Homework 3

Kevin Guillen

MATH 202 — Algebra III — Spring 2022

Problem 13.5.2 Find all irreducible polynomials of degrees 1,2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

Proof. For irreducible degree 1 polynomials it is pretty obvious that the only ones over $\mathbb{F}_2$ are $x+1$ and x.

For irreducible degree 2 polynomials, we know a quadratic polynomial must have linear factors if it were to be reducible. Meaning we can identify irreducible quadratic polynomial, $p(x)$, over $\mathbb{F}_2$ if it satisfies $p(1) = p(0) = 1$. We verify this requirement with the only quadratic polynomials of $\mathbb{F}_2$:

- $p(x) = x^2 + x + 1$, verifying $p(0) = 0 + 0 + 1 = 1$ and $p(1) = 1 + 1 + 1 = 1$, irreducible.
- $p(x) = x^2 + x$, verifying $p(0) = 0 + 0 = 0$, reducible.
- $p(x) = x^2 + 1$, verifying $p(0) = 0 + 1 = 1$, but $p(1) = 1 + 1 = 0$, reducible.
- $p(x) = x^2$, verifying $p(0) = 0$, but $p(1) = 1$, reducible.

so we have that the only irreducible polynomial of degree 2 over $\mathbb{F}_2$ is $x^2 + x + 1$.

For irreducible degree 4 polynomials the story a slightly different. We can still eliminate polynomials if they have linear factors through the same method as above. We then just have to check if any of the degree 4 polynomials that are left are a product of irreducible quadratic polynomials, that is, if any of them are equal to $(x^2 + x + 1)^2$. We see though,

$$(x^2 + x + 1)^2 = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 = x^4 + x^2 + 1$$

so we have eliminated that polynomial. We also note though that this polynomial will have to have an odd number of terms because if we plug in 1 to a polynomial of even terms the result will be 0. So we it leaves us with the following polynomials which we verify as before:

- $p(x) = x^4 + x^3 + x^2 + x + 1$, verifying, $p(0) = 0 + 0 + 0 + 0 + 1 = 1$ and $p(1) = 1 + 1 + 1 + 1 + 1 = 1$, irreducible.
- $p(x) = x^4 + x^3 + 1$, verifying, $p(0) = 0 + 0 + 1 = 1$ and $p(1) = 1 + 1 + 1 = 1$, irreducible.
- $p(x) = x^4 + x + 1$, verifying, $p(0) = 0 + 0 + 1 = 1$ and $p(1) = 1 + 1 + 1 = 1$, irreducible.

Meaning the above 3 polynomials are the only degree 4 irreducible polynomials over $\mathbb{F}_2$.

So to recap, all our irreducible polynomials of the desired degrees are: x, $x+1$, x^2+x+1, x^4+x+1, x^4+x^3+1, and $x^4+x^3+x^2+x+1$. So let us compute their product in this order,

$$\begin{aligned}
x(x+1) &= x^2+x \\
(x^2+x+1)(x^2+x) &= x^4+x^3+x^3+x^2+x^2+x = x^4+x \\
(x^4+x+1)(x^4+x) &= x^8+x^5+x^5+x^2+x^4+x = x^8+x^4+x^2+x \\
(x^4+x^3+1)(x^8+x^4+x^2+x) &= x^{12}+x^8+x^6+x^5+x^{11}+x^7+x^5+x^4+x^8+x^4+x^2+x \\
&= x^{12}+x^{11}+x^7+x^6+x^2+x
\end{aligned}$$

our final product,

$$\begin{aligned}
(x^4+x^3+x^2+x+1)(x^{12}+x^{11}+x^7+x^6+x^2+x) &= x^{16}+x^{15}+x^{11}+x^{10}+x^6+x^5 \\
&+x^{15}+x^{14}+x^{10}+x^9+x^5+x^4 \\
&+x^{14}+x^{13}+x^9+x^8+x^4+x^3 \\
&+x^{13}+x^{12}+x^8+x^7+x^3+x^2 \\
&+x^{12}+x^{11}+x^7+x^6+x^2+x \\
&= x^{16}+x.
\end{aligned}$$

Over $\mathbb{F}_2$ $x^{16}+x = x^{16}-x$, showing the desired product. □

Problem 13.5.3 Prove that d divides n if and only if x^d-1 divides x^n-1. [Note that if $n = qd+r$ then $x^n-1 = (x^{qd+r}-x^r)+(x^r-1)$.]

Proof. Assuming that d divides n then there exists q such that $n = qd$. We can apply the noted equation and have,

$$x^n-1 = x^{qd}-x^0+x^0-1 = x^{qd}-1.$$

Where we can factor out x^d-1 from above to get,

$$\begin{aligned}
x^n-1 &= x^{qd}-1 \\
&= (x^d-1)(x^{(q-1)d}+x^{(q-2)d}+\cdots+x^{(q-(q+1))d}+1)
\end{aligned}$$

meaning that if d divides n then x^d-1 divides x^n-1 as we see above.

Now we assume that d doesn't divide n, and we want to show that implies then that x^d-1 does not divide x^n-1. Because d does not divide n we have that, $n = qd+r$ where $0 < r < d$. So applying the noted equation we have,

$$\begin{aligned}
x^n-1 &= x^{qd+r}-x^r+x^r-1 \\
&= x^r(x^{qd}-1)+(x^r-1)
\end{aligned}$$

$$= x^r(x^d - 1)(x^{(q-1)d} + x^{(q-2)d} + \cdots + x^{(q-(q+1))d} + 1) + (x^r + 1)$$

we see from above that when we attempt to divide $x^n - 1$ by $x^d - 1$ we have remainder $x^r + 1$, and we know $x^r + 1$ can't be divided by $x^d - 1$ since $0 < r < d$. Therefore if d does not divide n then $x^d - 1$ does not divide $x^n - 1$.

All together we have d divides n if and only if $x^d - 1$ divides $x^n - 1$. $\square$

Problem 13.5.5 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. Let $p(x) = x^p - x + a$ and let α be a root of $p(x)$. We see $\alpha + 1$ is also a root of $p(x)$ through the following,

$$\begin{aligned}
p(\alpha+1) &= (\alpha+1)^p - (\alpha+1) + a && \text{Proposition 35: } (a+b)^p = a^p + b^p \\
&= \alpha^p + 1^p - \alpha + 1 + a \\
&= \alpha^p - \alpha + a \\
&= p(\alpha) \\
&= 0.
\end{aligned}$$

We have by induction then that $\alpha + k$ for all $k \in \mathbb{F}_p$ is also a root of $p(x)$. Because of this we know that α cannot be a root in $\mathbb{F}_p$ since that would mean that 0 is also a root of $p(x)$ but that could only be the case if $a = 0$ which goes against the given assumption that $a \neq 0$. Therefore if α were to be a root of $p(x)$, it must be in some extension of $\mathbb{F}_p$

Now assuming that α is in some extension of $\mathbb{F}_p$ and is a root of $p(x)$, then so are $\alpha + k$ for all $k \in \mathbb{F}_p$ by the reasoning above. This means then that for some d that the degree of $\alpha + k$ is d for all $k \in \mathbb{F}_p$ over $\mathbb{F}_p$.

Before we continue from here we note that $p(x)$ is separable since $D_x p(x) = -1 \neq 0$.

Now because $p(x)$ is separable we have that $p(x)$ must be the product of all the minimal polynomials of $\alpha + k$ for all $k \in \mathbb{F}_p$. Since they all have degree d we have that $p = dn$ for some n. Recall though that p was prime, so we have either $d = 1$ or $n = 1$. In the first case, that would imply that $\alpha \in \mathbb{F}_p$, but we already showed that can't be. Meaning we have that $n = 1$, but that means $p(x)$ is irreducible because it is the minimal polynomial, as desired. $\square$

Problem 13.5.6 Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive Wilson's Theorem: $(p-1)! \equiv -1 \mod p$.

Proof. We know from the textbook that the field $\mathbb{F}_{p^n}$ is the field whose p^n elements are the solutions to $x^{p^n} - x = 0$. We also know that $x^{p^n} - x$ is separable meaning it has p^n distinct roots, which gives us,

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha)$$

note though that $0 \in \mathbb{F}_{p^n}$, so we will be able to factor out an x on the RHS, and it is clear we can factor out an x on the LHS, so dividing both by x we get,

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$$

since $\mathbb{F}_{p^n}^\times$ is of order $p^n - 1$ ($\mathbb{F}_{p^n} - \{0\}$) which we know from the example in D&F.

Now if we evaluate the above equality for $x = 0$ we get,

$$\begin{aligned}
-1 &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-\alpha) \\
-1 &= (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha && \text{multiplying by } (-1)^{p^n-1} \\
(-1)^{p^n-1} - 1 &= (-1)^{p^n-1}(-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha \\
(-1)^{p^n} &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha
\end{aligned}$$

meaning the product of non-zero elements of $\mathbb{F}_{p^n}$ will be 1 when $p = 2$ and -1 otherwise, as desired.

Now for a non-even p and $n = 1$ we have,

$$-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha$$

so if we take modulo p we see that $(p-1) \cdot (p-2) \cdot \cdots \cdot 2 \cdot 1 = -1$ we have that $(p-1)! \equiv -1 \mod p$ as desired. $\square$

Problem 13.5.9 Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence prove that $\binom{pn}{pi} \equiv \binom{n}{i} \mod p$.

Proof. We can use the Binomial Theorem to express $(1+x)^{pn}$ as,

$$(1+x)^{pn} = \sum_{k=0}^{pn} \binom{pn}{k} x^k$$

so if we have $k = pi$ we see the coefficient of x^{pi} is indeed $\binom{pn}{pi}$

We know that $\mathbb{F}_p$ is obviously of characteristic p so, again by proposition 35, we have $(1+x)^{pn} = 1 + x^{pn} = (1+x^p)^n$, so over $\mathbb{F}_p$ we have that $\binom{pn}{pi}$ is the coefficient of $(x^p)^i$ in $(1+x^p)^n$.

Also $(1+x)^{pn}$ being equal to $(1+x^p)^n$ implies,

$$(1+x^p)^n = \sum_{k=0}^{n} \binom{n}{k} (x^p)^k = \sum_{k=0}^{pn} \binom{pn}{k} x^k$$

when over $\mathbb{F}_p$, therefore $\binom{pn}{pi} \equiv \binom{n}{i} \mod p$ as desired. □

Problem 13.6.2 Let ζ_n be the primitive n^{th} root of unity and let d be a divisor of n. Prove that ζ_n^d is a primitive $(n/d)^{th}$ root of unity.

Proof. Notice that,

$$(\zeta_n^d)^{n/d} = \zeta_n^n = 1$$

meaning then that ζ_n^d is an $(n/d)^{th}$ root of unity. Now let us consider i where $1 \leqslant i < n/d$, we see that,

$$(\zeta_n^d)^i = \zeta_n^{di}$$

and recall that d is a divisor of n and $i < n/d$ therefore $1 \leqslant di < n$, and so we have $\zeta_n^{di} \neq 1$, but this also means then that $(\zeta_n^d)^i \neq 1$.

Thus the order of ζ_n^d is exactly n/d, meaning it generates the cyclic group of all the other $(n/d)^{th}$ roots of unity. Which means that ζ_n^d is a primitive $(n/d)^{th}$ root of unity, as desired. □

Problem 13.6.3 Prove that if a field contains the n^{th} roots of unity for n odd then it also contains the $2n^{th}$ roots of unity.

Proof. Let K be a field containing the n^{th} roots of unity for an odd n. Now let ζ represent an $2n^{th}$ root of unity. So if $\zeta^n = 1$ that means that $\zeta \in K$. So let us assume that $\zeta^n\ neq 1$, we know though by definition that $\zeta^{2n} = 1$, so ζ^n is a root of unity for $x^2 - 1$.

We know however that the roots of this polynomial are ± 1, and by assumption that $\zeta^n \neq 1$ so it must be that $\zeta^n = -1$. Note though that,

$$(-\zeta)^n = -1^n \zeta^n = -1^n(-1) = -1^{n+1}$$

but n is odd, so this is 1, meaning that $-\zeta \in K$. Recall though that K is a field so we have that $\zeta \in K$ as desired. □

Problem 13.6.4 Prove that if $n = p^k m$ where p is a prime and m is relatively prime to p then there are precisely m distinct n^{th} roots of unity over a field of characteristic p.

Proof. Let K again be a field, but with characteristic p. The roots of unity over K are the roots in K that satisfy,

$$x^n - 1 = 0$$

by definition, but since $n = p^k m$ this is the same as,

$$x^n - 1 = x^{p^k m} - 1 = (x^m - 1)^{p^k}$$

the last equality comes again from Proposition 35. This means then the roots of unity over K are the roots of $x^m - 1$. Now we just want to show that they are distinct. Because $(m, p) = 1$, $x^m - 1$ and $D_x(x^m - 1)$ will be relatively prime, and by Proposition 33, $x^m - 1$ will be separable, meaning no repeated roots. Therefore there is m distinct n^{th} roots of unity over K which is of characteristic p. □

Problem 13.6.5 Prove that there are only a finite number of roots of unity in any finite extension K of $\mathbb{Q}$.

Proof. Recall the Euler totient function φ, we have that $\varphi(n) \geqslant \frac{\sqrt{n}}{2}$ for $1 \leqslant n$. Now letting K be an extension of $\mathbb{Q}$ with infinite number of roots of unity. Then we have that for $N \in \mathbb{N}$ that there is some n such that $4N^2 < n$ and that there exists some n^{th} root of unity in K which we denote ζ.

Therefore

$$[K : \mathbb{Q}] \geqslant [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) \geqslant \frac{\sqrt{n}}{2} > N$$

recall though that N was arbitrary, meaning that $N < [K : \mathbb{Q}]$ for every natural number N. Showing that $[K : \mathbb{Q}]$ is infinite. It follows from this that any finite extension of $\mathbb{Q}$ there will be only a finite number of roots of unity. □

Problem 13.6.6 Prove that for n odd, $n > 1$, $\psi_{2n}(x) = \psi_n(-x)$

Proof. We know from D&F that $\psi_{2n}(x)$ and $\psi_n(-x)$ are irreducible, meaning then that they are the minimal polynomial of any their roots. So all we need to do is find a common root between both of them.

Let ζ_n be the n^{th} primitive root of unity as usual, and let $\zeta_2 = -1$ be the 2nd primitive root of unity specifically. That way we have their product to be

$$\zeta_n \zeta_2 = -\zeta_n$$

We assumed though that n is odd so it is clear 2 and n must be relatively prime. We know then that $\zeta_n \zeta_2$ must then me the $2n^{th}$ primitive root of unity (assuming this from the first exercise from this chapter), which is a root of $\psi_{2n}(x)$. Also note that $-\zeta_n$ is a root of $\psi_n(-x)$, therefore we have $-\zeta_n$ to be the common root between both the given polynomials. Therefore $\psi_n(-x) = \psi_{2n}(x)$. □