Name: Rajal Rajesh shetty Assignment-9

CWID: 10477484

Exercise 9.1:

Let F_1, F_2 be subfields of a field E. TPT $F = F_1 \cap F_2$ is a subfield of E.

$\Rightarrow$ F_1, F_2 be two subfields of E,

Let $x \in F_1 \cap F_2$ & $y \in F_1 \cap F_2$.

So, $x - y \in F_1$ & $x - y \in F_2 \Rightarrow x - y \in F_1 \cap F_2$.

also

$x \cdot y \in F_1$, $x \cdot y \in F_2 \Rightarrow x \cdot y \in F_1 \cap F_2$

also,

$$\left.\begin{array}{l} x \in F_1 \Rightarrow x^{-1} \in F_1 \\ x \in F_2 \Rightarrow x^{-1} \in F_2 \end{array}\right\} \Rightarrow x^{-1} \in F_1 \cap F_2$$

Hence $F_1 \cap F_2$ is a subfields of E.

Exercise 9.2:

Let $f(x) = x^2 + x + 2 \in \mathbb{Z}_3(x)$

(a) ST $f(x)$ is irreducible. Hence $E = F[x]/f(x)$ is a field.

$\Rightarrow$ $f(x) \in \mathbb{Z}_3(x)$ is irreducible if and only if-

(a) f has a zero in $\mathbb{Z}_3$.

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

$f(x) = x^2 + x + 2$, $f(a) = 2 \neq 0$

$f(1) = 1$ in $\mathbb{Z}_3 \neq 0$

$f(2) = 2 \neq 0$, hence $f(x)$ is irreducible over $\mathbb{Z}_3$.

Hence, $E = F[x]/f(x)$ is a field.

(b) is $x^3 - x^2 - 1$ trivial in E, or not? why?

⇒ $f(x)$ is trivial in $\frac{Z_3(x)}{\langle x^2+x+2\rangle}$ if and only if

$x^3 - x^2 - 1 = 0 + \langle x^2+x+2\rangle$ or $x^3 - x^2 - 1 \in \langle x^2+x+2\rangle$

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

$\Rightarrow (x+1)(x^2+x+2)$

thus $x^3 - x^2 - 1$ is trivial in $\frac{Z_3(x)}{\langle x^2+x+2\rangle}$

$$\begin{array}{r|l} & x+1 \\ \hline x^2+x+2 & x^3 - x^2 - 1 \\ & x^3 + x^2 + 2x \\ \hline & x^2 + x + 2 \\ & x^2 + x + 2 \\ \hline & 0 \end{array}$$

(c) $x^3 + 2x = 2x^2$ in E, or not? why?

⇒ $x^3 - 2x^2 + 2x = x^3 + x^2 + 2x = x(x^2+x+2)$

so $x^3 - 2x^2 + 2x$ is divided by x^2+x+2.

⇒ $x^3 - 2x^2 + 2x \in \langle x^2+x+2\rangle$ ⇒ Hence, $x^3 + 2x = 2x^2$ in E

(d) Find the multiplicative inverse of $x+1$ in E.

⇒ to find inverse of $x+1$ in E, means that to find $ax+b + \langle x^2+x+2\rangle$.

for $((x+1) + \langle x^2+x+2\rangle)(ax+b + \langle x^2+x+2\rangle)$

$= 1 + \langle x^2+x+2\rangle$, $a, b \in Z_3$.

⇒ $(x+1)(ax+b) + \langle x^2+x+2\rangle = 1 + \langle x^2+x+2\rangle$

⇒ $ax^2 + (a+b)x + b + \langle x^2+x+2\rangle = 1 + \langle x^2+x+2\rangle$

⇒ $ax^2 + (a+b)x + (b-1) = (x^2+x+2)$

⇒ $\begin{cases} a = 1 \\ a+b = 1 \\ b-1 = 2 \end{cases}$ ⇒ $\begin{cases} a = 1 \\ b = 0 \end{cases}$ in $Z_3[x]$.

Or

$(x+1)^{-1}$ in E

now $(x+1)(ax+b) = 1$ ⇒ $x^2 = x - 2,\ 2x+1$ ⇒ $ax^2 + bx + ax + b = 1$

⇒ $a(2x+1) + x(a+b) + b = 1$ ⇒ $2ax + a + ax + bx + b = 1$ ⇒ $bx + a + b = 1$ $b = 0$ $a = 1$

so $(x+1)^{-1} = x$

(e) $\chi(E)$

since $3(x^2+x+2) \Rightarrow 3x^2+3x+6=0$

$\therefore \chi(E)=3.$

(f) $|E|$

$|E| = p^n = 3^2 = 9$

(g) Find the order of $x+2$ in E

$(x+2)^2 = (x+2)(x+2) = x^2+x+1 \Rightarrow (1)\cdot(x^2+x+1)+2 = 2$

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

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

$= (2)\cdot(x^2+x+2)+1$

$= \underline{1}$

So, since $(x+2)^4 = 1$

$\therefore |x+2| = 4$ in E

//

(h) is x a primitive root in E?

⇒ The size of multiplicative group i.e E^x of E is $p^n - 1 = 9 - 1 = 8$ which is not prime.

so, $ppf(p^n - 1) = 2^2 \cdot 2$.

Hence, x is a primitive root if & only if

$$x^{\frac{p^n-1}{p_i}} \neq 1 \Rightarrow x^{8/4} = x^2$$
$$\Rightarrow x^{8/2} = x^4$$

Then, to check if x is a primitive root we check that

* $x^2 \neq 1 \bmod x^2+x+2$ ⇒ True.

$$\begin{array}{r|l} & 1 \\ \hline x^2+x+2 & x^2 \\ & x^2+x+2 \\ \hline & 2x+1 \end{array}$$

* $x^4 \neq 1 \bmod x^2+x+2$ ⇒ true.

$$\begin{array}{r|l} & x^2+2x+2 \\ \hline x^2+x+2 & x^4 \\ & x^4+x^3+2x^2 \\ \hline & 2x^3+x^2 \\ & 2x^3+2x^2+x \\ \hline & 2x^2+2x \\ & 2x^2+2x+1 \\ \hline & 2 \end{array}$$

∴ So we can say,

x is a primitive root of E.