

$$p(x) = x^p + a$$

\mathbb{Z}_p $f(x) = x^p + a$

\downarrow

$$p'(x) = 0$$

$$p' \neq 0 \quad \text{על } p \text{ ו-} p \in F[x] \quad \text{על } \mathbb{Z}_p$$

$$\deg(\underbrace{\text{gcd}(p, p')}_g) = 0 \quad \Leftrightarrow \text{פרימיטיבי } p$$

יש α שבו $p(\alpha) = 0$ \Rightarrow

$$p(x) = (x - \alpha)^r \cdot h(x) \quad (r \geq 2)$$

\downarrow

הגורם $(x - \alpha)$ נחלק

$$p' \nmid p \text{ על } (x - \alpha) \Leftrightarrow g \text{ על } \alpha \text{ ו-} p(\alpha) \neq 0 \quad \Leftarrow$$

p על α שבו $p(\alpha) = 0$ \Leftarrow

$$(h(\alpha) \neq 0) \quad p = (x - \alpha)h(x) \quad \uparrow$$

\rightarrow α

$$p' = (x - \alpha)h'(x) + h(x)$$

\downarrow

$$p'(\alpha) \neq 0$$

(הגורם $(x - \alpha)$ אינו חלק)

על \mathbb{Z}_2 $f(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$

$$(F = \text{Frac}(\mathbb{Z}_2[x]))$$

$$F = \mathbb{Z}_2(x)$$

$$p(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$$

$$\text{פרימיטיבי } p \Leftrightarrow \text{יש } \sqrt{\lambda} \Leftrightarrow \sqrt{\lambda} = -\sqrt{\lambda} \Leftrightarrow \lambda \in \mathbb{Z}_2$$

$$p \text{ על } \sqrt{\lambda} \in F$$

על \mathbb{Z}_2 $f(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$ $\Leftrightarrow \lambda \in \mathbb{Z}_2$

$$(n \text{ אי-זוגי, } n \neq 0, \text{ ו-} n \text{ אי-זוגי, } n \neq 0)$$

על \mathbb{Z}_2 $f(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$ $\Leftrightarrow \lambda \in \mathbb{Z}_2$

f פרימיטיבי \Leftrightarrow אי-זוגי n \Leftrightarrow $n \neq 0$

על \mathbb{Z}_2 $f(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$ $\Leftrightarrow \lambda \in \mathbb{Z}_2$

על \mathbb{Z}_2 $f(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$ $\Leftrightarrow \lambda \in \mathbb{Z}_2$

על \mathbb{Z}_2 $f(x) = x^2 - \lambda = (x - \sqrt{\lambda})(x + \sqrt{\lambda})$ $\Leftrightarrow \lambda \in \mathbb{Z}_2$

• \mathbb{Z}_p ist ein

• \mathbb{Z}_p ist ein $\mathbb{Z}_p[x]$

• \mathbb{Z}_p ist ein

• $\mathbb{Z}_p[x] / \langle f \rangle$ ist ein

• $\mathbb{Z}_p[x] / \langle x^n - x \rangle$ ist ein

• $\mathbb{Z}_p[x] / \langle x^n - x \rangle$ ist ein