Mike O'Sullivan
Department of Mathematics
San Diego State University Spring 2012

Math 627B: Modern Algebra II
Homework III

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

(a) In Sage, 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 $\mathbb{F}_{81}$.

(b) 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 $\mathbb{F}_2$. In Sage, use $m(x)$ and $r(x)$ to construct two versions of $\mathbb{F}_{64}$. 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 $\mathbb{F}_{64}$. The following code will show how Sage treats elements of this new object. It appears that there is no way in Sage to create a "field;" the code below only creates a ring. In particular FF.list() will not work.

```
FF.<b> = F4.extension(x^3+a)
[b^i for i in [1..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: 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.

Problem 4: 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.