The problem of factoring $f(x) = x^n - 1$ is made easy with the imaginary exponential $e^{i\theta} = \cos\theta + i\sin\theta$ for which $(e^{i\theta})^j = e^{ij\theta}$ for any $j \in \mathbb{Z}$. Observe $e^{i\theta} = 1$ only if both $\cos\theta = 1$ and $\sin\theta = 0$. Hence $e^{i\theta} = 1$ iff $\theta \in 2\pi\mathbb{Z}$. Consider then,

$$\begin{aligned}(e^{i\theta})^n - 1 = 0 &\iff e^{in\theta} = 1 \\ &\iff n\theta = 2\pi k \text{ for } k \in \mathbb{Z} \\ &\iff \theta = \frac{2\pi k}{n} \text{ for } k \in \mathbb{Z}.\end{aligned}$$

Thus $f\left(\exp\left(\frac{2\pi k i}{n}\right)\right) = f(\zeta_n^k) = 0$ for $k \in \mathbb{Z}$

where $\boxed{\text{Def}^{\underline{n}}/\ \zeta_n = \exp\left(\frac{2\pi i}{n}\right) = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)}$

However, $\deg(x^n - 1) = n$ thus $\{\zeta_n^k \mid k \in \mathbb{Z}\}$ has at most n distinct roots for $f(x) = x^n - 1$. Observe, $f'(x) = nx^{n-1} = 0$ only for $x = 0$ thus $f(x) = x^n - 1$ has no multiple roots, $f(x)$ is separable.

> **Def$^{\underline{n}}$/** $1^{1/n} = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$ are the n^{th} roots of unity. Any generator of this group is called a <u>primitive</u> n^{th} root of unity.

If $K/\mathbb{Q}$ contains ζ_n then $1^{1/n} \subset K$ and $f(x) = x^n - 1$ completely splits in $K[x]$. It follows that $\mathbb{Q}(\zeta_n)$ is a splitting field for $x^n - 1$.

<u>Remark</u>: Dummit & Foote use μ_n for $1^{1/n}$.

Def^{n}/ The field $\mathbb{Q}(\zeta_n)$ is called the cyclotomic field of n^{th} roots of unity.

By explicit construction $\mathbb{Q}(\zeta_n) \subset \mathbb{C}$, however we should think about ~~the~~ a splitting field for $x^n - 1$ as an abstract field $K/\mathbb{Q}$ then that field K contains α, β for which $\alpha^n - 1 = 0$ and $\beta^n - 1 = 0$ thus $\alpha^n = 1$, $\beta^n = 1$ and $(\alpha\beta)^n = \alpha^n\beta^n = 1$ and we find $\{\alpha \in K^\times \mid \alpha^n = 1\}$ forms a subgroup of $K^\times$, the group of n^{th} roots of unity within K. This is not surprising, after all $\mathbb{C}$ contains $1^{1/n}$ which is isomorphic to the abstract group of units described above.

Remark: it is a times helpful to allow the abstraction above since an example may not reside within $\mathbb{C}$ and yet it may have a splitting field like $\mathbb{Q}(\zeta_n)$.

$$\zeta_1 = 1$$

$$\zeta_2 = -1$$

$$\zeta_3 = \frac{-1 + i\sqrt{3}}{2}$$

$$\zeta_4 = i$$

$$\zeta_5 = \frac{\sqrt{5} - 1}{4} + i\left(\frac{\sqrt{10 + 2\sqrt{5}}}{4}\right)$$

$$\zeta_6 = \frac{1 + i\sqrt{3}}{2}$$

$$\zeta_8 = \frac{\sqrt{2} + i\sqrt{2}}{2}$$

GOAL: explain why $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ where $\varphi(n)$ is Euler-φ function. In particular, $\Phi_n(x) = m_{\zeta_n, \mathbb{Q}}(x)$ is the n^{th} cyclotomic polynomial

The algebra of cyclotomic polynomials is very nice

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

When p is prime then the formula above reveals $\boxed{[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1}$,

$$x^p - 1 = (x-1)\underbrace{(x^{p-1} + x^{p-2} + \cdots + x + 1)}$$

$m_{\zeta_p, \mathbb{Q}}(x)$ since we showed this polynomial was irreducible in the previous lecture based on §9.4 Example 4 of D&F

When n is composite we'll have to think about how the factors of n are reflected in the factorization of $x^n - 1$

Def$^{\underline{n}}$/ The $n^{\underline{th}}$ cyclotomic polynomial $\Phi_n(x)$ is the polynomial whose roots are the primitive $n^{\underline{th}}$ roots of unity

Let's study the low cases of n to appreciate the structure,

$\underline{n=1|}$ $x - 1 = \Phi_1(x)$

$\underline{n=2|}$ $x^2 - 1 = (x-1)(x+1)$ $\therefore$ $\underbrace{\Phi_2(x) = x+1}$

$= \Phi_1(x)\Phi_2(x)$

has root $-1 = \zeta_2$ the only $2^{\underline{nd}}$ primitive root of unity.

$\underline{n=3|}$ $x^3 - 1 = (x-1)(x^2 + x + 1)$ $\therefore$ $\underbrace{\Phi_3(x) = x^2 + x + 1}$

$= \Phi_1(x)\Phi_3(x)$

has roots ζ_3 and ζ_3^2 which are the primitive $3^{\underline{rd}}$ roots of unity.

$\underline{n=4|}$ $x^4 - 1 = (x^2-1)(x^2+1)$

$= (x-1)(x+1)(x^2+1)$ $\therefore$ $\underbrace{\Phi_4(x) = x^2 + 1}$

$= \Phi_1(x)\,\Phi_2(x)\,\Phi_4(x)$

has roots $\zeta_4 = i$ and $\zeta_4^3 = -i$

$n=5$ $x^5-1=(x-1)(x^4+x^3+x^2+x+1) \therefore \Phi_5(x)=x^4+x^3+x^2+x+1$

$= \Phi_1(x)\,\Phi_5(x)$

it has roots $\zeta_5 = \exp\left(\frac{2\pi i}{5}\right)$ and $\zeta_5^2, \zeta_5^3, \zeta_5^4$ as well

$n=6$ $x^6-1=(x^3-1)(x^3+1)$

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

$=\Phi_1(x)\Phi_3(x)\,\Phi_2(x)\,\Phi_6(x)$

$\therefore$ $\Phi_6(x)=x^2-x+1$ and it has roots $\zeta_6 = e^{\frac{2\pi i}{6}} = \frac{1+i\sqrt{3}}{2}$ and $\zeta_6^2 = \frac{1-i\sqrt{3}}{2}$

$n=8$ $x^8-1=(x^4-1)(x^4+1)$

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

$=\Phi_1(x)\Phi_2(x)\Phi_4(x)\,\Phi_8(x)$

$\therefore$ $\Phi_8(x)=x^4+1$ and it has roots $\zeta_8 = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}$ and $\zeta_8^3, \zeta_8^5, \zeta_8^7$

$n=12$ $x^{12}-1=(x^6-1)(x^6+1)$

$=(x^3-1)(x^3+1)(x^2+1)(x^4-x^2+1)$

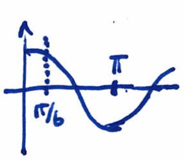
$\therefore$ $\Phi_{12}(x)=x^4-x^2+1$

$\gcd(k,12)=1$ for $k=1,5,7,11$ hence $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$ are the primitive 12^{th} roots of unity and so $\deg(\Phi_4(x))=4$

$\zeta_{12}^4 = \left[\exp\left(\frac{2\pi i}{12}\right)\right]^4 = e^{\frac{2\pi i}{3}}$

$\Phi_{12}(x) = (x-e^{\pi i/6})(x-e^{5\pi i/6})(x-e^{7\pi i/6})(x-e^{11\pi i/6})$

$= (x-e^{\pi i/6})(x-e^{-\pi i/6})(x-e^{5\pi i/6})(x-e^{-5\pi i/6})$



$= \left(x^2-(e^{\pi i/6}+e^{-\pi i/6})x+1\right)\left(x^2-(e^{5\pi i/6}+e^{-5\pi i/6})x+1\right)$

$= (x^2-2\cos(\pi/6)x+1)(x^2-2\cos(5\pi/6)+1)$

$= (x^2-\sqrt{3}x+1)(x^2+\sqrt{3}x+1)$

$= x^4+\cancel{\sqrt{3}x^3}+\underline{\underline{x^2}}-\cancel{\sqrt{3}x^3}-\underline{\underline{(\sqrt{3})^2x^2}}-\cancel{\sqrt{3}x}+\underline{\underline{x^2}}+\cancel{\sqrt{3}x}+1$

$= \underline{x^4-x^2+1}.$

Perhaps the pattern is clear, if n has $d_1, d_2, \ldots, d_k$ as positive divisors of n (excluding n in my current discussion) beginning with $d_1 = 1$ then

$$X^n - 1 = \Phi_{d_1}(x)\,\Phi_{d_2}(x)\cdots\Phi_{d_k}(x)\,\Phi_n(x)$$

Which yields

$$(x-1)(x^{n-1}+\cdots+x+1) = (x-1)\left(\Phi_{d_2}(x)\cdots\Phi_{d_k}(x)\,\Phi_n(x)\right)$$

$$\Rightarrow \Phi_n(x) = \frac{x^{n-1}+\cdots+x+1}{\Phi_{d_2}(x)\cdots\Phi_{d_k}(x)}$$

$n=12$ again, this time via long division

12 is divided by 1, 2, 3, 4, 6 thus

$d_2 = 2,\ d_3 = 3,\ d_4 = 4,\ d_5 = 6$ and

$$\Phi_{d_2}(x)\,\Phi_{d_3}(x)\,\Phi_{d_4}(x)\,\Phi_{d_5}(x) = \Phi_2(x)\,\Phi_3(x)\,\Phi_4(x)\,\Phi_6(x)$$

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

$$= (x^3+x^2+x+x^2+x+1)(x^4-x^3+x^2+x^2-x+1)$$

$$= (x^3+2x^2+2x+1)(x^4-x^3+2x^2-x+1)$$

$$\begin{aligned} = x^7 - x^6 + 2x^5 - x^4 + x^3 & \\ +2x^6 - 2x^5 + 4x^4 - 2x^3 + 2x^2 & \\ +2x^5 - 2x^4 + 4x^3 - 2x^2 + 2x & \\ +x^4 - x^3 + 2x^2 - x + 1 & \end{aligned}$$

$$= x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$$

$$\Phi_{12}(x) = \frac{x^{11}+x^{10}+\cdots+x+1}{x^7+x^6+2x^5+2x^4+2x^3+2x^2+x+1} = x^4 - x^2 + 1$$

Let's summarize the theory here,

If $d \mid n$ and ζ is an n^{th} root of unity ($\zeta \in \mu_n = 1^{1/n}$)

then $\zeta^n = (\zeta^d)^{n/d} = 1$ where n/d is a positive integer

CLAIM: if $d \mid n$ then $\mu_d \subseteq \mu_n$

Proof: $d \mid n$ then $n = md$ for some $m \in \mathbb{N}$ (assume d, n positive)

Thus if $\alpha \in \mu_d$ with $\alpha^d = 1$ then $(\alpha^d)^m = \alpha^{dm} = \alpha^n = 1$

consequently $\alpha \in \mu_n \therefore \mu_d \subseteq \mu_n$.

Note also, if $\alpha \in \mu_n$ then $|\alpha|$ must divide $|\mu_n| = n$, and if $|\alpha| = d$ then $\alpha \in \mu_d$ where $d \mid n$.

$$\boxed{x^n - 1 = \prod_{\zeta^n = 1} (x - \zeta) = \prod_{d \mid n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta) = \prod_{d \mid n} \Phi_d(x)}$$

Where $\Phi_k(x) = \prod_{\substack{\alpha \in \mu_k \\ \alpha \text{ primitive}}} (x - \alpha)$ defines the k^{th} cyclotomic polynomial.

Remark: since $\deg(\Phi_d(x)) = \varphi(d)$ and $\deg(x^n - 1) = n$ we find from the above boxed formula that

$$n = \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_s)$$

where $d_1 = 1, d_2, \ldots, d_s = n$ are the positive divisors of n.

E1 $12 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12)$

$= 1 + 1 + 2 + 2 + 2 + 4$ ✓

Lemma (40): The cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$

PROOF: we've already argued $\Phi_n(x)$ is monic (by construction) and degree $\varphi(n)$. It remains to show the coefficients of $\Phi_n(x)$ are in $\mathbb{Z}$. We proceed by induction on n. Suppose inductively $\Phi_d(x) \in \mathbb{Z}[x]$ for all $1 \leq d < n$. Consider that

$x^n - 1 = f(x)\,\Phi_n(x)$ where $f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ is monic with coefficients in $\mathbb{Z}$ by the induction hypothesis. Note

$f(x) \mid x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$ and both $f(x)$, x^n-1 have coeff. in $\mathbb{Q}$.

$\Rightarrow f(x) \mid x^n - 1$ in $\mathbb{Q}[x] \Rightarrow f(x) \mid x^n - 1$ in $\mathbb{Z}(x)$ (by §9.2)

$\Rightarrow \Phi_n(x) \in \mathbb{Z}[x]$. //

Th$^{\underline{m}}$ (41): The cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ with degree $\varphi(n)$

Proof: it remains, after Lemma 40, to show $\Phi_n(x)$ is irred. Suppose $\Phi_n(x) = f(x)\,g(x)$ with $f(x), g(x)$ monic in $\mathbb{Z}[x]$, and $f(x)$ is an irreducible factor of $\Phi_n(x)$. If ζ is a primitive $n^{\underline{th}}$ root of 1 which is a root of $f(x)$ then $f(x)$ is minimal polynomial for ζ over $\mathbb{Q}$. Further, let p be a prime not dividing n. Then ζ^p is a primitive $n^{\underline{th}}$ root of 1 hence is either a root of $f(x)$ or $g(x)$.

① If $g(\zeta^p) = 0$ then ζ is root of $g(x^p)$ and as $f(x)$ is the minimal poly. for ζ we see $f(x) \mid g(x^p)$ in $\mathbb{Z}(x)$. That is, $\underline{g(x^p) = f(x)h(x)}_*$ for some $h(x) \in \mathbb{Z}[x]$. Reduce $*$ modulo p, $\bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$ in $\mathbb{F}_p[x]$ hence via Frob. Endo, $(\bar{g}(x))^p = \bar{f}(x)\bar{h}(x)$ in the UFD $\mathbb{F}_p[x]$

$\Rightarrow \bar{f}(x), \bar{g}(x)$ share common factor in $\mathbb{F}_p[x]$.

Proof continued

We had $\Phi_n(x) = f(x)g(x)$ thus in $\mathbb{F}_p[x]$

$\bar{\Phi}_n(x) = \bar{f}(x)\bar{g}(x) \Rightarrow \bar{\Phi}_n(x) \in \mathbb{F}_p[x]$ has a multiple root. But, then $x^n - 1$ would also have multiple root over $\mathbb{F}_p$ since $\bar{\Phi}_n(x)$ is factor of $\overline{x^n-1}$. But, we have shown x^n-1 has n-distinct roots over any field with characteristic not dividing n.

② $\therefore$ ζ^p must be root of $f(x)$ (going back to ① just before, we saw $\exists$ two options either ζ^p is root of $f(x)$ or $g(x)$)

Hence, for each root ζ of $f(x)$ we have ζ^a is root of $f(x)$ for $a \in \mathbb{N}$ with $\gcd(a,n) = 1$.

Why? Well, suppose $a = p_1 p_2 \cdots p_k$ where $p_1, p_2, .., p_k$ are primes not dividing n thus ζ^{p_1} is root of $f(x)$, $(\zeta^{p_1})^{p_2}$ also root of $f(x)$ and so forth ζ^a is root of $f(x)$. Therefore, every primitive n^{th} root of unity is a root of $f(x) \Rightarrow f(x) = \Phi_n(x) \Rightarrow \Phi_n(x)$ is irreducible. //

Corollary (42)

The degree over $\mathbb{Q}$ of the cyclotomic field of n^{th} roots of unity is $\varphi(n)$

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

Proof: $\Phi_n(x)$ is an irreducible, monic poly. of degree $\varphi(n)$ ~~for~~ which serves as the minimal polynomial for ζ_n. Apply Th$^{\underline{m}}$ 6 of §13.1, $\dfrac{\mathbb{Q}[x]}{(\Phi_n(x))} \cong \mathbb{Q}(\zeta_n)$. //

$\boxed{\text{E2}}$ $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$ and $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_8)$ and, fun fact, $\zeta_8 + \zeta_8^7 = \sqrt{2}$ $\therefore$ $\underline{\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})}$

(we can argue this extension on RHS has deg. 4 over $\mathbb{Q}$)

Let's work out some details for $\mathbb{Q}(\zeta_n)$ for small n,

$\boxed{E3}$ $\zeta_2 = -1$ thus $\mathbb{Q}(\zeta_2) = \mathbb{Q}(-1) = \mathbb{Q}$.

$\boxed{E4}$ $\underbrace{\zeta_3 = \frac{-1+i\sqrt{3}}{2}}$ thus $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3})$

$2\zeta_3 + 1 = i\sqrt{3} \therefore i\sqrt{3} \in \mathbb{Q}(\zeta_3) \Rightarrow \mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\zeta_3)$

and $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$ hence we obtain equality since

$[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \deg(\zeta_3) = \varphi(3) = 2$.

Let's return to the discussion of the splitting field of $x^p - 2$ where p is prime.

① • If $f(x) = x^p - 2$ then $f(\alpha) = \alpha^p - 2 = 0 \longleftrightarrow \underline{\alpha^p = 2}$.

② • Let $\zeta \in \mu_p$ then $(\alpha\zeta)^p = \alpha^p\zeta^p = 2(1) = 2$

thus $\alpha\zeta$ is a root of $f(x)$ for any $\zeta \in \mu_p$

③ • For specificity's sake, let $\alpha = \sqrt[p]{2}$ then observe

the zeros of $x^p - 2$ are $\sqrt[p]{2}, \zeta_p\sqrt[p]{2}, \zeta_p^2\sqrt[p]{2}, \dots, \zeta_p^{p-1}\sqrt[p]{2}$

where $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$ is the principal p^{th} root of unity.

④ • The splitting field of $x^p - 2$ is given by $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$

where $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] \leq \underbrace{[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]}_{p \text{ since}} \underbrace{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}_{p-1 \text{ as}}$

Hence $\underline{[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] \leq p(p-1)}$ * $\quad m_{\sqrt[p]{2}, \mathbb{Q}}(x) = x^p - 2 \quad$ p prime gives $\varphi(p) = p-1$.

⑤ $\gcd(p, p-1) = 1$ hence

$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}]$ divisible by p and $p-1 \Rightarrow \underline{[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)}$.

$[\mathbb{Q}(\zeta_p)(\sqrt[p]{2}) : \mathbb{Q}(\zeta_p)] = p \quad \Rightarrow x^p - 2 \in \mathbb{Q}(\zeta_p)[x]$ is irreducible.

$[\mathbb{Q}(\sqrt[p]{2})(\zeta_p) : \mathbb{Q}(\sqrt[p]{2})] = p-1$

SPLITTING FIELD FOR $x^p - 2$

(p PRIME)

$$\begin{tikzcd} & \mathbb{Q}(\sqrt[p]{2}, \zeta_p) \arrow[dl, dash, "\boxed{p}"'] \arrow[dr, dash, "\boxed{p-1}"] & \\ \mathbb{Q}(\zeta_p) \arrow[dr, dash, "p-1"'] & & \mathbb{Q}(\sqrt[p]{2}) \arrow[dl, dash, "p"] \\ & \mathbb{Q} & \end{tikzcd}$$

$x^p - 2 \in \mathbb{Q}[x]$ remains irreducible in $\mathbb{Q}(\zeta_p)[x]$

$\Phi_p(x) = x^{p-1}+\cdots+x+1 \in \mathbb{Q}[x]$ remains irreducible in $\mathbb{Q}(\sqrt[p]{2})[x]$

$$[(\mathbb{Q}(\zeta_p))(\sqrt[p]{2}) : \mathbb{Q}(\zeta_p)] = \deg(m_{\sqrt[p]{2},\,\mathbb{Q}(\zeta_p)}(x)) = \boxed{p}$$

$$[(\mathbb{Q}(\sqrt[p]{2}))(\zeta_p) : \mathbb{Q}(\sqrt[p]{2})] = \deg(m_{\zeta_p,\,\mathbb{Q}(\sqrt[p]{2})}(x)) = \boxed{p-1}$$