Novosad Ivan

1. Find an isomorphism and its inverse for the fields $\mathbb{Z}_3[x]/(x^2+1)$ and $\mathbb{Z}_3[y]/(y^2+y-1)$.

$\mathbb{Z}_3[x](x^2+1) = \{ax+b \mid a,b \in \mathbb{Z}_3\} = A$

$\mathbb{Z}_3(x](y^2+y-1) = \{ax+b \mid a,b \in \mathbb{Z}_3\} = B$

$\varphi : A \mapsto B$ $\qquad$ $\psi : B \mapsto A$

$\varphi(ax+b) = ay+b$ $\qquad$ $\psi(ay+b) = ax+b$

Clearly $\varphi \circ \psi(y) = y$, $\psi \circ \varphi(x) = x$

Now let's construct φ:

$x^2+1 = 0 \pmod{x^2+1}$

$\varphi(x^2+1) = \varphi(0) = 0 \pmod{y^2+y-1}$ $(0_A \mapsto 0_B)$

$\varphi(x^2) + \varphi(1) = 0$ in $\mathbb{R}$

Hence, $\varphi(x)$ is a root at $t^2+t-1=0$

Plug $h = 1+2y$ in x^2+1 (instead of x)

$(1+2y)^2+1 = 1+4y+4y^2+1 \equiv 1+y+y^2+1 = y^2+y+2 \equiv y^2+y-1 \equiv 0 \pmod{y^2+y+1}$

Thus, $a+bx \mapsto a+b(1+2y) = a+b-2by$

For ψ:

$y^2+y-1 \equiv 0 \pmod{y^2+y-1}$

$\varphi(y^2) + \varphi(y) + \varphi(-1) \equiv 0 \pmod{y^2+y-1}$

$\varphi(y)$ is a root at $t^2+1 \equiv 0$ (x^2+1)

Take $h = 1+2x$ in $y^2+y-1 = (1+2x)^2+(1+2x)-1 =$

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

$= 4x^2+6x+1 \equiv x^2+1 \equiv 0 \pmod{x^2+1}$

Thus, $a+by \mapsto a+b(1+2x) = a+b+2bx$

$(\psi \circ \varphi)(a+bx) = \psi(a+b+2by) = a+b+2b+4bx = a+bx$

$(\varphi \circ \psi)(a+by) = \psi(a+b+2bx) = a+b+2b+4by = a+by$ ∎

2. Compute the generators of the group $\mathbb{F}_9^*$ if $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 - x - 1)$.

By th, if $|F^*| < \infty \Rightarrow F^* \simeq \mathbb{Z}_{|F|-1}$

Thus $F_9^* \simeq \mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

Then F_9^* has 4 generators also

$$\left.\begin{aligned}
(x+2) &= x+2 \\
(x+2)^2 &\equiv 2x+2 \\
(x+2)^3 &\equiv 2x \\
(x+2)^4 &\equiv 2 \\
(x+2)^5 &\equiv 2x+1 \\
(x+2)^6 &\equiv x+1 \\
(x+2)^7 &\equiv x \\
(x+2)^8 &\equiv 1
\end{aligned}\right\} \Rightarrow x+2 \text{ is a generator for } F_8^*$$

by th. if f is generator then f^i is also gen. if $\gcd(i, |F^*|-1) = 1$

Thus 3, 5, 7 are coprime with $|F^*|-1 \Rightarrow (x+2)^3, (x+2)^5$ & $(x+2)^7$ are generators

Hence $F_9^* = \langle x+2 \rangle = \langle 2x \rangle = \langle 2x+1 \rangle = \langle x \rangle$

3. Let $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + x + 2)$, $g = x$, and $h = x + 2$.

(a) Compute the matrix A of the map $\phi\colon \mathbb{F}_9 \to \mathbb{F}_9$ by the rule $f \mapsto xf$ in the basis $1, x$.

(b) Compute coefficients of hg^k for $0 \leqslant k \leqslant 8$ using the matrix A.

a) $\varphi(1) = x \equiv x \pmod{x^2+x+2}$

$\varphi(x) = x^2 \equiv 2x+1 \pmod{x^2+x+2}$

$\Rightarrow \varphi\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \wedge \varphi\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) \Rightarrow \begin{bmatrix} 1 \\ 2 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$ is coordinate matrix of φ.

b) $\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^0 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = x+2$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^1 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 4x+1 \equiv x+1$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^2 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 9x+4 \equiv 1$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^3 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 22x+9 \equiv x$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^4 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 53x+22 \equiv 2x+1$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^5 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 128x+53 \equiv 2x+2$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^6 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 309x+128 \equiv 2$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^7 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 746x+309 \equiv 2$

$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^8 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 1801x+746 \equiv x+2$

4. Consider the polynomial $x^2 + 2 \in \mathbb{Z}_5[x]$.

(a) Show that $x^2 + 2$ is irreducible.

(b) Now, we define $\mathbb{F}_{25} = \mathbb{Z}_5[x]/(x^2+2)$. Find inverse of the element $2 + 3x \in \mathbb{F}_{25}$.

(c) Compute the following expression in $\mathbb{F}_{25}$:

$$\frac{3+4x+x^2}{4+3x+x^2}$$

a) since $\deg(x^2+2) = 2 \Rightarrow (x^2+2) = p_1 p_1$ or p_2, where p_i is irr pol $\in \mathbb{Z}_5[x]$ of deg i

Thus $\{0,1,2,3,4\}$ are not roots of (x^2+2) x^2+2 is not a product of two irr. pol. of deg. 1, thus it's irreducible pol. itself

$0^2+2 \not\equiv 0\ (5)$ $\quad 3^2+2 \not\equiv 0\ (5)$

$1^2+2 \not\equiv 0\ (5)$ $\quad 4^2+2 \not\equiv 0\ (5)$ $\quad \Rightarrow$ no roots in $\mathbb{Z}_5$

$2^2+2 \not\equiv 0\ (5)$

$x^2+2 \equiv 0\ (x^2+2)$

$\Updownarrow$

$x^2 \equiv 3\ (x^2+2)$

2) $\mathbb{Z}_5(x^2+2) = \{ax+b \mid a,b \in \mathbb{Z}_5\}$

Thus $(ax+b)(3x+2) = 3ax^2 + 2ax + 3bx + 2b \equiv 4a + x(2a+3b) + 2b \pmod{x^2+2}$

$(ax+b) = (3x+2)^{-1}$ iff $x(2a+3b) + 2b + 4a \equiv 1 \pmod{x^2+2}$

$\Downarrow$

unique in $\mathbb{Z}_5$

$$\begin{cases} 2a+3b \equiv 0 \pmod 5 \\ 2b+4a \equiv 1 \pmod 5 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 1 \end{cases} \Rightarrow (x+1) = (3x+2)^{-1}$$

3) $x^2 \equiv 3\ (x^2+2)$

$$\frac{3+4x+x^2}{4+3x+x^2} \equiv \frac{3+4x+3}{4+3x+3} = \frac{6+4x}{7+3x} \equiv \frac{4x+1}{3x+2} \pmod{x^2+2}$$

$$(4x+1)(3x+2)^{-1} = (4x+1)(x+1) = 4x^2+1 \equiv 12+1 \equiv 3 \pmod{x^2+2}$$