Exercises, sheet 0, pseudo-finite fields. Later we will deduce from the compactness theorem that there exists a natural number $D = D(n, r, d)$ such that for all algebraically closed fields L, if $I \subseteq L[X_1, \dots, X_n]$ is an ideal generated by polynomials $h_1, \dots, h_r$ of degrees at most d, then:

$$\begin{cases} f \in I \iff (\exists g_1, \dots, g_r \in L[X_1, \dots, X_n]_{\leq D})\big(f = \sum_{i=1}^r h_i g_i\big), \\ I \text{ is prime} \iff (\forall f, g \in L[X_1, \dots, X_n]_{\leq D})(fg \in I \implies f \in I \text{ or } g \in I). \end{cases}$$

We will also show that for every field K and every first-order formula $\xi(z_1, \dots, z_n)$ there is a quantifier-free first-order formula $\zeta(z_1, \dots, z_n)$ such that for all $u \in (K^{\text{alg}})^n$, $\xi(u)$ holds in $K^{\text{alg}} \iff \zeta(u)$ holds in K^{alg}.

1. Let G be a finite group of order n. Assume that for every $d|n$, G has exactly one subgroup of index d. Show that G is cyclic. Hint: use the divisor sum formula of Gauss.
2. Let K be a field with its algebraic closure K^{alg}. Assume that for every $n \in \mathbb{N}$ there is a unique degree n extension $K \subseteq K_n \subseteq K^{\text{alg}}$. Show that $\text{Gal}(K_n/K) \simeq \mathbb{Z}/n$. Show that $K_n \subseteq K_m$ if and only if $n|m$.
3. Let $f_1(U, X), \dots, f_k(U, X)$ be polynomials in $K[U, X]$, where $U = (U_1, \dots, U_n)$ and $X = (X_1, \dots, X_m)$. For $u \in (K^{\text{alg}})^n$ consider the ideal I_u generated by $f_1(u, X), \dots, f_k(u, X)$ in $K^{\text{alg}}[X]$. Show that there is a first-order formula $\varphi(z_1, \dots, z_n)$ in the language of fields and with parameters in K such that for all $u \in (K^{\text{alg}})^n$, $\varphi(u)$ holds in $K^{\text{alg}} \iff I_u$ is prime.
4. Conclude that there is a quantifier-free first-order formula $\psi(z_1, \dots, z_n)$ in the language of fields (with parameters from K), such that for all $u \in K^n$, $\psi(u)$ holds in $K \iff I_u$ is prime.
5. A field K is called *pseudo-finite* if the following hold:
   (i) K is perfect, i.e., is either of characteristic zero, or of characteristic p and with the map $(\cdot)^p : K \to K$ being surjective;
   (ii) K has a unique degree n extension for every natural n in a fixed algebraic closure K^{alg};
   (iii) Whenever $f_1, \dots, f_k \in K[X_1, \dots, X_m]$ are such that $I = (f_1, \dots, f_k) \subseteq K^{\text{alg}}[X_1, \dots, X_m]$ is prime and $1 \notin I$, then there is $u \in K^m$ such that
   $$f_1(u) = \dots = f_k(u) = 0.$$
   Field satisfying this condition are called *pseudo-algebraically closed* (PAC).

   Show that there are first-order axioms that describe the class of pseudo-finite fields.
6. Recall the fundamental theorem of infinite Galois theory (we will give a model theoretic proof later). Show that if σ is an infinite order element of $\text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$, then its fixed-field satisfies (ii) (and (i)). In fact, for a full measure set of σ's with respect to the Haar measure, it also satisfies (iii) by a theorem of Jarden.
7. Lang-Weil estimate is the following statement: for every integers e, n, r there is a real constant $C > 0$ such that for all $f_1, \dots, f_r \in \mathbb{F}_q[X_1, \dots, X_n]$ of total degree $\leq e$, that generate a prime ideal over $\mathbb{F}_q^{\text{alg}}$ with the quotient algebra of transcendence degree d, we have
   $$\big|\#\{u \in \mathbb{F}_q^n : f_1(u) = \dots = f_r(u) = 0\} - q^d\big| \leq C q^{d - \frac{1}{2}}.$$
   Deduce from this theorem that if K is an infinite field that satisfies all first-order sentences that are true in all finite fields, then K is pseudo-finite. Ax's theorem says that the opposite is true.
8. Call a graph (V, E) random if for every finite disjoint $A, B \subseteq V$ there is $v \in V$ connected to all elements of A and not connected with any member of B. Show that a countable random graph is unique up to isomorphism.
9. Show that if A and B are disjoint subsets of $\mathbb{F}_q$, then in any sufficiently big finite extension $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ there is $x \in \mathbb{F}_{q'}$ such that for all $a \in A$ the element $x - a$ is a square in $\mathbb{F}_{q'}$ and for all $b \in B$ the element $x - a$ is not a square in $\mathbb{F}_{q'}$. In fact, in any pseudo-finite field K, the relation
   $$x \; E \; y \iff x - y \text{ is a square}$$
   defines a random graph.