Mike O'Sullivan
Department of Mathematics
San Diego State University

Fall 2008

Homework V

due: Wed. 11/26/08

Clarity of exposition is crucial in this assignment. You work should be understandable to a fellow student. You may work together to solve problems, but your solutions should be written independently.

Problem 1: Minimal polynomials for elements of $\mathbb{Q}(\sqrt[3]{2})$ (see [A] 3.1#4,5).

(a) Find the minimum polynomial of $\sqrt[3]{2}+1$ over $\mathbb{Q}$. [There is a clever way that involves little computation, but don't feel obliged to use it!]

(b) Find the minimum polynomial of $\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbb{Q}$.

Problem 2: Sixth roots of unity.

(a) Factor x^6-1 completely over $\mathbb{Q}$.

(b) Show that the splitting field of x^6-1 is of degree 2 over $\mathbb{Q}$.

Problem 3: Let E be the splitting field of x^6-2.

(a) Show that x^6-2 is irreducible over $\mathbb{Q}$.

(b) Analyze the splitting field of x^6-2 over $\mathbb{Q}$ in three ways:

- Adjoin a sixth root of unity, then split x^6-2.
- Adjoin $\sqrt{2}$ and refactor x^6-2. Then split the factors.
- First construct the splitting field, K, of x^3-2 in two steps. For each step, refactor x^6-2. Finally split the irreducible factors of x^6-2 over K.

(c) What is $[E:Q]$?

(d) Identify all of the subfields of E that you encountered.

Problem 4: Irreducible polynomials over $\mathbb{F}_p$. Suppose you have formulas for the number of irreducible monic polynomials of degree m over $\mathbb{F}_p$ for each $m < n$. Using some combinatorial arguments you can then compute the number of monic reducible polynomials of degree n. Subtracting this from the number of monic polynomials of degree n yields the number of monic irreducible polynomials of degree n.

(a) Show that the number of monic irreducible quadratics over $\mathbb{F}_p$ is $(p^2 - p)/2$.

(b) Show that the number of monic irreducible cubics over $\mathbb{F}_p$ is $(p^3 - p)/3$.

(c) You might want to guess at a general formula. A different counting method yields the result more easily than the one above. Try this if you want, noting:

- For $a \in \mathbb{F}_{p^n}$, a is in no proper subfield iff the minimal polynomial for a has degree n.
- Each monic irreducible of degree n has n distinct roots in $\mathbb{F}_{p^n}$.

Problem 5:

(a) Find all irreducible polynomials over $\mathbb{F}_2$ of degree at most 4. You should write a few sentences justifying your list.

(b) One of the irreducible polynomials of degree 4 has roots which are not primitive. Which one?

(c) Construct the field with 16 elements using one of the primitive irreducible polynomials of degree 4: Make a table showing the powers of the primitive element, say α and the corresponding vector form, using the basis $\{1, \alpha, \alpha^2, \alpha^3\}$. Give also the multiplicative order of each element and its minimal polynomial.

(d) Identify the subfield $\mathbb{F}_4$.

(e) Factor over $\mathbb{F}_4$ the irreducible polynomial that you chose to construct $\mathbb{F}_{16}$.

Please read the following problems and their solutions in Ash's text. I've grouped problems that are related. These should help you solve the assigned problems.

- §3.1 pr. 1,2; 3,10; 4,5; 9.
- §3.2 pr. 1,2,3,6; 5.
- §3.3 pr. 1; 4.
- §3.4 pr. 1,2,3,4.
- §3.6 pr. 1,2; 3; 5,6.

- §6.4 1,2,3; 9,10.