Example Set #3

1. Construct the field of order four and compute its full addition and multiplication tables.

2. Check that both polynomials $x^3 + x + 1$ and $x^3 + x^2 + 1$ from $\mathbb{Z}_2[x]$ are irreducible. Use these polynomials to construct two copies of the finite field of order eight. Find an explicit isomorphism between the two copies of the field. (In the second copy of the field find the roots of the polynomial $x^3 + x + 1$.)

3. Prove that the multiplicative group $F^{\#}$ of a finite field F is cyclic. (Hint: If it is not cyclic, it must contain a subgroup $\mathbb{Z}_p \times \mathbb{Z}_p$ for some p. How many roots can the polynomial $x^p - 1$ have in F?)

4. Generalize the above to prove that every finite subgroup in the multiplicative group of a (possibly infinite) field is cyclic.

5. Prove that every finite field is a simple extension of the prime subfield.

6. Prove that for every prime power $q = p^f$ there exists a field of size q. (Hint: Consider the splitting field F for the polynomial $x^q - x \in \mathbb{Z}_p[x]$. Show that the set of roots of this polynomial form a subfield, which then has size q.)

7. Prove that for every $n \geq 1$, $\mathbb{Z}_p[x]$ contains an irreducible polynomial of degree n.

8. Again, let $q = p^f$ be a prime power. Prove that any two fields of size q are isomorphic.

9. Determine the splitting field of each of the following polynomials:

$$x^4 - 8x^4 + 15,\ x^4 - 7,\ x^8 - 1 \in \mathbb{Q}[x].$$

10. Let L be the splitting field of the polynomial $f = x^8 - 1 \in \mathbb{Q}[x]$. Determine for which pairs of roots of f there exists an automorphism of L taking one root to the other.

11. With f and L as above find the explicit action of all those automorphisms on L (on any suitable basis that you choose).

12. Do the same for the splitting field of the polynomial $x^4 - 7 \in \mathbb{Q}[x]$.