Exercise sheet #6

Prof. Peter Bürgisser, Dr. Pierre Lairez, Paul Breiding and Jesko Hüttenhain

June 1, 2016

Exercise 1. We aim at proving that any finite Abelian group is isomorphic to the Galois group of some finite Galois extension of $\mathbb{Q}$. Let $H \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ be an abelian group.

1. Show that we can find distinct prime numbers $p_1, \ldots, p_r$ such that H is isomorphic to a quotient of $\mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_r}^\times$.

   Hint: Understand first the case where $r = 1$ and use the fact that for any $n \geqslant 1$, there exist infinitely many prime numbers p such that $p \equiv 1 \pmod{n}$.

2. Show that $\mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_r}^\times \simeq \mathbb{Z}_{p_1 \cdots p_r}^\times$.

3. Show that there is a finite Galois extension of $\mathbb{Q}$ whose Galois group is isomorphic to H.

Exercise 2. We consider the field $\mathbb{C}(X)$. Let $\zeta \in \mathbb{C}$ be a primitive cube root of unity.
Let $\sigma : f(X) \mapsto f(\zeta X)$ and $\tau : f(X) \mapsto f(X^{-1})$ be two automorphisms of $\mathbb{C}(X)$. Let G be the group generated by σ and τ.

1. Show that G has order 6.

2. Show that $\mathbb{C}(X)^G = \mathbb{C}(X^3 + X^{-3})$.

Exercise 3. Recall this unproven result given in the lecture:
Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial and let p be a prime number. If f is separable over $\mathbb{F}_p$ and factors as a product of irreducible polynomials of degrees $n_1, \ldots, n_r$, then the Galois group of f over $\mathbb{Q}$ contains a permutation of type $(n_1, \ldots, n_r)$. (The type of a permutation is the list of the lengths of the cycles in its cycle decomposition.)
Show that the Galois group of $X^4 + 4X^3 + 10X^2 + 7X + 4$ over $\mathbb{Q}$ is isomorphic to S_4.