MATH 103B – Discussion Worksheet 7
June 1, 2023

Topic: Finite fields (Judson Chapter 22)
The following facts concerning finite fields are worth knowing:

1. There is a finite field of order m if and only if $m = p^n$ for some prime number p and $n \in \mathbb{N}$.
2. If $\mathbb{F}$ is a finite field, then the group of nonzero elements of $\mathbb{F}$ (under multiplication) $\mathbb{F}^\times$ is cyclic.
3. If $\mathbb{F}_1$ and $\mathbb{F}_2$ are two finite fields of the same order, then they are isomorphic, i.e. for each prime number p and $n \in \mathbb{N}$, there is a unique finite field of order p^n up to isomorphism.
4. We have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m|n$.

Problem 1. True/False: $\mathbb{F}_4$ is a subfield of $\mathbb{F}_8$.

Problem 2. Let $F = \mathbb{F}_{p^n}$, and suppose α is a generator of $F^\times$ (why does α exist?). Let $K = \mathbb{F}_p(\alpha)$. The goal of this problem is to show $F = K$.

a) Explain why it is clear that $F \supseteq K$.

b) Let $x \in F$. Show $x \in K$ by considering the cases where $x = 0$ and $x \neq 0$ separately. Deduce that $F \subseteq K$.

Problem 3. Let α be a generator of $\mathbb{F}_{64}^\times$. It follows from Problem 2 that $\mathbb{F}_{64} = \mathbb{F}_2(\alpha)$. The goal of this problem is to explicitly construct a subfield of $\mathbb{F}_{64}$ isomorphic to $\mathbb{F}_4$.

a) Compute $|\mathbb{F}_{64}^\times|$ and $\mathrm{ord}_{\mathbb{F}_{64}^\times}(\alpha)$, the order of α in the group $\mathbb{F}_{64}^\times$.

b) Find an element β in terms of α so that $|\mathbb{F}_2(\beta)| = 4$. Then by Fact 3 above, it follows that $\mathbb{F}_4 \cong \mathbb{F}_2(\beta) \subseteq \mathbb{F}_{64}$.
Hint: You may find it helpful to recall some facts about cyclic groups. Find $n \in \mathbb{N}$ such that $\mathrm{ord}_{\mathbb{F}_{64}^\times}(\alpha^n) = |\mathbb{F}_4^\times|$.