Example Find the splitting field of $\underbrace{x^2+x+2}_{f(x)}$ over $\mathbb{Z}_3$.

If x^2+x+2 has a nontrivial factor, then it has a root, because the factors must be linear.

Check
$x=0 \Rightarrow f(0) = 2 \neq 0$
$x=1 \Rightarrow f(1) = 1 \neq 0$
$x=2 \Rightarrow f(2) = 2 \neq 0.$
$\Bigg\}$ No linear factor. $\therefore f(x)$ is irred.

From quadratic formula $\left(x - \left(\frac{-1 + \sqrt{1-8}}{2}\right)\right)\left(x - \left(\frac{-1-\sqrt{-7}}{2}\right)\right)$

$\frac{-1+i}{-1} = 1-i$ $\quad 1+i$

Check. $(1+i)^2 + (1+i) + 2 = 1+(-1)+2i + 1+i+2$
$= 3+3i = 0. \checkmark$

also $(1-i)^2 + (1-i) + 2 = 0$

So splitting field is $\mathbb{Z}_3[i] = \{a+bi : a,b \in \mathbb{Z}_3\}$

$x^2+x+2 = (x-(1+i))(x-(1-i))$.

Let's instead start from: if $\beta \in E$ is a root of x^2+x+2,
then $\mathbb{Z}_3(\beta) \cong \mathbb{Z}_3[x]/\langle x^2+x+2\rangle$

$= \{a+b\beta : a,b \in \mathbb{Z}_3\}$

$E = \{0, 1, 2, \beta, 1+\beta, 2+\beta, 2\beta, 1+2\beta, 2+2\beta\}$

Note $\beta^2+\beta+2=0$

Let's now factor x^2+x+2 using β:

$$
\begin{array}{r l}
 & x + (1+\beta) \\
x-\beta \,\big) & x^2 + x + 2 \\
 & \underline{x^2 - \beta x} \\
 & (1+\beta)x + 2 \\
 & \underline{(1+\beta)x - \beta(1+\beta)}
\end{array}
$$

$2+\beta(1+\beta) = 2+\beta+\beta^2 = 0.$

$\therefore \boxed{x^2+x+2 = (x-\beta)(x+(1+\beta))}$ ← roots $\beta, -1-\beta$

$\therefore E$ is the splitting field of x^2+x+2.

Moral of the story: For an irreducible poly. of degree 2, the splitting field is $F(\beta)$ for a root β.

Does this fit the previous extension field we found?

does $\beta = i$ work? No, but

$\beta = 1+i$ works

$\Rightarrow -1-\beta = -1-(1+i) = -2-i$

$= 1-i$. ✓

The second E we found was

$\mathbb{Z}_3(1+i)$, rather than $\mathbb{Z}_3(i)$.

Exercise ① Show that not every element of $\mathbb{Z}_p$ (for p prime) is a square. ie it is not true that

$\forall x \in \mathbb{Z}_p,\ x = y^2$ for some $y \in \mathbb{Z}_p$.

$\Longleftrightarrow \exists x \in \mathbb{Z}_p$ s.t. $x \neq y^2\ \forall y \in \mathbb{Z}_p$.

eg. $\mathbb{Z}_5$: $0, 1, 2, 3, 4 \xrightarrow{x^2} 0, 1, 4, 4, 1$

$\mathbb{Z}_7$: $0, 1, 2, 3, 4, 5, 6 \xrightarrow{x^2} 0, 1, 4, 2, 2, 4, 1$

$$\begin{array}{cccccccccccc} \mathbb{Z}_{11} & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10 \\ x^2 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \end{array}$$

In general $a^2 = (p-a)^2$ for $1 \le a \le p-$

$\therefore \left| \{ z \in \mathbb{Z}_p : z = a^2 \text{ for some } a \in \mathbb{Z}_p \} \right| \le \frac{p-1}{2} + 1 < p$
$= \frac{p+1}{2}$.

$\therefore \exists z_0 \in \mathbb{Z}_p : z$ is not a square.

(2) Prove that $\forall$ prime p, $\exists$ a field of order p^2.

By above $\exists z_0 \in \mathbb{Z}_p : z_0$ is not a square.

$\therefore x^2 - z_0$ is irreducible in $\mathbb{Z}_p$.

$\Rightarrow \mathbb{Z}_p[x] / \langle x^2 - z_0 \rangle$ is a field of order p^2.

$$\parallel$$

$\{ a_0 + a_1 x + \langle x^2 - z_0 \rangle : a_0, a_1 \in \mathbb{Z}_p \}$. $\boxed{Q}$

<u>Lemma</u> Let F be a field, $p(x)$ irreducible over F, α a zero of $p(x)$ in E, $F \le E$.

Let $\phi : F \to F'$ be an isomorphism (ring isomorphism)

another field.

Let β be a zero of $\phi(p(x)) \in F'[x]$ in some E'

Take ϕ of the coefficients

Then $\exists$ isomorphism $F(\alpha) \to F'(\beta)$ such that $\alpha \mapsto \beta$
$c \in F \mapsto \phi(c) \in F'$!

Thm (Proof is induction on the previous Lemma)

As above: Let E be the splitting field of $p(x)$ over F

$\Rightarrow E'$ . . . . . . $\phi(p(x))$ over F'

Then $E \cong E'$.

$F \to F'$

Moral: Splitting fields of polys. in $F[x]$ are uniquely defined (up to isomorphism).