Mathematics 100C Homework 5
Due: Friday May 10 2024

Instructions: Please write clearly and fully explain your solutions. It is OK to work with others to solve the problems, but if you do so, you should write your solutions up separately. Copying solutions from your peers or a solutions manual will be deemed academic misconduct. Chapter and problem numbers, if any, refer to *Algebra*, second edition, by Michael Artin. Please feel free to reach out to me or the TA if you have any questions.

Suppose F is a field, and K is a finite extension of F. Define

$$\mathrm{Aut}(K/F) = \{\sigma : K \simeq K : \sigma(\lambda) = \lambda \text{ for all } \lambda \in F\}.$$

That is, $\mathrm{Aut}(K/F)$ is the set of field isomorphisms from K to itself that are the identity on F. Observe that $\mathrm{Aut}(K/F)$ is a group. The next big topic for us in the course is to study this group, at least in the case when F has characteristic 0. In this homework, we understand $\mathrm{Aut}(K/F)$ when K, F are finite fields.

1. Suppose $K = F(\alpha)$, with $[K : F] = r$. Let $f(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0 \in F[x]$ be the irreducible polynomial for α. Let L be a field extension of K in which f splits completely, so that $f(x) = (x - \alpha_1)\cdots(x - \alpha_r)$ with $\alpha_1 = \alpha$. Let $\sigma \in \mathrm{Aut}(K/F)$. Let S be the set of α_i's that are K. So, $\alpha_1 \in S$, but we need not have all $\alpha_j \in K$. If $\sigma \in \mathrm{Aut}(K/F)$, prove that $\sigma(\alpha) \in S$.

2. Suppose $K = F(\alpha)$, with $[K : F] = r$. Prove that $\mathrm{Aut}(K/F)$ has size at most r. **Hint**: Use the previous question.

3. Suppose $F = \mathbf{F}_p$, $q = p^r$, and $K = \mathbf{F}_q$. Recall that Frobenius $\varphi \in \mathrm{Aut}(K/F)$ given by $\varphi(\alpha) = \alpha^p$. Prove that φ has exact order r in this group. Conclude that $\mathrm{Aut}(\mathbf{F}_{p^r}/\mathbf{F}_p)$ is a cyclic group of order r, generated by the Frobenius.

4. Suppose now $F = \mathbf{F}_{p^k}$, and $K = \mathbf{F}_{p^r}$, where $r = ks$ for some integer s. Let $\varphi_F = \varphi^k$ be the k^{th} power of Frobenius, as an automorphism of K.
   (a) Prove that $\varphi_F \in \mathrm{Aut}(K/F)$.
   (b) Prove that $\mathrm{Aut}(K/F)$ is the cyclic group of order s generated by φ_F. **Hint**: What is the order of φ_F in $\mathrm{Aut}(\mathbf{F}_{p^r}/\mathbf{F}_p)$?