$\boxed{\text{Example}}$ Consider x^3+x^2+1 over $\mathbb{Z}_2$

Is it irreducible? If α is a root, what is a simple extension of this?

Solution: since $\deg(x^3+x^2+1)=3$, if it factors nontrivially, then it must have a linear factor, i.e. a root in $\mathbb{Z}_2$. We check: $0^3+0^2+1=1 \not\equiv 0 \bmod 2$.

$1^3+1^2+1=1 \not\equiv 0 \bmod 2$.

$\therefore$ no linear factors $\Rightarrow p(x)=x^3+x^2+1$ is irreducible.

Let α be a root of x^3+x^2+1 in some extension field E of $\mathbb{Z}_2$.

α is algebraic since it is a root of the polynomial

By the theorem, $\phi_\alpha(\mathbb{Z}_2[x])$ is isomorphic to E.

$$\mathbb{Z}_2[x] = \{a_0+a_1x+a_2x^2+\cdots+a_kx^k : a_j\in\mathbb{Z}_2 \ \forall j\}.$$

$$\phi_\alpha(\mathbb{Z}_2[x]) = \{a_0+a_1\alpha+a_2\alpha^2+\cdots a_k\alpha^k : a_j\in\mathbb{Z}_2 \ \forall j, \ \underbrace{\alpha^3+\alpha^2+1=0}\}$$

$=$

$\alpha^3=-\alpha^2-1=\underline{\alpha^2+1}$

$\alpha^4=\alpha^3+\alpha$

$=\underline{\alpha^2+1+\alpha}$

$\alpha^5=\alpha^3+\alpha+\alpha^2$

$\alpha^5=\alpha^2+1+\alpha+\alpha^2$

$\alpha^5=\underline{1+\alpha}$

$\alpha^6 = \alpha + \alpha^2$
$\alpha^7 = \alpha^2 + \alpha^3$
$= \alpha^2 + \alpha^2 + 1$
$\alpha^7 = 1$

$$\Rightarrow \phi_\alpha(\mathbb{Z}_2[x]) = \{a_0 + a_1\alpha + a_2\alpha^2 : a_0, a_1, a_2 \in \mathbb{Z}_2\}$$

A vector space over $\mathbb{Z}_2$ with basis $\{1, \alpha, \alpha^2\}$. This is a field with 8 elements. (and characteristic $= 2$: $\beta + \beta = 0 \; \forall \beta$ in $\mathbb{Z}_2[\alpha]$.)

$[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2]$
$\shortparallel$
$[\mathbb{Z}_2[\alpha] : \mathbb{Z}_2]$ = The dimension of $\mathbb{Z}_2[\alpha]$ over $\mathbb{Z}_2$ is 3 $= \deg(p(x))$.

---

similar to: $\alpha = i$ is root of x^2+1, irreducible over $\mathbb{R}$

$$\mathbb{R}(i) = \{a_0 + a_1 i : a_0, a_1 \in \mathbb{R}\} = \mathbb{C}$$

$$[\mathbb{R}(i) : \mathbb{R}] = 2 = \deg(x^2+1)$$

$\mathbb{C}$ is a vector space of dim 2 over $\mathbb{R}$ with basis $1, i$.

<u>Definition:</u> Sp. E is an extension field of F, $f(x) \in F[x]$. We say $f(x)$ <u>splits in E</u> if $f(x)$ can be written as a product of linear factors in $E[x]$. E is called a <u>splitting field for $f(x)$ over F</u> if $f(x)$ splits in E but in no proper subfield.

Notation: If $\alpha_1, \alpha_2, \dots, \alpha_k \in E$, then

$F(\alpha_1, \alpha_2, \dots, \alpha_k)$ = smallest subfield of E containing $F, \alpha_1, \alpha_2, \dots \alpha_k$.

Cor of Kronecker Theorem. If F is a field & $f(x) \in F[x]$ is nonconstant. Then there exists a splitting field of $f(x)$ over F.

Pf: Induction + Kronecker theorem (getting field containing one root at a time). ∎

Thm. If F is a field, $p(x) \in F[x]$ is irreducible over F, If a is a zero of $p(x)$ in some extension field E of F, then

$$F(a) \cong F[x]/\langle p(x)\rangle.$$ If $\deg(p(x)) = n$,

then $$F(a) = \{c_0 + c_1 a + \cdots + c_{n-1}a^{n-1} : c_j \in F \; \forall j\}.$$

Cor. Let $p(x) \in F[x]$ be irreducible. Let a, b be two different roots of $p(x)$ in same extension field E. Then $F(a) \cong F(b)$.

Proof: $F(a) \cong F[x]/\langle p(x)\rangle \cong F(b)$. $\boxtimes$

[Also, when a is algebraic over F,

$F(a)$ is a vector space over F

of dimension $\deg(p(x))$.]