# 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 $\phi$ 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 $p$.

(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).

(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
$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$
is irreducible.

(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 $K$.

(e) Show that there exist formulas $\pi_n(v, a, b, c)$ (resp. $\mu_n(v, a, b, c)$), where for $I = \{0, 1, \ldots, n-1\}$, $v = (v_i)_{i \in I}$, $a = (a_i)_{i \in I}$, $b = (b_i)_{i \in I}$ 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
$$\Big(\sum_{i=0}^{n-1} a_i \alpha^i\Big) \cdot \Big(\sum_{i=0}^{n-1} b_i \alpha^i\Big) = \sum_{i=0}^{n-1} c_i \alpha^i,$$
where $\alpha$ 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 $\alpha$ can be expressed as a matrix acting on the vectorspace $K_n[X]$.*

(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 $n$.

(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.)

(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 $g$.*

## 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.

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

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

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

(e) Let $F$ be an algebraically closed field, $m \geq 0$ an integer and $P \subset F[X_1, \ldots, X_m]$ a prime ideal. Show that there exists $(x_1, \ldots, x_m) \in F^m$ 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 $F$.*

(f) Let $\phi$ 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 $\phi$)

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

*Hint: Use compactness and completeness.*

(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.