Mike O'Sullivan
Department of Mathematics
San Diego State University

Spring 2016

Math 627B: Modern Algebra I
HW 4

Due: Tuesday 4/12, 2016.

1 Problems

Problem 1: The field $\mathbb{F}_{81}$.

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

Problem 2: 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 $\mathbb{F}_8[x]$.

Problem 3: 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)** Show 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)** Use the fact that the set of roots of $x^{p^n-1} - 1$ is exactly the nonzero elements of $\mathbb{F}_{p^n}$.
- **(d)** Conclude that $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ iff d divides n.

Problem 4: Make a table showing the possible multiplicative orders and the number of elements of each order for $\mathbb{F}_{64}$, $\mathbb{F}_{128}$, and $\mathbb{F}_{256}$. Relate this information to subfields (refer to the previous problem).

Problem 5: 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 $\mathbb{F}_{p^n}$.

Problems 6: For a given prime p, let $I(d)$ be the set of irreducible polynomials of degree d over $\mathbb{F}_p$. Show that for $n > 0$,

$$\prod_{d|n} \prod_{f \in I(d)} f = x^{p^n} - x$$

Problems 7: Show that for any $\alpha \in \mathbb{F}_q$,

$$1 + \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{q-2} = \begin{cases} 1 \text{ if } \alpha = 0 \\ -1 \text{ if } \alpha = 1 \\ 0 \text{ otherwise} \end{cases}$$