Exercise sheet #12

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

July 13, 2016

Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $d > 0$. Let p be a prime number, and let $\bar{f} \in \mathbb{F}_p[X]$ be the reduction modulo p of f. *We assume that $\bar{f}$ has only simple roots in the algebraic closure $\overline{\mathbb{F}_p}$.* Let K be the splitting field of f over $\mathbb{Q}$ and let G be its Galois group. Let K' be the splitting field of $\bar{f}$ over $\mathbb{F}_p$ and let G' be its Galois group.

Let us write $\bar{f}$ as $\prod_{i=1}^{r} g_i$, where $g_i \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree e_i. This sheet is dedicated to the proof that G (considered as a subgroup of the group of permutations of the roots of f) contains an element whose cycle type is $(e_1, \dots, e_r)$. This is a result due to Dedekind.

Let A be the integral extension of $\mathbb{Z}$ generated by the roots of f in $\overline{\mathbb{Q}}$.

1. Show that there is a maximal ideal $\mathfrak{p} \subset A$ such that $\mathfrak{p} \cap \mathbb{Z} = (p)$.

2. Show that there is a ring homomorphism $\rho : A \to K'$ which maps bijectively the roots of f to the roots of $\bar{f}$.

Let $G_\mathfrak{p} \subseteq G$ denote the subgroup of all $\sigma \in G$ such that $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$.

3. For $\sigma \in G_\mathfrak{p}$, show that there is a unique $\sigma' \in G'$ such that $\sigma \circ \rho = \rho \circ \sigma'$.

4. Show that the map $\sigma \mapsto \sigma'$ defined above is an injective group homomorphism.

We will now show that the morphism $\sigma \in G_\mathfrak{p} \mapsto \sigma' \in G'$ is surjective. Let $H \subseteq G'$ denote the image of this morphism and let $y \in K'$ be an element which is fixed by H.

5. Show that there exists an $x \in A$ such that $\rho(x) = y$ and $\rho(\sigma(x)) = 0$ for any $\sigma \in G \setminus G_\mathfrak{p}$.

   Hint: Use the Chinese remainder theorem to the maximal ideals $\sigma(\mathfrak{p})$, with $\sigma \in G$.

Let $h(T) = \prod_{\sigma \in G}(T - \sigma(x)) \in A[T]$ and let $\bar{h}(T) \in K'[T]$ be the coefficient-wise image of h by ρ.

6. Show that $h(T) \in \mathbb{Z}[T]$ and that $\bar{h}(T) = T^{|G|-|H|}(T - y)^{|H|}$.

7. Deduce that $y \in \mathbb{F}_p$ and that $H = G$.

We may now conclude. Let $F : K' \to K'$ denote the Frobenius automorphism.

8. Show that the cycle type of F, considered as a permutation of the roots of $\bar{f}$, is $(e_1, \ldots, e_r)$ (in other words, F is a product of r cycles with disjoint supports of length $e_1, \ldots, e_r$).

9. Show that G contains a permutation whose cycle type is $(e_1, \ldots, e_r)$.