MATH 5591H HOMEWORK 10

BRENDAN WHITAKER

13.5 Exercises

5. *For any prime p and any nonzero $a \in \mathbb{F}_p$, prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach – prove first that if α is a root then $\alpha + 1$ is also a root. Another approach – suppose it's reducible and compute derivatives.]*

Proof. Suppose α is a root. Then we have $\alpha^p - \alpha + a = 0$. Behold:

$$\begin{aligned}(\alpha+1)^p - (\alpha+1) + a &= \left(\sum_{k=0}^{p} \binom{p}{k} \alpha^k\right) - \alpha - 1 + a \\ &= \left(\sum_{k=1}^{p-1} \binom{p}{k} \alpha^k\right) + \alpha^p - \alpha + a \\ &= \sum_{k=1}^{p-1} \binom{p}{k} \alpha^k \\ &= \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} \alpha^k.\end{aligned} \tag{1}$$

We claim that $\frac{p!}{k!(p-k)!}$ is divisible by p for all integer values of k in the range $[1, p-1]$. Note for these values of k that $p \nmid (k!(p-k)!)$ but that $p|p!$, and the binomial coefficient is an integer, so we must have that $p|\left(\frac{p!}{k!(p-k)!}\right)$. Thus:

$$\sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} \alpha^k \mod p \equiv 0.$$

And since we are over $\mathbb{F}_p$, we know that $\alpha + 1$ must then be a root. Now note that by induction, we have that if any $\alpha \in \mathbb{F}_p$ is a root, then all elements of $\mathbb{F}_p$ are roots, hence 0 is a root. So we have:

$$0^p - 0 + a = 0 \Rightarrow a = 0,$$

which is a contradiction, since we said $a \neq 0$. So we must have that $\nexists \alpha \in \mathbb{F}_p$ such that α is a root of the given polynomial. So let α be a root, then $\alpha \notin \mathbb{F}_p$. Then consider the extension $\mathbb{F}_p(\alpha)$. It must contain $\alpha + k$, for all $k \in \mathbb{F}_p$. Then $f(x)$ must be the product of all minimal polynomials. Also since $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p(\alpha + k)$ we know that they all have the same degree, say m. Then $p = km$, which tells us $k = 1$ since p prime. Then we must have that the minimal polynomial is f and it is irreducible. Now we show that it is separable. Simply recall from Proposition 37 in the book that every irreducible polynomial over a finite field is separable. □

13.6 Exercises

6. *Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.*

Proof. Let n be odd, and let $\varphi(x)$ be Euler's totient function. Then $\varphi(n) = \varphi(2n)$ since the only factor of $2n$ which is not already a factor of n is 2, and $2 \nmid n$ since n is odd. So then $\Phi_{2n}(x)$ has the same degree as $\Phi_n(-x)$. So they both have the same number of roots. But note we know that if ω is an n-th root of unity, then we know that $-\omega$ is also an n-th root of unity and also a $2n$-th root of unity. Then the roots of $\Phi_n(-x)$ are also roots of $\Phi_{2n}(x)$, and since we already proved that they

Date: SP18.

have the same number of roots, we know they are the same polynomial. (Note I got the idea for this proof from Jack Peltier) □

14.3 Exercises

4. *Construct a finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?*

We simply need to construct an irreducible polynomial of degree 4 over $\mathbb{F}_2$. Consider $f(x) = x^4+x^3+x^2+x+1$. Clearly $1, 0$ are not roots. So we need to check if it is divisible by any irreducible quadratics. So it would have to b $(x^2+x+1)^2$, as this is the only such quadratic. We have:

$$\begin{aligned}(x^2+x+1)^2 &= x^4+x^3+x^2+x^3+x^2+x+x^2+x+1 \\ &= x^4+x^2+1.\end{aligned} \tag{2}$$

So f is irreducible. Thus $\mathbb{F}_2[x]/(f) \cong \mathbb{F}_{2^4}$, a finite field of 16 elements. Note that the multiplicative group of this field is isomorphic to $\mathbb{Z}_{15}$ since we have 15 nonzero elements. Since we want to know how many generators we have, recall that the generators of $\mathbb{Z}_{15}$ are exactly those whose equivalence classes are coprime with the order. So we have $\varphi(15) = 8$ generators.

$$\begin{aligned}(x+1)^2 &= x^2+1 \\ (x+1)(x^2+1) &= x^3+x+x^2+1 \\ (x+1)(x^3+x^2+x+1) &= x^4+x^3+x^2+x+x^3+x^2+x+1 \\ &= x^4+1 \\ (x+1)^5 &= (x+1)(x^4+1) = x^5+x+x^4+1.\end{aligned} \tag{3}$$

And since $\mathbb{Z}_5$ is the largest subgroup in the lattice of $\mathbb{Z}_1 5$, we know that the elements with largest order not equal to 15 have order 5, and this element has order > 5 since $(x+1)^5 \neq 1$. So it must have order 15. Thus $x+1$ is a generator.