May 2021

1a) Prove that any finite field must have order a power of a prime p and for each $n \in \mathbb{Z}^+$, there is ***one and only one*** field of order p^n within a fixed algebraic closure of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

b) Prove that all finite extensions of $\mathbb{F}_p$ are both normal and separable. Briefly explain why this implies that all finite extensions of all finite fields must be both normal and separable.

c) Prove that the Galois group over $\mathbb{F}_p$ of any finite extension of $\mathbb{F}_p$ is cyclic and give an explicit generator of such a Galois group, being sure to completely justify your answer. Briefly explain why this implies that all finite extensions of all finite fields must be cyclic.

d) If $E = \mathbb{F}_q = \mathbb{F}_{p^d}$ is a finite field with $q = p^d$ elements, and $K = \mathbb{F}_{q^r}$ is an extension of E of degree r, give a generator for $\mathrm{Gal}(K/E)$. You do ***not*** have to justify your answer to this part.

2) Show that if α is algebraic over a field k, then the multiplicity of α in its minimal polynomial $f(x) = \mathrm{irr}(\alpha, k, x)$ must be 1 if the characteristic is 0, and p^μ for some nonnegative integer μ if the characteristic is $p > 0$. In the latter case, deduce that α^{p^μ} must be separable over k and

$$[k(\alpha): k] = p^\mu [k(\alpha): k]_s \tag{1}$$

Hint: Equation (1) follows easily from everything else. There are several different ways to show this, although I think the way that I did it in class is probably easiest.

3,4,5) For purposes of the prelims, your best 3 of the following 4 problems *(A, B, C, or D, all of which have multiple parts, and were all homework questions)* will count. For purposes of the class final, ***all 4*** will count, but you do not have to complete them all, as the scores will be curved.

Ai) Let k be a finite field of order q in characteristic p, let n be a positive integer not divisible by p, and let K be the splitting field of $x^n - 1$ over k. Prove that $[K: k]$ equals the smallest positive integer d such that $n \mid q^d - 1$.

ii) Let k be a field of characteristic p and let t, u be algebraically independent over k. Prove that $k(t, u)$ has degree p^2 over $k(t^p, u^p)$.

Bi) Suppose E and L are two finite extensions of a field k that are contained in the same algebraic closure of k. For each of the following, if the statement is true, provide a brief proof, and if the statement is false, provide a counterexample.

a) $[EL: E]$ must divide $[L: k]$

b) If $[EL: E] = [L: k]$, then $E \cap L = k$

c) If $E \cap L = k$, then $[EL: E] = [L: k]$.

ii) Would your answers to part a change any under the added hypothesis that L is Galois over k? Explain.

C) Let $\zeta = \zeta_{77}$ represent a primitive 77^{th} root of 1. Find all conjugates of the given element over the given field, and justify.

i. ζ over $\mathbb{Q}$

ii. ζ^{35} over $\mathbb{Q}$

iii. ζ over $\mathbb{Q}(\zeta^{35})$

iv. ζ over $\mathbb{Q}(\zeta^{44})$

v. ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$

vi. $\zeta + \zeta^{-1}$ over $\mathbb{Q}$

Hint: For Part iii, it might help if you find the Galois group of $k(\zeta) = \mathbb{Q}(\zeta)$ over $k = \mathbb{Q}(\zeta^{35})$ as a subgroup of Gal$(\mathbb{Q}(\zeta)/\mathbb{Q})$. A similar trick should work for Part iv.

Di) Let σ be an automorphism of k^a and let F be its fixed field. Prove that every finite extension of F is Galois with cyclic Galois group.

ii) Let E be a maximal subfield of $\mathbb{Q}^a$ not containing $\sqrt{2}$. *(Such a field exists by Zorn's Lemma–you do not have to prove that).* Prove that every finite extension of F is Galois with cyclic Galois group.