Math 5613

Assignment 12

Due Friday, November 14

Part one: Reading. Read through Chapter 14.4 in the textbook (more or less: see the "homework" page on the course web page for precise daily goals).

Part two: Problems to solve and write up.

I want your effort on both the problem-solving and the writeup to be collaborative. This week, you'll again be responsible for turning in writeups of three problems, but you'll also have to arrange to meet with me on Friday or early in the next week to present another orally.

Throughout, assume unless otherwise indicated that rings are commutative with 1, and that notation remains intuitive: $F \subset K$ are fields, $n \in \mathbb{Z}$, etc.

1. Consider $F = \mathbb{F}_8 = \dfrac{\mathbb{F}_2}{(x^3 + x + 1)}$. Elements of $\mathbb{F}_8$ may be expressed either as $\mathbb{F}_2$-linear combinations of the basis elements $\{1, x, x^2\}$ or as powers of x.

   Write out the following 8×8 tables:

   - The multiplication table for F, where each element is named as a vector.
   - The addition table for F, where each nonzero element is named as a power of x.

2. Recall that $\dfrac{\mathbb{F}_3[x]}{(x^3 - x - 1)} \cong \dfrac{\mathbb{F}_3[y]}{(y^3 - y + 1)}$ since both are isomorphic to $\mathbb{F}_{27}$. Find an explicit isomorphism.

3. Let $q = p^m$, and define the map $\mathrm{Frob}_q = (\mathrm{Frob}_p)^m : \mathbb{F}_q \to \mathbb{F}_q$. Prove that $\mathrm{Frob}_q = \mathrm{id}_{\mathbb{F}_q}$.

4. Let $f \in \mathbb{F}_p[x]$ be a squarefree polynomial, and write $f = \prod_{i=1}^{k} q_i$ with irreducible factors q_i. Let $g \in \mathbb{F}_p[x]$ be such that $\deg g \lneqq \deg f$. Prove that the following are equivalent:

   (a) Writing $g(x^p) = fQ + R$ with $\deg R \lneqq \deg g$ (as guaranteed by the division algorithm) yields $R = g(x)$.

   (b) f divides $g(x^p) - g(x)$.

   (c) f divides $\prod_{s \in \mathbb{F}_p} (g(x) - s)$.

   (d) Every q_i divides $g(x) - s$ for some $s \in \mathbb{F}_p$.

   (e) $g(x)$ is congruent to a constant modulo q_i for each i.

[Hint: Factor $x^p - x$ as a product of linear polynomials. What does this have to do with our setup?]

5. Let $f \in \mathbb{F}_p[x]$ be squarefree, and write $f = \prod_{i=1}^{k} q_i$ for distinct irreducibles q_i. Let $V = \{g \in \mathbb{F}_p[x] : \deg g \lneq \deg f \text{ and } f \text{ divides } g(x^p) - g(x)\}$. Prove that V is a k-dimensional $\mathbb{F}_p$-vector space.

   [Hint: Show that $g \in V$ implies q_i divides $g - s$ for some $s \in \mathbb{F}_p$, and hence $g \equiv s \pmod{q_i}$. Then use Sun Tzu's theorem to establish the cardinality of V.]

6. Prove that Berlekamp's factorization algorithm works. That is, for $f \in \mathbb{F}_p[x]$, prove that running the algorithm will find all the irreducible factors of f.

   (Berlekamp's algorithm is described in problem 14.3.16 on page 590; it depends on a understanding a moderately complicated setup which is described in problems 12–15. You may assume the results of those problems without proof.)

7. Let $f = x^5 + x^2 + 4x - 1 \in \mathbb{F}_7[x]$. Compute the remainders when x^7, x^{14}, x^{21}, and x^{28} are reduced modulo (f). Show your work, as if you didn't have access to a computer algebra system.

8. Let $f = x^5 + x^2 + 4x - 1 \in \mathbb{F}_7[x]$. Use Berlekamp's factorization algorithm to find the irreducible factorization of f. (Talk the reader through the computation as if neither of you had access to a computer algebra system. You may, of course, suppress tedious details such as row-reduction.)

9. Let $F = \mathbb{Q}(\sqrt{1 + \sqrt{2}})$. Find the Galois closure of F over $\mathbb{Q}$.

10. Find, with proof, a primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.

11. Find an example of field extensions $L/K/F$ such that $[L : K]$ and $[K : F]$ are powers of the same prime p, L is Galois over K, but, if $\overline{L}$ is the Galois closure of L over F, then $[\overline{L} : F]$ is not a power of p.

12. Suppose F has characteristic zero and K/F and L/F are both finite. Set $A = K \otimes_F L$. Prove that A has no nonzero nilopotent elements (i.e., elements a satisfying $a^n = 0$ for some n).

    [Recall the definition: The **tensor product** $K \otimes_F L$ is the F-vector space spanned by formal symbols called "simple tensors" $k \otimes \ell$ for $k \in K$, $\ell \in L$, and subject to the bilinearity relations (for all $f \in F$, $k \in K$, etc.):

    - $(k_1 + k_2) \otimes \ell = (k_1 \otimes \ell) + (k_2 \otimes \ell)$.
    - $k \otimes (\ell_1 + \ell_2) = (k \otimes \ell_1) + (k \otimes \ell_2)$.
    - $f(k \otimes \ell) = (fk) \otimes \ell = k \otimes (f\ell)$.

(Please assume without proof that $K \otimes_F L$ has basis given by the $\{\alpha_i \otimes \beta_j\}$ where $\{\alpha_i\}$ and $\{\beta_j\}$ form bases for K and L, respectively, as F-vector spaces.)

We make $K \otimes_F L$ into a ring by setting $(k_1 \otimes \ell_1) \cdot (k_2 \otimes \ell_2) = k_1 k_2 \otimes \ell_1 \ell_2$ for all $k_1, k_2 \in K$ and $\ell_1, \ell_2 \in L$.]

[Hint: We know that K/F is simple, so there exists a primitive element α, meaning that $K \cong \dfrac{F[x]}{(p)}$, where p is the minimal polynomial for α over f. Prove that $K \otimes_F L \cong \dfrac{K[x]}{(p)}$.]

Part three: Estimate the time you spent on this assignment. I will pay attention to this in writing future assignments. Meanwhile, if it's taking you longer than you think is reasonable, please talk to me so we can come up with a strategy.