Problem Set 11

Problems with (HW) are due Tuesday 11/29 at 11:00 in class. Your homework should be easily legible, but need not be typed in Latex. Use full sentences to explain your solutions, but try to be concise as well. Think of your audience as other students in the class.

Exercises 11.1. Irreducible polynomials over $\mathbb{F}_2$

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

(b) (HW) Find all all irreducible polynomials over $\mathbb{F}_2$ of degree 5. Use the list from part (a) to explain your result. Notice any patterns in the list of polynomials.

(c) (HW) Determine how many irreducible polynomials of degree 6 there are over $\mathbb{F}_2$ based on part (a). Justify your answer briefly.

Exercises 11.2. (Discussion) The field $\mathbb{F}_{2^3}$.

(a) Construct the field $\mathbb{F}_8$ using one of the polynomials from the previous problem that has the appropriate degree (there are two). Make a table showing the powers of the primitive element, call it η, and the corresponding vector form, using the basis $\{1, \eta, \eta^2\}$.

(b) Show that the polynomial that you did not choose also has roots in $\mathbb{F}_8$.

Exercises 11.3. (HW)

(a) One of the irreducible polynomials of degree 4 in 11.1(a) has roots which are not primitive. Which one?

(b) 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, call it η, and the corresponding vector form, using the basis $\{1, \eta, \eta^2, \eta^3\}$. Give also the multiplicative order of each element and its minimal polynomial.

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

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

(e) How many elements of $\mathbb{F}_{16}$ are primitive?

Exercises 11.4. (HW) The field $\mathbb{F}_{3^2}$.

(a) Write a multiplication table for $\mathbb{F}_3[x]/\langle x^2 + x + 2\rangle$. [You may omit 0. It may be easier to take the elements in the order $1, x, x+1, x+2$ followed by twice each.]

(b) Find all irreducible polynomials of degree 2 over $\mathbb{F}_3$ and find their roots in the table you constructed.

Exercises 11.5. (HW) Factoring a polynomial over different fields.

(a) Factor $x^9 - x$ over $\mathbb{F}_3$.

(b) Factor $x^5 + x^4 + 1$ over $\mathbb{F}_2$ (it is reducible!), $\mathbb{F}_4$ and $\mathbb{F}_8$.

(c) Factor $x^{16} - x$ over $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_{16}$.

Exercises 11.6. Let $n > m$ be positive integers and $d = \gcd(n, m)$. Show that the intersection of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ is $\mathbb{F}_{p^d}$ as follows.

(a) Recall that the remainder $x^n - 1$ divided by $x^m - 1$ is $x^r - 1$ where r is the remainder when n is divided by m.

(b) Show that the gcd of $x^n - 1$ and $x^m - 1$ is $x^d - 1$.

(c) (HW) Combine the previous results and the theorem that the roots of $x^{p^n} - x$ are the elements of $\mathbb{F}_{p^n}$ to conclude that $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ iff d divides n. (Strictly speaking $\mathbb{F}_{p^n}$ has a subfield isomorphic to $\mathbb{F}_{p^d}$. See 11.10.)

Exercises 11.7. (Optional)The field $\mathbb{F}_{81}$.

(a) (Discussion) The polynomials $x^2 + x + 2$ and $x^2 + 2x + 2$ are both irreducible over $\mathbb{F}_3$. Can you construct $\mathbb{F}_{81}$ by using one of these polynomials and then the other?

(b) (Optional) In a computer algebra system use $m(x) = x^4 + x + 2$ and $r(x) = x^4 + 2x + 2$ to construct two versions of $\mathbb{F}_{81}$. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that each composition is an automorphism of the appropriate version of $\mathbb{F}_{81}$.

(c) (Optional) Factor $x^{80} - 1$ over $\mathbb{F}_3$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_3[x]/m(x)$.

Exercises 11.8. (Optional)The field of 64 elements.

(a) The polynomials $m(x) = x^6 + x + 1$ and $r(x) = x^6 + x^5 + x^4 + x + 1$ are both irreducible over $\mathbb{F}_2$. Using a computer algebra system construct two versions of $\mathbb{F}_{64}$, using $m(x)$ for one and $r(x)$ for the other. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that each composition of the two isomorphisms is an automorphism of the appropriate version of the field.

(b) Factor $x^{63} - 1$ over $\mathbb{F}_2$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_2[x]/m(x)$. Use Sage, but also use your understanding of the theory.

(c) The field $\mathbb{F}_{64}$ can also be constructed as an extension of $\mathbb{F}_4$. Construct $\mathbb{F}_4$, then factor $x^{63} - 1$ in $\mathbb{F}_4[x]$. Choose one of the factors of degree 3 to construct $\mathbb{F}_{64}$.

(d) Now create $\mathbb{F}_8$ using an irreducible polynomial of degree 3 over $\mathbb{F}_2$, then factor $x^{63} - 1$, then create $\mathbb{F}_{64}$ using an irreducible polynomial of degree 2 in $\mathbb{F}_8[x]$.

Exercises 11.9. (Challenge) The number of irreducible polynomials.

(a) Let $a(n)$ denote the number of degree-n irreducible polynomials over $\mathbb{F}_p$ for p prim4. Prove that

$$p^n = \sum_{d|n} d \cdot a(d).$$

Hint: use the result about the factorization of $x^{p^d} - x$ factors over $\mathbb{F}_{p^d}$ and about subfields of $\mathbb{F}_{p^n}$.

(b) Prove that

$$\lim_{n\to\infty} \frac{a(n)}{p^n} = 0,$$

meaning that irreducible polynomials are "sparse" in $\mathbb{F}_p[x]$.

Exercises 11.10. (Challenge) The algebraic closure of $\mathbb{F}_p$. This problem extends 11.6, which showed that we may consider $\mathbb{F}_{p^d}$ as contained in $\mathbb{F}_{p^n}$ if and only if $d|n$.

(a) Let $\overline{\mathbb{F}}_p = \bigcup_{t\geq 1} \mathbb{F}_{p^t}$. Prove that F is a field.

(b) Prove that $\overline{\mathbb{F}}_p$ is algebraically closed.

(c) Prove that every element of $\overline{\mathbb{F}}_p$ is algebraic over $\mathbb{F}_p$ so there is no algebraically closed field properly contained in $\overline{\mathbb{F}}_p$.

(d) Conclude that $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_{p_n}$ for any n.