Introduction to Algebraic Information Theory for Quantitative Finance
Homework 4

August 30, 2025

Timothy Tarter
James Madison University
Department of Mathematics

1. Show that $x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$. Describe $\mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.
2. Show that $Gal(\mathbb{C} : \mathbb{R}) \simeq \mathbb{Z}_2$.
3. Describe $Gal(\mathbb{Q}[\sqrt{2}, \sqrt{3}, i\sqrt{7}] : \mathbb{Q})$. What is its polynomial? What are its subgroups? For each subgroup H, determine $\Phi(H)$.
4. Describe $Gal(\mathbb{Q}[i + \sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}])$. What is its polynomial? What are its subgroups? For each subgroup H, determine $\Phi(H)$.
5. Describe $Gal(GF(8) : \mathbb{Z}_2)$. What are its subgroups? For each subgroup H, determine $\Phi(H)$.
6. Describe the Galois Group of $f(x) = x^3 - 2$.
7. Describe the Galois Group of $f(x) = x^4 - x^2 + 1$.
8. Determine Aut$\mathbb{Q}$ and Aut$\mathbb{Z}_p$.
9. Show that if K is a finite field, K is unique up to isomorphism, and that it is isomorphic to $GF(p^n)$. Show that K is a splitting field of a $f = x^{p^n} - x$ over $\mathbb{Z}_p[x]$.
10. Prove that $\forall E$ subfields of L containing K, $\Gamma(E) \leq Gal(L : K)$. Hint: pick arbitrary elements in $\Gamma(E)$, then show that it is a subgroup.
11. Prove that $\forall H \leq Gal(L : K)$, $\Phi(H)$ is a subfield of L containing K. Hint: pick arbitrary elements in $\Phi(H)$, then show that it is a subgroup.
12. Let $z \in L\backslash K = \{\ell \in L : \ell \notin K\}$. Show that if z is a root of $f \in K[x]$ and if $\alpha \in Gal(L : K)$, $\alpha(z)$ is a root of f.
13. Show that $E \subseteq \Phi(\Gamma(E))$ and $H \subseteq \Gamma(\Phi(H))$. Hint: start with a proof by picture.
14.