

Introduzione

Lo scopo di questa tesi, come si evince facilmente dal titolo per nulla criptico, è mostrare come si può presentare il gruppo $SL_2(\mathbb{Q}_p)$ come somma amalgamata di due gruppi. La parte principale di questa trattazione si basa su un lavoro di Serre che sviluppa una teoria molto più generale su come si possono caratterizzare i gruppi che agiscono in un determinato modo sui grafi, io mi limiterò a considerarne le parti che sono funzionali al raggiungimento del risultato che mi interessa. Il primo capitolo contiene un po' di preliminari algebrici, che sono poi necessari per affrontare la parte seguente: si introducono l'azione di un gruppo su un insieme, i moduli e gli amalgami di gruppi. Nel secondo capitolo vengono trattati i grafi, gli alberi in particolare, e l'azione di gruppi su di essi. Si vedrà cosa si può dire di un gruppo che agisce su un albero, trattando i due casi in cui il gruppo è libero oppure è un amalgama di due gruppi. Questo ci porterà, nell'ultima parte, a definire un albero su cui agisce il gruppo $SL_2(\mathbb{Q}_p)$ e concludere che è un amalgama di due copie di $SL_2(\mathbb{Z}_p)$.

Indice

Introduzione	1
1 Preliminari Algebrici	1
1.1 Azione di un Gruppo su un Insieme	2
1.2 Moduli su un Dominio a Ideali Principali	4
1.3 Gruppi e Amalgami	16
2 Azione di Gruppi sui Grafi e SL_2	21
2.1 Grafi e Alberi	22
2.2 Azione di un Gruppo su un Grafo	31
2.3 L'albero di $SL_2(\mathbb{Q}_p)$	37
Bibliografia	47

Capitolo 1

Preliminari Algebrici

1.1 Azione di un Gruppo su un Insieme

Il concetto di gruppo che agisce su un insieme sta alla base di tutta la trattazione che seguirà, quindi introduciamo alcune definizioni fondamentali.

Definizione 1.1. Sia G un gruppo (denotato in maniera moltiplicativa con elemento neutro 1) e sia X un insieme. Diciamo che G *agisce sull'insieme* X se, per ogni $g \in G$, esiste una funzione biettiva $T_g : X \rightarrow X$ tale che:

- i) $T_1(x) = x, \forall x \in X$ (cioè $T_1(x) = Id_X$);
- ii) $(T_g \circ T_h)(x) = T_{gh}(x), \forall g, h \in G, \forall x \in X$.

Questa definizione è equivalente a dire che esiste un omomorfismo di gruppi tra G e l'insieme $S(X)$ delle funzioni biunivoche da X in se stesso, che è quello definito da $g \mapsto T_g$.

Visto che di solito non c'è rischio di creare confusione, per avere una notazione più snella indicheremo T_g solamente con g e quindi $T_g(x)$ con gx .

Vediamo ora alcuni semplici esempi di azione.

Esempio 1.1. Sia $X = G$, G agisce su se stesso, ad esempio prendiamo come gx il prodotto in G , questa è evidentemente un'azione in quanto è biunivoca (ha inversa $y \mapsto g^{-1}y$) e sono verificate i) $1x = x$ e ii) $g(hx) = (gh)x$.

Esempio 1.2. Sia ora H un sottogruppo di G e sia $X = G/H$ l'insieme delle classi laterali sinistre rispetto ad H , allora G agisce ancora tramite moltiplicazione, infatti definiamo $g(xH) = gxH$ e questa è un'azione.

Esempio 1.3. Se G è un gruppo che agisce su X e H è un sottogruppo di G , allora H agisce su X in modo ovvio.

Esempio 1.4. Per finire, se G agisce su X , si ha un'azione indotta anche su $P(X)$, l'insieme delle parti di X . Infatti sia $A \subset X$, se $A \neq \emptyset$ definiamo $gA = \{gx \mid x \in A\}$, e definiamo $g\emptyset = \emptyset, \forall g \in G$. Allora $1A = A$ e $g(hA) = (gh)A$, quindi è a sua volta un'azione.

Se G è un gruppo che agisce su un insieme X , possiamo definire una relazione su X , ponendo

$$x \sim y \Leftrightarrow \exists g \in G \text{ tale che } y = gx.$$

Verifichiamo che questa è una relazione di equivalenza perchè G è un gruppo, infatti è riflessiva perchè $1x = x$, è simmetrica perchè $y = gx \Rightarrow x = g^{-1}y$ ed è transitiva, visto che $y = gx$ e $z = hy \Rightarrow z = (hg)x$.

Definizione 1.2. La classe di equivalenza di x , $Gx = \{gx \mid g \in G\}$ è detta *l'orbita di x* , l'insieme quoziente si indica con X/G .

Se c'è una sola orbita, cioè $X = Gx$ per un qualche x (e quindi per tutti) si dice che l'azione di G su X è *transitiva*.

Un esempio di azione transitiva è quella che abbiamo visto nell'esempio 1.1, infatti dato $x \in G$, $\forall y \in G$ $y = gx$ con $g = yx^{-1}$.

Definizione 1.3. Si dice lo *stabilizzatore* di x , e si indica con G_x , il sottinsieme di G composto dagli elementi g tali che $gx = x$.

Lo stabilizzatore di x è un sottogruppo di G , infatti $1x = x$, poi $gx = x \Rightarrow g^{-1}(gx) = g^{-1}x \Rightarrow g^{-1}x = x$, ed infine $gx = x$ e $hx = x \Rightarrow (gh)x = g(hx) = gx = x$. Ritornando al nostro esempio 1.1 osserviamo che per ogni x lo stabilizzatore è il sottogruppo banale.

1.2 Moduli su un Dominio a Ideali Principali

Lo scopo di questa parte è arrivare al teorema dei fattori invarianti, che ci servirà poi nell'ultimo capitolo di questa trattazione. Per ottenere questo risultato, però, ci occorrono un po' di nozioni sui moduli. Lavoreremo in generale con moduli su un dominio ad ideali principali (PID), anche se il caso particolare che ci interessa è quello di \mathbb{Z}_p .

Definizione 1.4. Sia A un anello, M un gruppo abeliano (che denotiamo additivamente). M è un A -modulo (*sinistro*) se esiste una funzione (prodotto per scalare) $R \times M \longrightarrow M$, $(a, x) \mapsto ax$ tale che $\forall a, b \in A, \forall x, y \in M$:

$$i) \quad a(x + y) = ax + ay,$$

$$ii) \quad (a + b)x = ax + bx,$$

$$iii) \quad (ab)x = a(bx),$$

$$iv) \quad 1x = x.$$

E' possibile anche definire in modo del tutto analogo un modulo destro, indicando il prodotto per scalare con xa e modificando di conseguenza gli assiomi $i), ii), iii), iv)$, ma non ci soffermeremo su questo caso, anche perchè ci interessa lavorare su un anello commutativo in cui le due nozioni sono equivalenti. D'ora in poi tutte le volte che parleremo di modulo, indicheremo un modulo sinistro.

Osservazione 1. Se M è un A -modulo, possiamo notare alcune proprietà base. Distinguiamo il vettore nullo $0_M \in M$ dallo scalare $0_A \in A$, allora $\forall x \in M, \forall a \in A$ si ha:

$$1. \quad a0_M = 0_M \quad (a0_M = a(0_M + 0_M) = a0_M + a0_M)$$

$$2. \quad 0_Ax = 0_M \quad (0_Ax = (0_A + 0_A)x = 0_Ax + 0_Ax)$$

$$3. \quad (-a)x = a(-x) = -(ax) \quad (0_M = 0_Ax = (a + (-a))x = ax + (-a)x) \text{ e} \\ (0_M = a0_M = a(x + (-x)) = ax + a(-x))$$

Vediamo alcuni esempi di moduli.

Esempio 1.5. Se A è un campo, la nozione di A -modulo coincide con quella di spazio vettoriale su A .

Esempio 1.6. Ogni anello A è un modulo su se stesso, questo è evidente prendendo come prodotto per scalare il prodotto in A : $A \times A \longrightarrow A$, $(a, x) \mapsto ax$. La proprietà distributiva della moltiplicazione rispetto all'addizione ci garantisce che gli assiomi sono rispettati.

Esempio 1.7. Un gruppo abeliano M è sempre un modulo su \mathbb{Z} . Infatti se indichiamo l'operazione del gruppo additivamente, $\forall x \in M, n \in \mathbb{Z}$ poniamo

$$nx = \begin{cases} x + x + \dots + x \text{ (} n \text{ volte)} & n > 0 \\ 0 & n = 0 \\ -x - x - \dots - x \text{ (} n \text{ volte)} & n < 0. \end{cases}$$

Si vede subito che questa definizione rispetta $i) - iv)$.

Definizione 1.5. Sia M un A -modulo, un *sottomodulo* N è un sottogruppo di M , chiuso rispetto al prodotto per scalare, cioè:

$$y_1, y_2 \in N \Rightarrow y_1 + y_2 \in N \text{ e } y \in N, a \in A \Rightarrow ay \in N.$$

Osserviamo che se $\{N_\alpha\}$ è una famiglia di sottomoduli di M , allora $\bigcap_\alpha N_\alpha$ è ancora un sottomodulo, quindi se $S \subset M$ è un sottoinsieme non vuoto, $\langle S \rangle$, l'intersezione di tutti i sottomoduli di M che contengono S , è un sottomodulo di M . Questo viene detto il *sottomodulo generato da S* , ed è immediato il fatto che $\langle S \rangle = \{a_1 y_1 + a_2 y_2 + \dots + a_r y_r \mid a_i \in A, y_i \in S\}$.

Indichiamo con $\sum_\alpha N_\alpha$ il sottomodulo generato da $\bigcup_\alpha N_\alpha$, ed è l'insieme delle somme $y_{\alpha_1} + y_{\alpha_2} + \dots + y_{\alpha_r}$ con $y_{\alpha_k} \in N_{\alpha_k}$. Lo chiamiamo il *sottomodulo generato dagli N_α* .

Consideriamo ora il gruppo quoziente M/N di M relativo a un sottomodulo N (sono gruppi abeliani, quindi si può fare). Vogliamo dargli una struttura di A -modulo, con l'ovvio prodotto per scalare:

$$A \times M/N \longrightarrow M/N \quad (a, [x]_N) \mapsto a[x]_N = [ax]_N.$$

Controlliamo innanzitutto che la definizione non dipende dalla scelta del rappresentante, infatti se $[y]_N = [x]_N \Rightarrow y = x + n, n \in N \Rightarrow [ay]_N = [ax + an]_N = [ax]_N + [an]_N$. Ma $[an]_N = [0]_N$ perchè $an \in N$, quindi $[ay]_N = [ax]_N$. Verifichiamo ora gli assiomi $i) - iv)$:

$$i) a([x]_N + [y]_N) = a[x + y]_N = [ax + ay]_N = [ax]_N + [ay]_N = a[x]_N + a[y]_N.$$

Analogamente si mostra che $(a + b)[x]_N = a[x]_N + b[x]_N, (ab)[x]_N = a(b[x]_N)$ e $1[x]_N = [x]_N$.

Definizione 1.6. Questo che abbiamo appena definito è il *modulo quoziente* M/N di M rispetto al sottomodulo N .

Se abbiamo due moduli M, M' sullo stesso anello A possiamo definire dei morfismi tra essi.

Definizione 1.7. Siano M, M' A -moduli, si dice *omomorfismo di moduli* da M a M' , una funzione

$$f : M \longrightarrow M'$$

tale che f è un omomorfismo di gruppi abeliani da M ad M' e che

$$f(ax) = af(x) \quad \forall a \in A, \forall x \in M.$$

Chiaramente un *isomorfismo* è un omomorfismo biunivoco.

Si vede da come l'abbiamo definito che, se N è un sottomodulo di M , la proiezione sul quoziente $\pi : M \longrightarrow M/N, x \mapsto [x]_N$ è un omomorfismo di moduli.

Proposizione 1.2.1. *Sia $f : M \longrightarrow M'$ un omomorfismo di A -moduli, allora $\ker f = f^{-1}(0)$ è un sottomodulo di M e $\operatorname{im} f = f(M)$ è un sottomodulo di M' .*

Dimostrazione. Sappiamo che $\ker f$ è un sottogruppo di M , d'altra parte $\forall a \in A, \forall x \in \ker f, f(ax) = af(x) = a0 = 0$, quindi $ax \in \ker f$ e questo mostra che $\ker f$ è un sottomodulo. Per quanto riguarda $\operatorname{im} f$, sappiamo che è un sottogruppo di M' e poi se $y = f(x) \in \operatorname{im} f, \forall a \in A ay = af(x) = f(ax); ax \in M$ quindi $ay \in \operatorname{im} f$ che è quindi un sottomodulo. \square

Per gli omomorfismi tra moduli valgono praticamente tutti i risultati degli omomorfismi tra gruppi. Non ci soffermiamo troppo su questi, ricordiamo solo, senza dimostrarlo, il *teorema fondamentale degli omomorfismi per i moduli*.

Teorema 1.2.2. *Sia $f : M \longrightarrow M'$ un omomorfismo tra moduli, allora f si può fattorizzare come $f = F \circ \pi$, dove $\pi : M \longrightarrow M/\ker f$ è la proiezione sul quoziente e $F : M/\ker f \longrightarrow M'$ è l'omomorfismo iniettivo indotto. Se f è suriettivo, lo anche F che è quindi un isomorfismo.*

Sia A un anello, indichiamo con A^n l'insieme delle n -uple ordinate di elementi in A . Questo insieme ha molto naturalmente una struttura di A -modulo, definendo le operazioni nel modo ovvio:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n),$$

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n).$$

Poniamo $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ l'elemento di A^n con 1 all' i -esima posizione e = altrove. Allora $x_i e_i = (0, \dots, 0, x_i, 0, \dots, 0)$ e

$$x = (x_1, x_2, \dots, x_n) = \sum_{i=1}^n x_i e_i.$$

Quindi gli n elementi e_i generano A^n come A -modulo. Inoltre $\sum x_i e_i = 0$ implica $x_i = 0$ per ogni $1 \leq i \leq n$ (oppure, equivalentemente, $\sum x_i e_i = \sum y_i e_i$ implica $x_i = y_i$ per ogni $1 \leq i \leq n$) cioè e_i sono *linearmente indipendenti*.

Definizione 1.8. Un insieme di generatori linearmente indipendenti di un modulo M si chiama una *base* di M .

Proposizione 1.2.3. *Un A -modulo M , che possiede una base di n -elementi è isomorfo ad A^n e si dice che è un A -modulo libero di rango n .*

Dimostrazione. Sia (u_1, \dots, u_n) una base di M . Consideriamo la funzione

$$f: A^n \longrightarrow M, \quad (x_1, \dots, x_n) = \sum x_i e_i \mapsto \sum x_i u_i.$$

È ben definita perchè e_i è una base di A^n ed è un omomorfismo di moduli perchè

$$f(x+y) = f(x_1+y_1, \dots, x_n+y_n) = \sum (x_i+y_i)u_i = \sum x_i u_i + \sum y_i u_i = f(x) + f(y)$$

e

$$f(ax) = f(ax_1, \dots, ax_n) = \sum (ax_i)u_i = a \sum x_i u_i = af(x).$$

f è suriettiva perchè u_1, \dots, u_n generano M ed è iniettiva perchè u_1, \dots, u_n sono linearmente indipendenti, quindi è un isomorfismo. \square

Al contrario di quanto avviene per gli spazi vettoriali, esistono anche moduli che non possiedono una base, ma non ci interessa trattarli in questa circostanza.

Esempio 1.8. $M_{m,n}(A)$, l'insieme delle matrici $m \times n$ ad elementi in A è un A -modulo libero di rango mn con base $\{E_{ij}\}_{1 \leq i \leq m, 1 \leq j \leq n}$ dove E_{ij} indica la matrice con 1 al posto ij e 0 altrove.

I moduli liberi su anelli commutativi si comportano come ci si aspetta dal punto di vista della cardinalità delle basi (ciò non è vero in generale per tutti gli anelli), noi dimostriamo il risultato solo per i moduli di rango finito, ma si può generalizzare.

Proposizione 1.2.4. *Sia A un anello commutativo, allora due basi di un A -modulo libero M di rango finito hanno la stessa cardinalità.*

Per la dimostrazione di questa proposizione ci serve un piccolo risultato che non dimostriamo.

Lemma 1.2.5. *Sia A un anello commutativo e sia $B \in M_n(A)$ una matrice ad elementi in A . Allora è ben definito $\det(B)$ e B è invertibile se e solo se $\det(B) \in A^\times$ (il gruppo degli elementi invertibili di A).*

Dimostrazione. Siano (e_1, \dots, e_n) e (f_1, \dots, f_m) due basi di M , vogliamo provare che $m = n$. Innanzitutto possiamo scrivere

$$e_i = \sum_{j=1}^m b_{ij} f_j \quad f_j = \sum_{i=1}^n c_{ji} e_i$$

con $a_{ji}, b_{ij} \in A$. Sostituendo otteniamo

$$e_i = \sum_{j=1, i'=1}^{m, n} b_{ij} c_{ji'} e_{i'} \quad f_j = \sum_{i=1, j'=1}^{n, m} c_{ji} b_{ij'} f_{j'}.$$

Dal momento che gli f_j e gli e_i sono basi, abbiamo che

$$\sum_{j=1}^m b_{ij} c_{ji'} = \begin{cases} 1 & \text{se } i = i' \\ 0 & \text{se } i \neq i' \end{cases} \quad \sum_{i=1}^n c_{ji} b_{ij'} = \begin{cases} 1 & \text{se } j = j' \\ 0 & \text{se } j \neq j' \end{cases}.$$

Ora supponiamo $m < n$ e consideriamo le due matrici $n \times n$.

$$C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ \vdots & \vdots & \dots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} b_{11} & \dots & b_{1m} & 0 & \dots & 0 \\ b_{21} & \dots & b_{2m} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{n1} & \dots & b_{nm} & 0 & \dots & 0 \end{pmatrix}.$$

Allora la prima condizione che abbiamo scritto prima è equivalente a $BC = I_n$, ma dal momento che A è commutativo per il lemma 1.2.5 B e C sono matrici invertibili ($\det(BC) = \det(B)\det(C) = 1$) e sono l'una l'inversa dell'altra, quindi anche $CB = I_n$. Ma dalla forma delle due matrici è chiaro che le ultime $n - m$ righe di CB sono nulle e quindi $CB \neq I_n$. Quindi non può essere $m < n$, allora $m \geq n$. Rifacendo lo stesso ragionamento otteniamo la disuguaglianza inversa $n \geq m$, e così concludiamo. \square

La dimostrazione precedente mostra anche che se (e_1, \dots, e_n) e (f_1, \dots, f_n) sono basi con $f_j = \sum_{i=1}^n c_{ji} e_i$ e $e_i = \sum_{j=1}^n b_{ij} f_j$, allora $CB = I_n = BC$ per $C = (c_{ij})$ e $B = (b_{ij})$. Quindi le matrici C e B sono invertibili, cioè appartengono a $GL_n(A)$ il gruppo delle matrici invertibili $n \times n$ ad elementi in A . Viceversa,

supponiamo di avere una base $e = (e_1, \dots, e_n)$ e una matrice $C \in GL_n(A)$, allora vediamo $f=Ce$ è ancora una base (con Ce intendiamo chiaramente il prodotto di C con il vettore colonna e). Visto che C è invertibile, indichiamo con $B = (b_{ij})$ la sua inversa. Ora $e=Bf$, cioè $e_i = \sum_{j=1}^n b_{ij}f_j$, quindi visto che $\forall x \in M$ esistono x_1, \dots, x_n con $x = \sum_{i=1}^n x_i e_i$, (perchè e_i generano M) abbiamo che $x = \sum_{i=1}^n x_i (\sum_{j=1}^n b_{ij}f_j) = \sum_{j=1}^n (\sum_{i=1}^n x_i b_{ij})f_j$. Quindi (f_1, \dots, f_n) generano M . Ora supponiamo di avere d_1, \dots, d_n tali che $\sum d_j f_j = 0$, allora $0 = \sum_{j=1}^n d_j (\sum_{i=1}^n c_{ji}e_i) = \sum_{i=1}^n (\sum_{j=1}^n d_j c_{ji})e_i$. Quindi $\sum_{j=1}^n d_j c_{ji} = 0 \forall i$. Ma allora $\sum_{i,j=1}^n d_j c_{ji} b_{ih} = 0$ per ogni h . Dal momento che $CB = 1$, questo significa che $d_j = 0, j = 1, \dots, n$ e quindi f_1, \dots, f_n sono linearmente indipendenti.

Questo ragionamento ci dice che se abbiamo una base di M , tutte le altre le otteniamo moltiplicando per una matrice di $GL_n(A)$.

Ora vediamo i collegamenti tra i morfismi tra moduli e le matrici, sempre restando nel caso in cui A è un anello commutativo.

Definizione 1.9. Siano M e N due A -moduli liberi di rango rispettivamente m ed n . Siano quindi (e_1, \dots, e_m) e (f_1, \dots, f_n) le rispettive basi. Supponiamo di avere un omomorfismo $g : M \rightarrow N$, chiamiamo la *matrice associata* a g , la matrice $B = (b_{ij}) \in M_{n,m}$ ottenuta in questo modo:

$$g(e_j) = \sum_{i=1}^n b_{ji} f_i.$$

Chiaramente l'omomorfismo identifica univocamente la matrice perchè f_1, \dots, f_n son una base.

Osservazione 2. $\text{Hom}(M, N)$ l'insieme degli omomorfismi da M a N è un A -modulo con le operazioni $(g + h)(x) = g(x) + h(x)$ e $(ag)(x) = ag(x), \forall g, h \in \text{Hom}(M, N), \forall a \in A$.

Dimostrazione. L'unica cosa da notare è che ag è ancora un omomorfismo perchè

$$(ag)(bx) = ag(bx) = abg(x) = bag(x) = b(ag)(x)$$

e questo è vero perchè A è commutativo, ma non è vero in generale. \square

Proposizione 1.2.6. $\text{Hom}(M, N)$ e $M_{n,m}(A)$ sono isomorfi come A -moduli.

Dimostrazione. L'isomorfismo sarà quello che associa a $g \in \text{Hom}(M, N)$ la matrice B come in 1.9. Vediamo intanto che è un omomorfismo di moduli, per farlo

prendiamo $g, h \in \text{Hom}(M, N)$ e le loro rispettive matrici $B = (b_{ij})$ e $C = (c_{ij})$, allora

$$(g + h)(e_j) = g(e_j) + h(e_j) = \sum_{i=1}^n b_{ji} f_i + \sum_{i=1}^n c_{ji} f_i = \sum_{i=1}^n (b_{ji} + c_{ji}) f_i.$$

Questo ci dice che la matrice associata a $g + h$ è $B + C$, poi

$$(ag)(e_j) = ag(e_j) = a \sum_{i=1}^n b_{ji} f_i = \sum_{i=1}^n ab_{ji} f_i$$

che significa che $ag \mapsto aB$.

Ora, questo omomorfismo è sicuramente iniettivo, visto che, se g e h hanno la stessa matrice associata, devono essere uguali perchè sono determinati dall'immagine degli elementi della base; è anche suriettivo perchè, data una matrice $B = (b_{ij}) \in M_{n,m}(A)$, l'omomorfismo $x = \sum_{j=1}^m x_j e_j \mapsto Bx = \sum_{i=1}^n (\sum_{j=1}^m b_{ij} x_j) f_i$ ha come matrice associata proprio B ; quindi è un isomorfismo. \square

Fino ad adesso abbiamo lavorato con delle basi fissate per M ed N , cosa succede se cambiamo base? Sappiamo che tutte le basi di M le otteniamo moltiplicando una base data (e_1, \dots, e_m) per una matrice $P = (p_{hj}) \in GL_m(A)$. Quindi supponiamo di avere una base $l = (l_1, \dots, l_m)$, con $l = Pe$, allora per ottenere la matrice dell'omomorfismo g scriviamo

$$g(l_h) = g\left(\sum_{j=1}^m p_{hj} e_j\right) = \sum_{j=1}^m p_{hj} g(e_j) = \sum_{j=1}^m p_{hj} \left(\sum_{i=1}^n b_{ji} f_i\right) = \sum_{i=1}^n \left(\sum_{j=1}^m p_{hj} b_{ji}\right) f_i$$

Si vede così che la nuova matrice di g (rispetto alle basi l ed f) è PB . Allo stesso modo, se cambiamo la base di N in modo che $f = Qs$, con $Q \in GL_n(A)$ la nuova matrice di g sarà BQ .

Quello che cerchiamo di fare, quindi è cercare delle basi adatte di M ed N in modo che la matrice associata all'omomorfismo abbia una forma particolarmente semplice. Questo si può sempre fare, come stiamo per vedere, se richiediamo ulteriormente che l'anello A sia un dominio a ideali principali.

Definizione 1.10. Sia D un PID, due matrici $B, C \in M_{m,n}(D)$ si dicono *equivalenti* se esistono due matrici invertibili $P \in GL_m(D)$ e $Q \in GL_n(D)$ tali che $C = PBQ$.

E' chiaro che questa è una relazione di equivalenza sull'insieme $M_{m,n}(D)$, il nostro problema è quindi di scegliere un rappresentante della classe di equivalenza.

3. La moltiplicazione a sinistra di A per $P_{ij} \in M_m(D)$ è la stessa cosa che scambiare l' i -esima e la j -esima riga di A , mentre la moltiplicazione a destra di A per $P_{ij} \in M_n(D)$ scambia l' i -esima e la j -esima colonna di A .

Chiamiamo le matrici che abbiamo definito *matrici elementari* e l'operazione di moltiplicare a sinistra (o a destra) A per una di queste sarà una *trasformazione elementare sulle righe (o colonne)* di A . Un'altro tipo di matrice di cui abbiamo bisogno è una matrice della forma

$$\begin{pmatrix} x & s & & & & \\ y & t & & & & 0 \\ & & 1 & & & \\ & & & 1 & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{pmatrix} \quad (1.1)$$

dove $\begin{pmatrix} x & s \\ y & t \end{pmatrix}$ è invertibile. (Questo fa sì che tutta la matrice sia invertibile).

Le trasformazioni elementari e quelle ottenute moltiplicando a destra o a sinistra A per una matrice del tipo (1.1) danno luogo a matrici equivalenti ad A . Ci serve solo un'altra definizione, poi possiamo dimostrare il teorema.

Definizione 1.11. Sia $a \in D$ si definisce $l(a)$, la *lunghezza* di $a \neq 0$ come il numero di fattori primi che compaiono nella fattorizzazione in primi di $a = p_1 p_2 \dots p_r$. Questa è ben definita perchè D , in quanto PID è anche un dominio a fattorizzazione unica (UFD). Per convenzione fissiamo $l(u) = 0$ se u è un'unità di D .

Dimostrazione. Innanzitutto, se A è la matrice nulla non c'è niente da dimostrare. Supponiamo $A \neq 0$, sia allora a_{ij} un elemento non nullo tale che $l(a_{ij})$ sia minima tra gli elementi di A . Con trasformazioni elementari portiamo questo elemento nella posizione $(1, 1)$. Ora abbiamo quindi che $a_{11} \neq 0$ e $l(a_{11}) \leq l(a_{ij})$ per ogni $a_{ij} \neq 0$. Supponiamo esista k tale che $a_{11} \nmid a_{1k}$, scambiando la seconda e la k -esima colonna possiamo supporre $a_{11} \nmid a_{12}$. Scriviamo $a = a_{11}$ e $b = a_{12}$, sia $d = \text{MCD}(a, b)$ così $l(d) < l(a)$. Esistono $x, y \in D$ tali che $ax + by = d$. Poniamo $s = bd^{-1}$, $t = -ad^{-1}$. Allora abbiamo l'equazione matriciale

$$\begin{pmatrix} -t & s \\ y & -x \end{pmatrix} \begin{pmatrix} x & s \\ y & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

che implica che entrambe le matrici sono invertibili (dal momento che D è commutativo). Quindi (1.1) è invertibile. Moltiplicando a destra A per quest'ultima,

ci da una matrice la cui prima riga è $(d, 0, b_{13}, \dots, b_{1n})$. Abbiamo così ottenuto una matrice equivalente ad A per cui il minimo di l è minore di quello in A . Possiamo ripetere la procedura originale su questa nuova matrice. In modo simile, se $a_{11} \nmid a_{k1}$ per qualche k , trasformazioni elementari insieme alla moltiplicazione a sinistra per un'adatta matrice del tipo (1.1) ci dà una matrice equivalente in cui la lunghezza di un qualche elemento diverso da 0 è minore di $l(a_{11})$. Visto che la lunghezza è un intero non negativo, iterando questo processo un numero finito di volte, otteniamo una matrice equivalente $B = (b_{ij})$ in cui $b_{11} \mid b_{1k}$ e $b_{11} \mid b_{k1}$ per ogni k . A questo punto, trasformazioni elementari delle righe e delle colonne del tipo $T_{ij}(b)$ ci danno una matrice equivalente della forma

$$\begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & \dots & c_{mn} \end{pmatrix}. \quad (1.2)$$

Possiamo anche fare in modo che $b_{11} \mid c_{kl}$ per ogni k, l . Infatti se $b_{11} \nmid c_{kl}$ allora aggiungiamo la k -esima riga alla prima ottenendo la nuova prima riga $(b_{11}, c_{k2}, \dots, c_{kl}, \dots, c_{kn})$. Ripetendo ora il primo procedimento sostituiamo c_{kl} con un elemento diverso da zero di lunghezza strettamente inferiore a $l(b_{11})$. Un numero finito di passaggi simili ci darà quindi una matrice (1.2) equivalente ad A in cui $b_{11} \neq 0$ e $b_{11} \mid c_{kl}$ per ogni k, l . Ora ripetiamo tutto sulla sottomatrice (c_{kl}) . Questo ci dà una matrice equivalente della forma

$$\begin{pmatrix} b_{11} & 0 & 0 & \dots & 0 \\ 0 & c_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & d_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & d_{m3} & \dots & d_{mn} \end{pmatrix} \quad (1.3)$$

in cui $c_{22} \mid d_{pq}$ per ogni p, q . Inoltre, le trasformazioni elementari sulle righe e sulle colonne di (c_{kl}) che danno (1.3) non modificano la divisibilità per b_{11} . Quindi $b_{11} \mid c_{22}$ e $b_{11} \mid d_{pq}$. Continuando in questo modo otteniamo la matrice diagonale equivalente $\text{diag}\{d_1, d_2, \dots, d_r\}$ con $d_i \mid d_j$ per $i \leq j$ ($d_1 = b_{11}$, $d_2 = c_{22}$, etc.). \square

Una matrice equivalente ad A avente la forma diagonale data dal teorema 1.2.7 è detta una *forma normale* per A . Gli elementi diagonali di una forma normale sono detti *fattori invarianti* di A . Chiaramente uno qualunque di questi può essere sostituito da un suo associato (moltiplicato per un unità). Vogliamo mostrare che questa è l'unica modifica che si può fare nei fattori invarianti, che

cioè sono determinati a meno di multipli invertibili. Otterremo questo risultato dando una formula per calcolare i fattori invarianti a partire dagli elementi di A . Ricordiamo che la matrice A è detta avere *rango* (*determinantale*) r se esiste un minore non nullo di dimensione r e ogni minore di dimensione $r + 1$ è 0. Dal momento che i minori di dimensione i sono somme di prodotti di minori di dimensione $i - 1$ per elementi di D , è chiaro che se il rango di A è r , allora per ogni $1 \leq i \leq r$, A possiede dei minori non nulli di dimensione i .

Teorema 1.2.8. *Sia $A \in M_{m,n}(D)$ con D dominio a ideali principali e supponiamo che il rango di A sia r . Per ogni $i \leq r$ sia Δ_i un MCD dei minori di dimensione i di A . Allora ogni insieme di fattori invarianti per A differisce per multipli invertibili da*

$$d_1 = \Delta_1, d_2 = \Delta_2 \Delta_1^{-1}, \dots, d_r = \Delta_r \Delta_{r-1}^{-1}.$$

(E' chiaro che $\Delta_i \neq 0$ e che $\Delta_{i-1} \mid \Delta_i$.)

Dimostrazione. Sia $Q = (q_{kl}) \in M_m(D)$, allora l'elemento (k, i) di QA è $\sum_j q_{kj} a_{ji}$. Questo mostra che le righe di QA sono combinazioni lineari a coefficienti in D delle righe di A . Quindi i minori di dimensione i di QA sono combinazione lineare dei minori di dimensione i di A , così il MCD dei minori di dimensione i di A è un divisore del MCD dei minori di dimensione i di QA . In modo simile, visto che le colonne di AP , $P \in M_n(D)$, sono combinazioni lineari delle colonne di A , il MCD dei minori di dimensione i di A è un divisore del MCD dei minori di dimensione i di AP . Combinando questi due fatti, e sfruttando la simmetria delle relazioni di equivalenza, si vede che se A e B sono equivalenti, i MCD dei minori di dimensione i di A e di B sono gli stessi (o loro associati). Ora sia $B = \text{diag}\{d_1, d_2, \dots, d_r, 0, \dots, 0\}$ una forma normale per A . Allora la condizione sulla divisibilità $d_i \mid d_j$ se $i \leq j$ implica che un MCD dei minori di dimensione i di B sia $\Delta_i = d_1 d_2 \dots d_i$. Da questo segue il risultato. \square

Questi teoremi che abbiamo appena dimostrato ci permettono di ottenere poi dei teoremi di struttura dei moduli finitamente generati, che ci danno risultati interessanti sui gruppi abeliani. In particolare si dimostra che

Teorema 1.2.9. *Sia D un PID e sia M un D -modulo finitamente generato, allora M è la somma diretta di un sottomodulo libero e del suo sottomodulo di torsione $\text{tor } M$ (che è l'insieme degli $x \in M$ tali che $ax = 0$ per qualche $a \neq 0$ in D).*

Nel caso specifico di $D = \mathbb{Z}$ sappiamo che gli \mathbb{Z} -moduli sono i gruppi abeliani e quindi si ha che

Teorema 1.2.10. *Ogni gruppo abeliano finitamente generato è la somma diretta di un gruppo finito, il suo sottogruppo di torsione (costituito da tutti gli elementi di ordine finito), e di un gruppo libero.*

C'è un altro risultato sui moduli che ci servirà nell'ultima parte della trattazione, per arrivare al quale abbiamo bisogno innanzitutto di alcune definizioni.

Definizione 1.12. Un modulo M si dice *Artiniano* se soddisfa la condizione della catena discendente, cioè se per ogni N_i famiglia di sottomoduli di M tali che

$$N_0 \supset N_1 \supset \dots \supset N_i \supset N_{i+1} \supset \dots$$

esiste i_0 tale che $N_k = N_{i_0} \quad \forall k \geq i_0$.

M si dice *Noetheriano* se soddisfa la condizione della catena ascendente, cioè ogni successione N_i di sottomoduli con $N_i \subset N_{i+1}$ diventa costante.

Chiaramente un modulo finito (come ad esempio $\mathbb{Z}/n\mathbb{Z}$) è sia Artiniano che Noetheriano.

Definizione 1.13. Sia M un modulo, una *serie di composizione* per M è una catena di sottomoduli N_i di M con

$$0 = N_0 \subset N_1 \subset \dots \subset N_{k-1} \subset N_k = M$$

tali che N_i è un sottogruppo normale massimale di N_{i+1} .

Evidentemente un modulo che sia Artiniano e Noetheriano ammette una serie di composizione. Enunciamo ora, senza dimostrarlo, il teorema che ci interessa, nella sua versione per i moduli.

Teorema 1.2.11 (Teorema di Jordan-Hölder). *Sia M un modulo finito e siano*

$$0 = N_0 \subset N_1 \subset \dots \subset N_{r-1} \subset N_r = M$$

e

$$0 = L_0 \subset L_1 \subset \dots \subset L_{s-1} \subset L_s = M$$

due serie di composizione di M . Allora $r = s$ ed esiste una permutazione $i \mapsto i'$ di $1, \dots, r$ tale che $N_i/N_{i-1} \simeq L_{i'}/L_{i'+1} \quad \forall 1 \leq i \leq r$.

E' quindi ben posta la seguente definizione.

Definizione 1.14. Sia M un modulo, e sia $0 = N_0 \subset \dots \subset N_r = M$ una sua serie di composizione, l'intero r si dice la *lunghezza* di M e si indica con $l(M)$.

1.3 Gruppi e Amalgami

Sia $(G_i)_{i \in I}$ una famiglia di gruppi e, per ogni coppia (i, j) , sia F_{ij} un insieme di omomorfismi di G_i in G_j . Cerchiamo un gruppo $G = \varinjlim G_i$ e una famiglia di omomorfismi $f_i : G_i \rightarrow G$ tali che $f_j \circ f = f_i$ per ogni $f \in F_{ij}$, in modo che il gruppo e la famiglia siano universali nel senso seguente:

se H è un gruppo e se $h_i : G_i \rightarrow H$ è una famiglia di omomorfismi tale che $h_j \circ f = h_i$ per ogni $f \in F_{ij}$, allora c'è esattamente un omomorfismo $h : G \rightarrow H$ tale che $h_i = h \circ f_i$. Diciamo che G è il *limite diretto* dei G_i , relativo agli F_{ij} .

Proposizione 1.3.1. *La coppia costituita da G e dalla famiglia $(f_i)_{i \in I}$ esiste ed è unica a meno di isomorfismo unico.*

Dimostrazione. L'unicità segue dalla proprietà universale che abbiamo richiesto per G e per gli (f_i) , infatti se G e H sono due gruppi che hanno le caratteristiche richieste, allora abbiamo $h : G \rightarrow H$ con $h_i = h \circ f_i$ e $g : H \rightarrow G$ con $f_i = g \circ h_i$, e quindi

$$h_i = h \circ g \circ h_i \quad \text{e} \quad f_i = g \circ h \circ f_i$$

il che implica che g e h sono l'inversa l'una dell'altra e quindi G e H sono isomorfi (l'unicità dell'isomorfismo deriva dall'unicità di h e g). Per l'esistenza si può procedere definendo G per generatori e relazioni; si prende come famiglia generatrice l'unione disgiunta di quelle dei G_i e come relazioni da una parte xyz^{-1} dove $x, y, z \in G_i$ e $z = xy$ in G_i , dall'altra xy^{-1} dove $x \in G_i, y \in G_j$ e $y = f(x)$ per almeno un $f \in F_{ij}$. \square

In alcuni casi particolari esistono dei teoremi che ci permettono di conoscere la struttura del gruppo che si ottiene come limite diretto, ad esempio nel caso degli amalgami.

Definizione 1.15. Sia A un gruppo, $(G_i)_{i \in I}$ una famiglia di gruppi e per ogni $i \in I$ è dato un omomorfismo iniettivo $f_i : A \rightarrow G_i$. Identifichiamo A con la sua immagine in ognuno dei G_i . Indichiamo con $*_A G_i$ il limite diretto della famiglia (A, G_i) relativo a gli omomorfismi f_i e lo chiamiamo *l'amalgama* dei G_i lungo A .

Esempio 1.9. $A = \{1\}$; il gruppo che si ottiene si indica $*G_i$ e si chiama il *prodotto libero* dei G_i . Nel caso particolare in cui $1 \leq i \leq n$ e $G_i = \mathbb{Z} \forall i$ si ottiene il *gruppo libero con n generatori*.

Per vedere come sono fatti gli amalgami, abbiamo bisogno della definizione di cos'è una parola ridotta. Per ogni $i \in I$, scegliamo un insieme S_i di rappresentanti delle classi laterali destre di G_i modulo A , e assumiamo che $1 \in S_i$;

allora la funzione $(a, s) \mapsto as$ è una biiezione $A \times S_i \longleftrightarrow G_i$ attraverso cui l'immagine di $A \times (S_i \setminus \{1\})$ è $G_i \setminus A$.

Sia $\underline{i} = (i_1, \dots, i_n)$ una successione di elementi di I (con $n \geq 0$) che soddisfa la seguente condizione:

$$i_m \neq i_{m+1} \text{ for } 1 \leq m \leq n-1. \quad (1.4)$$

Definizione 1.16. Una *parola ridotta di tipo \underline{i}* è una famiglia

$$m = (a; s_1, \dots, s_n)$$

dove $a \in A$, $s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$ e $s_j \neq 1$ per ogni j .

Infine indichiamo con f (rispettivamente f_i) l'omomorfismo canonico di A (rispettivamente G_i) nel gruppo $G = *_A G_i$.

Teorema 1.3.2. Per ogni $g \in G$ esiste una successione \underline{i} che soddisfa (1.4) e una parola ridotta $m = (a; s_1, \dots, s_n)$ di tipo \underline{i} tale che

$$g = f(a)f_{i_1}(s_1) \cdots f_{i_n}(s_n). \quad (1.5)$$

Inoltre \underline{i} e m sono uniche.

Osservazione 3. Il teorema 1.3.2, per l'unicità di m , implica che f e f_i sono iniettive (che non è evidente a priori). Possiamo allora identificare A e i G_i con le loro immagini in G e la decomposizione ridotta (1.5) di un elemento $g \in G$ si scrive allora

$$g = as_1 \cdots s_n \text{ con } a \in A, s_1 \in S_{i_1} \setminus \{1\}, \dots, s_n \in S_{i_n} \setminus \{1\}.$$

Allo stesso modo, per l'unicità di i si vede che $G_i \cap G_j = A$ se $i \neq j$. In particolare gli insiemi $S_i \setminus \{1\}$ sono a due a due distinti in G .

Dimostrazione. Sia $X_{\underline{i}}$ l'insieme delle parole ridotte di tipo \underline{i} e sia $X = \coprod_{\underline{i}} X_{\underline{i}}$. Vogliamo far agire G su X ; vista la proprietà universale, sarà sufficiente far agire su X ognuno dei G_i e verificare che l'azione indotta su A come sottogruppo di G_i non dipende da i .

Supponiamo allora che $i \in I$ e sia Y_i l'insieme delle parole ridotte della forma $(1; s_1, \dots, s_n)$, con $i_1 \neq i$. Gli insiemi $A \times Y_i$ e $A \times (S_i \setminus \{1\}) \times Y_i$ sono mandati in X dalle funzioni

$$(a, (1; s_1, \dots, s_n)) \mapsto (a; s_1, \dots, s_n)$$

$$((a, s), (1; s_1, \dots, s_n)) \mapsto (a; s, s_1, \dots, s_n).$$

E' chiaro che questo ci dà una biiezione tra $A \times Y_i \cup A \times (S_i \setminus \{1\}) \times Y_i$ ed X . Ma $A \cup A \times (S_i \setminus \{1\})$ si identifica con G_i , abbiamo quindi una biiezione

$$\theta_i : G_i \times Y_i \longleftrightarrow X.$$

Ora facciamo agire G_i su $G_i \times Y_i$ nel modo ovvio:

$$g' \cdot (g, y) = (g'g, y)$$

e la trasferiamo ad una azione su X tramite θ_i ; la sua restrizione ad A è data da

$$a' \cdot (a; s_1, \dots, s_n) = (a'a; s_1, \dots, s_n)$$

che non dipende da i .

Abbiamo così definito un azione di G su X . Inoltre, vediamo che se $m = (a; s_1, \dots, s_n)$ è una parole ridotta e se g è la sua immagine in G secondo la formula (1.5), la trasformazione per g della parola identità $e = (1;)$ (relativa alla successione vuota $\underline{i} = \emptyset$) è m stessa. Si vede per induzione su n .

Per $n = 1$, sia $m = (a; s_1)$, allora abbiamo $g = f(a)f_{i_1}(s_1)$, che significa che g è l'immagine in G di $as_1 \in G_{i_1}$, e anche che $e \in Y_{i_1}$ quindi possiamo usare l'azione che abbiamo definito esplicitamente prima

$$g \cdot e = (a, s_1) \cdot (1;) = (a; s_1) = m.$$

Ora, supponiamo che ciò sia vero per tutte le parole ridotte della forma $(a; s_1, \dots, s_{n-1})$ e dimostriamolo per n . Siano $m = (a; s_1, \dots, s_n)$, $m' = (1; s_2, \dots, s_n)$ e siano $g'' = f(a)f_{i_1}(s_1)$, $g' = f(1)f_{i_2}(s_2) \cdots f_{i_n}(s_n)$, allora l'immagine di m' in G è g' e di m è $g = g''g'$. Ora

$$\begin{aligned} g \cdot e &= g''g' \cdot e = g'' \cdot m' \text{ (per ipotesi induttiva)} = \\ &= (a, s_1) \cdot (1; s_2, \dots, s_n) = (a; s_1, s_2, \dots, s_n) = m. \end{aligned}$$

Se indichiamo la funzione $g \mapsto g \cdot e$ con $\alpha : G \longrightarrow X$ e quella definita da (1.5) con $\beta : X \longrightarrow G$, allora $\alpha \circ \beta = id$ da cui l'iniettività di β , cioè l'unicità della scomposizione ridotta. Possiamo allora identificare X con $\beta(X) \subset G$ e rimane da vedere che $X = G$. Basta dimostrare che $G_i X \subset X$ per ogni i , perchè questo implica che $G X \subset X$ da cui, visto che $1 \in X$, $G = G \cdot 1 \subset X$. Questo si vede subito, infatti se $g_i = a's_i \in G_i$ e $x = as_1 \cdots s_n \in X$, $gx = a'(s_i a)s_1 \cdots s_n \in X$. \square

Osservazione 4. Nel caso del prodotto libero ($A = \{1\}$) abbiamo semplicemente $S_i = G_i$, in particolare se prendiamo come G_i il gruppo ciclico infinito generato

da x_i , in modo che $G = F((x_i)_{i \in I})$ il gruppo libero sulla famiglia di elementi $(x_i)_{i \in I}$, il teorema 1.3.2 ci dà l'esistenza e l'unicità della scomposizione di $g \in F((x_i)_{i \in I})$ nella forma

$$g = x_{i_1}^{m_1} \cdots x_{i_n}^{m_n}, \quad i_1 \neq i_2, \dots, i_{n-1} \neq i_n, \quad m_1 \neq 0, \dots, m_n \neq 0.$$

Capitolo 2

Azione di Gruppi sui Grafi e SL_2

2.1 Grafi e Alberi

I grafi sono strutture molto interessanti di per sè, ma a noi riguardano perchè ci permettono di dimostrare alcuni risultati sui gruppi.

Definizione 2.1. Un *grafo* Γ consiste di un insieme $X = \text{vert } \Gamma$, un insieme $Y = \text{edge } \Gamma$ e due funzioni

$$Y \longrightarrow X \times X, \quad y \mapsto (o(y), t(y))$$

e

$$Y \longrightarrow Y, \quad y \mapsto \bar{y}$$

che soddisfano le seguenti condizioni:

- i) $\bar{\bar{y}} = y$,
- ii) $\bar{y} \neq y$,
- iii) $o(y) = t(\bar{y})$.

Introduciamo un po' di terminologia: un elemento $P \in X$ si chiama *vertice* di Γ , un elemento $y \in Y$ è detto *spigolo (orientato)* di Γ e \bar{y} è detto lo *spigolo inverso*. Il vertice $o(y)$ si dice *origine* di y , mentre il vertice $t(y)$ è il *termine* di y . Questi due vertici sono gli *estremi* di y . Due vertici sono detti *adiacenti* se sono gli estremi di un qualche spigolo.

Possiamo definire dei morfismi tra grafi.

Definizione 2.2. Siano Γ, Γ' due grafi, con $X = \text{vert } \Gamma, Y = \text{edge } \Gamma$ e $X' = \text{vert } \Gamma', Y' = \text{edge } \Gamma'$. Un *morfismo* α tra Γ e Γ' è dato da due funzioni

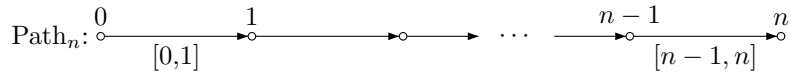
$$\alpha_1 : X \longrightarrow X' \text{ e } \alpha_2 : Y \longrightarrow Y'$$

tali che $o(\alpha_2(y)) = \alpha_1(o(y))$ e che $\alpha_2(\bar{y}) = \overline{\alpha_2(y)}$. Il morfismo si dirà *iniettivo* se sono iniettive le funzioni α_1 e α_2 che potremo indicare entrambe semplicemente con α per abuso di notazione.

Definizione 2.3. Sia Γ un grafo, allora esiste sempre un'*orientazione* di Γ , cioè un sottoinsieme $Y_+ \subset Y = \text{edge } \Gamma$, tale che Y è l'unione disgiunta di Y_+ e $\overline{Y_+}$. Un *grafo orientato* è definito, a meno di isomorfismo, dagli insiemi X e Y_+ e da una funzione $Y_+ \longrightarrow X \times X$. L'insieme degli spigoli sarà $Y = Y_+ \amalg \overline{Y_+}$ dove con $\overline{Y_+}$ si intende una copia di Y_+ .

Nella pratica, per rappresentare i grafi si usano diagrammi in cui i punti segnati corrispondono ai vertici del grafo e una linea che unisce due punti corrisponde ad un insieme di spigoli del tipo $\{y, \bar{y}\}$.

Sia $n \geq 0$ un numero naturale e consideriamo il grafo orientato



Ha $n+1$ vertici $0, 1, \dots, n$ e l'orientazione data dagli n spigoli $[i, i+1]$, $0 \leq i \leq n$ con $o([i, i+1]) = i$ e $t([i, i+1]) = i+1$.

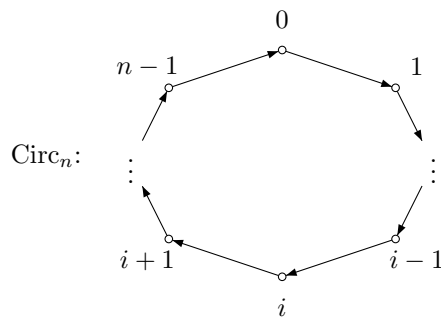
Definizione 2.4. Un *cammino* (di lunghezza n) in un grafo Γ è un morfismo c di Path_n in Γ .

Per $n \geq 1$ la successione (y_1, \dots, y_n) di spigoli $y_i = c([i-1, i])$ tali che $t(y_i) = o(y_{i+1})$, $1 \leq i \leq n$, determina c , quindi indichiamo anch'essa con c . Se $P_i = c(i)$ diciamo che c è un cammino da P_0 a P_n e che P_0 e P_n sono gli estremi del cammino. Una coppia della forma $(y_i, y_{i+1}) = (y_i, \bar{y}_i)$ è detta *backtracking*. In tal caso possiamo costruire un cammino (di lunghezza $n-2$) da P_0 a P_n , dato (per $n > 2$) dalla successione $(y_1, \dots, y_{i-1}, y_{i+2}, \dots, y_n)$. Per induzione, possiamo concludere che, se esiste un cammino da P_0 a P_n in Γ , allora ne esiste uno senza backtracking.

Possiamo generalizzare la nozione di cammino ad un *cammino infinito* prendendo una successione infinita (y_1, y_2, \dots) di spigoli tali che $t(y_i) = o(y_{i+1}) \forall i \geq 1$.

Definizione 2.5. Un grafo Γ è detto *connesso* se per ogni coppia di vertici P, Q di Γ esiste almeno un cammino da P a Q . I sottografi connessi di Γ massimali rispetto all'inclusione si dicono le *componenti connesse* di Γ .

Sia $n \geq 1$ un numero naturale e consideriamo il grafo orientato



L'insieme dei vertici è $\mathbb{Z}/n\mathbb{Z}$ e l'orientazione è data dagli n spigoli $[i, i+1]$ ($i \in \mathbb{Z}/n\mathbb{Z}$) con $o([i, i+1]) = i$ e $t([i, i+1]) = i+1$.

Definizione 2.6. Un *circuito* (di lunghezza n) in un grafo Γ è un sottografo di Γ isomorfo a Circ_n .

Un tale sottografo è definito da una successione (y_1, \dots, y_n) senza backtracking, tale che i $P_i = t(y_i)$ ($1 \leq i \leq n$) sono distinti a due a due e tale che $P_n = o(y_1)$. Un circuito di lunghezza 1 si chiama *loop*.

Definizione 2.7. Un grafo è detto *combinatorio* se non contiene circuiti di lunghezza ≤ 2 .

Sia Γ un grafo combinatorio. Un insieme $\{P, Q\}$ di estremi di uno spigolo y è detto *spigolo geometrico* di Γ e determina univocamente l'insieme $\{y, \bar{y}\}$ degli spigoli orientati. La struttura di Γ è determinata allora dall'insieme dei suoi vertici e dei suoi spigoli geometrici.

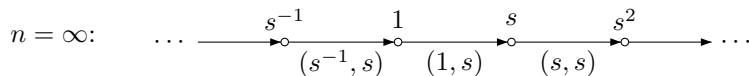
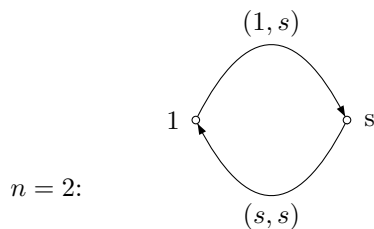
Vediamo ora un esempio di legame tra i gruppi e i grafi.

Definizione 2.8. Sia G un gruppo e sia S un sottinsieme di G . Indichiamo con $\Gamma = \Gamma(G, S)$ il grafo orientato che ha come insieme di vertici G , e come orientazione (edge Γ) $_+ = G \times S$ con

$$o(g, s) = g \text{ e } t(g, s) = gs \text{ per ogni spigolo } (g, s) \in G \times S.$$

La moltiplicazione a sinistra per gli elementi di G definisce un'azione di G su Γ che conserva l'orientazione.

Esempio 2.1. Sia G un gruppo ciclico di ordine n generato da $S = \{s\}$, questo è il diagramma per $\Gamma(G, S)$:



Proposizione 2.1.1. Sia $\Gamma = \Gamma(G, S)$ il grafo definito da un gruppo G e da $S \subset G$, allora

- i) Γ è connesso se e solo se S genera G ;
- ii) Γ contiene un loop se e solo se $1 \in S$;

iii) Γ è un grafo combinatorio se e solo se $S \cap S^{-1} = \emptyset$.

Dimostrazione. i) $g, g' \in G$ sono gli estremi di un cammino di lunghezza n se e solo se esistono $s_1, \dots, s_n \in S \cup S^{-1}$ tali che $g' = gs_1 \dots s_n$ e quindi se e solo se ogni elemento $g'g^{-1}$ (ogni elemento di G , quindi) è nel sottogruppo generato da S .

ii) Γ contiene un loop se e solo se esiste uno spigolo (g, s) con $o(g, s) = t(g, s)$, cioè $g = gs$, e questo succede se e solo se $1 \in S$.

iii) Abbiamo già visto in ii) la condizione per i circuiti di lunghezza 1, ci basta controllare quelli di lunghezza 2. Γ non contiene circuiti di lunghezza 2 se e solo se non esistono due spigoli (g, s) e (gs, s') con $o(g, s) = t(gs, s')$, cioè $g = gss'$, se e solo se non esistono $s, s' \in S$ con $ss' = 1$, quindi $S \cap S^{-1} = \emptyset$. \square

Definizione 2.9. Un *albero* è un grafo connesso, non vuoto senza circuiti.

In particolare, un albero è un grafo combinatorio.

Esempio 2.2. Sono alberi ad esempio



Definizione 2.10. Una *geodetica* in un albero è un cammino senza backtracking.

Proposizione 2.1.2. Siano P e Q due vertici di un albero Γ . Esiste una e una sola geodetica da P a Q ed è un cammino iniettivo.

Dimostrazione. L'esistenza deriva dal fatto che Γ è connesso.

Per l'iniettività, sia $c : \text{Path}_n \rightarrow \Gamma$ una geodetica da $P = c(0)$ a $Q = c(n)$ e poniamo $P_i = c(i)$. Per mostrare che c è iniettivo basta vedere che P_i sono distinti, perchè Γ è un grafo combinatorio e gli spigoli sono determinati univocamente dai loro estremi. Assumiamo $n > 0$ e che c sia definito dalla successione (y_1, \dots, y_n) . Se i P_i non sono distinti, esistono $j < k$ tali che $P_j = P_k$, ma allora (y_{j+1}, \dots, y_k) è un circuito, il che è impossibile dal momento che Γ è un albero. Ora dimostriamo l'unicità: intanto possiamo assumere $P \neq Q$, perchè una geodetica di lunghezza > 0 da P a P , essendo iniettiva, sarebbe un circuito. Siano ora (y_1, \dots, y_n) e (w_1, \dots, w_m) due geodetiche da P a Q , allora $y_n = w_m$ altrimenti il cammino $(y_1, \dots, y_n, \bar{w}_m, \dots, \bar{w}_1)$ sarebbe una geodetica da P a P .

Allora le geodetiche (y_1, \dots, y_{n-1}) e (w_1, \dots, w_{m-1}) hanno lo stesso termine quindi, iterando il ragionamento precedente, coincidono. \square

La lunghezza della geodetica da P a Q è detta la *distanza* da P a Q e si indica con $l(P, Q)$. Si ha che $l(P, Q) = 0$ se e solo se $P = Q$ e $l(P, Q) = 1$ se e solo se P e Q sono adiacenti.

Sia P un vertice di un albero Γ , per ogni intero $n \geq 0$ sia $X_n = \{Q \in \text{vert } \Gamma \mid l(P, Q) = n\}$. Se $Q \in X_n$, $n \geq 1$ esiste un solo vertice $Q' \in X_{n-1}$ a cui Q è adiacente: è il vertice $o(y_n)$ dove (y_1, \dots, y_n) è la geodetica da P a Q . Così si definisce una mappa $f_n : X_n \rightarrow X_{n-1}$ con $Q \mapsto Q'$, e quindi un sistema inverso

$$\dots \rightarrow X_n \rightarrow X_{n-1} \rightarrow \dots \rightarrow X_1 \rightarrow X_0 = \{P\}.$$

Conoscere questo sistema ci permette di ricostruire l'albero Γ , infatti $\text{vert } \Gamma = X = \bigcup_{n \geq 0} X_n$, e gli spigoli geometrici sono i $\{Q, f_n(Q)\}$ per $n \geq 1$ e $Q \in X_n$.

Sia Γ un albero e sia $X' \subset X = \text{vert } \Gamma$. Ogni sottoalbero di Γ contenente X' , contiene anche le geodetiche con estremi in X' . Viceversa, i vertici e gli spigoli di queste geodetiche formano un sottoalbero Γ' di Γ , contenente X' , questo è il sottoalbero *generato* da X' . Se X' è finito, anche Γ' è finito, ne segue che Γ è l'unione diretta dei suoi sottoalberi finiti, questo ci permette di ridurre alcune affermazioni sugli alberi ad affermazioni sugli alberi finiti.

Sia Γ un grafo e sia $X = \text{vert } \Gamma$, $Y = \text{edge } \Gamma$. Sia $P \in X$ e sia $Y_p = \{y \in Y \mid P = t(y)\}$. La cardinalità n di Y_p è l'indice di P . Se $n = 0$ P è un vertice *isolato*; se Γ è connesso questo non è possibile a meno che $X = \{P\}$, $Y = \emptyset$. Se $n \leq 1$ diciamo che P è un vertice *terminale*.

Indichiamo con $\Gamma \setminus P$ il sottografo di Γ che ha come vertici $X \setminus \{P\}$ e come spigoli $Y \setminus (Y_p \cup \overline{Y_p})$.

Proposizione 2.1.3. *Sia P un vertice terminale non isolato di un grafo Γ .*

i) Γ è connesso se e solo se $\Gamma \setminus \{P\}$ è connesso.

ii) Ogni circuito di Γ è contenuto in $\Gamma \setminus \{P\}$.

iii) Γ è un albero se e solo se $\Gamma \setminus \{P\}$ è un albero.

Dimostrazione. Per *i)* osserviamo che le ipotesi ci dicono che P è il termine di un unico spigolo y , quindi è chiaro che se Γ è connesso, il cammino che connette due vertici diversi da P non passa per P e quindi $\Gamma \setminus \{P\}$ è connesso. Viceversa se $\Gamma \setminus \{P\}$ è connesso, per ogni suo vertice Q possiamo trovare un cammino (y_1, \dots, y_n) tale che $o(y_1) = Q$, e $t(y_n) = o(y)$, allora (y_1, \dots, y_n, y) è il cammino da Q a P , quindi Γ è connesso.

La *ii*) segue dal fatto che ogni vertice di un circuito deve avere indice ≥ 2 , e la *iii*), vista la definizione di albero, segue da *i*) e *ii*). \square

L'insieme dei vertici di un albero Γ è uno spazio metrico con la distanza l che abbiamo definito, possiamo quindi parlare di *diametro* di un albero e di *alberi limitati*, cioè alberi di diametro finito. Ad esempio un albero finito è limitato.

Proposizione 2.1.4. *Sia Γ un albero di diametro $n < \infty$.*

- i*) *L'insieme $t(\Gamma)$ dei vertici terminali di Γ è non vuoto.*
- ii*) *Se $n \geq 2$, $\text{vert } \Gamma \setminus t(\Gamma)$ è l'insieme dei vertici di un sottoalbero di diametro $n - 2$.*
- iii*) *Se $n = 0$, $\Gamma \simeq \text{Path}_0$ (diagramma: \circ) e se $n = 1$, $\Gamma \simeq \text{Path}_1$ ($\circ \longrightarrow \circ$).*

Dimostrazione. L'affermazione *iii*) è immediata, e la *i*) segue da *ii*) e *iii*) perchè Path_0 e Path_1 hanno tutti i vertici terminali e la *ii*) ci assicura che ci sono vertici terminali nel caso $n \geq 2$ (altrimenti il diametro di $\Gamma \setminus t(\Gamma)$ e di Γ sarebbe uguale). Dimostriamo quindi la *ii*). Sia $X' = \Gamma \setminus t(\Gamma)$; se $P, Q \in X'$ tutti i vertici della geodetica da P a Q sono non terminali, quindi il sottoalbero Γ' generato da X' non ha altri vertici al di fuori di X' . Inoltre se $l(P, Q) = m$, la geodetica da P a Q può essere estesa (in entrambe le direzioni) ad una geodetica di lunghezza $m + 2$, da cui $m + 2 \leq n$ e quindi $\text{diam}(\Gamma') \leq n - 2$. D'altra parte in Γ esiste una geodetica di lunghezza n ; rimuovendo il primo e l'ultimo spigolo otteniamo una geodetica di lunghezza $n - 2$ in Γ' , e quindi $\text{diam}(\Gamma') \geq n - 2$, da cui $\text{diam}(\Gamma') = n - 2$. \square

Il grafo Γ' è conservato da tutti gli automorfismi di Γ , ne segue immediatamente per induzione sul diametro di Γ che:

Corollario 2.1.5. *Un albero di diametro finito pari (rispettivamente dispari) ha un vertice (rispettivamente uno spigolo geometrico) che è invariante tramite tutti gli automorfismi.*

Dimostrazione. Per alberi di diametro 0 o 1 l'affermazione è ovvia. Per alberi di diametro $n \geq 2$ si usa il punto *ii*) della proposizione appena dimostrata. \square

Osserviamo che se Q è un vertice di un albero Γ_1 , la proposizione 2.1.3 ci mostra che il grafo Γ ottenuto da Γ_1 aggiungendo uno spigolo geometrico $\{P, Q\}$ ad un vertice terminale P è ancora un albero. La proposizione 2.1.4 ci dice che ogni albero finito si ottiene con questo procedimento, cominciando da un albero con un solo vertice. Questo procedimento è a volte utile, perchè permette di ottenere risultati per induzione sul numero di vertici di un albero.

Definizione 2.11. Sia Γ un grafo non vuoto. Un sottografo Λ di Γ è un *albero massimale* se è un elemento massimale rispetto all'inclusione nell'insieme dei sottografi di Γ che sono alberi.

Proposizione 2.1.6. *Se Γ è un grafo non vuoto, allora esiste un albero massimale.*

Dimostrazione. Per provare questo, basta applicare il Lemma di Zorn all'insieme dei sottografi di Γ che sono alberi, ordinati rispetto all'inclusione. Una volta verificato che ogni catena

$$\Gamma_1 \subset \Gamma_2 \subset \dots \subset \Gamma_n \subset \dots$$

ha un estremo superiore, il Lemma ci garantisce l'esistenza di un elemento massimale. Prendiamo $\Gamma' = \bigcup_{i \geq 1} \Gamma_i$, questo sarà il nostro estremo superiore, una volta che avremo dimostrato che è ancora un albero. Innanzitutto, Γ' è connesso, perchè presi due vertici $P, Q \in \Gamma'$, esiste k tale che $P, Q \in \Gamma_k$; c'è quindi un cammino (y_1, \dots, y_m) da P a Q in Γ_k . Ma $y_1, \dots, y_m \in \Gamma'$, quindi (y_1, \dots, y_m) è un cammino da P a Q anche in Γ' . Per concludere, vediamo che Γ' non contiene circuiti. Supponiamo esista un circuito (y_1, \dots, y_n) in Γ' , allora esiste un h tale che $y_1, \dots, y_n \in \Gamma_h$, ma in tal caso (y_1, \dots, y_n) sarebbe un circuito in Γ_h , il che è assurdo perchè Γ_h è un albero. \square

Proposizione 2.1.7. *Sia Λ un albero massimale di un grafo Γ connesso e non vuoto. Allora Λ contiene tutti i vertici di Γ .*

Dimostrazione. Supponiamo non sia vero; allora, visto che Γ è connesso, esiste uno spigolo y con origine in Λ e termine in un vertice P fuori da Λ . Allora, secondo la proposizione 2.1.3 il grafo ottenuto da Λ aggiungendo il vertice P e gli spigoli y, \bar{y} è ancora un albero, ma questo è assurdo per la massimalità di Λ . \square

Proposizione 2.1.8. *Sia Γ un grafo connesso con un numero finito di vertici e siano*

$$s = \text{Card}(\text{vert } \Gamma), \quad a = \frac{1}{2} \text{Card}(\text{edge } \Gamma).$$

Allora $a \geq s - 1$ e l'uguaglianza vale se e solo se Γ è un albero.

Dimostrazione. Riduciamoci innanzitutto al caso in cui Γ è un albero e mostriamo che $a = s - 1$. Questo è sicuramente vero per un albero con un solo vertice ($s = 1, a = 0$) e rimane vero quando aggiungiamo un vertice terminale e una coppia di spigoli $\{y, \bar{y}\}$; è quindi vero per ogni albero finito. (Come avevamo già notato in precedenza, ogni albero finito si ottiene in questo modo.)

Passiamo ora al caso generale. Il risultato è chiaro se Γ è vuoto, altrimenti sia Γ' un albero massimale di Γ . Abbiamo dimostrato che $s(\Gamma) = s(\Gamma')$, e notiamo che $a(\Gamma) \geq a(\Gamma')$, con l'uguaglianza solo nel caso in cui $\Gamma = \Gamma'$. D'altra parte,

$$a(\Gamma') = s(\Gamma') - 1 \Rightarrow a(\Gamma') - a(\Gamma) + a(\Gamma) = s(\Gamma) - 1 \Rightarrow$$

$$a(\Gamma) = s(\Gamma) - 1 + (a(\Gamma) - a(\Gamma')).$$

Da cui il risultato, visto che $a(\Gamma) - a(\Gamma') \geq 0$. \square

Sia Γ un grafo connesso non vuoto, e sia Λ un sottografo di Γ che è l'unione disgiunta di una famiglia Λ_i ($i \in I$) di alberi. Vogliamo definire un grafo Γ/Λ in cui ognuno di questi alberi viene identificato con un punto. Più precisamente,

Definizione 2.12. l'insieme dei vertici di Γ/Λ è il quoziente di $\text{vert } \Gamma$ rispetto alla relazione di equivalenza le cui classi sono gli insiemi $\text{vert } \Lambda_i$ e gli elementi di $\text{vert } \Gamma - \text{vert } \Lambda$. Il suo insieme di spigoli è $\text{edge } \Gamma - \text{edge } \Lambda$ con l'involuzione $y \mapsto \bar{y}$ indotta da quella su $\text{edge } \Gamma$. Infine

$$\text{edge } (\Gamma/\Lambda) \longrightarrow \text{vert } (\Gamma/\Lambda) \times \text{vert } (\Gamma/\Lambda)$$

è indotto da

$$\text{edge } \Gamma \longrightarrow \text{vert } \Gamma \times \text{vert } \Gamma$$

passando al quoziente.

Proposizione 2.1.9. *Con le notazioni usate fino ad adesso, Γ è un albero se e solo se Γ/Λ lo è.*

Dimostrazione. Innanzitutto vediamo la connessione, Γ è sempre connesso per ipotesi quindi ci basta una delle due implicazioni. Supponiamo Γ connesso e siano P' e Q' due vertici di Γ/Λ ; scegliamone due rappresentanti $P, Q \in \Gamma$, allora esiste in Γ un cammino da P a Q e la sua proiezione su Γ/Λ è il cammino richiesto.

Ora mostriamo l'assenza di circuiti per assurdo. Supponiamo che Γ contenga un circuito di lunghezza n (y_1, \dots, y_n), e siano $P_i = o(y_{i+1})$ ($0 \leq i \leq n-1$), e $P_n = t(y_n) = P_0$. Siano P'_i le loro immagini in Γ/Λ , possiamo riscrivere la successione di vertici P'_0, \dots, P'_n eliminando quelli uguali consecutivi come $P'_{i_0}, \dots, P'_{i_r}$. Ora siano tra questi ultimi $P'_{i_k} = P'_{i_l}$ due vertici uguali tali che $|k-l|$ è minimo tra le coppie di vertici uguali, allora la proiezione sul quoziente di $(y_{i_k}, \dots, y_{i_{l-1}})$ è un circuito in Γ/Λ perchè $P'_{i_k}, \dots, P'_{i_{l-1}}$ sono distinti e non c'è backtracking. Infatti se $\{y', \bar{y}'\}$ fosse un backtracking, dal momento che $\text{edge } \Gamma/\Lambda = \text{edge } \Gamma - \text{edge } \Lambda$, avremmo che (y', \bar{y}') sono proiezione o di una

coppia consecutiva (y, \bar{y}) (impossibile perchè (y_1, \dots, y_n) è un circuito) o di una successione del tipo $(y, z_1, \dots, z_h, \bar{y})$ con z_1, \dots, z_h appartenenti ad uno stesso albero Λ_i (impossibile perchè z_1, \dots, z_h formerebbero un circuito in Λ_i). In conclusione, se c'è un circuito in Γ ce n'è uno anche in Γ/Λ .

Viceversa, sia (y'_1, \dots, y'_n) un circuito in Γ/Λ con $P'_i = o(y'_{i+1})$ e $P'_n = t(y'_n) = P'_0$. Per ogni P'_i abbiamo due possibilità: che sia la proiezione di un punto oppure che sia la proiezione di un albero Λ_i . Nel primo caso non ci sono problemi, nel secondo caso esiste una sola geodetica (z_1, \dots, z_r) in Λ_i da $t(y'_{i-1})$ a $o(y'_i)$. Interponendo dove necessario queste geodetiche otteniamo

$$(y'_1, \dots, y'_{i-1}, z_1, \dots, z_r, y'_i, \dots, y'_n)$$

che è un circuito in Γ . Con questo la dimostrazione è conclusa. □

2.2 Azione di un Gruppo su un Grafo

Diremo che un gruppo G agisce su un grafo X , se le funzioni biettive da X in sé stesso associate agli elementi di G sono degli automorfismi. Lo scopo di questo capitolo è ricavare delle proprietà dei gruppi in base alla loro azione su determinati grafi.

Definizione 2.13. Un' *inversione* è una coppia costituita da un elemento $g \in G$ e da uno spigolo $y \in \text{edge } X$ tali che $gy = \bar{y}$; se non esiste una tale coppia diciamo che G agisce *senza inversione* su X (Questo è equivalente a dire che esiste un'orientazione di X conservata da G).

Sia G un gruppo che agisce senza inversione su un grafo X . Possiamo allora definire il grafo quoziente $G \backslash X$ come grafo orientato. Sia $(\text{edge } X)_+$ un'orientazione di X conservata da G , allora $\text{vert } G \backslash X$ è il quoziente di $\text{vert } X$ rispetto all'azione di G ed $(\text{edge } G \backslash X)_+ = (\text{edge } X)_+ / G$. Chiaramente la funzione $(\text{edge } G \backslash X)_+ \rightarrow \text{vert } G \backslash X \times \text{vert } G \backslash X$ è data da $[y]_G \mapsto ([o(y)]_G, [t(y)]_G)$. Questa è ben definita perchè non dipende dalla scelta del rappresentante, infatti sia $[y]_G = [y']_G$, allora $\exists g \in G$ tale che $y' = gy$, ma allora $o(y') = o(gy) = go(y)$ e $t(y') = t(gy) = gt(y)$, quindi $([o(y)]_G, [t(y)]_G) = ([o(y')]_G, [t(y')]_G)$.

Proposizione 2.2.1. *Sia X un grafo connesso, su cui agisce senza inversione un gruppo G . Allora ogni sottoalbero T' di $G \backslash X$ si solleva ad un sottoalbero di X .*

Dimostrazione. Sia Ω l'insieme dei sottoalberi di X che si proiettano iniettivamente in T' , è un insieme parzialmente ordinato secondo la relazione di inclusione, che verifica le ipotesi del lemma di Zorn, quindi ha un elemento massimale. Sia T_0 un elemento massimale di Ω e sia T'_0 la sua immagine in T' e supponiamo che $T'_0 \neq T'$. Allora esiste uno spigolo y' di T' che non appartiene a T'_0 . Dal momento che T' è connesso possiamo assumere che $o(y')$ è un vertice di T'_0 , allora $P' = t(y')$ non appartiene a $\text{vert } T'_0$ (altrimenti la geodesica da $o(y')$ a P' in T'_0 , seguita da \bar{y}' sarebbe un circuito in T'). Sia y un sollevamento di y' ; visto che siamo liberi di sostituire y con gy , $g \in G$, possiamo assumere che $o(y)$ appartiene a T_0 . Sia T_1 il grafo ottenuto da T_0 aggiungendo il vertice $P = t(y)$ e gli spigoli y, \bar{y} . Secondo la proposizione 2.1.3, T_1 è un albero, ma $T_1 \rightarrow T'$ è iniettiva, il che contraddice la massimalità di T_0 , da cui il risultato. \square

Definizione 2.14. Un *albero di rappresentanti* di $X \text{ mod } G$ è un sottoalbero T di X che è il sollevamento di un albero massimale di $G \backslash X$.

Osservazione 5. Con queste notazioni, per quanto visto nella proposizione 2.1.7 ogni orbita di G in $\text{vert } X$ contiene esattamente un elemento di $\text{vert } T$.

Cominciamo ora a vedere come possiamo dedurre alcune proprietà dei gruppi sfruttando i grafi.

Proposizione 2.2.2. *Sia $X = \Gamma(G, S)$ il grafo definito da un gruppo G e da un sottoinsieme S di G (come nella definizione 2.8). Allora le seguenti proprietà sono equivalenti:*

- i) X è un albero
- ii) G è un gruppo libero con base S .

Dimostrazione. Supponiamo che G sia un gruppo libero con base S . Allora ogni elemento $g \in G$ si può scrivere in modo unico nella forma ridotta

$$g = s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n}, \quad s_i \in S, \quad \varepsilon_i \in \{\pm 1\}$$

con $\varepsilon_i = \varepsilon_{i+1}$ se $s_i = s_{i+1}$. L'intero n è detto *lunghezza* di G e si indica con $l(g)$. Sia G_n l'insieme degli elementi di G di lunghezza n . Se $g \in G_n$, $n \geq 1$, come sopra, è chiaro che g è adiacente in X ad un unico elemento di G_{n-1} , per la precisione $s_1^{\varepsilon_1} \dots s_{n-1}^{\varepsilon_{n-1}}$. Questo ci da una mappa $G_n \rightarrow G_{n-1}$ per ogni $n \geq 1$. Inoltre vediamo che X è il grafo definito dal sistema inverso

$$\dots \rightarrow G_n \rightarrow G_{n-1} \rightarrow \dots \rightarrow G_1 \rightarrow G_0 = \{1\}$$

ed è quindi un albero.

Ora supponiamo che X sia un albero. La proposizione 2.1.1 mostra che S genera G (dal momento che X è connesso) e che $S \cap S^{-1} = \emptyset$ (visto che X è combinatorio). Facciamo vedere che S è una famiglia libera; se così non fosse, esisterebbe un elemento non banale \hat{g} del gruppo libero $F(S)$ con base S , la cui immagine in G è 1. Scegliamo un tale elemento \hat{g} di lunghezza minima n e sia

$$\hat{g} = s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n}$$

la sua forma ridotta in $F(S)$. Il fatto che $S \cap S^{-1} = \emptyset$ implica che $n \geq 3$. Sia P_i , $0 \leq i \leq n$ l'immagine di $s_1^{\varepsilon_1} \dots s_i^{\varepsilon_i}$ in G . La minimalità di \hat{g} implica che P_1, \dots, P_{n-1} sono tutti distinti, inoltre P_i è adiacente a P_{i+1} e $P_n = P_0 = 1$. Dal momento che $n \geq 3$ gli spigoli geometrici $\{P_i, P_{i+1}\}$ ($0 \leq i \leq n-1$) sono tutti distinti. Quindi P_0, \dots, P_{n-1} sono i vertici di un circuito di lunghezza n in X il che contraddice l'ipotesi che X sia un albero, da cui il risultato. \square

Diciamo che un gruppo G agisce *liberamente* su un grafo X se agisce senza inversione e nessun elemento di $g \in G$, $g \neq 1$ lascia un vertice di X fissato. Per esempio, se S è un sottoinsieme di un gruppo G , il gruppo G agisce liberamente

(per moltiplicazione a sinistra) sul grafo $\Gamma(G, S)$. La proposizione che abbiamo appena dimostrato dice che, se G è un gruppo libero, esiste un albero sul quale G agisce liberamente, infatti questa proprietà caratterizza i gruppi liberi.

Teorema 2.2.3. *Sia G un gruppo che agisce liberamente su un albero X . Scegliamo un albero di rappresentanti di $X \text{ mod } G$ (vedi defin.2.14) e un orientazione $Y_+ \subset \text{edge } X$ conservata da G .*

i) Sia S l'insieme degli elementi $g \neq 1$ di G per i quali esiste uno spigolo $y \in Y_+$ con origine in T e termine in gT . Allora G è un gruppo libero con base S .

ii) Se $X^ = G \backslash X$ ha un numero finito s di vertici, e se $\text{Card}(\text{edge } X^*) = 2a$, allora $\text{Card}(S) - 1 = a - s$.*

Dimostrazione. Poichè G agisce liberamente e poichè $T \rightarrow X^*$ è iniettiva, la funzione $g \mapsto gT$ è una biiezione da G all'insieme dei traslati di T e questi traslati sono a due a due disgiunti. In particolare, (indichiamo con $G \cdot T = \{gT \mid g \in G\}$) possiamo formare il grafo $X' = X/G \cdot T$ (vedi defin.2.12) contraendo ogni albero gT ad un singolo vertice che indichiamo con (gT) . Per la proposizione 2.1.9, X' è un albero; inoltre l'inverso della biiezione $g \mapsto (gT)$ può essere considerata come una biiezione $\alpha : \text{vert } X' \rightarrow \text{vert } \Gamma(G, S) = G$, dove $\Gamma(G, S)$ è il grafo associato con G ed S . Vogliamo estendere α ad un isomorfismo $\alpha : X' \rightarrow \Gamma(G, S)$. Grazie alla proposizione 2.2.2, questo dimostrerò *i*).

Ricordiamo che $\text{edge } X' = \text{edge } X - \text{edge } (G \cdot T)$. Diamo a X' l'orientazione $Y'_+ = Y_+ \cap \text{edge } X'$ indotta da quella di X . Il morfismo α sarà un morfismo di grafi orientati, quindi basta definire $\alpha : Y'_+ \rightarrow G \times S = (\text{edge } \Gamma(G, S))_+$. Sia $y \in Y'_+$ e sia $(gT) = o(y)$, $(g'T) = t(y)$. Dal fatto che, in X , lo spigolo y connette gT a $g'T$ deduciamo che $s = g^{-1}g'$ appartiene a S ; poniamo allora $\alpha(y) = (g, s)$. La suriettività di $\alpha : Y'_+ \rightarrow G \times S$ segue immediatamente dalla definizione di S . L'iniettività segue dal fatto che X' è un albero e che $\alpha : \text{vert } X' \rightarrow \text{vert } \Gamma(G, S)$ è iniettiva (due spigoli con la stessa immagine hanno gli stessi estremi, quindi se fossero diversi tra loro formerebbero un circuito di lunghezza 2 in X').

ii) Sia W l'insieme degli spigoli $y \in Y_+$ tali che $o(y) \in T$ e $t(y)$ non sta in T . La dimostrazione di *i*) ci fornisce una biiezione $W \leftrightarrow S$, quindi $\text{Card } W = \text{Card } S$. D'altra parte, sia T^* l'immagine di T in $X^* = G \backslash X$; è un albero massimale. Assegnamo a X^* l'orientazione Y^*_+ , l'immagine di Y_+ . E' immediato che Y^*_+ è l'unione disgiunta di $Y^*_+ \cap \text{edge } T^*$ e W^* , l'immagine di W , e che $W \rightarrow W^*$ è biiettiva. Quindi se l'insieme $\text{vert } X^* = \text{vert } T^*$ è finito abbiamo

$$\text{Card } Y^*_+ - \text{Card } \text{vert } X^* = \text{Card } W^* + (\text{Card}(\text{edge } T^*)_+ - \text{Card}(\text{vert } T^*)) =$$

$$= \text{Card } W^* - 1 \quad (\text{per la prop.2.1.8}) \quad = \text{Card } S - 1$$

da cui il risultato. \square

Come applicazione di questo risultato possiamo ottenere il teorema di Schreier.

Teorema 2.2.4. *Ogni sottogruppo di un gruppo libero è libero.*

Dimostrazione. Sia G un gruppo libero, allora come abbiamo visto esiste un albero X su cui G agisce liberamente. Se H è un sottogruppo di G , anche H agisce liberamente su X ed è quindi un gruppo libero. \square

Se G è un gruppo libero, ogni sua base ha la stessa cardinalità, che chiamiamo *rango* di G e indichiamo r_G .

Corollario 2.2.5. *Sia G un gruppo libero e sia H un sottogruppo di indice finito n in G . Allora*

$$r_H - 1 = n(r_G - 1).$$

Dimostrazione. Poniamo $G_1 = G$ e $G_2 = H$, e sia Γ un albero su cui G agisce liberamente. Sia, per $i = 1, 2$ $\Gamma_i = G_i \backslash \Gamma$, $s_i = \text{Card}(\text{vert } \Gamma_i)$ e $a_i = \text{Card}(\text{edge } \Gamma_i)$. Si ha $s_2 = ns_1$ e $a_2 = na_1$. Possiamo scegliere Γ in modo che s_1 sia finito; per esempio l'albero associato con una base di G ha $s_1 = 1$. Il corollario segue allora dalla formula $r_{G_i} - 1 = \frac{1}{2}a_i - s_i$, $i = 1, 2$ (vedi il teo.2.2.3). \square

Ora arriviamo alla parte che più ci interessa di questo capitolo. Abbiamo già visto come l'azione di un gruppo su un grafo ci permette di dedurre dei risultati sui gruppi liberi nel caso in cui l'azione è libera, adesso vediamo cosa possiamo dire sugli amalgami di gruppi; in questa parte assumiamo, senza specificarlo ogni volta, che ogni gruppo agisce senza inversione.

Definizione 2.15. Sia G un gruppo che agisce su un grafo X . Un *dominio fondamentale* di $X \text{ mod } G$ è un sottografo T di X , tale che $T \longrightarrow G \backslash X$ è un isomorfismo.

Se $G \backslash X$ è un albero segue dalla proposizione 2.2.1 che un dominio fondamentale esiste, è vero anche il viceversa se X è un albero.

Proposizione 2.2.6. *Sia G un gruppo che agisce su un albero X . Un dominio fondamentale di $X \text{ mod } G$ esiste se e solo se $G \backslash X$ è un albero.*

Dimostrazione. L'unica implicazione che ci manca è che se esiste un dominio fondamentale T , allora il quoziente $G \backslash X$ è un albero. Ma dal momento che X è connesso e non vuoto, anche $G \backslash X$ è tale; T è quindi un sottografo connesso e non vuoto di un albero e quindi un albero. \square

Un grafo isomorfo a $\text{Path}_1 = \begin{array}{ccc} 0 & & 1 \\ \circ & \longrightarrow & \circ \end{array}$ è detto *segmento*.

Teorema 2.2.7. *Sia G un gruppo che agisce su un grafo X e sia $T = \begin{array}{ccc} P & y & Q \\ \circ & \longrightarrow & \circ \end{array}$ un segmento di X . Supponiamo che T sia un dominio fondamentale di X mod G . Siano G_P, G_Q e $G_y = G_{\bar{y}}$ gli stabilizzatori dei vertici e degli spigoli di T . Le seguenti proprietà sono allora equivalenti:*

- i) X è un albero.
- ii) L'omomorfismo $G_P *_{G_y} G_Q \longrightarrow G$ indotto dalle inclusioni $G_P \longrightarrow G$ e $G_Q \longrightarrow G$ è un isomorfismo.

(Notiamo che $G_y = G_P \cap G_Q$ è un sottogruppo di G_P e G_Q , quindi l'amalgama $G_P *_{G_y} G_Q$ ha senso.)

Viceversa, ogni amalgama di due gruppi agisce su un albero con un segmento come dominio fondamentale. Più precisamente:

Teorema 2.2.8. *Sia $G = G_1 *_A G_2$ un amalgama di due gruppi. Allora esiste un albero X (e uno solo, a meno di isomorfismo) su cui G agisce, con dominio*

fondamentale un segmento $T = \begin{array}{ccc} P & y & Q \\ \circ & \longrightarrow & \circ \end{array}$, i cui vertici e spigoli hanno $G_P = G_1$, $G_Q = G_2$ e $G_y = A$ come rispettivi stabilizzatori.

Dimostrazione Teorema 2.2.7. Il teorema segue dai prossimi due lemmi.

Lemma 2.2.9. *X è connesso se e solo se G è generato da $G_P \cup G_Q$.*

Sia X' la componente connessa di X contenente T , sia G' l'insieme degli elementi $g \in G$ tali che $gX' = X'$, e sia G'' il sottogruppo di G generato da $G_P \cup G_Q$. Se $h \in G_P \cup G_Q$ allora i segmenti T e hT hanno un vertice in comune. Allora $hT \subset X'$, quindi $hX' = X'$, cioè $h \in G'$; questo dimostra che $G'' \subset G'$. D'altra parte, $G''T$ e $(G \setminus G'')T$ sono sottografi disgiunti di X , la cui unione è X . Questo implica che $G''T$ contiene X' , così che $G' \subset G''$ e quindi $G' = G''$. Il grafo X è connesso se e solo se $X = X'$, cioè se $G = G' = G''$, da cui il lemma.

Lemma 2.2.10. *X non contiene circuiti se e solo se $G_P *_{G_y} G_Q \longrightarrow G$ è iniettiva.*

Dire che X contiene un circuito è la stessa cosa che dire che esiste un cammino $c = (w_0, \dots, w_n)$, $n \geq 1$ in X senza backtracking e tale che $o(c) = t(c)$. Scriviamo w_i nella forma $h_i y_i$ con $h_i \in G$ e $y_i \in \{y, \bar{y}\}$. Passando a $G \setminus X \simeq T$

si vede anche che $\bar{y}_i = y_{i-1}$ ($1 \leq i \leq n$). Sia $P_i = o(y_i) = t(y_{i-1})$; abbiamo $h_i = h_{i-1}g_i$ con $g_i \in G_{P_i}$, poichè

$$h_i P_i = h_i o(y_i) = o(h_i y_i) = t(h_{i-1} y_{i-1}) = h_{i-1} t(y_{i-1}) = h_{i-1} P_i$$

e g_i non sta in G_y perchè

$$\overline{h_i y_i} \neq h_{i-1} y_{i-1}.$$

Il fatto che $o(c) = t(c)$ è equivalente a $t(y_n) = P_0$, o ancora a

$$h_0 P_0 = h_n P_0 = h_0 g_1 \cdots g_n P_0, \text{ cioè } g_1 \cdots g_n \in G_{P_0}.$$

Concludiamo che X contiene un circuito se e solo se possiamo trovare una successione P_0, \dots, P_n di vertici di T con $\{P_{i-1}, P_i\} = \{P, Q\}$ per ogni i e una successione di elementi $g_i \in G_{P_i} \setminus G_y$ ($0 \leq i \leq n$) tale che $g_0 g_1 \cdots g_n = 1$. Visto il teorema 1.3.2 questo equivale a dire che $G_P *_{G_y} G_Q \rightarrow G$ non è iniettiva. \square

Dimostrazione Teorema 2.2.8. L'unicità di X è chiara: a meno di isomorfismo X è necessariamente il grafo seguente:

$$\text{vert } X = (G/G_1) \amalg (G/G_2), \quad \text{edge } X = (G/A) \amalg \overline{(G/A)}$$

con le funzioni $o : G/A \rightarrow G/G_1$ e $t : G/A \rightarrow G/G_2$ indotte dalle inclusioni $A \rightarrow G_i$ ($i = 1, 2$), cioè $[g]_A \mapsto [g]_{G_i}$, sono ben definite perchè se $[g]_A = [g']_A$, allora $g - g' \in A \subset G_i$ e quindi $[g]_{G_i} = [g']_{G_i}$.

Se poniamo $P = 1 \cdot G_1$, $Q = 1 \cdot G_2$ e $y = 1 \cdot G_A$, il segmento $T =$ è un dominio fondamentale per l'azione definita in modo ovvio di G su X . Il teorema 2.2.7 mostra quindi che X è un albero. \square

Quest'ultimo discorso che ci permette di mettere in relazione l'amalgama di due gruppi con l'azione su un albero con un segmento come dominio fondamentale, può essere generalizzato a domini fondamentali più complessi (ed equivalentemente ad amalgami o limiti diretti di gruppi più complicati). Comunque per arrivare al risultato che ci interessa, questo è sufficiente, quindi non è necessario approfondire ulteriormente la cosa.

2.3 L'albero di $SL_2(\mathbb{Q}_p)$

In quest'ultima parte usiamo i risultati ottenuti fino ad ora per arrivare a ciò che ci interessa, cioè che il gruppo $SL_2(\mathbb{Q}_p)$ si può scrivere come l'amalgama di due copie di $SL_2(\mathbb{Z}_p)$. Per fare questo definiremo un albero su cui $SL_2(\mathbb{Q}_p)$ agisce e vedremo cosa riusciamo a ricavarne in base a ciò che abbiamo visto nel capitolo precedente. Diamo per scontata la costruzione di \mathbb{Q}_p e le sue principali proprietà (si può vedere la mia tesina di tirocinio per i dettagli), l'unica cosa che ci serve vedere è che \mathbb{Z}_p è un dominio a ideali principali, per poter applicare i teoremi 1.2.7 e 1.2.8.

Proposizione 2.3.1. \mathbb{Z}_p è un dominio a ideali principali.

Dimostrazione. Sia I un ideale di \mathbb{Z}_p e scegliamo $a \in I$ tale che $a = \min_{x \in I} v_p(x)$, questo minimo esiste perchè $\forall x \in \mathbb{Z}_p, v_p(x) \in \mathbb{N}$. Vogliamo vedere che I è generato da $p^{v_p(a)}$. Innanzitutto $a = p^{v_p(a)}u$, con $u \in \mathbb{Z}_p^\times$, quindi

$$p^{v_p(a)} = au^{-1} \Rightarrow p^{v_p(a)} \in I$$

da cui $(p^{v_p(a)}) \subset I$. Ora sia $x \in I$, sappiamo che $v_p(x) \geq v_p(a)$ e che $x = p^{v_p(x)}w$, con w invertibile, quindi

$$x = p^{v_p(a)}(p^{v_p(x)-v_p(a)}w) \Rightarrow x \in (p^{v_p(a)}) \Rightarrow I \subset (p^{v_p(a)}).$$

□

Ora, sia V uno spazio vettoriale di dimensione 2 su \mathbb{Q}_p .

Definizione 2.16. Un reticolo L di V è uno \mathbb{Z}_p -sottomodulo finitamente generato di V che genera V come spazio vettoriale su \mathbb{Q}_p .

Proposizione 2.3.2. Un tale L è un modulo libero di rango 2.

Dimostrazione. Siano $(a_{11}, a_{12}), \dots, (a_{n1}, a_{n2})$ un insieme di generatori di L ; possiamo scriverli come matrice in questo modo

$$A = \begin{pmatrix} a_{11} & a_{12} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \end{pmatrix} a_{ij} \in \mathbb{Q}_p.$$

Se moltiplichiamo A a sinistra per una matrice $P \in GL_n(\mathbb{Z}_p)$ abbiamo ancora un insieme di generatori di L , invece moltiplicare A a destra per una matrice $Q \in GL_2(\mathbb{Q}_p)$ equivale a cambiare la base di V rispetto alla quale scrivo i generatori.

Ora sia $n \in \mathbb{Z}$ il minimo di $v_p(a_{ij})$, possiamo allora raccogliere p^n da A in modo da avere una matrice A' ad elementi in \mathbb{Z}_p . Per il teorema 1.2.7 A' è equivalente ad una matrice del tipo

$$D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$$

Quindi $A = A'p^n = P^{-1}DQ^{-1}p^n \Rightarrow PAQ' = D$ con $Q' = Qp^{-n} \in GL_2(\mathbb{Q}_p)$. Esiste quindi una base di V per cui $(d_1, 0), (0, d_2)$ sono dei generatori; sono evidentemente linearmente indipendenti quindi sono una base di L ($d_1, d_2 \neq 0$ perchè L genera V come spazio vettoriale su \mathbb{Q}_p). \square

Se $x \in \mathbb{Q}_p^*$ e L è un reticolo di V , xL è ancora un reticolo di V (se $\{e_1, e_2\}$ è una base di L , $\{xe_1, xe_2\}$ è una base di xL), quindi il gruppo \mathbb{Q}_p^* agisce sull'insieme dei reticoli.

Definizione 2.17. Chiamiamo l'orbita di un reticolo, sotto questa azione, la sua *classe*; due reticoli che appartengono alla stessa classe si dicono *equivalenti*. Indichiamo l'insieme delle classi dei reticoli con X .

Siano L, L' due reticoli di V e siano $\{(e_{11}, e_{12}), (e_{21}, e_{22})\}$ e $\{(f_{11}, f_{12}), (f_{21}, f_{22})\}$ le loro rispettive basi, che possiamo scrivere sotto forma di matrici $E = (e_{ij})$, $F = (f_{ij})$ in $GL_2(\mathbb{Q}_p)$, se moltiplico E (o F) per una matrice $P \in GL_2(\mathbb{Z}_p)$ ottengo ancora una base di E (o di F).

Proposizione 2.3.3. *Esiste una base $\{e_1, e_2\}$ di L e $a, b \in \mathbb{Z}$ tali che $\{p^a e_1, p^b e_2\}$ è una base di L' . Inoltre l'insieme $\{a, b\}$ non dipende dalla scelta delle basi.*

Dimostrazione. Possiamo scrivere $F = AE$, con $A \in GL_2(\mathbb{Q}_p)$; come abbiamo fatto nella dimostrazione precedente possiamo raccogliere p^n , $n \in \mathbb{Z}$ da A in modo che $A = A'p^n$ con $A' \in GL_2(\mathbb{Z}_p)$. Ora, cambiando la base E in PE ed F in QF , possiamo scrivere

$$QF = QAE = QAP^{-1}PE = p^n QA'P^{-1}(PE)$$

Per il teorema 1.2.7 possiamo scegliere P, Q in modo che $QA'P^{-1} = D$. Con D della forma

$$\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \quad d_1, d_2 \in \mathbb{Z}_p.$$

Per il teorema 1.2.8 possiamo fare in modo che $d_1 = p^r$, $d_2 = p^s$, $0 \leq s \leq r$ avremo quindi $QF = p^n D(PE) = D'(PE)$ con

$$D' = \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix} \quad a, b \in \mathbb{Z}.$$

Il fatto che $\{a, b\}$ non dipenda dalla scelta delle basi è garantito sempre dal teorema 1.2.8. \square

Proposizione 2.3.4. *Con le notazioni precedenti $L' \subset L$ se e solo se a e b sono ≥ 0 , in tal caso L/L' è isomorfo a $(\mathbb{Z}_p/p^a\mathbb{Z}_p) \oplus (\mathbb{Z}_p/p^b\mathbb{Z}_p) \simeq (\mathbb{Z}/p^a\mathbb{Z}) \oplus (\mathbb{Z}/p^b\mathbb{Z})$.*

Dimostrazione. Se $L' \subset L$, allora posso esprimere gli elementi della base di L' come combinazioni lineari a coefficienti in \mathbb{Z}_p degli elementi della base di L , cioè con le notazioni usate in precedenza

$$F = AE \quad \text{con } A \in GL_2(\mathbb{Z}_p)$$

quindi avrò che $QF = D(PE)$ con $D \in GL_2(\mathbb{Z}_p)$ diagonale della forma

$$\begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix} \quad a, b \geq 0.$$

Se invece ho $a, b \geq 0$ allora per ogni $x \in L'$

$$x = k_1 f_1 + k_2 f_2 = k_1 p^a e_1 + k_2 p^b e_2, \quad k_1 p^a, k_2 p^b \in \mathbb{Z}_p \Rightarrow x \in L$$

da cui $L' \subset L$.

Per quanto riguarda l'altra affermazione, consideriamo la funzione

$$f : L \longrightarrow \mathbb{Z}_p/p^a\mathbb{Z}_p \oplus \mathbb{Z}_p/p^b\mathbb{Z}_p$$

$$xe_1 + ye_2 \mapsto ([x]_{p^a}, [y]_{p^b})$$

Questo è chiaramente un omomorfismo di moduli,

$$\ker f = \{ze_1 + we_2 \in L \mid z = z'p^a, w = w'p^b\} = \{z'p^a e_1 + w'p^b e_2 \in L\} = L'$$

da cui per il teorema fondamentale degli omomorfismi si ottiene il risultato. \square

Ora, tornando al caso generale di $a, b \in \mathbb{Z}$, se sostituiamo L, L' con xL, yL' (con $x, y \in \mathbb{Q}_p^*$), abbiamo che $\{a, b\}$ diventa $\{a+c, b+c\}$ con $c = v_p(\frac{y}{x})$. Infatti con le solite notazioni $\{xe_1, xe_2\}$ è una base di xL e $\{yp^a e_1, yp^b e_2\}$ ne è una di yL' ; ma allora

$$yp^a e_1 = \frac{y}{x} p^a x e_1 = up^{v_p(\frac{y}{x})} p^a x e_1 = up^{a+c} x e_1,$$

$$yp^b e_2 = \frac{y}{x} p^b x e_2 = up^{v_p(\frac{y}{x})} p^b x e_2 = up^{b+c} x e_2$$

naturalmente possiamo moltiplicare entrambi per $u^{-1} \in \mathbb{Z}_p^\times$ per ottenere la base che ci interessa. Abbiamo quindi che l'intero $|a-b|$ dipende soltanto dalle classi Λ e Λ' di L e L' .

Definizione 2.18. Indichiamo $|a-b| = d(\Lambda, \Lambda')$ e lo chiamiamo la *distanza* tra Λ e Λ' .

Dato L , ogni classe Λ' ha esattamente un rappresentante L' che soddisfa le seguenti condizioni equivalenti:

- i) $L' \subset L$ e L' è massimale (in Λ') con questa proprietà;
- ii) $L' \subset L$ e $L' \not\subseteq pL$.

Per un tale L' abbiamo che

$$L/L' \simeq \mathbb{Z}_p/p^n \mathbb{Z}_p, \quad \text{dove } n = d(\Lambda, \Lambda').$$

Questo si vede facilmente: se abbiamo un $L'' \in \Lambda'$ e due basi $\{e_1, e_2\}$, $\{p^a e_1, p^b e_2\}$ ($a \leq b$) rispettivamente di L ed L'' , poniamo $L' = p^{-a} L''$. Abbiamo così che $\{e_1, p^{b-a} e_2\}$ è una base di L' da cui si verificano le proprietà richieste.

In particolare osserviamo che:

$$d(\Lambda, \Lambda') = 0 \Leftrightarrow \Lambda = \Lambda';$$

$$d(\Lambda, \Lambda') = 1 \Leftrightarrow \text{esistono rappresentanti } L' \subset L \text{ di } \Lambda' \text{ e di } \Lambda \text{ tali che } L/L' \simeq \mathbb{F}_p$$

(cioè $l(L/L') = 1$, se l indica la lunghezza vedi defin 1.14).

Definizione 2.19. Due elementi Λ, Λ' di X si dicono *adiacenti* se $d(\Lambda, \Lambda') = 1$. In questo modo si definisce una struttura di grafo combinatorio su X . (Λ sono i vertici e gli spigoli geometrici sono $\{\Lambda, \Lambda'\}$ con Λ, Λ' adiacenti.)

Teorema 2.3.5. *Il grafo X è un albero.*

Dimostrazione. Mostriamo innanzitutto che X è connesso. Se Λ e Λ' sono due vertici di X , scegliamone due rappresentanti L e L' con $L' \subset L$. Per il teorema di Jordan-Hölder applicato a L/L' abbiamo una serie di composizione

$$L' = L_n \subset L_{n-1} \subset \dots \subset L_0 = L$$

tale che $l(L_{i-1}/L_i) = 1$ per $1 \leq i \leq n$. Le classi $\Lambda_0, \dots, \Lambda_n$ di questi reticoli definiscono un cammino in X tra gli estremi Λ e Λ' , quindi X è connesso.

Per dimostrare che X è un albero ci rimane da dimostrare che, se $\Lambda_0, \dots, \Lambda_n$ ($n \geq 1$) è una successione di vertici in un cammino senza backtracking in X , allora $\Lambda_0 \neq \Lambda_n$. In effetti mostreremo (per induzione su n) che $d(\Lambda_0, \Lambda_n) = n$.

Per quello che abbiamo appena detto, possiamo trovare dei rappresentanti L_i dei Λ_i tali che $L_{i+1} \subset L_i$ e $l(L_i/L_{i+1}) = 1$. Abbiamo $l(L_0/L_n) = n$ e vogliamo mostrare che $L_n \not\subset pL_0$, perchè questo ci permette di concludere che $d(\Lambda_0, \Lambda_n) = n$. Sicuramente $L_1 \not\subset pL_0$ perchè $l(L_0/pL_0) = 2$, ora supponiamo che $L_{n-1} \not\subset pL_0$. I reticoli L_n e pL_{n-2} sono contenuti in L_{n-1} e sono la controimmagine di due rette del \mathbb{F}_p -piano L_{n-1}/pL_{n-1} . Queste rette sono distinte, altrimenti $L_n = pL_{n-2}$ e quindi $\Lambda_{n-2}, \Lambda_{n-1}, \Lambda_n$ sarebbe un backtracking nel cammino dato.

Abbiamo quindi che

$$L_{n-1} = L_n + pL_{n-2} \Rightarrow L_{n-1} \equiv L_n \pmod{pL_0}$$

da cui si ricava che $L_n \not\subset pL_0$. \square

Osservazione 6. La dimostrazione ci dice anche che $d(\Lambda, \Lambda')$ coincide con la distanza tra i vertici Λ e Λ' nell'albero X .

Sia L_0 un reticolo di V di classe $\Lambda_0 \in X$. Ogni vertice Λ di X è rappresentato da un unico reticolo $L \subset L_0$ tale che $L_0/L \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$, dove $n = d(\Lambda_0, \Lambda)$. L_0/p^nL_0 è un $\mathbb{Z}_p/p^n\mathbb{Z}_p$ -modulo libero di rango 2 e L/p^nL_0 ne è un fattore diretto di rango 1. Quindi vediamo che i vertici di X a distanza n da Λ_0 corrispondono biunivocamente ai fattori diretti di L_0/p^nL_0 di rango 1, cioè ai punti della retta proiettiva $P(L_0/p^nL_0) \simeq P_1(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. Per $n = 1$ questo significa che gli spigoli con origine Λ_0 corrispondono biunivocamente ai punti di $P(L_0/pL_0) \simeq P_1(\mathbb{F}_p)$ e quindi il numero di questi spigoli è $p + 1$.

Indichiamo con $GL(V)$ il gruppo degli automorfismi di V , che è isomorfo a $GL_2(\mathbb{Q}_p)$, e con $SL(V)$ il sottogruppo di $GL(V)$ costituito dai morfismi con determinante 1 (che è isomorfo a $SL_2(\mathbb{Q}_p)$). Possiamo definire un omomorfismo suriettivo di gruppi

$$v_p(\det) : GL(V) \longrightarrow \mathbb{Z}.$$

Osserviamo che $SL(V)$ è contenuto nel ker di questo omomorfismo.

Definizione 2.20. Se L_1 e L_2 sono due reticoli di V , possiamo definire

$$\chi(L_1, L_2) = l(L_1/L_3) - l(L_2/L_3) \text{ con } L_3 \subset L_1 \cap L_2.$$

Vediamo che questo intero non dipende dalla scelta di L_3 . Infatti, dal momento che posso scegliere una base $\{e_1, e_2\}$ di L_1 in modo che $\{p^a e_1, p^b e_2\}$ sia una base di L_2 , $L_1 \cap L_2$ è ancora un reticolo con base $\{p^{\max\{0, a\}} e_1, p^{\max\{0, b\}} e_2\}$. Supponiamo $l(L_1/L_1 \cap L_2) = n$ e $l(L_2/L_1 \cap L_2) = m$ e prendiamo un reticolo $L_3 \subset L_1 \cap L_2$. Avremo $l(L_1 \cap L_2/L_3) = r$, quindi $l(L_1/L_3) = n + r$ e

$l(L_2/L_3) = m + r$ da cui

$$\chi(L_1, L_2) = (n + r) - (m + r) = n - m$$

che non dipende da L_3 .

Proposizione 2.3.6. *Sia L un reticolo di classe Λ , e sia $s \in GL(V)$, chiaramente sL è ancora un reticolo e si ha*

$$\chi(L, sL) = v_p(\det(s))$$

Dimostrazione. Come sempre posso scegliere una base $\{e_1, e_2\}$ di L in modo che $\{p^a e_1, p^b e_2\}$ sia una base di sL . La matrice di s è allora il prodotto della matrice $D = \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix}$ con una matrice $A \in GL_2(\mathbb{Z}_p)$, quindi

$$v_p(\det(s)) = v_p(\det(DA)) = v_p(\det(D) \det(A)) = v_p(p^{a+b}) + v_p(u),$$

$u \in \mathbb{Z}_p^\times$ quindi $v_p(u) = 0$, allora

$$v_p(\det(s)) = a + b.$$

Ci rimane da controllare che $\chi(L, sL) = a + b$, e questo si vede perchè dal momento che $L \cap sL$ ha come base $\{p^{\max\{0,a\}} e_1, p^{\max\{0,b\}} e_2\}$, le combinazioni possibili per $n = l(L/L \cap sL)$ e $m = l(sL/L \cap sL)$ sono:

$$\begin{cases} n = a + b, m = 0 & \text{se } a, b \geq 0 \\ n = b, m = -a & \text{se } a < 0, b \geq 0 \\ n = a, m = -b & \text{se } a \geq 0, b < 0 \\ n = 0, m = -a - b & \text{se } a, b < 0 \end{cases}$$

Quindi in ogni caso

$$\chi(L, sL) = n - m = a + b.$$

□

Corollario 2.3.7. *Si ha che $d(\Lambda, s\Lambda) \equiv v_p(\det(s)) \pmod{2}$.*

Dimostrazione. Usando le notazioni precedenti

$$d(\Lambda, s\Lambda) = |a - b| \equiv a + b \pmod{2} = v_p(\det(s)).$$

□

Il gruppo $GL(V)$ agisce evidentemente sull'albero X , e quindi, ciò che a noi più interessa, $SL(V)$ agisce su X . Inoltre se consideriamo la seguente relazione di equivalenza sui vertici di X :

$$\Lambda \sim \Lambda' \text{ se } d(\Lambda, \Lambda') = 2k, k \in \mathbb{N};$$

vediamo che se $s \in SL(V)$, allora per il corollario appena dimostrato

$$d(\Lambda, s\Lambda) \equiv v_p(\det(s)) = v_p(1) = 0 \pmod{2},$$

e quindi s conserva le due classi di equivalenza dei vertici. In particolare ne risulta che $SL(V)$ agisce senza inversione su X .

Vediamo adesso come sono fatti gli stabilizzatori dei vertici e degli spigoli di X rispetto all'azione di $SL(V)$. Se L è un reticolo di V di classe Λ , indichiamo con G_L il sottogruppo di $SL(V)$ che stabilizza L e G_Λ rispettivamente quello che stabilizza Λ ; allo stesso modo se $\Lambda\Lambda'$ è uno spigolo di X indichiamo il suo stabilizzatore con $G_{\Lambda\Lambda'}$.

Per la definizione delle classi di reticoli, G_Λ è l'insieme di $s \in SL(V)$ per i quali esiste un $x \in \mathbb{Q}_p^*$ con $sL = xL$.

Lemma 2.3.8. *Se L è un reticolo di classe Λ , allora $G_L = G_\Lambda$.*

Dimostrazione. Un'inclusione è ovvia, infatti se $sL = L$, $xsL = xsL = xL$ quindi s stabilizza Λ , vediamo invece che $G_\Lambda \subset G_L$. Sia $s \in G_\Lambda$ abbiamo allora $sL = xL$ per un qualche $x \in \mathbb{Q}_p^*$. Scegliamo una base $\{e_1, e_2\}$ di L tale che $\{p^{v_p(x)}e_1, p^{v_p(x)}e_2\}$ sia una base di xL , allora $L \cap xL$ ha come base $\{p^{\max\{0, v_p(x)\}}e_1, p^{\max\{0, v_p(x)\}}e_2\}$. A seconda del segno di $v_p(x)$, ho quindi che o $l(L/L \cap xL) = 2v_p(x)$ e $l(L/L \cap xL) = 0$, oppure $l(L/L \cap xL) = 0$ e $l(L/L \cap xL) = -2v_p(x)$. Quindi in ogni caso $\chi(L, xL) = 2v_p(x)$. Per la proposizione 2.3.6 abbiamo allora

$$2v_p(x) = v_p(\det(s)) = 0 \Rightarrow v_p(x) = 0 \Rightarrow x \in \mathbb{Z}_p^\times.$$

Questo significa che $xL = L$ e quindi $s \in G_L$. □

Osserviamo che G_L si può identificare con $SL_2(\mathbb{Z}_p)$ perchè se scriviamo le matrici degli elementi di G_L rispetto ad una base di L , abbiamo che questi sono gli automorfismi di L che appartengono al gruppo $SL(V)$, cioè $GL_2(\mathbb{Z}_p) \cap SL_2(\mathbb{Q}_p)$. Ora sia Λ, Λ' uno spigolo di X e scegliamo due rappresentanti L, L' di Λ, Λ' , in modo che $L' \subset L$ e $l(L/L') = 1$. Per il lemma che abbiamo appena visto, lo stabilizzatore $G_{\Lambda\Lambda'}$ è $G_L \cap G_{L'}$. Questo possiamo vederlo come il sottogruppo di G_L costituito dagli elementi la cui immagine nel gruppo degli

automorfismi del piano L/pL , $GL(L/pL) \simeq GL_2(\mathbb{F}_p)$ stabilizza la retta L'/pL ; questo è detto il sottogruppo di Iwahori di $SL(V)$ rispetto a $\Lambda\Lambda'$. Come è fatto questo gruppo? Prendiamo come al solito una base $\{e_1, e_2\}$ di L tale che $\{e_1, pe_2\}$ sia una base di L' . Allora abbiamo la retta

$$L'/pL = \{(t, 0) \in L/pL \mid t \in \mathbb{F}_p\}.$$

Quindi il sottogruppo di $GL_2(\mathbb{F}_p)$ che fissa L/L' è costituito dalle matrici

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ tali che } A \begin{pmatrix} t \\ 0 \end{pmatrix} = \begin{pmatrix} at \\ ct \end{pmatrix} \text{ sia del tipo } \begin{pmatrix} x \\ 0 \end{pmatrix} \text{ cioè con } c = 0.$$

La controimmagine di questo in $SL_2(\mathbb{Z}_p)$ corrisponde alle matrici della forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ con } c \in p\mathbb{Z}_p.$$

Siamo ormai in dirittura d'arrivo, per poter applicare i risultati che conosciamo sull'azione dei gruppi sugli alberi ci manca solo un tassello fondamentale.

Teorema 2.3.9. *Siano L, L' due reticoli di V con $L' \subset L$ e $l(L/L') = 1$, e siano Λ, Λ' le rispettive classi; sono due vertici adiacenti nell'albero X . Si ha che il segmento $\Lambda \overset{\circ}{\longrightarrow} \overset{\circ}{\rightarrow} \Lambda'$ è un dominio fondamentale (vedi defin.2.15) per l'azione di $SL(V)$ sull'albero X .*

Dimostrazione. Vediamo innanzitutto l'azione sui vertici. Siano X^+ e X^- gli insiemi dei vertici che sono ad una distanza pari rispettivamente da Λ e Λ' . La partizione (X^+, X^-) è invariante sotto l'azione di $SL(V)$, dobbiamo quindi mostrare che per ogni $\Lambda_1 \in X^+$ (e rispettivamente $\Lambda_2 \in X^-$), esiste un $g \in SL(V)$ tale che $g\Lambda = \Lambda_1$ ($g\Lambda' = \Lambda_2$). Supponiamo di avere $\Lambda_1 \in X^+$ (il caso di X^- è analogo) con distanza $2n$ da Λ . Sia L_1 un rappresentante di Λ_1 , possiamo trovare una base $\{e_1, e_2\}$ di L in modo che $\{p^a e_1, p^b e_2\}$ con $|a-b| = 2n$ sia una base di L_1 . Moltiplicando per un opportuna costante $x \in \mathbb{Q}_p^*$ possiamo supporre $a = n$, $b = -n$. Sia g l'automorfismo di V con matrice $\begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix}$ rispetto a $\{e_1, e_2\}$; $g \in SL(V)$ e $gL = L_1$, e, dal momento che $gxL = xgL = xL_1$ per ogni $x \in \mathbb{Q}_p^*$, abbiamo che $g\Lambda = \Lambda_1$.

Per l'azione sugli spigoli, visto quanto detto prima, ci basta dimostrare che G_L agisce transitivamente sugli spigoli con origine Λ , o, equivalentemente, sull'insieme P_L dei sottoreticoli L_1 di L tali che $l(L/L_1) = 1$. Questo si identifica con l'insieme delle rette del \mathbb{F}_p -piano L/pL , ci basta allora vedere che l'immagine

di G_L in $GL(L/pL) \simeq GL_2(\mathbb{F}_p)$, che è $SL(L/pL) \simeq SL_2(\mathbb{F}_p)$, agisce transitivamente sulle rette. Scegliamo una base $\{e_1, e_2\}$ di L e sia L_0 il reticolo di base $\{e_1, pe_2\}$, allora la proiezione di L_0 è

$$L_0/pL = \{(t, 0) \in L/pL \mid t \in \mathbb{F}_p\}.$$

E' chiaro che una qualunque retta di L/pL la possiamo scrivere

$$r = \{(\alpha t, \beta t) \in L/pL \mid t \in \mathbb{F}_p, (\alpha, \beta) \neq (0, 0)\}.$$

Abbiamo quindi, a seconda che $\alpha \neq 0$ o $\beta \neq 0$,

$$\begin{pmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{pmatrix} \begin{pmatrix} t \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha t \\ \beta t \end{pmatrix} \text{ oppure } \begin{pmatrix} \alpha & -\beta^{-1} \\ \beta & 0 \end{pmatrix} \begin{pmatrix} t \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha t \\ \beta t \end{pmatrix}.$$

Gli automorfismi rappresentati da queste matrici stanno in $SL(L/pL)$ perchè il determinante è 1, e questo dimostra che l'azione è transitiva. \square

Possiamo così giungere al risultato finale.

Teorema 2.3.10. *Il gruppo $SL_2(\mathbb{Q}_p)$ si può scrivere come amalgama $SL_2(\mathbb{Z}_p) *_{\Gamma} SL_2(\mathbb{Z}_p)$, dove Γ indica il sottogruppo di $SL_2(\mathbb{Z}_p)$ che consiste delle matrici della forma $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $c \in p\mathbb{Z}_p$.*

Dimostrazione. Questo segue dal teorema 2.3.9 e dal teorema 2.2.7, infatti abbiamo che il gruppo $SL_2(\mathbb{Q}_p)$ agisce sull'albero X che abbiamo definito, con il segmento $\overset{\Lambda}{\circ} \longrightarrow \overset{\Lambda'}{\circ}$ come dominio fondamentale. Gli stabilizzatori dei vertici sono due copie di $SL_2(\mathbb{Z}_p)$ e lo stabilizzatore dello spigolo è Γ , i due omomorfismi iniettivi usati per definire l'amalgama sono

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ e } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & pb \\ p^{-1}c & d \end{pmatrix}.$$

\square

Bibliografia

- [1] J.P.Serre: *Trees*, Springer-Verlag, Berlin, Heidelberg, New York 1980
- [2] N.Jacobson: *Basic Algebra I*, W.H.Freeman and Company, San Francisco 1974
- [3] M.Reid: *Undergraduate Commutative Algebra*, Cambridge University Press, Cambridge 1995
- [4] W.Magnus, A.Karrass, D.Solitar: *Combinatorial Group Theory: Presentations of groups in terms of generators and relations*, Dover Publications, New York 1976