MTH 4104 Assessed Coursework II

Shu SASAKI

Please submit your work by **11am**, **the 15th of April** (QMplus).

A1. (1) By the division algorithm for polynomials, every polynomial in $\mathbb{F}_2[X]$, when divided by $X^2 + X + [1]$, has a unique remainder of the form either $[0], [1], X$ or $X + [1]$. Analogous to the way representative are chosen for $\mathbb{Z}_p$, these four polynomials of degree ≤ 1 naturally define the representatives with respect to $\mathcal{R}$ and therefore $|F| = 4$.

(2) Strictly speaking, it makes a key exercise to check the addition and multiplication are well-defined but this is not necessary. The content of this question is that it is rather straightforward to observe almost all field axioms follow from the ring axioms for $\mathbb{F}_2[X]$, except in finding the multiplicative inverse of an element in F– the addition inverse of $\{f\}$ is $\{-f\}$ but it does not make sense to say the multiplicative inverse of $\{f\}$ is $\{f^{-1}\}$ since f^{-1} does not make sense as an element of $\mathbb{F}_2[X]$.

We firstly prove that $(F, +)$ is an abelian group. To this end, we check all the group axioms.

(G0) Since $f + g \in \mathbb{F}_2[X]$ (by (R+0) for the ring $\mathbb{F}_2[X]$), $\{f\} + \{g\} = \{f + g\}$ defines an element of F.

(G1) Since $(f + g) + \gamma = f + (g + \gamma)$ (by (R+1) for $\mathbb{F}_2[X]$),

$$(\{f\}+\{g\})+\{\gamma\} = \{(f+g)\}+\{\gamma\} = \{(f+g)+\gamma\} = \{f+(g+\gamma)\} = \{f\}+\{g+\gamma\} = \{f\}+(\{g\}+\{\gamma\}).$$

(G2) The equivalence class $\{[0]\}$ is the identity element of F with respect to $+$. Indeed,

$$\{f\} + \{[0]\} = \{f + [0]\} = \{f\} = \{[0] + f\} = \{[0]\} + \{f\}$$

by (R+2) for $\mathbb{F}_2[X]$ (in which the polynomial $[0]$ is the identity element).

(G3) The inverse of $\{f\}$ is $\{-f\}$. Indeed,

$$\{f\} + \{-f\} = \{f + (-f)\} = \{[0]\} = \{(-f) + f\} = \{-f\} + \{f\}$$

by (R+3). In fact, since $-f = f$ in $\mathbb{F}_2[X]$, the inverse of $\{f\}$ is $\{f\}$ itself!

(G4) Since $\mathbb{F}_2[X]$ is commutative,

$$\{f\} + \{g\} = \{f + g\} = \{g + f\} = \{g\} + \{f\}$$

holds.

Secondly we prove that $(F - \{[0]\}, \times)$ is an abelian group.

(G0) This follows from (R×0) for $\mathbb{F}_2[X]$. Alternatively, we may spell out the multiplication table:

$\times$	$\{[0]\}$	$\{[1]\}$	$\{X\}$	$\{X+[1]\}$
$\{[0]\}$	$\{[0]\}$	$\{[0]\}$	$\{[0]\}$	$\{[0]\}$
$\{[1]\}$	$\{[0]\}$	$\{[1]\}$	$\{X\}$	$\{X+[1]\}$
$\{X\}$	$\{[0]\}$	$\{X\}$	$\{X+[1]\}$	$\{[1]\}$
$\{X+[1]\}$	$\{[0]\}$	$\{X+[1]\}$	$\{[1]\}$	$\{X\}$

which shows (G4) that $F - \{[0]\}$ is commutative with respect to $\times$.

(G1) This follows from (R$\times$1) for $(\mathbb{F}_2[X], +, \times)$.

(G2) The equivalence class $\{[1]\}$ is the identity element of F with respect to $\times$. Indeed,

$$\{f\}\{[1]\} = \{f[1]\} = \{f\} = \{[1]f\} = \{[1]\}\{f\}$$

since the $\mathbb{F}_2[X]$ is a ring with (multiplicative) identity $[1]$.

(G3) This is the heart of the problem. One can not simply say the inverse of $\{f\}$ is $\{f^{-1}\}$ since 'f^{-1}' does not make sense in $\mathbb{F}_2[X]$! It forces one to calculate the inverse only 'up to $X^2 + X + [1]$'!

The multiplication table above shows that the inverse of $[1]$ is $[1]$ itself, the inverse of $\{X\}$ is $\{X + [1]\}$ and the inverse of $\{X + [1]\}$ is, of course, $\{X\}$.

Finally, $\{[0]\}$ is evidently not equal to $\{[1]\}$ as $[1]-[0] = [1]$ can not be divided by $X^2+X+[1]$.

A2. I just want students to look back on what they have learned and internalise a proof or two.

Marking Scheme. **Q1**. (1) $+1$ for simply writing down representatives correctly, $+2$ for justification and $+1$ for computing $|F|$. (2) $+4$ for a proof ($+2$ for finding the multiplicative inverse of $\{f\}$ generally). **Q2**. (1) $+1$ for explanation (2) $+1$ for a correct proof.