Name: Kevin Guillen
Student ID: 1747199

Math 117 - SS2 - Mastery Problems 1 - July 30, 2021

Disclaimer: Sorry if I took too much abstract algebra properties as granted. A lot of this stuff popped up in 134 and 111b, so I solved it from what I remember from there and what's in Dummit and Foote's Abstract Algebra

3a) $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$. Let $f \in \mathbb{F}[x]$, where $f(x) = x^2 + x + 1$. Show f is irreducible.

Proof. First we will begin by showing $\mathbb{F}$ is a field, more generally that $\mathbb{Z}/p\mathbb{Z}$ is a field where p is a prime integer. We know from class that for any integer n, $\mathbb{Z}/n\mathbb{Z}$ will be a commutative ring. All we need to show now is that, when n is prime, every non-zero element in it will have multiplicative inverses.

By definition a prime number, p, will share no common divisors except 1 with another integer n ($n \neq p$). Thus take any non-zero element $n \in \mathbb{Z}/p\mathbb{Z}$. n represents a congruence class of elements which are by definition not multiples of p. Thus, $\gcd(n, p) = 1$.

From here we know from elementary number theory that there exists $u, v \in \mathbb{Z}$ such that

$$u \cdot n + v \cdot p = 1.$$

Bringing this into $\mathbb{Z}/p\mathbb{Z}$ we have

$$\overline{u} \cdot \overline{n} + \overline{0} \equiv \overline{1}$$

$$\overline{u} \cdot \overline{n} \equiv \overline{1}$$

That means for any non-zero $n \in \mathbb{Z}/p\mathbb{Z}$, where p is prime, that there exists a $u \in \mathbb{Z}/p\mathbb{Z}$ such that $\overline{u} \cdot \overline{n} = 1$. Which means that every non-zero element has a multiplicative inverse. Thus satisfying the criteria to be a field.

We know that since $\mathbb{F}$ is a field, $f \in \mathbb{F}[x]$ will have a factor of degree one if and only if f has a root in $\mathbb{F}$. In other words $a \in \mathbb{F}$, $f(a) = 0$

A quick proof of this is as follows. If $f(x)$ has a factor of degree one, and because $\mathbb{F}$ is a field, we can assume the factor to be a monic. Meaning for $a \in \mathbb{F}$ it will have the form $(x - a)$, but $f(a) = 0$. The converse direction is as follows, assuming $f(a) = 0$. We can use the division algorithm in $\mathbb{F}[x]$ to get $f(x) = q(x)(x - a) + r$. But we assumed $f(a) = 0$ that means r must be 0, therefore $f(x)$ will have $(x - a)$ as a factor. It follows from here that any polynomial of degree 2 or 3 in $\mathbb{F}[x]$ will be reducible if and only if it has a root in $\mathbb{F}$. Since a polynomial of degree 2 or 3 is reducible if and only if it has at least 1 linear factor.

Finally, we know the elements of $\mathbb{Z}/2\mathbb{Z}$ are $\{\overline{0}, \overline{1}\}$. Plugging this into $f(x) = x^2 + x + 1$ we get

$$f(0) = 0 + 0 + 1 \equiv \overline{1}$$

$$f(1) = 1 + 1 + 1 \equiv 3 \equiv \overline{1}$$

We see neither are 0, thus f cannot be reducible, meaning it is irreducible. $\square$

3b) Following the setup of part (a) let $(x^2+x+1) = \text{Span}\{x^2+x+1\}$. Show that $\dim_{\mathbb{F}}(\mathbb{F}[x]/(x^2+x+1)) = 2$ and $|F[x]/(x^2+x+1)| = 4$

Proof. By definition the span of vectors is just the set of all linear combination of said vectors. Since our only choices are $\overline{1}, \overline{0} \in \mathbb{Z}/2\mathbb{Z}$ then the set is simply f. First we will show $|F[x]/(x^2+x+1)| = 4$. We know that the complete set of representatives of the congruence classes of $\mathbb{F}[x]$ modulo f will be of degree < 2, since $\deg(f) = 2$. Since these polynomials are restricted to their degree being less than 2 and their coefficients being in $\mathbb{Z}/2\mathbb{Z}$ this becomes an easy counting problem. $F[x]/(x^2+x+1) = \{ax+b : \ a, b \in \mathbb{Z}/2\mathbb{Z}\}$. As stated before there are only 2 elements in $\mathbb{F}$, thus there are only $2 \cdot 2 = 4$ possible polynomials to choose from in this set of representatives. Hence, $|F[x]/(x^2+x+1)| = 4$.

From class, we know that the dimension of a finite dimensional vector space is the number of elements in a basis of said vector space. We also know from class that any basis of a finite dimensional vector space will be of the same dimension. So all we need to show is 2 vectors in $F[x]/(x^2+x+1)$ that can be a basis to show the dimension is 2.

$F[x]/(x^2+x+1) = \{0, 1, x, x+1\}$. Let the basis $U = \{x, 1\}$ we can see for $a, b \in \mathbb{F}$,

$$x + 1 = 1 \cdot (x) + 1 \cdot (1)$$

$$x = 1 \cdot (x) + 0 \cdot (1)$$

$$1 = 0 \cdot (x) + 1 \cdot (1)$$

$$0 = 0 \cdot (x) + 0 \cdot (1)$$

We can see $|U| = 2$. Restating as before we know the number of elements in any bass of a finite dimensional vector space is the same as in any other basis, thus $\dim_{\mathbb{F}}(\mathbb{F}[x]/(x^2+x+1)) = 2$ $\square$

3c) Show $E = F[x]/(x^2+x+1)$ forms a field with precisely four elements and of characteristic 2.

Proof. We already saw that E contains only 4 elements since the polynomials are restricted to degree less than 2 and coefficients in $\mathbb{Z}/2\mathbb{Z}$ meaning $E = \{ax+b : \ a, b \in \mathbb{Z}/2\mathbb{Z}\}$ which means there are 4 representatives.

To show it is a field though we will prove something more general in that if $\mathbb{F}$ is a field and $f(x) \in \mathbb{F}[x]$ irreducible then $\mathbb{F}[x]/f(x)$ is a field. We already know from abstract algebra that this does indeed form a commutative ring. All that is left is to show it has multiplicative inverses.

First we let $p(x) \in \mathbb{F}[x]$ with $p(x) + (f(x)) \neq 0 + (f(x))$. Meaning $f(x) \nmid p(x)$. Now we need to show there exists $u(x) \in \mathbb{F}[x]$ such that $p(x)u(x) \equiv 1 \bmod f(x)$. We know though that $f(x)$ is irreducible and because $p(x)$ is not a multiple of $f(x)$ it means that every common divisor of $f(x)$ and $p(x)$ must be of degree 0. Meaning the constant polynomial 1 is the greatest common divisor of both $f(x)$ and $p(x)$. We know by polynomial division with remainder that there exists polynomials $u(x), v(x) \in \mathbb{F}[x]$ such that

$$u(x) \cdot p(x) + v(x) \cdot f(x) = 1.$$

Implying that $u(x)p(x) \equiv 1 \bmod f(x)$, meaning $p(x) + (f(x))$ is invertible in $\mathbb{F}[x]/(f(x))$ as desired.

Thus, $F[x]/(x^2+x+1)$ does indeed form a field.

We know that since this is a field and thereby a ring that the characteristic is simply the minimum number of times we must take the multiplicative identity in a sum to get the additive identity. Since the coefficients are restricted to $\mathbb{Z}/2\mathbb{Z}$ this is simply

$$\overline{1} + \overline{1} = \overline{2} \equiv \overline{0}$$

Thus the characteristic is 2. $\square$