Indice

INDICE—*Continued*

Elenco delle figure

Introduzione

I quasianelli sono una struttura algebrica abbastanza recente, la cui più lontana origine si può far risalire agli inizi del secolo XX quando si impose nella comunità matematica, soprattutto grazie all'opera ed agli scritti di Hilbert, la tendenza a costruire *teorie assiomatiche,* non più fondate su verità elementari in sè evidenti, ma su una lista di assiomi cui si chiede la *consistenza* e l'*indipendenza.* In particolare, nel campo delle strutture algebriche, ci si cominciò a interrogare sull'indipendenza degli assiomi di campo o di spazio vettoriale. Si provò così che la commutatività della somma segue dagli altri assiomi di campo (Hankel, 1867), e che nel caso finito ciò è vero anche per la commutatività della moltiplicazione (Wedderburn, 1905). Quasi contemporaneamente, Dickson dimostrò che la commutatività della somma e una delle due distributive non possono essere dimostrate a partire dagli altri assiomi di campo (nemmeno nel caso finito) costruendo quello che noi oggi chiamiamo un quasicorpo (finito): $[\mathbb{Z}_3, +, \otimes]$, dove $\forall (a,b),(c,d) \in \mathbb{Z}_3$, convenendo di scegliere per a, b, c e d rappresentanti in $\{-1, 0, 1\}$,

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) \\ (a,b) \otimes (c,d) &= \big(ac - (-1)^{ab}bd, bc + (-1)^{ab}ad\big) \end{aligned}$$

Dickson stesso, successivamente, si pose il problema di classificare i quasicorpi, almeno nel caso finito, dimostrando che essi hanno ordine potenze di primi e che la commutatività della somma segue dagli altri assiomi; egli determinò poi un metodo di costruzione di quasicorpi a partire dal gruppo additivo di un campo K, definendo come moltiplicazione

$$a \circ b = a \cdot \rho_a(b)$$

dove $\cdot$ è la moltiplicazione in K e $a \to \rho_a$ è una funzione da K in $Aut(K^+)$ che soddisfi opportune propietà. L'idea di definire in questo modo una moltiplicazione è molto fruttuosa, ed è alla base della costruzione di un quasianello planare a partire da un coppia di Ferrero tramite la cosiddetta Fabbrica di Ferrero. Il problema della classificazione completa di *tutti* i quasicorpi fu poi risolto da Zassenhaus nel 1936, dimostrando che, eccetto sette quasicorpi eccezionali che egli descrisse, tutti i quasicorpi finiti possono essere ottenuti con il metodo di costruzione di Dickson. Il primo ad occuparsi dei quasianelli fu, partendo da lavoro di Zassenhaus sui quasicorpi, Wieland negli anni '30, con lo scopo di ottenere strumenti per la teoria dei gruppi, ma fu solo negli anni '50 che cominciò il loro studio sistematico, ad opera principalmente di Blackett, Deskins, Neumann e Frölich.

Più lontana origine ha la teoria dei grafi, che si può far risalire allo scritto di Eulero del 1735 sui sette ponti di Köninsberg: la sua dimostrazione che non esisteva alcun percorso che attraversasse una ed una sola volta tutti i ponti è sostanzialmente

il primo teorema di teoria dei grafi; tale problema si generalizza nel trovare condizioni necessarie e\o sufficienti affinchè un grafo ammetta un ciclo che attraversi tutti i lati una ed una sola volta (ciclo euleriano). Nella seconda metà dell'Ottocento Hamilton considerò una variante del problema di Eulero, che consiste nel considerare cicli che passino per ciascun *vertice* una ed una sola volta (cicli hamiltoniani); il problema di Hamilton risultò di più difficile soluzione e tuttora non si conoscono condizioni necessarie e sufficienti per un grafo (in termini di numero e grado dei suoi vertici) affinchè questo ammetta un ciclo hamiltoniano. Un'altra classe interessante di grafi è costituita dai grafi *planari*, cioè tali che possano essere disegnati su un piano senza che due lati distinti si incontrino, eccetto al più nei vertici; il problema di classificare i grafi planari fu generalizzato nel problema dell'embedding, che consiste nel determinare quali grafi possano essere embedded in una data superficie. E' evidente dai rapidi accenni fin qui fatti che la teoria dei grafi ha importanti collegamenti con molte altre branche della matematica (topologia, combinatorica, geometria); non deve sorprendere quindi se essa può essere, ed è, fruttuosamente utilizzata nello studio di strutture eminentemente algebriche quali i quasianelli, come ci proponiamo di dimostrare in questa tesi.

In particolare, inizieremo con l'introdurre le principali e basilari nozioni della teoria dei quasianelli (capitolo 1); passeremo poi a studiare in dettaglio i quasianelli planari, dimostrando per essi il teorema di struttura e descrivendo la costruzione nota come Fabbrica di Ferrero (capitolo 2). Introdurremo poi enti geometrico-combinatorici molto generali quali strutture d'incidenza e BIBD e vedremo come ai quasianelli planari si possano associare strutture di questo tipo, e come dallo studio di queste sorga il concetto di circolarità (capitolo 3). Passeremo poi a descrivere una modalità di costruzione di quasianelli planari da uno spazio vettoriale e dimostreremo un criterio di circolarità per tali quasianelli. Avremo poi bisogno di richiamare le definizioni di base della teoria dei grafi, per poter poi definire e studiare grafi associati a cerchi e sistemi di cerchi in un quasianello planare circolare qualunque (capitolo 4) e dimostrare teoremi combinatorici di conteggio di tali grafi nel caso particolare di quasianelli field-generated a partire dagli interi modulo p (capitolo 5), che risulteranno valere senza modifiche per sistemi di cerchi discreti nell'usuale piano complesso (capitolo 6). Riportiamo in appendice programmi MATLAB che implementano alcuni dei teoremi e delle costruzioni descritte, e che plottano i grafi con cui corrediamo l'esposizione.

Parte I

Quasianelli e quasianelli planari

Capitolo 1

QUASIANELLI

Iniziamo con la definizione di quasi-anello.

Definizione 1.1. *Un **quasianello sinistro** è una struttura* $[N, +, \cdot]$ *dove*

1. $[N, +]$ *è un gruppo*
2. $[N, \cdot]$ *è un semigruppo*
3. $\forall x, y, z \in N \; x \cdot (y + z) = x \cdot y + x \cdot z$ *(distributiva sinistra del prodotto rispetto alla somma)*

Indichiamo con 0 l'elemento neutro di $[N, +]$. Se $[N, \cdot]$ è un semigruppo con unità N si dice *quasianello con unità* e si indica con 1 l'unità di $[N, \cdot]$. Se $[N, +]$ è un gruppo abeliano il quasianello N si dice *abeliano*. Se al posto della proprietà 3) vale la

$3')$ $\forall x, y, z \in N \; (y + z) \cdot x = y \cdot x + z \cdot x$
(distributiva destra del prodotto rispetto alla somma)
si parla di *quasianello destro*. Se valgono contemporaneamente la 3) e la $3')$ il quasianello si dice *distributivo*. Nel seguito quando parleremo di quasianello (senz'altro) intenderemo quasianello sinistro. Sempre nel seguito indicheremo con N^+ il gruppo additivo $[N, +]$ e con $N^{\cdot}$ il semigruppo moltiplicativo $[N, \cdot]$ di un quasianello N. Osserviamo che un quasianello abeliano distributivo è un anello. L'assenza, nei quasianelli, della proprietà commutativa della somma e di una delle due distributive è origine di importanti differenze tra la teoria dei quasianelli e quella degli anelli. In particolare riguardo al comportamento dell'elemento neutro 0 di N^+: risulta infatti, $\forall x \in Nx$, $0 = x(0 + 0) = x0 + x0$ e dunque $x0 = 0$ ma in generale $0x$ non è zero. Poniamo

$$\begin{aligned} N_0 &= \{x \in N \mid \quad 0x = 0\} \\ N_c &= \{x \in N \mid \quad 0x = x\} \end{aligned}$$

N_0 si dice *parte simmetrica* di N, N_c *parte costante* di N. Si ha $N_c = \{x \in N \mid \forall y \in N \; yx = x\}$, infatti $\forall y \in N \; \forall x \in N_c \; yx = y(0x) = (y0)x = 0x = x$. Un quasianello si dice zerosimmetrico se $N = N_0$, costante se $N = N_c$. I quasianelli N tali che $[N \backslash \{0\}, \cdot]$ è un gruppo si dicono *quasicorpi*.

Fra gli esempi più significativi di quasianello presentiamo quello delle funzioni di un gruppo in sé e quello delle trasformazioni affini di un gruppo abeliano. Questi esempi mostrano l'interesse algebrico e geometrico delle strutture che vogliamo studiare.

Esempio 1.2. *Sia $[G,+]$ un gruppo e $M(G) = G^G = \{$funzioni da G in $G\}$. Si prova facilmente che $[M(G),+,\circ]$ è un quasianello destro, dove $+$ è la somma puntuale di funzioni e $\circ$ la composizione. Osserviamo che lo zero di $M(G)$ è la funzione costante uguale a zero, che indicheremo con* ***0,*** *che*

$$\begin{aligned} M(G)_0 &= \{f : G \to G \mid \quad f(0) = 0\} \\ M(G)_c &= \{f : G \to G \mid \quad f \text{ è costante}\} \end{aligned}$$

e che la funzione identica, che nel seguito indicheremo con ι, è unità sinistra per $M(G)$.

Esempio 1.3. *Sia $[G,+]$ un gruppo abeliano. Diciamo trasformazione affine di G una funzione $\varphi : G \to G$ tale che, $\forall g \in G$, $\varphi(g) = \alpha g + b$, con $\alpha \in End(G)$ e $b \in G$. Indichiamo con $M_{aff}(G)$ l'insieme delle trasformazioni affini di G. $[M_{aff}(G),+,\circ]$ è un quasianello, sottoquasianello di $M(G)$. Infatti $\forall \varphi, \psi \in M_{aff}(G)$ se $\forall g \in G$ $\varphi(g) = \alpha g + b$ e $\psi(g) = \beta g + c$ con $b, c \in G$ e $\alpha, \beta \in End(G)$, si ha $\forall g \in G$, poichè G è abeliano,*

$$(\varphi - \psi)(g) = (\alpha g + b) - (\beta g + c) = \alpha g - \beta g + b - c = (\alpha - \beta)g + (b - c)$$

con $\alpha - \beta \in End(G)$, $b - c \in G$, dunque $\psi - \varphi \in M_{aff}(G)$ e $M_{aff}(G)$ è un sottogruppo di $M(G)^+$; inoltre $\forall g \in G$

$$(\psi \circ \varphi)(g) = \psi(\varphi(g)) = \psi(\alpha g + b) = \beta(\alpha g + b) + c = \beta\alpha g + \beta b + c$$

con $\beta\alpha \in End(G)$ e $\beta b + c \in G$, dunque $\psi \circ \varphi \in M_{aff}(G)$ e $M_{aff}(G)$ è un sottosemigruppo di $M(G)^\circ$.

1.1 Sottostrutture ed omomorfismi

Le definizioni e le prime proprietà di sottoquasianelli e di omomorfismi fra quasianelli sono del tutto analoghe a quelle ben note sugli anelli. Tuttavia nei quasianelli hanno interesse sottostrutture particolari. Precisamente, un sottoinsieme A di un quasianello N si dice N-**sottoinsieme destro** (rispett. **sinistro**) di N se $AN \subset A$ (rispett. $NA \subset A$). Diremo **bilatero** un N-sottoinsieme contemporaneamente destro e sinistro. Se inoltre A è un sottogruppo di N^+ parleremo di N-**sottogruppo sinistro** (rispett. **destro/bilatero**) e di N-sottogruppo **normale** se A è un sottogruppo normale di N^+. Ancora un ideale I di un quasianello N sarà nucleo di un qualche omomorfismo da N ad un qualche quasianello N'. Così un sottoinsieme I di N è un **ideale** di N (scriveremo $I \lhd N$) se

1. I è un N-sottogruppo normale di N
2. $\forall x, y \in N$ $\forall i \in I$ si ha $(y + i)x - yx \in I$

La precedente definizione è motivata dal seguente teorema, di cui omettiamo la dimostrazione classica.

Teorema 1.4. *Sia I un ideale del quasianello N; la relazione su N definita ponendo $\forall x, y \in N$, $x \equiv_I y$ se e solo se $y - x \in I$ è una congruenza del quasianello N.*

Questo consente di considerare come di consueto il quoziente $\frac{N}{\equiv_I}$ e questo è un quasianello tale che la proiezione di N su $\frac{N}{\equiv_I}$ è un epimorfismo.

1.2 Funzioni di Clay e semigruppo di Clay

Molto importante per il seguito è la seguente

Definizione 1.5. *Sia N un quasianello; diciamo **funzione di Clay** associata ad $a \in N$ la traslazione sinistra di $N^{\cdot}$, cioè la funzione $\varphi_a : N \to N$ definita da $\varphi_a(x) = ax$.*

Osserviamo che in un quasianello N le traslazioni sinistre di $N^{\cdot}$ sono endomorfismi di N^+. Possiamo considerare pertanto la funzione $\varphi : N \to End(N^+)$ definita da $\varphi(a) = \varphi_a$, $\forall a \in N$. Se consideriamo $End(N^+)$ come semigruppo rispetto alla composizione, φ risulta un omomorfismo di semigruppi. Infatti $\forall a, b \in N$, $\forall x \in N$ $\varphi(ab)(x) = \varphi_{ab}(x) = (ab)(x) = a(bx) = \varphi_a(bx) = \varphi_a(\varphi_b(x)) = (\varphi_a \circ \varphi_b)(x)$ e dunque $\varphi(ab) = \varphi(a) \circ \varphi(b)$. Questo consente di dare la seguente

Definizione 1.6. *Sia φ la funzione di Clay di un quasianello N; diciamo **semigruppo di Clay** di N (che indicheremo con $\tilde{\Phi}$) il sottosemigruppo $Im\varphi$ di $End(N^+)$. Se $\Phi = \tilde{\Phi} \backslash \{0\}$ è un gruppo parleremo di gruppo di Clay Φ di N.*

E' immediato constatare che $\forall a \in N$ $\mathrm{Im}\varphi_a = aN$ è un N-sottoinsieme destro di N. Osserviamo che per la proprietà associativa del prodotto si ha che $\forall a, b \in N$ $\varphi_a \varphi_b = \varphi_{ab}$. Infatti $\forall x \in N$ $\varphi_a \varphi_b x = \varphi_a(bx) = a(bx) = (ab)x = \varphi_{ab}x$. E' degno di nota il fatto che un quasianello è univocamente determinato dal suo gruppo additivo e dalla sua funzione di Clay, cioè

Teorema 1.7. *Siano $[N, +]$ un gruppo e $\varphi : N \to End(N)$ una funzione tale che $Im\varphi$ sia un sottosemigruppo di $[End(N), +, \circ]$ e $\forall a, b \in N$ $\varphi(a) \circ \varphi(b) = \varphi(\varphi(a)(b))$. Se poniamo, $\forall a, b \in N$ $a \cdot b = \varphi(a)(b)$ si ha che $[N, +, \cdot]$ è un quasianello con funzione di Clay φ.*

Infatti, il fatto che $\forall a \in N$ $\varphi_a \in End(N)$ garantisce la distributiva sinistra del prodotto rispetto alla somma: $\forall a, b, c \in N$ $a(b + c) = \varphi_a(b + c) = \varphi_a(b)\varphi_a(c) = ab + ac$; inoltre $\forall a, b, c \in N$ $a(bc) = a(\varphi(b)(c)) = \varphi(a)(\varphi(b)(c)) = (\varphi(a) \circ \varphi(b))(c) = \varphi(\varphi(a)(b))(c) = \varphi(ab)(c) = (ab)c$.

1.3 Concetti legati alle funzioni di Clay

Il fatto che le funzioni di Clay sono endomorfismi del gruppo additivo di un quasianello consente di dare la seguente

Definizione 1.8. *Siano N un quasianello , $S \subset N$ e φ_s le funzioni di Clay associate agli elementi di S. Diciamo* ***annullatore destro*** *di S l'insieme $A_r(S) = \bigcap_{s\in S} \ker \varphi_s = \{n \in N \mid Sn = \{0\}\}$. Osserviamo che $A_r(S)$ è un sottogruppo normale di N^+.*
Chiamiamo ***annullatore sinistro*** *di S l'insieme $A_l(S) = \{n \in N \mid \varphi_n(S) = \{0\}\}$.*
Se risulta $A_l(S) = A_r(S)$ allora si pone $A(S) = A_l(S) = A_r(S)$ e si parla di annullatore bilatero.

La classica decomposizione di Peirce relativa ad un idempotente unita alla considerazione degli annullatori destri fornisce una importante proprietà del gruppo additivo di un quasianello. Infatti 0 è un elemento idempotente di N ed inoltre si ha $0N = N_c$; è immediato poi constatare che $A_r(0) = \{n \in N \mid 0n = 0\} = N_0$ e che $\forall n \in N\ n = (n - 0n) + 0n$, dove $n - 0n \in N_0$. Otteniamo quindi come caso particolare della decomposizione di Peirce che N^+ è somma semidiretta del suo sottogruppo normale N_0 e del suo sottogruppo N_c.

Sia Φ il semigruppo di Clay di un quasianello N; se $\Phi \subset \{\mathbf{0}, \iota\}$ dove $\mathbf{0}$ è la funzione nulla e ι l'identica, diciamo che N è un *quasianello banale*. Osserviamo che un quasianello costante è un quasianello banale, infatti in esso $\forall x, y \in N\ yx = x$ e dunque $\forall x \in N\ \varphi_x = \iota$. Si prova facilmente il seguente

Teorema 1.9. *Tutti e soli i quasianelli banali non costanti che hanno $[N, +]$ come gruppo additivo sono i quasianelli $[N, +, \cdot_S]$, dove $S \subset N\backslash\{0\}$ e*

$$\forall a, b \in N \quad a \cdot_s b = \begin{cases} 0 \, se \, a \notin S \\ b \, se \, a \in S \end{cases}$$

Importante per il seguito è la seguente

Definizione 1.10. *Un quasianello N si dice* ***monogeno*** *se $\exists n \in N$ tale che φ_n è suriettiva e fortemente monogeno se $A_l(N) \neq N$ e $\forall n \in N\backslash A_l(N)$ φ_n è suriettiva.*

La considerazione che ogni funzione suriettiva da un insieme finito in sé è una bigezione consente di asserire che in un quasianello finito N fortemente monogeno risulta, $\forall n \in N$, $\varphi_n = 0$ oppure $\varphi_n \in Aut(N^+)$.

Capitolo 2

QUASIANELLI PLANARI

In questo capitolo definiamo i quasianelli planari, dimostriamo un teorema che ne descrive nel dettaglio la struttura e descriviamo importanti costruzioni di quasianelli planari.

2.1 Definizioni e prime proprietà

Per capire l'idea di planarità ed il suo significato geometrico ricordiamo che nel piano euclideo due rette non parallele di equazioni

$$\begin{aligned} y &= mx + b \\ y &= m'x + b' \end{aligned}$$

con $m \neq m'$ hanno un unico punto di intersezione perchè l'equazione $mx = m'x + (b' - b)$ ha un'unica soluzione $x = (m - m')^{-1}(b' - b) \in \mathbb{R}$. Ciò motiva la seguente

Definizione 2.1. *Un quasianello N si dice **planare** se*

1. $\forall a, b, c \in N$ con $\varphi_a \neq \varphi_b$ l'equazione

$$ax = bx + c$$

   ha un'unica soluzione in N

2. detto $\tilde{\Phi}$ il semigruppo di Clay di N si ha $|\tilde{\Phi}| \geq 3$.

La 1) si dice proprietà di planarità. La richiesta 2) serve sostanzialmente ad escludere dalla classe dei quasianelli planari i quasianelli banali i quali soddisfano tutti la proprietà di planarità e quindi disturberebbero nella teoria generale dei quasianelli planari.

2.2 Teoremi di struttura

Teorema 2.2. *I quasianelli planari sono zero-simmetrici e fortemente monogeni.*

Dimostrazione. Sia N un quasianello planare con semigruppo di Clay $\tilde{\Phi}$. Dobbiamo mostrare che $\forall b \in N\ 0b = 0$. Poichè $|\tilde{\Phi}| \geq 3$, $\exists a \in N$ tale che $\varphi_a \neq \varphi_0$; $\forall b \in N$, 0 e $0b$ sono soluzioni in N dell'equazione $ax = 0x + 0$ con $\varphi_a \neq \varphi_0$ e dunque $0b = 0$. Dunque N è zero-simmetrico. Mostriamo ora che $\forall a \in N\ aN = \{0\}$ o $aN = N$. Sia $a \in N$: se $\varphi_a = \varphi_0$ allora $aN = 0N$, ma N è zero-simmetrico e dunque $0N = \{0\}$ ed allora $aN = \{0\}$, se $\varphi_a \neq \varphi_0$, $\forall b \in N$ l'equazione $ax = b$, cioè $ax = 0x + b$ ammette un'unica soluzione e dunque $aN = N$. □

I quasianelli planari hanno una struttura molto particolare come mostra il seguente teorema di struttura, per la cui dimostrazione abbiamo bisogno di un risultato di teoria dei semigruppi, che riportiamo senza dimostrazione, e di alcune definizioni.

Teorema 2.3. ***(Clifford e Preston)***
Sia R un semigruppo; sono equivalenti

1. *R è un gruppo destro, cioè $\forall a, b \in R\ \exists! x \in R$ tale che $ax = b$ (le traslazioni sinistre sono bigezioni)*
2. *R è semplice a destra, cioè R non ha ideali destri propri*
3. *R è prodotto diretto di un gruppo G e di un semigruppo E di zeri destri*

Definizione 2.4. *Siano X un insieme e Ψ un semigruppo (rispetto alla composizione) di funzioni da X in sé. Chiamiamo* ***orbita*** *di x determinata da Ψ l'insieme $\Psi x = \{\psi(x) \mid \psi \in \Psi\}$. Un'orbita Ψx si dice* ***regolare*** *se, $\forall \varphi, \psi \in \Psi$, $\varphi x = \psi x \Rightarrow \varphi = \psi$,* ***principale*** *se $|\Psi x| = |\Psi|$. Naturalmente un'orbita regolare è anche principale.*

Definizione 2.5. *Siano $[G, +]$ un gruppo e Ψ un sottogruppo di $Aut(G)$. Diciamo che Φ è un* ***gruppo di automorfismi senza punti fissi*** *(e scriviamo f.p.f.) se $\forall f \in \Psi \backslash \{\iota\}\ \forall x \in G \backslash \{0\}\ f(x) \neq x$. Osserviamo che se Ψ è un gruppo di automorfismi f.p.f. di G allora, $\forall \varphi \in \Phi \backslash \{\iota\}$, la funzione $-\varphi + \iota$ è iniettiva, infatti se $(-\varphi + \iota)(x) = (-\varphi + \iota)(y)$ allora $\varphi y - \varphi x = \varphi(y - x) = y - x$, e dunque $y - x = 0$, cioè $y = x$.*

Teorema 2.6. ***(Struttura dei quasianelli planari)***
Siano N un quasianello planare ed $R = N \backslash A_l(N)$, dove, ricordiamo, $A_l(N)$ indica l'annullatore sinistro di N. Allora

1. *R è un sottosemigruppo di $N^{\cdot}$ prodotto diretto di un gruppo G e di un semigruppo E di zeri destri.*
2. *Scrivendo, $\forall r \in R$, $r = \langle g, e \rangle$ con $g \in G$ ed $e \in E$ e chiamando U l'insieme delle unità sinistre di $N^{\cdot}$ si ha $U = \langle 1, E \rangle = \{\langle 1, e \rangle \mid e \in E\}$, dove 1 è l'unità di G.*

3. *Se $\tilde{\Phi}$ è il semigruppo di Clay di N si ha che $\Phi = \tilde{\Phi}\backslash\{0\}$ è un gruppo di automorfismi f.p.f di N^+ tale che, $\forall\psi \in \Phi\backslash\{\iota\}$, $(-\varphi + \iota)$ è un bigezione. Se φ è la funzione di Clay di N $\bar{\varphi} = \varphi|_R^{\Phi} : R \to \Phi$ è un epimorfismo di semigruppi.*

4. *Denotando con $\sim_{\bar{\varphi}}$ la relazione indotta da $\bar{\varphi}$ su R si ha $G \simeq \frac{R}{\sim_{\bar{\varphi}}} \simeq \Phi$.*

5. *Le orbite non banali (cioè determinate da elementi non nulli) di Φ sono regolari e costituiscono una partizione di $N\backslash\{0\}$.*

Dimostrazione. 1. Siano $a, b \in R = N\backslash A_l(N)$, sicché $\varphi_a \neq \mathbf{0}$ e $\varphi_b \neq \mathbf{0}$. Poichè N è fortemente monogeno $aN = bN = N$ e dunque $abN = N$; in particolare $\varphi_{ab} \neq \mathbf{0}$, cioè $ab \in R$. Dunque R è un sottosemigruppo di $N^{\cdot}$. Mostriamo che R è un gruppo destro. $\forall a, b \in R$, poichè $\varphi_a \neq \mathbf{0}$, per la planarità di N l'equazione $ax = 0x + b$ ha un'unica soluzione $\bar{x} \in N$ per la quale si ha, poichè N è zero-simmetrico, $a\bar{x} = 0\bar{x} + b = b$ ed inoltre, poiché la funzione di Clay di N φ è un omomorfismo di semigruppi φ, $\varphi_{a\bar{x}} = \varphi_a\varphi_{\bar{x}} = \varphi_b \neq \mathbf{0}$ e dunque $\varphi_{\bar{x}} \neq \mathbf{0}$, cioè $\in R$. Abbiamo così mostrato che $\forall a, b \in R$ $\exists! x \in R$ tale che $ax = b$, cioè R è un gruppo destro. Il teorema 2.3 di Clifford e Preston ci permette di concludere che R è prodotto diretto di un gruppo G e un semigruppo E di zeri destri.

2. Sia $u \in U$, dove U è l'insieme delle unità sinistre di $N^{\cdot}$; allora $\varphi_u = \iota$ ed in particolare $\varphi_u \neq \mathbf{0}$, cioè $u \in R$. Per quanto mostrato nel punto 1, $u = \langle g, e\rangle$, con $g \in G$ ed $e \in E$. Poichè u è un'unità sinistra $\langle 1, e\rangle = u \cdot \langle 1, e\rangle = \langle g, e\rangle \cdot \langle 1, e\rangle = \langle g, e\rangle$ e dunque $u \in \langle 1, E\rangle$. Viceversa, sia $l = \langle 1, e\rangle \in \langle 1, E\rangle$, allora $l^2 = \langle 1, e\rangle \cdot \langle 1, e\rangle = \langle 1, e^2\rangle = \langle 1, e\rangle = l$ ed inoltre $\forall n \in N$ l'equazione $lx = 0x + ln$ ha, per la planarità di N e poichè $\varphi_l \neq 0$, un'unica soluzione in N. Essendo l idempotente ed N zero-simmetrico, n ed ln sono soluzione della suddetta equazione, così $ln = n$, e dunque l è unità sinistra di $N^{\cdot}$, cioè $l \in U$.

3. Sia $\tilde{\Phi}$ il semigruppo di Clay di N e $\Phi = \tilde{\Phi}\backslash\{0\}$; poichè N è fortemente monogeno $\forall n \in N$ $\varphi_n = \mathbf{0}$ se e solo se $n \in A_l(N)$ e dunque $\Phi = \{\varphi_n \,|n \in R\}$. Osserviamo inoltre che $\forall n \in N$ $\varphi = \iota$ se e solo se $n \in U$. Mostriamo che gli elementi di Φ sono automorfismi di N^+ : sia $r = \langle g, e\rangle \in R$, poniamo $\bar{r} = \langle g^{-1}, e\rangle \in R$ ed $u = \langle 1, e\rangle \in \langle 1, E\rangle = U$; si ha $r\bar{r} = \langle g, e\rangle \cdot \langle g^{-1}, e\rangle = \langle 1, e\rangle = u \in \langle 1, E\rangle = U$ ed anche $\bar{r}r = u$ e dunque $\iota = \varphi_u = \varphi_{r\bar{r}} = \varphi_r\varphi_{\bar{r}}$ e $\iota = \varphi_u = \varphi_{\bar{r}r} = \varphi_{\bar{r}}\varphi_r$, cioè $\varphi_r \in Aut(N^+)$. Mostriamo ora che Φ è un gruppo di automorfismi f.p.f. di N. Sia $\varphi \in U\backslash\{\iota\}$; allora esiste $a \in R$ tale che $\varphi = \varphi_a$ e, poichè $\varphi \neq \iota$, deve essere $a \notin U$; sia $u \in U$ e consideriamo l'equazione $ax = ux + 0$ che, per planarità di N e poichè $\varphi_a \neq \varphi_u = \iota$, ha un'unica soluzione in N. Poichè 0 è una soluzione, deve essere $\forall x \in N\backslash\{0\}$ $ax \neq ux + 0$ e dunque $\varphi_a x \neq x$. Mostriamo ora che $\forall\varphi \in \Phi\backslash\{0\}$ $(-\varphi + \iota)$ è una bigezione. Sia $\varphi = \varphi_a \in \Phi\backslash\{0\}$, con $a \in R\backslash U$, e sia $u \in U$; $\forall b \in N$, poichè $\varphi_a \neq \varphi_u$, l'equazione $ux = ax + b$ ha

un'unica soluzione in N. Poichè tale equazione si può scrivere equivalentemente $b = -ax + ux = -ax + x = -\varphi_a x + x = (-\varphi_a + \iota)x$, possiamo concludere che $(-\varphi_a + \iota)$ è una bigezione.

4. La funzione di Clay $\varphi : N^{\cdot} \to \tilde{\Phi}$ è un epimorfismo di semigruppi, R è un sottosemigruppo di $N^{\cdot}$ e $\varphi(R) = \tilde{\Phi}\backslash\{0\} = \Phi$; dunque $\bar{\varphi} = \varphi|_R^{\Phi}$ è un epimorfismo di semigruppi. Se $\sim_{\bar{\varphi}}$ è la relazione di equivalenza indotta da $\bar{\varphi}$ su R si ha che $\forall a, b \in R$ a$\sim_{\bar{\varphi}} b$ se e solo se $\varphi_a = \varphi_b$. Poichè $\bar{\varphi}$ è una congruenza di R, possiamo considerare il semigruppo quoziente $\frac{R}{\sim_{\bar{\varphi}}}$; mostriamo che $\frac{R}{\sim_{\bar{\varphi}}} = \{\langle g, E\rangle \mid g \in G\}$: $\forall\, \langle g, e\rangle$,$\langle \tilde{g}, \tilde{e}\rangle \in R$ $\varphi_{\langle g,e\rangle} = \varphi_{\langle \tilde{g},\tilde{e}\rangle}$ se e solo se $\iota = \left(\varphi_{\langle \tilde{g},\tilde{e}\rangle}\right)^{-1} \varphi_{\langle g,e\rangle} = \varphi_{\langle \tilde{g}^{-1},\tilde{e}\rangle}\varphi_{\langle g,e\rangle} = \varphi_{\langle \tilde{g}^{-1},\tilde{e}\rangle\cdot\langle g,e\rangle} = \varphi_{\langle \tilde{g}^{-1}g,\tilde{e}\rangle}$ se e solo se $\langle \tilde{g}^{-1}g, \tilde{e}\rangle \in U = \langle 1, E\rangle$ se e solo se $g = \tilde{g}$. Tenendo conto che $\forall\, \langle g, E\rangle, \langle \tilde{g}, E\rangle \in \frac{R}{\sim_{\bar{\varphi}}}$ $\langle g, E\rangle \cdot \langle \tilde{g}, E\rangle = \langle g\tilde{g}, E\rangle$ è immediato osservare che la $\theta : G \to \frac{R}{\sim_{\bar{\varphi}}}$ tale che $\theta(g) = \langle g, E\rangle$ $\forall g \in G$ è un isomorfismo. Che sia $\frac{R}{\sim_{\bar{\varphi}}} = \bar{\varphi}(R) = \Phi$ è immediato dal primo teorema di omomorfismo.

5. Sia $x \in N\backslash\{0\}$; mostriamo che l'orbita Φx è regolare: siano $\varphi, \psi \in \Phi$ tali che $\varphi x = \psi x$; si ha $\psi^{-1}\varphi x = x$, con $\psi^{-1}\varphi \in \Phi$ gruppo di automorfismi f.p.f. di N e $x \neq 0$, e dunque $\psi^{-1}\varphi = \iota$, cioè $\varphi = \psi$. In generale le orbite di un semigruppo Ψ di automorfismi di un gruppo costituiscono una partizione, poichè sono le classi della relazione di equivalenza $a \sim b$ se e solo se $\exists \psi \in \Psi$ tale che $\psi a = b$.

□

Dal teorema di struttura discende il

Corollario 2.7. *Un quasianello planare N è integrale (cioè $\forall x, y \in N\backslash\{0\}$ $xy \neq 0$) se e solo se $A_l(N) = \{0\}$*

Dimostrazione. N è integrale se e solo se $N\backslash\{0\}$ è un sottosemigruppo di $N^{\cdot}$. Se $\mathrm{A}_l(N) = \{0\}$ allora, con le notazioni del Teorema di Struttura, $N\backslash\{0\} = N\backslash A_l(N) = R$ che è un sottosemigruppo di $N^{\cdot}$ e dunque N è integrale. Viceversa, siano N integrale ed $n \in A_l(N)$, allora $\forall x \in N$, $nx = 0$ e dunque $n = 0$. Si ha così $A_l(N) = \{0\}$. □

2.3 Costruzioni

Il teorema di struttura, oltre a fornire una caratterizzazione dei quasianelli planari, suggerisce anche un modo per costruirli. A tal proposito si ha il seguente

Teorema 2.8. ***(Fabbrica di Ferrero)***
Siano $[N, +]$ un gruppo, Φ un gruppo non banale di automorfismi f.p.f di N, tale che, $\forall \varphi \in \Phi$, $(-\varphi + \iota)$ sia una bigezione, e $U \subset N\backslash\{0\}$ tale che, $\forall x \in N$, $|U \cap \Phi x| \leq 1$. Poniamo $R = \bigcup_{u\in U} \Phi u$, $A = N\backslash R$ e $\varphi : N \to \Phi \cup \{0\}$ tale che, se $a \in A$, $\varphi_a = \mathbf{0}$ e, se $r \in R$, detto u l'unico elemento di $U \cap \Phi r$ e detto β l'unico elemento di Φ tale che

$\beta u = x$, $\varphi(r) = \beta$. Se poniamo $\forall a, b \in N\ a \cdot b = \varphi(a)(b)$, la struttura $[N, +, \cdot]$ risulta un quasianello planare con gruppo di Clay Φ.

Dimostrazione. E' bene innanzitutto notare che dato $r \in R$ è univocamente determinato β come nell'enunciato, infatti β è unico perchè se $\beta, \tilde{\beta} \in \Phi$ e $\beta u = \tilde{\beta} u = x$, allora $\tilde{\beta}^{-1}\beta u = u$ e dunque, essendo Φ gruppo di automorfismi f.p.f., $\tilde{\beta}^{-1}\beta = \iota$, cioè $\beta = \tilde{\beta}$. Osserviamo che essendo $U \subset N\backslash\{0\}$, $\forall x \in U\ 0 \notin \Phi x$, e dunque $0 \notin \bigcup_{x \in U} \Phi x = R$, cioè $0 \in A$. Poichè le orbite di Φ sono invarianti per gli elementi di Φ, tali risultano anche A ed R. Per semplificare le notazioni, poniamo $\forall a \in N\ \varphi(a) = \varphi_a$; mostriamo che φ soddisfa alla $\forall a, b \in N\ \varphi_a\varphi_b = \varphi_{\varphi_a b}$ che, come dimostrato precedentemente, garantisce che $[N, +, \cdot]$ sia un quasianello con funzione di Clay φ: consideriamo 3 casi

Caso 1) $a \in A$; allora $\varphi_a = \mathbf{0}$ e dunque $\varphi_a\varphi_b = \mathbf{0}$, inoltre $\varphi_a b = 0 \in A$ e dunque $\varphi_{\varphi_a b} = \mathbf{0}$

Caso 2) $a \notin A$, $b \in A$; allora $\varphi_b = \mathbf{0}$ e dunque $\varphi_a\varphi_b = \mathbf{0}$, inoltre $b \in A$ e dunque $\varphi_a b \in A$ e così $\varphi_{\varphi_a b} = \mathbf{0}$

Caso 3) $a, b \in R$; siano $\Phi a \cap U = \{u_2\}$ e $\Phi a \cap U = \{u_1\}$, dunque $a = \varphi_a u_1$ e $b = \varphi_b u_2$, allora $\varphi_a\varphi_b u_2 = \varphi_a b \in R$ e $U \cap \Phi(\varphi_a b) = U \cup \Phi b = \{u_2\}$, e così per definizione di φ, $\varphi_{\varphi_a b} = \varphi_a\varphi_b$.

Mostriamo ora che $[N, +, \cdot]$ è un quasianello planare. Detto $\tilde{\Phi}$ il semigruppo di Clay di N è $\tilde{\Phi} = \varphi(N) = \Phi \cup \{0\}$ e dunque $|\tilde{\Phi}| = |\Phi| + 1 \geq 3$ ($|\Phi| \geq 2$ perchè Φ gruppo non banale). Per quanto riguarda la proprietà di planarità, $\forall a, b, c \in N$ tali che $\varphi_a \neq \varphi_b$, l'equazione in N $ax = bx + c$ si può scrivere equivalentemente $c = -bx + ax = -\varphi_b x + \varphi_a x = (-\varphi_b + \varphi_a)x = \varphi_a(-\varphi_a^{-1}\varphi_b + \iota)x = \varphi_a(-\psi + \iota)x$, dove $\psi = \varphi_a^{-1}\varphi_b \in \Phi$. Poichè $\varphi_a \in \Phi \leq Aut(N^+)$, φ_a è una bigezione, inoltre $\varphi_a \neq \varphi_b$, dunque $\psi \neq \iota$ e così anche $(-\psi + \iota)$ è una bigezione. L'equazione $ax = bx + c$ ha quindi un'unica soluzione in N, ed N è planare. □

Viene spontaneo a questo punto dare la seguente

Definizione 2.9. *Siano $[N, +]$ un gruppo e Φ un gruppo non banale di automorfismi f.p.f. di N tale che $\forall \varphi \in \Phi\backslash\{\iota\}$, $(-\varphi + \iota)$ sia una bigezione. Allora la coppia (N,Φ) si dice* ***coppia di Ferrero.***

Abbiamo precedentemente osservato che se f è un automorfismo f.p.f. di un gruppo G allora la funzione $(-f+\iota)$ è iniettiva, e dunque se G è finito è una bigezione. Di conseguenza, se N è un gruppo finito, l'ultima richiesta nella definizione di coppia di Ferrero è automaticamente soddisfatta qualora lo siano le altre. Osserviamo inoltre che dal teorema di struttura si deduce immediatamente che se N è un quasianello planare e Φ il suo gruppo di Clay allora (N, Φ) è una coppia di Ferrero, che chiameremo coppia di Ferrero associata al quasianello N.

La Fabbrica di Ferrero è uno strumento potente perchè permette di costruire tutti i quasianelli planari, come dimostra il seguente

Teorema 2.10. *Siano N un quasianello planare, Φ il suo gruppo di Clay, U l'insieme delle unità sinistre di $N^{\cdot}$; allora il quasianello costruito con la Fabbrica di Ferrero a partire dalla coppia di Ferrero (N, Φ) associata a N è isomorfo a N.*

Dimostrazione. Per dimostrare il teorema è sufficiente far vedere che la funzione φ definita nella Fabbrica di Ferrero coincide con la funzione di Clay di N. Sia $x \in N$, se $x \in A_l(N)$, allora, per il teorema di struttura, $\Phi x \cap U = \varnothing$ e dunque $\varphi(x) = \mathbf{0} = \varphi_x$; se $x \in N \backslash A_l(N)$, allora, per il teorema di struttura, $\Phi x \cap U$ ha un unico elemento l ed esiste un unico $\beta \in \Phi$ tale che $\beta l = x$, e dunque $\beta = \varphi(x)$. Sia $a \in N$ tale che $\beta = \varphi_a$, cioè $x = au$ e dunque $\varphi_x = \varphi_a \varphi_u = \varphi_a = \beta = \varphi(x)$. □

Se F è un campo e K un sottogruppo non banale di F^*, identificando K con il sottogruppo di $Aut(F)$ $\{\psi_a \mid \ a \in K\}$, dove $\psi_a(b) = ab$ $\forall b \in F$, si ha che (F, K) è una coppia di Ferrero, infatti $\forall a \in K \backslash \{1\}, \forall x \in F \quad \psi_a x = x \Rightarrow ax = x \Rightarrow (a-1)x = 0 \Rightarrow x = 0$, e dunque K è un sottogruppo non banale di automorfisfi f.p.f di F. Inoltre $\forall a \in K \backslash \{1\}, \forall x \in F$ $(-\psi_a + \iota)x = (-a+1)x = \psi_{-a+1}x$ e dunque $-\psi_a + \iota$ è una bigezione.

Diamo allora la

Definizione 2.11. *Se F è un campo e K un sottogruppo non banale di F^*, un **quasianello** $[F, +, \cdot]$ ottenuto dalla coppia di Ferrero (F, K) si dice **field-generated.***

Nel capitolo 5 studieremo in particolare quasianelli field-generated a partire dalla coppia di Ferrero $(\mathbb{Z}_p, \Phi_k)$, dove p è un numero primo e Φ_k il sottogruppo di $\mathbb{Z}_p^*$ di ordine k, mentre nel capitolo 6 ci occuperemo di quasianelli field generated su $\mathbb{C}$ con gruppo di Clay il gruppo T_k delle radici k-esime dell'unità.

Forniamo ora una serie di esempi di quasianelli field-generated a partire da diversi sottogruppi di $\mathbb{C}^*$.

Esempio 2.12. *Sia $[\mathbb{C}, +, *_1]$ il quasianello ottenuto con la Fabbrica di Ferrero partendo dalla coppia di Ferrero $(\mathbb{C}, \mathbb{S}^1)$, dove $\mathbb{S}^1$ è il gruppo moltiplicativo dei complessi di modulo 1, scegliendo come insieme di unità sinistre $\mathbb{R}^+ = U$. Le orbite non banali di $\mathbb{S}^1$ in $\mathbb{C}$ sono i cerchi di centro 0, ed inoltre si ha $\bigcup_{z \in \mathbb{R}^+} \mathbb{S}^1 z = \mathbb{C}^*$, $\forall z \in \mathbb{C}^*$ $\mathbb{S}^1 z \cap \mathbb{R}^+ = |z|$ e dunque*

$$\forall z, w \in \mathbb{C} \qquad z *_1 w = \begin{cases} \frac{z}{|z|} w \, se \, z \neq 0 \\ 0 \, se \, z = 0 \end{cases}$$

Esempio 2.13. *Sia $[\mathbb{C}, +, *_2]$ il quasianello ottenuto con la Fabbrica planari di Ferrero partendo dalla coppia di Ferrero $(\mathbb{C}, \mathbb{R}^+)$ scegliendo come insieme di unità sinistre*

$\mathbb{S}^1 = U$. *Le orbite non banali di* $\mathbb{R}^+$ *in* $\mathbb{C}$ *sono semirette di origine 0, ed inoltre si ha* $\bigcup_{z\in\mathbb{R}^+} \mathbb{R}^+ z = \mathbb{C}^*$, $\forall z \in \mathbb{C}^*\ \mathbb{R}^+ z \cap \mathbb{S}^1 = \left\{\frac{z}{|z|}\right\}$ *e dunque*

$$\forall z, w \in \mathbb{C} \qquad z *_2 w = \begin{cases} |z|\, w \, se\, z \neq 0 \\ 0 \, se\, z = 0 \end{cases}$$

Due quasianelli ottenuti dalla stessa coppia di Ferrero possono anche essere molto diversi, come mostrano i seguenti due esempi.

Esempio 2.14. *Sia* $[\mathbb{C}, +, *_3]$ *il quasianello ottenuto con la Fabbrica di Ferrero partendo dalla coppia di Ferrero* $(\mathbb{C}, \mathbb{R}^*)$ *scegliendo come insieme di unità sinistre* $U = \{z \in \mathbb{C} | \mathrm{Re} z = 1\} \cup \{i\}$. *Le orbite non banali di* $\mathbb{R}^+$ *in* $\mathbb{C}$ *sono rette per l' origine private di 0, ed inoltre si ha* $\bigcup_{z\in\mathbb{U}} \mathbb{R}^* z = \mathbb{C}^*$, $\quad \forall z \in \mathbb{C}^*$;
se $\mathrm{Re} z \neq 0 \quad \mathbb{R}^* z \cap U = \left\{\frac{z}{\mathrm{Re} z}\right\}$, *se* $\mathrm{Re} z = 0 \quad \mathbb{R}^* z \cap U = \left\{\frac{z}{\mathrm{Im} z} = i\right\}$ *e dunque*

$$\forall z, w \in \mathbb{C} \qquad z *_3 w = \begin{cases} (\mathrm{Re} z) w \ se\ \mathrm{Re} z \neq 0 \\ (\mathrm{Im} z) w \ se\ \mathrm{Re} z = 0 \end{cases} .$$

Esempio 2.15. *Siano* a *e* b *due numeri reali positivi e* $[\mathbb{C}, +, *_4]$ *il quasianello ottenuto con la fabbrica di Ferrero partendo dalla coppia di Ferrero* $(\mathbb{C}, \mathbb{R}^*)$ *scegliendo come insieme di unità sinistre* $U = \left\{x + iy \in \mathbb{C} \,\middle|\, \left|\frac{x^2}{a^2} - \frac{y^2}{b^2}\right| = 1\right\} \cup \{i\}$. *Le orbite non banali di* $\mathbb{R}^+$ *in* $\mathbb{C}$ *sono rette per l' origine private di 0, ed inoltre si ha* $\bigcup_{z\in\mathbb{U}} \mathbb{R}^* z = \mathbb{C} \setminus \left\{x + iy \in \mathbb{C} \,\middle|\, \left|\frac{x^2}{a^2} - \frac{y^2}{b^2}\right| = 0\right\} = R$ *e* $\forall z \in R \quad \mathbb{R}^* z \cap U = \left\{\frac{z}{\left|\frac{x^2}{a^2} - \frac{y^2}{b^2}\right|^{\frac{1}{2}}}\right\}$ *e dunque*

$$\forall z, w \in \mathbb{C} \qquad z *_4 w = \left|\frac{x^2}{a^2} - \frac{y^2}{b^2}\right|^{\frac{1}{2}} w$$

Osserviamo che i quasianelli degli ultimi due esempi sono ottenuti dalla stessa coppia di Ferrero $(\mathbb{C}, \mathbb{R}^*)$. Il primo dei due è integrale ed ha come orbite rette per l'origine private di 0, il secondo ha come orbite le iperboli di asintoti le rette di equazione $\left|\frac{x^2}{a^2} - \frac{y^2}{b^2}\right| = 0$ e non è integrale perchè gli elementi degli asintoti sono divisori dello zero.

Parte II

Grafi e sistemi di cerchi

Capitolo 3

Strutture d'incidenza e quasianelli planari circolari

3.1 Strutture d'incidenza e BIBD

Introduciamo ora i principali concetti relativi a strutture geometriche molto generali, in cui si studiano sistemi di punti e le loro proprietà di intersezione.

Definizione 3.1. *Una* ***struttura d'incidenza*** *è una terna $(V, \mathcal{B}, R)$, dove V è un insieme, $\mathcal{B} \subset \wp(V)$ e $R \subset V \times \mathcal{B}$ una relazione.*

Particolarmente importante è il caso in cui R sia l'usuale relazione di appartenenza, come noi d'ora in poi supporremo. Se $(V, \mathcal{B}, \in)$ è una struttura d'incidenza, gli elementi di V si dicono *punti*, gli elementi di B si dicono *blocchi*. Se $\{p_1, p_2, .., p_n\} \subset V$ è un insieme di punti si pone

$$[p_1, p_2, .., p_n] = |\{\mathcal{B} \in V \,|\{p_1, p_2, .., p_n\} \subset \mathcal{B}\}|\,;$$

$|V|$ e $|\mathcal{B}|$ si dicono parametri della struttura d'incidenza.

Certe strutture d'incidenza risultano naturalmente associate a coppie di Ferrero; se (N, Φ) è una coppia di Ferrero, poniamo

$$\begin{aligned}
\mathcal{B}^*_\Phi &= \{\Phi a + b \,|a \in N \backslash \{0\}, b \in N\} \\
\mathcal{B}_\Phi &= \{(\Phi \cup \{0\})a + b \,|a \in N \backslash \{0\}, b \in N\} \\
\mathcal{B}^-_\Phi &= \{(\Phi \cup \{0\})\{a, -a\} + b \,|a \in N \backslash \{0\}, b \in N\}
\end{aligned}$$

Si ha che $(N, \mathcal{B}^*_\Phi, \in)$, $(N, \mathcal{B}_\Phi, \in)$ e $(N, \mathcal{B}^-_\Phi, \in)$ sono strutture d'incidenza.

Esempio 3.2. *Per $(N, \Phi) = (\mathbb{C}, \mathbb{S}^1)$ (vedi esempio 2.12) gli elementi di $\mathcal{B}^*_\Phi$ sono i cerchi di $\mathbb{C}$; infatti $\forall z, w \in \mathbb{C}^* \quad \Phi z + w = \mathbb{S}^1 z + w$ è il cerchio di centro w e raggio $|z|$. Per $(N, \Phi) = (\mathbb{C}, \mathbb{R}^*)$ (vedi esempio 2.14) gli elementi di $\mathcal{B}_\Phi$ sono le rette di $\mathbb{C}$: infatti $\forall z, w \in \mathbb{C}^* \quad (\Phi \cup \{0\})z + w = \mathbb{R}z + w$ è la retta per w di direzione $\frac{z}{|z|}$; per $(N, \Phi) = (\mathbb{C}, \mathbb{R}^+)$ (vedi esempio 2.13) gli elementi di $\mathcal{B}^-_\Phi$ sono le rette di $\mathbb{C}$, infatti $\forall z, w \in \mathbb{C}^* \quad (\Phi \cup \{0\})z + w = (\mathbb{R}^+ \cup \{0\})\{z, -z\} + w$ è la retta per w di direzione $\frac{z}{|z|}$.*

Vogliamo studiare strutture d'incidenza che presentino qualche proprietà particolare sul numero di blocchi che passano per uno o due punti dati.

Definizione 3.3. *Un **disegno a blocchi bilanciato incompleto** (che abbrevieremo con **BIBD**) è una struttura d'incidenza $(V, \mathcal{B}, \in)$ per cui esistano interi v, n, k, r, λ, detti parametri del BIBD, tali che $|V| = v$, $|\mathcal{B}| = b$, $\forall B \in \mathcal{B}\ |B| = k$, $\forall p \in V\ [p] = r$ e $\forall \{p, q\} \subset V\ [p, q] = \lambda$.*

Le proprietà di un BIBD impongono una restrizione sui suoi parametri v, n, k, r, λ, segnatamente:

$$\begin{aligned} \lambda(v-1) &= r(k-1) \\ vr &= bk \end{aligned}$$

Infatti, ogni elemento di V appartiene esattamente a r blocchi, e dunque

$$vr = |V|\, r = \sum_{B \in \mathcal{B}} |B| = k\, |\mathcal{B}| = kb$$

Ogni sottoinsieme di due elementi di V è contenuto in esattamente λ elementi di $\mathcal{B}$; inoltre V ha $\frac{v(v-1)}{2}$ sottoinsiemi di due elementi, ogni elemento di $\mathcal{B}$ ha $\frac{k(k-1)}{2}$ sottoinsiemi di due elementi, da cui $\frac{v(v-1)}{2}\lambda = \frac{k(k-1)}{2}b$, e poichè $vr = kb$ è anche $\lambda(v-1) = r(k-1)$

3.2 BIBD da coppie di Ferrero

Conviene a questo punto fare alcune osservazioni riguardo alle strutture $(N, \mathcal{B}_{\Phi^*}, \in)$. Se (N, Φ) è una coppia di Ferrero si ha

$$\{B \in \mathcal{B}^*_\Phi \mid \quad 0 \in B\} = \{\Phi a - a \mid \quad a \in N \backslash \{0\}\}$$

Infatti, poichè $\iota \in \Phi$, $\forall a \in N \quad 0 = a - a = \iota a - a \in \Phi a - a$; viceversa se $B = \Phi b + c \in \mathcal{B}$ è tale che $0 \in B$ si ha $0 = \varphi b + c$, con $\varphi \in \Phi$, e dunque $c = -\varphi b$, $B = \Phi b + c = \Phi b - \varphi b = \Phi(\varphi b) - \varphi b = \Phi a - a$, con $a = \varphi b$.

Per determinare se due blocchi coincidono o meno si utilizza il seguente

Teorema 3.4. *Siano N quasianello planare, Φ il suo gruppo di Clay e $\Phi a + b, \Phi c + d \in \mathcal{B}^*_\Phi$. Sono equivalenti:*

1. $\Phi a + b = \Phi c + d$;
2. $\Phi a = \Phi c$ e $b = d$;

Dimostrazione. Poichè la struttura di incidenza $(N, \mathcal{B}^*_\Phi, \in)$ dipende solo dalla coppia di Ferrero associata al quasianello N, possiamo supporre N integrale.
L'implicazione $2 \Longrightarrow 1$ è banale.

$1 \Rightarrow 2$
Supponiamo $\Phi a + b = \Phi c + d$, allora $\Phi a = \Phi c + (d - b)$. Poniamo $n = d - b$ ed osserviamo che per concudere basta dimostrare che $n = 0$. Se $a = 0$ allora $0 = |\Phi a| = |\Phi c + n| = |\Phi c|$, e dunque $c = n = 0$. Se $a \neq 0$ $|\Phi| = |\Phi a| = |\Phi c + n| = |\Phi c|$ e dunque anche $c \neq 0$. Supponiamo per assurdo $n \neq 0$. Poichè la struttura di incidenza Φa è un sottogruppo additivo di N invariante a sinistra rispetto al prodotto, tale è anche $\Phi c + n$, e dunque $\forall x \in N$ $\Phi c + n = x(\Phi c + n) = \Phi c + xn$. Poichè N è non banale e $n \neq 0$, esiste $x \in N$ tale che $xn \neq n$. Se poniamo $t = xn - n$ si ha $\Phi c + n = \Phi c + xn$ e dunque $\Phi c = \Phi c + t$; detta poi h la caratteristica di t, si ha $\Phi c = \Phi c + t = \Phi c = \Phi c + 2t = ... = \Phi c = \Phi c + (h - 1)t$, e dunque $\Phi c = \Phi c + \langle t \rangle$, dove $\langle t \rangle$ è il sottogruppo generato da t. Poichè $\Phi c + \langle t \rangle$ è unione di laterali di $\langle t \rangle$, e ciascuno di questi ha ordine h, deve essere $|\Phi c| = |\Phi c + \langle t \rangle| = wh$, con $w \in \mathbb{N}$. Detto $v = |N|$, si ha, poichè Φc è un sottogruppo di $N \backslash \{0\}$, $wh = |\Phi c|$ $|v - 1$, ed inoltre $h|v$. Quindi $h|(v, v - 1) = 1$, ed allora $h = |\langle t \rangle| = 1$ e $t = 0$, e dunque $xn = n$, col che siamo giunti ad una contraddizione. □

L'importanza dei BIBD nella teoria dei quasianelli è dovuta al fatto che se N è un quasianello finito la struttura di incidenza $(N, \mathcal{B}^*_\Phi, \in)$ è un BIBD, in virtù del seguente teorema, di cui omettiamo la dimostrazione.

Teorema 3.5. ***(Clay)***
Se (N, Φ) è una coppia di Ferrero, con $|N| = v < \infty$ e $|\Phi| = k$, allora $(N, \mathcal{B}^*_\Phi, \in)$ è un BIBD di parametri v, $|\mathcal{B}^*_\Phi| = \frac{v(v-1)}{k}$, k, $r = v - 1$, $\lambda = k - 1$.

Nel seguito sarà utile il seguente

Lemma 3.6. *Sia (N, Φ) una coppia di Ferrero, con $|N| = v < \infty$. Consideriamo il BIBD $(N, \mathcal{B}^*_\Phi, \in)$. Si ha $\forall \{x, y, z\} \subset N \qquad [x, y, z] = [0, y - x, z - x]$.*

3.3 Quasianelli e BIBD circolari

Introduciamo ora la proprietà di circolarità, che sarà fondamentale per la teoria che tratteremo nei capitoli 5 e 6.

Definizione 3.7. *Siano N un **quasianello planare** e Φ il suo gruppo di Clay. Il quasianello N si dice **circolare** se, considerando la struttura d'incidenza $(N, \mathcal{B}^*_\Phi, \in)$, si ha, $\forall \{x, y\} \subset N$, $[x, y] \geq 2$ e $\forall \{x, y, z\} \subset N$ $[x, y, z] \leq 1$.*

Definizione 3.8. *Se $(V, \mathcal{B}, \in)$ è un **BIBD** di parametri v, n, k, r, λ tale che $\lambda \geq 2$ e $\forall \{p, q, s\} \subset V \quad [p, q, s] \leq 1$, $(V, \mathcal{B}, \in)$ si dice **BIBD circolare** e gli elementi di $\mathcal{B}$ si dicono **cerchi.***

La proprietà fondamentale di un BIBD circolare è che due blocchi si intersecano in 2, 1 o 0 punti, come succede per i cerchi nel piano euclideo, da cui il nome circolare per il BIBD e cerchi per i blocchi.

E' immediato fare la seguente

Osservazione 3.9. *La circolarità di un quasianello planare N è una propietà che dipende solo dal suo gruppo additivo $[N,+]$ e dal suo gruppo di Clay Φ; quindi due quasianelli cui sia associata la stessa coppia di Ferrero o sono entrambi circolari o nessuno dei due lo è. Inoltre, in virtù del teorema di Clay (3.5) si ha che se N è un quasianello planare finito, N è circolare se e solo se il BIBD $(N, \mathcal{B}_{\Phi^*}, \in)$ è circolare.*

Se N è un quasianello circolare e $B = \Phi r + c \in \mathcal{B}_{\Phi^*}$, c si dice *centro* ed r *raggio* del cerchio B.

La circolarità di un quasianello impone un limite alla cardinalità del suo gruppo di Clay, come mostra il seguente teorema.

Teorema 3.10. *Siano $[N,+,\cdot]$ un quasianello planare circolare finito, Φ il suo gruppo di Clay, $|N| = v$ e $|\Phi| = k$; allora risulta*

$$k \leq \frac{3+\sqrt{4v-7}}{2} \tag{3.1}$$

Dimostrazione. Per il Teorema di Clay $(V, \mathcal{B}^*_\Phi, , \in)$ è un BIBD tale che $|\mathcal{B}^*_\Phi| = \frac{v(v-1)}{k}$ e $\forall B \in \mathcal{B}^*_\Phi, \quad |B| = |\Phi| = k$. Ogni elemento di $\mathcal{B}^*_\Phi$ ha $\frac{k(k-1)(k-2)}{6}$ sottoinsiemi di 3 elementi; dunque in tutto gli elementi di $\mathcal{B}^*_\Phi$ contengono $\frac{v(v-1)k(k-1)(k-2)}{6}$ sottoinsiemi di 3 elementi (contando ciascuno di essi in base al numero di volte che compare come sottoinsieme di qualche elemento di $\mathcal{B}_{\Phi^*}$). Il quasianello N ha $\frac{v(v-1)(v-2)}{6}$ sottoinsiemi di 3 elementi, ciascuno dei quali è contenuto in al più un elemento di $\mathcal{B}^*_\Phi$, per cui deve essere $\frac{v(v-1)k(k-1)(k-2)}{6} \leq \frac{v(v-1)(v-2)}{6}$ da cui $k^2 - 3k - v + 4 \leq 0$ e dunque $k \leq \frac{3+\sqrt{4v-7}}{2}$. □

Questo teorema è utile dal punto di vista computazionale, perchè permette di migliorare l'efficienza di programmi per determinare la circolarità di un quasianello finito. Infatti i quasianelli che non soddisfino la condizione 3.1 (che è molto facile da testare) vengono esclusi a priori.

3.4 Quasianelli planari da spazi vettoriali e criterio di circolarità

La costruzione del seguente teorema è un caso particolare di quella del teorema 1.7. Questa permette però di ottenere quasianelli planari.

Teorema 3.11. ***(Costruzione di quasianelli planari da spazi vettoriali)***
Siano V uno spazio vettoriale sul campo F, $f : V \to F$ tale che $|f(V)| \geq 3$ e, $\forall y \in V$, $\forall a \in f(V)$, $f(ay) = af(y)$. Sia, $\forall a \in F$, $\psi_a \in End(V)$ tale che $\forall y \in V$ $\psi_a(y) = ay$, $\varphi : V \to End(V^+)$ tale che $\forall y \in V$ $\varphi_y = \psi_{f(v)}$ e $\forall y, z \in V$ $y \cdot z = \varphi_y z$: allora la struttura $[V,+,\cdot]$ è un quasianello planare, con gruppo di Clay $\Phi_f = \{\psi_a \mid a \in f(V)\setminus\{0\}\}$ isomorfo a $f(V)\setminus\{0\} = K \lessdot F^*$.

Dimostrazione. Basta dimostrare che la funzione φ soddisfa alle ipotesi del teorema 1.7 e cioè $\forall y, z \in V \ \varphi_y \varphi_z = \varphi_{\varphi_y z}$.
Infatti $\forall y, z \in V \ \varphi_y \varphi_z = \psi_{f(v)} \psi_{f(z)} = \psi_{f(v)f(z)} = \psi_{f(f(v)z)} = \varphi_{f(v)z} = \varphi_{\varphi_v z}$ e dunque $[V, +, \cdot]$ è un quasianello. Osserviamo che in base alla definizione $\forall y, z \in V \ y \cdot z = f(y)z$. Mostriamo ora che V è planare.

Dobbiamo mostrare che, $\forall v, w, z \in V$ tali che $\varphi_v \neq \varphi_w$, l'equazione

$$vx = wx + z \qquad (*)$$

ha un'unica soluzione in V.

Poichè si ha $\psi_{f(v)} = \varphi_v \neq \varphi_w = \psi_{f(w)}$ allora $f(v) \neq f(w)$ così $f(v) - f(w) \in F^*$. Inoltre x è soluzione di $(*)$ se e solo se $f(v)x = f(w)x + z$ se e solo se $x = (f(v) - f(w))^{-1} z$, così N soddisfa allora alla propietà di planarità.

E' banale osservare che il semigruppo di Clay di N è $\tilde{\Phi}_f = \{\psi_a \,|a \in f(V)\}$ e dunque $\left|\tilde{\Phi}\right| = |f(V)| \geq 3$. Dunque N è planare ed ha come gruppo di Clay $\Phi_f = \tilde{\Phi}_f \backslash \{0\} = \{\psi a \,|a \in f(V) \backslash \{0\}\}$. Rimane da osservare che la $\theta : f(V) \backslash \{0\} \to \Phi_f$ tale che $\forall \lambda \in f(V) \backslash \{0\} \quad \theta(\lambda) = \psi_\lambda$ è un isomorfismo di gruppi. □

In particolare, se $[N, +, \cdot]$ è un quasianello planare field-generated a partire dalla coppia di Ferrero (F, K), dove F è un campo e $K \lessdot F^*$, N può essere ottenuto con la costruzione del teorema precedente considerando F come F-spazio vettoriale. Infatti ponendo $f : F \to F$ tale che, $\forall a \in F$, $f(a) = \lambda$, con $\varphi_a = \psi_\lambda$ si ha, in base alla definizione di f, che $\forall a \in F \ \varphi_a = \psi_{f(a)}$ e $\forall y, z \in F \quad f(y)z = \varphi_y z = y \cdot z$. Allora $\forall y, z \in F \quad \psi_{f(f(y)z)} = \psi_{f(\varphi_y z)} = \varphi_{\varphi_y z} = \varphi_y \varphi_z = \psi_{f(v)} \psi_{f(z)} = \psi_{f(v)f(z)}$ e dunque $f(f(y)z) = f(v)f(z)$; è inoltre immediato osservare che $f(V) = K \cup \{0\}$ e dunque $|f(V)| = |K \cup \{0\}| \geq 3$.

Dunque la f così definita soddisfa alle ipotesi del teorema precedente, ed è immediato constatare che applicando la costruzione ivi descritta si riottiene il quasianello di partenza.

Il seguente teorema fornisce una condizione necessaria e sufficiente di facile verifica pratica affinchè i quasianelli planari così costruiti siano circolari

Teorema 3.12. ***(Criterio di circolarità per quasianelli costruiti su spazi vettoriali)***

Sia V uno spazio vettoriale sul campo F, $f : V \to F$ tale che $|f(V)| \geq 3$ e $\forall y \in V, \forall a \in f(V)$, $f(ay) = af(y)$. Consideriamo il quasianello $[V, +, \cdot]$ ottenuto da V e f applicando la costruzione del teorema 3.11 e sia $\Phi_f = \{\psi a \,| \quad a \in f(V) \backslash \{0\}\}$ il suo gruppo di Clay. Supponiamo che, $\forall a, b, c \in V$, $\Phi_f a = \Phi_f b + c \Longrightarrow c = 0$ e poniamo $K = f(V) \backslash \{0\}$. Allora in $(V, \mathcal{B}^*_{\Phi_f}, \in)$ sono equivalenti:

1. $\forall \{x, y, z\} \subset V \quad [x, y, z] \leq 1$.

2. *$\forall a, b, c, d \in K \setminus \{1\}$ tali che $a \neq d$, $c \neq b$, $a \neq c$ e $b \neq d$ si ha $(a-1)(b-1) \neq (c-1)(d-1)$*

Dimostrazione. Osserviamo che $\forall a, b \in V \quad \Phi_f a + b = Ka + b$.

$2 \Longrightarrow 1$

Per assurdo esistano $\{x, y, z\} \subset V$ distinti tale che $[x, y, z] \geq 2$; ponendo $u = y - x, v = z - x$ si ha $u \neq v$ e $[0, u, v] = [0, y - x, z - x] = [x, y, z] \geq 2$ (vedi 3.6). Poichè i blocchi che contengono 0 sono tutti e soli quelli del tipo $\Phi_f a - a$, con $a \in V \setminus \{0\}$, $\exists w, \tilde{w} \in V \setminus \{0\}$ t.c. $w \neq \tilde{w}$ e $\{u, v\} \subset (Kw - w) \cap (K\tilde{w} - \tilde{w})$, e dunque $\exists a, b, c, d$ t.c. $u = aw - w = d\tilde{w} - \tilde{w}$ e $v = cw - w = b\tilde{w} - \tilde{w}$. Poichè $u \neq v$ e $w \neq \tilde{w}$, deve essere $a \neq d, c \neq b, a \neq c$ e $b \neq d$. E' dunque $u = (a-1)w = (d-1)\tilde{w}$ e $v = (c-1)w = (b-1)\tilde{w}$ e dunque $w = (b-1)(c-1)^{-1}\tilde{w} = (d-1)(a-1)^{-1}\tilde{w}$, cioè $(a-1)(b-1) = (c-1)(d-1)$, contraddicendo la (2).

$1 \Rightarrow 2$

Per assurdo esistano $a, b, c, d \in K \setminus \{1\}$ t.c. $a \neq d, c \neq b, a \neq c$ e $b \neq d$ e $(a-1)(b-1) = (c-1)(d-1)$. Allora $(d-1)(a-1)^{-1} = (b-1)(c-1)^{-1}$. Sia $\tilde{w} \in V$ e $w = (d-1)(a-1)^{-1}\tilde{w} = (b-1)(c-1)^{-1}\tilde{w}$. Poichè $a \neq d$ è $w \neq \tilde{w}$. Poniamo $u = aw - w = d\tilde{w} - \tilde{w} \in (Kw - w) \cap (K\tilde{w} - \tilde{w})$ e $v = cw - w = b\tilde{w} - \tilde{w} \in (Kw - w) \cap (K\tilde{w} - \tilde{w})$; poichè $a \neq c$ è $u \neq v$. Osserviamo che se fosse $Kw - w = K\tilde{w} - \tilde{w}$ sarebbe $Kw = K\tilde{w} + (w - \tilde{w})$ e dunque, per ipotesi, $w = \tilde{w}$; dunque $Kw - w \neq K\tilde{w} - \tilde{w}$ e $\{u, v\} \subset (Kw - w) \cap (K\tilde{w} - \tilde{w})$, da cui $[0, u, v] \geq 2$, contraddicendo la (1).

□

Si ha immediatamente il

Corollario 3.13. *Se V è un F-spazio vettoriale, $f, g : V \to F$ soddisfano le ipotesi del teorema precedente, $g(V) \subset f(V)$, e, in $(V, \mathcal{B}^*_{\Phi_f}, \in)$, $\forall \{x, y, z\} \subset V$, $[x, y, z] \leq 1$, allora anche in $(V, \mathcal{B}^*_{\Phi_f}, \in)$, $\forall \{x, y, z\} \subset V$, $[x, y, z] \leq 1$.*

Di particolare importanza per il seguito è il seguente

Corollario 3.14. *Siano V uno spazio vettoriale finito sul campo F, $f : V \to F$ soddisfacente alle ipotesi del teorema 3.11 e tale che $|f(V)| \geq 4$, $[V, +, \cdot]$ il quasianello planare ottenuto con la costruzione di tale teorema e Φ_f il suo gruppo di Clay. Allora sono equivalenti*

1. *$[V, +, \cdot]$ è circolare*
2. *$(V, \mathcal{B}_{\Phi^*_f}, \in)$ è BIBD circolare*

3. $\forall a, b, c, d \in K \setminus \{1\}$ *tali che* $a \neq d$, $c \neq b$, $a \neq c$ *e* $b \neq d$ *si ha* $(a-1)(b-1) \neq (c-1)(d-1)$

Dimostrazione. $1 \Leftrightarrow 2$ segue subito dall'osservazione 3.9.

$1 \Leftrightarrow 3$ segue subito dal teorema precedente, una volta osservato che l'ipotesi che $\forall a, b, c \in V \ \Phi_f a = \Phi_f b + c$ se e solo se $c = 0$ è garantita dall'essere $|V| < \infty$ (vedi teorema di Clay e teorema 3.4). □

E' bene notare che in particolare il precedente corollario si applica ad un quasi-anello field-generated su un campo finito.

Il criterio di circolarità appena dimostrato ha particolare importanza dal punto di vista computazionale, perchè fornisce un algoritmo per la determinazione della circolarità molto più efficiente della sistematica verifica che ogni insieme di tre punti appartenga al più ad un blocco. In appendice riportiamo il programma Matlab `iscircular` che sulla base di tale teorema è in gado di determinare per quali valori di k e p il BIBD $(\mathbb{Z}_p, \Phi_k, \in)$ è circolare.

Capitolo 4

Grafi, cerchi e sistemi di cerchi

In questo capitolo supporremo sempre (N, Φ) una coppia di Ferrero tale che $(N, \mathcal{B}^*_\Phi, \in)$ sia un BIBD circolare.

4.1 Grafi

Introduciamo ora le principali nozioni relative alla teoria dei grafi.

Definizione 4.1. *Un **grafo** è una coppia $\Gamma = (V, \mathcal{E})$ dove V è un insieme ed $\mathcal{E} \subset \wp(V)$ tale che $\forall l \in \mathcal{E}$ $|l| = 2$.*

Se $\Gamma = (V, \mathcal{E})$ è un grafo, gli elementi di V si dicono *vertici,* se $\{u, v\} \in \mathcal{E}$ si dice che nel grafo c'è un lato che collega i vertici u e v; si dice *grado di un vertice* v e si denota con $\deg(v)$ il numero di lati che hanno v come vertice. Un grafo si dice *regolare di grado n* se tutti i suoi vertici hanno grado n. L'insieme dei vertici di un grafo Γ si denota con $\Gamma(V)$, l'insieme dei lati con $\mathcal{E}(V)$. Due grafi $\Gamma_i = (V_i, \mathcal{E}_i)$ $i = 1, 2$ si dicono isomorfi se c'è una bigezione $f : V_1 \to V_2$ tale che $\forall u, v \in V_1$ distinti $\{u, v\} \in \mathcal{E}_1 \iff \{f(u), f(v)\} \in \mathcal{E}_2$.

Un *cammino* in un grafo è una sequenza di vertici $(v_1, v_2, .., v_n)$ tale che due verici consecutivi della sequenza siano collegati da un lato nel grafo. Se $(v_1, v_2, .., v_n)$ è un cammino, i vertici $v_1, v_2, .., v_n$ si dicono nodi del cammino, v_1 si dice estremo iniziale e v_n estremo finale, il cammino si dice chiuso se estremo iniziale e finale coincidono.

Un *ciclo* è un cammino chiuso in cui tutti i nodi sono distinti. Un grafo si dice *connesso* se per ogni coppia di vertici (u, v), con $u \neq v$ esiste un cammino che ha u e v come estremo inziale e finale.

Un grafo $\tilde{\Gamma}$ si dice sottografo di un grafo Γ se $V(\tilde{\Gamma}) \subset V(\Gamma)$ e $\mathcal{E}(\tilde{V}) \subset \mathcal{E}(V)$. Due sottografi Γ_1 e Γ_2 di un grafo si dicono disgiunti se $\mathcal{E}(\Gamma_1) \cap \mathcal{E}(\Gamma_2) = \varnothing$. Un sottografo $\tilde{\Gamma}$ di Γ si dice *spanning* se $V(\tilde{\Gamma}) = V(\Gamma)$. Un grafo si dice *hamiltoniano* se ha un sottografo che sia un ciclo spanning, cioè ammette un cammino chiuso che passa per tutti i vertici una ed una sola volta.

Un *grafo ciclico su n vertici* è un grafo hamiltoniano regolare di grado 2; tutti i grafi ciclici sono isomorfi e si indicano con C_n. Un grafo si dice completo se ogni coppia di vertici è collegata da un lato; tutti i grafi completi con n vertici sono isomorfi e si indicano con K_n.

Nel seguito considereremo grafi con diversi tipi di lati; diamo allora la seguente

Definizione 4.2. *Sia E un insieme; un **grafo etichettato** con etichette in E è una coppia $(V, \mathcal{E})$ dove V è un insieme e $\mathcal{E} \subset \{l \subset V \mid |l| = 2\} \times E$.*

Se $(V, \mathcal{E})$ è un grafo etichettato con etichette in E, gli elementi di V si dicono vertici e se $(\{u, v\}, e) \in \mathcal{E}$ diciamo che nel grafo c'è un lato etichetato con e che collega u e v. Notazioni e terminologia per i grafi etichettati sono del tutto analoghe a quelle per i grafi non etichettati.

Dati due grafi, possiamo ottenere da esse un nuovo grafo in vari modi:

Definizione 4.3. *Se $\Gamma_i = (V_i, \mathcal{E}_i)$ $i = 1, 2$ sono due grafi tali che $V_1 = V_2 = V$, il grafo $(V, \mathcal{E}_1 \cup \mathcal{E}_2)$ si dice unione di Γ_1 e Γ_2 e si denota con $\Gamma_1 \vee \Gamma_2$.*

Se $\Gamma_i = (V_i, \mathcal{E}_i)$ $i = 1, 2$ sono due grafi tali che $V_1 \cap V_2 = \varnothing$, il grafo $(V_1 \cup V_2, \mathcal{E}_1 \cup \mathcal{E}_2)$ si dice unione disgiunta di Γ_1 e Γ_2 e si denota con $\Gamma_1 \sqcup \Gamma_2$.

E' importante notare che unione ed unione disgiunta sono *due operazioni diverse.*

Un modo per caratterizzare un grafo è scriverlo come unione di sottografi semplici, di cui si conosca la struttura. A tal proposito introduciamo il seguente concetto.

Definizione 4.4. *Siano k,j due interi $k \geq 3$ e $1 \leq j \leq k$. Si dice j-esimo **k-grafo di base** il grafo Δ_j^k tale che $V(\Delta_j^k) = \mathbb{Z}_k$ e $\mathcal{E}(\Delta_j^k) = \{\{s, t\} \in \wp(\mathbb{Z}_k) \mid s - t = j\}$.*

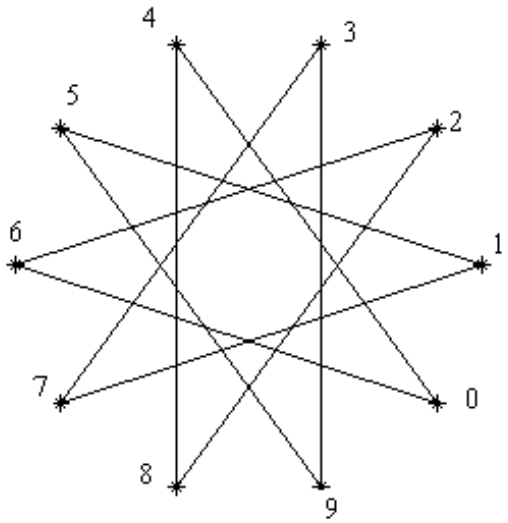


FIGURA 4.1. Quarto 10-grafo di base

E' immediato constatare che, $\forall k \geq 3$, $\forall j \in I_k$, $\Delta_j^k = \Delta_{k-j}^k$.

Osserviamo che per ogni k pari lo j-esimo k-grafo di base con $j = \frac{k}{2}$ è un grafo su k vertici regolare di grado uno, tale che per ogni $s \in \mathbb{Z}_k$ l'unico lato che ha s come vertice è $\left\{s, s + \frac{k}{2}\right\}$.

Per k dispari o per k pari e $j \neq \frac{k}{2}$ il j-esimo k-grafo di base è un grafo regolare di grado due.

Infatti $\forall s \in \mathbb{Z}_k$ gli unici lati che hanno s come vertice sono $\{s, s+j\}$ e $\{s, s-j\}$ e sono distinti perchè se $s+j \equiv_k s-j$ allora $2j \equiv_k 0$ dunque $k|2j$ e $k = 2j$ (perchè $1 \leq j \leq k-1$).

Inoltre $\forall n \in \mathbb{Z}_k$ la $\alpha_n : \mathbb{Z}_k \to \mathbb{Z}_k$ tale che $\alpha_n(x) = x + n$ induce un isomorfismo di Δ_j^k in sé; infatti $\forall s, t \in \mathbb{Z}_k \{s, t\} \in \mathcal{E}(\Delta_j^k)$ se e solo se $s - t = j$, cioè se e solo se $(s+n) - (t+n) = j$. In base alla definizione di α_n ciò accade se e solo se $\alpha_n(s) - \alpha_n(t) = j$, cioè se e solo se $\{\alpha_n(s), \alpha_n(t)\} \in \mathcal{E}(\Delta_j^k)$.

I grafi di base possono a loro volta essere scritti come *unione disgiunta* di grafi più semplici, come dimostra il seguente

Teorema 4.5. *Siano k, j interi $k \geq 3$, $1 \leq j \leq k$ e sia $l = M.C.D.(k, j)$. Allora Δ_j^k è isomorfo all'unione disgiunta di l copie del grafo ciclico su $\frac{k}{l}$ vertici $C_{\frac{k}{l}}$.*

Dimostrazione. E' $\forall n \in \mathbb{N}$, $nj \equiv 0 \mathrm{mod} k$ se e solo se $k|nj$ se e solo se, poichè $l = M.C.D.(k, j)$, $\frac{k}{l}|n$; dunque $\frac{k}{l} = \min\{n \in \mathbb{N} | \quad nj \equiv 0 \mathrm{mod} k\}$ e $\sigma_0 = (0, j, 2j, .., (\frac{k}{l} - 1)j)$ è ciclo in Δ_j^k. Tenendo conto che, $\forall h \in I_{l-1}^0$, la α_h definita in precedenza è un isomorfismo di Δ_j^k in sé, si ha che, $\forall h \in I_{l-1}^0$, $\sigma_h = (h, h+j, h+2j, .., h+(\frac{k}{l}-1)j)$ è un ciclo in Δ_j^k. Mostriamo che tali cicli non hanno vertici in comune: poichè in un grafo regolare di grado 1 o 2, come Δ_j^k, due cicli o sono disgiunti o coincidono, basta mostrare che i cicli σ_h $h \in I_{l-1}^0$ sono distinti. Poichè, $\forall h, h' \in I_{l-1}^0$ $\sigma_h = \sigma_{h'}$ se e solo se $\sigma_{h-h'} = \sigma_0$, è sufficiente verificare che $\forall h \in I_{l-1}^0$ $\sigma_h = \sigma_0 \Rightarrow h = 0$. Sia quindi $h \in I_{l-1}^0$ e $\sigma_h = \sigma_0$, allora $\exists s \in I_{\frac{k}{l}-1}^0$ tale che $h + sj \equiv_k 0$, allora $l|k|h + sj$ e $l|j$, dunque $l|h$ e $h = 0$. □

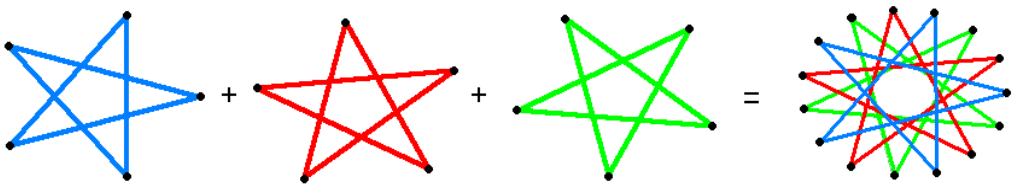


FIGURA 4.2. $C_5 \sqcup C_5 \sqcup C_5 = \Delta_6^{15}$

4.2 Cerchi e sistemi di cerchi

Ricordiamo che se, come stiamo supponendo, $(N, \mathcal{B}_\Phi^*, \in)$ è un BIBD circolare, gli elementi di $\mathcal{B}_\Phi^*$ si dicono cerchi. Definiamo sull'insieme dei cerchi la relazione.

$$\forall\ \Phi a + b, \Phi c + d \in \mathcal{B}_\Phi^* \quad \Phi a + b \equiv \Phi c + d \text{ se e solo se } (\Phi a = \Phi c \wedge \Phi b = \Phi d)$$

E' immediato osservare che la relazione sopra definita è di equivalenza.

Definizione 4.6. *Se $r, c \in N\setminus\{0\}$ si definisce* ***sistema di cerchi*** *di raggio principale c raggio secondario r nel BIBD circolare $(N, \mathcal{B}^*_\Phi, \in)$ la famiglia di cerchi*

$$E^r_c = [\Phi r + c]_{\equiv} = \{\Phi r + \varphi c \,|\varphi \in \Phi\} = \{\varphi(\Phi r + c) \,|\varphi \in \Phi\}$$

E^r_c è l'insieme dei cerchi di raggio r che hanno per centro un elemento del cerchio di centro 0 e raggio Φc.

E' immediato dalla definizione che $\forall\, r, c \in N\setminus\{0\}$, $\forall \varphi \in \Phi$, $E^r_c = E^r_{\varphi c}$ e $|E^r_c| = |\Phi|$; inoltre se $|N| = v < \infty$ e $|\Phi| = k$ $\forall r \in N\setminus\{0\}$ $|\{E^r_c \,|c \in N\setminus\{0\}\}| = \left(\frac{v-1}{k}\right)^2$.

Supponiamo da ora in avanti $|\Phi| = k < \infty$; i cerchi risulteranno allora insiemi finiti di k elementi.

Siamo interessati a studiare le proprietà di intersezione dei sistemi di cerchi; a questo scopo è utile associare a ciascun sistema di cerchi una sequenza nel seguente modo. Scegliamo un ordinamento per Φ: $\Phi = \{\varphi_1, \varphi_2, ..., \varphi_{k-1}, \iota\}$ poniamo

$$\forall r, c \in N\setminus\{0\}, \forall j \in I_{k-1} \quad s(r, c, i) = |(\Phi r + c) \cap (\Phi r + \varphi_i c)| \tag{4.1}$$

Osserviamo che, poichè in un BIBD circolare due cerchi hanno al più due punti di intersezione, $s(r, c, i) \in \{0, 1, 2\}$. La sequenza $(s(r, c, i))_{i\in I_{k-1}}$ è detta sequenza associata al sistema di cerchi di raggio minore r e raggio maggiore c. E' bene notare che se consideriamo due diversi ordinamenti per Φ : $\Phi = \{\varphi_1, \varphi_2, ..., \varphi_{k-1}, \iota\} = \left\{\varphi_{\beta(1)}, \varphi_{\beta(2)}, ..., \varphi_{\beta(k-1)}, \iota\right\}$ con $\beta \in S_{k-1}\setminus\{\iota\}$ otteniamo *due sequenze associate diverse,* la seconda delle quali si ottiene dalla prima permutandone gli elementi secondo β.

Osserviamo che, $\forall i \in I_{k-1}$, $\forall r, c \in N\setminus\{0\}, \forall \psi \in \Phi$

$$s(r, c, i) = s(\psi r, c, i)$$

e

$$\text{se } \psi^{-1}\varphi_i\psi = \varphi_{\beta(i)} \text{ allora } s(r, \psi c, i) = s(r, c, \beta(i))$$

Infatti

$$\begin{aligned} s(\psi r, c, i) &= |(\Phi r + \psi c) \cap (\Phi r + \varphi_i \psi c)| = \psi(\Phi r + c) \cap \psi(\Phi r + \psi^{-1}\varphi_i\psi c) = \\ &= \left|\psi((\Phi r + c) \cap (\Phi r + \psi^{-1}\varphi_i\psi c))\right| = \left|(\Phi r + c) \cap (\Phi r + \psi^{-1}\varphi_i\psi c)\right| = \\ &= \left|(\Phi r + c) \cap (\Phi r + \varphi_{\beta(i)} c)\right| = s(r, c, \beta(i)) \end{aligned}$$

Dunque, in particolare, se Φ è abeliano, $\forall\, r, c \in N\setminus\{0\}$, $\forall \psi \in \Phi$,

$$s(r, \psi c, i) = s(r, c, i)$$

Se, in aggiunta, Φ è ciclico con generatore φ si ha, $\forall i \in I_{k-1}$,

$$\begin{aligned} s(r, c, k-i) &= \left|(\Phi r + c) \cap (\Phi r + \varphi^{k-i} c)\right| = \left|\varphi^{-i}(\Phi r + \varphi^i c) \cap (\Phi r + \varphi^k c)\right| = \\ &= \left|\varphi^{-i}(\Phi r + \varphi^i c) \cap (\Phi r + c)\right| = \left|(\Phi r + \varphi^i c) \cap (\Phi r + c)\right| = s(r, c, i) \end{aligned}$$

La configurazione più semplice riguardo alle mutue intersezioni dei cerchi di un sistema E_c^r è che siano tutti disgiunti, cioè che sia identicamente nulla la sequenza $(s(r,c,i))_{i\in I_{k-1}}$. Diamo la seguente

Definizione 4.7. *Se un sistema di cerchi E_c^r è tale che i suoi elementi sono a due a due disgiunti, esso si dice* ***toro*** *di raggio minore r e raggio maggiore c.*

4.3 Grafi associati a sistemi di cerchi

Le possibili configurazioni di mutue intersezioni dei cerchi in un sistema sono numerose e complicate. Un valido aiuto nel loro studio è quello di associare ad esse grafi che ne permettano anche una visualizzazione concreta.

Definizione 4.8. *Se E_c^r è un sistema di cerchi del BIBD circlare $(N, \mathcal{B}_\Phi^*, \in)$, diciamo* ***grafo associato a*** *E_c^r il grafo etichettato in $\mathbb{Z}_2$ $\Gamma(E_c^r)$ tale che*

$$V(\Gamma(E_c^r)) = \Phi c$$

$$\begin{aligned}\mathcal{E}(\Gamma(E_c^r)) &= \{(\{a,b\},0) \mid \quad a,b \in \Phi c \quad |(\Phi r + a) \cap (\Phi r + b)| = 2\} \\ &\quad \cup \{(\{a,b\},1) \mid \quad a,b \in \Phi c \quad |(\Phi r + a) \cap (\Phi r + b)| = 1\}.\end{aligned}$$

Dunque i vertici del grafo sono i centri dei cerchi di E_c^r, e cioè gli elementi del cerchio di centro 0 e raggio c; due vertici sono collegati da un lato etichettato con 0 se i cerchi del sistema che li hanno come centri hanno come intersezione due punti, mentre sono collegati da un lato etichettato con 1 se i cerchi del sistema che li hanno come centri hanno come intersezione un punto. I lati etichettati con 0 si dicono lati pari, i lati etichettati con 1 si dicono lati dispari. Se $a \in V(\Gamma(E_c^r)) = \Phi c$ si denota con $e(a)$ il numero di lati pari che hanno a come vertice e con $o(a)$ il numero di lati dispari che hanno a come vertice.

Osservazione 4.9. *La conoscenza della sequenza $(s(r,c,i))_{i\in I_{k-1}}$ definita come in 4.1 permette di costruire il grafo associato a E_c^r, perchè risulta*

$$\begin{aligned}\mathcal{E}(\Gamma(E_c^r)) &= \left\{\left(\left\{a, \varphi_j a\right\},0\right) \mid a \in \Phi c,\ s(r,c,j) = 2\right\} \\ &\quad \cup \left\{\left(\left\{a, \varphi_j a\right\},0\right) \mid a \in \Phi c,\ s(r,c,j) = 1\right\}\end{aligned}$$

In particolare

$$\forall a \in \Phi c \quad e(a) = |\{j \in I_{k-1} \,|s(r,a,j) = 2\}|, \quad o(a) = |\{j \in I_{k-1} \,|s(r,a,j) = 1\}|$$

Poichè, come precedentemente osservato, $\forall a,b \in \Phi c$ $(s(r,b,i))_{i\in I_{k-1}}$ si ottiene da $(s(r,a,i))_{i\in I_{k-1}}$ permutandone gli elementi, si ha, $\forall a,b \in \Phi c$, $e(a) = e(b) = e$, $o(a) = o(b) = o$ e dunque anche $\deg(a) = o(a) + e(a) = o(b) + e(b) = \deg(b)$, cioè $\Gamma(E_c^r)$ è n-grafo regolare.

I grafi associati a sistemi di cerchi sono simmetrici per rotazioni, nel senso che ogni $\psi \in \Phi$ induce un isomorfismo di $\Gamma(E_c^r)$ in sè.

Infatti $\psi : \Phi c = V(\Gamma(E_c^r)) \to V(\Gamma(E_c^r)) = \Phi c$ è una bigezione, inoltre $\forall a, b \in \Phi c$

$$\begin{aligned} |(\Phi r + \psi a) \cap (\Phi r + \psi b)| &= |\psi(\Phi r + a) \cap \psi(\Phi r + b)| = \\ &= |\psi\left((\Phi r + a) \cap (\Phi r + b)\right)| = |(\Phi r + a) \cap (\Phi r + b)| \end{aligned}$$

e dunque

$$\begin{aligned} (\{a, b\}, 0) &\in \mathcal{E}(\Gamma(E_c^r)) \iff (\{\psi a, \psi b\}, 0) \in \mathcal{E}(\Gamma(E_c^r)) \\ (\{a, b\}, 1) &\in \mathcal{E}(\Gamma(E_c^r)) \iff (\{\psi a, \psi b\}, 1) \in \mathcal{E}(\Gamma(E_c^r)) \end{aligned}$$

Se poi Φ è ciclico con generatore φ, tali grafici hanno anche simmetrie assiali, nel senso che $\forall a \in \Phi c$ la $\beta_a : \Phi c \to \Phi c$ tale che, $\forall j \in I_{k-1}^0$, $\beta_a(\varphi^j a) = \varphi^{k-j} a$ induce un isomorfismo di $\Gamma(E_c^r)$ in sé; infatti β_a è una bigezione ed inoltre $\forall l, s \in I_{k-1}^0$

$$\begin{aligned} & \left|(\Phi r + \beta_a(\varphi^l a)) \cap (\Phi r + \beta_a(\varphi^s a))\right| \\ = & \left|(\Phi r + \varphi^{k-l} a) \cap (\Phi r + \varphi^{k-s} a)\right| \\ = & \left|(\Phi r + \varphi^{k-l} a) \cap (\Phi r + \varphi^{k-s} a)\right| \\ = & \left|\varphi^{k-l-s}\left((\Phi r + \varphi^s a) \cap (\Phi r + \varphi^l a)\right)\right| \\ = & \left|(\Phi r + \varphi^s a) \cap (\Phi r + \varphi^l a)\right| \end{aligned}$$

L'importanza dei grafi di base per descrivere i grafi associati a sistemi di cerchi è messa in luce dal seguente teorema.

Teorema 4.10. *Se N è abeliano, Φ ciclico di ordine k, ed E_c^r un sistema di cerchi in $(N, \mathcal{B}_\Phi^*, \in)$, allora $\Gamma(E_c^r)$ o è nullo o è unione di sottografi spanning disgiunti, ciascuno dei quali isomorfo ad un k-grafo di base.*

Dimostrazione. Poniamo per semplicità $\Gamma = \Gamma(E_c^r)$, $V = V(\Gamma(E_c^r))$, $\mathcal{E} = \mathcal{E}(\Gamma(E_c^r))$; sia inoltre φ un generatore di Φ. Si ha

$$\begin{aligned} \mathcal{E}(\Gamma(E_c^r)) &= \left\{\left(\left\{a, \varphi^j a\right\}, 0\right) \mid a \in \Phi c,\ s(r, c, i) = 0\right\} \\ &\quad \cup \left\{\left(\left\{a, \varphi^j a\right\}, 1\right) \mid a \in \Phi c\ s(r, c, i) = 2\right\} \end{aligned}$$

Sia,

$$\forall t \in I_{k-1},\ \mathcal{E}_t = \begin{cases} \varnothing & \text{se } s(r, c, i) = 0 \\ \{(\{a, \varphi^t a\}, 1) \mid \quad a \in \Phi c\} & \text{se } s(r, c, i) = 1 \\ \{(\{a, \varphi^t a\}, 0) \mid \quad a \in \Phi c\} & \text{se } s(r, c, i) = 2 \end{cases}$$

è chiaro che $\{\mathcal{E}_t |\ t \in \mathbb{N}, 1 \le t \le \left[\frac{k}{2}\right]\}$ è una partizione di $\mathcal{E}$; dunque se consideriamo i sottografi $\Gamma_t = (V, \mathcal{E}_t)$ di Γ per $1 \le t \le \left[\frac{k}{2}\right]$ e $s(c, r, t) \neq 0$, abbiamo che tali grafi sono

disgiunti e non vuoti e la loro unione è Γ. Mostriamo che ciascuno di essi è isomorfo a Δ_t^k.

Sia $\theta : V \to \mathbb{Z}_k$ tale che $\theta(\varphi^j a) = j \ \forall \in I_{k-1}^0$; θ è una bigezione. Inoltre, $\forall b, c \in \Phi c$, b e c sono collegati da un lato in Γ_t, se e solo se $c = \varphi^t b$ o $b = \varphi^t c$, se e solo se $\theta(c) = \theta(b) + c$ o $\theta(b) = \theta(c) + c$, se e solo se $\{\theta(c), \theta(b)\} \in \mathcal{E}(\Delta_t^k)$. □

Figura:grafoasssociato

Corollario 4.11. *Se $c, r \in N \setminus \{0\}$ ed $\exists j \in I_{k-1}$ tale che $s(c, r, j) \neq 0$ e $(j, k) = 1$, allora $\Gamma(E_c^r)$ è hamiltoniano.*

Dimostrazione. Basta osservare che, con le notazioni del teorema, il sottografo Γ_j è isomorfo a Δ_j^k e dunque, poichè $(j, k) = 1$, a C_k, il grafo ciclico su k vertici. Dunque Γ_j è un ciclo spanning di Γ. □

4.4 Geometria delle intersezioni

Allo scopo di costruire i grafi associati ai sistemi di cerchi abbiamo bisogno di criteri pratici e computazionalmente utilizzabili per determinare il numero di intersezioni di due cerchi. In questo paragrafo dimostreremo alcuni teoremi utili a tale scopo.

Particolarmente interessanti e facili da studiare sono i sistemi di cerchi del tipo E_c^c in cui raggio minore e raggio maggiore coincidono. Il seguente teorema fornisce, sotto certe ipotesi, una caratterizzazione completa dei grafi ad essi associati.

Teorema 4.12. ***(Sistemi di cerchi per 0)***
Se N è abeliano, non ha elementi di caratteristica 2 e $-\iota \in \Phi$, allora

$$1)\ \forall c \in N \setminus \{0\}, \forall \varphi \in \Phi \setminus \{\iota, -\iota\}, \quad (\Phi c + c) \cap (\Phi c + \varphi c) = \{0, c + \varphi c\} \tag{4.2}$$

$$2)\ \forall c \in N \setminus \{0\}, \quad (\Phi c + c) \cap (\Phi c - c) = \{0\} \tag{4.3}$$

In particolare $\Gamma(E_c^r)$ è un grafo completo tale che $o = 1$ ed $e = |V(\Gamma(E_c^r))| - 2 = |\Phi| - 2$. Inoltre

3) i sistemi di cerchi E_c^c con $c \in N \setminus \{0\}$ sono tutti e soli quelli per cui $|(\Phi r + c) \cap (\Phi r - c)| = 1$ ed anche tutti e soli quelli i cui elementi passano per 0.

Dimostrazione.

1. $0 = -\iota c + c = (-\iota\varphi)c + \varphi c \in (\Phi c + c) \cap (\Phi c + \varphi c)$ e $\varphi c + c = \iota c + \varphi c \in (\Phi c + c) \cap (\Phi c + \varphi c)$; poichè $\varphi \neq -\iota$, $\varphi c + \neq 0$ e dunque $(\Phi c + c) \cap (\Phi c + \varphi c) = \{0, \varphi c + c\}$.

2. $0 = (-\iota)c + c = \iota c - c \in (\Phi c + c) \cap (\Phi c - c)$; mostriamo ora che 0 è l'unico elemento di $(\Phi c + c) \cap (\Phi c - c)$. Sia per assurdo $w \in (\Phi c + c) \cap (\Phi c - c)$ e $w \neq 0$, allora $w = \mu r + r = \mu' r - r$, con $\mu, \mu' \in \Phi$; si ha $-w = -\mu r - r = (-\iota\mu)r - r$ e $-w = -\mu' r + r = (-\iota\mu)r + r$ e dunque, poichè $-\iota \in \Phi$, $w \in (\Phi c + c) \cap (\Phi c - c)$; dato che $|(\Phi c + c) \cap (\Phi c - c)| \leq 2$ e $w \neq 0$, deve essere $-w = w$ e dunque w ha caratteristica 2, contro l'ipotesi.

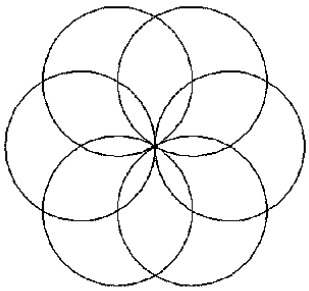


FIGURA 4.3. Sistema di cerchi tangenti in 0

3. E' chiaro dai punti 1 e 2 che $\forall c \in N\setminus\{0\}$ tutti gli elementi di E_c^c passano per zero e $|(\Phi c + c) \cap (\Phi c - c)| = 1$. Viceversa, se E_c^r è tale che tutti i suoi elementi passano per 0, allora, in particolare, $0 \in \Phi r - c$ e dunque $\exists \psi \in \Phi$ tale che $c = \psi r$, cioè $\Phi c = \Phi r$. Supponiamo ora $r, c \in N\setminus\{0\}$ tali che $|(\Phi r + c) \cap (\Phi r - c)| = 1$ e poniamo $(\Phi r + c) \cap (\Phi r - c) = \{w\}$, dunque $w = \mu r + c = \mu' r - c$ con $\mu, \mu' \in \Phi$ e $-w = -\mu r - c = -\mu' r + c \in (\Phi r + c) \cap (\Phi r - c) = \{w\}$, così $-w = w$ ed allora, poichè N non ha elementi di caratteristica 2, $w = 0$. Così $c = -\mu r$, $\Phi c = \Phi r$ e $E_c^r = E_c^c$.

□

Il seguente teorema fornisce, sotto ipotesi del tutto generali, una condizione necessaria e sufficiente affinchè due cerchi si intersechino.

Teorema 4.13. ***(Cerchi non disgiunti)***
Siano $r, c \in N\setminus\{0\}$, $\psi \in \Phi\setminus\{\iota\}$*; si ha*

$(\Phi r + c) \cap (\Phi r + \psi c) \neq \varnothing$ *se e solo se* $\exists \lambda, \mu \in \Phi$ *distinti tali che* $c = (\iota - \psi)^{-1}(-\lambda + \mu)r$

Dimostrazione. Sia $(\Phi r + c) \cap (\Phi c + \psi c) \neq \varnothing$, allora $\exists \lambda, \mu \in \Phi$ tali che $\lambda r + c = \mu r + \psi c$ e, poichè $\psi \neq \iota$, $\lambda \neq \mu$; dunque $(\iota - \psi)c = (-\lambda + \mu)r$, cioè $c = (\iota - \psi)^{-1}(-\lambda + \mu)r$. Viceversa, se $c = (\iota - \psi)^{-1}(-\lambda + \mu)r$, con $\lambda, \mu \in \Phi$ e $\lambda \neq \mu$, allora $(\iota - \psi)c = (-\lambda + \mu)r$ e così $\lambda r + c = \mu r + \psi c \in (\Phi r + c) \cap (\Phi c + \psi c)$. □

Il teorema che segue fornisce, sotto le stesse ipotesi del teorema sui cerchi per 0, una condizione necessaria e sufficiente affinchè due cerchi siano tangenti, cioè affinchè si intersechino in un solo punto.

Teorema 4.14. ***(Cerchi tangenti)***
Se N *è abeliano e non ha elementi di caratteristica 2,* $-\iota \in \Phi$, $r, c \in N\setminus\{0\}$, $\psi \in \Phi\setminus\{\iota\}$; *si ha*

$|(\Phi r + c) \cap (\Phi c + \psi c)| = 1$ *se e solo se* $\exists \lambda \in \Phi$ *tale che* $c = (\iota - \psi)^{-1}(-2\lambda r)$

ed in tal caso è $(\Phi r + c) \cap (\Phi c + \psi c) = \{a\}$ *, con* $a = -\lambda r + c = \lambda r + \psi c$.

Dimostrazione. Supponiamo $(\Phi r + c) \cap (\Phi c + \psi c) = \{a\}$, allora $\exists \lambda, \mu \in \Phi$ tali che $a = \lambda r + c = \mu r + \psi c$ e, poichè $\psi \neq \iota$, $\lambda \neq \mu$; si ha, poichè $-\iota \in \Phi$, $-\mu r + c = -\lambda r + \psi c \in (\Phi r + c) \cap (\Phi c + \psi c) = \{a\}$ e dunque $a = \lambda r + c = -\lambda r + \psi c$ e $(\iota - \psi)c = -2\lambda r$, cioè $c = (\iota - \psi)^{-1}(-2\lambda r)$.

Viceversa sia $c = (\iota - \psi)^{-1}(-2\lambda r) = (\iota - \psi)^{-1}(-\lambda r - \lambda r)$, dunque $c = (\iota - \psi)^{-1}(-2\lambda r) = (\iota - \psi)^{-1}(-\lambda r - \lambda r)$, $(\iota - \psi)c = -\lambda r - \lambda r$ e

$$-\lambda r + \psi c = \lambda r + c = a \in (\Phi r + c) \cap (\Phi c + \psi c).$$

Mostriamo che a è l'unico elemento di $(\Phi r + c) \cap (\Phi c + \psi c)$. Sia per assurdo $b \in (\Phi r + c) \cap (\Phi c + \psi c)$ e $b \neq a$, allora

$$b = \alpha r + \psi c = \beta r + c$$

con $\alpha \neq -\lambda$, $\beta \neq \lambda$ e $\alpha \neq \beta$; è allora

$$w = -\beta r + \psi c = -\alpha r + c \in (\Phi r + c) \cap (\Phi c + \psi c) = \{a, b\}.$$

Se $w = -\alpha r + c = \beta r + c = b$ allora $-\alpha = \beta$ e dunque $b = \alpha r + \psi c = -\alpha r + c$, da cui $2\alpha r = (\iota - \psi)c = -2\lambda r$. Poichè $r \neq 0$ e N non ha elementi di caratteristica 2, $2r \neq 0$; ma le orbite non banali di Φ sono regolari, e dunque $\alpha = -\lambda$, ed anche $b = a$, contro l'ipotesi.

Se $w = -\beta r + \psi c = -\lambda r + \psi c = a$ allora $\beta = \lambda$ e dunque ancora $a = b$. □

Il teorema che segue fornisce, sotto le stesse ipotesi dei teoremi precedenti, una condizione necessaria e sufficiente per determinare quando due cerchi sono secanti (si intersecano cioè in due punti).

Teorema 4.15. ***(Cerchi secanti)***

Se N *è abeliano e non ha elementi di caratteristica 2,* $-\iota \in \Phi$, $r, c \in N \setminus \{0\}$ $\psi \in \Phi \setminus \{\iota\}$ *; si ha*

$$\begin{aligned} |(\Phi r + c) \cap (\Phi c + \psi c)| &= 2 \text{ se e solo se} \\ \exists \lambda, \mu &\in \Phi \text{ tali che } \lambda \neq \pm\mu \text{ e } c = (\iota - \psi)^{-1}(\lambda - \mu)r \end{aligned}$$

ed in tal caso è $(\Phi r + c) \cap (\Phi c + \psi c) = \{a, b\}$ *, con* $a = \lambda r + c = \mu r + \psi c$, $b = -\lambda r + \psi c = -\mu r + c$.

Osserviamo che la somma delle intersezioni è uguale alla somma dei centri, analogamente a quanto succede in geometria euclidea piana ove il punto medio tra i punti di intersezione di due cerchi di ugual raggio coincide con il punto medio dei centri. Tale affermazione rimane vera anche nel caso di cerchi tangenti, a patto di pensare il punto di intersezione come due punti coincidenti.

Dimostrazione. Supponiamo $(\Phi r + c) \cap (\Phi c + \psi c) = \{a, b\}$; allora, in particolare, $(\Phi r + c) \cap (\Phi c + \psi c) \neq \varnothing$ e dunque, per il teorema dei cerchi non disgiunti, $\exists \lambda, \mu \in \Phi$ tali che $\lambda \neq \mu$ $c = (\iota - \psi)^{-1}(-\lambda + \mu)r$; se fosse $\lambda = -\mu$ sarebbe, per il teorema dei cerchi tangenti, $|(\Phi r + c) \cap (\Phi c + \psi c)| = 1$. Dunque $\lambda \neq \pm\mu$.

Viceversa, sia $c = (\iota - \psi)^{-1}(\lambda - \mu)r$ con $\lambda, \mu \in \Phi$ e $\lambda \neq \pm\mu$. Si ha $(\iota - \psi)c = (\lambda - \mu)r$ ed allora

$$\begin{aligned} a &= \mu r + c = \lambda r + \psi c \in (\Phi r + c) \cap (\Phi c + \psi c) \\ b &= -\lambda r + c = -\mu r + \psi c \in (\Phi r + c) \cap (\Phi c + \psi c) \end{aligned}$$

Poichè $\lambda \neq -\mu$, $a \neq b$ e $(\Phi r + c) \cap (\Phi c + \psi c) = \{a, b\}$. □

Capitolo 5

Struttura dei grafi di sistemi di cerchi dagli interi modulo p

In questo capintolo considereremo coppie di Ferrero $(\mathbb{Z}_p, \Phi_k)$, dove p è un numero primo ≥ 5 e Φ_k il sottogruppo di ordine k di $\mathbb{Z}_p^*$ e supporremo sempre che i BIBD $(\mathbb{Z}_p, \mathcal{B}_{\Phi_k}, \in)$ siano circolari; in appendice riporteremo il programma MATLAB `circular` che calcola proprio per quali valori di p e k ciò avviene.Utilizzando tale progamma abbiamo costruito la tabella che qui riportiamo, nelle cui righe dispari sono scritti, sulla prima colonna, i primi p compresi tra 13 e 199, e sulle colonne successive i divisori k di $p-1$ tali che il BIBD $(\mathbb{Z}_p, \Phi_k)$ è circolare, e nelle cui righe pari sono scritti, sulla prima colonna un elemento primitivo di $\mathbb{Z}_p$, e sulle colonne successive un generatore di Φ_k per ogni valore di $k|p-1$ determinato.

p	k1	k2	k3	k4	*	p	k1	k2	k3	k4
13	4	*	*	*	*	73	4	6	8	*
2	8	*	*	*	*	5	27	90	10	*
17	4	*	*	*	*	79	6	*	*	*
3	13	*	*	*	*	3	24	*	*	*
29	4	*	*	*	*	89	4	8	*	*
2	12	*	*	*	*	3	34	37	*	*
31	5	6	*	*	*	97	4	6	8	*
3	16	26	*	*	*	5	22	36	64	*
37	4	6	*	*	*	101	4	5	*	*
2	31	27	*	*	*	2	10	95	*	*
41	4	5	*	*	*	103	6	*	*	*
6	32	10	*	*	*	5	57	*	*	*
43	6	*	*	*	*	109	4	6	*	*
3	37	*	*	*	*	6	33	64	*	*
53	4	*	*	*	*	113	4	7	8	*
2	3	*	*	*	*	3	98	49	18	*
61	4	5	6	*	*	127	6	7	*	*
2	11	*	*	*	*	3	108	4	*	*
67	6	*	*	*	*	131	5	10	*	*
2	38	*	*	*	*	2	53	70	*	*
71	5	7	*	*	*	137	4	8	*	*
7	54	45	*	*	*	3	100	127	*	*

p	k1	k2	k3	k4	*	p	k1	k2	k3	k4	k5
139	6	*	*	*	*	173	4	*	*	*	*
2	97	*	*	*	*	2	80	*	*	*	*
149	4	*	*	*	*	181	4	5	6	9	10
2	105	*	*	*	*	2	162	59	49	43	56
151	5	6	10	*	*	191	5	10	*	*	*
6	8	33	87	*	*	19	39	82	*	*	*
157	4	6	*	*	*	193	4	6	8	*	*
5	129	13	*	*	*	5	112	85	43	*	*
163	6	9	*	*	*	197	4	7	*	*	*
2	105	40	*	*	*	2	183	104	*	*	*

E' utile la seguente

Osservazione 5.1. *Per il corollario 3.13, se* $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$ *è circolare e* $l|k$ *allora anche* $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_l}, \in)$ *è circolare.*

Studieremo ora i sistemi di cerchi in $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$ ed in particolare i grafi ad essi associati. Per semplicità, indichiamo $\mathcal{B}^*_{\Phi_k}$ con $\mathcal{B}^*_k$.

Il nostro scopo è costruire i grafi degli E^r_c come unione di grafi di base, e poichè i primi sono grafi etichettati in $\mathbb{Z}_2$, conviene considerare due tipi di grafi di base.

Definizione 5.2. *Siano k,j interi,* $k \geq 3$ *e* $1 \leq j \leq k$*: si dice j-esimo k-**grafo di base pari** (rispett. **dispari**) e lo di si denota con* Π^k_j *(rispett.* Γ^k_j*) lo j-esimo k-grafo di base con lati tutti etichettati con 0 (rispett. 1).*

Poichè è $\Delta^k_j = \Delta^k_{k-j}$ si ha anche $\Gamma^k_j = \Gamma^k_{k-j}$ e $\Pi^k_j = \Pi^k_{k-j}$, mentre se $1 \leq s, j \leq \left[\frac{k}{2}\right]$ $\Gamma^k_j \neq \Gamma^k_{k-j}$ e $\Pi^k_j \neq \Pi^k_{k-j}$.

E' interessante a questo punto introdurre i seguenti concetti:

Definizione 5.3. *Sia* $j \in I_{k-1}$, $r \in \mathbb{Z}^*_p$*; si pone*

$$\begin{aligned}
\gamma(j,r;k,p) &= \left|\left\{E^r_c \text{ in } (\mathbb{Z}_p, \mathcal{B}^*_k, \in) \,\middle|\, c \in \mathbb{Z}^*_p,\ \Gamma^k_j \text{ sottografo di } \Gamma(E^r_c))\right\}\right| \\
\pi(j,r;k,p) &= \left|\left\{E^r_c \text{ in } (\mathbb{Z}_p, \mathcal{B}^*_k, \in) \,\middle|\, c \in \mathbb{Z}^*_p,\ \Pi^k_j \text{ sottografo di } \Gamma(E^r_c))\right\}\right|
\end{aligned}$$

Segue subito dalla definizione di $\Gamma(E^r_c)$ che, se $(s(r,c,i))_{i \in I_{k-1}}$ è una sequenza definita come in 4.1 rispetto ad un qualsiasi ordinamento di Φ_k, si ha

$$\begin{aligned}
\gamma(j,r;k,p) &= \left|\left\{\Phi_k c \,\middle|\, c \in \mathbb{Z}^*_p, s(c,r,j) = 1\right\}\right| = \\
&= \left|\left\{\Phi_k c \,\middle|\, c \in \mathbb{Z}^*_p,\ |(\Phi_k r + c) \cap (\Phi_k r + \varphi_j c)| = 1\right\}\right| \\
\pi(j,r;k,p) &= \left|\left\{\Phi_k c \,\middle|\, c \in \mathbb{Z}^*_p, s(c,r,j) = 2\right\}\right| = \\
&= \left|\left\{\Phi_k c \,\middle|\, c \in \mathbb{Z}^*_p,\ |(\Phi_k r + c) \cap (\Phi_k r + \varphi_j c)| = 2\right\}\right|
\end{aligned}$$

Poichè $\Gamma^k_j = \Gamma^k_{k-j}$ e $\Pi^k_j = \Pi^k_{k-j}$ si ha anche $\gamma(j,r;k,p) = \gamma(k-j,r;k,p)$ e $\pi(j,r;k,p) = \pi(k-j,r;k,p)$ $\forall k \geq 3$, $\forall 1 \leq j \leq k$.

In questo capitolo daremo una descrizione completa di γ e π, distinguendo i casi k pari e k dispari, e mostreremo in particolare che il loro valore dipende unicamente da k e non da j, r e p.

5.1 Caso k pari

Supporremo in questo paragrafo che p sia un numero primo, k un divisore pari di $p-1$ tale che $(\mathbb{Z}_p, \mathcal{B}_k^*, \in)$ sia circolare, e φ un generatore di Φ_k.

Se k è pari $2|k$ e dunque Φ_k contiene il sottogruppo di ordine due di $\mathbb{Z}_p^*$, che è generato da -1; allora la coppia di Ferrero $(\mathbb{Z}_p, \Phi_k)$ soddisfa alle ipotesi dei teoremi dei cerchi tangenti e secanti e dei sistemi di cerchi per 0.

Il Teorema dei Cerchi Tangenti permette di determinare il valore di γ.

Teorema 5.4. $\forall r \in \mathbb{Z}_p^*$, $\forall j \in I_{k-1}$, $\gamma(j, r; k, p) = 1$

Dimostrazione. Γ_j^k è sottografo di $\Gamma(E_c^r)$ se e solo se $|(\Phi_k r + c) \cap (\Phi_k r + \varphi^j c)| = 1$, se e solo se $\exists \lambda \in \Phi_k$ tale che $c = (\varphi^j - 1)^{-1}(-2\lambda r)$, se e solo se $c \in \Phi_k a$, dove $a = (\varphi^j - 1)^{-1}(-2r)$. Dunque $\left\{E_c^r \text{ in } (\mathbb{Z}_p, \mathcal{B}_k, \in) \;\middle|\; \Gamma_j^k \text{ sottografo di } \Gamma(E_c^r)\right\} = \{E_a^r\}$ e $\gamma(j, r; k, p) = 1$. □

Il Teorema dei Cerchi Secanti permette di determinare il valore di π.

Teorema 5.5. $\forall r \in \mathbb{Z}_p^*$, $\forall j \in I_{k-1}$, $\pi(j, r; k, p) = \frac{k}{2} - 1$

Dimostrazione. Π_j^k sottografo di $\Gamma(E_c^r)$ se e solo se $|(\Phi_k r + c) \cap (\Phi_k r + \varphi^j c)| = 2$, se e solo se $\exists \lambda, \mu \in \Phi_k$ tali che $c = (\varphi^j - 1)^{-1}(\lambda - \mu)r$, se e solo se $\exists \psi \in \Phi_k \backslash \{\pm\iota\}$, $\gamma \in \Phi_k$ tali che $c = \gamma(\varphi^j - 1)^{-1}(\psi - \iota)r$, se e solo se $\exists l \in I_{k-1} \backslash \{\frac{k}{2}\}$ tale che $c \in \Phi_k a_l$, con $a_l = (\varphi^j - 1)^{-1}(\varphi^l - \iota)r$.

Si ha che, $\forall l \in I_{\frac{k}{2}}$, $\Phi_k a_{k-l} = \Phi_k a_l$. Infatti

$$\begin{aligned} a_{k-l} &= (\varphi^j - 1)^{-1}(\varphi^{k-l} - \iota)r = (\varphi^j - 1)^{-1}(\varphi^{-l} - 1)r \\ &= -\varphi^{-l}(\varphi^j - 1)^{-1}(\varphi^l - 1)r \in \Phi_k a_l \end{aligned}$$

Mostriamo che, per $l \in I_{\frac{k}{2}-1}$ i cerchi $\Phi_k a_l$ sono tutti distinti.

$\forall l \in I_{k-1} \backslash \{\frac{k}{2}\}$ $(\varphi^j - 1)a_l = (\varphi^l - 1)r$, così

$$\begin{aligned} \alpha_l &: = r + \varphi^j a_l = \varphi^l r + a_l \in (\Phi_k r + \varphi^j a_l) \cap (\Phi_k r + a_l) \\ \beta_l &: = -\varphi^l r + \varphi^j a_l = -r + a_l \in (\Phi_k r + \varphi^j a_l) \cap (\Phi_k r + a_l) \end{aligned}$$

con $\alpha_l \neq \beta_l$ perchè $\varphi^l \neq -\iota$; dunque se $a_s = \lambda a_l$ con $\lambda \in \Phi_k$ è anche

$$r + \lambda \varphi^j a_s = \varphi^l r + \lambda a_s$$

e

$$-\varphi^l r + \lambda \varphi^j a_s = -r + \lambda a_s$$

e quindi

$$\lambda^{-1}r + \varphi^j a_s = \lambda^{-1}\varphi^l e + a_s \in (\Phi_k r + \varphi^j a_s) \cap (\Phi_k r + a_s) = \{\alpha_s, \beta_s\}$$

e

$$-\lambda^{-1}\varphi^l r + \varphi^j a_s = -\lambda^{-1}r + a_s \in \{\alpha_s, \beta_s\};$$

se $\lambda^{-1}r+\varphi^j a_s = \alpha_s = r+\varphi^j a_s$ allora $\lambda = \iota$ e $a_s = a_l$, se $\lambda^{-1}r+\varphi^j a_s = \beta_s = -\varphi^l r+\varphi^j a_s$ allora $\lambda^{-1} = -\varphi^l$e $\lambda = -\varphi^{-l}$ e dunque

$$\begin{aligned} a_s &= \lambda a_l = -\varphi^{-l}(\varphi^j - 1)^{-1}(\varphi^l - \iota)r = \\ &= -(\varphi^j - 1)^{-1}(1 - \varphi^{-j})r = (\varphi^j - 1)^{-1}(\varphi^{k-j} - 1)r = a_{k-l} \end{aligned}$$

Si conclude

$$\left\{E_c^r \text{ in } (\mathbb{Z}_p, \mathcal{B}_k^*, \in) \;\middle|\; \Gamma_j^k \text{ sottografo di } \Gamma(E_c^r))\right\} = \left\{E_{a_l}^r \text{ in } (\mathbb{Z}_p, \mathcal{B}_k^*, \in) \;\middle|\; l \in I_{\frac{k}{2}-1})\right\}$$

e

$$\pi(j, r; k, p) = \left|\left\{E_{a_l}^r \text{ in } (\mathbb{Z}_p, \mathcal{B}_k^*, \in) \;\middle|\; l \in I_{\frac{k}{2}-1})\right\}\right| = \frac{k}{2} - 1.$$

□

Il Teorema dei Sistemi di Cerchi per 0 permette di dare una descrizione completa dei grafi associati ai sistemi di cerchi E_r^r in $(\mathbb{Z}_p, \mathcal{B}_k, \in)$.

Teorema 5.6. *Si ha* $\Gamma(E_r^r) = \left(\bigvee_{j=1}^{\frac{k}{2}-1} \Pi_j^k\right) \vee \Gamma_{\frac{k}{2}}^k$, $\forall r \in \mathbb{Z}_p^*$

Dimostrazione. Dal teorema 4.10 abbiamo che $\forall r, c \in \mathbb{Z}_p^*$ $\Gamma(E_c^r) = \bigvee_{j=1}^{\frac{k}{2}} \Theta_j$, dove Θ_j è isomorfo a Π_j^k se $s(r, c, j) = 2$, a Γ_j^k se $s(r, c, j) = 1$ ed al grafo nullo se $s(r, c, j) = 0$. Osservando che $\varphi^{\frac{k}{2}} = -1$ abbiamo, dal teorema dei sistemi di cerchi per 0, che $s(r, r, j) = 2$ $\forall j \in I_{\frac{k}{2}-1}$ e $s(r, r, \frac{k}{2}) = 1$ e dunque $\forall r \in \mathbb{Z}_p^*$ $\Gamma(E_r^r) = \left(\bigvee_{j=1}^{\frac{k}{2}-1} \Pi_j^k\right) \vee \Gamma_{\frac{k}{2}}^k$. □

Possiamo ora contare il numero di grafi elementari che otteniamo come sottografi di $\Gamma(E_c^r)$ al variare di c in $\mathbb{Z}_p^*$.

Teorema 5.7. *Il numero di grafi elementari che sono sottografi di* $\Gamma(E_c^r)$ *per qualche* $c \in \mathbb{Z}_p^*$, *contati ciascuno con la molteplicità con cui compare, è* $\left(\frac{k}{2}\right)^2$

Dimostrazione. Infatti $\forall j \in I_{\frac{k}{2}}$ Π_j^k è sottografo di $(\frac{k}{2} - 1)$ dei $\Gamma(E_c^r)$ e Γ_j^k di 1; poichè i k-grafi di base (pari e dispari) sono tutti e soli i Γ_j^k e Π_j^k con $j \in I_{\frac{k}{2}}$ e sono tutti distinti, si hanno in totale $((\frac{k}{2} - 1) + 1)\frac{k}{2} = \left(\frac{k}{2}\right)^2$ grafi di base, sottografi dei $\Gamma(E_c^r)$. □

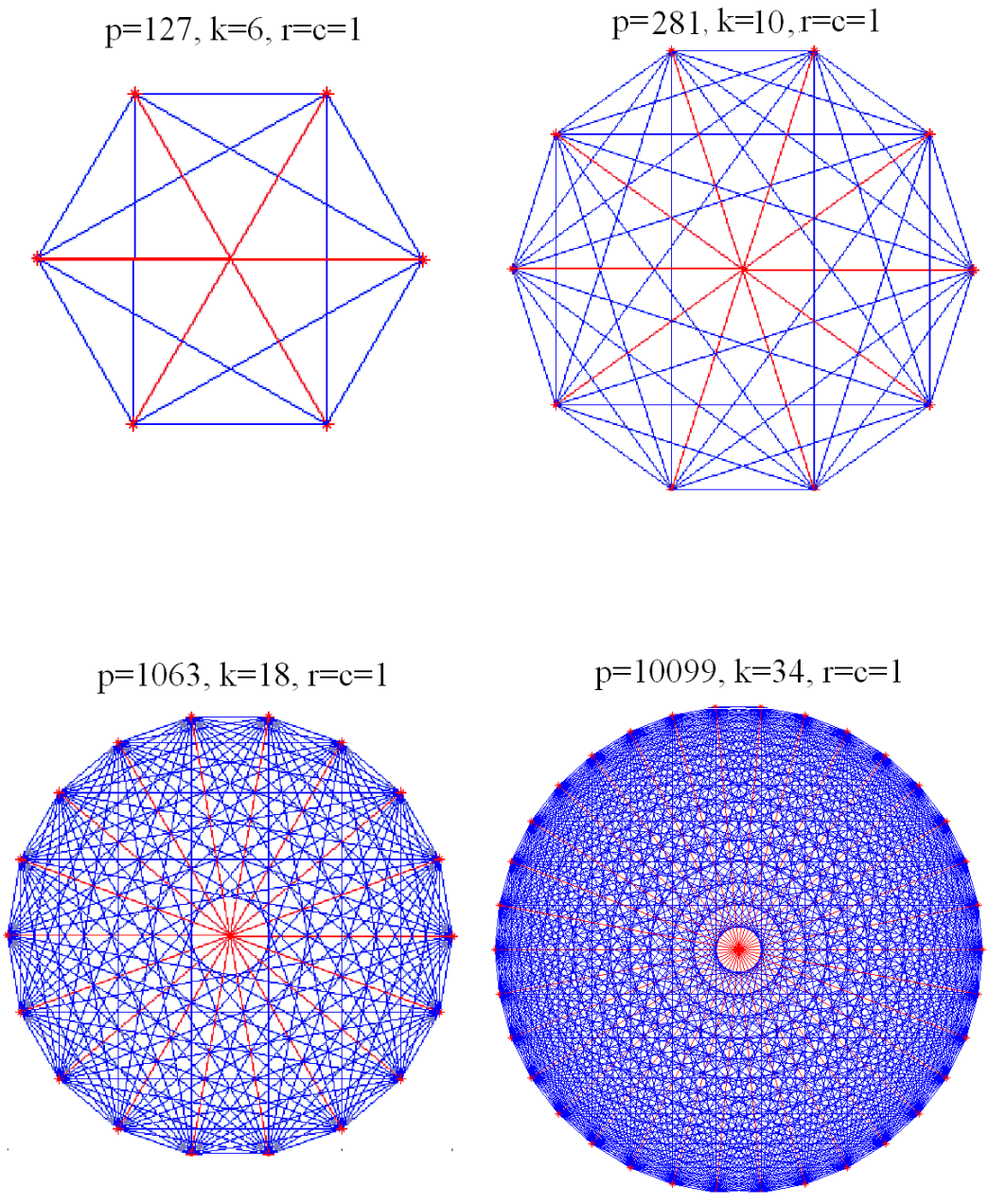


FIGURA 5.1. $\Gamma(E_1^1)$ per $k = 6, 18, 16, 34$

Osserviamo che è possibile che i grafi di base siano essi stessi grafi di qualche sistema di cerchi, ma non necessariamente; ad esempio il grafo di base $\Gamma^k_{\frac{k}{2}}$ per k pari non è grafo di alcun sistema di cerchi, infatti se un sistema E^r_c avesse come grafo $\Gamma^k_{\frac{k}{2}}$ sarebbe $|(\Phi_k r + c) \cap (\Phi_k r + -c)| = 1$ e dunque, per il teorema dei cerchi tangenti, $\Phi_k r = \Phi_k c$ e dunque $\Gamma(E^r_c) = \Gamma(E^r_r) = \left(\bigvee_{j=1}^{\frac{k}{2}-1} \Pi^k_j \right) \vee \Gamma^k_{\frac{k}{2}}$. E' vero però che i grafi di base pari diversi da $\Pi^k_{\frac{k}{2}}$ sono sempre *sottografi* di un qualche sistema di cerchi. Questo segue come corollario del

Teorema 5.8. *$\forall i_1, i_2 \in I_{k-1} \backslash \{\frac{k}{2}\}$, $\forall r \in \mathbb{Z}^*_p$, $\exists c \in \mathbb{Z}^*_p$ tale che $\Pi^k_{i_1} \wedge \Pi^k_{i_2}$ sottografo di $\Gamma(E^r_c)$*

Dimostrazione. Per il teorema dei cerchi secanti, $\Pi^k_{i_1} \vee \Pi^k_{i_2}$ è sottografo di $\Gamma(E^r_c)$ se e solo se $\exists \psi_1, \psi_2 \in \Phi \backslash \{\pm 1\}, \lambda_1, \lambda_2 \in \Phi$ tali che $c = (\psi_1 - 1)(\varphi^{i_1} - 1)^{-1} \lambda_1 r = (\psi_2 - 1)(\varphi^{i_2} - 1)^{-1} \lambda_2 r$ se e solo se $\exists \psi_1, \psi_2 \in \Phi \backslash \{\pm 1\}, \lambda \in \Phi$ tali che $c = \lambda(\psi_1 - 1)(\varphi^{i_2} - 1)r = (\varphi^{i_1} - 1)(\psi_2 - 1)r$; dunque $\forall i_1, i_2 \in I_{k-1} \backslash \{\frac{k}{2}\}$, $\forall r \in \mathbb{Z}^*_p$ se consideriamo $c = \lambda(\psi_1 - 1)(\varphi^{i_2} - 1)r = (\varphi^{i_1} - 1)(\psi_2 - 1)r$ per $\lambda = 1$, $\psi_1 = \varphi^{i_1}$, $\psi_2 = \varphi^{i_2}$ abbiamo che $\Pi^k_{i_1} \wedge \Pi^k_{i_2}$ è sottografo di $\Gamma(E^r_c)$. □

5.1.1 Caso k=4

E' banale che per $k = 3$, per ogni primo p tale che $k|p-1$ il BIBD $(\mathbb{Z}_p, \mathcal{B}^*_k, \in)$ è circolare, infatti in esso i cerchi hanno tre punti, e dunque per tre punti necessariamente passa al più un cerchio. E' non banale invece che la stessa cosa valga per $k = 4$, come afferma un teorema di Modisett, di cui omettiamo la dimostrazione. Dunque per ogni primo p tale che $4|p-1$ possiamo considerare il BIBD circolare $(\mathbb{Z}_p, \mathcal{B}_4, \in)$: intendiamo dare una classificazione completa dei grafi associati ai sistemi di cerchi in tale struttura. Premettiamo a questo proposito il seguente

Lemma 5.9. *$\Gamma^4_1 \vee \Pi^4_2$ non è grafo di alcun sistema di cerchi in $(\mathbb{Z}_p, \mathcal{B}^*_4, \in)$.*

Dimostrazione. Osserviamo preliminarmente che se p è un primo tale che $4|p-1$ allora $p \geq 13$.

Siano per assurdo $r, c \in \mathbb{Z}^*_p$ tali che $\Gamma(E^r_c) = \Gamma^4_1 \vee \Pi^4_2 \vee \Gamma^4_3$: detto φ un elemento di ordine 4 di $\mathbb{Z}^*_p$, per il teorema dei cerchi secanti

$$\exists \psi \in \Phi_4 \backslash \{\pm 1\} \text{ tale che } (\varphi^2 - 1)^{-1}(\psi - 1)r = (-2)^{-1}(\psi - 1)r \in \Phi_4 c,$$

e per il teorema dei cerchi tangenti

$$(\varphi - 1)^{-1}(-2r) \in \Phi_4 c,$$

e dunque

$$\exists \lambda \in \Phi_4 \text{ tale che } (\varphi - 1)^{-1}(-2r) = \lambda(-2)^{-1}(\psi - 1)r$$

ed anche

$$4\lambda = (-2)^2\lambda = (\varphi - 1)(\psi - 1).$$

Poichè $\psi \in \Phi_4 \backslash \{\pm 1\}$ è $\psi = \varphi$ o $\psi = -\varphi$.

Se $\psi = -\varphi$ allora

$$4\lambda = (-2)^2\lambda = (\varphi - 1)(-\varphi - 1) = -(\varphi^2 - 1) = -(-2) = 2,$$

e dunque $2\lambda = 1$ ed anche ($\lambda \in \Phi_4$) $1 = (2\lambda)^4 = 16\lambda^4 = 16$, e quindi $15 = 0$, cioè $p|15$; ma è $p \geq 13$, e dunque siamo giunti ad un assurdo.

Se $\psi = \varphi$ allora $4\lambda = (\varphi - 1)^2 = \varphi^2 - 2\varphi - 1 = -2\varphi = 2\varphi^3$ e dunque $2\lambda = -\varphi = \varphi^3$; poichè $\lambda \in \Phi_4$, abbiamo 4 possibilità

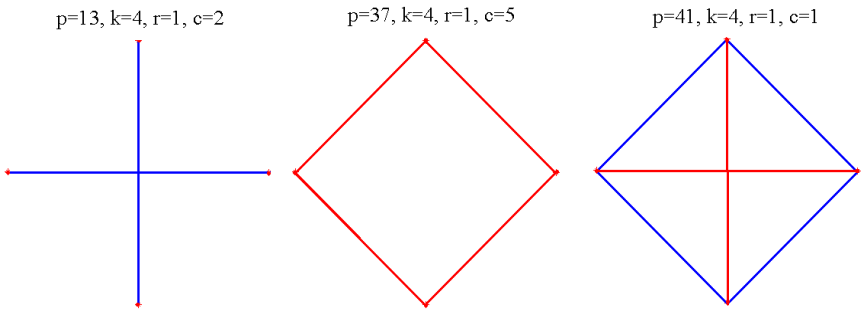
- $\lambda = \varphi \Rightarrow 2\varphi = -\varphi \Rightarrow 2 = -1 \Rightarrow p|3$
- $\lambda = \varphi^2 = -1 \Rightarrow \varphi = 2 \Rightarrow 1 = \varphi^4 = 16 \Rightarrow p|15$
- $\lambda = \varphi^3 = -\varphi \Rightarrow -2\varphi = -\varphi \Rightarrow \varphi = 0$
- $\lambda = 1 \Rightarrow 2 = -\varphi \Rightarrow 1 = \varphi^4 = (-\varphi)^4 = 2^4 = 16 \Rightarrow p|15$

Nei casi 1,2,4 abbiamo una contraddizione con il fatto che $p \geq 13$, nel caso 3) col fatto che φ è un generatore di Φ_4. □

Possiamo a questo punto dimostrare il

Teorema 5.10. ***(Classificazione dei grafi per k=4)***
Gli unici grafi non nulli associati a sistemi di cerchi in $(\mathbb{Z}_p, \mathcal{B}_4^*, \in)$ *sono* Γ_1^4, Π_2^4 *e* $\Pi_1^4 \vee \Gamma_2^4$*; inoltre,* $\forall r \in \mathbb{Z}_p^*$*, ciascuno di essi è grafo di esattamente un sistema di cerchi di raggio secondario* r*.*

Dimostrazione. Notiamo che i grafi di base (pari e dispari) sono $\Gamma_1^4, \Gamma_2^4, \Pi_1^4, \Pi_2^4$. Sia $r \in \mathbb{Z}_p^*$. Per il teorema dei fasci di cerchi per 0, $\forall r \in \mathbb{Z}$ E_r^r è l'unico sistema di cerchi di raggio secondario r con grafo associato $\Pi_1^4 \vee \Gamma_2^4$, mentre $\Gamma_1^4 \vee \Gamma_2^4$ non è grafo di alcun sistema di cerchi. Per il lemma precedente anche $\Gamma_1^4 \vee \Pi_2^4$ non è grafo di alcun sistema di cerchi. Poichè $\forall j \in I_3$ $\gamma(j, r; k, p) = 1$ e $\pi(j, r; k, p) = \frac{4}{2} - 1 = 1$, ogni grafo di base è sottografo di esattamente un $\Gamma(E_c^r)$ al variare di c in $\mathbb{Z}_p^*$ e dunque Γ_1^4 e Π_2^4 devono essere essi stessi i grafi di esattamente un sistema di cerchi di raggio secondario r. □



5.2 Caso k dispari

Per calcolare π e γ nel caso pari abbiamo usato i teoremi dei cerchi tangenti e secanti e dei sistemi di cerchi per 0, teoremi che, per k dispari, non sono più applicabili perchè $-1 \notin \Phi_k$. Abbiamo perciò bisogno di ricondurci in qualche modo al caso pari considerando anche il BIBD $(\mathbb{Z}_p, \mathcal{B}^*_{2k}, \in)$. Otterremo risultati che si congettura valgano per tutti i valori di p e k con k dispari tali che $(\mathbb{Z}_p, \mathcal{B}_k, \in)$ sia circolare, solo sotto l'ulteriore ipotesi che anche $(\mathbb{Z}_p, \mathcal{B}^*_{2k}, \in)$ sia circolare.

Supporremo così in questo paragrafo p un primo ≥ 5, k un intero dispari tale che $2k|p-1$ e che $(\mathbb{Z}_p, \mathcal{B}^*_{2k}, \in)$ (e dunque anche $(\mathbb{Z}_p, \mathcal{B}_{\Phi_k}, \in)$, vedi osservazione 5.1) sia circolare.

Per quanto riguarda i grafi di base pari abbiamo il

Teorema 5.11. *Risulta che,*$\forall r, c \in \mathbb{Z}^*_p$, $\forall A, B \in E^r_c$ *in* $(\mathbb{Z}_p, \mathcal{B}^*_k, \in)$, *se*$A \neq B$ *è* $|A \cap B| \leq 1$. *Da qui segue che* $\forall r \in \mathbb{Z}^*_p$, $\forall j \in I_{k-1}$ *è* $\pi(j, r; k, p) = 0$, *cioè i grafi* $\Gamma(E^r_c)$ *non hanno k-sottografi di base pari.*

Dimostrazione. Siano φ un generatore di Φ_{2k}, e dunque φ^2 un generatore di Φ_k. Per assurdo siano $A, B \in E^r_c$ in $(\mathbb{Z}_p, \mathcal{B}^*_k, \in)$ tali che $|A \cap B| \geq 2$. Non si lede la generalità supponendo $A = \Phi_k r + c$ e $B = \Phi_k r + \psi c$ con $\psi \in \Phi_k \backslash \{\iota\}$; esistono allora $a, a' \in A \cap B$ distinti

$$\begin{aligned} a &= \psi_1 r + c = \psi_2 r + \psi c, \\ a' &= \psi'_1 r + c = \psi'_2 r + \psi c, \end{aligned}$$

ove $\psi_1, \psi_2, \psi'_1, \psi'_2 \epsilon \Phi_k$, $\psi_1 \neq \psi'_1$, $\psi_2 \neq \psi'_2$ (perchè $a \neq a'$) e $\psi_1 \neq \psi_2$, $\psi'_1 \neq \psi'_2$ (perchè $\psi \neq \iota$). Poniamo

$$b = -\psi_2 r + c = -\psi_1 r + \psi c,$$

poichè $\psi \neq \iota$ $b \neq b'$ e poichè $-1 \in \Phi_{2k}$ è $\{a, a', b, b'\} \subset (\Phi_{2k} r + c) \cap (\Phi_{2k} r + \psi c)$ e dunque, per circolarità di $(\mathbb{Z}_p, \mathcal{B}^*_{2k}, \in)$, $b = a$ o $b = a'$. Se $b = a$, $-\psi_2 r + c = \psi_1 r + c$ allora $-1 = \psi_2^{-1}\psi_1 \in \Phi_k$ e dunque $2|k$ e k dispari, ciò che è assurdo. Se $b = a'$ $-\psi_2 r + c = \psi'_1 r + c$ allora $-1 = \psi_2^{-1}\psi'_1 \in \Phi_k$, che è assurdo. □

Contiamo ora il numero di sottografi dispari

Teorema 5.12. *Risulta che* $\forall r \in \mathbb{Z}_p^*$ *e* $\forall j \in I_{k-1}$ *è* $\gamma(j,r;k,p) = k-1$

Dimostrazione. Infatti $\forall c \in \mathbb{Z}_p^*$ Γ_j^k è sottografo di $\Gamma(E_c^r)$ se e solo se $|(\Phi_k r + \varphi^j c) \cap (\Phi_k r + c)| = 1$, se e solo se (per il teorema precedente) $(\Phi_k r + \varphi^j c) \cap (\Phi_k r + c) \neq \varnothing$, se e solo se (per il teorema dei cerchi non disgiunti, che vale anche nel caso k dispari)

$$\exists \lambda, \mu \in \Phi_k \text{ distinti tali che } c = (\iota - \varphi^j)^{-1}(-\lambda + \mu)r$$

se e solo se

$$\exists \psi \in \Phi_k \backslash \{1\} \text{ tali che } (\varphi^j - 1)^{-1}(\psi - 1)r \in \Phi_k c$$

se e solo se $\exists l \in I_{k-1}$ tale che $\Phi_k c = \Phi a_l$, dove

$$\forall l \in I_{k-1}, a_l = (\varphi^j - 1)^{-1}(\varphi^l - 1)r \ .$$

Mostriamo che per $l \in I_{k-1}$ i $\Phi_k a_l$ sono tutti distinti.

Siano $l, s \in I_{k-1}$ tali che $\Phi_k a_l = \Phi_k a_s$, e dunque $\exists \lambda \in \Phi_k$ tale che $a_s = \lambda a_l$; poichè $a_l = (\varphi^j - 1)^{-1}(\varphi^l - 1)r$ sarà $(\varphi^j - 1)a_l = (\varphi^l - 1)r$ e dunque

$$\alpha := r + \varphi^j a_l = \varphi^j r + a_l,$$

ma $|(\Phi_k r + a_l) \cap (\Phi_k r + \varphi^j a_l)| = 1$ e dunque

$$(\Phi_k r + a_l) \cap \left(\Phi_k r + \varphi^j a_l\right) = \{\alpha\};$$

analogamente sarà

$$(\Phi_k r + a_l) \cap \left(\Phi_k r + \varphi^j a_l\right) = \{\beta\}$$

con

$$\beta = r + \varphi^j a_s = \varphi^j r + a_s \ .$$

Poichè $\lambda a_l = a_s$ è anche

$$\begin{aligned} \lambda\alpha &\in \lambda\left((\Phi_k r + a_l) \cap \left(\Phi_k r + \varphi^j a_l\right)\right) = \\ &= (\Phi_k r + \lambda a_l) \cap \left(\Phi_k r + \varphi^j \lambda a_l\right) = (\Phi_k r + a_s) \cap \left(\Phi_k r + \varphi^j a_s\right) = \{\beta\} \end{aligned}$$

e dunque

$$r + \varphi^j a_s = \lambda(r + \varphi^j a_l) = \lambda r + \varphi^j \lambda a_l = \lambda r + \varphi^j a_s$$

e così $\lambda = 1$. Dunque

$$\gamma(j,r;k,p) = \left|\{E_r^c | c \in \mathbb{Z}_p^*, \Gamma_j^k \text{ sottografo di } \Gamma(E_c^r)\}\right| = \left|\{E_{a_l}^r | l = 1, 2, ..k-1\}\right| = k-1.$$

□

Otteniamo quindi subito il seguente

Corollario 5.13. *Il numero totale di k-grafi di base (necessariamente dispari, per il teorema precedente) sottografi di* $\Gamma(E_c^r)$ $\forall r \in \mathbb{Z}_p^*$, *con* E_c^r *in* $(\mathbb{Z}_p, \mathcal{B}_k^*, \in)$, *contati ciascuno con la molteplicità con cui appare, al variare di c in* $\mathbb{Z}_p^*$, *è* $\frac{(k-1)^2}{2}$.

Dimostrazione. I k-grafi di base dispari sono tutti e soli i Γ_j^k *con* $j \in I_{\frac{k-1}{2}}$; $\forall j \in I_{(\frac{k-1}{2})}$ $\gamma(j, r; k, p) = k-1$, e dunque Γ_j^k è sottografo di $k-1$ dei $\Gamma(E_c^r)$ al variare di c in $\mathbb{Z}_p^*$, così in totale i $\Gamma(E_c^r)$ hanno $(k-1)(\frac{k-1}{2}) = \frac{(k-1)^2}{2}$ sottografi di base dispari. □

E' possibile dare una cartterizzazione dei grafi associati ai sistemi di cerchi E_r^r

Teorema 5.14. $\forall r \in \mathbb{Z}_p^*$, $\Gamma(E_r^r) = \bigvee_{j=1}^{\frac{k-1}{2}} \Gamma_j^k$.

Dimostrazione. Dal teorema 4.10 abbiamo che $\forall r, c \in \mathbb{Z}_p^*$, $\Gamma(E_c^r) = \bigvee_{j=1}^{\frac{k}{2}} \Theta_j$, dove Θ_j è isomorfo a Π_j^k se $s(r, c, j) = 2$, a Γ_j^k se $s(r, c, j) = 1$ ed al grafo nullo se $s(r, c, j) = 0$. Per $r = c$ si ha che, $\forall j \in I_{k-1}$, $c = r = (1 - \varphi^j)(\varphi^j - 1)r$ e dunque, per il teorema dei cerchi non disgiunti, $s(r, r, j) \neq 0$; inoltre per il teorema 5.11 è $s(r, r, j) \neq 2$, e dunque $s(r, r, j) = 1$ $\forall j \in I_k$ e $\Gamma(E_r^r) = \bigvee_{j=1}^{\frac{k-1}{2}} \Gamma_j^k$. □

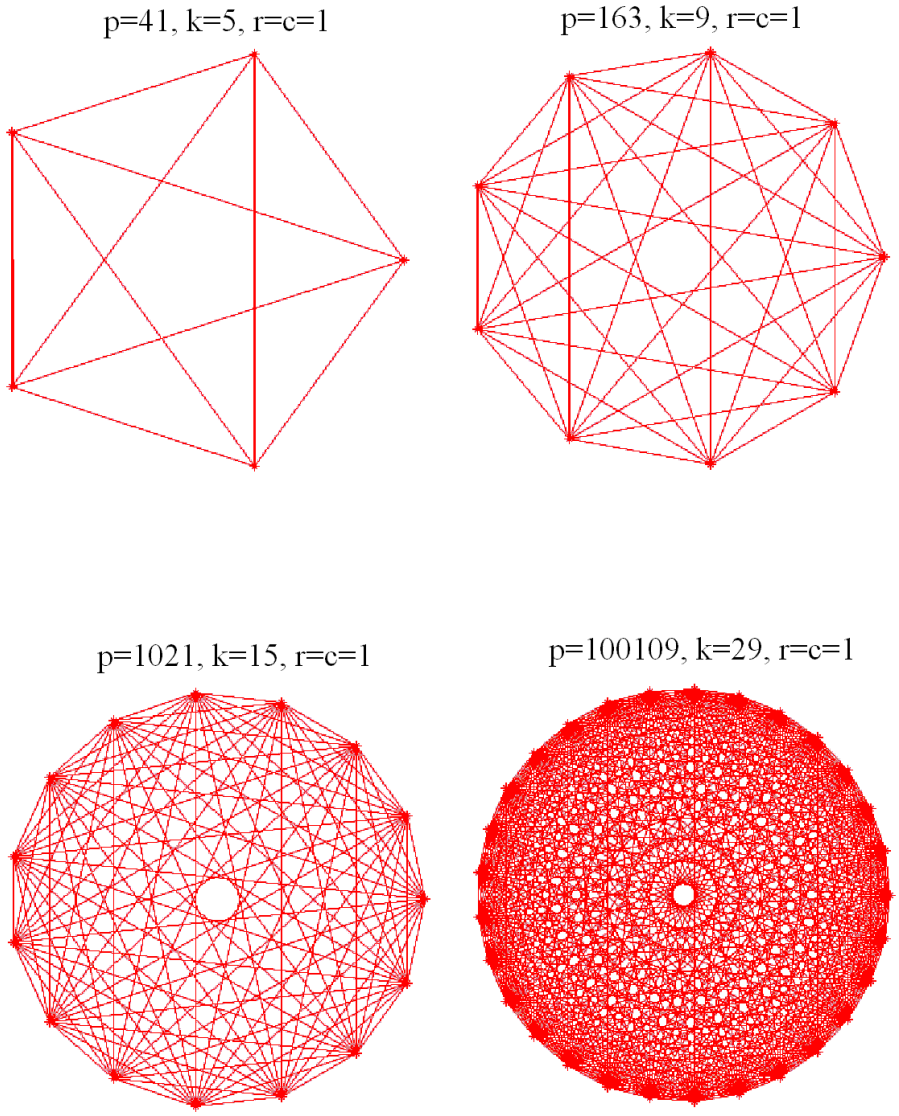


FIGURA 5.2. $\Gamma(E_1^1)$ per $k = 5, 9, 15, 29$

Capitolo 6

Sistemi di cerchi nel piano complesso

Abbiamo visto che alcune proprietà dei cerchi dei BIBD $(\mathbb{Z}_p, \mathcal{B}_k^*, \in)$ sono analoghe a quelle degli usuali cerchi del piano complesso; ad esempio, se k è pari la somma dei punti di intersezione di due cerchi secanti è uguale alla somma dei centri. Ricordiamo inoltre che i cerchi del piano complesso sono i blocchi del BIBD $(\mathbb{C}, \mathcal{B}_T^*, \in)$ associato alla coppia di Ferrero $(\mathbb{C}, T)$ dove T è il sottogruppo di $\mathbb{C}^*$ dei complessi di modulo 1. Allo scopo di estendere e generalizzare questi esempi, consideriamo, per k intero ≥ 3, il sottogruppo T_k di $\mathbb{C}^*$ delle radici k-esime dell'unità, la coppia di Ferrero $(\mathbb{C}, T_k)$ e il BIBD $(\mathbb{C}, \mathcal{B}_{T_k}^*, \in)$ i cui blocchi sono cerchi discreti $T_k r + c$, con $r, c \in \mathbb{C}^*$. In modo analogo al caso degli $\mathbb{Z}_p$, si definiscono i parametri γ e π : $\forall r \in \mathbb{C}^*$, $\forall k$ intero ≥ 3, $\forall j \in I_{k-1}$

$$\begin{aligned} \gamma(j, r; k) &= \{E_c^r \text{ in } (\mathbb{C}^*, \mathcal{B}_{T_k}^*, \in) |\ c \in \mathbb{C}^*,\ \Gamma_j^k \text{ sottografo di } \Gamma(E_c^r)\} \\ \pi(j, r; k) &= \{E_c^r \text{ in } (\mathbb{C}^*, \mathcal{B}_{T_k}^*, \in) |\ c \in \mathbb{C}^*,\ \Pi_j^k \text{ sottografo di } \Gamma(E_c^r)\} \end{aligned}$$

Poichè $\forall k$ intero ≥ 2 $e^{\frac{2\pi i}{k}}$ è un generatore di T_k, è anche

$$\begin{aligned} \gamma(j, r; k) &= \{E_c^r \text{ in } (\mathbb{C}^*, \mathcal{B}_{T_k}^*, \in) |\ \left|(T_k r + c) \cap \left(T_k r + e^{\frac{2\pi i}{k} j} c\right)\right| = 1\} \\ \pi(j, r\, k) &= \{E_c^r \text{ in } (\mathbb{C}^*, \mathcal{B}_{T_k}^*, \in) |\ \left|(T_k r + c) \cap \left(T_k r + e^{\frac{2\pi i}{k} j} c\right)\right| = 2\} \end{aligned}$$

6.1 Contare le intersezioni

Supponiamo inizialmente che $\bar{C}$ e $\bar{C}'$ siano tangenti, e che il punto di tangenza appartenga anche a C e C'; osserviamo che essendo $\bar{C}$ e $\bar{C}'$ tangenti la somma dei raggi è uguale alla distanza dei centri, cioè $2\,|r| = |c - c'|$.

Teorema 6.1. *Se* $\left|\bar{C} \cap \bar{C}'\right| = 1$ *e* $C \cap C' \neq \varnothing$ *allora* k *è pari e* $C \cap C' = \bar{C} \cap \bar{C}'$.

Dimostrazione. Poichè $\varnothing \neq C \cap C' \subset \bar{C} \cap \bar{C}'$ e $\left|\bar{C} \cap \bar{C}\right| = 1$ allora $C \cap C' = \bar{C} \cap \bar{C}'$. Da $|c - c'| = 2|r|$ si ottiene $|r| \leq \frac{|c-c'|}{2} \leq \frac{|c|+|c'|}{2} = |c|$.

Caso 1) $|r| = |c|$
$2|r| = |c - c'| \Rightarrow 4|r|^2 = |c - c'|^2 = |c|^2 - 2\langle c, c'\rangle + |c'|^2 = 2\,|r|^2 - 2\langle c, c'\rangle \Rightarrow$
$-1 = \left\langle \frac{c}{|c|}, \frac{c'}{|c'|} \right\rangle \Rightarrow c' = -c \Longrightarrow \varphi = -1 \in T_k \Rightarrow k$ pari

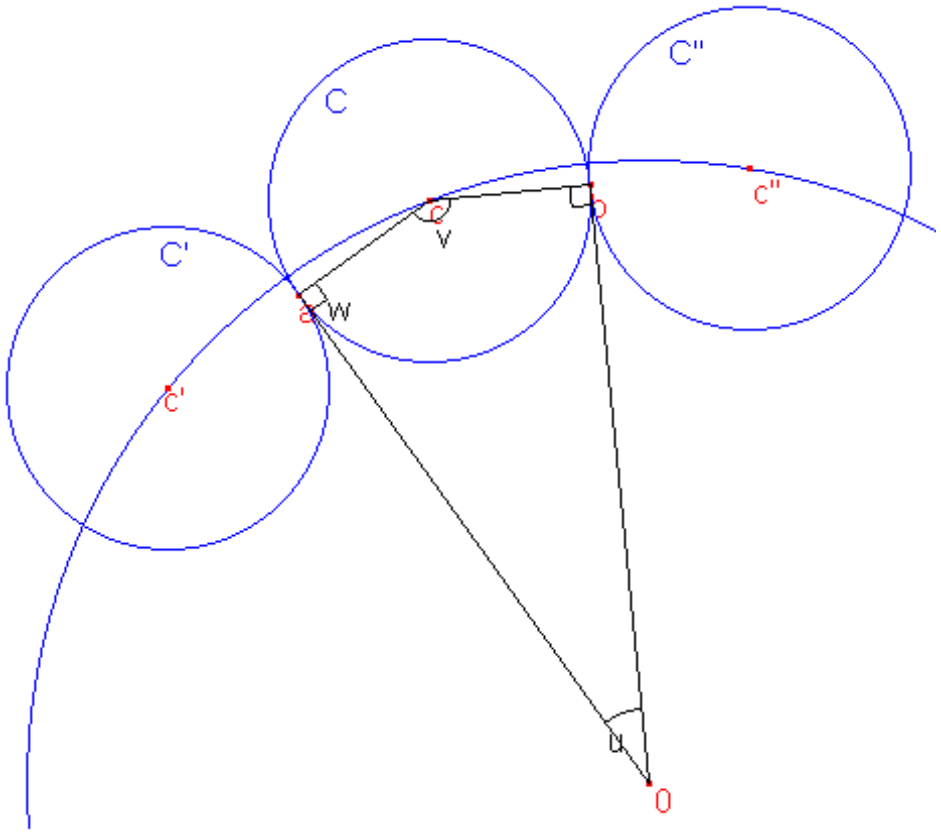


FIGURA 6.1.

Caso 2) $|r| < |c|$ (vedi Figura 6.1)

Sia $\{a\} = \bar{C} \cap \bar{C}' = C \cap C'$ e$\{b\} = \{\varphi a\} = C \cap C'' = \bar{C} \cap \bar{C}''$, allora $\{a, b\} \subset C$ e dunque $\exists s \in \mathbb{N}^*$ $v = \widehat{acb} = \frac{2\pi}{k}s$; inoltre, poichè $b = \varphi a$, $u = \widehat{a0b} = \frac{2\pi}{k}n$ con $n \in \mathbb{N}^*$ e dunque $\pi = u + v = \frac{2\pi}{k}(s + n)$, cioè $k = 2(s + n)$.

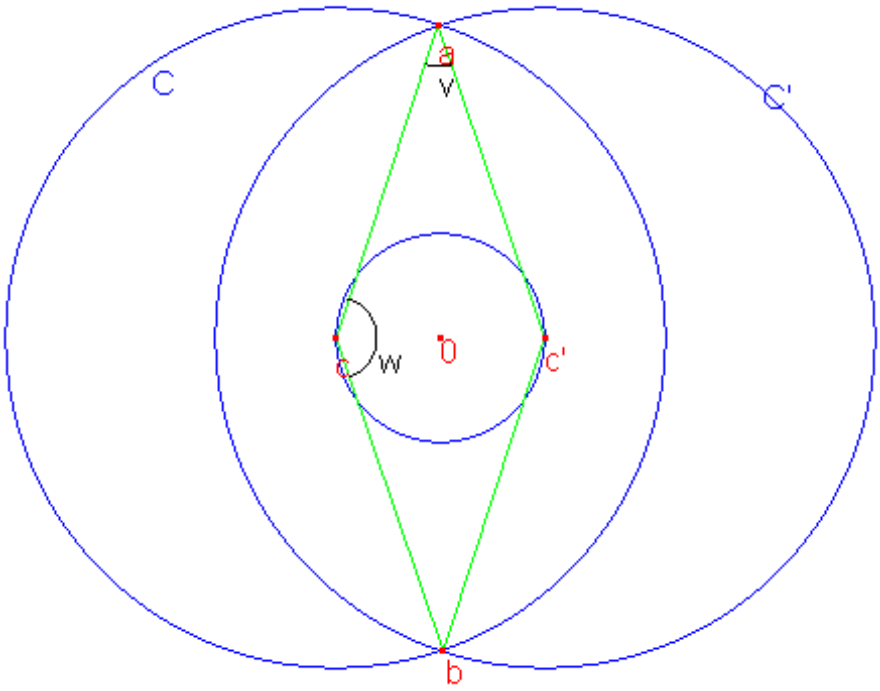


FIGURA 6.2.

□

Supponiamo ora che $\bar{C}$ e $\bar{C}'$ siano secanti, e poniamo $\bar{C} \cap \bar{C}' = \{a, b\}$. Osserviamo che essendo $\bar{C}$ e $\bar{C}'$ secanti la somma dei raggi è maggiore della distanza dei centri; ci sono 4 casi:

Caso1) $c = c'$ (vedi Figura 6.2)

Allora $\varphi = e^{\frac{2\pi i}{k}n} = -1 \in T_k$, cioè $n = \frac{k}{2}$ e dunque deve esere k pari, inoltre $2|r| > |c - c'| = 2|c|$, $a + b = c + c' = 0$ e $|a - c| = |b - c| = |-a - c| = |a - c'| = |b - c'|$ e dunque $acbc'$ è un rombo e $v + w = \widehat{cac'} + \widehat{bca} = \pi$.

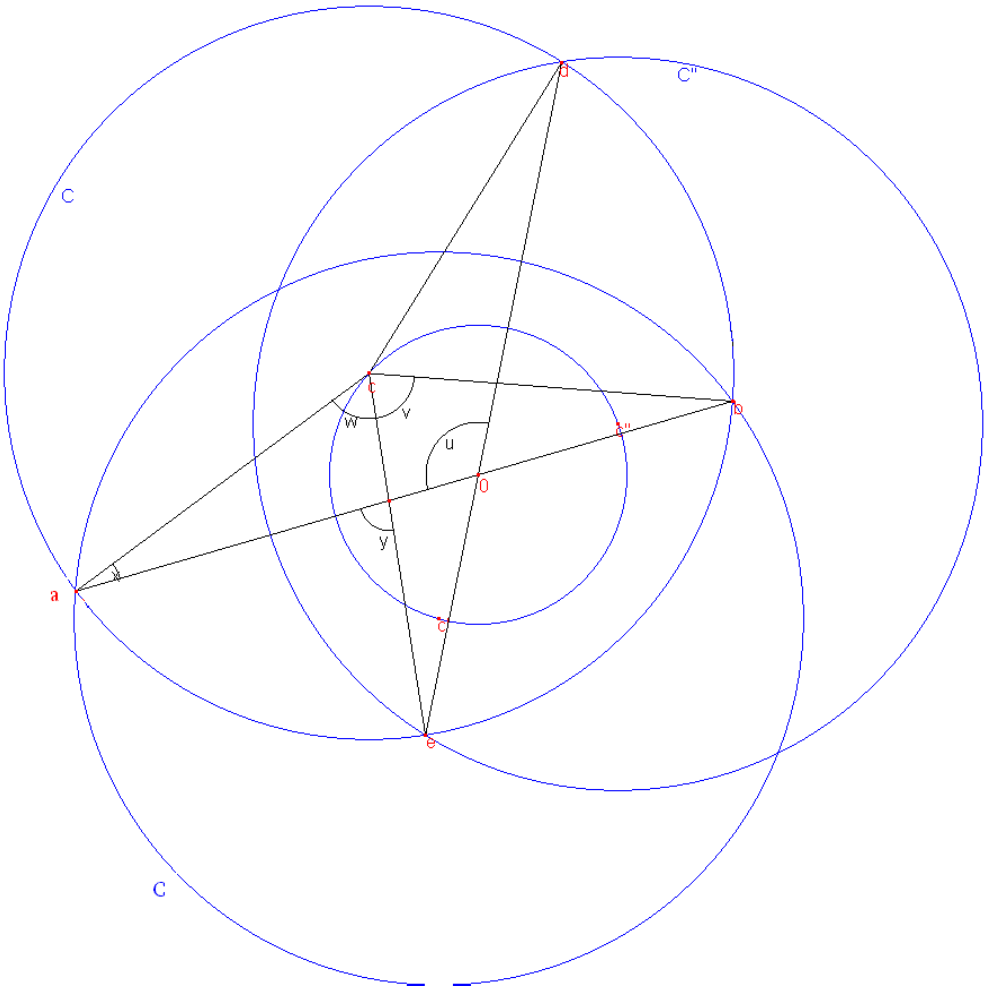


FIGURA 6.3.

Caso2) $c \neq c'$**,** $|r| > |c|$ (vedi Figura 6.3)

Poniamo $d = \varphi a$, e=φb, dunque $\{e, d\} = \bar{C} \cap \bar{C}''$; siano inltre $x = \widehat{bac}$, $w = \widehat{ace}$, $v = \widehat{acb}$, $u = \widehat{a0d}$, $y = w+x$. Poichè $d = \varphi a$ è $u = \frac{2\pi}{k}n$; inoltre $u+v+2w+2x = u + v + 2y = 2\pi$ (somma angoli interni del quadrilatero $a0dc$), $w + v + 2x = \pi$ (somma angoli interni del triangolo isoscele abc), e dunque $w + u = w + (2\pi - 2y - v) = w+2\pi-2(w+x)-v = 2\pi-w-2x-v = 2\pi-(w+2x+v) = 2\pi-\pi = \pi$.

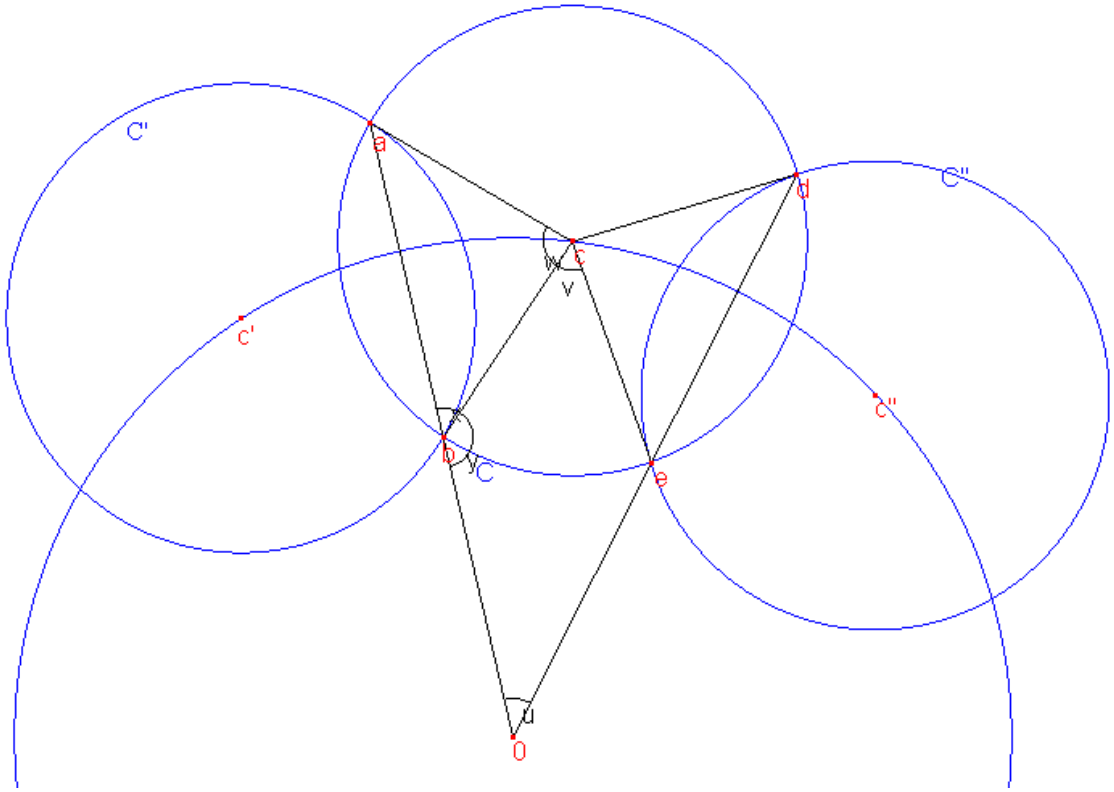


FIGURA 6.4.

Caso 3) $c' \neq -c$**,** $|r| < |c|$ (vedi Figura 6.4)

Come prima sia $\varphi a = d$, $\varphi b = e$, e dunque $\bar{C} \cap \bar{C}'' = \{d, e\}$; inoltre $w = \widehat{acb}$, $u = \widehat{a0d} = \frac{2\pi}{k}n$, $x = \widehat{abc} = \widehat{bca}$, $y = \widehat{0ec} = \widehat{0bc}$; si ha $u+v+2y = 2\pi$ (somma degli angoli interni del quadrilatero $0bce$), $w+2x = \pi$ (somma degli angoli interni del triangolo isoscele abc), $x+y = \pi$ e dunque $w+u+v = (\pi-2x)+(2\pi-v-2y)+v = 3\pi - 2(x+y) = \pi$.

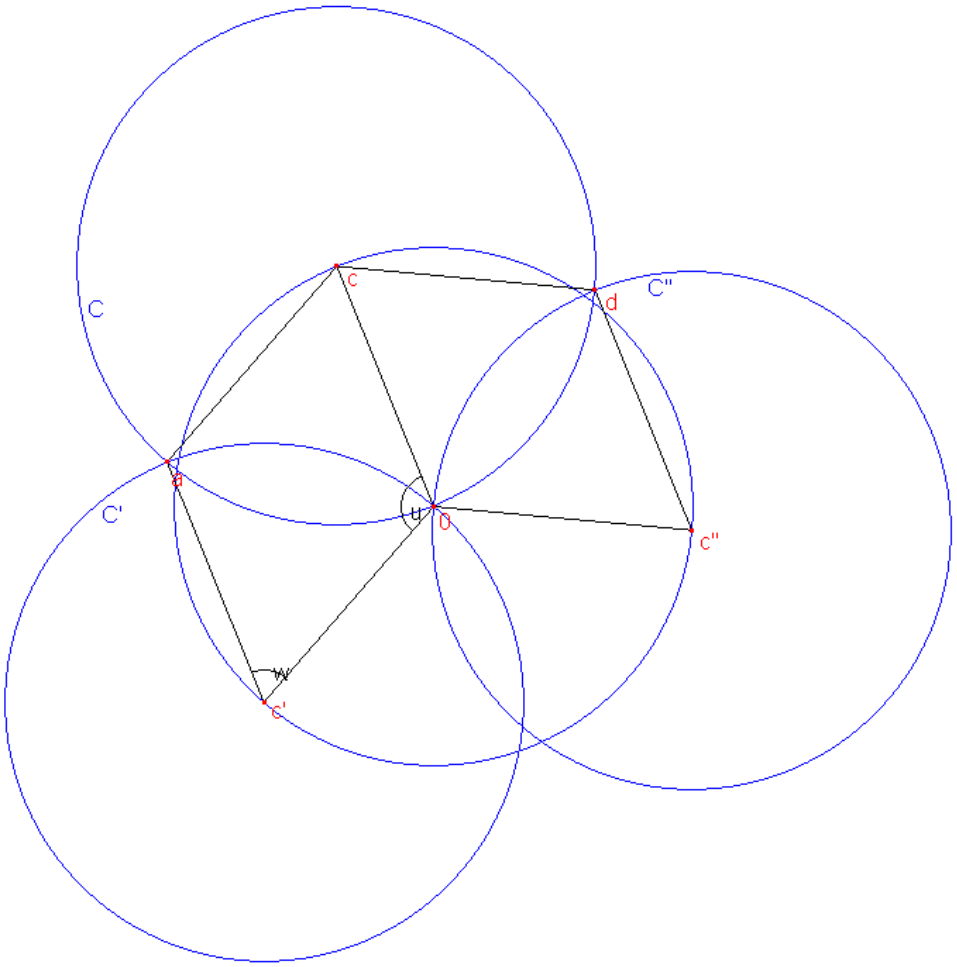


FIGURA 6.5.

Caso 4) $|c| = |r|$, $c' \neq c$ (vedi Figura 6.5)

E' $\{a, 0\} = \bar{C} \cap \bar{C}'$, e poniamo $d = \varphi a$, dunque $\{d, 0\} = \bar{C} \cap \bar{C}''$. Siano $u = \widehat{c'0c} = \frac{2\pi}{k} n$, $w = \widehat{ac'0}$; si ha $|a - c'| = |a - c| = |r| = |c| = |c - 0| = |c' - 0|$ e dunque $ac0c'$ è un rombo e $u + w = \pi$.

E' facile dopo questa discussione dimostrare il

Teorema 6.2. *Se* $\bar{C} \cap \bar{C}' = \{a, b\}$, $C \cap C' \neq \varnothing$ *e* $\{a, b\} \subset C$ *allora* k *pari e* $C \cap C' = \{a, b\}$.

Dimostrazione. Osserviamo preliminarmente che $\varnothing \neq C \cap C \subset \bar{C} \cap \bar{C}' = \{a, b\}$, e dunque almeno uno tra a e b appartiene a C'. Ma $\widehat{ac'b} = \widehat{acb}$ e dunque $a \in C'$ se

e solo se $b \in C'$ e dunque $\{a, b\} = C'$, cioè $C \cap C' = \bar{C} \cap \bar{C}' = \{a, b\}$, così come $\{\varphi a, \varphi b\} = C \cap C' = \bar{C} \cap \bar{C}'$.

Trattiamo separatamente i 4 casi precedenti, facendo riferimento alle stesse figure:

Caso 1) Abbiamo già osservato che deve essere k pari.

Caso 2) E' $\{a, b, d, e\} \subset C$, dove ricordiamo $d = \varphi a$, $e = \varphi b$, dunque $\widehat{acb} = v + w \in \frac{2\pi}{k}\mathbb{N}$, $\widehat{ace} = w \in \frac{2\pi}{k}\mathbb{N}$ e così anche $(v + w) - w = w = \pi - u = \frac{2\pi}{k}\left(\frac{k}{2} - n\right) \in \frac{2\pi}{k}\mathbb{N}$, cioè $2|k$.

Caso 3) E' $\{a, b, d, e\} \subset C$ e dunque $\widehat{acb} = w \in \frac{2\pi}{k}\mathbb{N}$, $v = \widehat{bce} \in \frac{2\pi}{k}\mathbb{N}$ e così anche $v + w = \pi - u = \frac{2\pi}{k}\left(\frac{k}{2} - n\right) \in \frac{2\pi}{k}\mathbb{N}$, cioè $2|k$.

Caso 4) E' $b = 0$, $\{a, 0\} \subset C$ e dunque $w = \widehat{ac0} = \pi - u = \frac{2\pi}{k}\left(\frac{k}{2} - n\right) \in \frac{2\pi}{k}\mathbb{N}$, cioè $2|k$.

□

E' poi immediato il

Corollario 6.3. *Se k è dispari e $C \cap C' = \varnothing$ allora $|C \cap C'| = 1$ e $\left|\bar{C} \cap \bar{C}'\right| = 2$*

Dimostrazione. E' $0 < |C \cap C'| \leq \left|\bar{C} \cap \bar{C}'\right| \leq 2$. Se fosse $\left|\bar{C} \cap \bar{C}'\right| = 1$ sarebbe k pari per il teorema 6.1, dunque $\left|\bar{C} \cap \bar{C}'\right| = 2$; a questo punto se fosse $|C \cap C'| = 2$ sarebbe k pari per il teorema 6.2 □

Una sorta di proposizioni inverse dell'ultimo teorema sono le seguenti.

Teorema 6.4. *Se k è pari e $\bar{C} \cap \bar{C}' = \{a, b\} \subset C$, allora $\{a, b\} = C \cap C'$.*

Dimostrazione. Osserviamo preliminarmente che basta dimostrare che $d = \varphi a \in C$ ed $e = \varphi b \in C$, infatti allora $C \cap C' = \varphi^{-1}(C \cap C'') = \varphi^{-1}(C \cap \varphi C) = \varphi^{-1}\{\varphi a, \varphi b\} = \{a, b\}$. Abbiamo i 4 casi:

Caso 1) $a = -b$ e $\varphi = -1$, dunque $\{\varphi a, \varphi b\} = \{-a, -b\} = \{a, b\} \subset C$.

Caso 2) $u = \widehat{a0d} = \frac{2\pi}{k}n$ e dunque $w = \pi - u = \frac{2\pi}{k}(\frac{k}{2} - n) \in \frac{2\pi}{k}\mathbb{N}$, $\{a, b\} \subset C$ e dunque $\widehat{acb} = v + w \in \frac{2\pi}{k}\mathbb{N}$ ed anche $\widehat{bce} = v = (v + w) - w \in \frac{2\pi}{k}\mathbb{N}$; adesso $\widehat{ecd} = \widehat{acb} \in \frac{2\pi}{k}\mathbb{N}$ e dunque anche $d \in \frac{2\pi}{k}\mathbb{N}$.

Caso 3) Poichè $w = \widehat{acb} \in \frac{2\pi}{k}\mathbb{N}$ e $u = \widehat{a0d} \in \frac{2\pi}{k}\mathbb{N}$, anche $\widehat{bce} = v = \pi - (v + w) = \frac{2\pi}{k}\left(\frac{k}{2} - \frac{v+w}{\frac{2\pi}{k}}\right) \in \frac{2\pi}{k}\mathbb{N}$, dunque $d \in C$, ma, come prima, $\widehat{dce} = \widehat{acb} \in \frac{2\pi}{k}\mathbb{N}$ e dunque anche $d \in C$.

Caso 4) E' $w = \widehat{ac0} = \widehat{acb} \in \frac{2\pi}{k}\mathbb{N}$ e dunque $\widehat{acd} = 2w$, cioè $d \in C$; poichè $\varphi b = \varphi 0 = 0$, banalmente $e = \varphi b \in C$.

□

Teorema 6.5. *Se $\bar{C} \cap \bar{C}' = \{a, b\}$, $C \cap C' \neq \varnothing$ e k pari allora $C \cap C' = \{a, b\}$, ed in particolare a e b sono vertici di C, k-agono regolare inscritto in $\bar{C}$.*

Dimostrazione. Consideriamo sempre gli stessi 4 casi:

Caso 1) $a+b = c+c' = 0$, dunque $a = -b$; se $a \in C \cap C'$ allora $b = -a \in -(C \cap C') = (-C) \cap (-C') = C' \cap C$, analogamente se $b \in C \cap C'$, allora $a \in C \cap C'$.

Caso 2) Se $a \in C \cap C'$ allora $d = \varphi a \in C \cap C''$ e dunque $\widehat{acd} = 2w + v \in \frac{2\pi}{k}\mathbb{N}$; ma $w = \pi - u = \pi - \frac{2\pi n}{k} = \frac{2\pi}{k}(\frac{k}{2} - n) \in \frac{2\pi}{k}\mathbb{N}$ e dunque anche $\widehat{acb} = w + v \in \frac{2\pi}{k}\mathbb{N}$, cioè $b \in C$ e dunque, poichè $\widehat{ac'b} = \widehat{acb}$, $b \in C \cap C'$. Se $b \in C \cap C'$ allora $e = \varphi b \in C \cap C''$, e dunque $v = \widehat{ecb} \in \frac{2\pi}{k}\mathbb{N}$, ma, come prima, $u \in \frac{2\pi}{k}\mathbb{N}$ e dunque anche $\widehat{acb} = v + w \in \frac{2\pi}{k}\mathbb{N}$, cioè $a \in C$ e, poichè $\widehat{acb} = \widehat{ac'b}$, $a \in C \cap C'$.

Caso 3) Se $a \in C \cap C'$ allora $d = \varphi a \in C \cap C''$ e dunque $\widehat{acd} = 2w + v \in \frac{2\pi}{k}\mathbb{N}$; ma $w + v = \pi - u = \frac{2\pi}{k}(\frac{k}{2} - n) \in \frac{2\pi}{k}\mathbb{N}$ e così anche $\widehat{ac'b} = \widehat{acb} = w = (2w - v) - (w + v) \in \frac{2\pi}{k}\mathbb{N}$, cioè $b \in C \cap C'$. Se $b \in C \cap C'$, allora $e = \varphi b \in C \cap C'$ e dunque $v = \widehat{bce} \in \frac{2\pi}{k}\mathbb{N}$, e dunque , poichè $w + v = \pi - u \in \frac{2\pi}{k}\mathbb{N}$, anche $\widehat{ac'b} = \widehat{acb} = w = (v + w) - v \in \frac{2\pi}{k}\mathbb{N}$, cioè $a \in C \cap C'$.

Caso 4) In questo caso è $\bar{C} \cap \bar{C}' = \{a, 0\}$. Se $a \in C \cap C'$, poichè $\widehat{ac0} = \widehat{ac'0} = w = \pi - u = \pi(\frac{k}{2} - n) \in \frac{2\pi}{k}\mathbb{N}$, $0 \in C \cap C'$. Se $0 \in C \cap C'$ in modo del tutto analogo, poichè $\widehat{ac0} = \widehat{ac'0} \in \frac{2\pi}{k}\mathbb{N}$ è $a \in C \cap C'$.

□

Corollario 6.6. *Se k è pari e $C \cap C' \neq \varnothing$ allora $C \cap C' = \bar{C} \cap \bar{C}'$.*

Dimostrazione. Se $\left|\bar{C} \cap \bar{C}'\right| = 1$ è ovvio; se $\left|\bar{C} \cap \bar{C}'\right| = 2$ segue immediatamente dall'ultimo teorema. □

6.2 Contare i sottografi

Possiamo a questo punto calcolare il valore di γ e π. Supponiamo k intero ≥ 3, $r \in \mathbb{C}^*$, $j \in I_{n-1}$, $\varphi = e^{\frac{2\pi i}{k}j} \in T_k$.

6.2.1 Caso k pari

Teorema 6.7. *Se k è pari allora $\gamma(j,r;k)=1$*

Dimostrazione. Sia E_c^r in $(\mathbb{C},\mathcal{B}^*_{T_k},\in)$ tale che Γ_j^k è sottografo di $\Gamma(E_c^r)$; è allora

$$\forall C\in E_c^r \quad \left|C\cap e^{\frac{2\pi i}{k}j}C\right|=1.$$

Sia

$$C=T_kr+c\in E_c^r,\ C'=\varphi^{-1}C,\ \bar{C}=Tr+c,\ \bar{C}'=\varphi^{-1}\bar{C}.$$

Per l'ultimo corollario del precedente paragrafo è $\left|\bar{C}\cap\bar{C}'\right|=\left|C\cap C'\right|$. Sia $\{a\}=C\cap C'$, $\psi\in T_k$ tale che $a=\psi r+c$; poichè $E_c^r=E_c^{\psi r}$, possiamo supporre, a meno di cambiare r con ψr, che sia $a=r+c$, e che dunque il quadrilatero $0rac$ sia un parallelogramma. Facciamo riferimento alle notazioni della figura 1; $\widehat{a0c}=\widehat{c0b}$ e $\widehat{a0b}=\frac{2\pi}{k}j$ e dunque $\tilde{u}:=\widehat{a0c}=\frac{\pi j}{k}$, $\tilde{v}:=ac0=\frac{\pi}{2}-\tilde{u}=\frac{\pi}{k}(\frac{k}{2}-j)$; inoltre, considerando il triangolo rettangolo $0ac$

$$|r|=|a-c|=|c-0|\sin(\tilde{u})=|c|\sin(\frac{\pi j}{k}).$$

Poichè $0rac$ è un parallelogramma, e $\widehat{r0c}=\widehat{a0c}+\widehat{0ac}=\frac{\pi}{2}+\frac{\pi j}{k}$, è

$$c=|c|\,\frac{r}{|r|}e^{-i(\frac{\pi}{2}+\frac{\pi j}{k})}=\frac{r}{\sin(\frac{\pi j}{k})}e^{-i(\frac{\pi}{2}+\frac{\pi j}{k})},$$

e dunque c è univocamente determinato da j,r e k (a meno di un fattore $e^{\frac{2\pi is}{k}}$ con $s\in\mathbb{N}$) e $\gamma(j,r;k)\le 1$.

Mostriamo ora che, dati k,r e j, per

$$c=\frac{r}{\sin(\frac{\pi j}{k})}e^{-i(\frac{\pi}{2}+\frac{\pi j}{k})}$$

(come sopra) è Γ_j^k sottografo di E_c^r. Siano

$$\begin{aligned}\varphi &= e^{\frac{2\pi i}{k}j},\qquad c'=\varphi^{-1}c,\qquad a=\frac{c+c'}{2}\\ C &= T_kr+c,\ C'=\varphi^{-1}C,\ \bar{C}=Tr+c,\ \bar{C}'=\varphi^{-1}\bar{C}\end{aligned}$$

E' $c'0c=a'0a+a0c=\frac{2\pi j}{k}$ e $c'0a=a0c$, e dunque $\widehat{c'0a}=\widehat{a0c}=\frac{\pi j}{k}$; inoltre, considerando i triangoli rettangoli $\widehat{c'0a}$ e $\widehat{a0c}$, si ha

$$\begin{gathered}|c-c'|=|c'-a|+|a-c|=\\ =|c'|\sin(c'0a)+|c'|\sin(a0c)=2\,|c|\sin(\tfrac{\pi j}{k})=2\tfrac{|r|}{\sin(\frac{\pi j}{k})}\sin(\tfrac{\pi j}{k})=2\,|r|\,,\end{gathered}$$

dunque

$$\bar{C} \cap \bar{C}' = \{\frac{c+c'}{2}\} = \{a\}.$$

Dobbiamo mostrare che $a = \frac{c+c'}{2} \in C \cap C'$, o equivalentemente che $\{a-c, a-c'\} \subset T_k r$. Osserviamo che

$$a - c = \frac{c+c'}{2} - c = \frac{c'-c}{2}, a - c' = \frac{c+c'}{2} - c' = \frac{c-c'}{2}.$$

E' $\widehat{c0(-c')} = \pi - c'0c = \pi - \frac{2\pi j}{k}$, e dunque $\widehat{c0\left(\frac{c-c'}{2}\right)} = \frac{\pi}{2} - \frac{\pi j}{k}$, e anche $\widehat{r0\left(\frac{c-c'}{2}\right)} = r0c + c0\left(\frac{c-c'}{2}\right) = \frac{\pi}{2} + \frac{\pi j}{k} + \frac{\pi}{2} - \frac{\pi j}{k} = \pi$. Considerando il triangolo rettangolo $c0\left(\frac{c-c'}{2}\right)$, è

$$\left|\frac{c-c'}{2}\right| = \left|\frac{c-c'}{2} - 0\right| =$$
$$= |c-0| \cos(\widehat{c0\left(\frac{c-c'}{2}\right)}) = |c| \cos(\frac{\pi}{2} - \frac{\pi j}{k}) = |c|\, sen(\frac{\pi j}{k}).$$

Dunque

$$a - c' = \frac{c-c'}{2} = \left|\frac{c-c'}{2}\right| \frac{r}{|r|} e^{-\pi i} =$$
$$= |c| \sin(\frac{\pi j}{k}) \frac{r}{|r|}(-1) = \frac{|r|}{\sin(\frac{\pi j}{k})} \sin(\frac{\pi j}{k}) \frac{r}{|r|}(-1) = -r \in T_k r,$$

perchè $2|k$ e dunque $-1 \in T_k$. Da qui

$$a - c = \frac{c'-c}{2} = -\frac{c-c'}{2} = r \in T_k r.$$

□

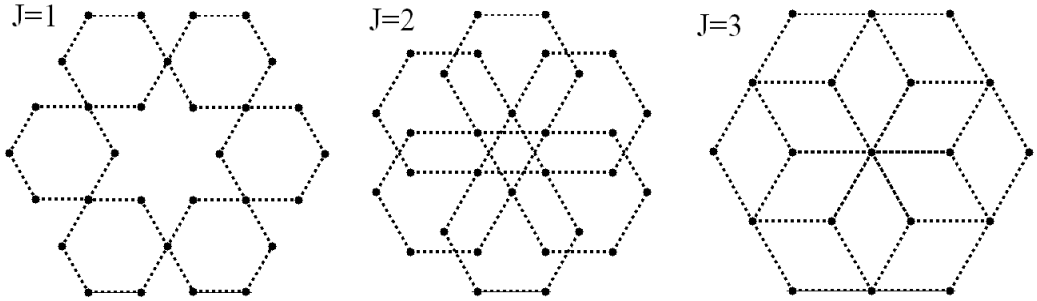


FIGURA 6.6. Tutti i sistemi di cerchi per $r = 1$, $k = 6$, $j = 1, 2, 3$ tali che Γ_1^6 sia sottografo di $\Gamma(E_c^r)$

Teorema 6.8. *Se k è pari, allora $\pi(j, r; k) = \frac{k}{2} - 1$.*

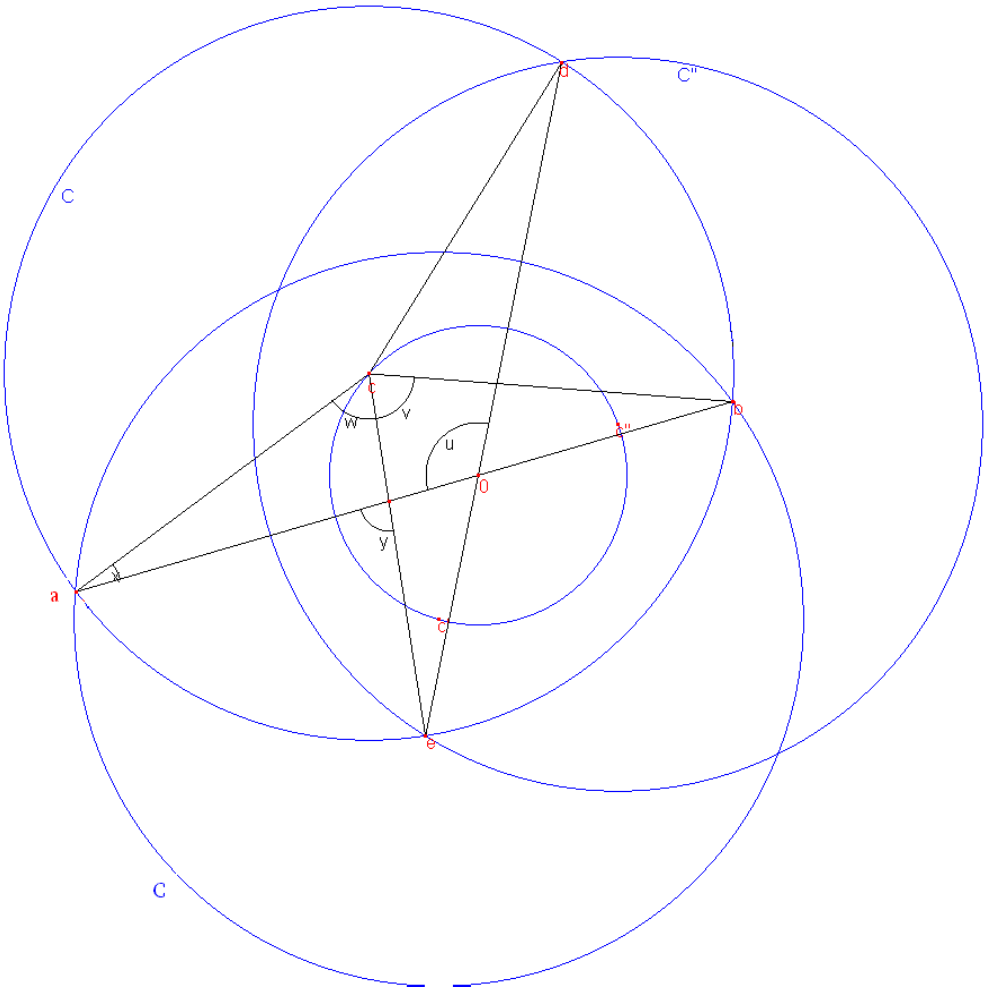
Dimostrazione. Sia E_c^r in $(\mathbb{C}, \mathcal{B}^*_{T_k}, \in)$ tale che Π_j^k è sottografo di $\Gamma(E_c^r)$; allora

$$\forall C \in E_c^r \quad \left| C \cap e^{\frac{2\pi i}{k} j} C \right| = 1.$$

Sia

$$C = T_k r + c \in E_c^r,\ C' = \varphi^{-1} C,\ \bar{C} = Tr + c,\ \bar{C}' = \varphi^{-1} \bar{C}.$$

Per l'ultimo corollario del precedente paragrafo è $\left|\bar{C} \cap \bar{C}'\right| = |C \cap C'|$. Sia $\{a, b\} = C \cap C'$, $\psi \in T_k$ tale che $a = \psi r + c$; poichè $E_c^r = E_c^{\psi r}$, possiamo supporre, a meno di cambiare r con ψr, $a = r + c$, e dunque $0, r, a$ e c sono vertici di un parallelogramma. Possiamo trattare contemporaneamente i casi 1,2,3 e 4, riportando, per chiarezza, la figura del caso 3.



Poichè $\widehat{a0c} = \widehat{c0d}$ e $\widehat{a0c} + \widehat{c0d} = \widehat{a0d} = \frac{2\pi j}{k}$, è $\widehat{a0c} = \widehat{c0d} = \frac{\pi j}{k}$; inoltre è $0 < \widehat{acb} < \pi$, infatti, se fosse $\widehat{acb} = \pi$, sarebbe $b - c = -(a - c)$ e dunque $\frac{c+c'}{2} = \frac{a+b}{2} = c$, e

dunque $c' = \varphi c = c$, cioè $\varphi = e^{\frac{2\pi i}{k}j} = 1$. Poichè $\{a, b\} \subset C$, $\exists t \in I_{\frac{k}{2}-1}$ tale che $\widehat{acb} = \frac{2\pi}{k}t$; inoltre $|a-c| = |b-c| = |r|$, e dunque il triangolo bac è isoscele e $\widehat{bac} = \widehat{abc} = \frac{\pi - \widehat{a0b}}{2} = \frac{\pi}{2}(\frac{k}{2} - t) = \frac{\pi}{k}s$, con $s = \frac{k}{2} - t \in \mathbb{N}$. Poniamo

$$\alpha = \frac{\pi j}{k} \text{ e } \beta = \frac{\pi s}{k}.$$

Considerando i triangoli rettangoli $ac(\frac{c+c'}{2})$ e $\frac{c+c'}{2}c0$ si ha

$$\begin{gathered} |a| = \left|a - \tfrac{c+c'}{2}\right| + \left|\tfrac{c+c'}{2}\right| = \\ = |a-c|\cos(\widehat{bac}) + |c|\cos(\widehat{a0c}) = |r|\cos\beta + |c|\cos\alpha \end{gathered}$$

e dunque

$$|a|^2 = |r|^2\cos^2(\alpha) + |c|^2\cos^2\beta + 2|rc|\cos\alpha\cos\beta;$$

ma è anche, poichè $\widehat{r0c} = \alpha + \beta$,

$$\begin{gathered} |a|^2 = |r+c|^2 = |r|^2 + |c|^2 + 2|rc|\cos(\alpha+\beta) = \\ = |r|^2 + |c|^2 + 2|rc|(\cos\alpha\cos\beta - \sin\alpha\sin\beta) \end{gathered}$$

e dunque, sottraendo membro a membro le due espressioni per $|a|^2$,

$$\begin{gathered} 0 = (1-\cos^2\alpha)|c|^2 + (1-\cos^2\beta)|r|^2 - 2|rc|\sin\alpha\sin\beta = \\ \sin^2\alpha|c|^2 + \sin^2\beta|r|^2 - 2|rc|\sin\alpha\sin\beta = (|c|\sin\alpha - |r|\sin\beta) = 0 \end{gathered}$$

e così

$$\begin{aligned} |c| &= \frac{\sin\beta}{\sin\alpha}|r|, \\ c &= |c|\frac{r}{|r|}e^{-i(\alpha+\beta)} = r\frac{\sin\beta}{\sin\alpha}e^{-i(\alpha+\beta)}. \end{aligned}$$

Dunque, fissati r, k e j, scelto $T \in I_{\frac{k}{2}-1}$, risulta univocamente determinato (a meno di un fattore $e^{\frac{2\pi in}{k}}$) c tale che Π_j^k sia sottografo di $\Gamma(E_c^r)$. Dunque $\pi(j, r; k) \leq \frac{k}{2} - 1$.

Mostriamo ora che $\forall t \in I_{\frac{k}{2}-1}$, se definimo s, α, β e c come sopra, abbiamo

$$\left|(T_k r + c) \cap \varphi^{-1}(T_k r + c)\right| = 2$$

e dunque Π_j^k è sottografo di $\Gamma(E_c^r)$. Poniamo come al solito

$$c' = \varphi^{-1}c, C = T_k r + c, C' = \varphi^{-1}C, \bar{C} = Tr + c, \bar{C} = \varphi^{-1}\bar{C}.$$

Poichè $\varphi = e^{\frac{2\pi ij}{k}} = e^{2i\alpha}$, è

$$c' = \varphi^{-1}c = r\frac{\sin\beta}{\sin\alpha}e^{-i(\beta-\alpha)}.$$

Consideriamo i triangoli rettangoli $c0\frac{c+c'}{2}$ e $\frac{c+c'}{2}0c$, si ha

$$|c'-c| = \left|c'-\tfrac{c+c'}{2}\right| + \left|\tfrac{c+c'}{2}-c\right| = |c'|\sin\left(c'0\tfrac{c+c'}{2}\right) + |c|\sin\left(\tfrac{c+c'}{2}0c\right) = \\ = 2\,|c|\sin\alpha = 2\tfrac{\sin\beta}{\sin\alpha}\,|r|\sin\alpha = 2\sin\beta r < 2\,|r|$$

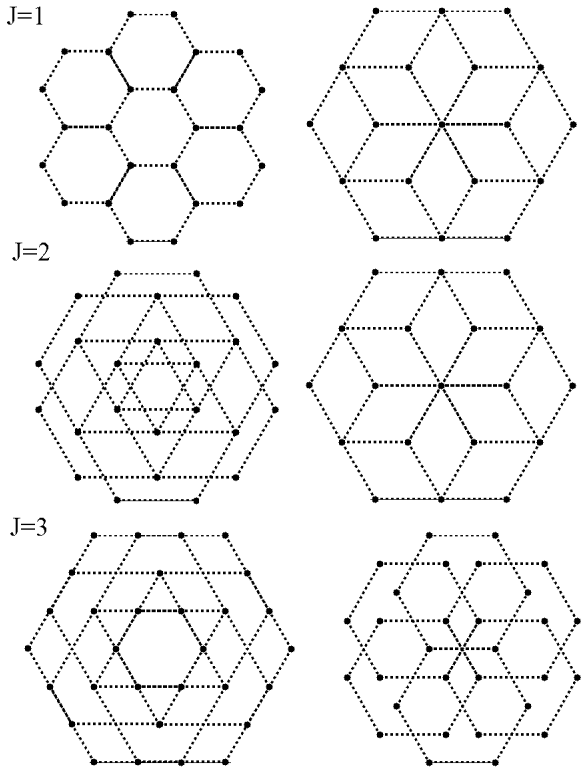
dunque $\left|\bar{C}\cap\bar{C}'\right| = 2$. Sia $\{a,b\} = \bar{C}\cap\bar{C}'$, con $|a| > |b|$; poichè $a \in \mathbb{R}\frac{c+c'}{2}$ e $\widehat{c'0c} = \widehat{c'0a} + \widehat{a0c} = 2\alpha$, si ha e $\widehat{c'0a} = \widehat{a0c} = \alpha$; inoltre $\alpha+\beta = r0c = r0a + a0c = r0a + \alpha$, e dunque

$$a = |a|\,\frac{r}{|r|}e^{-i\beta}.$$

Ora,

$$r + c = r\left(1 + \tfrac{\sin\beta}{\sin\alpha}e^{-i(\alpha+\beta)}\right) = re^{-i\beta}\left(\tfrac{\sin\beta}{\sin\alpha}e^{-i\alpha} + e^{i\beta}\right) = \\ = e^{-i\beta}\left(\tfrac{\sin\beta}{\sin\alpha}(\cos\alpha - i\sin\alpha) + \cos\beta + i\sin\beta\right) = \\ = re^{-i\beta}\tfrac{\sin\beta\cos\alpha+\cos\beta\sin\beta}{\sin\alpha} = re^{-i\beta}\tfrac{\sin(\alpha+\beta)}{\sin\alpha} \in \mathbb{R}a$$

dunque $|(r+c)-c'| = |(r+c)-c| = |r|$, cioè $r+c \in \bar{C}\cap\bar{C}' = \{a,b\}$, ma $|r+c| = \frac{\sin(\alpha+\beta)}{\sin\alpha}\,|r| > \frac{\sin\beta}{\sin\alpha}\,|r| = |c|$, e dunque $a = r+c \in C$. Considerando il triangolo isoscele $a0b$, si ha $\widehat{a0b} = \pi - 0ab - 0ba = \pi - 2\beta = \pi - 2\frac{\pi\left(\frac{k}{2}-t\right)}{k} = \frac{2\pi}{k}(\frac{k}{2} - \frac{k}{2} + t) = \frac{2\pi}{k}t \in \frac{2\pi}{k}\mathbb{N}$, e anche $b \in C$. Si conclude che $\{a,b\} = C\cap C'$ con il teorema 6.4. □



Tutti i sistemi di cerchi per $r = 1, k = 6$, $j = 1,2,3$ tali che Π_j^k sottografo di $\Gamma(E_c^r)$

E' a questo punto agevole contare il numero totale di sottografi di base.

Corollario 6.9. *Se k è pari, il numero totale di grafi di base (pari o dispari) che compaiono come sottografo $\Gamma(E_c^r)$ al variare di c in $\mathbb{C}^*$ (ciascuno contato in base al numero di volte in cui compare) è $\left(\frac{k}{2}\right)^2$.*

Dimostrazione. I grafi di base pari e dispari sono Γ_j^k, Π_j^k, con $j \in I_{\frac{k}{2}}$; ciascuno dei Π_j^k compare $\frac{k}{2}-1$ volte, ciascuno dei Γ_j^k compare 1 volta, per cui in totale abbiamo $\left(\left(\frac{k}{2}-1\right)+1\right)\frac{k}{2} = \left(\frac{k}{2}\right)^2$ sottografi di base. □

6.2.2 Caso k dispari

Teorema 6.10. *Se k è dispari allora $\gamma(j,r;k) = k-1$ e $\pi(j,r;k) = 0$.*

Dimostrazione. Il corollario del teorema 6.2 dice che se k è dispari, $C, C' \in E_c^r$ in $(\mathbb{C}, \mathcal{B}_{T_k}, \in)$ e $C \cap C' \neq \varnothing$ allora $|C \cap C'| = 1$ e $\left|\bar{C} \cap \bar{C}'\right| = 2$; dunque $\pi(j,r;k) = 0$, mentre $\gamma(j,r;k) = \left|\{E_c^r \text{ in } (\mathbb{C}, \mathcal{B}_{T_k}, \in)|\ c \in \mathbb{C}^*,\ \forall C \in E_c^r\ C \cap C' \neq \varnothing\}\right|$. Per chiarezza poniamo $\forall c \in \mathbb{C}^*$, $\forall n \in \mathbb{N}$ $E_{c,n}^r = \{T_n r + d|\ d \in T_n c\}$, e osserviamo che se Γ_j^k è sottografo di $\Gamma(E_{c,k}^r)$ allora Π_j^k è sottografo di $\Gamma(E_{c,2k}^r)$; infatti, sia $C = T_k r + c \in E_c^r$, $C' = \varphi^{-1}C$, $\{a\} = C \cap C'$ e $\{a,b\} = \bar{C} \cap \bar{C}'$, allora se poniamo $C_2 = T_{2k} r + c$, $C_2' = \varphi^{-1}C_2 = e^{-\frac{2\pi i}{2k}(2j)}C_2$, è, per il corollario al teorema 6.5 $C_2 \cap C_2' = \{a,b\}$. Sia $l \in I_{2k-1}$ tale che $\widehat{acb} = \frac{2\pi}{2k}l$; poichè è, come sopra, $\widehat{acb} < \pi$, deve essere $l \neq k$. Osserviamo inoltre che se fosse l pari sarebbe $b - c = e^{\frac{2\pi i}{k}\frac{l}{2}}(a-c)$ e dunque anche $b \in C$ e, in modo del tutto analogo, $b \in C'$ e dunque $\{a,b\} \subset C \cap C'$; ma abbiamo osservato che è $|C \cap C'| = 1$, dunque è $l \in I_{2k-1}\backslash\{k\}$ dispari. Per quanto dimostrato nel teorema precedente, $\exists \psi \in T_{2k}$ tale che

$$\psi c = c_l := r\frac{\sin\beta}{\sin\alpha}e^{-i(\alpha+\beta)},$$

dove

$$\begin{aligned} \beta &= \frac{\pi}{2k}\left(\frac{2k}{2} - l\right) \\ \alpha &= \frac{\pi j}{2k} \end{aligned}$$

ed $a = \psi r + c$. Poichè $a \in C$, deve essere $\psi \in T_k$ e dunque $E_c^r = E_c^{\psi r}$; così $E_{c,k}^r \in \{E_{c_t,k}^r|\ t \in I_{2k-1},\ t \text{ dispari}\}$ e $\gamma(j,r;k) \leq k-1$.

Mostriamo ora per $l \in I_{2k-1}\backslash\{k\}$ dispari che gli $E_{c_t}^r$ sono tutti distinti. Abbiamo che $\forall l, s \in I_{2k-1}$

$$|c_l| = \frac{\left|\sin\frac{\pi}{k}\left(\frac{2k}{2k}-l\right)\right|}{\sin\frac{\pi j}{2k}}|r| = \frac{\left|\sin\frac{\pi}{k}\left(\frac{2k}{2k}-s\right)\right|}{\sin\frac{\pi j}{2k}}|r| = |c_s|$$

se e solo se

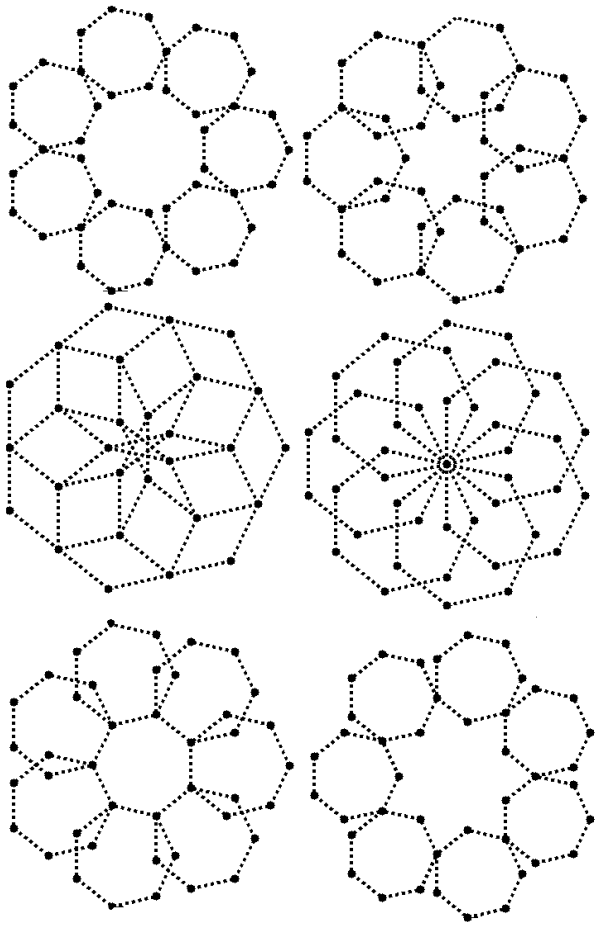
$$|s-l| \in \{0,k\}$$

Dunque se $l, s \in I_{2k-1}\backslash\{k\}$ sono dispari e tali che $E^r_{c_s} = E^r_{s_l}$ si ha, in particolare, $|c_l| = |c_s|$, e dunque, poichè k è dispari, $l = s$.

Mostriamo ora che $\forall l \in I_{2k-1}\backslash\{k\}$ dispari $\Gamma(E^r_{c_t,k})$ ha Γ^k_j come sottografo: sia $l \in I_{2k-1}\backslash\{k\}$ dispari,

$$\begin{aligned} \varphi &= e^{\frac{2\pi ij}{2k}} = e^{\frac{2\pi i}{2k}(2j)},\ c = c_t,\ C = T_k r + c,\ C\prime = \varphi^{-1}C, \\ C_2 &= T_{2k} r + c,\ C'_2 = \varphi^{-1}C_2,\ \bar{C} = Tr + c,\ \bar{C}' = \varphi^{-1}\bar{C}; \end{aligned}$$

abbiamo, sempre per quanto mostrato in precedenza $\bar{C} \cap \bar{C}' = C_2 \cap C'_2 = \{a, b\}$, dove $a = r + c \in C$ e $|a| > |b|$. E' $\widehat{acb} = \frac{2\pi}{2k}l$,e, con le notazioni del teorema precedente, $\widehat{a0c} = \widehat{0ar} = \alpha = \frac{\pi(2j)}{2k} = \frac{\pi j}{k}$, $\widehat{a0r} = \widehat{ca0} = \widehat{abc} = \beta = \frac{\pi}{2k}(\frac{2k}{2} - l)$, $a = r + c$, $a + b = c + c'$, e dunque $b = c' - r$, cioè $b \in C'_2\backslash C'$ (perchè k dispari e dunque $-1 \notin T_k$); ora, $\widehat{ac'b} = \widehat{acb} = \frac{2\pi}{2k}l$ e l è dispari, dunque $a \in C'$, dunque $C \cap C' \neq \varnothing$ e così per il corollario al teorema 6.2, $|C \cap C'| = 1$ e Γ^k_j sottografo di $\Gamma(E^r_c)$. □



Tutti i sistemi di cerchi per $r = 1, k = 7$, $j = 1$ tali che Γ^k_j sottografo di $\Gamma(E^r_c)$

Appendice A

Programmi MATLAB

A.1 Grafi dagli interi modulo p

A.1.1 primitivelement

Function che, dato un primo p, calcola un elemento primitivo di $\mathbb{Z}_p$.

```
function l=primitivelement(p)
j=2;
K=[1];
for l=2:p-1
    if all(l~=K)
        n=1;
        s=l;
        K(j)=s;
        j=j+1;
        while s~=1&&n<p
            s=mod(s*l,p);
            K(j)=s;
            n=n+1;
            j=j+1;
        end
        if n==p-1, break; end
    end
end
```

A.1.2 findgenerator

Function che, dati due naturali p, k e un elemento primitivo l di $\mathbb{Z}_p$, calcola un generatore f di $\Phi_k \leq \mathbb{Z}_p$

```
function f=findgenerator(k,p,l)
f=1;
N=(p-1)/k;
for i=1:N
     f=mod(f*l,p);
end
```

A.1.3 iscircular

Function che, dati un primo p, un divisore k di p-1 e un generatore f di $\Phi_k \leq \mathbb{Z}_p$, stabilisce, usando il criterio di circolarità per quasianelli costruiti su spazi vettoriali, se il BIBD $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$ è circolare

```
function [r,K]=iscircular(k,p,f)
if k<4, disp('k dev"essere >3'); r=0; K=[]; return; end
if isprime(p)==0
    fprintf('%d non è primo\n',p);r=0; K=[]; return;
end
if mod(p-1,k)~=0
    fprintf('%d non divide %d\n',k,p-1);r=0; K=[]; return;
end
if k>(3+sqrt(4*p-7))/2, r=0; K=[]; return; end
    K=zeros(1,k);
    K(1)=1;
    for i=2:k
        K(i)=mod(f*K(i-1),p);
    end
    K1=mod(K-1,p);
    for i=2:k
        for j=2:k
            for h=[2:min([i,j])-1,min([i,j])+1:...
                max(i,j)-1,max(i,j)+1:k]
                for s=[2:min([i,j])-1,min([i,j])+1:...
                   max(i,j)-1,max(i,j)+1:k]
                alpha=mod(K1(i)*K1(j)-K1(h)*K1(s),p);
                if alpha==0,r=0; K=[]; return; end
            end
        end
    end
end
r=1;
```

A.1.4 tabcircular

Function che, dati due interi p1 e p2 determina, per tutti i numeri primi maggiori o uguali di 13 compresi tra p1 e p2, un elemento primitivo di $\mathbb{Z}_p$, i divisori k di p-1 per cui il BIBD $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$ è circolare e per ciascuno di questi un generatore di $\Phi_k \leq \mathbb{Z}_p$, memorizzando i risultati in una matrice A. Il teorema sfrutta il teorema 3.10 e l'osservazione 5.1 per fare meno conti.

```
function A=tabcircular(p1,p2)
```

```
h=0;
for p=p1:p2
    if isprime(p)==1
        j=1;
        C=[1];
        l=primitivelement(p);
        f=zeros(1,p-1);
        ind=zeros(1,p-1);
        n=0;
        for k=(3+sqrt(4*p-7))/2-mod((3+sqrt(4*p-7))/2,1):-1:4
            if mod(p-1,k)==0
                if ~all(mod(C,k)~=0)
                    generator=findgenerator(k,p,l);
                    r=1;
                else
                    generator=findgenerator(k,p,l);
                     [r,K]=iscircular(k,p,generator);
                    C=[C K];
                    j=j+length(K);
                end
                 if r==1
                     n=n+1;
                     ind(n)=k;
                     f(n)=generator;
                end
            end
        end
        if n>0
            h=h+1;
            A(h,1)=p;
            A(h+1,1)=l;
            A(h,2:n+1)=ind(n:-1:1);
            A(h+1,2:n+1)=f(n:-1:1);
            h=h+1;
        end
    end
end
```

A.1.5 numberintersection

Function che, dati due interi r e c, un primo p, un divisore k di p-1 e un vettore riga K che contiene gli elementi di $\Phi_k \leq \mathbb{Z}_p^*$, determina la sequenza s delle intersezioni

associata al sistema di cerchi E_c^r, usando il teorema dei cerchi non disgiunti ed il teorema 5.11 se k è dispari, i teoremi dei cerchi non disgiunti e dei cerchi tangenti se k pari.

```
function s=numberintersection(r,c,k,p,K)
r=mod(r,p);
c=mod(c,p);
if r==0||c==0
disp('raggio e centro devono essere non nulli');s=[]; return; end
if mod(k,2)==1
    if ~all(mod(c-K*r,p)~=0), s=ones(k-1,1);
    else
        s=zeros(k-1,1);
        [A,B]=meshgrid(K);
        for j=1:k-1
            if ~all(all(mod((1-K(j+1))*c-(-A+B)*r,p)~=0))
                s(j)=1;
            end
        end
    end
else if ~all(mod(c-K*r,p)~=0), s=2*ones(k-1,1); s(k/2)=1;
        else
            s=2*ones(k-1,1);
            [A,B]=meshgrid(K);
            for j=1:k-1
                if all(all(mod((1-K(j+1))*c-(-A+B)*r,p)~=0))
                    s(j)=0;
                end
                if ~all(mod((1-K(j+1))*c+2*K*r,p)~=0)
                    s(j)=1;
                end
            end
        end
end
```

A.1.6 plotgraph

Function che dato un intero k ed una matrice $k \times 3$, disegna il grafo di insieme di vertici T_k tale che due vertici $v_{i_1} = e^{\frac{2\pi i}{k} i_1}$ e $i_2 = e^{\frac{2\pi i}{k} i_2}$ sono collegati da un lato rosso (rispett. blu) se e solo se la matrice E ha come riga $[i_1, i_2, 1]$ (rispett. $[i_1, i_2, 1]$).

```
function plotgraph(k,E)
hold on
for j=0:k-1
```

```
    v(j+1,1)=cos(j/k*2*pi);
    v(j+1,2)=sin(j/k*2*pi);
    plot(v(j+1,1),v(j+1,2),'r*')
end
[m,n]=size(E);
for k=1:m
    if E(k,3)==0
        plot(v([E(k,1)+1,E(k,2)+1],1),v([E(k,1)+1,E(k,2)+1],2));
    else if E(k,3)==1
    plot(v([E(k,1)+1,E(k,2)+1],1),v([E(k,1)+1,E(k,2)+1],2),'r');
    end
end
hold off
```

A.1.7 plotroundgraph

Function che dato un intero k e un vettore S con entrate in {0,1} di lunghezza k-1, disegna il grafo di insieme di vertici T_k tale che due vertici $v_{i_1} = e^{\frac{2\pi i}{k} i_1}$ e $i_2 = e^{\frac{2\pi i}{k} i_2}$ con $i_2 > i_1$ sono collegati da un lato rosso (rispett. blu) se e solo se l' $(i_2 - i_1) - esimo$ elemento di S è 1 (rispett 0)

```
function plotroundgraph(k,S)
[m,n]=size(S);
E=[zeros(m,1),S];
hold on;
for j=1:k
    plotgraph(k,E);
    E(:,1:2)=mod(E(:,1:2)+1,k);
end
hold off
```

A.1.8 plotgraphErc

Function che, dati due interi r e c, un primo p, un divisore k di p-1 ed un vettore K che contiene gli elementi di $\Phi_k \leq \mathbb{Z}_p^*$, disegna il grafo associato al sistema di cerchi E_c^r in $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$

```
function plotgraphErc(r,c,k,p,K)
s=numberintersection(r,c,k,p,K);
n=0;
S=[];
for j=1:k-1
    if s(j)==1
        n=n+1;
```

```
        S(n,1)=j;
        S(n,2)=1;
    elseif s(j)==2
        n=n+1;
        S(n,1)=j;
        S(n,2)=0;
    end
end
if length(S)==0
    fprintf('grafo nullo:  Erc è un toro per...
                p=%d, k=%d, r=%d, c=%d\n',p,k,r,c);
else
    plotroundgraph(k,S)
end
```

A.1.9 tantigrafi

Function che, dati due naturali p1 e p2, e due interi r e c, disegna, per ogni primo p compreso tra p1 e p2, per ogni divisore k di p-1 tale che $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$ sia circolare, il grafo associato al sistema di cerchi E^r_c nel BIBD $(\mathbb{Z}_p, \mathcal{B}^*_{\Phi_k}, \in)$.

```
function tantigrafi(p1,p2,r,c)
n=0;
for p=max(p1,13):p2
    if isprime(p)==1
        j=1;
        C=[1];
        l=primitivelement(p);
        for k=(3+sqrt(4*p-7))/2-mod((3+sqrt(4*p-7))/2,1):-1:4
            if mod(p-1,k)==0
                if ~all(mod(C,k)~=0)
                    f=findgenerator(k,p,l);
                    K=zeros(1,k);
                    K(1)=1;
                    for i=2:k
                        K(i)=mod(f*K(i-1),p);
                    end
                    an=1;
                else
                    f=findgenerator(k,p,l);
                    [an,K]=iscircular(k,p,f);
                    C=[C K];
                    j=j+length(K);
```

```
                end
                if an==1
                    n=n+1;
                    figure(n);
                    plotgraphErc(r,c,k,p,K);
                    s=sprintf('Grafo associato a Erc per p=%d,...
                                    k=%d, r=%d, c=%d',p,k,r,c)';
                    title(s');
                    axis('equal');
                end
            end
        end
    end
end
```

A.2 Grafi sui complessi

A.2.1 plotdiscretecircle

Function che dati due numeri complessi r e c ed un naturale k, disegna il cerchio $T_k r + c \in B^*_{T_k}$, collegandone due elementi successivi con una linea tratteggiata.

```
function plotdiscretecircle(r,c,k)
hold on
for j=1:k
plot(real(c+r*exp(2*pi*i*j/k)),imag(c+r*exp(2*pi*i*j/k)),'.k');
plot([real(c+r*exp(2*pi*i*j/k)),real(c+r*exp(2*pi*i*(j+1)/k))],...
[imag(c+r*exp(2*pi*i*j/k)),imag(c+r*exp(2*pi*i*(j+1)/k))],':k');
end
hold off
```

A.2.2 plotcomplexErc

Function che dati due numeri complessi r e c ed un intero k, disegna il sistema di cerchi E^r_c in $(\mathbb{C}, \mathcal{B}_{T_k}, \in)$

```
function plotcomplexErc(r,c,k)
alpha=1;
for j=1:k
    plotdiscretecircle(r,c*alpha,k);
    alpha=alpha*exp(2*pi*i/k);
end
axis('equal');
```

A.2.3 intersezioni

Function che, dati un intero j compreso tra 1 e k-1, un numero complesso non nullo r ed un intero k, calcola tutti e soli i valori di $c \in \mathbb{C}^*$ tali che $\Gamma(E_c^r)$ è non nullo e per ciascuno di essi disegna il sistema di cerchi E_c^r.

```
function intersezioni(j,r,k)
p=mod(k,2);
n=0;
alpha=pi*j/k;
d=r/sin(alpha);
if p==0
    n=n+1;
    figure(n);
    beta=pi/k*(k/2);
    c=d*sin(beta)*exp(-i*(alpha+beta));
    plotcomplexErc(r,c,k);
    s=sprintf('Sistema di cerchi per r=%d il cui grafo...
           associato ha come sottografo Gamma(%d,%d)',r,k,j);
    title(s);
    for t=1:k/2-1
        n=n+1;
        figure(n);
        beta=pi/k*(k/2-t);
        c=d*sin(beta)*exp(-i*(alpha+beta));
        plotcomplexErc(r,c,k);
        s=sprintf('Sistema di cerchi per r=%d il cui grafo...
            associato ha come sottografo Pi(%d,%d)',r,k,j);
        title(s);
    end
else
    for t=1:2:2*k-1
        if t~=k
            n=n+1;
            figure(n);
            beta=pi/(2*k)*(k-t);
            c=d*sin(beta)*exp(-i*(alpha+beta));
            plotcomplexErc(r,c,k);
            s=sprintf('Sistema di cerchi per r=%d il cui grafo...
               associato ha come sottografo Gamma(%d,%d)',r,k,j);
            title(s);
        end
    end
```

Bibliografia

[1] Giovanni Ferrero e Celestina Cotti Ferrero 2002, *Nearrings: Some Developments Linked to Semigroups and Groups,* Advances in Matematics, Kluwer Academic Publishers.

[2] James R. Clay 1992, *Nearrings: Geneses and Applications,* Oxford University Press.

[3] Wen-Fong Ke 1992, *Structures of Circular Planar Nearrings,* Tesi di Dottorato, Università dell'Arizona.