Math 146: Homework 5
Due: Sunday, March 10, by 11:59pm
Please submit your solutions as a single PDF on Canvas

Reminders:

- You are encouraged to work together on homework. If you work with other students, please indicate who you worked with on this assignment.
- The usual extension policy applies to this assignment: if you would like an extension on this homework over the weekend, simply email the professor to ask for it. No justification is required.

1. This problem is relatively computational, with the aim of having you probe irreducibility in degrees larger than 3.

a) Find all eight irreducible polynomials in $\mathbb{F}_2[x]$ with degree at most 4.

b) Determine which of the following polynomials are irreducible in $\mathbb{Q}[x]$:

(i) $x^3 - 7x^2 + 16x - 1001$
(ii) $x^4 + x^3 - 1$
(iii) $x^4 + x^3 + x + 1$
(iv) $x^7 + 12x^5 - 24x + 18$
(v) (0 points; unfair, but not *so* unfair) $x^{1024} + 1$.

2. Let F be a field and K an extension of F. Let $f \in F[x]$ be a non-zero polynomial. Prove that the number of roots of f in K is at most $\deg f$.

3. Let p be a prime number. Let $\mathbb{F}_{p^2}$ be the field of order p^2. On your last homework, you proved that there is also a field of order p^3, which we'll denote $\mathbb{F}_{p^3}$. Prove that $\mathbb{F}_{p^3}$ is not an extension of $\mathbb{F}_{p^2}$.

4. Let p be an odd prime. Recall that we've shown there is a field of order p^2, denoted $\mathbb{F}_{p^2}$. Somewhat more concretely, $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(f)$ for some monic irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree 2. This problem will have you show that this field is essentially unique, in that all fields of order p^2 are isomorphic. In other words, you will show that it does not matter which irreducible polynomial f was chosen to construct $\mathbb{F}_{p^2}$. To this end, we'll keep in mind an arbitrary, but fixed, choice of f, and use the letter g for other polynomials.

a) Let $\alpha \in \mathbb{F}_{p^2}$, and consider the polynomial $g = (x - \alpha)^2 \in \mathbb{F}_{p^2}[x]$. Prove that g is in fact in $\mathbb{F}_p[x]$ if and only if $\alpha \in \mathbb{F}_p$.

b) Prove that every $\alpha \in \mathbb{F}_{p^2}$ that is not in $\mathbb{F}_p$ is the root of a monic irreducible polynomial of degree 2.

c) Prove that if $g \in \mathbb{F}_p[x]$ is monic irreducible of degree 2, then g has exactly two roots in $\mathbb{F}_{p^2}$. (*Hint:* How many such polynomials g are there?[1])

d) Finally, let $g \in \mathbb{F}_p[x]$ be any monic irreducible polynomial of degree 2. By part *d)*, there are two roots of g in $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(f)$. Let $a_g + b_g x + (f)$ be one of these roots.[2]

(i) Prove that $b_g \neq 0$.
(ii) Define a homomorphism $\phi_g \colon \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(f)$ by $\phi_g(x) = a_g + b_g x$ and $\phi_g(a) = a$ for all $a \in \mathbb{F}_p$. Prove that ϕ_g is a surjective homomorphism and that $\ker \phi_g = (g)$.

[1] Recorded on Homework 4, if you don't remember offhand.
[2] If this notation is confusing, please ask.

(iii) Conclude that $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_p[x]/(f)$.

e) (0 points) Think about how this picture extends to finite fields $\mathbb{F}_{p^k}$ for $k \geq 3$.