Solutions: Sheet 1

Exercise 1

Let K be a fixed field. Define a language $\mathcal{L}$ such that K-vector spaces are naturally $\mathcal{L}$-structures.

Lösung:

Consider the infinite language $\mathcal{L} = \{0, (+, 2), (m_k, 1) \colon k \in K\}$. Given a vector space $(V, 0, +, \cdot)$, where $\cdot$ is the scalar multiplication, we interprete 0 and $+$ as they are in V and define $(m_k) \colon V \to V$ by $v \mapsto k \cdot v$ for every $k \in K$.

Exercise 2

Let $\mathcal{L}_\mathrm{r} = (+, -, \cdot, 0, 1)$ be the language of rings.

(a) Explain why the notion of isomorphic rings (considered as $\mathcal{L}_\mathrm{r}$-structures in the obvious way) corresponds to that of isomorphism in the usual algebraic sense.

(b) Show that if we consider a field as an $\mathcal{L}_\mathrm{r}$-structure, the substructures do not coincide with the subfields.

Lösung:

(a) Since $\mathcal{L}_r$ does not contain relation symbols, the definition of an isomorphism of $\mathcal{L}_r$-structures is the same as the definition of a ring-homomorphism (we use the definition of bijective ring-homorphism and not that there exists a morphism in both directions here).

(b) Indeed the ring $\mathbb{Z}$ is a $\mathcal{L}_r$-substructure of the field $\mathbb{Q}$, but $\mathbb{Z}$ is not a subfield of $\mathbb{Q}$. It holds that every subfield is a $\mathcal{L}_r$ substructure.

Exercise 3

In the language $(\cdot, e)$ of groups, show that there exists a sentence ϕ such that $\mathcal{M} \models \phi$ if and only if $\mathcal{M}$ if isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lösung:
Consider the sentence

$$\phi = \exists v_1 v_2 v_3 v_4 \bigwedge_{i \neq j} \neg(v_i = v_j) \wedge \forall v_5 \bigvee_{i=1}^{4} v_i = v_5 \wedge \bigwedge_{i=1}^{4} v_i \cdot v_i = e$$

that states that there are four mutually distinct elements and only four that all have order 2. By the classification of finite groups we know that there are only two groups with order 4 and only in one of them $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ do all elements have order 2.

Exercise 4

Find an axiomatization of integral domains in the language of rings, i.e., a set $\mathcal{A}$ of sentences in the language of rings such that a ring A is an integral domain if and only if $A \models \phi$ for all $\phi \in \mathcal{A}$.

Lösung:
We first need the axioms for a ring (ring with 1):

$$\begin{aligned}
&\phi_0\colon \neg 0 = 1\\
&\phi_1\colon \forall abc\colon (a+b)+c = a+(b+c)\\
&\phi_2\colon \forall a\colon 0+a = a \wedge a+0 = a\\
&\phi_3\colon \forall a \exists b\colon a+b = 0\\
&\phi_4\colon \forall ab\colon a+b = b+a\\
&\phi_5\colon \forall abc\colon (a\cdot b)\cdot c = a\cdot(b\cdot c)\\
&\phi_6\colon \forall a\colon 1\cdot a = a \wedge a\cdot 1 = a\\
&\phi_7\colon \forall abc\colon (a+b)\cdot c = (a\cdot c)+(b\cdot c) \wedge a\cdot(b+c) = (a\cdot b)+(a\cdot c)
\end{aligned}$$

An integral domain additionally satisfies

$$\begin{aligned}
&\phi_8\colon \forall ab\colon a\cdot b = b\cdot a\\
&\phi_9\colon \forall ab\colon a = 0 \vee b = 0 \vee \neg a\cdot b = 0
\end{aligned}$$

Then $\mathcal{A} = \{\phi_i\colon i \in \{0,\dots,9\}\}$ is an axiomatisation of integral domains in the language of rings.

Exercise 5

Find a language $\mathcal{L}$ and a sentence ϕ in $\mathcal{L}$ such that the set of cardinalities of the finite $\mathcal{L}$-structures that satisfy ϕ coincides with the set of powers of primes (excluding $p^0 = 1$).

Lösung:
We note that finite fields always have order a power of a prime. This is because every field F has a prime number p as the characteristic and every finite field is also a finite-dimensional vectorspace over that field. Finite dimensional vectorspaces are isomorphic to F^n, which has $|F|^n = p^n$ many elements.

To describe fields we use the language of rings $\mathcal{L}$ and we can use the axioms $\phi_0, \dots, \phi_8$ from the solution to the previous exercise, but we have to also add in

$$\psi_1 = \forall ab\colon a \cdot b = b \cdot a$$
$$\psi_2 = \forall a\colon a = 0 \vee \exists b(a \cdot b) = 1$$

The sentence

$$\phi = \bigwedge_{i=0}^{8} \phi_i \wedge \psi_1 \wedge \psi_2$$

is an $\mathcal{L}$-sentence and every finite $\mathcal{L}$-structure satisfying ϕ is a finite field and hence has order a prime power. On the other hand, for every prime power there is a finite field with that order. These can be constructed as $\mathbb{F}_p[X]/f(X)$, where $f(X)$ is an irreducible polynomial.

Exercise 6

In the language $\mathcal{L} = (+, 0)$ (with $+$ a binary function and 0 a constant), show that there exists a sentence ϕ such that $\mathbb{Z} \times \mathbb{Z} \models \phi$ but $\mathbb{Z} \not\models \phi$ (we say that $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}$ are *not elementarily equivalent*)

Lösung:
We note that the sum of two odd elements in $\mathbb{Z}$ is even. However, in $\mathbb{Z} \times \mathbb{Z}$, the elements $(1, 0)$ and $(0, 1)$ should be considered odd (not divisible by 2), but also $(1, 0) + (0, 1) = (1, 1)$ is odd. The sentence

$$\phi = \forall ab\colon (\neg\exists a'\colon a' + a' = a \wedge \neg\exists b'\colon b' + b' = b) \to \exists c\colon c + c = a + b$$

encodes this.

Exercise 7

Let $\mathcal{L}_r = (+, -, \cdot, 0, 1)$ be the language of rings. Let $\mathcal{M} = \mathbb{C}(T)$ viewed as an $\mathcal{L}_r$-structure in the obvious way.

(a) Show that there do not exist non-constant rational functions $f, g \in \mathbb{C}(T)$ such that $g^2 = f^3 + 1$.

(b) Deduce that the formula $\phi(v) = \exists x \exists y\colon (y^2 = v \wedge x^3 + 1 = v)$ has the property that $\phi(\mathbb{C}(T)) = \mathbb{C}$ (so the field of constants is definable in $\mathbb{C}(T)$.)

Lösung:

(a) We give two proofs. One uses Algebraic Geometry, the other is elementary, but rather long.

Proposition 0.1. There are no non-constant rational functions f, g in $\mathbb{C}(T)$ such that
$$f^2 = g^3 + 1.$$

Algebraic geometry. If one knows some algebraic geometry, the argument is that (f, g) would define a non-constant morphism of curves

$$\mathbf{A}^1 - \{\text{poles of } f \text{ or } g\} \to E$$

where E is the (projective) elliptic curve with Weierstrasse equation $y^2 = x^3+1$. But then this would extend to a non-constant morphism of curves $\mathbf{P}^1 \to E$ (by known properties of projective curves), and this is not possible since the genus can only decrease under such morphisms, but the genus of $\mathbf{P}^1$ is 0 and that of E is 1. □

Descent. Writing $f = a/b$ and $g = c/d$ with $(a, b) = (c, d) = 1$ (coprime), the equation becomes

$$a^2d^3 = c^3b^2 + b^2d^3 = b^2(c - d)(d - \zeta d)(c - \zeta^2 d)$$

where $\zeta = e^{2i\pi/3}$.

We have $b^2 \mid a^2d^3$ and b is coprime to a so $b^2 \mid d^3$. Similarly, from the fact that $d^3 \mid b^2(c - d)(c - \zeta d)(c - \zeta^2 d)$, but d is coprime to c so also coprime to each of the three factors $c - \zeta^j d$, we deduce that $d^3 \mid b^2$. Combining, we conclude that in fact $b^2 = \alpha d^3$ for some $\alpha \in \mathbb{C}^\times$. The polynomial equation becomes

$$a^2 = \alpha(c - d)(c - \zeta d)(c - \zeta^2 d). \tag{1}$$

We now claim that there exist β, γ, δ in $\mathbb{C}^\times$ such that

$$\alpha d, \quad \beta(c - d), \quad \gamma(c - \zeta d), \quad \delta(c - \zeta^2 d)$$

are all squares in $\mathbb{C}[T]$.

For the first, this follows from $\alpha d = (b/d)^2$ (and because a polynomial which is the square of a rational function is the square of a polynomial).

For the others, this follows from (1) and unique factorization in $\mathbb{C}[T]$, since all three factors $c - d$, $c - \zeta d$ and $c - \zeta^2 d$ are pairwise coprime (the equation implies that the order of vanishing of any of the three polynomials at any point is even, and only one can be non-zero).

Now the lemma which follows gives the result.

□

Lemma 0.2. Let c, d be coprime polynomials in $\mathbb{C}[T]$. Assume that there exist combinations $\lambda_i c + \mu_i d$ which are squares for $1 \leq i \leq 4$, with the lines $\lambda_i X + \mu_i Y = 0$ distinct. Then c and d are constant.

Proof. If the statement is wrong, then there is a pair of polynomials (c, d) satisfying the conditions with $\max(\deg(c), \deg(d))$ *minimal* and positive. We will see that this is impossible by *infinite descent.* To do this, assume that (c, d) is chosen with this property.

By linear changes of variables, we can assume that for some $\lambda \notin \{0,1\}$, the polynomials

$$c, \quad c-d, \quad c-\lambda d, \quad d$$

are squares (this will note change $\max(\deg(c),\deg(d))$. We then see in particular that if c or d is constant, then so is the other so both c and d are non-constant.

We write $c=\gamma^2$ and $d=\delta^2$; the polynomials γ and δ are coprime, and

$$\max(\deg(\gamma),\deg(\delta)) < \max(\deg(c),\deg(d)).$$

Now observe that

$$c-d=\gamma^2-\delta^2=(\gamma-\delta)(\gamma+\delta)$$

but $c-d$ is a square and $\gamma-\delta$ is coprime to $\gamma+\delta$, so that both $\gamma-\delta$ and $\gamma+\delta$ are squares.

Similarly, we can write

$$c-\lambda d=u^2-\lambda v^2=(u-\mu v)(u+\mu v)$$

where $\mu^2=\lambda$. The left-hand side is a square, the two factors on the right are coprime (because $\mu\neq 0$) so they are both squares.

We thus have the two polynomials γ and δ such that

$$\gamma-\delta, \quad \gamma+\delta, \quad \gamma-\mu\delta, \quad \gamma+\mu\delta,$$

are all squares, but have smaller $\max(\deg(\gamma),\deg(\delta))$ than before, which is a contradiction (note that the coefficients do define four different lines since $\lambda\neq 1$).

□

(b) We have

$$\phi(\mathbb{C}(T))=\{v\in\mathbb{C}(T)\colon \mathbb{C}(T)\models\phi(v)\}$$

We note that every constant function satisfies ϕ due to the fundamental theorem of algebra. On the other hand, if $v\in\mathbb{C}(T)$ is a function that satisfies ϕ, then we have other functions $f,g\in\mathbb{C}(T)$ with $g^2(T)=v(T)=f^3(T)+1$. From (a) we conclude that f and g must be constant and hence also $v=g^2$ is constant.