Galois Theory Additional Exercises

Zexiang Chen

While doing these exercises, you may wish to refer to the notes by Dr. T. Yoshida: https://www.dpmms.cam.ac.uk/~ty245/Yoshida_2012_Galois.pdf which cover everything (perhaps more than enough) you need to know for Galois Theory. There are some useful facts in these exercises. Some of them might be challenging!

1. Let $L/M/K$ be field extensions such that $[L : K] = p$ where $p$ is a prime. Show that $M = K$ or $M = L$.

2. Let $L/K$ be an algebraic field extension and $\psi : L \to L$ a $K$-homomorphism. By considering the minimal polynomials, show that for each $\alpha \in L$, there exists $\beta \in L$ such that $\psi(\beta) = \alpha$. Hence show that $\psi$ is an isomorphism.

3. Can you find an inseparable irreducible polynomial $f(X) \in \mathbb{F}_p[X]$? Perhaps it is helpful to think about some condition on the derivative of the any inseparable polynomial.

4. Let $L/K$ be a finite Galois extension and $F, M$ intermediate fields, i.e. $K \subset F, M \subset L$. What is the subgroup of $\text{Gal}(L/K)$ corresponding to the subfield $F \cap M$? What about $FM$? ($FM$ is the smallest field inside $L$ containing $F$ and $M$).

5. Let $L_1/Q, L_2/Q$ be quadratic field extensions such that $L_1 = \mathbb{Q}(\sqrt{a}), L_2 = \mathbb{Q}(\sqrt{b})$. Show that $L_1 = L_2$ if and only if $a/b$ is a square in $\mathbb{Q}^\times$. Moreover, let $K$ be a field containing an $n$th primitive root of unity for some $n$. Let $a, b \in K$ such that $f(X) = X^n - a$ and $g(X) = X^n - b$ are irreducible. Show that $f$ and $g$ have the same splitting field if and only if $b = c^na^r$ for some $c \in K$ and $r \in \mathbb{N}$ with $\gcd(r, n) = 1$.

6. Let $f(X) = X^5 - 2 \in \mathbb{Q}[X]$ and $K$ be the splitting field of $f(X)$. Find the Galois group $\text{Gal}(K/Q)$.

7. Show that the minimal polynomial of $\sqrt[3]{3} + \sqrt[5]{5}$ is reducible modulo $p$ for every prime $p$. This gives an example of an irreducible polynomial which is reducible in $\mathbb{F}_p$ for each $p$.

8. Let $\zeta_n$ be a primitive $n$th root of unity. Determine (i) $\mathbb{F}_2(\zeta_4)$ (ii) $\mathbb{F}_2(\zeta_7)$ (iii) $\mathbb{F}_3(\zeta_{10})$. Can you find some general pattern to determine $\mathbb{F}_p(\zeta_n)$?

9. Let $L/K$ be an extension of finite fields. Show that $L = K(\zeta_n)$ for some $n$. You will (probably) see a similar result for the case $K = \mathbb{Q}$ in Part III, which is called Kronecker-Weber theorem. It states that every abelian extension of $\mathbb{Q}$ (that is, a Galois extension with abelian Galois group) is contained within some cyclotomic field $\mathbb{Q}(\zeta_n)$. 