Solutions: Sheet 3

Exercise 1

Let $\mathcal{L} = (+, -, \cdot, 0, 1)$ be the language of rings, and let T be the $\mathcal{L}$-theory of finite fields, namely, the theory whose sentences are those $\mathcal{L}$-sentences ϕ such that $E \models \phi$ for *all* finite fields E.

(a) Show that T has models of characteristic 0, and infinite models of characteristic p for any prime number p.

Solution:
For a model of characteristic 0 we can choose a non-principal ultrafilter on the prime numbers and use the ultraproduct $C = \hat{\prod}_{\mathcal{F}} \mathbb{F}_p$ over the finite fields $\mathbb{F}_p$. Since all sentences in T are satisfied in all finite fields $\mathbb{F}_p$, and $\emptyset \notin \mathcal{F}$, by Łos theorem, $C \models T$.

For characteristic p we can choose finite fields of order p^n of characteristic p and a non-principal ultrafilter on the natural numbers. By the same argument as above the ultraproduct is a model of T and the ultraproduct is infinite as it contains subfields of size p^n for increasing n.

(b) Show that any model of T is a perfect field (i.e., it is either of characteristic 0, or the Frobenius morphism $x \mapsto x^p$ is surjective).

Solution:
We first note that for finite fields of characteristic p, the Frobenius map $x \mapsto x^p$ is a homomorphism (this can be seen by binomial-expansion). In finite fields of characteristic p, the Frobenius homomorphism has trivial kernel (since otherwise we there would be zero-divisors) and hence is injective. An injective map from a finite set to itself is also surjective, hence the $\mathcal{L}$-sentences

$$\varphi_p \quad = \quad \underbrace{1 + 1 + \ldots + 1}_{p-\text{times}} = 0 \to \forall y \exists x, \underbrace{x \cdot x \cdots x}_{p-\text{times}} = y$$

holds in every finite field, hence also holds in every model of T. If the characteristic of a model $\mathcal{M} \models T$ is $p \neq 0$, then $\mathcal{M} \models \varphi_p$ and hence the Frobenius-map is surjective.

(c) Let K be a field. Show that for every integer $n \geq 1$, there exists a formula $\phi_n(v_0, \ldots, v_{n-1})$ such that that $K \models \phi_n(a_0, \ldots, a_{n-1})$ if and only if the polynomial

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = 0$$

is irreducible.

Solution:
A polynomial $f(X) = \sum v_i X^i$ is irreducible iff for any polynomials h, g, $h(X) \cdot g(X) = f(X)$ implies that h or g are constant polynomials.

$$\begin{aligned}\phi_n(v_0, \dots, v_{n-1}) \quad = \quad & \forall b_0, \dots, b_n, c_0, \dots, c_n, \\ & \left(\forall x, \left(\sum_{i=0}^{n} b_i x^i\right) \cdot \left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} v_i x^i\right) \to \\ & \bigwedge_{i=1}^{n} b_i = 0 \ \vee \bigwedge_{i=1}^{n} c_i = 0\end{aligned}$$

(d) Show that if K is a model of T, then K is not algebraically closed, and in fact admits for any $n \geq 1$ at least one extension of degree n in an algebraic closure $\bar{K}$ of K.

Solution:
Finite fields are not algebraically closed, so there exists an irreducible polynomial. In fact for every n, there exists an irreducible polynomial of degree n This can be formulated as an $\mathcal{L}$-sentence

$$\exists v_0, \dots, v_{n-1}, \phi_n(v_0, \dots, v_{n-1})$$

and hence also holds in any model of T. Hence no model of T is algebraically closed.

(e) Show that there exist formulas $\pi_n(v, a, b, c)$ (resp. $\mu_n(v, a, b, c)$), where for $I = \{0, 1, \dots, n-1\}$, $v = (v_i)_{i \in I}$, $a = (a_i)_{i \in I}$, $b = (b_i)_{i \in I}$ and $c = (c_i)_{i \in I}$ are variables, such that if K is a model of T and v, a, b, $c \in K^n$, then $K \models \pi_n(v, a, b, c)$ if and only if

$$\sum_{i=0}^{n-1} a_i \alpha^i + \sum_{i=0}^{n-1} b_i \alpha^i = \sum_{i=0}^{n-1} c_i \alpha^i,$$

resp. $K \models \mu_n(v, a, b, c)$ if and only if

$$\left(\sum_{i=0}^{n-1} a_i \alpha^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i \alpha^i\right) = \sum_{i=0}^{n-1} c_i \alpha^i,$$

where α is the class of X in the ring

$$K[X]/(v_0 + v_1 X + \cdots + v_{n-1} X^{n-1} + X^n).$$

Hint: multiplication by α can be expressed as a matrix acting on the vectorspace $K_n[X]$.

Solution:
The elements of $K[X]/f(X)$ can be expressed as $a = \sum_{i=0}^{n-1} a_i\alpha^i$, where α is the class of X in $K[X]/f(X)$ and $f(X) = \sum v_i X^i$. The sum of two such elements coincides with the sum in $K[X]/f(X)$ viewed as a K-vectorspace. Hence

$$\pi_n(v,a,b,c) \quad = \quad \bigwedge_{i=0}^{n-1} a_i + b_i = c_i$$

is an $\mathcal{L}$-formula describing the addition. The multiplication is more complicated, as for instance

$$\alpha^{n-1}\cdot\alpha^{n-1} = \alpha^{2n-2} = \alpha^n\alpha^{n-2} = \left(-\sum_{i=0}^{n-1} v_i\alpha^i\right)\cdot\alpha^{n-2} = \dots$$

is not straightforward to calculate. The trick is to see multiplication by α as a matrix-multiplication on the vectorspace $K[X]/f(X)$. In facht we have

$$\alpha\cdot a = b \quad\iff\quad \begin{pmatrix} 0 & & & & & -v_0 \\ 1 & 0 & & & & -v_1 \\ & 1 & \ddots & & & \vdots \\ & & \ddots & & & \\ & & & 1 & 0 & -v_{n-2} \\ & & & & 1 & -v_{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

and the equation for $\mu_n(v,a,b,c)$ becomes a system of linear equations which can be expressed in a $\mathcal{L}$-formula, but becomes quite complicated.

(f) Show that there is a $\mathcal{L}$-formula $\theta_n(w,v,a,b)$ expressing that $f(a) = b \in K[X]/g(X)$, where

$$f(X) = \sum_{i=0}^{n} v_i X^i, \quad g(X) = \sum_{i=0}^{n} w_i X^i$$

are two monic polynomials of degree n.

Solution:
We write

$$a = \sum_{i=0}^{n-1} a_i\alpha^i \quad \text{and} \quad b = \sum_{i=0}^{n-1} b_i\alpha^i,$$

where α is the class of X in $K[X]/g(X)$. We introduce new variables $a^\ell = ((a^\ell)_0, (a^\ell)_1, \dots, (a^\ell)_{n-1})$ for $0 \le \ell \le n$ for the powers of a

$$a^\ell = \sum_{i=0}^{n-1} (a^\ell)_i\alpha^i \in K[X]/g(X).$$

Using (e) we can formulate this as a $\mathcal{L}$-formula by writing

$$\begin{aligned}\theta_{n,1}(w,a,a^0,\dots,a^n) \quad &= \quad (a^0)_0 = 1 \wedge \bigwedge_{i=1}^{n-1}(a^0)_i = 0 \wedge \bigwedge_{i=0}^{n-1}(a^1)_i = a_i \\ &\wedge \bigwedge_{\ell=2}^{n} \mu_n(w,a,a^{\ell-1},a^\ell)\end{aligned}$$

Next we introduce new elements $c^\ell = ((c^\ell)_0,(c^\ell)_1,\dots,(c^\ell)_{n-1})$ for $0 \le \ell \le n$ such that

$$c^\ell = \sum_{i=0}^{\ell} v_i a^i \in K[X]/g(X),$$

which we can write as a $\mathcal{L}$-sentence by

$$\begin{aligned}\theta_{n,2}(w,v,a,a^0,\dots,a^n,c^0,\dots,c^n) \quad &= \\ &(c^0)_0 = v_0 \wedge \bigwedge_{i=1}^{n}(c^0)_i = 0 \wedge \\ &\bigwedge_{\ell=1}^{n} \pi_n(w,c^{\ell-1},(v_\ell\cdot(a^\ell)_0, v_\ell\cdot(a^\ell)_1,\dots,v_\ell\cdot(a^\ell)_n),c^\ell)\end{aligned}$$

The statement $f(a) = b$ can be described as an $\mathcal{L}$-sentence

$$\begin{aligned}\theta_n(w,v,a,b) \quad = \quad &\exists (a^0)_0,\dots,(a^n)_{n-1},(c^0)_0,\dots,(c^n)_{n-1}, \\ &\theta_{n,1}(w,a,a^0,\dots,a^n) \wedge \theta_{n,2}(w,v,a,a^0,\dots,a^n,c^0,\dots,c^n) \wedge \\ &\bigwedge_{i=0}^{n-1}(c^n)_i = b_i.\end{aligned}$$

(g) Let K be a model of T and $f \in K[X]$ a monic degree n polynomial. Show that if f is irreducible, then any root of f generates its splitting field $K[X]/f(X)$. (This statement holds for finite fields.)

Solution:

We first express the following statement as an $\mathcal{L}$-sentence: any root $a \in$

$K[X]/f(X)$ of f generates n distinct roots $b^1, \dots, b^n \in K[X]/f(X)$.

$$\begin{aligned}
\theta_{n,3}(v) \quad = \quad & \forall a_0, \dots, a_{n-1}, \theta_n(v, v, a, 0) \wedge \\
& \exists (b^1)_0, \dots, (b^n)_{n-1}, \bigwedge_{\ell=1}^{n} \theta_n(v, v, b^\ell, 0) \wedge \\
& \bigwedge_{k \neq \ell = 1}^{n} \bigvee_{i=0}^{n-1} (b^k)_i \neq (b^\ell)_i \wedge \\
& \bigwedge_{\ell=1}^{n} \exists c_0, \dots, c_{n-1}, \theta_n(v, (c_0, \dots, c_{n-1}, 0), a, b^\ell).
\end{aligned}$$

If $\theta_{n,3}$ holds, then it follows that the whole splitting field $K[X]/f(X)$ is generated by a. Finally we can express the statement, if a monic degree n polynomial $f \in K[X]$ is irreducible, then any root of f generates its splitting field $K[X]/f(X)$ by

$$\theta_{n,4} \quad = \quad \forall v_0, \dots, v_n, (v_n = 1 \ \wedge \phi_n(v)) \to \theta_{n,3}(v),$$

where we used ϕ_n from (c) to express irreducibility.

Since this statement holds for all finite fields, it holds for K.

(h) Deduce that if K is a model of T and $\bar{K}$ is an algebraic closure of K, then for any integer $n \geq 1$, the field K has a unique extension of degree n in $\bar{K}$. (This statement holds for finite fields.)

Hint: using the previous questions, show how to express, using the language of rings, the fact that if we have two irreducible polynomials f and g of degree n, then the roots of f are in the field generated by the roots of g.

Solution:
We want to write an $\mathcal{L}$-sentence ψ_n to formalize that if $f, g \in K[X]$ are irreducible monic polynomials of degree n, then there is an element $b \in K[X]/g(X)$ such that $f(b) = 0 \in K[X]/g(X)$. We then note that ψ_n holds for all finite fields, hence also for K. By $K \models \psi_n$, there is a root b of f in the field $K[X]/g(X)$ and hence by (g), $K[X]/f(X) \subseteq K[X]/g(X)$. Clearly we can switch f and g to get equality.

It remains to formalize ψ_n:

$$\begin{aligned}
\psi_n \quad = \quad & \forall v_0, \dots, v_n, w_0, \dots, w_n, (v_n = 1 \wedge w_n = 1 \wedge \phi_n(v) \wedge \phi_n(w)) \to \\
& \exists b_0, \dots, b_{n-1}, \theta_n(w, v, b, 0).
\end{aligned}$$

Exercise 2

(a) Following the methods seen in class for real-closed fields, prove that the theory ACF of algebraically closed fields has q.e. in the language of rings.

Solution:
In Chapter IV, section 2 a model theoretic criterion for having quantifier elimination was given. It thus suffices to show the following:

Let $\mathcal{M}, \mathcal{N} \models ACF$ be models of ACF, $\mathcal{A} \subseteq \mathcal{M} \cap \mathcal{N}$ be a substructure and

$$\varphi(\underline{\mathrm{x}}) = \exists y, \psi(\underline{\mathrm{x}}, y)$$

where $\underline{\mathrm{x}} = (x_1, \ldots, x_n)$ and $\psi(\underline{\mathrm{x}}, y)$ is a quantifier-free formula. Let $\underline{\mathrm{a}} = (a_1, \ldots, a_n) \in \mathcal{A}^n$ such that $\mathcal{M} \models \varphi(\underline{\mathrm{a}})$. Then we have to prove that also $\mathcal{N} \models \varphi(\underline{\mathrm{a}})$.

Since there are no relations in the language of rings, we may assume that ψ is of the form

$$\psi(\underline{\mathrm{x}}, y) = \bigvee_{i=1}^{n_i} \bigwedge_{j=1}^{n_j} t_{ij}(\underline{\mathrm{x}}, y)$$

where the terms t_{ij} are either $p_{ij}(\underline{\mathrm{x}}, y) = 0$ or $\neg q_{ij}(\underline{\mathrm{x}}, y) = 0$ for polynomials $p_{ij}, q_{ij} \in \mathbb{Q}[\underline{\mathrm{x}}, y]$. Since $\mathcal{M} \models \varphi(\underline{\mathrm{a}})$ holds, let $b \in \mathcal{M}$ such that $\mathcal{M} \models \psi(\underline{\mathrm{a}}, b)$. So there is an i, such that

$$\mathcal{M} \models \bigwedge_{j=1}^{k} p_{ij}(\underline{\mathrm{a}}, b) = 0 \wedge \bigwedge_{j=k+1}^{n_j} \neg q_{ij}(\underline{\mathrm{a}}, b) = 0$$

If there is a term t_{ij} with $j \leq k$ that has $p_{ij}(\underline{x}, y) \not\equiv 0$, then b is algebraic over $\mathcal{A}$. Since $\mathcal{N}$ is algebraically closed, $b \in \mathcal{N}$ and $\mathcal{N} \models \psi(\underline{\mathrm{a}}, b)$. Thus $\mathcal{N} \models \varphi(\underline{\mathrm{a}})$.

If all the polynomials $p_{ij}(\underline{x}, y) \equiv 0$, then

$$\bigwedge_{j=k+1}^{n_j} q(\underline{\mathrm{a}}, y) \neq 0$$

has only finitely many solutions y in the infinite field $\mathcal{N}$, so taking any one of these solutions c will give us $\mathcal{N} \models \psi(\underline{\mathrm{a}}, c)$ and hence $\mathcal{N} \models \varphi(\underline{\mathrm{a}})$.

(b) Show that if $F_1 \subset F_2$ are algebraically closed, then $F_2 \equiv F_1$ (i.e., they are elementarily equivalent).

Solution:
Let φ be an $\mathcal{L}$-sentence. with $F_1 \models \varphi$. Then we know by quantifier elimination that φ is equivalent (modulo ACF) to a quantifier-free $\mathcal{L}$-sentence

$$\psi = \bigvee_i \bigwedge_j t_{ij},$$

where t_{ij} are terms that are (in)equalities of polynomials of the constant symbols 0 or 1. Since $F_1 \models ACF$, we have $F_1 \models \psi$. Since

$F_1 \subseteq F_2$, they have the same characteristic p and there is a *prime-field* $\mathbb{F}_p$ or $\mathbb{F}_0 := \mathbb{Q}$ contained in F_1. Thus ψ is really just a statement about (in)equalities of elements in the prime field. Such statements are true in F_1 if and only they are true in the prime field. We get

$$F_1 \models \varphi \iff F_1 \models \psi \iff \mathbb{F}_p \models \psi \iff F_2 \models \psi \iff F_2 \models \varphi.$$

This means F_1 and F_2 are elementarily equivalent.

(c) Let p be a prime number or zero, and ACF_p the theory of algebraically closed fields of characteristic p. Show that the theory ACF_p is complete (i.e., for any sentence ϕ in the language of rings, either $\mathrm{ACF}_p \models \phi$ or $\mathrm{ACF}_p \models \neg\phi$).

Solution:
Let ϕ be a sentence. By the argument in (b), $F \models \phi$ if and only if $\mathbb{F}_p \models \phi$, as long as $F \models ACF_p$. So if $\mathbb{F}_p \models \phi$, then $F \models \phi$ for all $F \models ACF_p$, i.e. $ACF_p \models \phi$. Otherwise $\mathbb{F}_p \models \neg\phi$, then $F \models \neg\phi$ for all $F \models ACF_p$, i.e. $ACF_p \models \neg\phi$. This shows ACF_p is complete.

(d) Let F be an algebraically closed field. Show that definable subsets of F are either finite or have finite complement.

Solution:
Consider the definable subset $\varphi(F) = \{a \in F : F \models \varphi(a)\}$. By quantifier elimination, $\varphi(F) = \psi(F)$ for a quantifier-free formula $\psi(x)$ with one free variable x. As in (a) we may assume

$$\psi(x) = \bigvee_i \psi_i(x) \quad \text{with}$$

$$\psi_i(x) = \bigwedge_{j=1}^{k} p_{ij}(x) = 0 \wedge \bigwedge_{j=k+1}^{n_j} \neg q_{ij}(x) = 0.$$

For every i, if there is a $j \leq n_j$ with $p_{ij} \not\equiv 0$, then $\psi_i(F)$ is finite, since it consists of at most $\deg p_{ij}$ many solutions to the polynomial p_{ij}. If for all i, $p_{ij} \equiv 0$, then $\psi_i(F)$ is cofinite ($F \setminus \psi_i(F)$ is finite), since only for finitely many $a \in F$, $q_{ij}(a) = 0$. We see that

$$\psi(F) = \bigcup_i \psi_i(F)$$

is a union of finitely many finite or cofinite sets and hence is also finite or cofinite.

(e) Let F be an algebraically closed field, $m \geq 0$ an integer and $P \subset F[X_1, \dots, X_m]$ a prime ideal. Show that there exists $(x_1, \dots, x_m) \in F^m$ such that $f(x) = 0$ for all $f \in P$. This is known as Hilbert's Nullstellensatz.

Hint: use Hilbert's Basis-Satz to reduce to finitely many equations to be able to find an x with this property in some algebraically closed extension of F.

Solution:
Hilbert's Basis-Satz states that every ideal in a polynomial ring is finitely generated. Let thus $f_1, \ldots, f_n$ be generators of the ideal P. Since P is a prime ideal, $F[X_1, \ldots, X_m]/P$ is an integral domain and we can take an algebraic closure $\overline{F}$ of its field of fractions $\mathrm{Frac}(F[X_1, \ldots, X_m]/P)$. We have an inclusion $F \subseteq \overline{F}$ of algebraically closed fields and thus by (b) elementary equivalence. Consider the sentence

$$\varphi \quad = \quad \exists x_1, \ldots x_m \bigwedge_{i=1}^{n} f_i(x_1, \ldots, x_m) = 0$$

which holds in $\overline{F}$, since we can consider the elements $x_i = [X_i]$. By elementary equivalence, $\overline{F} \models \varphi$ implies $F \models \varphi$. Since $P = \langle f_1, \ldots, f_n \rangle$ there are $a_1, \ldots, a_m \in F$ such that $f(a_1, \ldots, a_m) = 0$ for all $f \in P$.

(f) Let ϕ be a sentence in the language of rings. Show that the following properties are equivalent:

(a) $ACF_0 \models \phi$

(b) $ACF_p \models \phi$ for all primes p large enough (depending on ϕ)

(c) $ACF_p \models \phi$ for all primes p in an infinite set (depending on ϕ)

Hint: Use compactness and completeness.

Solution:
(a) $\Longrightarrow$ (b), We have $ACF_0 \models \phi$. By quantifier elimination, let

$$\psi = \bigvee_i \bigwedge_j (\neg) z_{ij} = 0$$

with $z_{ij} \in \mathbb{Z}$ be an equivalent formula (mod ACF). Choose a prime $p > \max\{|z_{ij}|\}$. Then we have for all i, j that $\mathbb{Q} \models z_{ij} = 0$ if and only if $\mathbb{F}_p \models z_{ij} = 0$. Thus

$$\begin{aligned} ACF_0 \models \phi \iff ACF_0 \models \psi \iff \mathbb{Q} \models \psi \iff \mathbb{F}_p \models \psi \\ \iff ACF_p \models \psi \iff ACF_p \models \phi. \end{aligned}$$

(b) $\Longrightarrow$ (c), This is immediate. The infinite set is the set of all primes that are large enough in (b).

(c) $\Longrightarrow$ (a), Let $p_1, p_2, \ldots$ be such that $ACF_{p_i} \models \phi$ for $i = 1, 2, \ldots$. Consider the $\mathcal{L}$-sentence

$$\varphi_n \quad = \quad (\neg \underbrace{1 + 1 + \ldots + 1}_{n-\text{times}} = 0) \wedge \phi$$

and the $\mathcal{L}$-theory $T = ACF \cup \{\varphi_n : n = 1, 2, \ldots\}$. We show that T is finitely satisfiable: let $\Delta \subsetneq T$ and let i be such that $p_i > \max n : \varphi_n \in \Delta$. Then we have $\bar{\mathbb{F}}_{p_i} \models \Delta$, since $ACF_{p_i} \models \phi$ and $ACF_{p_i} \models \neg \underbrace{1 + 1 + \ldots + 1}_{n-\text{times}} = 0$ for all $n < p_i$.

By the compactness theorem there is a model $\mathcal{M} \models T$. This model $\mathcal{M}$ is a field and has to have characteristic 0, since it cannot have finite characteristic by $\mathcal{M} \models \varphi_n$ for all $n \in \mathbb{N}$. By completeness $\mathcal{M}$ is elementarily equivalent to every model of ACF_0 and hence $ACF_0 \models \phi$.

(g) Deduce from the previous question another solution of Question 9 of Exercise 3 of Sheet 2: every injective map $\mathbb{C}^n \to \mathbb{C}^n$ given by polynomials is surjective.

Solution:
We write a finite set of polynomials in n variables and degree at most d in multiindex notation as $f_i(\underline{\mathrm{X}}) = \sum_\alpha a^i_\alpha \underline{\mathrm{X}}^\alpha$. We can write that injectivity implies surjectivity as a first order formula in the following way:

$$\begin{aligned} \varphi_{n,d} \quad &= \quad \forall a^i_\alpha \left(\forall \underline{\mathrm{x}}, \underline{\mathrm{y}} \left(\bigwedge_{i=1}^n \sum_\alpha a^i_\alpha (\underline{\mathrm{x}})^\alpha = \sum_\alpha a^i_\alpha (\underline{\mathrm{y}})^\alpha \right) \to \underline{\mathrm{x}} = \underline{\mathrm{y}} \right) \\ &\to \left(\forall \underline{\mathrm{y}} = (y_1, \ldots, y_n) \exists \underline{\mathrm{x}}, \bigwedge_{i=1}^n \sum_\alpha a^i_\alpha (\underline{\mathrm{x}})^\alpha = y_i \right) \end{aligned}$$

For all n, d, the sentence $\phi_{n,d}$ holds in finite fields (just because every injective map from a finite set to itself is surjective). As in Question 1 of Exercise 3 of Sheet 2, $\phi_{n,d}$ also holds in the algebraic closures of finite fields, since we can take the finite extensions of $\mathbb{F}_p$ by the elements a^i_α and the coordinates of any point in the image.

We thus have $\bar{\mathbb{F}}_p \models \varphi_{n,d}$, where $\bar{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. By completeness, $ACF_p \models \varphi_{n,d}$ for every prime p and by exercise (f), $ACF_0 \models \varphi_{n,d}$. Since in particular $\mathbb{C} \models ACF_0$, we have $\mathbb{C} \models \varphi_{n,d}$ for all n and d, hence injectivity implies surjectivity for any polynomial map $\mathbb{C}^n \to \mathbb{C}^n$.