Math 146: Homework 6

Due: Sunday, April 7, 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. Let $a \in \mathbb{Z}$ be non-zero and not a perfect cube, and let $f \in \mathbb{Q}[x]$ be given by $f = x^3 - a$.

a) Prove that f is irreducible.

b) Prove that the splitting field L of f over $\mathbb{Q}$ is $L = \mathbb{Q}(\sqrt[3]{a}, \sqrt{-3})$, and that $[L : \mathbb{Q}] = 6$. (*Hint:* The three solutions in $\mathbb{C}$ to the equation $x^3 = 1$ are $x = 1$, $x = \frac{-1+\sqrt{-3}}{2}$, and $x = \frac{-1-\sqrt{-3}}{2}$.)

c) Prove that $\mathrm{Gal}(f) \simeq S_3$.

2. Let p be a prime. This problem will have you prove some properties of $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$. These properties are true for general finite fields $\mathbb{F}_{p^k}$, and we'll give a different proof in class of that more general statement.

a) Prove that every polynomial $f \in \mathbb{F}_p[x]$ with degree 2 splits completely in $\mathbb{F}_{p^2}$. (*Hint:* There's a very quick proof available if you use some results from Homework 5. Alternatively, you could follow the strategy suggested below for $\mathbb{F}_{p^3}$.)

We'll now show that every irreducible degree 3 polynomial in $\mathbb{F}_p[x]$ splits completely in $\mathbb{F}_{p^3}$.

b) Let $\alpha \in \mathbb{F}_{p^3}$, and suppose that α is not an element of $\mathbb{F}_p$. Prove that α is a root of some monic, irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree 3.

c) By considering the number of monic, irreducible, degree 3 polynomials in $\mathbb{F}_p[x]$ (which you found on an earlier homework assignment), prove that every irreducible degree 3 polynomial in $\mathbb{F}_p[x]$ splits completely in $\mathbb{F}_{p^3}$.

d) Decide whether the following statement is true or false, and explain your answer. Every degree 3 polynomial in $\mathbb{F}_p[x]$ splits completely in $\mathbb{F}_{p^3}$.

3. Let p be a prime and let $q = p^k$ for some integer $k \geq 1$. Let $\mathbb{F}_q$ denote the finite field with q elements, and recall that $\mathbb{F}_q$ is an extension of $\mathbb{F}_p$. This problem will explore some of the properties of an explicit family of polynomials. It has four parts, one of which runs onto the next page.

a) Prove that every element of $\mathbb{F}_q$ is a root of the polynomial $x^q - x \in \mathbb{F}_p[x]$, with multiplicity 1. (*Hint:* Observe that $x^q - x = x \cdot (x^{q-1} - 1)$. What do we know about the non-zero elements of $\mathbb{F}_q$?)

b) In fact, prove that if we consider it in the ring $\mathbb{F}_q[x]$,[1] the polynomial $x^q - x$ splits completely as $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$.

c) Prove that if $f \in \mathbb{F}_p[x]$ is an irreducible factor of $x^q - x$ in $\mathbb{F}_p[x]$, then the degree of f is at most k.

[1] Note the distinction! $\mathbb{F}_q$ vs. $\mathbb{F}_p$. This is the only part of the problem where we'll use $\mathbb{F}_q[x]$.

d) Describe completely how the polynomials $x^p - x$, $x^{p^2} - x$, and $x^{p^3} - x$ factor in $\mathbb{F}_p[x]$. (*Hint:* The statements of the various parts of Problem 2 above may be useful, but you don't need to understand their proofs.)