AL210 - Appunti integrativi - 2

Prof. Stefania Gabelli - a.a. 2016-2017

Classi laterali e Teorema di Lagrange

Se G è un gruppo finito, il numero degli elementi di G si chiama l'*ordine* di G e si indica con $|G|$.

J.-L. Lagrange ha dimostrato che se G è un gruppo finito, l'ordine di ogni sottogruppo H di G necessariamente divide l'ordine di G. Per dimostrare questo teorema, introduciamo il concetto di *classe laterale rispetto a un sottogruppo.*

Sia G un gruppo (in notazione moltiplicativa) e sia $H \subseteq G$ un sottogruppo. Per ogni $g \in G$, definiamo i due sottoinsiemi:

$gH = \{gh\,;\ h \in H\}$ (*classe laterale sinistra di H rispetto a g*);
$Hg = \{hg\,;\ h \in H\}$ (*classe laterale destra di H rispetto a g*).

Osservazioni 1. Se il gruppo G non è commutativo, può essere $Hg \neq gH$ per qualche $g \in G$. I sottogruppi H tali che insiemisticamente $Hg = gH$ per ogni $g \in G$ si chiamano *sottogruppi normali* e verranno studiati in seguito.

Ricordiamo che una famiglia $\{X_i\}_{i\in I}$ di sottoinsiemi di un insieme X è una *partizione* di X se (1) $X = \bigcup_{i\in I} X_i$, (2) comunque scelti $i, j \in I$, risulta $X_i = X_j$ oppure $X_i \cap X_j = \emptyset$.

Proposizione 2. *L'insieme delle classi laterali sinistre (rispettivamente, destre) di H formano un* partizione *di G. Cioè:*

(1) G è unione delle classi laterali sinistre (rispettivamente, destre) di H, ovvero $G = \bigcup_{g\in G} gH = \bigcup_{g\in G} Hg$;

(2) Due classi laterali sinistre (rispettivamente, destre) di H coincidono oppure sono disgiunte, ovvero, se $g, g' \in G$, risulta $gH = g'H$ oppure $gH \cap g'H = \emptyset$ (rispettivamente, $Hg = Hg'$ oppure $Hg \cap Hg' = \emptyset$).

Dimostrazione. Per il punto 1, basta notare che ogni elemento di G appartiene alla sua classe laterale sinistra e destra di H. Infatti $e \in H$ e dunque $g = ge \in gH$ e $g = eg \in Hg$.

Per il punto 2, supponiamo $g_1H \cap g_2H \neq \emptyset$ e sia $x \in g_1H \cap g_2H$. Allora $x = g_1h_1 = g_2h_2$, con $h_1, h_2 \in H$. Ne segue che $h_2h_1^{-1} \in H$ e $g_1 = g_2(h_2h_1^{-1}) \in g_2H$. Dunque $g_1H \subseteq g_2H$. Simmetricamente, $g_2H \subseteq g_1H$, da cui $g_1H = g_2H$.

Analogamente si vede che due classi laterali destre di H coincidono oppure sono disgiunte. □

Lemma 3. *Sia H un sottogruppo di G. Allora le applicazioni*

$$gH \longrightarrow H \longrightarrow Hg\,, \quad gh \mapsto h \mapsto hg$$

sono biunivoche, per ogni $g \in G$.

In particolare, se G è finito, tutte le classi laterali di H hanno lo stesso numero di elementi di H.

Dimostrazione. In un gruppo G, la moltiplicazione sinistra $x \mapsto gx$, per un fissato elemento $g \in G$, è biiettiva per l'esistenza dell'inverso. Infatti è iniettiva: se $gx = gy$ allora $x = y$ (legge di cancellazione) ed è suriettiva: per ogni $y \in G$, risulta $y = g(g^{-1}y)$. Analogamente per la moltiplicazione destra. □

Teorema 4 (Lagrange)**.** *Sia G un gruppo finito di ordine n e sia H un suo sottogruppo. Allora l'ordine d di H divide l'ordine n di G.*

Dimostrazione. L'insieme delle classi laterali sinistre (o destre) di H è finito, supponiamo che abbia m elementi. Inoltre ogni classe laterale ha d elementi. Poiché le classi laterali formano una partizione di G, risulta $n = md$. □

Se G è un gruppo, la cardinalità dell'insieme delle classi laterali di un sottogruppo H si chiama l'*indice* di H in G e si indica con $[G : H]$. Per il Teorema di Lagrange, se G è finito, risulta $[G : H] = |G|/|H|$.

Osservazioni 5. Vedremo in seguito che se G è un gruppo finito commutativo, allora per ogni divisore d del suo ordine esiste un sottogruppo H di ordine d.

Tuttavia, se G non è commutativo questo può non essere vero. Ad esempio, si può verificare direttamente che il gruppo alterno $\mathbb{A}_4$ di grado 4, che ha ordine 12, non ha sottogruppi di ordine 6.

Gruppi ciclici

Se $g \in G$ e $n > 0$, definiamo

$$g^n = g \cdot g \cdot \cdots \cdot g,\ n \text{ volte}\ ; \quad g^0 = e\ ; \quad g^{-n} = (g^n)^{-1}.$$

Dato un sottoinsieme S di G, si verifica subito che il sottogruppo di G generato da S, ovvero il più piccolo sottogruppo di G contenente S, è

$$H := \langle S \rangle = \{g_1^{z_1} \dots g_n^{z_n}\ ; g_i \in S, z_i \in \mathbb{Z}, i = 1 \dots, n\}.$$

Se $S = \{g\}$ è formato da un solo elemento, il sottogruppo di G generato da S si indica con $\langle g \rangle$. Questo sottogruppo

$$\langle g \rangle = \{g^z, z \in \mathbb{Z}\}$$

si chiama il *sottogruppo ciclico* di G generato da g. Il gruppo G si dice *ciclico* se esiste $g \in G$ tale che $G = \langle g \rangle$. I (sotto)gruppi ciclici sono commutativi.

Esempi 6. Esempi di gruppi ciclici sono: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, il gruppo delle radici n-sime dell'unità ($n \geq 2$), il gruppo delle rotazioni di un poligono regolare.

Se $g \in G$, l'ordine del gruppo $\langle g \rangle$ si chiama anche l'*ordine* (o *periodo*) di g.

Proposizione 7. *Siano $(G, \cdot)$ un gruppo e $g \in G$:*

(a) g ha ordine finito se e soltanto se esiste $m > 0$ tale che $g^m = e$. In tal caso, se n è il minimo di tali interi positivi, l'ordine di g è uguale a n e $\langle g \rangle = \{g, g^2, \ldots, g^{n-1}, g^n = e\}$.

(b) Se g ha ordine n e $a, b \in \mathbb{Z}$, si ha $g^a = g^b$ se e soltanto se $a \equiv b \mod n$. In particolare, $g^a = e$ se e soltanto se n divide a.

(c) Se g ha ordine n e $z \in \mathbb{Z}$, allora $\langle g^z \rangle = \langle g^d \rangle$, dove $d = \mathrm{MCD}(z, n)$. Quindi g^z e g^d hanno stesso ordine, uguale a $\frac{n}{d}$.

(d) g e g^{-1} hanno lo stesso ordine.

Dimostrazione. (a) Sia $g \neq e$. Supponiamo che esista $m > 0$ tale che $g^m = e$ e sia n il minimo di tali interi positivi. Sicuramente gli n elementi $g, g^2, \ldots, g^{n-1}, g^n = e$ sono tutti distinti. D'altra parte, scrivendo $z = nq + r$, con $n > r \geq 0$, si ha $g^z = g^r$. Perciò $\langle g \rangle = \{g, g^2, \ldots, g^{n-1}, g^n = e\}$. In particolare g ha ordine n.

Viceversa, se il sottogruppo $\langle g \rangle$ è finito, si ha $g^a = g^b$, per qualche $a, b \in \mathbb{Z}$. In questo caso, risulta $g^{a-b} = e = g^{b-a}$ e dunque l'insieme degli interi positivi m tali che $g^m = e$ è non vuoto.

(b) Scrivendo $a - b = nq + r$, con $n > r \geq 0$, si ha $g^{a-b} = g^r$. Dunque, per la miimalità di n, $g^{a-b} = e$ se e soltanto se $r = 0$, cioè n divide $a - b$.

(c) Se $z = dt$, allora $g^z = (g^d)^t \in \langle g^d \rangle$. Inoltre scrivendo $d = an + bz$ (Identità di Bezout), si ottiene $g^d = g^{an} g^{bz} = (g^z)^b \in \langle g^z \rangle$. Quindi $\langle g^z \rangle = \langle g^d \rangle$.

Basta ora osservare che gli elementi $g^d, g^{2d}, \ldots, g^{\frac{n}{d} d} = e$ sono tutti distinti per il punto (b).

(d) segue da (c). □

Corollario 8. *Un elemento $g \in G$ ha ordine infinito se e soltanto se $g^n \neq e$ per ogni $n > 0$*

Dimostrazione. Per la Proposizione 7(a). □

Osservazioni 9. (1) Se G è un gruppo finito di ordine n, l'ordine di ogni elemento g è finito ed è uguale ad un divisore positivo di n (Teorema di Lagrange). Quindi $g^n = e$, per ogni $g \in G$.

(2) G è ciclico di ordine n se e soltanto se ha un elemento di ordine n. Inoltre se G è ciclico esso è generato da ogni elemento di ordine n.

(3) Un elemento g ha ordine 1 se e soltanto se $g = e$.

(4) Se G è un gruppo finito di ordine n e d è un divisore positivo di n, indichiamo con G_d l'insieme degli elementi di ordine d. Allora la famiglia $\{G_d; G_d \neq \emptyset\}$ è una partizione di G; infatti l'ordine di un elemento è univocamente determinato. In altre parole G è l'unione disgiunta dei suoi sottoinsiemi formati dagli elementi di ordine fissato.

Il risultato seguente implica che il numero dei generatori di un gruppo ciclico di ordine n, cioè il numero degli elementi di ordine n, è uguale al valore $\varphi(n)$ della Funzione di Eulero.

Proposizione 10. *Sia $G = \langle g \rangle$ un gruppo ciclico e $a \in \mathbb{Z}$.*

(a) Se G è finito di ordine n, g^a genera G se e soltanto se $d := \mathrm{MCD}(a, n) = 1$.

(b) Se G è infinito, g^a genera G se e soltanto se $a = \pm 1$.

Dimostrazione. (a) g^a ha ordine $n = \frac{n}{d}$ se e soltanto se $d = 1$ (Proposizione 7(c)).

(b) Se $G = \langle g^a \rangle$, allora $g = (g^a)^m = g^{am}$, per qualche $m \in \mathbb{Z}$. Allora $g^{1-am} = e$ e $1 - am = 0$, ovvero $am = 1$ (Proposizione 7(b)). Ne segue che $a = \pm 1$. □

Teorema 11 (Piccolo Teorema di Fermat)**.** *Sia $n \geq 2$. Se $a \in \mathbb{Z}$ è coprimo con n, allora $a^{\varphi(n)} \equiv 1 \mod n$.*

Dimostrazione. Il gruppo moltiplicativo delle unità di $\mathbb{Z}_n$ è costituito dalle classi degli interi coprimi con n ed ha perciò ordine $\varphi(n)$. Allora, se $a \in \mathbb{Z}$ è coprimo con n, $\overline{a}^{\varphi(n)} = \overline{1}$ (Osservazione 1). □

Corollario 12. *Sia $p \geq 2$ un numero primo. Se $a \in \mathbb{Z}$ non è diviso da p, allora $a^p \equiv a \mod p$.*

Sottogruppi di gruppi ciclici

Ogni gruppo G ha sottogruppi ciclici; infatti ogni $g \in G$ genera un sottogruppo ciclico di G. Come sappiamo dagli esempi, in generale questi non sono tutti i sottogruppi di G, tuttavia lo sono se G è esso stesso ciclico.

Proposizione 13. *Ogni sottogruppo di un gruppo ciclico è ciclico. Precisamente, se $G = \langle g \rangle$ e H è un sottogruppo di G, risulta $H = \langle g^m \rangle$, dove m è il minimo intero positivo tale che $g^m \in H$.*

Dimostrazione. Sia $G = \langle g \rangle$ un gruppo ciclico e sia $H \neq \{e\}$ un suo sottogruppo. Se $g^z \in H$, anche $g^{-z} \in H$, quindi in H ci sono potenze di g con esponente positivo. Sia $m > 0$ il minimo intero positivo tale che $g^m \in H$. Chiaramente $\langle g^m \rangle \subseteq H$; mostriamo che $H = \langle g^m \rangle$. Se $h = g^a \in H$, scrivendo $a = mq + r$, con $n > r \geq 0$, otteniamo che $g^r = g^{a-mq} = h(g^m)^{-q} \in H$. Per la minimalità di m, deve essere allora $r = 0$ e $h = (g^m)^q \in \langle g^m \rangle$. □

Corollario 14. *Tutti e soli i sottogruppi di $\mathbb{Z}$ sono i sottogruppi $n\mathbb{Z}$, con $n \geq 0$.*

Proposizione 15. *Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n. Allora, G ha uno e un solo sottogruppo di ordine D, per ogni divisore D di n. Questo è il sottogruppo ciclico $\langle g^{\frac{n}{D}} \rangle$.*

Dimostrazione. Per ogni D, il sottogruppo $\langle g^{\frac{n}{D}} \rangle$ ha ordine D (Proposizione 7(c)). Sia $H \subseteq G$ un sottogruppo di ordine D. Per la Proposizione 13, H è ciclico, diciamo $H = \langle g^m \rangle$. Se $d = \mathrm{MCD}(m, n)$, ancora per la Proposizione 7(c), risulta $H = \langle g^d \rangle$ e $D = \frac{n}{d}$. Allora $d = \frac{n}{D}$ e $H = \langle g^{\frac{n}{D}} \rangle$. □

Corollario 16. *Sia G un gruppo finito di ordine $n \geq 2$. Sono equivalenti:*
(i) G non ha sottogruppi propri;
(ii) G è ciclico di ordine primo;
(iii) G ha ordine primo;.

Dimostrazione. (i) $\Rightarrow$ (ii). Se $g \in G$, $g \neq e$, risulta $G = \langle g \rangle$. Quindi G è ciclico. Inoltre il suo ordine è primo, altrimenti avrebbe sottogruppi propri (Proposizione 15).

(ii) $\Rightarrow$ (iii) è ovvio.

(iii) $\Rightarrow$ (i). Se G ha ordine primo p, ogni elemento di G diverso da e ha ordine p (Osservazione 1). Quindi genera tutto G. □

Corollario 17. *Sia G ciclico di ordine n. Per ogni divisore positivo d di n, G ha esattamente $\varphi(d)$ elementi di ordine d (dove $\varphi(d)$ è la Funzione di Eulero di d).*

Dimostrazione. Gli elementi di ordine d sono i generatori dell'unico gruppo ciclico di ordine d di G. □

Diamo ora una utile formula.

Proposizione 18. *Se $n \geq 1$, risulta*

$$n = \sum_{n \geq d \geq 1, d|n} \varphi(d),$$

dove $\varphi(d)$ è la Funzione di Eulero di d.

Dimostrazione. Sia G ciclico di ordine n. Per ogni divisore positivo d di n, l'isieme G_d degli elementi di ordine d è non vuoto ed ha $\varphi(d)$ elementi (Corollario 17). Poiché G è unione disgiunta dei suoi sottoinsiemi G_d (Osservazione 4), la formula segue. □

Notiamo che se tutti i sottogruppi propri di un gruppo G sono ciclici (quindi commutativi), non è detto che G sia commutativo. Ad esempio si può considerare il gruppo $\mathbf{S_3}$. Però vale la seguente inversa della Proposizione 15.

Proposizione 19. *Sia G un gruppo finito di ordine n. Se G ha al più un sottogruppo di ordine d, per ogni divisore positivo d di n, allora G è ciclico (e quindi ha uno e un solo sottogruppo, necessariamente ciclico, di ordine d).*

Dimostrazione. Sia G_d l'insieme degli elementi di ordine d, per ogni divisore positivo d di n, e supponiamo che G_d abbia n_d elementi (eventualmente $n_d = 0$). Poiché G è unione disgiunta di tutti i suoi sottoinsiemi G_d non vuoti (Osservazione 4), si ha $n = \sum n_d$.

Osserviamo che $n_d \neq 0$ se e soltanto se esistono elementi, e quindi sottogruppi ciclici, di ordine d. Ne segue che, se per ogni d esiste al più un sottogruppo di ordine d, quando $n_d \neq 0$ c'è esattamente un solo sottogruppo ciclico di ordine d. Quindi $n_d = \varphi(d)$. Usando la Proposizione 18, vediamo che $n = \sum n_d \leq \sum \varphi(d) = n$.

Allora non puó mai essere $n_d = 0$; cioè, per ogni d esistono elementi di ordine d. In particolare esistono elementi di ordine n e quindi G è ciclico. □

Corollario 20. *Sia K un campo. Ogni sottogruppo finito del gruppo moltiplicativo di K è ciclico.*

Dimostrazione. Sia G un sottogruppo di ordine n di $(K, \cdot)$ e sia d un divisore positivo di n. Se H è un sottogruppo di G di ordine d, si ha $h^d = 1$, per ogni $h \in H$. Dunque h è radice del polinomio $X^d - 1$ a coefficienti in K. Poiché le radici di questo polinomio sono al più d, G ha al più un sottogruppo di ordine d. Possiamo allora applicare la proposizione precedente. □

Esempi 21. (1) Se p è primo, il gruppo delle unità di $\mathbb{Z}_p$ è ciclico di ordine $p - 1$.

(2) Per ogni $n \geq 2$, il gruppo delle radici complesse n-sime dell'unitá è ciclico di ordine n. Le radici di ordine n sono le radici primitive n-sime.

Il gruppo ciclico delle radici complesse n-sime dell'unità

Le radici complesse del polinomio $f(X) := X^n - z \in \mathbb{C}[X]$, per $n \geq 1$, si chiamano le *radici complesse n-sime* di z. Poiché, per $n \geq 2$, il polinomio derivato $f'(X) = nX^{n-1}$ ha come unica radice lo zero, se $z \neq 0$, i polinomi $f(X)$ e $f'(X)$ non hanno radici in comune; quindi le radici n-sime di z sono tutte distinte. Per determinarle, si possono usare le *Formule di De Moivre* per la moltiplicazione dei numeri complessi in forma trigonometrica. Se

$$z_1 := \rho_1(\cos(\theta_1) + \imath \sin(\theta_1)); \quad z_2 := \rho_2(\cos(\theta_2) + \imath \sin(\theta_2))$$

con ρ_1, ρ_2 numeri reali positivi, allora usando le proprietà delle funzioni trigonometriche risulta

$$z_1 z_2 = \rho_1\rho_2(\cos(\theta_1 + \theta_2) + \imath \sin(\theta_1 + \theta_2)).$$

Sia dunque $z := \rho(\cos(\theta) + \imath \sin(\theta))$, $\rho > 0$. Se $\zeta := \sigma(\cos(\varphi) + \imath \sin(\varphi))$ è una radice n-sima di z, deve risultare:

$$\sigma^n(\cos(n\varphi) + \imath \sin(n\varphi)) = \rho(\cos(\theta) + \imath \sin(\theta)),$$

da cui $\sigma^n = \rho$ e $n\varphi = \theta + 2k\pi$, $k \in \mathbb{Z}$, ovvero

$$\sigma = \sqrt[n]{\rho}; \quad \varphi = \frac{\theta + 2k\pi}{n}.$$

Notiamo ora che, se $k \in \mathbb{Z}$ e $k = nq + r$ con $0 \leq r < n$, risulta

$$\frac{\theta + 2k\pi}{n} = \frac{\theta + 2r\pi}{n} + 2q\pi$$

e dunque le funzioni trigonometriche di $\dfrac{\theta+2k\pi}{n}$ e $\dfrac{\theta+2r\pi}{n}$ sono le stesse. Ne segue che le radici complesse n-sime di z si ottengono tutte per $k=0,1,\dots,n-1$ e sono precisamente i numeri complessi

$$\zeta_k := \sqrt[n]{\rho}\left(\cos\left(\frac{\theta+2k\pi}{n}\right)+\imath\sin\left(\frac{\theta+2k\pi}{n}\right)\right).$$

Per $z := 1 = \cos(2\pi)+\imath\sin(2\pi)$, le formule precedenti forniscono le *radici complesse n-sime dell'unità*, che sono i numeri:

$$\zeta_k := \cos\left(\frac{2k\pi}{n}\right)+\imath\sin\left(\frac{2k\pi}{n}\right),$$

per $k=1,\dots,n$. Poiché, per le formule di De Moivre, risulta $\zeta_1^k=\zeta_k$, posto

$$\xi := \zeta_1 := \cos\left(\frac{2\pi}{n}\right)+\imath\sin\left(\frac{2\pi}{n}\right),$$

possiamo scrivere le radici complesse n-sime dell'unità come

$$\zeta_1 =: \xi\,,\quad \zeta_2=\xi^2\,,\quad \dots,\quad \zeta_{n-1}=\xi^{n-1}\,,\quad \zeta_n=\xi^n=1.$$

Quindi tali radici formano un gruppo moltiplicativo ciclico di ordine n. Notiamo che, se $\zeta\in\mathbb{C}$ ha modulo uguale a 1, indicando con $\overline{\zeta}$ il coniugato di ζ, si ha $\zeta\overline{\zeta}=1$, da cui $\zeta^{-1}=\overline{\zeta}$. Quindi le radici ξ^k e ξ^{n-k} sono numeri complessi coniugati.

I generatori del gruppo ciclico delle radici complesse n-sime dell'unità sono le radici $\xi^k=\zeta_k$ con $\mathrm{MCD}(k,n)=1$ (Proposizione 7(a)). Questi numeri complessi si chiamano le *radici n-sime primitive* dell'unità e sono le radici n-sime che non sono anche radici m-sime per qualche $m<n$. Tale terminologia fu introdotta da Eulero mentre l'esistenza di radici primitive, ovvero il fatto che il gruppo delle radici n-sime è ciclico, fu dimostrata da Gauss nel suo trattato *Disquisitiones Arithmeticae*, del 1801.

Il numero delle radici primitive n-sime dell'unità è dato allora dal valore $\varphi(n)$ della funzione di Eulero.

Notiamo che, per $n\geq 3$, le radici complesse n-sime dell'unità si rappresentano nel piano di Gauss come i vertici di un poligono regolare di n lati che ha un vertice in 1. Inoltre, se m divide n, le radici m-sime si rappresentano come i vertici di un poligono regolare di m lati che ha ancora un vertice in 1 ed è inscritto nel primo.

Osserviamo infine che, per le formule di De Moivre, tutte le radici n-sime di un numero complesso z si possono scrivere come il prodotto di una qualsiasi radice n-sima ζ di z per tutte le radici n-sime dell'unità, e quindi esse sono esattamente i numeri complessi

$$\zeta\xi\,,\quad \zeta\xi^2\,,\quad \dots,\quad \zeta\xi^{n-1}\,,\quad \zeta\xi^n=\zeta\,,$$

dove ξ è una radice primitiva n-sima dell'unità. Per $n\geq 3$, questi numeri complessi si rappresentano nel piano di Gauss come i vertici di un poligono regolare di n lati con centro nell'origine e un vertice in ζ.

Esempi 22. **(1)** Le radici complesse terze dell'unità sono i numeri complessi

$$\begin{aligned}\xi &:= \cos\left(\frac{2\pi}{3}\right) + \imath \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \imath\frac{\sqrt{3}}{2}\,;\\ \xi^2 &= \cos\left(\frac{4\pi}{3}\right) + \imath \sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \imath\frac{\sqrt{3}}{2}\,;\\ \xi^3 &= \cos(2\pi) + \imath \sin(2\pi) = 1.\end{aligned}$$

Invece le radici quarte sono

$$\xi := \cos\left(\frac{\pi}{2}\right) + \imath \sin\left(\frac{\pi}{2}\right) = \imath\,; \quad \imath^2 = -1\,; \quad \imath^3\,; \quad \imath^4 = 1\,.$$

(2) Le radici complesse n-sime di $-1 = \cos(\pi) + \imath\sin(\pi)$ sono i numeri:

$$\begin{aligned}\zeta_k &:= \cos\left(\frac{\pi + 2k\pi}{n}\right) + \imath \sin\left(\frac{\pi + 2k\pi}{n}\right)\\ &= \cos\left(\frac{(2k+1)\pi}{n}\right) + \imath \sin\left(\frac{(2k+1)\pi}{n}\right),\end{aligned}$$

per $k = 0, \ldots, n$.

Notiamo che, essendo $(X^{2n} - 1) = (X^n + 1)(X^n - 1)$, se ξ è una radice primitiva $2n$-sima dell'unità, ad esempio $\xi := \cos\left(\frac{\pi}{n}\right) + \imath \sin\left(\frac{\pi}{n}\right)$, le radici n-sime di 1 sono le potenze pari di ξ, mentre le radici n-sime di -1 sono le potenze dispari di ξ.

(3) La forma trigonometrica di un numero reale r positivo è

$$r = r \cdot 1 = r(\cos(2\pi) + \imath \sin(2\pi)),$$

mentre ogni numero reale r negativo si scrive in forma trigonometrica come

$$r = |r|(-1) = |r|(\cos(\pi) + \imath \sin(\pi)).$$

Le radici complesse n-sime di r si ottengono allora moltiplicando per $\sqrt[n]{|r|}$ le radici complesse n-sime di 1 o di -1, a seconda che r sia positivo o negativo.

il polinomio monico su $\mathbb{C}$ che ha per radici tutte e sole le radici primitive n-sime dell'unità si chiama l'*n-simo polinomio ciclotomico* e si indica con $\Phi_n(X)$. Dunque risulta

$$\Phi_n(X) := \prod_{\mathrm{MCD}(n,k)=1} (X - \xi^k),$$

in particolare $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$.

Se $n = p$ è un numero primo tutte le radici p-esime diverse da 1 hanno ordine p e perciò sono tutte primitive. Ne segue che

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$$

e

$$X^p - 1 = \Phi_1(X)\Phi_p(X).$$

In generale, indicando con R_d le radici primitive d-sime dell'unità, abbiamo che gli insiemi R_d, al variare dei divisori positivi d di n, formano una partizione del gruppo delle radici n-sime (Osservazione 4). Allora si ha che

$$X^n - 1 = \prod_{0 \le k \le n-1} (X - \xi^k) = \prod_{d>0, d|n} \Phi_d(X).$$

Questa formula permette di determinare $\Phi_n(X)$ per ricorsione. Infatti risulta

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{n>d>0, d|n} \Phi_d(X)}.$$

Ad esempio

$$\begin{aligned}
&\Phi_1(X) = X - 1;\\
&\Phi_2(X) = \frac{X^2-1}{\Phi_1(X)} = \frac{X^2-1}{X-1} = X + 1;\\
&\Phi_3(X) = \frac{X^3-1}{\Phi_1(X)} = \frac{X^3-1}{X-1} = X^2 + X + 1;\\
&\Phi_4(X) = \frac{X^4-1}{\Phi_1(X)\Phi_2(X)} = \frac{X^4-1}{(X-1)(X+1)} = X^2 + 1;\\
&\Phi_6(X) = \frac{X^6-1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = \frac{X^6-1}{(X^2-1)(X^2+X+1)} = X^2 - X + 1;\\
&\Phi_8(X) = \frac{X^8-1}{\Phi_1(X)\Phi_2(X)\Phi_4(X)} = \frac{X^8-1}{(X^2-1)(X^2+1)} = X^4 + 1;
\end{aligned}$$

e così via.

Il prossimo risultato è di importanza fondamentale, ma verrà dimostrato in seguito.

Proposizione 23. *Per ogni $n \ge 1$, l'n-simo polinomio ciclotomico $\Phi_n(X)$ ha coefficienti interi ed è irriducibile su $\mathbb{Q}$ (ed essendo monico, anche su $\mathbb{Z}$)*

Una prima dimostrazione dell'irriducibilità del p-esimo polinomio ciclcotomico su $\mathbb{Q}$, con p primo, è stata data da F. Gauss (*Disquisitiones Arithmeticae*, 1801). Questa dimostrazione è stata successivamente semplificata da L. Kronecker, nel 1845, ed una dimostrazione diversa è stata poi data da F. G. Eisenstein nel 1850. Infine, la prova dell'irriducibilità di $\Phi_n(X)$ su $\mathbb{Q}$, per ogni intero $n \ge 1$, è stata ottenuta da R. Dedekind nel 1857.