algebraic elements over their prime subfields have bounded degree, we speak about fields with finite algebraic degree over their prime subfields.

For an infinite field K of characteristic 0 with finite algebraic degree over its prime subfield $\mathbf{K}$, we proved that $\mathsf{n}(\mathsf{Th}\, K) > \omega$. This might be true for characteristic prime p. An analogous proof to Proposition 2.3.4 will not work, since the subfield of algebraic elements over $\mathbf{K}$ is then a finite-dimensional extension of $\mathbf{K}$, and so a finite field, since $\mathbf{K}$ is a finite field. So an infinite field of characteristic prime p with finite algebraic degree over its prime subfield $\mathbf{K}$ contains an element transcendental over $\mathbf{K}$.

2.3.3 Further work

Suppose K is a field with infinite algebraic degree over its prime subfield. Is necessarily $\mathsf{n}(\mathsf{Th}\, K) > \omega$? The answer to this is negative, we showed in Proposition 2.3.1 that $\mathsf{n}(\mathsf{Th}\, \overline{\mathbf{Q}}) = \omega$.

Suppose K is a field with infinite algebraic degree over its prime subfield. Is necessarily $\mathsf{n}(\mathsf{Th}\, K) = \omega$? The answer to this is negative, in the next section we show that there is a field R of cardinality ω having characteristic 0, with infinite algebraic degree over its prime subfield and $\mathsf{n}(\mathsf{Th}\, R) > \omega$.

Suppose K is a field with infinite algebraic degree over its prime subfield and $\overline{K}$ is a finite extension of K. Is necessarily $\mathsf{n}(\mathsf{Th}\, K) = \omega$? The answer to this is negative, in the next section we show that there is a field R of cardinality ω having characteristic 0, with infinite algebraic degree over its prime subfield, $[\overline{R} : R] = 2$, and $\mathsf{n}(\mathsf{Th}\, R) > \omega$.

We proved that $\mathsf{n}(\mathsf{Th}\, K) = 0$ for a finite field K. For infinite fields we proved that if K is algebraically closed, then $\mathsf{n}(\mathsf{Th}\, K) = \omega$. For other infinite fields K we observed that $\mathsf{n}(\mathsf{Th}\, K) > \omega$. Since mathematics is the study of patterns, we are interested in the following possibility: "If K is an infinite field which is not algebraically closed, then $\mathsf{n}(\mathsf{Th}\, K) > \omega$". At least for the case with characteristic 0. In Proposition 2.3.4, the assumption "finite algebraic degree over its prime subfield" implies a field which is not algebraically closed.

For a complete theory T extending TF, we asked the question "how many?" about the

isomorphism classes of models of cardinality ω. Another natural question about the isomorphism classes is "how do they relate?".

2.4 Ordered fields

The theory of ordered fields TOF is a theory of $(+, \cdot, 0, 1, \leq)$–structures extending TF with

$$\begin{aligned}
&\forall x \forall y \ \ (x \leq y \vee y \leq x) \\
&\forall x \forall y \ \ (x \leq y \wedge y \leq x \longrightarrow x = y) \\
&\forall x \forall y \forall z \ \ (x \leq y \wedge y \leq z \longrightarrow x \leq z) \\
&\forall x \forall y \forall z \ \ (x \leq y \longrightarrow x + z \leq y + z) \\
&\forall x \forall y \ \ (0 \leq x \wedge 0 \leq y \longrightarrow 0 \leq x \cdot y)
\end{aligned}$$

An ordered field is a $(+, \cdot, 0, 1, \leq)$–structure satisfying TOF. The set $P = \{x : 0 \leq x\}$ is the set of positive elements. By $(\forall x \forall y \forall z \ \ (x \leq y \longrightarrow x + z \leq y + z))$, we deduce that $0 \leq x$ implies $(-x) \leq 0$, so either $0 \leq x$ or $0 \leq (-x)$ for an element x. If $0 \leq x$, then $0 \leq x \cdot x = x^2$. If $0 \leq (-x)$, then $0 \leq (-x) \cdot (-x) = x^2$. So squares are positive in an ordered field. In particular, 1 is a square, so

$$\mathsf{TOF} \vdash \ 0 \leq 1$$

Suppose $0 \leq x$ and $0 \leq y$. Then $0 + y \leq x + y$ and so $0 \leq x + y$. Hence a sum of positive elements is positive,

$$\mathsf{TOF} \vdash \ \forall x \forall y \ \ (0 \leq x \wedge 0 \leq y \longrightarrow 0 \leq x + y)$$

Suppose (-1) is a sum of squares, $({x_1}^2 + \cdots + {x_n}^2) + 1 = 0$. Since ${x_1}^2 + \cdots + {x_n}^2$ is a sum of positive elements, (-1) is positive which is a contradiction. Hence (-1) is not a sum of squares in an ordered field. In particular, $(1 + \cdots + 1) + 1 \neq 0$ for $i + 1$ summands, so

$$\mathsf{TOF} \vdash \ \neg C_{i+1}$$

for all i. Hence an ordered field has characteristic 0.

Let K be a $(+, \cdot, 0, 1)$–structure satisfying TF. K is called *real* if (-1) is not a sum of squares. K is called *real closed* if for any algebraic extension L of K with L real we have $L = K$. Let K be a real field. By [6, Theorem XI.2.2] there exists a real closure R of K. By [6, Theorem XI.2.2] any real closed field R can be equipped with an ordering making it an ordered field, in a unique way. Since K is a subfield of R, there is at least one ordering on K making it an ordered field. Hence a $(+, \cdot, 0, 1)$–structure K satisfying TF can be ordered if and only if (-1) is not a sum of squares. In particular, an algebraically closed field can not be ordered.

Proposition 2.4.1. *Let A be an ordered field.*

$$\mathsf{n}(\mathsf{Th}\, A) > \omega$$

Proof. Define the following sets of formulas by

$$\begin{aligned} M_r\, x = \; & \{(m \cdot 1) < x(n \cdot 1) \; : \; m/n < r\} \cup \\ & \{x(n \cdot 1) \leq (m \cdot 1) \; : \; r \leq m/n\} \end{aligned}$$

for each real number $r \in [0, 1)$. Since A has characteristic 0, $\mathbf{Q}$ is a substructure of A, so for each finite subset M of M_r there is an element in A realizing M. Since M_r is a consistent set, there is a 1–type N_r of $\mathsf{Th}\, A$ containing M_r. If $r_0 \neq r_1$ then $M_{r_0} \neq M_{r_1}$ since $\mathbf{Q}$ is dense in A, and so $N_{r_0} \neq N_{r_1}$. Hence $\mathsf{Th}\, A$ has uncountable many 1–types, and so by Lemma 2.1.1, $\mathsf{n}(\mathsf{Th}\, A)$ is not countable. □

Since ordered fields have more structural properties than fields, there are more possibilities of different structures. So we will have a richer set of isomorphism classes when considering an ordered field as a $(+, \cdot, 0, 1, \leq)$–structure rather than a $(+, \cdot, 0, 1)$–structure. From Lemma 2.1.2 we know that if we can express the properties of $(\leq)$ in the language of $(+, \cdot, 0, 1)$, the two sets of isomorphism classes will be "equal". This fact is used in the two results below. The first one is an alternative proof to Proposition 2.3.2 that $\mathsf{n}(\mathsf{Th}\, \mathbf{Q}) > \omega$. The second is a proof that $\mathsf{n}(\mathsf{Th}\, \mathbf{R}) > \omega$.

Proposition 2.4.2. *For the $(+, \cdot, 0, 1)$–structure $\mathbf{Q}$ we have*

$$\mathsf{n}(\mathsf{Th}\, \mathbf{Q}) > \omega$$

Proof. Let $(\mathbf{Q}, \leq)$ be the $(+, \cdot, 0, 1, \leq)$–structure of the rational numbers. Let P be the predicate

$$\begin{aligned} P\, x = \; & \exists a_1 \exists a_2 \exists a_3 \exists a_4 \exists b_1 \exists b_2 \exists b_3 \exists b_4 \\ & ({a_1}^2 + {a_2}^2 + {a_3}^2 + {a_4}^2) = x({b_1}^2 + {b_2}^2 + {b_3}^2 + {b_4}^2) \end{aligned} \tag{2.1}$$

If $P\, x$ holds then x is positive, since both sums ${a_1}^2 + {a_2}^2 + {a_3}^2 + {a_4}^2$ and ${b_1}^2 + {b_2}^2 + {b_3}^2 + {b_4}^2$ are positive. Conversely, let x by a positive element. Then $x = m/n$ for positive integers m and n. By Lagrange's theorem, every positive integer r can be written as a sum ${r_1}^2 + {r_2}^2 + {r_3}^2 + {r_4}^2$ where r_i are positive integers. Hence $P\, x$ holds. We notice that

$$(\mathbf{Q}, \leq) \models x \leq y \longleftrightarrow \forall z \;\; (x + z = y \longrightarrow P\, z)$$

so the relation $(\leq)$ can be defined in the language given by the signature $(+, \cdot, 0, 1)$. By Proposition 2.4.1, there are uncountable many $(+, \cdot, 0, 1, \leq)$–isomorphism classes of $\mathsf{Th}\, (\mathbf{Q}, \leq)$, and by Lemma 2.1.2 these are "the same" as the $(+, \cdot, 0, 1)$–isomorphism classes of $\mathsf{Th}\, \mathbf{Q}$. So $\mathsf{n}(\mathsf{Th}\, \mathbf{Q})$ is uncountable for the $(+, \cdot, 0, 1)$–structure $\mathbf{Q}$. □

Proposition 2.4.3. *For the* $(+, \cdot, 0, 1)$*–structure* $\mathbf{R}$ *we have*

$$\mathsf{n}(\mathsf{Th}\,\mathbf{R}) > \omega$$

Proof. Let $(\mathbf{R}, \leq)$ be the $(+, \cdot, 0, 1, \leq)$–structure of the real numbers. We notice that

$$(\mathbf{R}, \leq) \models x \leq y \longleftrightarrow \exists z \;\; x + z^2 = y$$

so the relation $(\leq)$ can be defined in the language given by the signature $(+, \cdot, 0, 1)$. By Proposition 2.4.1, there are uncountable many $(+, \cdot, 0, 1, \leq)$–isomorphism classes of $\mathsf{Th}\,(\mathbf{R}, \leq)$, and by Lemma 2.1.2 these are "the same" as the $(+, \cdot, 0, 1)$–isomorphism classes of $\mathsf{Th}\,\mathbf{R}$. So $\mathsf{n}(\mathsf{Th}\,\mathbf{R})$ is uncountable for the $(+, \cdot, 0, 1)$–structure $\mathbf{R}$. □

2.4.1 A countable field R

We now show that there is a field R of cardinality ω having characteristic 0, such that R has infinite algebraic degree over its prime subfield $\mathbf{K}$, $[\overline{R} : R] = 2$, and $\mathsf{n}(\mathsf{Th}\,R) > \omega$. Let R be a model of $\mathbf{R}$ of cardinality ω (downward Löwenheim–Skolem). Then $\mathsf{n}(\mathsf{Th}\,R) > \omega$ as proven above. For each prime p, the polynominal $x^p - 2$ is irreducible over $\mathbf{Q}$ by Lemma 2.3.3. Since $\mathbf{R} \models \exists x \;\; x^p = (1 + 1)$ and R is a model of $\mathsf{Th}\,\mathbf{R}$, there are elements in R of algebraic degree p over $\mathbf{K}$ for any prime p. Hence R has infinite algebraic degree over its prime subfield. Let $R(i)$ be R extended with a root of $x^2 + 1$. We now show that $R(i)$ is the algebraic closure of R, and so $[\overline{R} : R] = 2$.

Lemma 2.4.4. *Let* R *be a model of* $\mathsf{Th}\,\mathbf{R}$*. Every element in* $R(i)$ *has a square root.*

Proof. Let $a + ib$ be an element of $R(i)$. For all x, y in $\mathbf{R}$ there are elements

$$z = \sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}}$$

$$w = \sqrt{\frac{-x + \sqrt{x^2 + y^2}}{2}}$$

in $\mathbf{R}$ with the indicated properties. Therefore, since R is a model of $\mathsf{Th}\,\mathbf{R}$, there are elements

$$c = \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \tag{2.2}$$

$$d = \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \tag{2.3}$$

in R with the indicated properties. By computing

$$\begin{aligned}(2cd)^2 &= 4c^2d^2 \\ &= 4\left(\frac{a+\sqrt{a^2+b^2}}{2}\right)\left(\frac{-a+\sqrt{a^2+b^2}}{2}\right) \\ &= (a+\sqrt{a^2+b^2})(-a+\sqrt{a^2+b^2}) \\ &= -a^2+(a^2+b^2) \\ &= b^2\end{aligned}$$

we see that either $2cd = b$ or $(-2cd) = b$. If $(-2cd) = b$, we can set c to $(-c)$. So there are elements c, d in R having properties (2.2), (2.3) and $2cd = b$. We then have

$$(c+id)^2 = (c^2-d^2)+i(2cd)$$

and so

$$2cd = b$$

and

$$\begin{aligned}c^2-d^2 &= \frac{a+\sqrt{a^2+b^2}}{2} - \frac{-a+\sqrt{a^2+b^2}}{2} \\ &= \frac{2a}{2} \\ &= a\end{aligned}$$

□

The following algebraic proof of the fundamental theorem of algebra, found in [10], shows that $R(i)$ is algebraically closed:

Theorem 2.4.5. *Let R be a model of $\mathsf{Th}\,\mathbf{R}$.*

$$\overline{R} = R(i)$$

Proof. Let R be a model of $\mathsf{Th}\,\mathbf{R}$. We show that there is no proper finite algebraic extension of $R(i)$. Let $K : R(i)$ be a finite extension, then $K : R$ is a finite extension and by [3, Corollary 9.2] there is a field extension $K' : K : R$ such that K' is a finite normal extension of R. R has characteristic 0, so $K' : R$ is also separable, and we can then form the Galois group $G = \mathsf{Gal}(K' : R)$, which has finite order. Let H be a Sylow 2–group of G. Then the order of H is a power of 2, and the index of H in G is odd. By Galois theory, there is a subextension $K' : L : R$ such that $\mathsf{Gal}(K' : L) = H$. Since $[L : R] = [G : H]$ is odd and every polynominal in R of odd degree has a root, $[L : R] = 1$, so $[K' : R] = [K' : L][L : R] = [K' : L] = |H|$. Since also $[K' : R] = [K' : R(i)][R(i) : R]$, the degree of K' over $R(i)$ must be a power of 2. So the Galois group $G' = \mathsf{Gal}(K' : R(i))$

has order a power of 2. Since every element in $R(i)$ has a square root by Lemma 2.4.4, every polynominal of degree 2 in $R(i)$ splits by using the quadratic formula. Hence there is no extension of $R(i)$ of degree 2. Suppose G' is not trivial. Then by Sylow theorems, the group $\mathsf{Gal}(K' : R(i))$ contains a subgroup of order 2. But then K' is an extension of $R(i)$ of degree 2, which is a contradiction. Hence G' is trivial, so $K' = R(i)$, and also $K = R(i)$. □

2.5 Elementary equivalence

Let A, B be structures with signature S. If for all sentences F in the language we have

$$A \models F \iff B \models F$$

then A and B are said to be elementary equivalent, and we write $A \equiv B$. An equivalent condition is $\mathsf{Th}\, A = \mathsf{Th}\, B$. If A and B are isomorphic, then they surely are elementary equivalent. But the converse, if A and B are elementary equivalent they are isomorphic, is not true. Let T be a complete theory. If A and B are models of T, they are elementary equivalent.

Let K be a field. We are only able to express algebraic statements about elements in K with our language. This is obvious, since we consider a $(+, \cdot, 0, 1)$–structure K. One might therefore think that extending a field K with a transcendental element c, giving a field $K(c)$, gives us an elementary equivalent field. This is not true, since we can describe algebraic properties between elements, and these elements can be transcendental, as the following example shows.

Example 2.5.1. With $K = \mathbf{F}_2$ we have

$$K \models \forall x \exists y \;\; y^2 = x$$
$$K(c) \not\models \forall x \exists y \;\; y^2 = x$$

since there is no element y in $\mathbf{F}_2(c)$ such that $y^2 = c$.

Consider the field $\mathbf{Q}$. Are $\mathbf{Q}$ and $\mathbf{Q}(c)$ elementary equivalent? Suppose they are isomorphic, so $\phi : \mathbf{Q} \longrightarrow \mathbf{Q}(c)$ is an isomorphism. Since ϕ is a $(+, \cdot, 0, 1)$–homomorphism between fields, we have $\phi\, 1 = 1$ and so also $\phi\,(m/n) = m/n$ for all m/n. Hence ϕ is not a surjection, which is a contradiction. The following can be said about elements in the extension $\mathbf{Q}(c)$ of $\mathbf{Q}$:

Proposition 2.5.2. *Every element in* $\mathbf{Q}(c)$ *which is not in* $\mathbf{Q}$ *is transcendental over* $\mathbf{Q}$.

Proof. Let x be an element in $\mathbf{Q}(c)$, $x = (\frac{p\,c}{q\,c})$ for some p, q in $\mathbf{Q}[c]$ with no common

factor of non–zero degree. Suppose for some $a_0 \ldots a_n$ in $\mathbf{Q}$ we have

$$\left(\frac{p\,c}{q\,c}\right)^{n+1} + a_n\left(\frac{p\,c}{q\,c}\right)^{n} + \cdots + a_0 = \frac{(p\,c)^{n+1} + a_n(q\,c)(p\,c)^n + \cdots + a_0(q\,c)^{n+1}}{(q\,c)^{n+1}}$$
$$= 0$$

This gives

$$(p\,c)^{n+1} + a_n(q\,c)(p\,c)^n + \cdots + a_0(q\,c)^{n+1} = 0$$

and so

$$(-a_n)(q\,c)(p\,c)^n + \cdots + (-a_0)(q\,c)^{n+1} = (p\,c)^{n+1}$$

Now $(q\,c)$ divides $(p\,c)^{n+1}$, so $(q\,c)$ has zero degree, $(q\,c) = b$ for some $b \in \mathbf{Q}$. This means that

$$(p\,c)^{n+1} + (a_n b)(p\,c)^n + \cdots + (a_0 b) = 0$$

and since c is transcendental over $\mathbf{Q}$, $(p\,c)$ must have zero degree, $(p\,c) = d$ for some $d \in \mathbf{Q}$. So $x = d/b$ is an element of $\mathbf{Q}$. □

We now show that $\mathbf{Q}$ and $\mathbf{Q}(c)$ are not elementary equivalent, we find a sentence F such that $\mathbf{Q} \models F$ and $\mathbf{Q}(c) \not\models F$. Recall the predicate P defined in (2.1) on page 29. We know that the predicate $P\,x$ holds in $\mathbf{Q}$ if and only if $0 \leq x$. So the sentence

$$F = \forall x \;\; (P\,x \vee \forall y \;\; (x + y = 0 \longrightarrow P\,y))$$

saying that for any element x of $\mathbf{Q}$, either x or $(-x)$ is positive, holds in $\mathbf{Q}$. But the sentence F does however not hold in $\mathbf{Q}(c)$.

Proposition 2.5.3.

$$\mathbf{Q}(c) \not\models \forall x \;\; (P\,x \vee \forall y \;\; (x + y = 0 \longrightarrow P\,y))$$

Proof. Suppose $P\,c$ is true in $\mathbf{Q}(c)$, then

$$\left(\frac{p_1\,c}{q_1\,c}\right)^2 + \left(\frac{p_2\,c}{q_2\,c}\right)^2 + \left(\frac{p_3\,c}{q_3\,c}\right)^2 + \left(\frac{p_4\,c}{q_4\,c}\right)^2 =$$
$$c\left(\left(\frac{r_1\,c}{s_1\,c}\right)^2 + \left(\frac{r_2\,c}{s_2\,c}\right)^2 + \left(\frac{r_3\,c}{s_3\,c}\right)^2 + \left(\frac{r_4\,c}{s_4\,c}\right)^2\right)$$

for polynominals in $\mathbf{Q}[c]$. Hence

$$\frac{(p_1\,c)^2}{(q_1\,c)^2}+\frac{(p_2\,c)^2}{(q_2\,c)^2}+\frac{(p_3\,c)^2}{(q_3\,c)^2}+\frac{(p_4\,c)^2}{(q_4\,c)^2}=$$
$$c\left(\frac{(r_1\,c)^2}{(s_1\,c)^2}+\frac{(r_2\,c)^2}{(s_2\,c)^2}+\frac{(r_3\,c)^2}{(s_3\,c)^2}+\frac{(r_4\,c)^2}{(s_4\,c)^2}\right)$$

and multiplying out we get

$$\begin{aligned}&(p_1\,c)^2(q_2\,c)^2(q_3\,c)^2(q_4\,c)^2(s_1\,c)^2(s_2\,c)^2(s_3\,c)^2(s_4\,c)^2+\\&(p_2\,c)^2(q_1\,c)^2(q_3\,c)^2(q_4\,c)^2(s_1\,c)^2(s_2\,c)^2(s_3\,c)^2(s_4\,c)^2+\\&(p_3\,c)^2(q_1\,c)^2(q_2\,c)^2(q_4\,c)^2(s_1\,c)^2(s_2\,c)^2(s_3\,c)^2(s_4\,c)^2+\\&(p_4\,c)^2(q_1\,c)^2(q_2\,c)^2(q_3\,c)^2(s_1\,c)^2(s_2\,c)^2(s_3\,c)^2(s_4\,c)^2=\end{aligned}$$

$$\begin{aligned}c\,(\,&(r_1\,c)^2(s_2\,c)^2(s_3\,c)^2(s_4\,c)^2(q_1\,c)^2(q_2\,c)^2(q_3\,c)^2(q_4\,c)^2+\\&(r_2\,c)^2(s_1\,c)^2(s_3\,c)^2(s_4\,c)^2(q_1\,c)^2(q_2\,c)^2(q_3\,c)^2(q_4\,c)^2+\\&(r_3\,c)^2(s_1\,c)^2(s_2\,c)^2(s_4\,c)^2(q_1\,c)^2(q_2\,c)^2(q_3\,c)^2(q_4\,c)^2+\\&(r_4\,c)^2(s_1\,c)^2(s_2\,c)^2(s_3\,c)^2(q_1\,c)^2(q_2\,c)^2(q_3\,c)^2(q_4\,c)^2\,)\end{aligned}$$

Consider the two sums of products of squared polynominals. The leading coefficient of a squared polynominal is positive, and its degree is even. Multiplying two polynominals of even degree with positive leading coefficients, gives a polynominal of even degree with positive leading coefficient. Hence the two sums of products of squared polynominals do both have even degree. But now the left side has even degree and the right side has odd degree, which is a contradiction. The same argument goes for $P\,(-c)$. Hence neither $P\,c$ nor $P\,(-c)$ is true, so the sentence F is false in $\mathbf{Q}(c)$. □

Bibliography

[1] C.C. Chang and H.J. Keisler. Model Theory. North–Holland Publishing Company, 1973.

[2] John B. Fraleigh. A First Course in Abstract Algebra. Seventh Edition. Addison Wesley, 2003.

[3] D.J.H Garling. A Course in Galois Theory. Cambrigde University Press, 1986.

[4] Jr. Hartley Rogers. Theory of Recursive Functions and Effective Computability. McGraw-Hill Book Company, 1967.

[5] Wilfrid Hodges. Model Theory. Cambridge University Press, 1993.

[6] Serge Lang. Algebra. Revised Third Edition. Springer–Verlag, 2005.

[7] David Marker. Model Theory: An Introduction. Springer-Verlag, 2002.

[8] Gerald E. Sacks. Saturated Model Theory. W. A. Benjamin, Inc., 1972.

[9] B.L van der Waerden. Moderne Algebra, Erster Teil, Zweite verbesserte Auflage. Verlag von Julius Springer, 1937.

[10] Wikipedia. `http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra#Algebraic_proofs`, October 2011.