HOMEWORK #5 IN ALGEBRAIC STRUCTURES 2

Problem 5.1. Prove Lemma 5.2.

Problem 5.2. Prove Lemma 5.5.

Problem 5.3. Let $\mathbb{F}_p$ be the field with p elements. For any $r > 0$ we define $Q_r(t) := t^{p^r} - t$. Let M_r be a splitting field of $Q_r(t)$ over $\mathbb{F}_p$. Show that:

(a) M_r is a finite field with p^r elements.

A hint. Let $N_r \subset M_r$ be the set of roots of $Q_r(t)$. Show that N_r is a subfield of M_r.

(b) any finite field K such that $|K| = p^r$ is a splitting field of $Q_r(t)$,

A hint. Consider the multiplicative group $K^\times$.

(c) for any $q = p^r$ there exists a unique [up to an isomorphism] finite field $\mathbb{F}_q$ with q elements.

Problem 5.4. Let K be a finite field with q elements and let $K \subset L$ be a finite extension. Show that:

(a) $q = p^r$ where $p :=$ch(K) and $r \geq 1$,

(b) $|L| = q^{[L:K]}$,

(c) the map $\mathcal{F} : L \to L$ defined by $\alpha \mapsto \alpha^q, \alpha \in L$ is a K-isomorphism,

We will consider $\mathcal{F}$ as an element of the group Gal$(L : K)$.

(d) $\mathcal{F}^n \neq Id$ if $0 < n < [L : K]$ and $\mathcal{F}^{[L:K]} = Id$,

(e) the group Gal$(L : K)$ is a cyclic group of order $[L : K]$ generated by $\mathcal{F} \in$Gal$(L : K)$.