David Owen Horace Cutler Math 146: Homework 5 March 12, 2024

Exercise 1. (a) Find all eight irreducible polynomials in $\mathbb{F}_2[x]$ with degree at most 4.

Computing these we get:

We can characterize them by degree; degree 1 is trivial, it suffices to check for roots in degree 2 and 3, and we need to compute products for degree 4.

After finishing this process we get the eight irreducible polynomials over $\mathbb{F}_2$ are:

- x
- $x+1$
- x^2+x+1
- x^3+x^2+1
- x^3+x+1
- $x^4+x^3+x^2+x+1$
- x^4+x^3+1
- x^4+x+1

(b) Determine which of the following polynomials are irreducible in $\mathbb{Q}[x]$.

(i) $x^3-7x^2+16x-1001$

It is irreducible. Reducing modulo $p=2$ we get the polynomial x^3+x^2+1 in $\mathbb{F}_2[x]$, which we established to be irreducible $\mathbb{F}_2[x]$. Thus it is irreducible in $\mathbb{Z}[x]$, which has irreducibility in $\mathbb{Q}[x]$.

(ii) x^4+x^3-1

It is irreducible. Repeating the same process given with the previous polynomial gets x^4+x^3+1, which is irreducible in $\mathbb{F}_2[x]$. irreducibility in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ follows.

(iii) x^4+x^3+x+1

It is reducible. Note it admits the factorization into polynomials of strictly lesser degree given by $(x+1)(x^3+1)$.

(iv) $x^7+12x^5-24x+18$

It is irreducible. Consider the Eisenstein criterion with $p=2$. We note p divides all nonleading coefficients, and that it does not divide the leading coefficient. Moreover, $p^2=4$ does not divide the constant term. Thus irreducible.

Exercise 2. Let F be a field and K an extension of F. Let $f \in F[x]$ be a non-zero polynomial. Prove that the number of roots of f in K is at most $\deg(f)$.

Proof. Let $n \geq 0$. We will prove this by proving that all polynomials $f \in F[x]$ with $\deg(f) \leq n$ with more than n roots are the zero polynomial.

To accomplish this, we will give a proof by induction. Note the base case $k = 0$ is obvious, as the only cases to consider are non-zero constants (no roots) and the zero polynomial.

For induction then, assume that all polynomials in $K[x]$ (note, not in $F[x]$, but this result will imply the result in $F[x]$) with degree at most k and more than k roots in K are the zero polynomial.

Let then $f \in K[x]$ be a polynomial with degree at most $k+1$ with more than $k+1$ distinct roots, a subset of which is denoted

$$\alpha_1, ..., \alpha_{k+2},$$

with the corresponding linear polynomials in $K[x]$ denoted by

$$m_{\alpha_i} = x - \alpha_i.$$

We quickly prove all of these m_{α_i} divide $f \in K[x]$ by the division algorithm (this is just a proof minimal polynomials divide). Note we have

$$\begin{aligned} f &= m_{\alpha_i} q + r \\ \deg(\mathrm{r}) &< \deg(m_{\alpha_i}) \end{aligned}$$

We want to argue it must be $r = 0$. Assuming for the sake of contradiction this is not the case, we note:

$$0 = f(\alpha_i) = m_{\alpha_i}(\alpha_i) q(\alpha_i) + r(\alpha_i) = 0 \cdot q(\alpha_i) + r(\alpha_i) = r(\alpha_i)$$

But this is a contradiction, as then r is a nonzero polynomial of degree less than m_{α_i} with α_i as a root, i.e. it contradicts the minimality of m_{α_i} (note these are the minimal polynomials in $K[x]$ of the roots in K).

Thus it must be that $m_{\alpha_i} | f$ for all α_i. Consider the factorization of f by the division algorithm given by

$$f = m_{\alpha_{k+2}} g = (x - \alpha_{k+2}) g$$

for some $g \in K[x]$. Obviously, g has degree at most k. Substituing x for each α_i where $1 \leq i \leq k+1$ gets

$$f(\alpha_i) = (\alpha_i - \alpha_{k+2}) g(\alpha_i),$$

where of course for each i we have $f(\alpha_i) = 0$. But of course $(\alpha_i - \alpha_{k+2})$ is nonzero for each $1 \leq i \leq k+1$, as these are distinct roots.

It must then be that $g(\alpha_i) = 0$ for each α_i where $1 \leq i \leq k+1$. But then g has $k+1$ roots, more than its degree k. By the induction hypothesis then, it must be $g = 0$.

But of course our earlier factorization thus has that then it must be $f = 0$. It follows the induction holds.

Finally, to resolve the problem we notice that for any given nonzero $f \in F[x]$, it is also that $f \in K[x]$ with the same degree and distinct roots in K. Thus the result in $K[x]$ proves the desired result for $f \in F[x]$. □

Exercise 3. Let p be a prime number. Let $\mathbb{F}_{p^2}$ be the field of order p^2. Prove that $\mathbb{F}_{p^3}$ is not an extension of $\mathbb{F}_{p^2}$.

Proof. Assume for the sake of contradiction that $\mathbb{F}_{p^3}$ is an extension of $\mathbb{F}_{p^2}$, i.e. there is an injection $\phi : \mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_{p^3}$. Naturally then, $\phi(\mathbb{F}_{p^2})$ is a *subfield* of $\mathbb{F}_{p^3}$ of order p^2.

Note then the multiplicative group underlying $\phi(\mathbb{F}_{p^2})$ has $p^2 - 1$ elements then, and it is of course a subgroup of the multiplicative group underlying $\mathbb{F}_{p^3}$, which has p^3 elements.

This is a contradiction however, as by **Lagrange's Theorem**, it should be then that $\frac{p^3-1}{p^2-1}$ is an integer. However we note

$$\frac{p^3-1}{p^2-1} = \frac{(p^2+p+1)(p-1)}{(p+1)(p-1)} = \frac{p^2+p+1}{p+1},$$

where performing polynomial long division furthermore gets

$$\frac{p^2+p+1}{p+1} = p + \frac{1}{p+1},$$

which is clearly never an integer for any prime p. Thus we have a contradiction, so it cannot be that $\mathbb{F}_{p^3}$ is an extension of $\mathbb{F}_{p^2}$. □

Exercise 4. Let p be an odd prime.

(a) Let $\alpha \in \mathbb{F}_{p^2}$, and consider the polynomial $g = (x-\alpha)^2 \in \mathbb{F}_{p^2}[x]$. Prove that g is in fact in $\mathbb{F}_p[x]$ if and only if $\alpha \in \mathbb{F}_p$.

Proof. Note the reverse direction is clearly immediate, (seen by the given expansion later) so we just move to prove the forward direction, assuming $g \in \mathbb{F}_p[x]$.

Note we can expand $g = (x-\alpha)^2$ into

$$g = (x-\alpha)^2 = x^2 - (\alpha+\alpha)x + \alpha^2;$$

as we assumed $g \in \mathbb{F}_p[x]$ then, it must be the coefficient $-(\alpha+\alpha) \in \mathbb{F}_p$, and so $\alpha+\alpha \in \mathbb{F}_p$. Note then $0 \neq 1+1 \in \mathbb{F}_p$ (the only prime order field in which $1+1=0$ is $\mathbb{F}_2$, but we excluded even primes). We get then

$$\begin{aligned} \alpha+\alpha &= \alpha(1+1) \\ \to (1+1)^{-1}(\alpha+\alpha) &= \alpha \end{aligned}$$

But the terms on the left are in $\mathbb{F}_p$ then clearly, so $\alpha \in \mathbb{F}_p$ by closure under multiplication, as desired. □

(b) Prove that every $\alpha \in \mathbb{F}_{p^2}$ that is not in $\mathbb{F}_p$ is the root of a monic irreducible polynomial of degree 2 in $\mathbb{F}_p[x]$.

Proof. Note that of course $\mathbb{F}_{p^2}$ is a finite extension of $\mathbb{F}_p$, as argued in class. Thus it is algebraic; i.e. every $\alpha \in \mathbb{F}_{p^2}$ is the root of some polynomial in $\mathbb{F}_p[x]$.

We note specifically that $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, which has that the minimal polynomial of each α has degree at most 2 (follows as the set $\{\alpha^2, \alpha, 1\}$ must be linearly dependent as so we can reduce higher degree terms).

Consider the minimal polynomial for an $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Of course, this minimal polynomial is monic and irreducible, so we want just to show it has degree exactly 2.

For this, note the only alternative possibility is that is is linear (as degree at most 2), but if α were a root of a monic linear polynomial with constant term $a \in \mathbb{F}_p$, we could rearrange

$$\alpha + a = 0 \to \alpha = -a,$$

which would clearly imply $\alpha \in \mathbb{F}_p$. Thus it must be the minimal polynomial is degree 2, and so α is the root of a monic irreducible polynomial of degree 2 in $\mathbb{F}_p[x]$.

□

(c) Prove that if $g \in \mathbb{F}_p[x]$ is a monic irreducible of degree 2, then g has exactly two roots in $\mathbb{F}_{p^2}$.

Proof. Let $g \in \mathbb{F}_p[x]$ a monic irreducible polynomial of degree 2. We note here that $\mathbb{F}_{p^2}$ is an extension of $\mathbb{F}_p$.

We appeal to a pigeonhole style argument then of ϕ, with the mapping ϕ being the one that sends an element of $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ to the monic, irreducible, degree 2 polynomial it is a root of.

This mapping is well-defined as if an element of $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ was sent to more than one polynomial, i.e. it was a root of more than one monic degree 2 polynomial, its minimal polynomial would then need to be linear, as the least degree monic polynomial with α as a root is unique.

However, a linear minimal polynomial would imply $\alpha \in \mathbb{F}_p$ in a similar argument to the one outlined in the previous step. Thus the mapping must send an element to one polynomial, i.e. it is well-defined.

Thus $p^2 - p$ (the cardinality of $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$) pigeons must be fit into $\frac{p^2-p}{2}$ boxes (the amount of monic, irreducible degree 2 polynomials in $\mathbb{F}_p[x]$), but each box can have at most 2 pigeons by our earlier observation in **Exercise 2**. Thus the only possibility is each box has 2 pigeons, i.e. each monic, irreducible, degree 2 polynomials has exactly two roots. □

(d) Finally, let $g \in F[x]$ be any monic irreducible polynomial of degree 2. Recall g has two roots in $\mathbb{F}_{p^2} = {}^{\mathbb{F}[x]}/_{(f)}$. Let $a_g + b_g x + (f)$ be one of these roots.

(i) Prove that $b_g \neq 0$.

Proof. Assume for the sake of contradiction that $b_g = 0$. It follows that $a_g + (f)$ is a root of $g \in \mathbb{F}_p[x]$.

So $a_g + (f)$ is algebraic over $\mathbb{F}_p$, so we can consider its minimal polynomial. In particular, it is clear this polynomial is exactly

$$x - a_g \in \mathbb{F}_p[x]$$

But this is problematic, as we showed in **Exercise 2** that this minimal polynomial should then divide g.

In particular, this contradicts the fact g is irreducible as the given polynomial is linear, i.e. g is reduced into a product of linear polynomials. It follows $b_g \neq 0$. □

(ii) Define a homomorphism $\phi_g : \mathbb{F}_p[x] \to {}^{\mathbb{F}_p[x]}/_f$ by $\phi_g(x) = a_g + b_g x + (f)$ and $\phi_g(a) = a + (f)$ for all $a \in \mathbb{F}_p$. Prove that ϕ_g is a surjective homomorphism and that $\ker(\phi_g) = (g)$.

Proof. We need to prove ϕ_g is surjective and that we have $\ker(\phi_g) = (g)$.

(1) *(Surjectivity)* Recall that every element of ${}^{\mathbb{F}_p[x]}/_f$ has a unique representative of degree less than f.

It follows the these representatives are constants and linear polynomials (as f is degree 2).

The constant case is immediately resolved as we have $\phi_g(a) = a + (f)$ for $a \in \mathbb{F}_p$. Consider a linear representative, i.e. $ax + b$. We want to produce an element that maps to $ax + b + (f)$.

Now as $b_g \neq 0$, we have that b_g^{-1} exists. Thus

$$\phi_g(b_g^{-1}x) = \phi_g(b_g^{-1})\phi(x) = (b_g^{-1} + (f))(a_g + b_g x + (f)) = b_g^{-1}a_g + x + (f),$$

which in particular has that

$$\phi(b_g^{-1}x - b_g^{-1}a_g) = \phi_g(b_g^{-1}x) + \phi(-b_g^{-1}a_g) = b_g^{-1}a_g + x - b_g^{-1}a_g + (f) = x + (f),$$

and so finally

$$ax + b + (f) = \phi(a)\phi(b_g^{-1}x - b_g^{-1}a_g) + \phi(b) = \phi(ab_g^{-1}x - ab_g^{-1}a_g + b),$$

which thus shows surjection.

(2) *(Kernel is (g))* Let $h \in (g)$, i.e. $h = gi$ for $i \in \mathbb{F}_p[x]$. We want first to show $h \in \ker(\phi_g)$ so that we have $(g) \subseteq \ker(\phi_g)$.

First note clearly that $\phi_g(g) = 0 + (h)$, as ϕ_g has

$$x \mapsto a_g + b_g x + (f),$$

but this is root of g, i.e. $\phi_g(g)$ is evaluating g at $a_g + b_g x + (f)$, which returns zero. Thus

$$\phi_g(h) = \phi_g(gi) = \phi_g(g)\phi_g(i) = 0 \cdot \phi_g(i) = 0,$$

and so $h \in \ker(\phi_g)$ which has $(g) \subseteq \ker(\phi_g)$.

We want to show $\ker(\phi_g) \subseteq (g)$ then. However, this is immediate, as the irreducibility of g has that (g) is maximal.

It follows (g) cannot be a proper subset of $\ker(\phi_g)$ unless this kernel is the whole $\mathbb{F}_p[x]$, but by definition this is clearly not the case. It follows then that $\ker(\phi_g) = (g)$.

□

(e) Conclude that ${}^{F_p[x]}/_{(g)} \cong {}^{F_p[x]}/_{(f)}$.

Proof. This is a straightforward application of the **First Isomorphism Theorem**, which here specifically says

$${}^{\mathbb{F}_p[x]}/_{(g)} = {}^{\mathbb{F}_p[x]}/_{\ker(\phi_g)} \cong \phi_g(\mathbb{F}_p[x]) = {}^{\mathbb{F}_p[x]}/_{(f)}$$

□