**HOMEWORK #5**
**SOLUTIONS TO SELECTED PROBLEMS**

**Problem 5.3 – Construction of finite fields.** Let $p$ be a prime and let $\mathbb{F}_p$ be the field with $p$ elements. Let $r \geq 1$ be an integer and set $q = p^r$. We will construct a field with $q$ elements and prove its uniqueness (up to an isomorphism).

(a) Consider the polynomial $Q(t) = t^q - t$. Let $M$ be a splitting field of $Q$ over $\mathbb{F}_p$. Define a subset $N \subseteq M$ as the set of roots of $Q$ in $M$, that is,

$$N = \{x \in M \,:\, Q(x) = 0\}$$

**Lemma 1.** *$N$ is a subfield of $M$ containing $\mathbb{F}_p$.*

*Proof.* If $x \in \mathbb{F}_p$ then $x^p = x$ and in particular $x^{p^r} = x$, hence $Q(x) = x$ so that $\mathbb{F}_p \subseteq N$.

If $x, y \in N$ then $x^q = x$ and $y^q = y$. It follows that $(xy)^q = x^q y^q = xy$ so that $xy \in N$. A similar argument shows that $x^{-1} \in N$ for $0 \neq x \in N$. Moreover, since $(x+y)^p = x^p + y^p$ and $q$ is a power of $p$, one has $(x+y)^q = x^q + y^q = x + y$ so that $x + y \in N$. Hence $N$ is a subfield. $\square$

Since $N$ is a subfield of $M$ that contains $\mathbb{F}_p$ and all the roots of $Q$ (by its definition), by the minimality of $M$ as a splitting field of $Q$ over $\mathbb{F}_p$ we see that $N = M$. We deduce that $M$ consists of the roots of $Q(t)$ over $\mathbb{F}_p$.

**Lemma 2.** *$|M| = q$.*

*Proof.* By the last remark, it is enough to show that $Q(t)$ has precisely $q$ roots in its splitting field. Now $\deg Q = q$ so we need to verify that there are no multiple roots. We do this by considering the g.c.d $(Q, Q')$ and showing it is equal to 1. Indeed, for $Q(t) = t^q - t$ one has $Q'(t) = qt^{q-1} - 1 = -1$. $\square$

(b) If $K$ is a finite field with $q$ elements, the multiplicative group $K^\times$ has $q - 1$ elements. It follows that for any $x \in K^\times$, $x^{q-1} = 1$. Multiplying by $x$ we get $x^q = x$ (or $Q(x) = 0$) for all $x \in K$. Since $\deg Q = q$ we see that the elements of $K$ are all the roots of $Q$ over $\mathbb{F}_p$. In addition, since $K$ has characteristic $p$, it contains $\mathbb{F}_p$ as its prime field (take $1, 1+1, \dots$). We conclude that $K$ is a splitting field of $Q$ over $\mathbb{F}_p$.

(c) The *existence* of a field with $q = p^r$ elements was proved in (a); just take the splitting field of $t^q - t$ over $\mathbb{F}_p$. The *uniqueness* follows from the claim in (b) that any such field is a splitting field of $Q(t)$ over $\mathbb{F}_p$, and the fact that a splitting field is unique up to an isomorphism.

**Problem 5.4 – Galois groups of finite fields.** Let $K$ be a finite field with $q$ elements and $L/K$ be a finite extension, $[L : K] = n$.

(a) If $K$ has characteristic $p$ then it contains $\mathbb{F}_p$ as a subfield. Therefore we can view $K$ as a vector space over $\mathbb{F}_p$. Since $K$ is finite, the dimension is finite, say $r \geq 1$, and $|K| = p^r$.

(b) By the same reasoning, $L$ is a vector space over $K$ of dimension $n$, so that $|L| = |K|^n = q^n$.

(c) Define a map $F : L \to L$ by $F(x) = x^q$ for $x \in L$. The fact that $F$ is a field homomorphism was shown in lemma 1 above. We know that $x^q = x$ for all $x \in K$ (because $K$ is a field with $q$ elements, see (b) of the previous problem), hence $F$ acts as identity on $K$ so that $F$ is a $K$-homomorphism. Finally, view $F$ as a $K$-linear map $L \to L$. Since it is one-to-one (any field homomorphism is such) and the dimension $[L : K]$ is finite, it follows that $F$ is also onto. We deduce that $F$ is a $K$-isomorphism.

(d) Let $0 \leq i$. Then $F^i(x) = x^{q^i}$ for $x \in L$. If $0 < i < n$ then $F^i = id_L$ implies that all elements of $L$ are roots of the polynomial $t^{q^i} - t$ over $\mathbb{F}_p$, which has degree $q^i$. But $|L| = q^n > q^i$ so this is impossible. For $i = n$, since $|L| = q^n$ we already know that elements of $L$ are (the) roots of $t^{q^n} - t$ so that $F^n$ is identity on $L$.

(e) The previous paragraph shows that $C = \{id_L, F, \ldots, F^{n-1}\}$ is a cyclic subgroup of order $n$ of $\mathrm{Gal}(L/K)$ generated by $F$. But one always has $|\mathrm{Gal}(L/K)| \leq [L : K] = n$. It follows that $\mathrm{Gal}(L/K) = C$ is cyclic of order $n$, generated by $F$.