Thm: $\forall n \in \mathbb{N}$, $\Phi_n \in \mathbb{Z}[x]$.

Pf: Induction on n. True for $n=1$. Suppose true for $1 \le m < n$.

Then $x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) f(x)^{(*)}$, where $f \in \mathbb{Z}[x]$

by the inductive hypothesis.

By the div. alg. in $\mathbb{Q}[x]$, $\exists\, q, r \in \mathbb{Q}[x]$ s.t.

$$x^n - 1 = q(x) f(x) + r(x), \text{ and } r = 0 \text{ or } \deg r < \deg f.$$

If $r \neq 0$ then this would also satisfy the div alg. over $\mathbb{Q}(\zeta_n)[x]$, $\zeta_n = e^{2\pi i/n}$, but that would contradict the uniqueness of the remainder in the div. alg. (by (*)).

By Gauss's lemma $\exists\, a \in \mathbb{Q} \setminus \{0\}$ s.t.

$$a\Phi_n(x),\ a^{-1} f(x) \in \mathbb{Z}[x].$$

Since all polys. in the factorization (*) are monic, this forces $a = 1$, so $\Phi_n \in \mathbb{Z}[x]$. ∎

Thm: $\forall n \in \mathbb{N}$, $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.

Pf: If not then (let $n \geq 3$) $\Phi_n(x) = f(x)g(x)$ with $f, g \in \mathbb{Z}[x]$, $\deg f, \deg g > 1$, and we can also assume that f is irred. Let ζ be a prim. nth root of 1 with $f(\zeta) = 0$ and let p be any prime not dividing n. Then ζ^p is also a prim. nth root of 1, so $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

Claim: $f(\zeta^p) = 0$.

Suppose not. Then $g(\zeta^p) = 0$

$\Rightarrow$ ζ is a root of $g(x^p) \in \mathbb{Z}[x]$

$\Rightarrow$ $f(x) = \min_{\mathbb{Q}}(\zeta) \mid g(x^p)$

$\Rightarrow$ $g(x^p) = f(x)h(x)$ for some $h \in \mathbb{Z}[x]$.

Now think about this equation in $\mathbb{F}_p[x]$:

(Note: Suppose $g(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{F}_p[x]$.

Then
$$g(x^p) = \sum_{i=0}^{m} b_i (x^i)^p = \sum_{i=0}^{m} b_i^p (x^i)^p = \sum_{i=0}^{m} (b_i x^i)^p = \left(\sum_{i=0}^{m} b_i x^i\right)^p = g(x)^p.)$$

In $\mathbb{F}_p[x]$, $g(x)^p = f(x)h(x)$.

Since $\mathbb{F}_p[x]$ is a UFD, this implies that g and f have a common factor $l(x)$ with $\deg l > 1$.

Then $x^n - 1 = f(x)g(x) \Rightarrow \ell^2(x) \mid x^n - 1$ in $\mathbb{F}_p[x]$

$\Rightarrow x^n - 1$ has a repeated root in $\overline{\mathbb{F}_p}$

Since $D_x(x^n - 1) = nx^{n-1} \neq 0$ in $\mathbb{F}_p[x]$ (since $p \nmid n$),

has only $x = 0$ as a root, and

since $0^n - 1 \neq 0$, the polynomial

$x^n - 1$ is separable over $\mathbb{F}_p$.

This gives a contradiction, so we conclude

that $g(\zeta^p) \neq 0$. This forces $f(\zeta^p) = 0$.

Now suppose $f(\zeta) = 0$ and that $a \in \mathbb{N}$, $(a, n) = 1$.

Write $a = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are primes

Then $\zeta^a = ((\zeta^{p_1})^{p_2} \cdots)^{p_k}$ is also a root of $f(x)$.

Since all primitive nth roots of 1 can be written

in this way, we have $f(x) = \Phi_n(x)$, which

is a contradiction.

This implies that Φ_n is irreducible over $\mathbb{Z}$. $\square$

Exs: 1(a) What is the splitting field of $f(x) = x^n - 1$ over $\mathbb{Q}[x]$? Call it K.

$$\begin{tikzcd} K = \mathbb{Q}(\zeta_n) \arrow[d, dash, "\varphi(n)"] \\ \mathbb{Q} \end{tikzcd} \qquad \min_{\mathbb{Q}}(\zeta_n) = \Phi_n(x)$$

b) Let $f(x) = x^{15} - 2 \in \mathbb{Q}[x]$ what is the spl. field? Call it K.

$$\{z \in \mathbb{C} : z^{15} = 2\}$$

$$= \{z = 2^{1/15} e^{2\pi i a/15} : 0 \leq a < 15\}$$

$$\Rightarrow 2^{1/15},\ e^{2\pi i/15} \in K$$

$$\begin{tikzcd}
 & \mathbb{C} \arrow[d, dash] & \\
 & K = \mathbb{Q}(2^{1/15}, \zeta_{15}) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
\mathbb{Q}(\zeta_{15}) \arrow[dr, dash, "\varphi(15) = 8"'] & & \mathbb{Q}(2^{1/15}) \arrow[dl, dash, "15"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Note that $K = \mathbb{Q}(2^{1/15}, \zeta_{15}) = \mathbb{Q}(\zeta_{15}) \cdot \mathbb{Q}(2^{1/15})$,

$[\mathbb{Q}(2^{1/15}) : \mathbb{Q}] = 15$, and $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = \varphi(15) = (3-1)(5-1) = 8$.

Since $8 \mid [K : \mathbb{Q}]$, $15 \mid [K : \mathbb{Q}]$, and $[K : \mathbb{Q}] \leq 8 \cdot 15$,

we have that $[K : \mathbb{Q}] = 8 \cdot 15 = 120$.