Peter Rauscher HW 9

I pledge my honor that I have abided by the Stevens Honor System.

Exercise 9.1

Consider any $h_1(x), h_2(x) \in F[X]$

If $h_1(X) \equiv_{f(x)} h_2(X)$, then they must have the same remainder from polynomial division by $f(x)$, or

$$h_1(X) = \alpha(X)f(X) + r(X)$$
$$h_2(x) = \beta(X)f(x) + r(x)$$

$$h_1(x) - h_2(x) = \alpha(x)f(x) + r(x) - \beta(x)f(x) - r(x)$$
$$= \alpha(X)f(X) - \beta(X)f(X)$$
$$= f(X)(\alpha(X) - \beta(X))$$

We are given that $g(x) = \frac{1}{C_n}f(X)$, or $f(X) = C_n g(X)$

So, using the formulas for h_1 and h_2 from above,

$$h_1(X) = \alpha(X)f(X) + r(X) = \alpha(X)C_n g(X) + r(X)$$
$$h_2(X) = \beta(X)f(X) + r(x) = \beta(x)C_n g(x) + r(x)$$

$$h_1(X) - h_2(X) = \alpha(x)C_n g(x) + r(x) - \beta(x)C_n g(x) - r(x)$$
$$= \alpha(X)C_n g(x) - \beta(x)C_n g(x)$$
$$= g(X)(\alpha(x)C_n - \beta(x)C_n)$$
$$\Rightarrow g(X) \mid h_1(x) - h_2(X)$$

Thus, clearly, $h_1(x) \equiv_{f(x)} h_2(x) \Rightarrow h_1(x) \equiv_{g(x)} h_2(X)$

Recall $\alpha(x)C_n g(X) - \beta(x)C_n g(x) = h_1(x) - h_2(x)$ and $g(x) = \frac{1}{C_n}f(x)$

So, $h_1(X) - h_2(X) = \alpha(x)C_n\frac{1}{C_n}f(x) - \beta(x)C_n\frac{1}{C_n}f(x)$
$$= f(X)(\alpha(X) - \beta(X))$$

And thus $h_1(X) \equiv_{g(x)} h_2(X) \Rightarrow h_1(x) \equiv_{f(x)} h_2(X)$

Exercise 9.2

Since F_1, F_2 are subfields of E, we know by the definition of subfields that

$$0, 1 \in F_1 \text{ and } 0, 1 \in F_2$$

Clearly, then, $0, 1 \in F_1 \cap F_2$

Similarly, by the definition of groups

For any $a, b \in F_1 \cap F_2$

$$a, b \in F_1 \text{ and } a, b \in F_2$$
$$a - b \in F_1 \text{ and } a - b \in F_2$$
$$\Rightarrow a - b \in F_1 \cap F_2$$

Lastly, consider any $a, b \in F_1 \cap F_2$ where $b \neq 0$

$$a, b \in F_1 \text{ and } a, b \in F_2$$
$$a \cdot b^{-1} \in F_1 \text{ and } a \cdot b^{-1} \in F_2$$
$$\Rightarrow a \cdot b^{-1} \in F_1 \cap F_2$$

Since $0, 1 \in F_1 \cap F_2$ and for any $a, b, c \in F_1 \cap F_2$ $a - b \in F_1 \cap F_2$ and $a \cdot c^{-1} \in F_1 \cap F_2$ and $F_1 \cap F_2$ is a subset of E, it is clear that $F_1 \cap F_2$ is a subfield of E.

Exercise 9.3

a) $\mathbb{Z}_3 = \{0, 1, 2)$

$f(0) = 0^2 + 0 + 2 = 2 \neq 0$
$f(1) = 1^2 + 1 + 2 = 4 \equiv_3 1 \neq 0$
$f(2) = 2^2 + 2 + 2 = 8 \equiv_3 2 \neq 0$

f has no zeros in $\mathbb{Z}_3$, therefore, $\mathbb{Z}_3 / \langle x^2 + x + 2 \rangle$ is a field

b) $E = \mathbb{Z}_3 / \langle x^2 + x + \rangle$ $g(x) = x^3 - x^2 - 1$

$g(x) \in E$ is non-trivial if $f(x) \nmid g(x)$

$$\begin{array}{r|l} x^3 - x^2 - 1 & x^2 + x + 2 \text{ in } \mathbb{Z}_3 \\ - \quad x^3 + x^2 + 2x & x + 1 \\ \hline -2x^2 - 2x - 1 & \\ - \quad x^2 + x + 2 & \\ \hline 0 & \end{array}$$

$\frac{g(x)}{f(x)} = x + 1$ in $\mathbb{Z}_3$, so

$f(x) \mid g(x)$

Therefore, $g(x)$ is trivial in E

c) $x^3 + 2x = 2x^2$
$x^3 - 2x^2 + 2x = 0$

$$\begin{array}{r|l} x^3 - 2x^2 + 2x & x^2 + x + 2 \text{ in } \mathbb{Z}_3 \\ - \quad x^3 + x^2 + 2x & x \\ \hline 0 & \end{array}$$

$\Rightarrow x^3 + 2x = 2x^2$ in E

e) $\chi(E) = 3$ (E is a subfield of $\mathbb{Z}_3$)

f) $|E| = |\mathbb{Z}_3|^2 = 9$

g)