Exercise sheet 7

1. Let $L : K$ be a splitting field of a separable polynomial $f(x) \in K[x]$ of degree n. Show that if f is irreducible then n divides $|\mathrm{Gal}(L : K)|$.

2. Let p be a prime and $\mathbb{F}_{p^n}$ be the finite field of p^n elements. Show that $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and a generator is given by the Frobenius homomrphism $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ where $\varphi(x) = x^p$.

3. For $p^r = 8, 9, 16$ find the minimal polynomial over $\mathbb{F}_p$ of a generator of $\mathbb{F}_{p^r}^\times$.

4. Let n be a positive integer. Let p be a prime number and let K be a finite field of order p^n. Prove:

(a) If $p = 2$, then each element of K is a square. (*Hint:* Consider the Frobenius homomorphism)

(b) Each element of K can be written as a sum of two squares.

(c) For $p > 2$, we have that -1 is a square in K if and only if $p^n \equiv 1 \pmod 4$.

5. Let $p > 2$ be a prime number. Prove that p can be written as a sum of two squares in $\mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.

Hint: Look at the prime factorization of p in $\mathbb{Z}[i]$. See also Exercise sheet 1, question 3.