Alcune note per un corso di Teoria dei Gruppi

Andrea Caranti

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, 38123 Trento
Email address: andrea.caranti@unitn.it
URL: http://caranti.maths.unitn.it/

Introduzione

Nell'A.A. 2015/16 tengo per la prima volta il corso di Teoria dei Gruppi. Raccolgo qui alcuni brevi appunti, nella parte iniziale con qualche riciclo da quelli del corso di Algebra.

Gli appunti sono stati ampliati in modo sostanziale nell'A.A. 2017/18. Questa è la versione 2020/21, a cui fra le altre cose è stato aggiunta la sezione 5.6 sulla semplicità dei gruppi alterni, e la sezione 6.5 con la dimostrazione del Teorema di Kummer.

La versione più recente è reperibile presso

http://www.science.unitn.it/∼caranti/

Testi consigliati

Fra i tanti buoni testi di teoria dei gruppi disponibili segnalo

- [**Mac12**] (mi sono laureato con l'autore),
- [**Hup67**], in tedesco, sempre eccellente,
- [**Gor80**], un altro grande classico,
- [**Rob96**], completo e molto chiaro,
- [**Rot95**], splendido, e con una eccellente scelta di argomenti.
- Ho da poco cominciato a leggere [**Ser16**], bellissimo come tutte le cose di Serre, un po' denso.

Indice

CAPITOLO 1

Preliminari

1.1. Definizioni

1.1.1. Definizione. Un gruppo è una terna $(G, \cdot, 1)$, dove

- G è un insieme,
- "$\cdot$" è una operazione binaria associativa su G,
- $1 \in G$ soddisfa
$$a \cdot 1 = 1 \cdot a = a$$
per ogni $a \in G$, e
- per ogni $a \in G$ esiste $b \in G$ tale che
$$a \cdot b = b \cdot a = 1.$$

Nei testi più recenti si trova spesso scritto "e" al posto di "1"; qualche volta lo faremo anche noi. Noi tenderemo a usare la notazione *moltiplicativa* della Definizione 1.1.1, abbreviando come d'uso $a \cdot b = ab$, ma naturalmente se un gruppo si porta appresso una operazione scritta in altro modo, useremo quest'ultima. Per esempio gli interi sono un gruppo rispetto alla somma, dunque parleremo del gruppo *additivo* $(\mathbf{Z}, +, 0)$ degli interi.

Dalla definizione segue subito

(1) L'elemento 1 è unico, e viene detto *elemento neutro* o *unità* (o *zero* in notazione additiva). Infatti se ho due elementi e, f con la proprietà che $ae = ea = a = af = fa$ per ogni $a \in G$, allora $e = ef = f$. (Qui come altrove basta assumere $ea = a = af$ per ogni $a \in G$, ma in genere non staremo a fare queste distinzioni, tranne quando sia significativo ai fini dell'esposizione.)

(2) L'elemento "b" è unico, e viene detto l'*inverso* di a, e indicato con a^{-1} (*opposto* $-a$ in notazione additiva). Infatti se $ab = 1 = ca$, allora $c = c1 = c(ab) = (ca)b = 1b = b$, dove abbiamo messo in risalto l'uso della proprietà associativa.

Segnaliamo due *curiosità*.

(1) Si può definire un gruppo come una terna $(G, \cdot, e)$, ove $\cdot$ è una operazione binaria, associativa su G, l'elemento $1 \in G$ soddisfa $ae = a$ per ogni $a \in G$, e per ogni $a \in G$ esiste $b \in G$ tale che $ab = e$. Cercate "`one-side definition of group`" per vedere che una simile struttura è in effetti un gruppo.

(2) Un'altra definizione alternativa di gruppo [**HN52**] dice che un gruppo è una coppia $(G, /)$, ove G è un insieme non vuoto, e "$/$" è un'operazione

binaria su G che soddisfa il singolo assioma

$$x/((((x/x)/y)/z)/(((x/x)/x)/z)) = y,$$

per ogni $x, y, z \in G$. In termini della Definizione 1.1.1, dovete pensare che $a/b = ab^{-1}$.

Per quanto riguarda il primo punto, ecco uno **spoiler**. Per ogni $a \in G$, indichiamo con a' un elemento tale che $aa' = e$. (E a'' sarà un elemento tale che $a'a'' = e$.)

Si ha dapprima, per ogni $a \in G$,

$$a = ae = a(a'a'') = (aa')a'' = ea''. \tag{1.1.1}$$

Poi, moltiplicando a sinistra per e questa eguaglianza,

$$ea = e(ea'') = (ee)a'' = ea'' = a.$$

Dunque e è anche unità sinistra, e da (1.1.1) si ottiene $a = a''$, cioè $a'a = a'a'' = e$, e a' è anche un inverso sinistro per a.

1.2. Sottogruppi

Un sottogruppo H di un gruppo G è un sottoinsieme non vuoto che è ancora un gruppo rispetto alla stessa operazione di G. Dunque vale

- $1 \in H$,
- se $a \in H$, allora $a^{-1} \in H$.
- se $a, b \in H$, allora $a \cdot b \in H$,

In simboli, si scrive $H \leq G$ per indicare che H è un sottogruppo di G.

A volte torna utile il seguente

1.2.1. Lemma. *Sia G un gruppo, $H \subseteq G$. Sono equivalenti*

(1) H è un sottogruppo di G, e
(2) $H \neq \emptyset$, e se $a, b \in H$, allora $ab^{-1} \in H$.

Al posto di $H \neq \emptyset$ si può anche richiedere $1 \in H$.

Dimostrazione. Che (1) implichi (2) è immediato.

Viceversa, valga (2). Dato che H non è vuoto, conterrà un elemento a. Allora $1 = aa^{-1} \in H$. Dunque se $b \in H$, si ha $b^{-1} = 1 \cdot b^{-1} \in H$. Infine, se $a, b \in H$, allora $b^{-1} \in H$, dunque $ab = a(b^{-1})^{-1} \in H$. □

1.3. Classi laterali e Teorema di Lagrange

Se H è un sottogruppo di un gruppo G, possiamo definire una relazione su G mediante

$$a \sim b \text{ se e solo se } a \cdot b^{-1} \in H.$$

Si vede subito che si tratta di una relazione di equivalenza:

Proprietà riflessiva: Se $a \in G$, allora $a \cdot a^{-1} = 1 \in H$,e dunque $a \sim a$.

Proprietà simmetrica: Se $a \sim b$, allora $a \cdot b^{-1} \in H$, dunque anche $H \ni (a \cdot b^{-1})^{-1} = b \cdot a^{-1}$, e quindi $b \sim a$.

Proprietà transitiva: Se $a \sim b$ e $b \sim c$, allora $a \cdot b^{-1}, b \cdot c^{-1} \in H$, dunque $H \ni (a \cdot b^{-1}) \cdot (b \cdot c^{-1}) = a \cdot c^{-1}$, e quindi $a \sim c$.

Per la classe di equivalenza di $a \in G$ abbiamo

$$\begin{aligned}
[a] &= \{\, x \in G : x \sim a \,\} \\
&= \left\{\, x \in G : x \cdot a^{-1} \in H \,\right\} \\
&= \left\{\, x \in G : \text{esiste } h \in H \text{ tale che } x \cdot a^{-1} = h \,\right\} \\
&= \{\, x \in G : \text{esiste } h \in H \text{ tale che } x = ha \,\} \\
&= \{\, ha : h \in H \,\} \\
&= Ha,
\end{aligned}$$

ove le ultime due righe costituiscono la definizione della *classe laterale destra* ha di H in G.

In maniera del tutto analoga, si possono definire le classi laterali *sinistre* aH. Badate che non è detto che in generale valga $aH = Ha$. Ad esempio, consideriamo $G = S_3$, $H = \langle\, (12) \,\rangle = \{\, 1, (12) \,\}$, e $a = (123)$. Allora

$$aH = \{\, (123), (23) \,\} \neq \{\, (123), (13) \,\} = Ha.$$

Per ragioni generali, le classi laterali sono una partizione di G. Sia ora G un gruppo con un numero finito di elementi, H un sottogruppo di G, e $n = |G : H|$ sia il numero di classi laterali (destre) di G in H. Il numero $|G : H|$ si dice *indice* di H in G. Siano $Ha_1, Ha_2, \ldots, Ha_n$ le classi laterali distinte. Si ha quindi che G è unione disgiunta di esse, e quindi

$$|G| = \sum_{i=1}^{n} |Ha_i| \tag{1.3.1}$$

D'altra parte

1.3.1. Lemma. *Per ogni $a \in G$ si ha che H e Ha hanno lo stesso numero di elementi.*

Dimostrazione. Mostriamo che c'è una corrispondenza biunivoca fra gli elementi di H e quelli di Ha. Questa corrispondenza è data da $h \mapsto ha$. E' suriettiva per definizione, e iniettiva perché da $h_1 a = h_2 a$ segue $h_1 = h_2$, moltiplicando a destra per a^{-1}. □

A questo punto possiamo completare (1.3.1):

$$|G| = \sum_{i=1}^{n} |Ha_i| = |H| \cdot |G : H|. \tag{1.3.2}$$

Abbiamo ottenuto

1.3.2. Teorema (Teorema di Lagrange). *Sia G un gruppo finito, e H un suo sottogruppo. Allora l'ordine di H divide l'ordine di G.*

Una prima conseguenza utile è che se un gruppo G ha ordine un numero primo, allora sappiamo subito come è fatto.

1.4. Indici

Se G è un gruppo finito, e $K \leq H \leq G$, allora applicando due volte il teorema di Lagrange si ha

$$|\, G \,| = |\, G : H \,| \cdot |\, H \,| = |\, G : H \,| \cdot |\, H : K \,| \cdot |\, K \,|\,,$$

Da cui

$$|\, G : K \,| = \frac{|\, G \,|}{|\, K \,|} = |\, G : H \,| \cdot |\, H : K \,|\,.$$

In realtà vale più in generale

1.4.1. Teorema. *Sia G un gruppo, $K \leq H \leq G$.*
Se $|\, G : K \,|$ è finito, allora sono finiti anche $|\, G : H \,|\,, |\, H : K \,|$.
Se sono finiti $|\, G : H \,|\,, |\, H : K \,|$, allora è finito $|\, G : K \,|$, e si ha

$$|\, G : K \,| = |\, G : H \,| \cdot |\, H : K \,|\,.$$

Dimostrazione. Per la prima parte, è chiaro che le classi laterali di K in H sono un sottoinsieme delle classi laterali di K in G, e che la funzione $gK \mapsto gH$ è ben definita (verificare) e suriettiva.

Per la seconda parte, cominciamo col definire un *trasversale* $R(G, K)$ di K in G come un sistema completo di rappresentanti per le classi laterali di K in G, cioè un insieme che consiste di un elemento per ogni classe laterale, è similmente per altre classi laterali.

Notate che, nonostante il simbolo usato, in generale un trasversale è tutt'altro che unico. Se il gruppo finito G ha un sottogruppo di ordine n e di indice m, ogni scelta di una degli n elementi in ognuna delle m classi laterali mi dà un trasversale, dunque di trasversali ce ne sono n^m.

1.4.2. Commento. Una definizione alternativa, e più precisa, di trasversale, poggia su questa osservazione. La funzione $\sigma : g \mapsto gk$ è una funzione suriettiva $G \to \mathcal{L}$, ove $\mathcal{L} = \{\, gK : g \in G \,\}$ è l'insieme delle classi laterali sinistre di K in G. Dunque ha un'inversa sinistra $\tau : \mathcal{L} \to G$ tale che $\tau \circ \sigma$ sia l'identità su $\mathcal{L}$. In altre parole, $(gK)\tau \in gK$, ovvero $gK = ((gK)\tau)K$, anche se in generale non sarà $(gK)\tau = g$. Un trasversale secondo la nostra definizione è l'immagine di una tale funzione τ.

Siano dunque

$$R(G : H), R(H : K)$$

trasversali per le varie classi laterali. Affermo che gli elementi

$$x \cdot y, \text{ per } x \in R(G : H) \text{ e } y \in R(H : K) \tag{1.4.1}$$

(sono distinti e) formano un trasversale $R(G : K)$ di K in G. Questo proverà il risultato annunciato. La dimostrazione è analoga a quella della formula dei gradi.

Sia allora gK una classe laterale di K in G. Allora $gKH = gH = xH$ per un *unico* $x \in R(G : H)$. Dunque $x^{-1}g \in H$, e quindi $x^{-1}gK = yK$ per un *unico* $y \in R(H : K)$, da cui $gK = xyK$.

Questo mostrerebbe anche che gli elementi di (1.4.1) sono distinti, ma rivediamolo comunque in dettaglio.

Siano $x, x' \in R(G : H)$, $y, y' \in R(H : K)$. Se $xyK = x'y'K$, allora $xH = xyH = x'y'H = x'H$, dunque $x = x'$, da cui $yK = y'K$ e dunque $y = y'$. Dunque tutte le classi laterali xyK sono distinte, per $x \in R(G : H), y \in R(H : K)$, e a maggior ragione lo sono gli elementi. □

Quando $|\, G : K \,|$ è finito, c'è una dimostrazione alternativa interessante, che consiste nel notare che il sottogruppo normale $N = \bigcap_{g \in G} K^g$ ha indice finito in G (Lemma 5.5.1), dunque si può applicare il teorema di Lagrange nel gruppo finito G/N.

1.5. Sottogruppi normali

1.5.1. Definizione. Un sottogruppo N del gruppo G si dice *normale* se soddisfa la condizione che $aN = Na$ per ogni $a \in G$.

Certamente se G è commutativo (ovvero è commutativa l'operazione in G), allora ogni sottogruppo di G è normale. Infatti $an = na$ per ogni $a \in G$ e ogni $n \in N$. Ma in generale sto solo sostenendo che i due insiemi

$$aN = \{\, an : n \in N \,\} \qquad Na = \{\, na : n \in N \,\}$$

abbiano gli stessi elementi, non che si abbia $an = na$ per ogni $a \in G$ e ogni $n \in N$. (Un esempio in S_3.)

Vale la seguente

1.5.2. Proposizione. *Sia G un gruppo, N un suo sottogruppo. Sono equivalenti:*

(1) per ogni $a \in G$, si ha $aN = Na$;
(2) per ogni $a \in G$, si ha $a^{-1}Na = N$;
(3) per ogni $a \in G$, si ha $a^{-1}Na \subseteq N$;
(4) per ogni $a \in G$ e ogni $n \in N$, si ha $a^{-1}na \in N$.

1.6. Gruppo quoziente

Sia G un gruppo, e N un suo sottogruppo normale. Allora l'insieme

$$G/N = \{\, aN : a \in G \,\}$$

diventa un gruppo con l'operazione

$$aN \cdot bN = (ab)N.$$

Il punto essenziale è mostrare che questa operazione è ben definita, poi il resto segue direttamente. L'elemento neutro di G/N è $N = 1N$, e $(aN)^{-1} = a^{-1}N$.

1.6.1. Esercizio. *Sia $N \leq G$. Supponiamo che l'operazione*

$$aN \cdot bN = (ab)N.$$

sia ben definita. Si mostri che N è un sottogruppo normale di G.

1.7. Morfismi

Con la questione di algebra universale.

1.8. Teoremi di isomorfismo

Per ora vi rimando agli appunti del corso di algebra [**CM19**]. Ecco comunque gli enunciati.

1.8.1. Teorema (Primo teorema di isomorfismo fra gruppi). *Siano A, C gruppi. (Per semplicità, scriviamo allo stesso modo, come "$\cdot$", o semplicemente con la giustapposizione, le operazioni su A e C.)*

Sia $f : A \to C$ un morfismo di gruppi suriettivo.

Si consideri il nucleo *di f*

$$N = \ker(f) = \{\, x \in A : f(x) = 1 \,\}.$$

Allora N è un sottogruppo normale di A.. Si consideri il gruppo quoziente A/N, e sia $\pi : A \to A/N$ la funzione tale che $\pi(a) = aN$.

Allora π è un morfismo di gruppi.

(1.8.1)
$$\begin{array}{ccc} A & \xrightarrow{f} & C \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle g} & \\ A/N & & \end{array}$$

Inoltre esiste un'unica funzione $g : A/N \to C$ *che fa commutare il diagramma* (1.8.1)*, ovvero tale che $f = g \circ \pi$. Tale g è un isomorfismo di gruppi.*

C'è un'utile estensione del primo teorema.

1.8.2. Teorema. *Siano A, C gruppi, $N \trianglelefteq A$, sia $\pi : A \to A/N$ il morfismo $\pi(a) = aN$.*

Sia $f : A \to C$ un morfismo.

Allora sono equivalenti:

(1) esiste un morfismo $g : A/N \to C$ che fa commutare il diagramma (1.8.2)*, e*
(2) $N \leq \ker(f)$.

(1.8.2)
$$\begin{array}{ccc} A & \xrightarrow{f} & C \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle g} & \\ A/N & & \end{array}$$

Dimostrazione. Se esiste g, e dunque è ben definito, sia $x \in N$. Allora $xN = N = 1N$ implica $f(x) = g(xN) = g(1N) = f(1) = 1$, cioè $N \leq \ker(f)$.

Viceversa, se $N \leq \ker(f)$, la funzione $g : A/N \to C$ definita da $g(aN) = f(a)$ è ben definita, perchè se $xN = yN$, allora $x^{-1}y \in N$, dunque $f(x^{-1}y) = 1$, ovvero $f(x) = f(y)$. □

1.8.3. Teorema (Secondo teorema di isomorfismo per gruppi). *Sia G un gruppo, H un suo sottogruppo, N un suo sottogruppo normale.*

(1) $HN = \{\, xy : x \in H, y \in N \,\}$ *è un sottogruppo di* G *contenente il sottogruppo normale* N*.*
(2) $H \cap N$ *è un sottogruppo normale di* H*.*
(3) La funzione

$$\begin{aligned} \psi : \frac{H}{H \cap N} &\to \frac{HN}{N} \\ xH \cap N &\mapsto xN \end{aligned}$$

è un isomorfismo di gruppi.

1.8.4. Teorema (Terzo teorema di isomorfismo per gruppi). *Sia* G *un gruppo,* N *un suo sottogruppo normale,* $\pi : G \to G/N$ *il morfismo canonico.*

(0) Se $H \leq G$*, allora* $\pi^{-1}(\pi(H)) = HN$*.*
(1) I sottogruppi di G/N *si scrivono in modo unico nella forma* H/N*, ove* H *è un sottogruppo di* G *che contiene* N*;*
(2) sia H *un sottogruppo di* G *che contiene* N*, allora* H/N *è normale in* G/N *se e solo se* H *è normale in* G*;*
(3) se H *è un sottogruppo normale di* G *che contiene* N*, si ha un isomorfismo fra*

$$\frac{G/N}{H/N} \qquad e \qquad G/H.$$

Tanto per ribadire, il punto (1) dice che c'è una corrispondenza biunivoca

$$\begin{aligned} \{\, H : N \leq H \leq G \,\} &\to \{\, \mathcal{H} : \mathcal{H} \leq G/N \,\} \\ H &\mapsto H/N \end{aligned}$$

1.9. Gruppi ciclici

Sia G un gruppo, $a \in G$, e $C = \langle\, a \,\rangle$ un gruppo ciclico, ovvero il più piccolo sottogruppo di G che contenga a. È facile vedere che $C = \{\, a^i : i \in \mathbf{Z} \,\}$.

La funzione

$$\begin{aligned} f : \mathbf{Z} &\to \langle\, a \,\rangle \\ i &\mapsto a^i \end{aligned}$$

è dunque una funzione suriettiva, ed è un morfismo di gruppi, per la regola delle potenze $a^{i+j} = a^i a^j$.

Si ha $\ker(f) = \{\, i \in \mathbf{Z} : a^i = 1 \,\}$.

Quando $\ker(f) = \{\, 0 \,\}$, si ha che f è anche iniettiva, e dunque è un isomorfismo.

Sia dunque $\ker(f) = n\mathbf{Z}$, con $n > 0$. Ricordiamo che

$$n = \min \{\, i \in \ker(f) : i > 0 \,\} = \min i > 0 : a^i = 1.$$

n si dice *ordine* o *periodo* di a, e si indica con $|\, a \,|$. Dato che $\mathbf{Z}/n\mathbf{Z} \cong \langle\, a \,\rangle$, abbiamo che l'ordine del gruppo $\langle\, a \,\rangle$ è eguale all'ordine dell'elemento a. Inoltre, dato che $\mathbf{Z}/n\mathbf{Z}$ è l'insieme delle classi di $0, 1, \ldots, n-1$, si ha che $\langle\, a \,\rangle = \{\, a^0 = 1, a^1 = a, a^2, \ldots, a^{n-1} \,\}$.

Vale la seguente

1.9.1. Proposizione. *Sia $C = \langle\, a \,\rangle$ un gruppo ciclico di ordine n. Allora G ha un unico sottogruppo di ordine m, per ogni $m \mid n$.*

Dimostrazione. **Primo modo.** Per $k \mid n$ si ha che

$$\left|\, a^k \,\right| = \frac{|\, a \,|}{\gcd(|\, a \,|, k)} = \frac{n}{\gcd(n,k)} = \frac{n}{k}.$$

Ponendo $k = n/m$ si ha dunque che $\left|\left\langle\, a^{n/m} \,\right\rangle\right| = m$.

Viceversa, se H è un sottogruppo di C di ordine m, allora $H \trianglelefteq C$ dato che C è abeliano, dunque il gruppo quoziente C/H ha ordine n/m, e per l'elemento $aH \in C/H$ si ha $(aH)^{n/m} = a^{n/m}H = 1H = H$, da cui $a^{n/m} \in H$. Dunque $\left\langle\, a^{n/m} \,\right\rangle \leq H$, e dato che i due sottogruppi hanno lo stesso ordine m, sono eguali.

Secondo modo. Dato che $\mathbf{Z}/n\mathbf{Z} \cong \langle\, a \,\rangle$, cerchiamo i sottogruppi di $\mathbf{Z}/n\mathbf{Z}$. Per il terzo teorema di isomorfismo, sono tutti e soli della forma $k\mathbf{Z}/n\mathbf{Z}$, ove $n\mathbf{Z} \leq k\mathbf{Z}$. Ora $n\mathbf{Z} \subseteq k\mathbf{Z}$ se e solo se $k \mid n$, e in tal caso $|\, k\mathbf{Z}/n\mathbf{Z} \,| = n/k$. □

CAPITOLO 2

Coniugio, sottogruppi generati, prodotti

2.1. Coniugio

2.2. Permutazioni

2.2.1. PROPOSIZIONE. *Sia A un insieme non vuoto. L'insieme delle mappe biiettive su A forma un gruppo rispetto alla composizione, in cui la mappa identica è l'elemento neutro.*

Particolarmente quando A è finito, gli elementi di G si dicono le *permutazioni* di A. Se $A = \{1, 2, \ldots, n\}$, G è detto il *gruppo simmetrico su n lettere,* e viene indicato con S_n.

Notate che per $A = \{1, 2, \ldots, n\}$ si ha che il monoide M ha n^n elementi, e il gruppo S_n ne ha $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$.

Ogni elemento $\sigma \in S_n$ si può scrivere come *prodotto di cicli disgiunti,* usando questo algoritmo. Da questo momento in poi, e per tutto il resto della sezione, scriviamo le funzioni a destra dell'argomento, e le componiamo da sinistra a destra. Dunque scrivo $x\sigma$ per il valore di σ sull'elemento $x \in A$, e $x\sigma\tau = (x\sigma)\tau$, per $\sigma, \tau \in S_n$.

(1) Apro uno parentesi tonda.
(2) Scrivo il più piccolo numero a che non abbia già scritto.
(3) Se b è il numero che ho appena scritto, dopo di lui (separando eventualmente con una virgola) scrivo $b\sigma$.
(4) Ripeto il passaggio (3) finché non dovrei riscrivere a, il primo numero scritto dopo la parentesi tonda. Allora *non* riscrivo a, e chiudo la parentesi tonda.
(5) Se non ho ancora scritto tutti i numeri di $\{1, 2, \ldots, n\}$, vado a (1), altrimenti termino.

Ad esempio, parto dalla permutazione σ

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 19 & 10 & 20 & 14 & 9 & 13 & 2 & 6 & 8 & 1 & 17 & 7 & 3 & 5 & 18 & 15 & 11 & 4 & 12 & 16 \end{pmatrix}$$

dove si intende che $1\sigma = 19$, $2\sigma = 20$, ecc, cioè σ manda un numero nella prima riga in quello subito sotto. Allora σ si scrive come

$$\sigma = (1, 19, 12, 7, 2, 10)(3, 20, 16, 15, 18, 4, 14, 5, 9, 8, 6, 13)(11, 17).$$

Gli oggetti fra due parentesi tonde aperte e chiuse, in questo caso $(1, 19, 12, 7, 2, 10)$, $(3, 20, 16, 15, 18, 4, 14, 5, 9, 8, 6, 13)$ e $(11, 17)$ si dicono *cicli.* In generale un k-ciclo è

una permutazione che fissa (cioè manda ognuno in sé stesso) tutti gli elementi tranne i k elementi $a_1, a_2, \ldots, a_k$, e su questi opera come $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$. Per tradizione, gli 1-cicli non si scrivono, dunque un k-ciclo si scrive $(a_1 a_2 \ldots a_k)$.

Ad esempio gli elementi di S_3 sono

$$(1)(2)(3), (1,2,3), (1,3,2), (1,2)(3), (1,3)(2), (2,3)(1).$$

Dato che gli 1-cicli non si scrivono, e le virgole si possono omettere, in genere si scrive

$$S_3 = \{\, 1, (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3) \,\},$$

dove $1 = (1)(2)(3)$ è la funzione identica. Notate che

$$(1\,2)(1\,3) = (1\,2\,3), \qquad (1\,3)(1\,2) = (1\,3\,2),$$

dunque S_n non è un gruppo commutativo, per $n \geq 3$.

Si può vedere che valgono i seguenti due fatti.

(1) Nell'algoritmo sopra descritto, quando scrivo un ciclo che comincia con a, il primo elemento che si ripeterà è proprio a.
(2) I cicli che risultano dall'algoritmo sono *disgiunti*, ovvero due ciclic distinti non hanno elementi in comune.

2.2.2. Esercizio. *Si mostri che due cicli disgiunti σ, τ commutano fra loro, cioè $\sigma\tau = \tau\sigma$.*

Più in generale,

2.2.3. Esercizio. *Se σ, τ sono permutazioni sull'insieme Ω, che è unione disgiunta di due sottoinsiemi A e B, tali che*

- *$A\sigma = A$,*
- *σ agisce come l'identità su B,*
- *$B\sigma = B$, e*
- *τ agisce come l'identità su A,*

allora σ e τ commutano.

La ragione è che se $x \in A$, allora

$$x(\sigma\tau) = (x\sigma)\tau = x\sigma,$$

dato che $x\sigma \in A$, e τ agisce come l'identità su A. D'altra parte

$$x(\tau\sigma) = (x\tau)\sigma = x\sigma,$$

dato che $x \in A$, e τ agisce come l'identità su A. Lo stesso ragionamento vale se $x \in B$.

2.2.4. Lemma. *Sia G un gruppo finito, e siano $g, h \in G$ due elementi tali che*

(1) g e h commutano, cioè $gh = hg$,
(2) $\langle\, g \,\rangle \cap \langle\, h \,\rangle = \{\, 1 \,\}$.

Allora

$$|\, gh \,| = \operatorname{lcm}(|\, g \,|, |\, h \,|).$$

2.2.5. Esercizio. *La condizione* (2) *è automaticamente soddisfatta se*

$$\gcd(|\,g\,|\,,|\,h\,|) = 1.$$

In tal caso si ha dunque $|\,gh\,| = |\,g\,| \cdot |\,h\,|$.

Dimostrazione del Lemma. Dato che g, h commutano, per ogni intero n si ha $(gh)^n = g^n h^n$. Se per $n > 0$ si ha $(gh)^n = 1$, allora $g^n = h^{-n} \in \langle\, g\,\rangle \cap \langle\, h\,\rangle = \{\,1\,\}$, dunque $g^n = h^n = 1$, e dunque $|\,g\,|\,,|\,h\,| \mid n$. Ne segue che il più piccolo n tale che $(gh)^n = 1$ è $\mathrm{lcm}(|\,g\,|\,,|\,h\,|)$. □

Ora un n-ciclo ha periodo n, ne segue che se $\sigma \in S_n$ ha struttura ciclica

$$(n_1, \ldots, n_k),$$

allra σ ha periodo $\mathrm{lcm}(n_1, \ldots, n_k)$.

2.2.6. Esercizio. *Si mostri che*

$$(1, 2, 3 \ldots, k-1, k) = (1,2)(1,3)\ldots(1,k-1)(1,k).$$

Dall'Esercizio 2.2.6 segue

2.2.7. Proposizione. *Ogni elemento di* S_n *si scrive come prodotto di* 2*-cicli.*

Notate che i 2-cicli non sono necessariamente disgiunti.
La scrittura come prodotto di 2-cicli non è affatto unica, ad esempio

$$(2,3)(1,2)(2,3) = (1,3).$$

Vale però l'importante

2.2.8. Teorema. *Se una permutazione si può scrivere come il prodotto di* h 2*-cicli, e anche come prodotto di* k 2*-cicli, allora* h *e* k *hanno la stessa parità.*

Dimostrazione. Anticipando un po' un argomento sulle azioni, consideriamo l'anello dei polinomi $A = \mathbf{Z}[x_1, x_2, \ldots, x_n]$. Ad ogni permutazione $\sigma \in S_n$ possiamo associare una permutazione di A, data da

$$p = p(x_1, x_2, \ldots, x_n) \mapsto p\sigma = p(x_{1\sigma}, x_{2\sigma}, \ldots, x_{n\sigma})$$

e questa funzione

$$\begin{aligned} \varphi : S_n &\to S(A) \\ \sigma &\mapsto (p \mapsto p\sigma) \end{aligned}$$

si verifica essere un morfismo.

Consideriamo il polinomio

$$P = P(x_1, x_2, \ldots, x_n) = \prod_{1 \le s < t \le n} (x_s - x_t) \neq 0.$$

Faremo vedere che se (ij), con $i < j$, è un 2-ciclo, allora $P(ij) = -P$. Dato che φ è un morfismo, se $\sigma \in S_n$ è prodotto di h 2-cicli, si avrà $P\sigma = (-1)^h \sigma$, da cui il Teorema.

Consideriamo quindi cosa è $P(ij)$. Scriviamo i soli termini di P che contengono x_i e x_j, dato che gli altri sono invariati in $P(ij)$. In

$$\begin{array}{ccccccccc}
x_1 - x_i & & & & x_1 - x_j & & & & \\
x_2 - x_i & & & & x_2 - x_j & & & & \\
\vdots & & & & \vdots & & & & \\
x_{i-1} - x_i & & & & x_{i-1} - x_j & & & & \\
 & x_i - x_{i+1} & \dots & x_i - x_{j-1} & x_i - x_j & x_i - x_{j+1} & \dots & x_i - x_n & \\
 & & & & x_{i+1} - x_j & & & & \\
 & & & & \vdots & & & & \\
 & & & & x_{j-1} - x_j & & & & \\
 & & & & & x_j - x_{j+1} & \dots & x_j - x_n &
\end{array}$$

le due colonne rosse si scambiano fra loro. Lo stesso avviene per le due righe blu. Per quel che riguarda i termini magenta, notiamo che il loro prodotto è

$$\prod_{k=i+1}^{j-1} (x_i - x_k)(x_k - x_j),$$

e il termine $(x_i - x_k)(x_k - x_j)$ in P viene mandato in $P(ij)$ in $(x_j - x_k)(x_k - x_i) = (x_i - x_k)(x_k - x_j)$. Dunque in $P(ij)$ niente è cambiato, tranne il termine in nero $x_i - x_j$ in $P(ij)$, che viene mandato in $x_j - x_i = -(x_i - x_j)$. Dunque $P(ij) = -P$. □

Dunque la *parità* di una permutazione (cioè la parità del numero di 2-cicli di cui si scrive come prodotto) è ben definita. Una permutazione si dice *pari* o *dispari* a seconda di questa parità. E' abbastanza facile vedere che il prodotto di due permutazioni pari è ancora pari, e che l'inversa di una permutazione pari è ancora pari. (Inoltre la mappa identica è il prodotto di zero 2-cicli, dunque è pari.) Dunque le permutazioni pari formano un sottogruppo di S_n, che si dice *gruppo alterno*, e si indica con A_n.

2.2.9. Definizione. Il *segno* di una permutazione è 1 se la permutazione è pari, -1 se essa è dispari. Dunque il segno di $\sigma \in S_n$ è dato da $P\sigma = \text{segno}(\sigma)P$. La funzione segno : $S_n \to \{1, -1\}$ è subito vista essere un morfismo di gruppi, e il suo nucleo è il gruppo alterno A_n, che dunque è un sottogruppo normale di S_n di indice 2.

2.2.10. Osservazione. Notate che P è, a meno del segno, il determinante della matrice $\mathcal{V}$ di Vandermonde. Dunque applicando (ij) stiamo scambiando le colonne i-sima e j-sima di $\mathcal{V}$, ed è chiaro che il determinante cambi segno. Tranne che per definire il determinante in genere si usa il segno di una permutazione...

2.3. Struttura ciclica e coniugio

Una *partizione* del numero intero positivo n è una successione finita

$$n_1 \geq n_2 \geq \cdots \geq n_k > 0 \tag{2.3.1}$$

tale che $n_1 + n_2 + \dots n_k = n$.

La *struttura ciclica* di una permutazione $\sigma \in S_n$ è la partizione (2.3.1) tale che σ abbia cicli di lunghezza $n_1, n_2, \ldots$. Per esempio la struttura ciclica di $(123)(4567)(8910)(11)(1213)$ è $4, 3, 3, 2, 1$.

Ricordiamo dall'Algebra Lineare che se V è uno spazio vettoriale di dimensione finita n, e $f : V \to V$ è una funzione lineare, scelta una base di V si può associare a f una matrice $n \times n$. Se A e B sono due matrici $n \times n$, allora esse rappresentano la stessa funzione lineare rispetto a due basi diverse se e solo se esiste una matrice $n \times n$ invertibile σ tale che $B = \sigma^{-1} A \sigma$.

Qualcosa di simile vale per le permutazioni. Consideriamo le permutazioni $(123) \in S_6$ e $(456) \in S_6$. Allora

$$(456) = \sigma^{-1}(123)\sigma,$$

ove $\sigma = (14)(25)(36)$. In effetti, se $(a_1, \ldots, a_k) \in S_n$ è un ciclo, e $\sigma \in S_n$, allora si vede

2.3.1. Esercizio.

$$\sigma^{-1}(a_1, \ldots, a_k)\sigma = (a_1\sigma, \ldots, a_k\sigma).$$

2.3.2. Definizione. Sia G un gruppo.

La relazione di *coniugio* su G è definita da definita da aRb se e solo se a e b esiste $x \in G$ tale che $b = x^{-1}ax$.

Si abbrevia $a^x = x^{-1}ax$.

2.3.3. Esercizio.

Sia G un gruppo, $a, x \in G$.

Si mostri che per $a, b, x, y \in G$ valgono

(1) $a^{xy} = (a^x)^y$, e

(2) $(ab)^x = a^x b^x$.

Si mostri che la relazione di coniugio *è una relazione di equivalenza su G.*

La classe $a^G = \{\, x^{-1}ax : x \in G \,\}$ di $a \in G$ rispetto alla relazione di coniugio è detta la classe di coniugio *di a.*

2.3.4. Teorema. *Siano $\alpha, \beta \in S_n$. Sono equivalenti*

(1) α e β sono coniugati, e

(2) α e β hanno la stessa struttura ciclica.

Dimostrazione. Che (1) implichi (2) segue da 2.3.1 e 2.3.3(2).

Viceversa, se α e β hanno la stessa struttura ciclica $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, dunque

$$\alpha = \prod_{i=1}^{k} (a_{i,1}, \ldots, a_{i,n_i}), \qquad \beta = \prod_{i=1}^{k} (b_{i,1}, \ldots, b_{i,n_i}),$$

allora $\beta = \alpha^\sigma$, ove σ è la permutazione che manda $a_{i,j}$ in $b_{i,j}$. □

2.3.5. Esercizio (Probabilmente un po' difficile a questo punto del corso).

Nella dimostrazionwe del Teorema 2.3.4 abbiamo trovato una *permutazione che coniuga α a β, ma in generale ce ne saranno altre. Quante e quali sono le permutazioni σ che coniugano α a β?*

2.4. Automorfismi

Sia G un gruppo.

2.4.1. Esercizio. *I morfismi da G a G (a volte detti* endomorfismi *di G) formano un monoide rispetto alla composizione.*

Dunque l'insieme $\mathrm{Aut}(G)$ degli isomorfismi da G a G formano un gruppo, dato che sono gli elementi invertibili di questo monoide. I suoi elementi vengono detti *automorfismi* di G.

2.4.2. Esercizio. *Sia G un gruppo, $x \in G$.*

Si mostri che la funzione $\iota(x)$, che manda $a \in G$ in a^x, è un automorfismo di G, detto l'automorfismo interno *indotto da x.*

Si mostri che la funzione

$$\begin{aligned} \iota : G &\to \mathrm{Aut}(G) \\ x &\mapsto (a \mapsto a^x) \end{aligned}$$

è un morfismo di gruppi.

L'immagine di ι è un sottogruppo di $\mathrm{Aut}(G)$*, denotato* $\mathrm{Inn}(G)$.

(1) Si mostri che $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

(2) Si mostri che

$$\ker(\iota) = Z(G)$$

ove $Z(G) = \{\, x \in G : ax = xa \text{ per ogni } a \in G \,\}$ è il centro *di G.*

2.5. Gruppi diedrali

Introduciamo una classe di gruppi non commutativi che forniscono esempi interessanti per i concetti di teoria dei gruppi che abbiamo introdotto.

Consideriamo $A = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, \ldots, n-1 \,\}$, e nel monoide delle funzioni da A a sé stesso consideriamo le funzioni della forma $f_{a,b} : x \mapsto ax + b$, per qualche $a, b \in A$, e l'insieme di tali *funzioni affini*

$$S = \{\, f_{a,b} : a, b \in A \,\}.$$

S è un monoide rispetto alla composizione, contiene la funzione identica $\{\, 1 \,\} = \{\, 1 \,\}_A = f_{1,0}$, e si ha

$$x f_{a,b} \circ f_{c,d} = c(ax + b) + d = acx + bc + d = f_{ac,bc+d}(x),$$

e dunque

2.5.1. Lemma.

$$f_{a,b} \circ f_{c,d} = f_{ac,bc+d} \in S.$$

Notate anche che se $f_{a,b} = f_{c,d}$, allora $b = 0 f_{a,b} = 0 f_{c,d} = d$, e $a + b = 1 f_{a,b} = 1 f_{c,d} = c + d$, da cui

2.5.2. Lemma.

$$f_{a,b} = f_{c,d} \quad \textit{se e solo se} \quad a = b, c = d.$$

Quand'è che $f_{a,b}$ è invertibile? Quando esiste $f_{c,d}$ tale che $f_{a,b} \circ f_{c,d} = f_{ac,bc+d} = f_{1,0}$, e dunque $ac = 1$, cioè a è invertibile con inversa $c = a^{-1}$, e $d = -a^{-1}b$.

2.5.3. Lemma. *$f_{a,b}$ se e solo se a è invertibile, e in tal caso*

$$f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}.$$

Consideriamo, nell'anello delle matrici 2×2 a coefficienti in A, l'insieme

$$S' = \left\{ \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} : a, b \in A \right\}.$$

Notiamo che

$$\begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} \cdot \begin{bmatrix} 1 & d \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & d+bc \\ 0 & ac \end{bmatrix},$$

dunque la funzione

$$\varphi : S \to S'$$
$$f_{a,b} \mapsto \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

è un isomorfismo di monoidi. Dato che

$$\det \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} = a,$$

questo spiega il Lemma 2.5.3.

Noi consideremo il cosiddetto *gruppo diedrale*, per $n > 2$, che è un sottogruppo del gruppo degli elementi invertibili del monoide S:

$$D_n = \{ f_{\varepsilon,b} : \varepsilon = \pm 1, b \in A \},$$

che ha $2n$ elementi (mentre se $n = 2$ ne ha solo 2). (Purtroppo nella letteratura più di qualcuno lo chiama D_{2n}.) Dunque $f_{\varepsilon,b}^{-1} = f_{\varepsilon,-\varepsilon b}$.

Consideriamo dapprima il sottoinsieme

$$C_n = \{ f_{1,b} : b \in A \} \subseteq D_n,$$

che ha n elementi. Questo è un sottogruppo ciclico, generato da $f_{1,1}$, infatti si verifica facilmente che $f_{1,1}^b = f_{1,b}$. In effetti, se disponiamo gli elementi di A (qui ci vorrebbe un disegno, che spero di fare in qualche momento) sui vertici di un n-gono regolare, diciamo in senso orario, allora $f_{1,b}$ è la rotazione in senso orario di $2\pi b/n$ (radianti, che altro?). (Qui bisogna intendersi, nel senso che $f_{1,-1}$ è la rotazione di $-2\pi/n$ in senso orario, ovvero di $2\pi/n$ in senso antiorario.)

Invece se consideriamo un elemento $f_{-1,b}$, si ha $f_{-1,b}^2 = f_{(-1)^2,-b+b} = f_{1,0} = \{ 1 \}$. Vogliamo vedere che questi elementi rappresentano *riflessioni* dell'n-gono regolare. Qui ci sono duie casi da considerare, a seconda della parità di n.

Cominciamo col caso n dispari, pensate per semplicità al caso del pentagono regolare, $n = 5$. Qui ci sono cinque riflessioni, rispetto alle rette che passano per un vertice, e bisecano il lato opposto. Per esempio $f_{-1,0}$ ha come unico punto fisso 0, unica soluzione dell'equazione $-x = x f_{-1,0} = x$. Infatti, dato che n è dispari, l'equazione $-x = x$, dunque $2x = 0$ ha come unica soluzione $x = 0$, dato che 2 è

invertibile in A. In generale , $f_{-1,b}$ ha un solo punto fisso, che si ottiene notando come l'equazione

$$-x + b = x f_{-1,b} = x \tag{2.5.1}$$

ovvero $2x = b$ ha come unica soluzione, dato che 2 è invertibile in A,

$$\begin{cases} \frac{b}{2} & \text{se } b \text{ è pari} \\ \frac{b+n}{2} & \text{se } b \text{ è dispari.} \end{cases}$$

Come esempio, sempre per $n = 5$, l'unico punto fisso di $f_{-1,2}$ è 1, mentre l'unico punto fisso di $f_{-1,1}$ è $3 = -2 = -3 + 1$ in $A = \mathbf{Z}/5\mathbf{Z}$.

Nel caso pari, pensate per semplicità al caso dell'esagono regolare $n = 6$. Qui ci sono due tipi di riflessioni, quelle rispetto a una retta che passa per due vertici opposti, e che dunque hanno due punti fissi, e quelle rispetto a una retta che biseca due lati opposti, e queste non hanno punti fissi. Del primo tipo sono le $f_{-1,b}$ con b pari, dato che l'equazione (2.5.1) ha soluzioni $b/2$ e $(b + n)/2$. Per esempio la riflessione $f_{-1,0}$ fissa 0 e $3 = -3$. Del secondo tipo sono le $f_{-1,b}$ con b dispari, dato che l'equazione (2.5.1) non ha soluzioni, perchè implicherebbe negli interi

$$2x = b + kn$$

per qualche k, il che non è possibile per b dispari e n pari.

Notate che la composizione di due riflessioni è una rotazione, infatti

$$f_{-1,b} \circ f_{-1,c} = f_{1,c-b}.$$

In particolare

$$f_{-1,0} \circ f_{-1,1} = f_{1,1}. \tag{2.5.2}$$

Notate che i due elementi di sinistra hanno periodo 2, mentre quello di destra ha periodo n. Questo mostra come D_n sia non commutativo, altrimenti per due elementi u, v di periodo 2 avrei $(uv)^2 = uvuv = uuvv = u^2v^2 = 1$. In effetti

$$f_{-1,1} \circ f_{1,0} = f_{1,1} \neq f_{1,-1} = f_{1,0} \circ f_{-1,1}$$

perché $n > 2$.

Una conseguenza di (2.5.2) è che un ciclo $(12 \dots n)$, con $n > 2$, si può scrivere come prodotto di due involuzioni (cioè elementi di ordine 2). Infatti scrivendo tutti gli elementi di D_n come permutazioni di $A = \mathbf{Z}/n\mathbf{Z}$, si ha

$$f_{1,1} = (01 \dots n-1) = f_{-1,0} \circ f_{-1,1}$$

che è eguale a (ho indicato per chiarezza anche gli 1-cicli, cioè i punti fissi)

$$(0)(1, n-1)(2, n-2) \cdots (n/2-1, n/2+1)(n/2) \circ \\ \circ (01)(2, n-1)(3, n-2) \cdots (n/2, n/2+1)$$

se n è pari, e a

$$(0)(1, n-1)(2, n-2) \cdots ((n-1)/2, (n+1)/2) \circ \\ \circ (01)(2, n-1)(3, n-2) \cdots ((n-1)/2, (n+1)/2+1)((n+1)/2)$$

se n è dispari.

2.6. Sottogruppo generato da un sottoinsieme

Sia G un gruppo, e S un suo sottoinsieme.

2.6.1. Definizione. Si dice *sottogruppo di G generato da S*, in simboli $\langle S \rangle$, il più piccolo sottogruppo di G che contenga S.

Naturalmente dalla definizione non segue l'esistenza. Si vede che in effetti il sottogruppo di G generato da S esiste, ed è l'intersezione di tutti i sottogruppi di G che contengano S:

$$\langle S \rangle = \bigcap \{ H \leq G : S \subseteq H \}.$$

Si usa

2.6.2. Lemma. *L'intersezione di una famiglia qualsiasi di sottogruppi è un sottogruppo.*

Invece si può vedere

2.6.3. Esercizio. *L'unione di due sottogruppi è un sottogruppo se e solo se uno dei due contiene l'altro.*

Notate il seguente semplice ma importante fatto, che deriva direttamente dalla definizione.

2.6.4. Lemma. *Sia G un gruppo, $H \leq G$, e $S \subseteq G$.*
Sono equivalenti

- *$S \subseteq H$, e*
- *$\langle S \rangle \leq H$.*

Torna spesso utile il seguente risultato.

2.6.5. Lemma. *Siano G, H gruppi, $S \subseteq G$, e $f : G \to H$ un morfismo.*
Allora

$$f(\langle S \rangle) = \langle f(S) \rangle.$$

Ricordate che se $f : G \to H$ è una funzione, e $T \subseteq H$, allora $f^{-1}(T) = \{ x \in G : f(x) \in T \}$. Dunque per $S \subseteq G$ sono equivalenti $S \subseteq f^{-1}(T)$ e $f(S) \subseteq T$.

Dimostrazione. Dato che $S \subseteq \langle S \rangle$ si ha anche $f(S) \subseteq f(\langle S \rangle)$ e dunque $\langle f(S) \rangle \subseteq f(\langle S \rangle)$, dato che quest'ultimo è un sottogruppo di H.

Poi da $f(S) \subseteq \langle f(S) \rangle$ segue $S \subseteq f^{-1}(f(S)) \subseteq f^{-1}(\langle f(S) \rangle)$, e dato che quest'ultimo è un sottogruppo di G segue $\langle S \rangle \subseteq f^{-1}(\langle f(S) \rangle)$, da cui

$$f(\langle S \rangle) \subseteq f(f^{-1}(\langle f(S) \rangle)) = \langle f(S) \rangle,$$

dato che $\langle f(S) \rangle \leq f(G)$ poiché $f(S) \subseteq f(G)$. □

Se $S = \{ g_1, \ldots, g_n \}$, si scrive $\langle g_1, \ldots, g_n \rangle$ invece di $\langle \{ g_1, \ldots, g_n \} \rangle$. In generale su come è fatto $\langle S \rangle$ non si può dire molto di più di

$$\langle S \rangle = \{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} : k \in \mathbf{N}, x_i \in S, \varepsilon_i \in \{ +1, -1 \} \}.$$

Se il gruppo è abeliano, allora si può dire più semplicemente

$$\langle g_1, \ldots, g_n \rangle = \{ g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_n^{\alpha_k} : \alpha_i \in \mathbf{Z} \}.$$

Il caso particolare quando $S = \{ g \}$ consiste di un solo elemento si può invece descrivere completamente il *gruppo ciclico* $G = \langle g \rangle$.

Consideriamo il morfismo suriettivo

$$\begin{aligned} \varphi : \mathbf{Z} &\to \langle g \rangle \\ n &\mapsto g^n. \end{aligned}$$

Se $\ker(\varphi) = \{ 0 \}$, allora φ è anche iniettivo, e dunque un isomorfismo. Se invece $\ker(\varphi) = n\mathbf{Z}$, con $n > 0$, allora si ottiene dal Primo Teorema di Isomorfismo, l'isomorfismo

$$\begin{aligned} \psi : \mathbf{Z}/n\mathbf{Z} &\to \langle g \rangle \\ [n] &\mapsto g^n. \end{aligned}$$

Dunque un gruppo ciclico è isomorfo a $\mathbf{Z}$ o a $\mathbf{Z}/n\mathbf{Z}$.

Abbiamo usato il

2.6.6. Lemma. *Siano G, H gruppi, $\varphi : G \to H$ un morfismo.*
Sono equivalenti

(1) φ è una funzione iniettiva, e
(2) $\ker(\varphi) = \{ 1 \}$.

Usando il Teorema di Corrispondenza, e quello che sappiamo sui sottogruppi di $\mathbf{Z}$ si può anche verificare che

2.6.7. Proposizione. *Un gruppo ciclico G di ordine n ha uno e un solo sottogruppo di ordine m, per ogni divisore m di n.*
Se $G = \langle a \rangle$, il sottogruppo di ordine m è $\left\langle a^{n/m} \right\rangle$.

Ricordiamo anche

2.6.8. Lemma. *Sia a un elemento di ordine finito di un gruppo. Sia $m \in \mathbf{Z}$. Allora l'ordine di a^m è*

$$\frac{|\, a \,|}{\gcd(|\, a \,|, m)}.$$

2.7. Il prodotto di due sottogruppi

In generale, se $H, K \leq G$, non è detto che il prodotto

$$HK = \{ hk : h \in H, k \in K \}$$

sia anch'esso un sottogruppo di G, come si vede considerando i sottogruppi

$$H = \{ 1, (12) \}, \quad K = \{ 1, (13) \}$$

di S_3. Vale

2.7.1. Lemma. *Sia G in gruppo qualsiasi, e $H, K \leq G$. Il* sottoinsieme *HK è unione di classi laterali sinistre di K.*

(1) C'è una corrispondenza biunivoca fra
  (a) L'insieme delle classi laterali di K in HK, e
  (b) l'insieme delle classi laterali di $H \cap K$ in H.

(2) Se gli insiemi di classi laterali del punto precedente sono finiti, si ha dunque

$$|\, HK : K \,| = |\, H : H \cap K \,|\,.$$

(3) Se poi G è finito, si ha

$$\frac{|\, HK \,|}{|\, K \,|} = \frac{|\, H \,|}{|\, H \cap K \,|}$$

Questo aiuterebbe a mostrare senza calcoli l'esempio precedente, visto che per il Teorema di Lagrange S_3, che ha ordine 6, non può avere sottogruppi di ordine 4.

Dimostrazione. Sia

$$\mathcal{S} = \{\, hkK : h \in H, k \in K \,\} = \{\, hK : h \in H \,\}\,,$$

l'insieme delle classi laterali di K in HK (quest'ultimo non è sempre un sottogruppo, ma è comunque unione di classi laterali di K), e

$$\mathcal{T} = \{\, h(H \cap K) : h \in H \,\}$$

l'insieme delle classi laterali di $H \cap K$ in H.

La funzione $H \to \mathcal{S}$ che manda h in hK è suriettiva, e la relazione di equivalenza associata è $h_1 R h_2$ se e solo se $h_1 K = h_2 K$, ovvero $h_1^{-1} h_2 \in H \cap K$, che è proprio la relazione che definisce le classi laterali di $H \cap K$ in H, dunque dal Primo Teorema di Isomorfismo di Insiemi si ottiene la biiezione richiesta $\mathcal{T} \to \mathcal{S}$. □

Dunque in generale, se $H, K \leq G$, si ha $HK \neq \langle\, H, K \,\rangle$. Vale però l'importante fatto, già parte del secondo teorema di isomorfismo:

2.7.2. Lemma. *Se $H \leq G$, $K \trianglelefteq G$, allora $HK \leq G$.*

Dimostrazione. Se $h_1, h_2 \in H$, $k_1, k_2 \in K$, allora

$$h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 h_2^{-1} h_2 k_1 k_2^{-1} h_2^{-1} \in HK,$$

dato che $h_2 (k_1 k_2^{-1}) h_2^{-1} \in K$. □

Il risultato si estende facilmente a mostrare che se $H_1, \ldots, H_n$ sono sottogruppi normali di un gruppo G, allora il prodotto $H_1 H_2 \ldots H_n$ è un sottogruppo di G. Da notare anche il seguente risultato

2.7.3. Proposizione. *Sia H un gruppo, $H, K \leq G$. Allora sono equivalenti*

(1) HK è un sottogruppo di G, e
(2) $HK = KH$.

Notate che HK può essere un sottogruppo anche se nessuno dei due sottogruppi è normale. Un esempio ragionevolmente piccolo è quello di S_4, con i sottogruppi $H = \langle\, (12) \,\rangle, K = \langle\, (34) \,\rangle$. Ma questo in un certo senso non vale, perché $H, K \trianglelefteq \langle\, (12), (34) \,\rangle$. Un esempio migliore, sempre in S_4, è dato da $H = \langle\, (123) \,\rangle$ di ordine 3 e $K = \langle\, (1234), (13) \,\rangle$ di ordine 8 (il gruppo delle congruenze del quadrato). Allora per il Lemma 2.7.1 si ha $HK = S_4$.

Premettiamo il

2.7.4. Lemma. *Sono equivalenti*

(1) $KH \subseteq HK$, *e*
(2) $HK \leq G$.

Dimostrazione del Lemma. Se $KH \subseteq HK$, e $h_i \in H$, $k_i \in K$, allora

$$(h_1k_1)^{-1} \cdot h_2k_2 = k_1^{-1}h_1^{-1}h_2k_2 \in KHK \subseteq HKK = HK$$

Viceversa, se $HK \leq G$, allora $K, H \leq HK$, e dunque $KH \subseteq HK$. □

Dimostrazione della Proposizione. Basta ora da vedere che se $HK \leq G$, allora $HK \subseteq KH$. Sia $x \in HK$. Allora $x^{-1} \in HK$, dunque $x^{-1} = hk$ per qualche $h \in H$ e $k \in K$. Dunque $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$. □

2.8. Prodotti di un numero finito di fattori

Cominciamo con il caso di due gruppi G_1, G_2. Il prodotto cartesiano

$$G_1 \times G_2 = \{\, (g_1, g_2) : g_i \in G_i \,\}$$

diventa un gruppo, che chiamiamo *prodotto esterno* dei due gruppi, con le operazioni per componenti

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2).$$

Consideriamo i sottoinsiemi

$$G_1' = \{\, (g_1, 1) : g_1 \in G_1 \,\}, \qquad G_2' = \{\, (1, g_2) : g_2 \in G_2 \,\}$$

di $P = G_1 \times G_2$. Si ha ovviamente $G_i \cong G_i'$, ove "$\cong$" è il simbolo per l'isomorfismo. Essi godono delle seguenti proprietà.

(1) $G_i' \trianglelefteq P$,
(2) $G_1' \cap G_2' = \{\, 1 \,\}$,
(3) $\langle\, G_1', G_2' \,\rangle = P$.

Da queste proprietà segue che ogni elemento di P si scrive in modo unico come x_1x_2, per $x_i \in G_i'$.

Notiamo il

2.8.1. Lemma. *Sia P un gruppo e X_1, X_2 tali che*

(1) $X_i' \trianglelefteq P$,
(2) $X_1 \cap X_2 = \{\, 1 \,\}$

Allora $x_1x_2 = x_2x_1$ per $x_i \in X_i$. Si dice che X_1 e X_2 commutano elemento per elemento.

Introduciamo un oggetto che ci sarà utile, il *commutatore*

$$[x, y] = x^{-1}y^{-1}xy.$$

Notate che $xy = yx[x, y]$, dunque $xy = yx$ se e solo se $[x, y] = 1$, da cui il nome. E' comodo introdurre anche la notazione del *coniugato* $a^b = b^{-1}ab$. Notate che $[x, y] = x^{-1}x^y = (y^{-1})^x y$.

DIMOSTRAZIONE. Se $x_i \in G_i'$ il commutatore

$$[x_1, x_2] = x_1^{-1} x_1^{x_2} = (x_2^{-1})^{x_1} x_2$$

sta sia in X_1 che in X_2, dato che ognuno dei due è normale, dunque $[x_1, x_2] = 1$. □

Sia ora G un gruppo che contiene due sottogruppi G_1, G_2 tali che

(1) $G_i \trianglelefteq P$,
(2) $G_1 \cap G_2 = \{ 1 \}$, e
(3) $G = \langle G_1, G_2 \rangle$.

Allora G si dice *prodotto interno* dei G_i. Come sopra si ha che G_1, G_2 commutano elemento per elemento, e che $G = G_1 G_2$. Si vede (esercizio!) che ogni elemento di G si scrive *in modo unico* nella forma $g_1 g_2$, per $g_i \in G_i$.

2.8.2. TEOREMA. *Sia G prodotto interno dei sottogruppi G_1, G_2. Allora la funzione*

$$\begin{aligned} \varphi : G_1 \times G_2 &\to G \\ (g_1, g_2) &\mapsto g_1 g_2 \end{aligned}$$

è un isomorfismo di gruppi.

Dunque prodotto esterno o interno sono di fatto "la stessa cosa". O in altre parole, se un gruppo è prodotto interno di G_1, G_2, la sua struttura è determinata solo da G_1 e G_2, senza alcuna altra informazione.

DIMOSTRAZIONE. Provate a farla, in caso chiedete o guardate su un libro. □

Passiamo ora al caso di un numero finito di fattori $G_1, \ldots, G_n$. Se il gruppo G contiene i sottogruppi G_i, e si ha che

(1) $G_i \trianglelefteq P$,
(2) per ogni i vale $G_i \cap G_1 G_2 \ldots G_{i-1} G_{i+1} \ldots G_n = \{ 1 \}$, e
(3) $G = \langle G_i : i = 1, 2, \ldots, n \rangle$

allora vale anche $G = G_1 G_2 \ldots G_n$. In questo caso G si dice *prodotto interno* dei G_i. Si ha

2.8.3. TEOREMA. *Sia G prodotto interno dei sottogruppi $G_1, \ldots, G_n$. Allora la funzione*

$$\begin{aligned} \varphi : G_1 \times G_2 \times \ldots G_n &\to G \\ (g_1, g_2, \ldots, g_n) &\mapsto g_1 g_2 \ldots g_n \end{aligned}$$

è un isomorfismo di gruppi.

2.9. Il teorema di Goursat

Viene da [**Gou89**].

Sia $G = G_1 \times G_2$. Vogliamo determinare i sottogruppi di G. Notate che se $\pi_i : G \to G_i$ sono le proiezioni, e $H_i = \pi_i(H)$, allora $H \leq H_1 \times H_2$. Dunque possiamo limitarci al caso in cui $G_i = \pi_i(H)$, per $i = 1, 2$, e dunque $G = HG_2 = G_1 H$.

Poniamo $N_i = H \cap G_i$, per $i = 1, 2$. Notate che $N_1 \trianglelefteq H$ dato che $G_1 \trianglelefteq G$, inoltre G_2 centralizza G_1 e quindi N_1. Ne segue che $N_i \trianglelefteq G$, per $i = 1, 2$.

Da $G = HG_2$ segue che per ogni $x_1 \in G_1$, esiste $x_2 \in G_2$ tale che $(x_1, x_2) \in H$. Se anche $(x_1, x_2') \in H$, allora $x_2^{-1}x_2' \in H \cap G_2 = N_2$. Dunque la funzione $G_1 \to G_2/N_2$ data da $x_1 \to x_2G_2$ è ben definita, ed è un morfismo di gruppi, dato che se $(x_1, x_2), (y_1, y_2) \in H$, allora $(x_1y_1, x_2y_2) \in H$. La sua immagine è tutto G_2/N_2, perché da $G = G_1H$ segue simmetricamente che per ogni $x_2 \in G_2$ esiste $x_1 \in G_1$ tale che $(x_1, x_2) \in H$. Il suo nucleo è dato da

$$\{\, x_1 \in G_1 : x_1x_2 \in H, x_2 \in H \cap G_2 \,\} \leq H \cap G_1 = N_1,$$

e viceversa se $x_1 \in H \cap G_1$, e $x_1x_2 \in H$, allora $x_2 \in H \cap G_2 = N_2$. Ora abbiamo

$$H = \{\, (x_1, x_2) : \varphi(x_1N_1) = x_2N_2 \,\}. \tag{2.9.1}$$

L'eguaglianza deriva dal fatto che abbiamo proprio *definito* $\varphi(x_1N_1) = x_2N_2$ se $(x_1, x_2) \in H$.

Resta da notare che il termine di sinistra di (2.9.1) è sempre un sottogruppo.

Abbiamo dimostrato il seguente

2.9.1. Teorema (Goursat). *Sia $G = G_1 \times G_2$,e $H \leq G$ tale che $\pi_i(H) = G_i$, per $i = 1, 2$.*

Allora esistono $N_i \trianglelefteq G_i$ e un isomorfismo $\varphi : G_1/N_1 \to G_2/N_2$ tale che

$$H = \{\, (x_1, x_2) : \varphi(x_1N_1) = x_2N_2 \,\}.$$

Vieversa, ogni H di questa forma è un sottogruppo di G tale che $\pi_i(H) = G_i$, per $i = 1, 2$.

2.10. Parentesi: prodotti semidiretti

Se $G = \langle\, H, N \,\rangle$ è un gruppo, $H, N \leq G$, con $N \cap G = \{\, 1 \,\}$ ma solo $N \trianglelefteq G$, allora per determinare la struttura di G non basta solo conoscere la struttura di H e N, ma anche qualcosa d'altro. Cosa sia si capisce dal fatto che per moltiplicare due elementi devo fare

$$h_1n_1h_2n_2 = h_1h_2n_1^{h_1}n_2,$$

e dunque devo conoscere, per ogni $h \in H$, la funzione $N \to N$ data da $n \mapsto n^h$. Ora si vede che

(1) ognuna di queste funzioni è un *automorfismo* di H (cioè un isomorfismo $H \to H$),
(2) gli automorfismi di un gruppo formano sempre un gruppo rispetto alla composizione, in questo caso $\mathrm{Aut}(H)$,
(3) la funzione

$$\begin{aligned} H &\to \mathrm{Aut}(N) \\ h &\mapsto (n \mapsto n^h) \end{aligned}$$

è un morfismo di gruppi.

Si potrebbe vedere (lo facciamo più avanti) che quest'ultimo dato permette di ricostruire completamente la struttura di G.

2.11. Gruppi abeliani finiti

Ricordiamo di nuovo il

2.11.1. Lemma. *Sia g un elemento di ordine n di un gruppo. Allora l'ordine di g^k è*

$$\frac{n}{\gcd(n,k)}.$$

2.11.2. Lemma. *Sia G un gruppo, e $g \in G$ di ordine finito n.*
Sia $n = ab$, con $\gcd(a,b) = 1$. Allora esistono due potenze h, k di G, di ordine rispettivamente a e b, tali che $g = hk$.

Dimostrazione. Esistono $x, y \in \mathbf{Z}$ tali che $ax + by = 1$. In particolare

$$\gcd(a,y) = 1 = \gcd(b,x).$$

Siano $h = g^{by}$, $k = g^{ax}$, sicché $g = g^1 = g^{ax+by} = g^{ax}g^{by} = kh = hk$. Per il Lemma 2.11.1, abbiamo dapprima

$$|\, g^a \,| = \frac{n}{\gcd(n,a)} = \frac{n}{a} = b,$$

e dunque $|\, k \,| = |\, (g^a)^x \,| = b$, e similmente $|\, h \,| = a$. □

2.11.3. Corollario. *Ogni elemento di ordine finito*

$$n = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l},$$

con i p_i primi distinti, è il prodotto di elementi di ordini $p_i^{e_i}$.

Sia ora G un gruppo abeliano di ordine finito

$$|\, G \,| = p_1^{t_1} p_2^{t_2} \dots p_l^{t_l},$$

con i p_i primi distinti. Consideriamo i suoi sottogruppi (*di Sylow*, si veda il Capitolo 6)

$$P_i = \left\{ x \in G : x^{p_i^{t_i}} = 1 \right\}. \tag{2.11.1}$$

Nella sezione 5.4 (ma si veda anche l'Osservazione 6.2.2), vedremo il seguente

2.11.4. Lemma (Cauchy). *Sia G un gruppo finito, e p un numero primo che ne divide l'ordine. Allora G contiene un elemento di ordine p.*

Diamone qui una dimostrazione per il solo caso che per ora ci interessa dei *gruppi abeliani finiti*.

Dimostrazione. Sia G un gruppo abeliano finito, di ordine divisibile per il primo p. Sia $1 \neq a \in G$. Se $p \mid |\, a \,|$, e dunque $|\, a \,| = pn$ per qualche n, allora $|\, a^n \,| = p$. Altrimenti, sia $q \neq p$ un primo che divide $|\, a \,|$, per cui $|\, a \,| = qn$ per qualche n, sicché $b = a^n$ ha periodo q. Poniamo $B = \langle\, b \,\rangle$; procedendo per induzione, in G/B c'è un elemento cB di periodo p. Sia $m = |\, c \,|$ l'ordine di c in G. Se consideriamo il morfismo canonico $\pi : G \to G/B$ tale che $\pi(x) = xB$, allora abbiamo

$$1 = \pi(1) = \pi(c^m) = \pi(c)^m = (cB)^m.$$

Dunque l'ordine p di cB in G/B divide m, e siamo nel caso precedente. □

2.11.5. Esercizio. *Nella precedente dimostrazione abbiamo in pratica mostrato che se G, H sono gruppi, se $f : G \to H$ è un morfismo, e se $g \in G$ ha periodo finito m, allora il periodo di $f(g)$ divide m.*

Se ne deduce che P_i ha ordine una potenza di p_i. Ora un elemento $g \in G$ ha ordine che divide $|\, G \,|$. Dunque per il risultati precedenti si scrive come prodotto di elementi g_i di ordini $p_i^{s_i}$, con $s_i \leq t_i$. Ne segue che $g_i^{p^{t_i}} = 1$, cioè $g_i \in P_i$, e dunque ogni elemento di G si scrive come prodotto di elementi dei P_i. Inoltre questa scrittura è *unica*. Infatti se

$$g = h_1 h_2 \dots h_l = k_1 k_2 \dots k_l,$$

con $h_i, k_i \in P_i$, si ha

$$h_1^{-1} k_1 = h_2 \dots h_l k_2 \dots k_l.$$

Ora il primo elemento ha ordine un divisore di $p_1^{t_1}$, il secondo un divisore di $p_2^{t_2} \dots p_l^{t_l}$, Dato che questi due numeri sono coprimi avrò

$$h_1 = k_1, \qquad h_2 \dots h_l = k_2 \dots k_l.$$

Ora si può procedere per induzione, o semplicemente scrivere lo stesso argomento con un generico p_i al posto di p_1.

Ne segue che

$$|\, P \,| = \prod_{i=1}^{l} |\, P_i \,|,$$

e dunque per la fattorizzazione unica in $\mathbf{Z}$ si ha $|\, P_i \,| = p_i^{t_i}$ per ogni i.

Fissiamo un numero primo p. Un gruppo (finito o infinito) in cui ogni elemento ha ordine una potenza di p si dice un p-gruppo. Per il Lemma di Cauchy, un gruppo finito è un p-gruppo se e solo se ha ordine una potenza di p. Un esempio di un p-gruppo infinito è dato da uno spazio vettoriale di dimensione infinita sul campo F_p, dato che ogni elemento, a parte lo zero, ha periodo (additivo) p. Vedremo un altro esempio, naturale e importante, nella sezione 2.13.

Notiamo intanto che dato che G è finito, è anche finito l'insieme $\{\, |\, x \,| : x \in G \,\}$ degli ordini degli elementi di G. Da qui segue l'esistenza di un elemento di ordine massimo.

2.11.6. Lemma. *Sia G un p-gruppo abeliano finito.*
Sia $a \in G$ un elemento di ordine massimo in G.
Allora esiste un sottogruppo $B \leq G$ tale che $G = \langle\, a \,\rangle \times B$.

2.11.7. Proposizione. *Un p-gruppo abeliano finito è prodotto diretto di gruppi ciclici.*

La proposizione seguirà dal Lemma per induzione sull'ordine del gruppo.

Dimostrazione del Lemma. Procediamo per induzione sull'ordine del gruppo.

Se G ha ordine 1, non c'è molto da dire. Sia dunque $G \neq \{\, 1 \,\}$, e sia $1 \neq a \in G$ un elemento di ordine massimo p^n.

Naturalmente se $G = \langle\, a \,\rangle$ basta prendere $B = 1$. Sia dunque $G \neq A = \langle\, a \,\rangle$.

Sia $x \in G \setminus A$. Sia p^k il periodo di xA in G/A. Dato che $xA \neq A$, sarà $k \geq 1$.

Abbiamo $x^{p^k} \in A$, mentre $x^{p^{k-1}} \notin A$. In particolare $p^k \mid |\, x \,|$, per l'Esercizio 2.11.5.

Sarà $x^{p^k} = a^{ip^t}$, per qualche i con $\gcd(i,p) = 1$, e qualche $t \leq n$ (dato che posso prendere $0 < ip^t \leq p^n = |\, a \,|$).

Abbiamo da un lato $\left|\, x^{p^k} \,\right| = |\, x \,| / p^k$, e dall'altro dapprima

$$\left|\, a^{p^t} \,\right| = \frac{|\, a \,|}{\gcd(|\, a \,|, p^t)} = \frac{|\, a \,|}{p^t} = p^{n-t},$$

e poi

$$\left|\, (a^{p^t})^i \,\right| = \frac{\left|\, a^{p^t} \,\right|}{\gcd(|\, a^{p^t} \,|, i)} = \left|\, a^{p^t} \,\right|,$$

dato che $\left|\, a^{p^t} \,\right| = p^{n-t}$, e $p \nmid i$, e dunque $\gcd(\left|\, a^{p^t} \,\right|, i) = 1$.

Dunque

$$\frac{|\, x \,|}{p^k} = \left|\, x^{p^k} \,\right| = \left|\, a^{ip^t} \,\right| = \left|\, a^{p^t} \,\right| = \frac{|\, a \,|}{p^t},$$

ovvero $p^t \cdot |\, x \,| = p^k \cdot |\, a \,|$. Dato che $|\, a \,| \geq |\, x \,|$ sarà $t \geq k \geq 1$.

Dato che $t \geq k \geq 1$, possiamo considerare $z = x^{p^{k-1}} a^{ip^{t-1}}$. Si ha $z^p = 1$, e $z \notin A$, altrimenti $x^{p^{k-1}} \in A$, contro l'ipotesi. Dunque $z \neq 1$ ha ordine p, e quindi $Z = \langle\, z \,\rangle \not\leq A$ implica $Z \cap A = 1$.

Affermo che $aZ \in G/Z$ ha lo stesso ordine p^n di a in G. Infatti se fosse $(aZ)^{p^{n-1}} = Z$, allora $a^{p^{n-1}} \in A \cap Z$ dovrebbe essere 1, contro $|\, a \,| = p^n$.

Per induzione, esiste B, con $Z \leq B \leq G$, tale che $G/Z = \langle\, aZ \,\rangle \times B/Z$. Affermo che $G = A \times B$.

Se $g \in G$, allora $gZ = (a^i Z)(bZ)$ per qualche i e $b \in B$. Ma allora $g \in a^i BZ = a^i B \subseteq AB$. Si ha poi $\langle\, aZ \,\rangle \cap B/Z = Z$. Se allora $g \in A \cap B$, allora $g = a^i \in B$, dunque $a^i Z \in B/Z$, dunque $a^i Z = Z$ e $a^i \in Z$, sicché $a^i = 1$. □

2.12. p-gruppi abeliani finiti e partizioni

Abbiamo appena visto che per un p-gruppo abeliano finito P di ordine $p^n > 1$ si ha

$$P \cong P_1 \times \cdots \times P_l,$$

con P_i ciclico, di ordine $p^{e_i} > 1$, e dunque

$$e_1 + \cdots + e_l = n.$$

Dato che per i prodotti diretti vale $G_1 \times G_2 \cong G_2 \times G_1$, possiamo permutare i P_i e supporre $e_1 \geq e_2 \geq \cdots \geq e_l > 0$. Dunque

$$(e_1, e_2, \ldots, e_l)$$

è una *partizione* di n. Vogliamo vedere che questa partizione è univocamente determinata da P, dunque che se

$$P_1 \times \cdots \times P_l \cong Q_1 \times \cdots \times Q_m,$$

con P_i, Q_i ciclici, $|\,P_i\,| = p^{e_i}$, $|\,Q_i\,| = p^{f_i}$, $e_1 \geq e_2 \geq \cdots \geq e_l > 0$, $f_1 \geq f_2 \geq \cdots \geq f_m > 0$, allora $l = m$ e $e_i = f_i$ per ogni i.

Sia $e = (e_1, e_2, \ldots, e_l)$ una partizione di n. Ad essa associamo l'insieme dei punti a coordinate intere del piano

$$E = \{\, (i,j) : 1 \leq j \leq e_i \,\}.$$

Dunque E consiste di n punti *positivi* (cioè con entrambe le coordinate intere e positive), con un segmento verticale

$$(i,1), (i,2), \ldots, (i,e_i)$$

per ogni $1 \leq i \leq l$.

2.12.1. Lemma. *Un insieme associato E a una partizione e gode delle seguenti proprietà:*

(1) se $(i,j) \in E$, allora $(i,1), (i,2), \ldots, (i,j) \in E$, ovvero $(i,k) \in E$ per $1 \leq k \leq j$;

(2) se $(i,j) \in E$, allora $(1,j), (2,j), \ldots, (i,j) \in E$, ovvero $(k,j) \in E$ per $1 \leq k \leq i$.

(3) se $(i,j) \in E$, allora è in E tutto il rettangolo di punti positivi di vertici $(i,j), (i,1), (1,1), (1,j)$, ossia tutti i punti (h,k) con $1 \leq h \leq i$ e $1 \leq k \leq j$.

Notate come (1) dica che se in E c'è un punto, allora ci sono tutti quelli positivi sotto di esso, mentre (2) dice che ci sono tutti quelli positivi alla sua sinistra.

Notate inoltre come i punti (1) e (2) presi insieme siano equivalenti al punto (3).

Dimostrazione.

(1) Se $(i,j) \in E$, allora per la definizione di E si ha $1 \leq j \leq e_i$. Dunque per $1 \leq k \leq j$ si ha $1 \leq k \leq j \leq e_i$, e dunque anche $(i,k) \in E$.

(2) Se $(i,j) \in E$, allora $1 \leq j \leq e_i$. Se $1 \leq k \leq i$, allora per definizione di partizione si ha $e_i \leq e_k$, dunque $1 \leq j \leq e_i \leq e_k$, e dunque $(k,j) \in E$.

(3) segue dai due punti precedenti. □

2.12.2. Lemma. *Sia E un insieme di $n > 0$ punti positivi del piano che soddisfi le condizioni del Lemma* (2.12.1).

Allora E è associato a una partizione e di n.

Dimostrazione. Sia $l = \max\{\, i : \text{esiste } j \text{ tale che } (i,j) \in E \,\}$. Per la proprietà (1), si ha $(l,1) \in E$. Per la proprietà (2) si ha $(1,1), (2,1), \ldots, (l,1) \in E$. Per ogni $1 \leq i \leq l$, possiamo dunque definire $e_i = \max\{\, j : (i,j) \in E \,\}$, dato che questo insieme non è vuoto.

Per la proprietà (1), E consiste di segmenti verticali $(i,1), (i,2), \ldots, (i,e_i)$.

Sia $i \leq i+1 \leq l$. Si ha $(i+1, e_{i+1}) \in E$, dunque per la proprietà (2) $(i, e_{i+1}) \in E$, da cui, per definizione di e_i, si ha $e_{i+1} \leq e_i$.

Dunque $e = (e_1, \ldots, e_l)$ è una partizione di n. □

Dato adesso un insieme E di punti positivi che soddisfi le condizioni del Lemma (2.12.1), notiamo che anche l'insieme *trasposto*

$$E^\star = \{\, (i,j) : (j,i) \in E \,\}$$

le soddisfa — è sufficiente considerare la condizione (3) . Dunque $E^\star$ è associato a una partizione $e^\star$, detta la *partizione duale* di e.

Se ad esempio $e = (3,3,2,1)$, allora $e^\star = (4,3,2)$. In altra parole $e^\star$ ha e_1 elementi, e

$$e_k^\star = |\{ i : e_i \geq k \}|.$$

In particolare $e_1^\star = l$, il numero di elementi di e.

Si può notare come $(e^\star)^\star = e$.

2.12.3. Proposizione. *Un p-gruppo abeliano finito di ordine p^n determina univocamente una partizione.*

Breve cenno di dimostrazione. Si può vedere che se a P è associata la partizione e, allora la partizione *duale* è determinata da

$$p^{e_1^\star + \cdots + e_i^\star} = \left| \left\{ x \in P : x^{p^i} = 1 \right\} \right|,$$

per $1 \leq i \leq l$. □

2.13. Il gruppo di Prüfer

(In fondo a questa sezione ho quasi scritto l'analogo della sezione precedente per il sottogruppo di torsione di $\mathbf{C}^\star$.)

Consideriamo il gruppo moltiplicativo $(\mathbf{C}, \cdot, 1)$ dei numeri complessi non nulli. Fissiamo un numero primo p. Consideriamo l'insieme di tutte le radici p^k-sime dell'unità, per qualche $k \geq 0$:

$$\mathbf{Z}(p^\infty) = \left\{ a \in \mathbf{C} : a^{p^k} = 1 \text{ per qualche } k \in \mathbf{N} \right\}. \tag{2.13.1}$$

Dalla relazione

$$e^{ix} = \cos(x) + i\sin(x)$$

sappiamo che le radici p^k dell'unità in $\mathbf{C}$ sono p^k, e sono date dalle potenze di

$$\omega_k = e^{\frac{2\pi i}{p^k}} = \cos(2\pi/p^k) + i\sin(2\pi/p^k).$$

Per $k > 0$ vale poi $\omega_k^p = (e^{\frac{2\pi i}{p^k}})^p = e^{\frac{2\pi i}{p^{k-1}}} = \omega_{k-1}$.

2.13.1. Teorema.

(1) $\mathbf{Z}(p^\infty) = \left\{ e^{\frac{2\pi i m}{p^k}} : k \in \mathbf{N}, 0 \leq m < p^k \right\}$.

(2) Ogni elemento di $\mathbf{Z}(p^\infty)$ *si scrive* in modo unico *nella forma* $e^{\frac{2\pi i m}{p^k}}$*, per qualche* $k \geq 0$*, e* $0 \leq m < p^k$ *tale che* $p \nmid m$.

(3) $\mathbf{Z}(p^\infty)$ *è infinito*

(4) $\mathbf{Z}(p^\infty)$ *non è un gruppo ciclico, ma*

(5) ogni suo sottogruppo proprio *(cioè diverso dall'intero gruppo) è ciclico, di ordine una potenza di* p.

Dimostrazione. Se $a \in \mathbf{Z}(p^\infty)$, si avrà $a^{p^k} = 1$ per qualche $k \in \mathbf{N}$. Dunque a ha ordine una potenza di p, diciamo sia proprio p^k.

Dunque $\langle a \rangle$ ha ordine p^k, e gli elementi di $\langle a \rangle$ sono radici del polinomio $x^{p^k} - 1$, dunque sono tutte le radici di questo polinomio. Ma lo stesso vale anche per $\langle \omega_k \rangle$,

dunque in particolare $a = \omega_k^m$ per qualche m, e deve essere $\gcd(m, p^k) = 1$, dato che $|\,\omega_k\,| = |\,a\,| = p^k$.

Questo è il punto (1). Per l'unicità, cioè il punto (2), se

$$\omega_h^m = \omega_k^n$$

con $p \nmid m, n$, allora $p^h = p^k$, dato che sono gli ordini dell'elemento di sinistra e di quello di destra, e poi $m = n$ dato che $0 \leq m, n < p^k$, e ω_k ha ordine p^k.

(3) è chiaro dai due punti precedenti.

Per vedere (4), notiamo che se $a \in \mathbf{Z}(p^\infty)$, allora $\langle\, a \,\rangle$ è un sottogruppo finito, dunque diverso da $\mathbf{Z}(p^\infty)$

Per l'ultimo punto, sia H un sottogruppo di $\mathbf{Z}(p^\infty)$. Scriviamo ogni elemento di H nella forma di (2). Consideriamo il sottoinsieme dei naturali

$$A = \left\{ k \in \mathbf{N} : e^{\frac{2\pi i m}{p^k}} \in H, \text{ per qualche } m, \text{ con } 0 \leq m < p^k \text{ e } p \nmid m \right\}.$$

Certamente $0 \in A$, perché $1 \in H$, dunque A non è vuoto. Se A *non* ha un massimo, allora è facile vedere (esercizio) che $H = Z(p^\infty)$. Se H ha un massimo k_0, allora si vede (esercizio) che $H = \left\langle\, \frac{2\pi i}{p^{k_0}} \,\right\rangle$ è ciclico di ordine p^{k_0}.

Forse un modo più semplice di dimostrare l'ultimo punto è il seguente. Sia $H \leq \mathbf{Z}(p^\infty)$. Sia $B = \{\, |\,a\,| : a \in H \,\} \subseteq \mathbf{N}$. Se B è finito, allora ha un massimo p^m, dunque c'è $a \in H$ tale che $|\,a\,| = p^m$, e tutti gli elementi di H hanno ordine un divisore di p^m, dunque sono una potenza di a, e $H = \langle\, a \,\rangle$. Se invece B è infinito, sia $z \in \mathbf{Z}(p^\infty)$ un elemento arbitrario, di periodo p^k, allora esiste $a \in H$ con periodo $p^m \geq p^k$, dunque z è una potenza di a, e $H = \mathbf{Z}(p^\infty)$. □

Consideriamo $T = \{\, a \in \mathbf{C}^* : a \text{ ha ordine finito} \,\}$. Dato che $\mathbf{C}^*$ è abeliano, si vede che $T \leq \mathbf{C}^*$. Se

$$|\,a\,| = p_1^{e_1} \cdots p_n^{e_n},$$

con i p_i primi distinti, e gli $e_i > 0$, allora per il Corollario 2.11.3 a è prodotto di elementi degli $\mathbf{Z}(p_i^\infty)$. Da questo segue (sto omettendo qualcosa) che T è coprodotto degli $\mathbf{Z}(p^\infty)$.

CAPITOLO 3

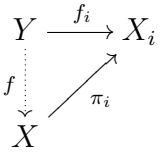
Prodotti e coprodotti

3.1. Definizioni

Siano $(X_i)_{i\in I}$ oggetti in una categoria $\mathcal{C}$. (Non parleremo tanto di categorie, ma ne faremo alcuni esempi noti.) Quel poco che so di categorie l'ho imparato sulle prime pagine di [**ML98**].

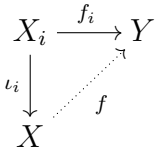
Sia Y un oggetto di $\mathcal{C}$.

3.1.1. Definizione. Un oggetto X si dice un *prodotto* di $(X_i)_{i\in I}$ se esistono morfismi $\pi_i : X \to X_i$ tali che se $f_i : Y \to X_i$ sono morfismi, allora esiste un unico morfismo $f : Y \to X$ che fa commutare il diagramma

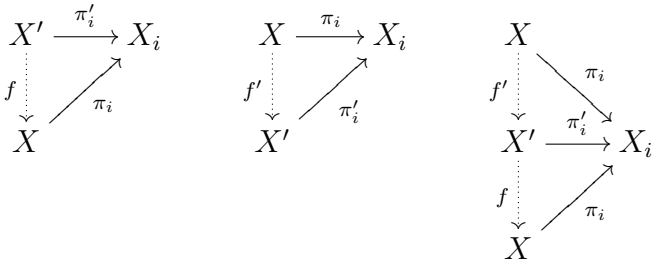


3.1.2. Definizione. Un oggetto X si dice un coprodotto $(X_i)_{i\in I}$ se esistono morfismi $\iota_i : X_i \to X$ tali che se $f_i : X_i \to Y$ sono morfismi, allora esiste un unico morfismo $f : X \to Y$ che fa commutare il diagramma

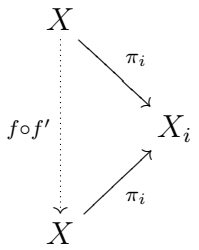
(3.1.1)



Prodotti e coprodotti, sempre se esistono in una particolare categoria, sono unici a meno di isomorfismi. Per esempio se X, X' sono due prodotti degli $(X_i)_{i\in I}$, con morfismi π_i, π'_i, allora ci sono morfismi f, f' che fanno commutare i due primi diagrammi (il terzo è solo la giustapposizione dei primi due)



Allora $f \circ f'$ (composizione da destra a sinistra) fa commutare



e siccome già l'identità fa commutare questo diagramma, l'unicità mostra che $f \circ f' = \mathbf{1}_X$, e allo stesso modo $f' \circ f = \mathbf{1}_{X'}$.

3.2. Esempi

Esemplifichiamo i concetti di cui sopra in alcune categorie, tendenzialmente senza dimostrazioni.

3.2.1. Insiemi. Nella categoria **Set** degli insiemi, ove i morfismi sono semplicemente le funzioni, il prodotto è il prodotto cartesiano $\prod_{i \in I} X_i$, mentre il coprodotto è l'unione disgiunta $\dot{\bigcup} X_i$. Spesso si usa il simbolo generale $\coprod_{i \in I} X_i$ per il coprodotto.

3.2.2. Spazi topologici. Nella categoria **Top** degli spazi topologici, dove i morfismi sono le funzioni continue, prodotto e coprodotto sono come per gli insiemi, con le opportune topologie, la topologia prodotto sul prodotto, quella naturale sull'unione disgiunta, cioè un sottoinsieme $A \subseteq \dot{\bigcup} X_i$ è aperto se e solo ogni $A \cap X_i$ è aperto in X_i.

3.2.3. Spazi vettoriali. Nella categoria **K-Vect** degli spazi vettoriali su un campo fissato K, dove i morfismi sono le funzioni lineari, il prodotto è sempre il prodotto cartesiano, mentre il coprodotto è quello che si chiama *somma diretta*

$$\coprod_{i \in I} X_i = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i : \text{l'insieme degli } i \text{ tali che } x_i \neq 0 \text{ è finito} \right\}.$$

3.2.4. Gruppi abeliani. La categoria **Ab** dei gruppi abeliani si comporta come quella degli spazi vettoriali.

3.2.5. Gruppi. Nella categoria **Grp** dei gruppi coi loro morfismi, il prodotto è sempre il prodotto cartesiano, mentre il coprodotto è il notevolmente più complicato *prodotto libero*, che potete vedere ad esempio in [**Rob96**]. I gruppi liberi che vedremo nel Capitolo 4 sono un caso particolare, quando gli X_i sono gruppi ciclici infiniti.

3.2.6. Una nota sui coprodotti. Nelle categorie sopra elencate, esiste il concetto di sottooggetto $\langle S \rangle$ generato da un sottoinsieme S di un oggetto X, definito come il più piccolo sottoogetto di X che contenga S.

Per **Ab** e **Grp**, $\langle S \rangle$ è il sottogruppo generato da S. Per **K-Vect**, $\langle S \rangle$ è il sottospazio generato da S. Per **Set** e **Top** si ha semplicemente $\langle S \rangle = S$.

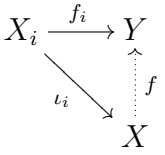
Notate che si scrive $\langle S_i : i \in I \rangle$ per denotare $\langle \bigcup_{i\in I} S_i \rangle$.

3.2.1. Proposizione. *Nelle categorie sopra elencate, si ha che*

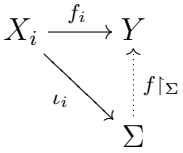
$$\coprod_{i\in I} X_i = \langle \iota_i(X_i) : i \in I \rangle .$$

Dimostrazione. Sia X il coprodotto, sia $\Sigma = \langle \iota_i(X_i) : i \in I \rangle$.

Chiaramente $\iota_i : X_i \to \Sigma$ è un morfismo. (A stretto rigore, dovrei usare un simbolo diverso per ι_i, dato che una funzione è determinata da dominio, *codominio* e un insieme di coppie, ma sorvoliamo per semplicità.) Se Y è un oggetto, $f_i : X_i \to Y$ sono morfismi, e $f : X \to Y$ è il morfismo che fa commutare il diagramma

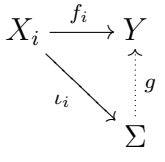


allora $f\restriction_\Sigma : \Sigma \to Y$ fa commutare il diagramma



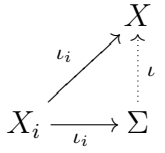
dato che per $x \in X_i$ si ha $f_i(x) = f(\iota_i(x)) = f\restriction_\Sigma(\iota_i(x))$.

Inoltre $f\restriction_\Sigma$ è unico. Infatti nelle categorie in oggetto si ha che un morfismo su $\langle Y_i : i \in I \rangle$ è determinato dalle sue restrizioni agli Y_i (per esempio in **Grp** perché un elemento di $\langle Y_i : i \in I \rangle$ è un prodotto di elementi degli Y_i), e se

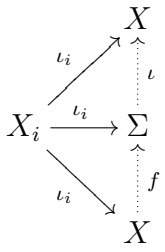


commuta, allora per ogni i e $x \in X_i$ si ha che $g(\iota_i(x)) = f_i(x)$ è univocamente determinato.

Dunque anche Σ è un coprodotto. Riprendendo la dimostrazione dell'unicità vista sopra (sopra è scritta per il prodotto, ma per il coprodotto è solo questione di rivoltare le frecce), avrò che se $\iota : \Sigma \to X$ è l'inclusione, allora questa fa commutare il diagramma



per cui ottengo un diagramma commutativo



da cui, per l'unicità, $\iota \circ f$ (la composizione è da destra a sinistra) è l'identità, dunque ι è suriettiva, cioè $X = \iota(\Sigma) = \Sigma$. □

CAPITOLO 4

Gruppi liberi

Sto ancora scrivendo questa parte, che è dunque al momento incompleta.

4.1. Gruppi liberi

4.1.1. Definizione. Sia F un gruppo, X un *insieme*, e $\iota : X \to F$ una funzione iniettiva.

Si dice che (F, ι) *è un gruppo libero con base* X (o gruppo libero su X) se per ogni gruppo G, e ogni *funzione* $f : X \to G$, esiste unico un morfismo $\varphi : F \to G$ che fa commutare il diagramma

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ \downarrow{\scriptstyle \iota} & \nearrow_{\varphi} & \\ F & & \end{array}$$

In altre parole, il morfismo φ è tale che $\varphi(\iota(x)) = f(x)$ per $x \in X$.

Naturalmente dobbiamo far vedere che i gruppi liberi esistono. Vediamo prima l'unicità a meno di isomorfismo.

4.1.2. Lemma. *Un gruppo libero su X, se esiste, è unico a meno di isomorfismi.*

Dimostrazione.

$$\begin{array}{ccc} X & \xrightarrow{\iota_1} & F_1 \\ \downarrow{\scriptstyle \iota_2} & \nearrow_{\varphi} & \\ F_2 & & \end{array}$$

Se (F_1, ι_1) e (F_2, ι_2) sono liberi su X, applichiamo la definizione per $F = F_1$, $G = F_2$, e $f(x) = \iota_2(x)$. Si ottiene un morfismo $\varphi : F_1 \to F_2$ tale che $\varphi(\iota_1(x))) = \iota_2(x)$ per $x \in X$. Scambiando i ruoli, si ottiene un morfismo $\psi : F_2 \to F_1$ tale che $\psi(\iota_2(x)) = \iota_1(x)$ per $x \in X$. Componendo, si ottieme un morfismo $\psi \circ \varphi : F_1 \to F_1$ tale che $\psi \circ \varphi(\iota_1(x)) = \iota_1(x)$ per $x \in X$. Dato che l'identità su F_1 fa la stessa cosa, per l'unicità del morfismo nella definizione di gruppo libero deve essere $\psi \circ \varphi = \mathbf{1}_{F_1}$, e allo stesso modo $\varphi \circ \psi = \mathbf{1}_{F_2}$, per cui φ e ψ sono isomorfismi. □

Dalla costruzione che faremo seguirà che per un gruppo libero (F, ι) si ha

4.1.3. Lemma. $F = \langle\, \iota(X) \,\rangle$.

Di questo diamo comunque una dimostrazione diretta.

DIMOSTRAZIONE. Sia $j : \langle\, \iota(X) \,\rangle \to F$ l'inclusione, e ι' è la funzione la funzione ovvia $X \to \langle\, \iota(X) \,\rangle$ tale che $\iota'(x) = \iota(x)$ per $x \in X$..

Dal diagramma

$$\begin{array}{ccc} X & \xrightarrow{\iota'} & \langle\, \iota(X) \,\rangle \\ & {\scriptstyle\iota}\searrow & \nearrow{\scriptstyle j} \\ & F & \\ & {\scriptstyle\varphi}\nwarrow & \end{array}$$

otteniamo un morfismo $\varphi : F \to \langle\, \iota(X) \,\rangle$ tale che $\varphi(\iota(x)) = \iota'(x) = \iota(x)$, per $x \in X$. Dunque $\varphi(F)$ è un sottogruppo di $\langle\, \iota(X) \,\rangle$ che contiene $\iota(X)$, e quindi $\varphi(F) = \langle\, \iota(X) \,\rangle$.

Dunque $j \circ \varphi(\iota(x)) = \varphi(\iota(x)) = \iota(x)$ per $x \in X$, dunque $j \circ \varphi = \mathbf{1}_F$ perché F è libero su X, e dunque $F = \mathbf{1}_F(F) = j(\varphi(F)) = j(\langle\, \iota(X) \,\rangle) = \langle\, \iota(X) \,\rangle$, da cui $F = \langle\, \iota(X) \,\rangle$. □

Notate l'analogia con spazi vettoriali e basi: per dare una funzione lineare da uno spazio vettoriale a un altro, basta definirla su una base del primo spazio, e questo si può fare in maniera arbitraria.

Notate che non tutti i gruppi sono liberi. Per esempio il gruppo $H = \langle\, h \,\rangle$ ciclico di ordine 2 non è libero su nessun suo sottoinsieme, dato che 1 deve essere sempre mandato in 1 da un morfismo, e h deve essere mandato in un elemento di periodo 2 o 1. Dunque non posso mandare h, ad esempio, in un elemento di periodo 3.

Invece abbiamo

4.1.4. ESERCIZIO.

(1) Il gruppo libero su $X = \emptyset$ è $\{\, 1 \,\}$.
(2) Il gruppo libero su un insieme $X = \langle\, x \,\rangle$ con un elemento è $\mathbf{Z}$.

Notiamo questo semplice ma utile

4.1.5. LEMMA. *Sia (F, ι) un gruppo libero sull'insieme X. Sia Y un altro insieme, e $\beta : Y \to X$ una biezione. Sia $j = \iota \circ \beta : Y \to F$. Allora (F, j) è libero su Y.*

Questo Lemma ci permette dunque di rimpiazzare l'insieme X su cui un gruppo è libero con qualsiasi insieme Y con cui X sia in biiezione.

DIMOSTRAZIONE. Sia G un gruppo, e $f : Y \to G$ una funzione, Consideriamo $f' = f \circ \beta^{-1} : X \to G$.

$$\begin{array}{ccccc} Y & \xrightarrow{\beta} & X & \xrightarrow{\iota} & F \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle f'} & \swarrow{\scriptstyle\varphi} & \\ & & G & & \end{array}$$

Allora esiste unico un morfismo $\varphi : F \to G$ tale che

$$f' = \varphi \circ \iota.$$

Sosituendo $f' = f \circ \beta^{-1}$ e $\iota = j \circ \beta^{-1}$ si ottiene

$$f = \varphi \circ j.$$

□

Per costruire un gruppo libero, cominciamo col prendere un insieme di *simboli* x^{-1}, per ogni $x \in X$, in modo che $X \cap X^{-1} = \emptyset$, e un altro simbolo $1 \notin X \cup X^{-1}$.

Questo si può realizzare con il Lemma 4.1.5, sostituendo X con $X \times \{ 1 \}$ (ove quell'1 è negli interi), e prendendo $X^{-1} = X \times \{ -1 \}$ e $1 = (0, 0)$ (dove in quest'ul;tima espressioone 1 è un simbolo a parte, ma di nuovo -1 e 0 sono interi). Dunque quello che poco sopra ho chiamato il simbolo x^{-1}, per $x \in X$, sarebbe $(x, -1)$ con questa costruzione, mentre $x \in X$ viene identificato con $x^{+1} = (x, 1)$.

Più in generale, se $y \in X \cup X^{-1}$, scriviamo $y^1 = y$, e $y^0 = 1$.

Una *parola* in X sarà una successione

$$(a_1, a_2, \dots)$$

ove $a_i \in X \cup X^{-1} \cup \{ 1 \}$, e $a_i = 1$ da un certo punto in poi (dunque una successione definitivamente eguale alla costante 1). La successione

$$(1, 1, \dots)$$

viene detta la *parola vuota*, e indicata con 1.

Una notazione compatta per una parola non vuota

$$(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, x_3^{\varepsilon_3}, \dots)$$

ove $x_i \in X$, $\varepsilon_i \in \{ +1, -1, 0 \}$, è

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}, \quad \text{con } \varepsilon_n \neq 0. \tag{4.1.1}$$

(Dunque $x_n^{\varepsilon_n}$ è l'ultimo termine prima che la successione diventi costante 1.) Badate che fino a qui non si fanno semplificazioni, dunque per un elemento $x \in X$

$$x \cdot 1 \cdot x, x \cdot x^{-1}, x \cdot 1 \cdot 1 \cdot \dots \cdot 1 \cdot x^{-1}$$

sono tutte parole validissime.

Visto che le parole sono successioni, due parole non vuote sono eguali se e solo si scrivono letteralmente allo stesso modo nella forma (4.1.1).

L'inverso della parola (4.1.1) è la parola

$$x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1},$$

anche se occorre un minimo di cautela, perché potrebbe ben essere $\varepsilon_1 = 0$, quindi non è detto che quest'ultima parola sia nella forma (4.1.1).

Una parola è *ridotta* se è vuota, oppure è nella forma (4.1.1), con tutti gli $\varepsilon_i \neq 0$, e non si ha mai

$$x_{i+1}^{\varepsilon_{i+1}} = x_i^{-\varepsilon_i}$$

per $i = 1, 2, \dots, n-1$. Data una qualsiasi parola (4.1.1), possiamo trasformarla in una parola ridotta cancellando i termini $x_i^{\varepsilon_i} = 1$ (usando dunque il fatto che in un gruppo 1 è elemento neutro) e i termini $x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}}$ per cui $x_{i+1} = x_i$ e $\varepsilon_{i+1} = -\varepsilon_i$ (dunque semplificando un elemento col suo inverso).

4.1.6. Osservazione. Andrebbe mostrato che anche quando ci sono più modi apparentemente diversi di effettuare questa sequenza di semplificazioni, il risultato è comunque unico. Questo segue comunque dalla discussione successiva.

Date due parole

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}, \qquad y_1^{\eta_1} y_2^{\eta_2} \dots y_m^{\varepsilon_m},$$

la loro *giustapposizione* è la parola

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} y_1^{\eta_1} y_2^{\eta_2} \dots y_m^{\eta_m}.$$

Se le due parola di partenza sono ridotte, la giustapposizione non è detto che lo sia, per esempio per $x \in X$ le parole x e x^{-1} sono ridotte, ma xx^{-1} non lo è.

Esiste una *moltiplicazione* di parole ridotte che dà luogo a una parola ridotta. Date due parole ridotte w_1, w_2, se la loro giustapposizione $w_1 w_2$ non è ridotta, vuol dire che ci sono termini alla fine di w_1 che si cancellano con termini all'inizio di w_2. Allora si può scrivere

$$w_1 = u_1 v, \quad w_2 = v^{-1} u_2,$$

in modo che la parola $u_1 u_2$ sia ridotta, e questa è la giustapposizione delle due parola ridotte w_1, w_2.

Si potrebbe vedere (ma è laborioso) che la giustapposizione è una operazione di gruppo sull'insieme F delle parole ridotte. Usiamo invece il trucco di van der Waerden.

Per $x \in X$, definiamo funzioni $|\, x^\varepsilon \,| : F \to F$, per $\varepsilon \in \{ +1, -1 \}$, mediante

$$(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}) \,|\, x^\varepsilon \,| = \begin{cases} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} x^\varepsilon & \text{se } x^\varepsilon \neq x_n^{-\varepsilon_n}, \\ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_{n-1}^{\varepsilon_{n-1}} & \text{se } x^\varepsilon = x_n^{-\varepsilon_n}. \end{cases}$$

(Notate che ho scritto la funzione a destra, perché è una permutazione, come vediamo fra un attimo.)

Si vede che ogni $|\, x^\varepsilon \,|$ appartiene al gruppo delle permutazioni su F, basta fare l'esercizio seguente, che richiede una distinzione di casi.

4.1.7. Esercizio.

$$|\, x^\varepsilon \,| \circ \left|\, x^{-\varepsilon} \,\right| = \mathbf{1}$$

ove $\mathbf{1}$ *è l'identità su* F.

Dunque abbiamo $|\, x^\varepsilon \,|^{-1} = |\, x^{-\varepsilon} \,|$.

Sia $\mathcal{F}$ il gruppo di permutazioni generato dagli $|\, x^\varepsilon \,|$. Ogni suo elemento si scriverà dunque nella forma

$$|\, x_1^{\varepsilon_1} \,| \circ |\, x_2^{\varepsilon_2} \,| \circ \dots \circ |\, x_n^{\varepsilon_n} \,|, \tag{4.1.2}$$

ove $\varepsilon_i \in \{ +1, -1 \}$, e grazie a (4.1.7) posso assumere sia per ogni i

$$x_{i+1}^{\varepsilon_{i+1}} \neq x_i^{-\varepsilon_i},$$

altrimenti grazie a (4.1.7) cancello i due termini.

Ma allora questa scrittura per gli elementi di $\mathcal{F}$ è unica, perché applicando a 1 questa parola ottengo

$$1 \,|\, x_1^{\varepsilon_1} \,| \circ |\, x_2^{\varepsilon_2} \,| \circ \dots \circ |\, x_n^{\varepsilon_n} \,| = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n},$$

e quest'ultima è una parola ridotta, che si scrive in modo unico in questa forma.

Notate che questo mostra che l'ordine delle semplificazioni in un'espressione $|\, x_1^{\varepsilon_1} \,| \circ |\, x_2^{\varepsilon_2} \,| \circ \cdots \circ |\, x_n^{\varepsilon_n} \,|$ o nella parola corrispondente $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$ non cambia l'espressione/parola ridotta finale, come affermato nell'Osservazione 4.1.6

Grazie a questa corrispondenza abuseremo nel seguito il linguaggio, e parleremo di $|\, x_1^{\varepsilon_1} \,| \circ |\, x_2^{\varepsilon_2} \,| \circ \cdots \circ |\, x_n^{\varepsilon_n} \,|$ come di una parola ridotta, anche se ci riferiamo in realtà a $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$. La giustapposizione di parole ridotte come quest'ultima corrisponde alla composizione di espressioni (4.1.2) nel gruppo $\mathcal{F}$.

Ora mostriamo che $\mathcal{F}$ è libero sull'insieme $\mathcal{X} = \{\, |\, x\, | : x \in X \,\}$. Sia $f : \mathcal{X} \to G$ una funzione, ove G è un gruppo. Visto che la scrittura (4.1.2) (con le condizioni specificate) è unica, posso definire senza ambiguità $\varphi : \mathcal{F} \to G$ mediante

$$\varphi(|\, x_1^{\varepsilon_1} \,| \circ |\, x_2^{\varepsilon_2} \,| \circ \cdots \circ |\, x_n^{\varepsilon_n} \,|) = f(|\, x_1 \,|)^{\varepsilon_1} f(|\, x_2 \,|)^{\varepsilon_2} \dots f(|\, x_n \,|)^{\varepsilon_n}.$$

Ora mostriamo che questo φ è un morfismo di gruppi.

Siano w_1, w_2 due parole ridotte in $\mathcal{X}$. Se anche la moltiplicazione $w_1 \circ w_2$ è ridotta (intendo quindi che la parola associata, che si ottiene togliendo le sbarrette verticali, è ridotta), allora è chiaro che

$$\varphi(w_1 \circ w_2) = \varphi(w_1)\varphi(w_2).$$

Altrimenti, scriviamo come sopra

$$w_1 = u_1 \circ v, \quad w_2 = v^{-1} \circ u_2,$$

con $u_1 \circ u_2$ ridotta.

Vediamo in (laborioso) dettaglio questo fatto. Sia

$$w_1 = x_0^{\varepsilon_0} x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}, \qquad w_2 = y_0^{\eta_0} y_1^{\eta_1} \dots y_m^{\eta_m},$$

supponiamo che si abbia

$$y_0^{\eta_0} = x_n^{-\varepsilon_n}, y_1^{\eta_1} = x_{n-1}^{-\varepsilon_{n-1}}, \dots, y_k^{\eta_k} = x_{n-k}^{-\varepsilon_{n-k}},$$

e poi, o

$$x_{n-k-1}^{\varepsilon_{n-k-1}} \neq y_{k+1}^{-\eta_{k+1}},$$

oppure sono finiti o gli x_i o gli y_i. Allora pongo

$$v = x_{n-k}^{\varepsilon_{n-k}} \cdots x_{n-1}^{\varepsilon_{n-1}} x_n^{\varepsilon_n},$$

sicché

$$v^{-1} = (x_{n-k}^{\varepsilon_{n-k}} \cdots x_{n-1}^{\varepsilon_{n-1}} \cdot x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} \cdots x_{n-k}^{-\varepsilon_{n-k}} = y_0^{\eta_0} y_1^{\eta_1} \cdots y_k^{\eta_k},$$

e ho le due parole (eventualmente vuote)

$$u_1 = x_0^{\varepsilon_0} \cdots x_{n-k-1}^{\varepsilon_{n-k-1}}, \qquad u_2 = y_{k+1}^{\eta_{k+1}} \cdots y_m^{\eta_m}$$

Allora abbiamo da un lato

$$\varphi(w_1) = \varphi(u_1)\varphi(v), \quad \varphi(w_2) = \varphi(v)^{-1}\varphi(u_2),$$

dunque

$$\varphi(w_1)\varphi(w_2) = \varphi(u_1)\varphi(u_2).$$

D'altra parte

$$\varphi(w_1 \circ w_2) = \varphi(u_1 \circ u_2) = \varphi(u_1)\varphi(u_2),$$

e dunque

$$\varphi(w_1 \circ w_2) = \varphi(w_1)\varphi(w_2)$$

anche in questo caso.

Notate che abbiamo visto in particolare che $\mathcal{F} = \langle \mathcal{X} \rangle$, cosa peraltro già dimostrata in generale per i coprodotti nella Proposizione 3.2.1.

4.1.1. Esempi. Consideriamo il gruppo libero $F_1 = \langle x \rangle$ su un insieme $\{ x \}$ consistente di un'unico elemento x.

Le parole ridotte sono

$$\begin{cases} 1 \\ xx \cdots x \\ x^{-1}x^{-1} \cdots x^{-1} \end{cases}$$

Dunque $F_1 \cong \mathbf{Z}$. In effetti avevamo già visto la proprietà universale del gruppo additivo $\mathbf{Z}$ — se ho un gruppo G, a $a \in G$, allora esiste un unico morfismo $\varphi : \mathbf{Z} \to G$ tale che $\varphi(1) = a$, ed esso è $\varphi(k) = a^k$. In termini di F_1, il morfismo è $x^k \mapsto a^k$.

Se x, y sono distinti, $F_2 = \langle x, y \rangle$ è già pareccchio più complicato, qui le parole ridotte (cioè gli elementi di F_2 scritti in modo unico) sono tutte le espressioni

$$z_1 z_2 \cdots z_n,$$

al variare di $n \in \mathbf{N}$, ove $z_i \in \{ x, x^{-1}, y, y^{-1} \}$, e $z_{i+1} \neq z_i^{-1}$ per $1 \leq i < n$.

4.2. Presentazioni

Sappiamo già che se a è un elemento di periodo finito n in un gruppo g, allora il morfismo $\varphi : \mathbf{Z} \to G$ tale che $\varphi(1) = a$ ha immagine $\langle a \rangle$ e nucleo $n\mathbf{Z}$, sicché $\mathbf{Z}/n\mathbf{Z} \cong \langle a \rangle$.

Rivediamo questo fatto in maniera apparentemente più contorta nel contesto di F_1; la tecnica ci torna però utile più sotto.

Consideriamo quell'unico morfismo $\psi : F_1 \to G$ tale che $\psi(x) = a$. Dunque anche qui $\psi(x^k) = a^k$, e l'immagine di ψ è $\langle a \rangle$. Consideriamo $\ker(\psi)$. dato che $F_1/\ker(\psi) \cong \langle a \rangle$, e quest'ultimo ha ordine n, si ha $|\, F_1 : \ker(\psi) \,| = n$. Ora $x^n \in \ker(\psi)$, dato che $\psi(x^n) = a^n = 1$. Consideriamo il più piccolo sottogruppo normale N di F_1 che contenga x^n.

4.2.1. Esercizio. *Sia G un gruppo, $S \subseteq G$.*
Mostrate che esiste un più piccolo sottogruppo normale di G contenente S.

Abbiamo dunque $N \leq \ker(\psi)$, dato che quest'ultimo è un sottogruppo normale contenente x^n. Affermo che $|\, F_1/N \,| \leq n$. Ne seguirà

$$n \geq |\, F_1 : N \,| = |\, F_1 : \ker(\psi) \,| \cdot |\, \ker(\psi) : N \,| = n \cdot |\, \ker(\psi) : N \,|,$$

da cui $|\, \ker(\psi) : N \,| = 1$, e dunque $\ker(\psi) = N$.

Un elemento di $|\, F_1/N \,| \leq n$ sarà della forma $x^k N$, per qualche $k \in \mathbf{Z}$. Dividiamo con resto k per n, ottenendo $k = nq + r$, con $0 \leq r < n$. Abbiamo

$$x^k N = x^{r+nq} N = x^r (x^n)^q N = x^r N,$$

dato che $(x^n)^q \in N$. Dunque F_1/N ha *al più* gli n elementi $N, xN, \dots, x^{n-1}N$. L'argomento più sopra mostra che essi sono distinti.

In questa situazione si dice che $\langle\, x : x^n \,\rangle$ (o anche $\langle\, x : x^n = 1 \,\rangle$) è una presentazione per $\langle\, a \,\rangle$, intendendo che $\langle\, a \,\rangle$ è isomorfo al quoziente del gruppo libero $F_1 = \langle\, x \,\rangle$ rispetto al più piccolo sottogruppo normale che contenga x^n.

Consideriamo S_3. Si ha subito $S_3 = \langle\, (123), (12) \,\rangle$. Se F è il gruppo libero su x, y, c'è un unico morfismo $\varphi : F \to S_3$ tale che $\varphi(x) = (123)$, $\varphi(y) = (12)$. Si ha dunque $F/\ker(\varphi) \cong S_3$. Vogliamo capire come è fatto $\ker(\varphi)$.

Notiamo che $x^3 \in \ker(\varphi)$, dato che $\varphi(x^3) = \varphi(x)^3 = (123)^3 = 1$. Allo stesso modo $\varphi(y^2) = 1$, e

$$\varphi(xyxy) = (123)(12)(123)(12) = (123)(123)^{(12)} = (123)(213) = 1.$$

Sia ora N *il più piccolo sottogruppo normale di* F *che contenga* $x^3, y^2, xyxy$. Che esista lo si vede come per il sottogruppo generato, è l'intersezione di tutti i sottogruppi normali di F che contengono gli elementi dati.

4.2.2. Esercizio. *Si mostri che l'intersezione di una famiglia arbitraria di sottogruppi normali è un sottogruppo normale.*

Consideriamo $G = F/N$, e denotiamo $a = xN$, $b = yN$. Abbiamo dunque in G

$$a^3 = b^2 = 1, a^b = b^{-1},$$

ove l'ultima relazione è una riscrittura di $abab = 1$, tenendo conto che $b = b^{-1}$. Affermo che ogni elemento di G si scrive nella forma $a^i b^j$, con $0 \le i < 3$ e $0 \le j < 2$. Abbiamo intanto $G = \langle\, a, b \,\rangle$, dato che $F = \langle\, x, y \,\rangle$. Consideriamo l'insieme

$$A = \left\{\, a^i b^j : 0 \le i < 3, 0 \le j < 2 \,\right\}.$$

Chiaramente $a, b \in A$, e $A \subseteq \langle\, a, b \,\rangle$. Affermo che A è un sottogruppo di G. Ne seguirà che $A = \langle\, a, b \,\rangle = G$, come richiesto.

In effetti se $a^i b^j, a^s b^t \in A$, distinguiamo due casi. Se $j = 0$, allora chiaramente il prodotto $a^i b^j a^s b^t = a^{i+s} b^t$ è in A, eventualmente dopo aver usato $a^3 = 1$ per ridurre modulo 3 l'esponente $i + s$. Se invece $j = 1$, allora

$$\begin{aligned} a^i b^j a^s b^t &= a^i b a^s b^t \\ &= a^i b^{-1} a^s b b b^t \\ &= a^i (a^s)^b b b^t \\ &= a^i (a^b)^s b^{t+1} \\ &= a^i a^{-s} b^{t+1} \\ &= a^{i-s} b^{t+1} \in A, \end{aligned}$$

ove ho usato $b^2 = 1$ (dunque $b = b^{-1}$ e $a^b = a^{-1}$). Allo stesso modo si vede che $(a^i b^j)^{-1} \in A$.

Abbiamo visto che $|\, G/N \,| \le 6$. D'altra parte $N \le \ker(\varphi)$, e $|\, G/\ker(\varphi) \,| = |\, S_3 \,| = 6$, dunque

$$6 \ge |\, G/N \,| = |\, G : N \,| = |\, G : \ker(\varphi) \,| \cdot |\, \ker(\varphi) : N \,| = 6 \cdot |\, \ker(\varphi) : N \,|,$$

da cui $|\ker(\varphi) : N| = 1$, e quindi $\ker(\varphi) = N$.

Tutto ciò si esprime con una scrittura

$$S_3 = \left\langle a, b : a^3 = 1, b^2 = 1, a^b = a^{-1} \right\rangle$$

che si chiama una *presentazione mediante generatori e relazioni*, e che continuo a spiegare quando ho tempo.

Con le stesse tecniche si vede che per $n \geq 3$ si ha

$$D_n = \left\langle a, b : a^n = 1, b^2 = 1, a^b = a^{-1} \right\rangle.$$

4.3. Prodotti semidiretti

Sia G un gruppo, $H, K \leq G$, con $K \trianglelefteq G$, $G = \langle H, K \rangle = HK$, e $H \cap K = \{1\}$. Allora si vede che ogni elemento di G si scrive in modo unico nella forma hk, con $h \in H$ e $k \in K$.

Ma G non è determinato univocamente dalla sola conoscenza di H e K, come avviene invece per il prodotto diretto (dove si ha anche $H \trianglelefteq G$). Basta pensare al gruppo ciclico, dunque abeliano, $G\langle a \rangle$ di ordine 6, con $H = \langle a^3 \rangle$ di ordine 2 e $K = \langle a^2 \rangle$ di ordine 3, e al gruppo non abeliano $G = S_3$, con $H = \langle (12) \rangle$ e $K = \langle (123) \rangle$. Occorre dunque qualche informazione suppletiva.

Vediamo allora come si moltiplicano due elementi di G. Se $h_i \in H$, $k_i \in K$, abbiamo

$$(h_1k_1)(h_2k_2) = h_1h_2k_1^{h_2}k_2,$$

con $h_1h_2 \in H$, e $k_1^{h_2}k_2$ dato che K è un sottogruppo normale. Dunque per calcolare in $G = HK$ occorre conoscere i coniugati k^h, per $k \in K$ e $h \in H$.

Ora notiamo che per $h \in H$ fissato, la funzione $k \to k^h$ è un automorfismo di K, cioè un isomorfismo $K \to K$. Indichiamo con $\mathrm{Aut}(K)$ l'insieme degli automorfismi di K, che si vede essere un gruppo. Inoltre la funzione $\psi : H \to \mathrm{Aut}(K)$ che manda $h \mapsto (h \to k^h)$ è un morfismo di gruppi.

Dunque per calcolare in $G = HK$, che viene detto un *prodotto semidiretto interno di K mediante H*, occorre conoscere questo morfismo ψ.

Viceversa, siano H, K gruppi, e $\psi : H \to \mathrm{Aut}(K)$ un morfismo. Consideriamo l'*insieme* $H \times K$, con l'operazione data da

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1^{\psi(h_2)}k_2), \tag{4.3.1}$$

ove $k^{\psi(h)}$ indica l'azione su $k \in K$ dell'automorfismo $\psi(h)$.

Allora si vede che con questa operazione l'insieme $H \times K$ diventa un gruppo, che si indica con $K \rtimes_\psi H$ o $H \ltimes_\psi K$ (omettendo la ψ se è implicita), e si chiama *prodotto semidiretto esterno di K mediante H*.

Vediamo specificatamente la dimostrazione del fatto che l'operazione (4.3.1) è associativa. Abbiamo

$$\begin{aligned}((h_1, k_1) \cdot (h_2, k_2)) \cdot (h_3, k_3) &= (h_1h_2, k_1^{\psi(h_2)}k_2) \cdot (h_3, k_3) \\ &= (h_1h_2h_3, (k_1^{\psi(h_2)}k_2)^{\psi(h_3)}k_3) \\ &= (h_1h_2h_3, k_1^{\psi(h_2)\psi(h_3)}k_2^{\psi(h_3)}k_3),\end{aligned}$$

ove nell'ultimo passaggio abbiamo usato il fatto che $\psi(h_3) \in \mathrm{Aut}(K)$. Abbiamo poi

$$\begin{aligned}(h_1,k_1)\cdot((h_2,k_2))\cdot(h_3,k_3)) &= (h_1,k_1)\cdot(h_2h_3, k_2^{\psi(h_3)}k_3)\\ &= (h_1h_2h_3, k_1^{\psi(h_2h_3)}k_2^{\psi(h_3)}k_3)\\ &= (h_1h_2h_3, k_1^{\psi(h_2)\psi(h_3)}k_2^{\psi(h_3)}k_3),\end{aligned}$$

ove nell'ultimo passaggio abbiamo usato il fatto che $\psi : H \to \mathrm{Aut}(K)$ è un morfismo.

Ora notate che $H' = \{\,(h,1) : h \in H\,\}$ e $K' = \{\,(1,k) : k \in K\,\}$ sono sottogruppi di $K \rtimes_\psi H$ isomorfi rispettivamente a K e H. e che $K \rtimes_\psi H = K'H' = H'K'$. Inoltre si ha

$$(1,k)^{(h,1)} = (h,1)^{-1}(1,k)(h,1) = (h^{-1},k)(h,1) = (h^{-1}h, k^{\psi(h)}) = (1,k^{\psi(k)}),$$

e dunque $K \rtimes_\varphi H$ è prodotto diretto interno di K' mediante H', proprio con il morfismo ψ, o meglio col morfismo $\psi' : H' \to \mathrm{Aut}(K')$ che manda $(h,1) \in H'$ nell'automorfismo di K' che manda $(1,k)$ in $(1,k^{\psi(h)})$. Dunque si può semplicemente parlare di prodotto semidiretto.

4.3.1. Esercizio. *Siano H, K gruppi, e $G = H \ltimes_\psi K$ un prodotto semidiretto. Si mostri che*

$$\begin{aligned}H \times K &\to H \ltimes_\psi K\\ (h,k) &\mapsto (h,k)\end{aligned}$$

è un isomorfismo se e solo se $\psi(h) = 1$ per ogni $h \in H$.

4.3.2. Esercizio. *Sia $K = S_3$, $H = \langle\, b \,\rangle$ ciclico di ordine 2.*

Sia $\psi : H \to \mathrm{Aut}(K)$ data da $\psi(b) = \iota((12))$. Dunque $\psi(b)$ è l'automorfismo interno dato dal coniugio $x \mapsto x^{(12)}$.

Si mostri che esiste un isomorfismo $f : H \times K \to H \ltimes_\psi K$.

Quest'ultimo esercizio non è in contraddizione col precedente Esercizio 4.3.1, perché l'isomorfismo f non è $(h,k) \mapsto (h,k)$. Il punto è che l'elemento $b' = (b,(12))$ di $H \ltimes_\psi K$ ha ordine 2, e si può verificare che $b'y = yb'$ per ogni $y \in 1 \times K$. Dunque un isomorfismo f è dato da $f(1,x) = (1,x)$ per $x \in K$, $f(b,1) = b'$.

4.4. L'anello degli endomorfismi di un gruppo abeliano

Un endomorfismo di un gruppo G è un morfismo $G \to G$. L'insieme degli endomorfismi di G si indica con $\mathrm{End}(G)$. Su $\mathrm{End}(G)$ è definita l'operazione $\circ$ di composizione di mappe (che indico semplicemente con la giustapposizione), che rende $(\mathrm{End}(G), \circ)$ un monoide. Incidentalmente, il gruppo degli elementi invertibili di questo monoide non è altro che $\mathrm{Aut}(G)$.

La somma $\varphi + \psi$ di due endomorfismi φ, ψ del gruppo G è definita come la *funzione* data da

$$x^{\varphi+\psi} = x^\varphi x^\psi.$$

A differenza della composizione, la somma di due endomorfismi non è sempre un endomorfismo, anzi, in generale non lo è.

4.4.1. Lemma. *Sia G un gruppo, e $\mathbf{1} : G \to G$ l'endomorfismo identico. Sono equivalenti:*

(1) $\mathbf{1} + \mathbf{1}$ è un endomorfismo, e
(2) G è abeliano.

Dimostrazione. $\mathbf{1} + \mathbf{1}$ non è altro che la funzione $x \mapsto x^2$.
Si ha $abab = (ab)^2 = a^2b^2 = aabb$ se e solo se $ba = ab$. □

Inoltre la somma di endomorfismi non è necessariamente commutativa.

4.4.2. Esempio. Sia $G = S_3$, sia $\varphi = \mathbf{1}$ la mappa identica, e ψ il coniugio per $a = (123)$. Allora si ha

$$(12)^{\mathbf{1}+\psi} = (12)(23) = (132), \quad (12)^{\psi+\mathbf{1}} = (23)(12) = (123).$$

4.4.3. Esercizio ([**Car13**, Proposition 2.1]).
Sia G un gruppo, e $\varphi, \psi \in \mathrm{End}(G)$. Mostrate che sono equivalenti:

(1) $\varphi + \psi \in \mathrm{End}(G)$, e
(2) $[g^\varphi, h^\psi] = 1$ per ogni $g, h \in G$.

Se valgono queste condizioni, allora $\varphi + \psi = \psi + \varphi$.

4.4.4. Teorema. *Sia G un gruppo abeliano.*
Allora l'insieme $\mathrm{End}(G)$ degli endomorfismi di G diventa un anello con unità, con le operazioni di somma sopra descritta, e di prodotto dato dalla composizione.

Cenno di dimostrazione. Il punto fondamentale è che la somma di due endomorfismi φ, ψ è ancora un endomorfismo. Infatti, sfruttando il fatto che G è abeliano, si ha

$$(xy)^{\varphi+\psi} = (xy)^\varphi (xy)^\psi = x^\varphi y^\varphi x^\psi y^\psi = x^\varphi x^\psi y^\varphi y^\psi = x^{\varphi+\psi} y^{\varphi+\psi}.$$

□

4.5. Spazi vettoriali, e gruppi abeliani elementari

Un modo compatto di definire uno spazio vettoriale è il seguente.

4.5.1. Teorema. *Sia V un gruppo abeliano, e $\mathrm{End}(V)$ il suo anello di endomorfismi. Sia F un campo.*
I seguenti dati sono equivalenti:

(1) Una struttura di F-spazio vettoriale su V, e
(2) un morfismo di anelli con unità $F \to \mathrm{End}(V)$.

Dimostrazione. Partiamo da un morfismo $f : F \to \mathrm{End}(V)$. Per $\lambda \in F$, $v \in V$, denotiamo con $\lambda \cdot v$ l'azione di $f(\lambda)$ su v.
Abbiamo allora i seguenti fatti.

$f(1) = 1$: Questo implica

$$1 \cdot v = v$$

per ogni $\lambda \in F$ e $v \in V$.

Ogni $f(\lambda)$ è un endomorfismo di V: Questo implica

$$\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w,$$

per ogni $\lambda \in F$ e $v, w \in V$.

f è un morfismo di anelli: Questo implica

$$\begin{cases} (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v, \\ (\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v), \end{cases}$$

per ogni $\lambda, \mu \in F$ e $v \in V$.

Abbaimo quindi ottenuto tutti gli assiomi di spazio vettoriale, e ogni implicazione è reversibile. □

Sia ora p un primo, e $(G, +, 0)$ un p-gruppo finito *abeliano elementare*, cioè abeliano, e tale che $px = 0$ per ogni $x \in G$. In termini del teorema di struttura dei gruppi abeliani finiti, si ha

$$G = C_p \times \cdots \times C_p,$$

ove $C_p \cong \mathbf{Z}/p\mathbf{Z}$ è ciclico di ordine p.

Dato che G è abeliano, l'operazione "multiplo n-simo" è un endomorfismo di G, cioè per $n \in \mathbf{Z}$ e $x, y \in G$ si ha

$$n(x + y) = nx + ny.$$

Inoltre la funzione

$$\begin{aligned} \mu : \mathbf{Z} &\to \mathrm{End}(G) \\ n &\mapsto (x \mapsto nx) \end{aligned}$$

è un morfismo di anelli, dato che, in accordo con le operazione su $\mathrm{End}(G)$, e usando le regole delle potenze

$$\mu(m + n)x = (m + n)x = mx + nx = (\mu(m) + \mu(n))x$$

e

$$\mu(mn)x = (mn)x = m(nx) = (\mu(m)\mu(n))x.$$

Dato che $\mu(1) = 1$, e che $\mu(p) = 0$ (infatti $\mu(p)x = px = 0$ per ipotesi), si ha che $\ker(\mu) = p\mathbf{Z}$, e quindi il primo teorema di isomorfismo per gli anelli ci fornisce un morfismo (inettivo) di anelli con unità

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \to \mathrm{End}(G).$$

Dunque G diventa uno spazio vettoriale sul campo $\mathbf{F}_p$ con p elementi. Esplicitamente, se $x \in G$ e $n + p\mathbf{Z} \in \mathbf{F}_p$, il multiplo scalare di x per $n + p\mathbf{Z}$ è

$$(n + p\mathbf{Z})x = nx, \tag{4.5.1}$$

che è ben definito perché $px = 0$. Da (4.5.1) segue che gli endomorfismi del gruppo G non sono altro che le funzioni $\mathbf{F}_p$-lineari sullo spazio vettoriale G, dunque se $|\, G \,| = p^n$ si ha che $\mathrm{End}(G)$ è l'anello delle matrici $n \times n$ a coefficienti in $\mathbf{F}_p$, e $\mathrm{Aut}(G) = \mathrm{GL}(n, p)$ è il gruppo delle matrici invertibili $n \times n$ a coefficienti in $\mathbf{F}_p$.

Se per esempio G ha ordine p^2, e dunque $G = C_p \times C_p$, allora G ha automorfismi che non mandano ciascuno dei C_p in se stesso (questo servirà dopo).

4.5.2. Esercizio. *Si verifichi questo fatto, anche solo nel caso $p = 2$, in cui G elementare abeliano di ordine 4 viene detto il gruppo di Klein V_4, e si ha $\mathrm{Aut}(V_4) \cong S_3$ (verificare).*

4.6. Esempi di prodotti semidiretti

Sia $C_n = \langle\, a \,\rangle$ un gruppo ciclico di ordine n.

4.6.1. Lemma.

(1) *Un endomorfismo di C_n è completamente determinato dal suo valore su a.*
(2) *La scelta $a \to a^i$, per $i = 0, \dots, n-1$ determina un endomorfismo $\eta(i)$ di C_n, che vale $a^k \mapsto a^{ki}$.*
(3) *L'endomorfismo $a \mapsto a^i$ è un automorfismo se e solo se $\gcd(i, n) = 1$.*
(4) *La funzione $i \mapsto \eta(i)$ è un isomorfismo fra il gruppo $U(n)$ delle unità di $\mathbf{Z}/n\mathbf{Z}$ e $\mathrm{Aut}(C_n)$.*

Se $n = p_1^{e_1} \cdots p_l^{e_l}$, con i p_i primi distinti, e $e_i > 0$, allora $C_n = \prod_{i=1}^{l} C_{n,p_i}$, con $|\, C_{n,p_i} \,| = p_i^{e_i}$. Ora ogni sottogruppo di un gruppo ciclico è *caratteristico*, ovvero è mandato in sé da ogni automorfismo, dato che è l'unico sottogruppo del suoindice. (Mentre un sottogruppo è normale se è mandato in sé da ogni automorfismo *interno*.) Ne segue

4.6.2. Lemma.

$$\mathrm{Aut}(C_n) \cong \prod_{i=1}^{l} \mathrm{Aut}(C_{n,p_i}).$$

Dimostrazione. Notiamo intanto che per il Corollario 2.11.3 si ha che se $C_n = \langle\, a \,\rangle$, allora $a = \prod_{i=1}^{l} a_i$, con $C_{n,p_i} = \langle\, a_i \,\rangle$.

Il fatto che i C_{n,p_i} siano caratteristici ci dice che è ben definito un morfismo

$$\Theta :\ \mathrm{Aut}(C_n) \to \prod_{i=1}^{l} \mathrm{Aut}(C_{n,p_i})$$
$$\eta \mapsto (\dots, \eta \restriction_{C_{p_n,p_i}}, \dots)$$

Dato che la funzione di Eulero è moltiplicativa (nel senso della teoria dei numeri), basta ora vedere che sia iniettiva, o che sia suriettiva. Vediamo comunque entrambe le cose.

Per far vedere che sia iniettiva, è sufficiente notare che se $\eta \in \mathrm{Aut}(C_n)$ è tale che $a_i^\eta = a_i$ per ogni i, allora $a^\eta = a$.

Per far vedere che sia suriettiva, si può vedere che se prendo automorfismi $\eta_i \in \mathrm{Aut}(C_{n,p_i})$, per ogni i, allora c'è un automorfismo $\eta \in \mathrm{Aut}(C_n)$ tale che $\eta \restriction_{C_{n,p_i}}$ per ogni i: si ha $a^\eta = \prod_{i=1}^{l} a_i^{\eta_i}$. □

Piccola divagazione. Se G è il prodotto diretto (interno) dei due sottogruppi H e K (ma funziona eguale con più fattori), allora c'è un morfismo iniettivo

$$\begin{aligned} \Xi :\ & \mathrm{Aut}(H) \times \mathrm{Aut}(K) \to \mathrm{Aut}(G) \\ & (\alpha, \beta) \mapsto (hk \mapsto h^\alpha k^\beta). \end{aligned} \tag{4.6.1}$$

(Le verifiche sono immediate.) In generale $\mathrm{Aut}(G)$ sarà più grande dell'immagine di Ξ , si veda l'Esercizio 4.5.2, Ma quando sia H che K sono *caratteristici* in G, nel senso appena enunciato che $H^\gamma = H$ e $K^\gamma = K$ per ogni $\gamma \in \mathrm{Aut}(G)$, allora $\mathrm{Aut}(G) = \Xi(\mathrm{Aut}(H) \times \mathrm{Aut}(K))$ (in pratica si dice $\mathrm{Aut}(G) = \mathrm{Aut}(H) \times \mathrm{Aut}(K)$). Infatti se $\gamma \in \mathrm{Aut}(G)$ si ha intanto che $\gamma_{\restriction H} \in \mathrm{Aut}(H)$ e $\gamma_{\restriction K} \in \mathrm{Aut}(K)$, e dunque per $h \in H$ e $k \in K$ si ha

$$(hk)^\gamma = h^\gamma k^\gamma = h^{\gamma_{\restriction H}} k^{\gamma_{\restriction K}},$$

per cui ogni $\gamma \in \mathrm{Aut}(G)$ è nell'immagine del morfismo Ξ di (4.6.1).

Tornando all'argomento principale, si può vedere il fatto seguente.

4.6.3. Proposizione. *Sia P un gruppo ciclico di ordine $p^e > 1$, ove p è un primo.*

(1) $|\,\mathrm{Aut}(P)\,| = \varphi(p^e) = p^{e-1}(p-1)$.
(2) Se p è dispari, allora $\mathrm{Aut}(P)$ *è ciclico.*
(3) Se $p = 2$, allora
  (a) $\mathrm{Aut}(P)$ *è ciclico se $e = 1, 2$,*
  (b) $\mathrm{Aut}(P)$ *è isomorfo a $C_2 \times C_{2^{e-2}}$ se $e > 2$.*
  (c) Se $p = 2$, $e \geq 3$, le tre involuzioni di $\mathrm{Aut}(P)$ *sono*
    (i) $a \mapsto a^{-1}$,
    (ii) $a \mapsto a^{1+2^{e-1}}$,
    (iii) $a \mapsto a^{-1+2^{e-1}}$.

L'esempio più semplice da vedere nel caso $p = 2$ è quanto $e = 3$, dove $U(\mathbf{Z}/8\mathbf{Z}) = \{\,[1], [3], [5], [7]\,\}$ e $[3], [5], [7]$ sono involuzioni.

Studiamo adesso i possibili prodotti semidiretti di $K = C_n = \langle\, a \,\rangle$ per $H = C_m = \langle\, b \,\rangle$. È utile questo

4.6.4. Lemma. *Sia $H = \langle\, b \,\rangle$ un gruppo ciclico di ordine m, e L un gruppo. C'è una corrispondenza biunivoca fra*

(1) morfismi $\psi : H \to L$, e
(2) elementi di L di ordine un divisore di m.

La corrispondenza è data dal fatto che per ogni $c \in L$ di ordine un divisore di m c'è un unico morfismo ψ tale che $\psi(b) = c$, e ogni morfismo è di questo tipo.

Notate che il Lemma vale anche per $m = 0$, ove un elemento ha ordine 0 se le sue potenze sono distinte. (Ricordate che questo torna con la formula $\langle\, b \,\rangle \cong \mathbf{Z}/m\mathbf{Z}$ per un elemento di ordine m, dato che $\mathbf{Z}/o\mathbf{Z} \cong \mathbf{Z}$.)

Dimostrazione. Se $\psi : H \to L$ è un morfismo, allora

$$1 = \psi(1) = \psi(b^m) = \psi(b)^m,$$

e dunque $\psi(b)$ ha ordine un divisore di m.

Viceversa, se $c \in L$ ha ordine un divisore di m, allora la funzione

$$\begin{aligned} \psi : H &\to L \\ a^i &\mapsto c^i \end{aligned}$$

è ben definita, dato che

$$\begin{aligned} a^i = a^j &\iff i \equiv j \pmod{m} \\ &\iff m \mid i-j \\ &\implies |c| \mid i-j \\ &\iff i \equiv j \pmod{|c|} \\ &\iff c^i = c^j, \end{aligned}$$

ed è poi immediatamente vista essere un morfismo. □

Sia $\psi : C_m \to \mathrm{Aut}(C_n)$ un morfismo. Allora si ha $1 = \psi(b^m) = \psi(b)^m$, ma anche $\psi(b)^{|\mathrm{Aut}(C_n)|} = \psi(b)^{\psi(n)} = 1$. Ne segue subito

4.6.5. Lemma. *Se* $\gcd(m, \varphi(n)) = 1$*, allora l'unico prodotto semidiretto* $C_n \rtimes C_m$ *è quello diretto.*

Per esempio un prodotto semidiretto di un gruppo ciclico di ordine 5 per uno di ordine 3 è sempre diretto, dunque ciclico per il Teorema Cinese. (Più avanti vedremo che un gruppo di ordine 15 è sempre ciclico.)

Se invece $\gcd(m, \varphi(n)) = d > 1$, esistono senza'altro prodotti semidiretti non banali (cioè che non siano già diretti). Sia infatti p un primo che divide d. Allora per il Lemma di Cauchy esiste in $\mathrm{Aut}(C_n)$ un elemento β di ordine p, e dunque si può prendere $\psi : C_m \to \mathrm{Aut}(C_n)$ tale che $b^\psi = \beta$.

Un esempio che conosciamo già è dato dal gruppo diedrale. Notiamo che se $n \geq 3$, allora $-1 \neq 1$ è un elemento di ordine 2 in $U(\mathbf{Z}/n\mathbf{Z})$ (e dunque $\varphi(n)$ è pari). Dunque se $m = 2$, posso considerare il morfismo $\psi : C_2 \to \mathrm{Aut}(C_n)$ tale che $b \mapsto (a \mapsto a^{-1})$. Il corrispondente prodotto semidiretto $C_n \rtimes_\psi C_2$ è il gruppo diedrale, come si può vedere passando per esempio da una presentazione.

Per considerare un altro esempio, -2 ha ordine 6 in $U(\mathbf{Z}/7\mathbf{Z})$, dunque $\psi : C_6 \to \mathrm{Aut}(C_7)$ data da $b \mapsto (a \mapsto a^{-2}$ dà luogo a un prodotto semidiretto $C_7 \rtimes_\psi C_6$, che ha presentazione

$$\left\langle a, b : a^7, b^6, a^b = a^{-2} \right\rangle.$$

Il caso quando $n = 2^e$ è una potenza di 2, con $e \geq 2$, dà luogo a tre gruppi interessanti. Secondo la Proposizione 4.6.3(3c), ho tre scelte per $\psi : C_2 \to \mathrm{Aut}(C_{2^e})$ dato da $b \mapsto (a \mapsto a^k)$

$$\begin{cases} \text{per } k = -1 \text{ ho il gruppo diedrale } D_{2^e} \\ \text{per } k = -1 + 2^{e-1} \text{ ho il gruppo } \textit{semidiedrale} \text{ o } \textit{quasidiedrale} \\ \text{per } k = 1 + 2^{e-1} \text{ ho quello che a volte viene chiamato il gruppo } \textit{modulare} \end{cases}$$

4.6.6. Esercizio (Impegnativo). *Fate vedere che questi tre gruppi sono a due a due non isomorfi.*

Un modo di risolvere questo esercizio consiste nel contare quante involuzioni ci siano fuori da $C_n \times 1$. Sappiamo già che nel caso $i = 1$ abbiamo il gruppo diedrale, e quindi tutti gli n elementi fuori da $C_n \times 1$ sono involuzioni. Nel caso $i = 2$ si può vedere che ci sono $n/2 < n$ involuzioni. Nel caso $i = 3$ si può vedere che ce ne sono solo $2 < n/2$.

Per finire, citiamo l'importante esempio del *gruppo quaternionico* generalizzato. Qui $n = 2^e$, con $e \geq 2$, e $m = 4$. Si comincia con $\psi : C_4 \to \mathrm{Aut}(C_{2^e})$ dato da $b \mapsto (a \mapsto a^{-1})$ per ottenere un prodotto semidiretto H. Ora si nota che in H l'elemento $a^{2^{e-1}}b^2$ è centrale. Infatti basta verificare che

$$a^{b^2} = a^{(-1)^2} = a, \quad \text{da cui anche} \quad (b^2)^a = b^2.$$

(Qui c'è una semplice osservazione, che $x^y = x$ equivale a $yx = xy$, dunque a $y^x = y$. Usando i commutatori, $x^y = x[x, y]$, e $y^x = y[y, x]$, ma $[x, y]^{-1} = [y, x]$.) Ne segue

$$(a^{2^{e-1}}b^2)^a = a^{2^{e-1}}b^2,$$

e anche

$$(a^{2^{e-1}}b^2)^b = (a^{2^{e-1}})^b b^2 = a^{-2^{e-1}}b^2 = a^{2^{e-1}}b^2$$

dato che $2^{e-1} \equiv -2^{e-1} \pmod{2^e}$, dunque $\left\langle\, a^{2^{e-1}}b^2 \,\right\rangle$ è un sottogruppo normale, e ora il quoziente $Q_{2^e} = H/\left\langle\, a^{2^{e-1}}b^2 \,\right\rangle$ è il gruppo quaternionico generalizzato di ordine 2^{e+1}, che ha presentazione

$$\left\langle\, a, b : a^{2^e}, b^2 = a^{2^{e-1}}, a^b = a^{-1} \,\right\rangle.$$

(Se $e = 2$ si parla semplicemente del gruppo quaternionico, o dei quaternioni, di ordine 8. Se avete visto i quaternioni di Hamilton, è isomorfo a $\langle\, i, j, k \,\rangle$.)

CAPITOLO 5

Azioni

5.1. Azioni di gruppi su insiemi

Se Ω è un insieme un sottogruppo $G \leq S(\Omega)$ si dice *un gruppo di permutazioni su* Ω. Torna spesso utile un concetto più debole.

5.1.1. Definizione. Sia G un gruppo Ω un insieme.
Un'*azione* di G su Ω è un morfismo $\vartheta : G \to S(\Omega)$.

Dunque se G agisce su Ω, una sua immagine omomorfa (cioè un suo gruppo quoziente) è un gruppo di permutazioni su Ω.

5.1.2. Definizione. Se ϑ è un'azione di G su Ω, $\ker(\vartheta)$ si dice nucleo dell'azione. Un'azione si dice *fedele* se il nucleo è 1.

5.1.3. Proposizione. *Sia G un gruppo, Ω un insieme. Sono equivalenti*
(1) un'azione $\vartheta : G \to S(\Omega)$;
(2) una funzione $\Omega \times G \to \Omega$ che manda $(\alpha, g) \mapsto \alpha^g$ che soddisfi
(a) $\alpha^1 = \alpha$ per ogni $\alpha \in \Omega$, e
(b) $(\alpha^g)^h = \alpha^{gh}$, per $\alpha \in \Omega$ e $g, h \in G$.

Dimostrazione. Se vale (1), definiamo $\alpha^g = \alpha^{\vartheta(g)}$. Allora $\alpha^1 = \alpha^{\vartheta(1)} = \alpha^{\mathbf{1}} = \alpha$, ove $\vartheta(1) = \mathbf{1}$ è la funzione identica, che è l'elemento neutro di $S(\Omega)$, dato che ϑ è un morfismo. E poi $\alpha^{gh} = \alpha^{\vartheta(gh)} = \alpha^{\vartheta(g)\vartheta(h)} = (\alpha^{\vartheta(g)})^{\vartheta(h)} = (\alpha^g)^h$, dato che ϑ è un morfismo, e l'operazione in $S(\Omega)$ è la composizione.

Viceversa, se vale (2), affermo che per ogni $g \in G$ la funzione $\Omega \to \Omega$ che manda $\alpha \mapsto \alpha^g$ è una biiezione, cioè sta in $S(\Omega)$. In effetti ha inversa $\alpha \mapsto \alpha^{g^{-1}}$, dato che $(\alpha^g)^{g^{-1}} = \alpha^{gg^{-1}} = \alpha^1 = \alpha$. E la funzione $\vartheta : g \mapsto (\alpha \mapsto \alpha^g)$ è un morfismo da G a $S(\Omega)$, dato che $\alpha^{\vartheta(gh)} = \alpha^{gh} = (\alpha^g)^h = (\alpha^{\vartheta(g)})^{\vartheta(h)} = \alpha^{\vartheta(g)\vartheta(h)}$. □

5.1.4. Definizione. Se G agisce su Ω, e $\alpha \in \Omega$, $\alpha^G = \{\, \alpha^g : g \in G \,\}$ si dice l'*orbita* di α sotto G.

5.1.5. Lemma. *Le orbite formano una partizione.*

Dimostrazione. Le orbite sono le classi della relazione $\alpha R \beta$ se e solo se $\beta = \alpha^g$ per qualche $g \in G$. Questa relazione è di equivalenza;

- è riflessiva, $\alpha^1 = \alpha$;
- è simmetrica, se $\alpha^g = \beta$, allora $\beta^{g^{-1}} = \alpha$;
- è transitiva, se $\alpha^g = \beta$ e $\beta^h = \gamma$, allora $\alpha^{gh} = \gamma$.

□

5.1.6. Definizione. Un'azione si dice *transitiva* se ha un'unica orbita.

Dunque un'azione è transitiva se esiste $\alpha \in \Omega$ tale che $\alpha^G = \Omega$, o equivalentemente se per ogni $\alpha \in \Omega$ si ha $\alpha^G = \Omega$. In altro modo, dati $\alpha, \beta \in \Omega$, c'è $g \in G$ tale che $\alpha^g = \beta$. Questo è formalizzato nel seguente esercizio.

5.1.7. Esercizio. *Il gruppo G agisca su un insieme Ω.*
Si mostri che i fatti seguenti sono equivalenti.

(1) G ha un'unica orbita su Ω.
(2) Esiste $\alpha \in \Omega$ tale che $\alpha^G = \Omega$.
(3) Esiste $\alpha \in \Omega$ tale che per ogni $\beta \in \Omega$ esiste $g \in G$ tale che $\alpha^g = \beta$.
(4) Per ogni $\alpha \in \Omega$ si ha che $\alpha^G = \Omega$
(5) Per ogni $\alpha, \beta \in \Omega$ esiste $g \in G$ tale che $\alpha^g = \beta$.

5.1.8. Definizione. Se G agisce su Ω, e $\alpha \in \Omega$, $G_\alpha = \{\, g \in G : \alpha^g = \alpha \,\}$ è lo *stabilizzatore* di α in G.

5.1.9. Lemma.

(1) Lo stabilizzatore è un sottogruppo.
(2) $G_{\alpha^g} = g^{-1} G_\alpha g$.
(3) Il nucleo di un'azione è $\bigcap_{\alpha\in\Omega} G_\alpha$.

Dimostrazione. $\alpha^1 = \alpha$, dunque $1 \in G_\alpha$. Se $g, h \in G_\alpha$, allora $\alpha^{gh} = (\alpha^g)^h = \alpha^h = \alpha$. Infine, se $g \in G_\alpha$, allora da $\alpha^g = \alpha$ si ottiene, applicando g^{-1}, che $\alpha = \alpha^1 = \alpha^{gg^{-1}} = (\alpha^g)^{g^{-1}} = \alpha^{g^{-1}}$.

$x \in G_{\alpha^g}$ se e solo se $\alpha^g = (\alpha^g)^x = \alpha^{gx}$ se e solo se $gxg^{-1} \in G_\alpha$ se e solo se $x \in g^{-1} G_\alpha g$.

$$\begin{aligned}\ker(\vartheta) &= \{\, g \in G : \vartheta(g) = \mathbf{1} \,\} \\ &= \left\{\, g \in G : \alpha^g = \alpha^{\vartheta(g)} = \alpha \text{ per ogni } \alpha \in \Omega \,\right\} \\ &= \bigcap_{\alpha\in\Omega} G_\alpha.\end{aligned}$$

□

5.1.10. Teorema (Orbita/Stabilizzatore, versione 1). *Sia G un gruppo che agisce sull'insieme Ω. Sia $\alpha \in \Omega$.*

C'è una corrispondenza biunivoca fra l'insieme $\{\, G_\alpha g : g \in G \,\}$ delle classi laterali dello stabilizzatore G_α, e l'orbita α^G.

In particolare, se G è finito, si ha

$$|\, G \,| = |\, G_\alpha \,| \cdot \left|\, \alpha^G \,\right|.$$

Dimostrazione. Consideriamo la funzione suriettiva

$$\begin{aligned} f : G &\to \alpha^G \\ g &\mapsto \alpha^g \end{aligned}$$

Applichiamo il primo teorema di isomorfismo per gli insiemi. Dunque consideriamo la relazione di equivalenza R su G data da gRh se e solo se $f(g) = f(h)$.

Si ha gRh sse $\alpha^g = \alpha^h$ sse $\alpha^{gh^{-1}} = \alpha$ sse $gh^{-1} \in G_\alpha$. Ma quest'ultima è la relazione di equivalenza che ha come classi le classi laterali $G_\alpha g$. Dunque il primo teorema di isomorfismo per gli insiemi ci fornisce una biezione

$$\begin{aligned} f' : \{ G_\alpha g : g \in G \} &\to \alpha^G \\ G_\alpha g &\mapsto \alpha^g \end{aligned}$$

In particolare, usando il Teorema di Lagrange

$$| \{ G_\alpha g : g \in G \} | = | G : G_\alpha | = \frac{| G |}{| G_\alpha |} = \left| \alpha^G \right|,$$

da cui la formula. □

Più direttamente, stiamo dicendo

5.1.11. Lemma.

$$\{ x \in G : \alpha^x = \alpha^g \} = G_\alpha g.$$

Dimostrazione. $\alpha^x = \alpha^g$ se e solo se $\alpha^{xg^{-1}} = \alpha$ se e solo se $xg^{-1} \in G_\alpha$ se e solo se $x \in G_\alpha g$. □

Sia ora $\vartheta : G \to S(\Omega)$ un'azione, con G finito, e $g \in G$ di periodo d. Consideriamo l'azione di $\langle g \rangle$ su G ereditata in modo naturale da quella di G. Sia $\alpha \in \Omega$, e consideriamo l'orbita di α sotto l'azione di $\langle g \rangle$. Per il Teorema 5.1.10, si ha che $m = \left| \alpha^{\langle g \rangle} \right| = | \langle g \rangle : \langle g \rangle_\alpha |$. Dunque $\langle g \rangle_\alpha$ è quell'unico sottogruppo $\langle g^m \rangle$ di $\langle g \rangle$ di indice m (e ordine d/m). In particolare m è il più piccolo intero positivo k tale che $\alpha^{g^k} = \alpha$. Ora se $x \in \mathbf{Z}$ posso dividere con resto x per m, ottenendo

$$\begin{cases} x = mq + r \\ 0 \leq r < m \end{cases}$$

Dunque $g^x = g^r (g^m)^q$, da cui segue che le classi laterali distinte di $\langle g \rangle_\alpha$ in $\langle g \rangle$ sono $\langle g \rangle_\alpha, \langle g \rangle_\alpha g, \ldots, \langle g \rangle_\alpha g^{m-1}$. Dunque

$$\alpha^{\langle g \rangle} = \left\{ \alpha^{g^i} : i = 0, 1, \ldots, m-1 \right\}.$$

Abbiamo visto

5.1.12. Proposizione. *Se il gruppo finito G agisce sull'insieme Ω, la permutazione $\vartheta(g)$ si scrive come prodotto di cicli (disgiunti)*

$$(\alpha, \alpha^g, \ldots, \alpha^{g^{m-1}}),$$

ove $m = | \langle g \rangle : \langle g \rangle_\alpha |$.

Dunque i cicli disgiunti di $\vartheta(g)$ corrispondono alle orbite di $\langle g \rangle$.

5.2. Esempi

5.2.1. La rappresentazione regolare destra. Sia G un gruppo qualsiasi, e $S(G)$ il gruppo delle permutazioni sull'*insieme* G.

La *rappresentazione regolare destra* è l'azione del gruppo G sull'insieme G data da

$$\begin{aligned} \rho : G &\to S(G) \\ g &\mapsto (x \mapsto xg) \end{aligned}$$

In questa azione ogni stabilizzatore è 1, infatti per ogni $\alpha \in G$ si ha

$$G_\alpha = \{\, g \in G : \alpha^g = \alpha g = \alpha \,\} = \{\, 1 \,\}$$

moltiplicando a sinistra per α^{-1} in $\alpha g = \alpha$.

Dunque se G è un gruppo finito, e $g \in G$ ha periodo d, allora per la Proposizione 5.1.12 $\rho(g)$ ha struttura ciclica $(d, d, \dots)$. (Oppure si può semplicemente notare che ogni orbita è lunga d.) Ne deriva una dimostrazione alternativa di

5.2.1. Corollario. *Se G è un gruppo finito, e $g \in G$, allora l'ordine di g divide l'ordine di G.*

5.2.2. Teorema (Cayley). *Ogni gruppo G è isomorfo a un sottogruppo di $S(\Omega)$, per qualche insieme Ω.*

Dimostrazione. ρ è iniettiva, dunque un isomorfismo fra G e $\rho(G) \leq S(G)$. □

5.2.3. Proposizione. *Sia G un gruppo di ordine $2k$, con k dispari. Allora G ha un sottogruppo (normale) di ordine k.*

Dimostrazione. Consideriamo la rappresentazione regolare destra $\rho : G \to S_n$, con $n = 2k$.

Per il Lemma di Cauchy, in G c'è un elemento a di ordine 2. Dunque $\rho(a)$ è il prodotto di k 2-cicli (disgiunti), e quindi è una permutazione dispari. Ne segue che $\rho(G) \not\leq A_n$, e dunque la composizione, diciamo f,

$$G \xrightarrow{\rho} S_n \longrightarrow S_n/A_n$$

è un morfismo suriettivo. Ne segue che $G/\ker(f) \cong S_n/A_n$, e dunque $\ker(f)$ è il sottogruppo cercato. □

5.2.4. Esercizio. *Trovate un gruppo G di ordine $2k$ che non abbiamo un sottogruppo di ordine k. Naturalmente k deve essere pari.*

(Suggerimento: Prendete $G = A_4$. Forse conviene aspettare di avere i risultati di 6.8.2.)

5.2.2. La rappresentazione regolare sinistra. Questa è

$$\begin{aligned} \lambda : G &\to S(G) \\ g &\mapsto (x \mapsto g^{-1}x) \end{aligned}$$

L'inverso ci vuole per far tornare la condizione $\alpha^{gh} = (\alpha^g)^h$, provare per credere.

5.2.3. Azione di un sottogruppo sul gruppo per moltiplicazione destra. Sia $H \leq G$, allora si può far agire H su G per moltiplicazione destra,

$$\begin{aligned} \rho : H &\to S(G) \\ h &\mapsto (x \mapsto xh) \end{aligned}$$

Gli stabilizzatori sono tutti 1, e le orbite sono le classi laterali xH. Nel caso G sia finito, dal Teorema 5.1.10 e dal Lemma 5.1.5 segue la dimostrazione del Teorema di Lagrange.

Più in generale, se $\varphi : G \to S(\Omega)$ è un'azione, e $H \leq G$, la si può restringere ad H, e $\varphi_{|H} : H \to S(\Omega)$ sarà un'azione di H su Ω.

5.2.4. Una dimostrazione alternativa del Lemma 2.7.1. Sia G un gruppo, e $H, K \leq G$. Consideriamo la funzione

$$\begin{aligned} f : H \times K &\to G \\ (h, k) &\mapsto hk. \end{aligned}$$

Qui $H \times K$ è solo l'insieme prodotto cartesiano, e f non sarà in generale un morfismo.

L'immagine di f è HK, Inoltre si ha $f(h_1, k_1) = f(h_2, k_2)$ se e solo se $h_1 k_1 = h_2 k_2$ se e solo se $h_1^{-1} h_2 = k_1 k_2^{-1} = x \in H \cap K$. Dunque la classe di (h_1, k_1) rispetto alla relazione di equivalenza indotta da f è data da $\{ (h_1 x, x^{-1} k_1) : x \in H \cap K \}$. In altre parole le le classi sono le orbite dell'azione di $H \cap K$ su $H \times K$ data da $(h, k)^x = (hx, x^{-1}k)$. Si vede subito che gli stabilizzatori sono tutti $\{ 1 \}$. Dunque se G è finito, si avrà che

$$| H \times K | = | H | \cdot | K | = | HK | \cdot | H \cap K | .$$

5.3. Azione per coniugio

L'azione per coniugio di un gruppo G su G, è data da $\alpha^g = g^{-1} \alpha g$. L'orbita $\alpha^G = \{ g^{-1} \alpha g : g \in G \}$ è la classe di coniugio di α, e lo stabilizzatore

$$G_\alpha = \left\{ g \in G : g^{-1} \alpha g = \alpha \right\} = \{ g \in G : \alpha g = g \alpha \}$$

è il centralizzante $C_G(\alpha)$ di α in G. Il nucleo è il centro di G

$$\bigcap_{\alpha \in G} \{ g \in G : \alpha g = g \alpha \} = \{ g \in G : \alpha g = g \alpha \text{ per ogni } \alpha \in G \} = Z(G).$$

5.3.1. Contare gli elementi di una classe di coniugio di S_n. Come sappiamo, una classe di coniugio in S_n corrisponde a una struttura ciclica, cioè a una partizione di n. Nel seguito indicheremo una classe col suo rappresentante *più semplice*, ad esempio la classe corrispondente alla partizione $(4, 32, 1)$ di $n = 10$ con $(1234)(567)(89)$.

Scriviamo le strutture cicliche nella forma

$$(n_{1,1}, \ldots, n_{1,l_1}, n_{2,1}, \ldots, n_{2,l_2}, \ldots, n_{k,1}, \ldots, n_{k,l_k}), \tag{5.3.1}$$

ove

$$n_{1,1} = \cdots = n_{1,l_1} > n_{2,1} = \cdots = n_{2,l_2} > \cdots > n_{k,1} = \cdots = n_{k,l_k}). \tag{5.3.2}$$

5.3.1. Proposizione. *La classe corrispondente alla partizione* (5.3.1) *con la condizione* (5.3.2) *ha un numero di elementi pari a*

$$\frac{n!}{\prod_{i=1}^{k}\left(l_i! \cdot \prod_{j=1}^{l_i} n_{i,j}\right)}.$$

Dimostrazione. Cominciamo col riempire le posizioni della struttura ciclica con i numeri da 1 a n in tutti i modi possibili. Questo ci dà il numeratore $n!$. Poi notiamo che ogni ciclo lungo m si può scrivere in m modi

$$(a_1 a_2 \dots a_m) = (a_2 a_3 \dots a_m a_1) = \cdots = (a_m a_1 \dots a_{m-1}),$$

il che ci dà i fattori $n_{i,j}$ al denominatore. Infine gli l_i cicli di lunghezza $n_{i,1}$ si possono permutare fra loro senza cambiare la permutazione, e questo ci dà i termini $l_i!$ al denominatore. □

Ad esempio, il numero di elementi di struttura ciclica $(2,2)$ in S_4 è dato da

$$\frac{4!}{2!2!2!} = 3,$$

il numero di elementi di struttura ciclica $(2,2,1)$ in S_5 è dato da

$$\frac{5!}{2!2!2!} = 15,$$

il numero di elementi di struttura ciclica $(2,2,2)$ in S_6 è dato da

$$\frac{6!}{2!2!3!} = 30.$$

5.3.2. Classi di coniugio di S_n e A_n, per $n = 4, 5$. Qui contiamo gli elementi delle classi con la Proposizione 5.3.1, deduciamo l'ordine del centralizzante mediante il Teorema Orbita-Stabilizzatore, dopodiché conoscendone l'ordine è facile vedere chi sia effettivamente il centralizzante.

Le classi di coniugio di $G = S_4$ sono

Elemento α	α^G	$\lvert C_G(\alpha) \rvert$	$C_G(\alpha)$
1	1	24	G
(12)	6	4	$\langle (12), (34) \rangle$
(123)	8	3	$\langle (123) \rangle$
(1234)	6	4	$\langle (1234) \rangle$
(12)(34)	3	8	$\langle (1324), (34) \rangle$

Qui l'ultimo centralizzante è un gruppo diedrale. Notate che (1324) centralizza la sua potenza $(1324)^2 = (12)(34)$.

Le classi di coniugio di $G = S_5$ sono

Elemento α	$\left\vert \alpha^G \right\vert$	$\vert\, C_G(\alpha)\,\vert$	$C_G(\alpha)$
1	1	120	G
(12)	10	12	$\langle\,(12),(345),(45)\,\rangle$
(123)	20	6	$\langle\,(123),(45)\,\rangle$
(1234)	30	4	$\langle\,(1234)\,\rangle$
(12345)	24	5	$\langle\,(12345)\,\rangle$
(12)(34)	15	8	$\langle\,(1324),(34)\,\rangle$
(123)(45)	20	6	$\langle\,(123)(45)\,\rangle$

Qui il centralizzante di (12) è $\langle\,(12)\,\rangle \times T$, dove T è il gruppo delle permutazioni su $\{\,3,4,5\,\}$ (dunque $T \cong S_3$), dato che permutazioni che agiscono su insiemi disgiunti commutano.

Per vedere le classi di coniugio di A_n, per $n = 4, 5$, si può usare il seguente argomento.

Sia G un gruppo finito, e H un suo sottogruppo di indice 2, dunque normale. G agisca su Ω, e sia $\alpha \in \Omega$.

$$\begin{aligned}\left\vert \alpha^H \right\vert &= \vert\, H : H_\alpha \,\vert \\ &= \vert\, H : H \cap G_\alpha \,\vert \\ &= \vert\, HG_\alpha : G_\alpha \,\vert \\ &= \frac{1}{\vert\, G : HG_\alpha \,\vert} \cdot \vert\, G : G_\alpha \,\vert\,.\end{aligned}$$

Ora $HG_\alpha \leq G$, dato che $H \trianglelefteq G$, e

$$2 = \vert\, G : H \,\vert = \vert\, G : HG_\alpha \,\vert \cdot \vert\, HG_\alpha : H \,\vert\,.$$

Dunque $\vert\, G : HG_\alpha \,\vert = 2$ se $\vert\, HG_\alpha : H \,\vert = 1$, cioè $HG_\alpha = H$, ovvero $G_\alpha \leq H$, mentre se $G_\alpha \nleq H$, allora $HG_\alpha \gneq H$, dunque $\vert\, HG_\alpha : H \,\vert = 2$, da cui $\vert\, G : HG_\alpha \,\vert$ e $G = HG_\alpha$. Abbiamo ottenuto

5.3.2. Lemma. *Sia H un sottogruppo di indice 2 del gruppo finito G.*
G agisca su Ω, e sia $\alpha \in \Omega$.
Allora

$$\left\vert \alpha^H \right\vert = \begin{cases} \left\vert \alpha^G \right\vert & \text{se } G_\alpha \nleq H \\ \frac{1}{2} \cdot \left\vert \alpha^G \right\vert & \text{se } G_\alpha \leq H \end{cases}$$

Notate in particolare che se α^G ha un numero dispari di elementi, deve valere il primo caso.

Ne otteniamo i due seguenti fatti, dove scriviamo G per l'appropriato S_n.

Le classi di coniugio di $H = A_4$ sono

Elemento α	$\left\vert \alpha^H \right\vert$	$\vert\, C_H(\alpha)\,\vert$	$C_H(\alpha)$
1	1	12	H
(123)	4	3	$\langle\,(123)\,\rangle$
(132)	4	3	$\langle\,(132)\,\rangle$
(12)(34)	3	4	$\langle\,(12)(34), (13)(24)\,\rangle$

Per vedere come la singola classe α^{S_4} si spezza in due, notiamo che $(123)^{(23)} = (132)$. Ora per il Lemma 5.1.11, $(123)^x = (132)$ se e solo se $x \in C_G((123))(23)$, che è fatto tutto di permutazioni dispari. Dunque (123) non è coniugato a (132) in H.

Le classi di coniugio di $H = A_5$ sono

Elemento α	$\left\vert \alpha^H \right\vert$	$\vert\, C_H(\alpha)\,\vert$	$C_H(\alpha)$
1	1	60	H
(123)	20	3	$\langle\,(123)\,\rangle$
(12345)	12	5	$\langle\,(12345)\,\rangle$
(13524)	12	5	$\langle\,(15432)\,\rangle$
(12)(34)	15	4	$\langle\,(12)(34), (13)(24)\,\rangle$

Notate che $(13524) = (12345)^2 = (12345)^{(2354)}$.

5.3.3. Corollario. *A_5 è un gruppo semplice, ovvero i suoi soli sottogruppi normali sono 1 e A_5.*

Dimostrazione. Sia $N \trianglelefteq A_5$, con $N \neq 1, A_5$. Dato che è normale, deve essere unione di classi di coniugio, e naturalmente contenere 1.

Se contiene la classe con 20 elementi, dato che $1 + 20 = 21 \nmid 60$, deve contenere almeno un'altra classe. Se contiene la classe con 15 elementi, si ha che $1+20+15 = 36$ non divide $60 = \vert\, A_5 \,\vert$, ed è maggiore di 30 elementi, che è il più grande divisore proprio di 60.

Se contiene la classe con 15 elementi, dato che $1 + 15 = 16 \nmid 60$, deve contenere almeno un'altra classe. Se contiene una classe con 12 elementi, dato che $1 + 15 + 12 = 28 \nmid 60$, deve contenere un'altra classe, ma allora ha più di 30 elementi

Se non contiene la classe con 15 elementi, può avere $1+12 = 13$ o $1+12+12 = 25$ elementi, ma nessuno dei due numeri divide 60. □

Il seguente Esercizio generalizza un pochino il Lemma 5.3.2.

5.3.4. Esercizio. *Sia G un gruppo finito, e H un suo sottogruppo* normale *di indice p primo.*

G agisca su un insieme Ω, e sia $\alpha \in \Omega$.

Si mostri che

$$\left\vert \alpha^H \right\vert = \begin{cases} \left\vert \alpha^G \right\vert & \text{se } G_\alpha \not\leq H \\ \dfrac{1}{p} \cdot \left\vert \alpha^G \right\vert & \text{se } G_\alpha \leq H \end{cases}$$

5.3.5. Esercizio. *Sia G un gruppo finito, e H un suo sottogruppo di indice n.*

G agisca su un insieme Ω, e sia $\alpha \in \Omega$.

Si mostri che

$$\left|\, \alpha^H \,\right| = \frac{|\, HG_\alpha \,|}{|\, G \,|} \cdot \left|\, \alpha^G \,\right|$$

In particolare, se $G_\alpha \leq H$*, allora*

$$\left|\, \alpha^H \,\right| = \frac{1}{n} \cdot \left|\, \alpha^G \,\right|.$$

Notate che se H non è normale, HG_α potrebbe *non* essere un sottogruppo, per cui la frazione $|\, HG_\alpha \,| \,/ |\, G \,|$ non è detto che sia della forma $1/n$, per n un intero; si veda l'esercizio seguente.

5.3.6. Esercizio. *Sia* $G = S_3$ *che agisce in modo naturale su* $\Omega = \{\, 1, 2, 3 \,\}$. *Dunque* $1^G = \Omega$.

Sia $H = \langle\, (12) \,\rangle$. *Allora* $1^H = \{\, 1, 2 \,\}$.

Dunque $\left|\, 1^H \,\right| \nmid \left|\, 1^G \,\right|$. *Questo è il caso nell'esercizio precedente in cui* HG_α *(qui* $\alpha = 1$*) non è un sottogruppo, dato che* $HG_1 = \langle\, (12) \,\rangle \langle\, (13) \,\rangle = \{\, 1, (12), (13), (123) \,\}$. *Dunque nelle notazioni dell'esercizio precedente*

$$\frac{|\, HG_\alpha \,|}{|\, G \,|} = \frac{4}{6} = \frac{2}{3}$$

non è una frazione del tipo $1/n$ *con* n *intero.*

5.4. Lemma di Cauchy

5.4.1. Teorema (Lemma di Cauchy). *Sia* G *un gruppo finito, e sia* p *un primo che divide l'ordine di* G.

Allora G *contiene un elemento di ordine* p.

Dimostrazione. Consideriamo l'insieme

$$G^p = \{\, (x_0, \ldots, x_{p-1}) : x_i \in G \,\}.$$

In realtà conviene considerare l'insieme (in biiezione con questo) Δ delle funzioni $x : \mathbf{Z}/p\mathbf{Z} \to G$, dove una funzione x è rappresentata dalla p-pla $(x_0, \ldots, x_{p-1}) \in G^p$ dei suoi valori. Chiaramente $|\, \Delta \,| = |\, G \,|^p$.

Ora il gruppo $\mathbf{Z}/p\mathbf{Z}$ agisce (fedelmente) su Ω, mediante

$$(x_0, x_1, \ldots, x_{p-1})^k = (x_k, x_{1+k}, \ldots, x_{p-1+k}),$$

ove si verificano facilmente gli assiomi delle azioni, $x^0 = x$ è immediato, e

$$x^{k+h} = (x^k)^h$$

pure.

Consideriamo ora il sottoinsieme di Δ

$$\Omega = \{\, (x_0, \ldots, x_{p-1}) \in \Delta : x_0 x_1 \cdots x_{p-1} = 1 \,\}.$$

Notiamo che $|\, \Omega \,| = |\, G \,|^{p-1}$. Infatti se $x \in \Omega$, allora

$$x_0 = (x_1 \cdots x_{p-1})^{-1}, \tag{5.4.1}$$

e viceversa, dati arbitrariamente $x_1, \ldots, x_{p-1}$, scegliendo x_0 come in (5.4.1) si ottiene un elemento di Ω.

Inoltre $\mathbf{Z}/p\mathbf{Z}$ agisce ancora su Ω, perché se $x_0x_1\cdots x_{p-1}=1$, allora

$$1 = x_0^{-1}\cdot 1\cdot x_0 = x_0^{-1}(x_0x_1\cdots x_{p-1})x_0 = x_1\cdots x_{p-1}x_0,$$

che è il prodotto ordinato degli elementi di

$$x^1 = (x_1, x_2, \ldots, x_{p-1}, x_0),$$

ove x^1 indica l'azione di $1\in\mathbf{Z}/p\mathbf{Z}$ su x. Proseguendo, si vede che $x^k\in\Omega$ per ogni k.

Per il Teorema 5.1.10, ogni orbita ha lunghezza 1 o p. Se n_1 è il numero di orbite lunghe 1, e n_p è il numero di orbite lunghe p, si ha

$$|\,G\,|^{p-1} = |\,\Omega\,| = n_1 + pn_p.$$

Dunque $p\mid n_1$, dato che p divide sia $|\,\Omega\,|$ che pn_p.

Sia $(x_0, x_1, \ldots, x_{p-1})$ un elemento che ha un'orbita lunga 1. Allora si avrà

$$(x_0, x_1, \ldots, x_{p-1}) = (x_0, x_1, \ldots, x_{p-1})^1 = (x_1, x_2, \ldots, x_0)$$

dunque $x_0 = x_1 = \cdots = x_{p-1}$. In altre parole

$$(x_0, x_1, \ldots, x_{p-1}) = (y, y, \ldots, y),$$

con $y^p = 1$.

Ora senz'altro $(1, 1, \ldots, 1)$ ha un'orbita lunga 1. Dunque $n_1 > 0$, e dunque $n_1 \geq p$, dato che è divisibile per p. Ma allora se $(y, y, \ldots, y)\neq(1, 1, \ldots, 1)$ è un'orbita lunga 1, vuol dire che y è un elemento di periodo p. □

5.5. Azione sulle classi laterali

Sia G un gruppo, e $H\leq G$. Allora G agisce sull'insieme $\Omega = \{\, Hc : c\in G\,\}$ delle classi laterali di H in G per moltiplicazione a destra, $(Hc)^g = H(cg)$, per $g\in G$.

L'azione è evidentemente transitiva. Per quanto riguarda gli stabilizzatori, si ha

$$\begin{aligned} G_{Hc} &= \{\, g\in G : Hcg = Hc\,\} \\ &= \left\{\, g\in G : Hcgc^{-1} = H\,\right\} \\ &= \left\{\, g\in G : cgc^{-1}\in H\,\right\} \\ &= \left\{\, g\in G : g\in c^{-1}Hc\,\right\} \\ &= c^{-1}Hc. \end{aligned}$$

Dunque il nucleo dell'azione è $\bigcap_{c\in G} c^{-1}Hc$. Se $|\,G : H\,| = n$ è finito, allora $|\,\Omega\,| = n$, e dunque l'azione fornisce un morfismo $\vartheta : G\to S_n$; dato che $G/\ker(\vartheta)$ è isomorfo a un sottogruppo di S_n, si ottiene il

5.5.1. Lemma. *Se $|\,G : H\,|$ è finito, allora è finito anche*

$$\left|\, G : \bigcap_{c\in G} c^{-1}Hc\,\right|.$$

che avevamo annunciato nella Sezione 1.4.

5.6. Semplicità dei gruppi alterni

Vogliamo mostrare, per induzione su n, il seguente

5.6.1. Teorema. *Il gruppo alterno A_n è semplice, per $n \geq 5$.*

5.6.1. Multipla transitività. Il gruppo G agisca sull'insieme Ω, e sia $|\,\Omega\,| \geq k \geq 1$. Si dice che G agisce k-transitivamente su Ω (o che è k-transitivo), se date due k-ple

$$(a_1, \ldots, a_k), (b_1, \ldots, b_k)$$

di elementi distinti di Ω, esiste $g \in G$ tale che $a_i^g = b_i$ per ogni i.

5.6.2. Esercizio. *Il gruppo G agisca sull'insieme Ω. Sia $(c_1, \ldots, c_k)$ una k-pla* fissata *di elementi distinti di Ω. Sono equivalenti*

(1) G agisce k-transitivamente su Ω,
(2) per ogni k-pla $(b_1, \ldots, b_k)$ di elementi distinti di Ω esiste $g \in G$ tale che $c_i^g = b_i$ per ogni i, e
(3) per ogni k-pla $(b_1, \ldots, b_k)$ di elementi distinti di Ω esiste $g \in G$ tale che $b_i^g = c_i$ per ogni i.

5.6.3. Proposizione. *Il gruppo G agisca* transitivamente *sull'insieme Ω, con $|\,\Omega\,| \geq k \geq 1$.*

Sono equivalenti

(1) G è $(k+1)$-transitivo,
(2) per ogni $\alpha \in \Omega$ lo stabilizzatore G_α è k-transitivo su $\Omega \setminus \{\,\alpha\,\}$,
(3) esiste $\alpha \in \Omega$ tale che lo stabilizzatore G_α è k-transitivo su $\Omega \setminus \{\,\alpha\,\}$.

Dimostrazione. Se vale la condizione (1), allora vale (2). Infatti, per ogni $\alpha \in \Omega$, prese le $(k+1)$-ple di elementi distinti

$$(\alpha, a_1, \ldots, a_k), (\alpha, b_1, \ldots, b_k)$$

esiste $g \in G$ tale che

$$\alpha^g = \alpha, \qquad a_i^g = b_i, \text{ per ogni } i,$$

ovevro G_α è k-transitivo su $\Omega \setminus \{\,\alpha\,\}$.

La condizione (2) implica ovviamente la condizione (3).

Mostriamo infine che la condizione (3) implica la condizione (1). Supponiamo che lo stabilizzatore G_β di un particolare elemento β sia k-transitivo su $\Omega \setminus \{\,\beta\,\}$. Fissiamo una $(k+1)$-pla

$$(\beta, b_1, \ldots, b_k)$$

di elementi distinti, e sia

$$(\alpha, a_1, \ldots, a_k)$$

una $(k+1)$-pla arbitraria di elementi distinti di Ω. Dato $g \in G$ tale che $\alpha^g = \beta$, gli elementi $x \in G$ tali che $\alpha^x = \beta$ sono gli elementi della classe laterale $G_\alpha g = gg^{-1}G_\alpha g = gG_{\alpha^g} = gG_\beta$. Affermo che esiste $h \in G_\beta$ tale che $a_i^{gh} = b_i$ per ogni i. Infatti $a_i^g \neq \beta = \alpha^g$ per ogni i, dato che $a_i \neq \alpha$ per ogni i; e per ipotesi $b_i \neq \beta$ per

$i \geq 1$. Dato che G_β è per ipotesi k-transitivo su $\Omega \setminus \{\beta\}$, esiste $h^{-1} \in G_\beta$ tale che $b_i^{h^{-1}} = a_i^g$ per $i \geq 1$. □

Il gruppo simmetrico S_n è evidentemente n-transitivo nella sua azione naturale su $\Omega = \{1, 2, \ldots, n\}$. Invece il gruppo alterno A_n è $(n-2)$-transitivo, per $n \geq 3$, ma non $(n-1)$-transitivo. Infatti sia $(b_1, \ldots, b_{n-2})$ una n-pla di elementi distinti in Ω, e siano d_1, d_2 gli elementi rimanenti. Ci sono esattamente due permutazioni g_1, g_2 che portano i in b_i per $i = 1, 2, \ldots, n-2$, e queste sono

$$\begin{cases} 1^{g_i} = b_i & \text{per } i = 1, 2, \ldots, n-2, \\ (n-1)^{g_1} = d_1, n^{g_1} = d_2 & \\ (n-1)^{g_2} = d_2, n^{g_2} = d_1. & \end{cases}$$

Dato che $g_2 = g_1 \cdot (d_1, d_2)$ (o anche $g_2 = (n-1, n) \cdot g_1$, in entrambi i casi con la composizione da sinistra a destra), una fra g_1, g_2 è pari, l'altra è dispari. Dunque A_n è almeno $(n-2)$-transitivo, ma non $(n-1)$-transitivo, perché l'unica permutazione g tale che

$$\begin{cases} i^g = i & \text{per } i = 1, 2, \ldots, n-2, \\ (n-1)^g = n & \end{cases}$$

è $(n-1, n)$, che è dispari.

5.6.2. Primitività. Il gruppo G agisca sull'insieme Ω. Una partizione $\mathcal{P}$ di Ω si dice G-invariante se $P^g \in \mathcal{P}$ per ogni $P \in \mathcal{P}$ e $g \in G$. Ci sono due partizioni G-invarianti banali, $\mathcal{P} = \{\Omega\}$, e $\mathcal{P} = \{\{a\} : a \in \Omega\}$. Per esempio, il gruppo diedrale $G = \langle (1234), (13) \rangle$ nell'azione naturale sul *quadrato* $\Omega = \{1, 2, 3, 4\}$ ha la partizione G-invariante non banale data dalle diagonali $\mathcal{P} = \{\{1, 3\}, \{2, 4\}\}$.

Nel seguito, anche se non specificato esplicitamente, prenderemo G come gruppo di permutazioni sull'insieme Ω di cardinalità maggiore di 1, dunque $G \leq S(\Omega)$ che agisce naturalmente su Ω.

5.6.4. Definizione. Sia Ω un insieme di cardinalità maggiore di 1.
Sia $G \leq S(\Omega)$ un sottogruppo transitivo.
Si dice che G è *primitivo* se non ci sono partizioni G-invarianti non banali, *imprimitivo* altrimenti.

Un *blocco* è un sottoinsieme non vuoto $A \subseteq \Omega$ tale che per $g \in G$ si abbia o $A = A^g$, o $A \cap A^g = \emptyset$. I blocchi banali sono $A = \Omega$ e $A = \{a\}$, per qualche $a \in \Omega$.

5.6.5. Lemma. *Sia Ω un insieme di cardinalità maggiore di 1.*
Sia $G \leq S(\Omega)$ un sottogruppo transitivo.
Sia $\alpha \in \Omega$ fissato.
Sono equivalenti:

(1) G è primitivo,
(2) i soli blocchi sono quelli banali, e
(3) i soli blocchi contenenti α sono $\{\alpha\}$ e Ω.

DIMOSTRAZIONE. Supponiamo che G sia imprimitivo, e sia $\mathcal{P}$ una partizione G-invariante non banale. Allora ogni $A \in \mathcal{P}$ è un blocco non banale.

Viceversa, se A è un blocco non banale, allora $\mathcal{P} = \{ A^g : g \in G \}$ è una partizione G-invariante non banale. Infatti $\cup\mathcal{P} = \Omega$ perchè G agisce transitivamente. E se $A^g \cap A^h \neq \emptyset$ per qualche $g, h \in G$, allora $A^{gh^{-1}} \cap A \neq \emptyset$, e siccome A è un blocco, si ha $A^{gh^{-1}} = A$, e dunque $A^g = A^h$.

In particolare, se A è un blocco, uno degli A^g, per $g \in G$, sarà un blocco contenente α. □

5.6.6. PROPOSIZIONE. *Sia Ω un insieme di cardinalità maggiore di 1.*
Sia $G \leq S(\Omega)$ un sottogruppo transitivo.
Sia $\alpha \in \Omega$ fissato.
Allora c'è una corrispondenza biunivoca fra

(1) i blocchi contenenti α, e
(2) i sottogruppi H tali che $G_\alpha \leq H \leq G$.

La corrispondenza è data

(1) se $G_\alpha \leq H \leq G$, allora

$$\alpha^H = \left\{ \alpha^h : h \in H \right\}$$

è un blocco contenente α;

(2) se A è un blocco contenente α, allora

$$H = \{ g \in G : A^g = A \} \tag{5.6.1}$$

è un sottogruppo di G che contiene G_α.

DIMOSTRAZIONE. Sia A un blocco contenente α, e H come in (5.6.1). Si vede subito che $H \leq G$, e che $G_\alpha \leq H$, dato che se $g \in G_\alpha$, allora $\alpha \in A \cap A^g$, e dunque $A = A^g$.

Viceversa, sia $G_\alpha \leq H \leq G$, e sia $A = \alpha^H$. Chiaramente $\alpha \in H$. Mostriamo che A è un blocco. Sia $g \in G$ tale che $A^g \cap A \neq \emptyset$. Dunque esistono $h_1, h_2 \in H$ tale che $\alpha^{h_1 g} = \alpha^{h_2}$. Ne segue che $h_1 g h_2^{-1} \in G_\alpha$, e quindi $g \in H G_\alpha H = H$, per cui $A^g = A$.

Le due mappe sono una l'inversa dell'altra. Infatti, sia A un blocco contenente α, e $H = \{ g \in G : A^g = A \}$. Se $\beta \in A$, dato che G è transitivo esiste $g \in G$ tale che $\alpha^g = \beta$. Dunque $\beta \in A \cap A^g$. Dato che A è un blocco, ne segue che $A^g = A$, ovvero $g \in H$, e quindi $\alpha^H = A$.

Viceversa, sia $G_\alpha \leq H \leq G$, e $A = \alpha^H$. Se $g \in G$ è tale che $A^g = A = \alpha^H$, allora esiste $h \in H$ tale che $\alpha^g = \alpha^h$. Dunque $gh^{-1} \in G_\alpha \leq H$, da cui $g \in H$. □

5.6.7. COROLLARIO. *Nelle ipotesi della Proposizione precedente, sono equivalenti*

(1) G è primitivo, e
(2) G_α è un sottogruppo massimale di G, nel senso che se $G_\alpha \leq H \leq G$, allora o $H = G_\alpha$, e $H = G$.

5.6.8. LEMMA. *Se $G \leq S(\Omega)$ agisce 2-transitivamente su Ω, allora G è primitivo.*

DIMOSTRAZIONE. Sia A un blocco con più di un elemento. Siano dunque a_1, a_2 elementi distinti di A, e sia $b \in \Omega$ un qualsiasi elemento distinto da a_1. La 2-transitività implica che esiste $g \in G$ tale che $a_1^g = a_1$, e $a_2^g = b$. Dato che $a_1 \in A \cap A^g$, deve essere $A^g = A$, e dunque $b \in A^g = A$. Dato che $b \neq a_1$ era arbitrario, e che $a_1 \in A$, ne segue che $A = \Omega$. □

5.6.9. ESEMPIO. Sia $\Delta = \{ 1, 2, \dots, n \}$, per $n \geq 5$, e sia Ω l'insieme delle coppie non ordinate di elementi di Δ.

Sia $G = S(\Delta)$, sicché G agisce in modo naturale su Ω.

G non è 2-transitivo su Ω, perché se a, b, c, d sono quattro elementi distinti, non c'è modo di portare $\{ a, b \}$ in $\{ a, b \}$, e $\{ a, c \}$ in $\{ c, d \}$.

Ma G è primitivo su Ω, perché lo stabilizzatore di $\{ n-1, n \}$ è $S_{n-2} \times \langle (n-1, n) \rangle$, e questo si vede nel lemma seguente essere massimale.

Premessa. Sia $\Omega = \{ 1, 2, \dots, n \}$. Per $0 < k < n$, siano

$$\Delta_1 = \{ 1, 2, \dots, k \}, \qquad \Delta_2 = \{ k+1, k+2, \dots, n \}.$$

Consideriamo $S_k \leq S_n$ come il sottogruppo delle permutazioni su Δ_1, che fissano ogni elemento di Δ_2, e $S_{n-k} \leq S_n$ come il sottogruppo delle permutazioni su Δ_2, che fissano ogni elemento di Δ_1. I due sottogruppi S_k e S_{n-k} si centralizzano a vicenda, dunque S_n contiene un sottogruppo $S_k \times S_{n-k}$.

5.6.10. LEMMA. *Sia $2k \neq n \geq 4$. Allora*

$$S_k \times S_{n-k}$$

è un sottogruppo massimale di S_n.

Se $n = 2k$, c'è un'involuzione che scambia i due S_k, e quindi $S_k \times S_k$ non è massimale. In dettaglio, l'involuzione

$$\sigma = (1, k+1)(2, k+2) \cdots (k, 2k)$$

scambia fra loro per coniugio le due copie di S_k nel prodotto $P = S_k \times S_k$, ove la prima copia S_k opera su $\{ 1, 2, \dots, k \}$, e la seconda copia su $\{ k+1, k+2, \dots, 2k \}$. Dunque σ normalizza P, e dunque il prodotto semidiretto $\langle \sigma \rangle P$ ha ordine $2 \cdot k! < (2k)! = n!$ per $k > 1$.

DIMOSTRAZIONE. Sia senza perdita di generalità $k > n - k$. Sia $L = S_k \times S_{n-k} < M \leq S_n$. Vogliamo mostrare che $M = S_n$. Per questo, mostreremo che M contiene tutti i 2-cicli. In L ci sono già i 2-cicli (x, y), con $x, y \in \Delta_1$, e quelli con $x, y \in \Delta_2$.

Dato che

$$L = \{ g \in S_n : \Delta_1^g = \Delta_1, \Delta_2^g = \Delta_2 \},$$

esisterà $g \in M > L$ che non manda in sé i Δ_i. Dato che $k = |\Delta_1| > |\Delta_2| = n - k$, esisteranno $a, b, c \in \Delta_1$ e $d \in \Delta_2$ tali che

$$\begin{cases} a^g = c, \\ b^g = d. \end{cases}$$

Dunque in M c'è $(a, b)^g = (c, d)$. Coniugando (c, d) con gli elementi di L, trovo che in M ci sono tutti i 2-cicli (x, y), con $x \in \Delta_1$, $y \in \Delta_2$. □

5.6.3. Dimostrazione del Teorema 5.6.1. La base dell'induzione è il caso $n = 5$. Sia dunque $n > 5$, e, procedendo per assurdo, sia K un sottogruppo normale di $G = A_n$, che sia diverso da $\{1\}$ e G. Ovviamente G è un gruppo di permutazioni su $\Omega = \{1, 2, \ldots, n\}$.

$S = A_{n-1}$ è un sottogruppo di G, come stabilizzatore di n.

Dato che S è semplice per ipotesi, e $K \cap S \trianglelefteq S$, può essere solo $K \geq S$, o $K \cap S = \{1\}$.

Sia $K \geq S$. Per il Corollario 5.6.7, S è massimale in G, dunque $K = S$, ma si vede subito che S non è normale in G. (Per esempio $(12)(34) \in S$, ma $((12)(34))^{(12)(4n)} = (12)(3n) \notin S$.

Sia dunque $K \cap S = \{1\}$.

5.6.11. Lemma. *Sia $G \leq S(\Omega)$ primitivo, e $\{1\} \neq K \trianglelefteq G$.*
Allora K è transitivo.

Dimostrazione del Lemma. Fissato $\alpha \in \Omega$, mostriamo che α^K è un blocco.

Per $g \in G$, si ha $\alpha^{Kg} = (\alpha^g)^K$. Dunque α^K e α^{Kg} sono due orbite dell'azione di K, e quindi o coincidono, o sono disgiunte.

Se fosse ora $\alpha^K = \{\alpha\}$, allora sarebbe $K \leq G_\alpha$, e dunque $K \leq \bigcap \{ G_\alpha^g : g \in G \} = \bigcap \{ G_\beta : \beta \in \Omega \} = \{1\}$. Dunque $\alpha^K = \Omega$. □

Dato che K è transitivo, e interseca banalmente lo stabilizzatore S di n, è anche regolare. In altre parole la funzione

$$\begin{aligned} f : K &\to \Omega \\ k &\mapsto n^k \end{aligned}$$

del Teorema Orbita/Stabilizzatore è una biiezione. S agisce per coniugio su K (dunque come automorfismi), e in modo naturale su Ω. Affermo che f è un isomorfismo di azioni. Infatti per $x \in S$ si ha

$$f(k^x) = f(x^{-1}kx) = n^{x^{-1}kx} = (n^k)^x = f(k)^x.$$

Ora $S = A_{n-1}$ agisce $(n-3)$-transitivamente su $\Omega \setminus \{n\}$, dunque agisce per coniugio, quindi mediante automorfismi, $(n-3)$-transitivamente su $K \setminus \{1\}$, con $n - 3 \geq 6 - 3 = 3$.

Tutto segue ora da

5.6.12. Lemma. *Sia K un gruppo finito, e $T \leq \mathrm{Aut}(K)$.*

(1) Se T agisce transitivamente su $K \setminus \{1\}$, allora K è un p-gruppo elementare abeliano, per un primo p.
(2) Se T agisce 2-transitivamente su $K \setminus \{1\}$, allora
  (a) o $|K| = 3$,
  (b) oppure K è un 2-gruppo elementare abeliano.
(3) Se T agisce 3-transitivamente su $K \setminus \{1\}$, allora $K \cong C_2 \times C_2$ ha ordine 4.
(4) T non può agire 4-transitivamente su $K \setminus \{1\}$.

Dimostrazione. Sia p un primo che divida l'ordine di K, sicché K ha un elemento di ordine p. Se T agisce transitivamente su $K \setminus \{1\}$, allora tutti gli

elementi diversi da 1 hanno ordine p, e dunque K è un p-gruppo. Ora il centro $Z(K)$ del p-gruppo non banale K è non banale (Proposizione 6.3.1). Dato che il centro è un sottogruppo caratteristico, si ha $Z(K) = K$, e dunque K è abeliano.

Sia ora T 2-transitivo. Dunque K è un p-gruppo elementare abeliano. Se $p > 2$, allora per $1 \neq x \in K$ si ha $x \neq x^{-1}$. Se $y \in K$ è diverso da x, esiste $t \in T$ tale che $x^t = x$ e $(x^{-1})^t = y$. Ma dato che t è un automorfismo, si ha $y = (x^{-1})^t = (x^t)^{-1} = x^{-1}$. Dunque $K = \{ 1, x, x^{-1} \}$.

Sia ora T 3-transitivo, per cui K è un 2-gruppo elementare abeliano. Fissiamo $a, b \neq 1$ distinti, e sia $c \notin \{ 1, a, b \}$. Affermo che $c = ab$. Dato che $a, b \neq 1$, si ha $a \neq ab \neq b$. Dunque esiste $t \in T$ tale che

$$\begin{cases} a^t = a, \\ b^t = b, \\ (ab)^t = c. \end{cases}$$

Come sopra, ne segue $c = ab$, e dunque $K = \{ 1, a, b, ab \}$. Dato che $K \setminus \{ 1 \}$ ha tre elementi, T non può essere 4-transitivo. □

CAPITOLO 6

Teoremi di Sylow

6.1. Azione per coniugio sui sottogruppi

Sia G un gruppo, e Ω l'insieme dei suoi sottogruppi. L'azione per coniugio di G su Ω è data da $H^g = g^{-1}Hg$. Qui lo stabilizzatore è $N_G(H) = \{\, g \in G : H^g = H \,\}$, che è un sottogruppo di G (come tutti gli stabilizzatori) contenente H.

6.2. Primo Teorema di Sylow

6.2.1. Teorema (Primo Teorema di Sylow). *Sia G un gruppo finito, e p un primo che divide l'ordine di G.*
Sia $|\, G \,| = p^e m$, con $p \nmid m$.
Allora G ha un sottogruppo di ordine p^e.

Un sottogruppo come nell'enunciato del Teorema si dice un *p-sottogruppo di Sylow* di G. In realtà vedremo nella Proposizione 6.3.4 che G ha sottogruppi di ordine p^f, per ogni $f \leq e$.

6.2.2. Osservazione. Notate come il Primo Teorema di Sylow implichi il Lemma di Cauchy, perché se S è un p-sottogruppo di Sylow, e $1 \neq a \in S$ ha ordine p^k, allora $a^{p^{k-1}}$ ha ordine p.

Dimostrazione del Primo Teorema. Sia Ω l'insieme dei sottoinsiemi di G di ordine p^e. Dunque

$$|\, \Omega \,| = \binom{p^e m}{p^e}.$$

Affermo che

$$\binom{p^e m}{p^e} \equiv m \pmod{p}. \tag{6.2.1}$$

Posto $F = \mathbf{Z}/p\mathbf{Z}$, si calcola in $F[x]$

$$(1+x)^{p^e m} = (1 + x^{p^e})^m = 1 + mx^{p^e} + \dots$$

G agisca su Ω per moltiplicazione a destra. Dato che l'ordine di Ω è congruo a $m \not\equiv 0 \pmod{p}$, c'è un'orbita α^G di lunghezza non divisibile per p. Consideriamo G_α. Si ha $|\, G \,| = \left|\, \alpha^G \,\right| \cdot |\, G_\alpha \,|$, dunque $p^e \mid |\, G_\alpha \,|$. D'altra parte se $a \in \alpha$, si ha

$$aG_\alpha \subseteq \alpha G_\alpha = \alpha,$$

dunque

$$|\, G_\alpha \,| = |\, aG_\alpha \,| \leq p^e$$

da cui $|\, G_\alpha \,| = p^e$, come richiesto. □

6.3. Equazione delle classi

Se il gruppo finito G agisce su se stesso per coniugio, dato che le orbite formano una partizione, abbiamo che la somma delle cardinalità delle classi è eguale all'ordine di G. Ora la classe di $\alpha \in G$ ha ordine 1 se e solo se $\alpha \in Z(G)$. Dunque possiamo scrivere l'*equazione delle classi*

$$|\, G \,| = |\, Z(G) \,| + \sum n_i, \tag{6.3.1}$$

ove gli $n_i > 1$ sono le cardinalità delle classi di coniugio distinte di elementi non centrali.

Sia ora G un p-gruppo finito. Dato che la cardinalità di una classe è l'indice dello stabilizzatore, e dunque divide $|\, G \,|$, abbiamo che gli n_i sono tutti potenze di p. Dunque p divide $|\, G \,|$ e gli n_i, e dunque secondo (6.3.1) divide $|\, Z(G) \,|$. dato che $Z(G)$ è un sottogruppo, ne segue che $|\, Z(G) \,| \geq p$. Dunque vale

6.3.1. Proposizione. *Un p-gruppo finito non banale ha centro non banale.*

6.3.2. Lemma. *Sia G un gruppo.*
Se $G/Z(G)$ è ciclico, allora G è abeliano.

Dimostrazione. Sia $G/Z(G) = \langle\, aZ(G) \,\rangle$. Allora ogni elemento di G si scrive come $a^n z$, per $n \in \mathbf{Z}$, e $z \in Z(G)$. Dato un altro elemento $a^m w$ di G, con $m \in \mathbf{Z}$, e $w \in Z(G)$, si ha

$$(a^n z) \cdot (a^m w) = a^n a^m z w = a^m a^n z w = (a^m w)(a^n z).$$

□

Ne segue

6.3.3. Lemma. *Un gruppo di ordine un quadrato di un primo è abeliano.*

Dimostrazione. Sia ora G un p-gruppo di ordine p^2. Si ha $Z(G) \neq 1$. Se $Z(G) = G$, allora G è abeliano. Se per assurdo $Z(G)$ avesse ordine p, sicché $G/Z(G)$ è di ordine p, e dunque ciclico, allora G sarebbe abeliano, per il Lemma seguente. □

Un'altra conseguenza della Proposizione 6.3.1 è

6.3.4. Proposizione. *Un p-gruppo finito G di ordine p^n ha sottogruppi normali di ordine p^m, per ogni $0 \leq m \leq n$.*

Dimostrazione. Procediamo per induzione su n, il caso $n = 0$ essendo ovvio.

Se $n \geq 1$, allora per la Proposizione 6.3.1 $Z(G) \neq 1$. Sia $z \in Z(G)$ un elemento di ordine p. Dunque $N = \langle\, z \,\rangle$ è un sottogruppo normale di ordine p, e G/N è un gruppo di ordine p^{n-1}. Per ipotesi induttiva, e per il Terzo Teorema di Isomorfismo, G/N ha sottogruppi $H/N \trianglelefteq G/N$ di ogni ordine p^{m-1}, per $m \leq n$. Dunque H è un sottogruppo normale di ordine p^m di G. □

6.4. Il teorema di Lucas

Si tratta di una forma generale di (6.2.1), formulata in [**Luc78a, Luc78c, Luc78b**]. Esiste una vasta letteratura di generalizzazioni, si veda ad esempio [**Gra97**].

Sia p un numero primo. Sia a un intero positivo, che scriviamo in base p, dunque

$$a = a_0 + pa_1 + \cdots + p^k a_k,$$

con $0 \leq a_i < p$. Sia $\mathbf{F} = \mathbf{Z}/p\mathbf{Z}$, e calcoliamo in $\mathbf{F}[x]$

$$\begin{aligned}
\sum_{b=0}^{a} \binom{a}{b} x^b &= (1+x)^a \\
&= (1+x)^{a_0 + pa_1 + \cdots + p^k a_k} \\
&= (1+x)^{a_0} \cdot (1+x)^{pa_1} \cdots (1+x)^{p^k a_k} \\
&= (1+x)^{a_0} \cdot (1+x^p)^{a_1} \cdots (1+x^{p^k})^{a_k} \\
&= \left(\sum_{b_0=0}^{a_0} \binom{a_0}{b_0} x^{b_0} \right) \cdot \left(\sum_{b_1=0}^{a_1} \binom{a_1}{b_1} x^{pb_1} \right) \cdots \left(\sum_{b_k=0}^{a_k} \binom{a_k}{b_k} x^{p^k b_k} \right) \\
&= \left(\sum_{b_0=0}^{p-1} \binom{a_0}{b_0} x^{b_0} \right) \cdot \left(\sum_{b_1=0}^{p-1} \binom{a_1}{b_1} x^{pb_1} \right) \cdots \left(\sum_{b_k=0}^{p-a} \binom{a_k}{b_k} x^{p^k b_k} \right) \\
&= \sum_{b=0}^{a} \left(\binom{a_0}{b_0} \cdot \binom{a_1}{b_1} \cdots \binom{a_k}{b_k} \right) \cdot x^{b_0 + pb_1 + \cdots + p^k b_k},
\end{aligned}$$

dove

$$b = b_0 + pb_1 + \cdots + p^k b_k$$

è la scrittura di b in base p, dato che $0 \leq b_i \leq a_i < p$, e questa scrittura è unica.

Abbiamo ottenuto il

6.4.1. Teorema (di Lucas, [**Luc78a, Luc78c, Luc78b**]). *Sia p un primo. Siano a, b interi, scritti in base p come*

$$a = a_0 + pa_1 + \cdots + p^k a_k, \qquad b = b_0 + pb_1 + \cdots + p^k b_k,$$

con $0 \leq a_i, b_i < p$.

Allora

$$\binom{a}{b} \equiv \binom{a_0}{b_0} \cdot \binom{a_1}{b_1} \cdots \binom{a_k}{b_k} \pmod{p}.$$

Notate la seguente conseguenza immediata

6.4.2. Corollario. *Nelle notazioni di questa sezione, sono equivalenti:*

(1) $\binom{a}{b} \equiv 0 \pmod{p}$, *e*

(2) $b_i > a_i$ per uno (o più) valori di i

6.5. Il Teorema di Kummer

Vale la pena di segnalare anche il

6.5.1. Teorema (Kummer). *Il numero di volte che il primo p divide $\binom{a}{b}$ è pari al numero di riporti nella somma in base p di b e $a-b$.*

Dimostrazione. Se n è un intero positivo, il numero di volte che il primo p divide $n!$ è dato da

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^i} \right\rfloor + \dots$$

dato che un numero ogni p è divisibile per p, uno ogni p^2 è divisibile per p^2, ecc. La somma è finita perché quando $p^k > n$ si ha $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$.

Dunque il numero di volte che p divide $\binom{a}{b}$ è dato, ponendo $c = a - b$, da

$$\left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{a}{p^2} \right\rfloor + \cdots - \left\lfloor \frac{b}{p} \right\rfloor - \left\lfloor \frac{b}{p^2} \right\rfloor - \cdots - \left\lfloor \frac{c}{p} \right\rfloor - \left\lfloor \frac{c}{p^2} \right\rfloor - \dots$$

Ora se la scrittura di a in base p è data da $a = a_0 + a_1 p + \dots$, con $0 \le a_i < p$, e analogamente per b e c, si ha

$$\begin{aligned} \left\lfloor \frac{a}{p} \right\rfloor - \left\lfloor \frac{b}{p} \right\rfloor - \left\lfloor \frac{c}{p} \right\rfloor &= a_1 + pa_2 + \cdots - b_1 - pb_2 - \cdots - c_1 - pc_2 - \dots \\ &= \frac{a - a_0}{p} - \frac{b - b_0}{p} - \frac{c - c_0}{p} \\ &= \frac{b_0 + c_0 - a_0}{p}. \end{aligned} \tag{6.5.1}$$

Ora $b_0 + c_0 = a_0$ se $b_0 + c_0 < p$, altrimenti c'è un riporto, $b_0 + c_0 = p + a_0$, e dunque (6.5.1) vale 1.

Proseguendo in questo modo,

$$\begin{aligned} \left\lfloor \frac{a}{p^i} \right\rfloor - \left\lfloor \frac{b}{p^i} \right\rfloor - \left\lfloor \frac{c}{p^i} \right\rfloor &= a_i + pa_{i+1} + \cdots - b_i - pb_{i+1} - \cdots - c_i - pc_{i+1} - \dots \\ &= \frac{a - a_0 - a_1 p - \cdots - a_{i-1}p^{i-1}}{p^i} \\ &\quad - \frac{b - b_0 - b_1 p - \cdots - b_{i-1}p^{i-1}}{p^i} \\ &\quad - \frac{c - c_0 - c_1 p - \cdots - c_{i-1}p^{i-1}}{p^i} \\ &= \frac{b_0 + b_1 p + \cdots + b_{i-1}p^{i-1} + c_0 + c_1 p + \cdots + c_{i-1}p^{i-1} - a_0 - a_1 p - \cdots - a_{i-1}p^{i-1}}{p^i}. \end{aligned}$$

Come sopra, l'ultimo numeratore è 0 se

$$b_0 + b_1 p + \cdots + b_{i-1} p^{i-1} + c_0 + c_1 p + \cdots + c_{i-1} p^{i-1} < p^i,$$

ovvero se non c'è riporto sommando le cifre $(i-1)$-sime, altrimenti vale p^i. □

6.6. Secondo Teorema di Sylow

6.6.1. Teorema (Secondo Teorema di Sylow). *Sia G un gruppo finito, e p un primo che divide l'ordine di G.*

Sia S un p-sottogruppo di Sylow di G, e $P \leq G$ un p-sottogruppo (cioè un sottogruppo di ordine una potenza di p.

(1) Esiste $g \in G$ tale che $P^g \leq S$.
(2) I p-sottogruppi di Sylow di G formano una classe di coniugio,
(3) G ha un numero $n_p = |\, G : N_G(S) \,|$ di p-sottogruppi di Sylow. Dunque n_p divide $|\, G : S \,|$.

Notate un paio di conseguenze.

(1) In un gruppo abeliano finito, c'è uno e un solo p-sottogruppo di Sylow, per ogni primo p che divida l'ordine del gruppo. Questi sono i sottogruppi visti in (2.11.1).
(2) In un gruppo G, che sia divisibile per il primo p, si ha $n_p = 1$, cioè c'è un solo p-sottogruppo di Sylow, se e solo un (qualsiasi) p-sottogruppo di Sylow è normale in G.
(3) Il fatto che se un p-sottogruppo di Sylow è normale, allora è unico, segue anche dal Lemma 6.9.5.

Dimostrazione. Consideriamo l'insieme

$$\Omega = \{\, S^g : g \in G \,\}$$

dei coniugati di S. Si ha $|\,\Omega\,| = |\, G : N_G(S) \,|$ che divide m, un numero non divisibile per p.

P agisce per coniugio su Ω, e ogni orbita ha ordine un divisore dell'ordine di P. Dato che Ω ha ordine non divisibile per p, c'è un'orbita di un elemento S^h di ordine non divisibile per p, e dunque di ordine 1. Dunque per $x \in P$ si ha $x^{-1} S^h x = S^h$, ovvero $S^h x = x S^h$, e quindi $S^h P = P S^h$ è un sottogruppo di G. L'ordine

$$\left|\, S^h P \,\right| = \frac{\left|\, S^h \,\right| |\, P \,|}{|\, S^h \cap P \,|}$$

del sottogruppo $S^h P$ è una potenza di p, maggiore o eguale di $\left|\, S^h \,\right|$, dato che $|\, P \,| \geq \left|\, S^h \cap P \,\right|$. Ma l'ordine del sottogruppo $S^h P$ deve dividere l'ordine di G per il Teorema di Lagrange, dunque deve essere anche minore o eguale a $|\, S \,| = \left|\, S^h \,\right|$. Dunque $|\, P \,| = \left|\, S^h \cap P \,\right|$, ovvero $P \leq S^h$ e $P^{h^{-1}} \leq S$.

Con questo abbiamo dimostrato il primo punto. Se ora prendo per P un qualsiasi p-sottogruppo di Sylow, ottengo il secondo punto, e dato che lo stabilizzatore nell'azione per coniugio sui sottogruppi è il normalizzante, ottengo anche il terzo punto. □

6.7. Terzo Teorema di Sylow

6.7.1. Teorema (Terzo Teorema di Sylow). *Sia G un gruppo finito, e p un primo che divide l'ordine di G.*

Sia n_p il numero di p-sottogruppi di Sylow di G.

Allora $n_p \equiv 1 \pmod{p}$.

Dimostrazione. Sia Ω l'insieme dei p-sottogruppi di Sylow, fissiamo $P \in \Omega$, e facciamolo agire su Ω per coniugio. Dato che $|\,\Omega\,| = |\,G : N_G(P)\,|$ divide $|\,G : P\,|$, si ha che $p \nmid |\,\Omega\,|$. Dunque nell'azione di P su Ω ci saranno punti fissi. Se S è uno di questi, avremo $x^{-1}Sx = S$ per $x \in P$, da cui $SP = PS$ è un sottogruppo che contiene P, e che ha ordine una potenza di p. Dunque $SP = P$, da cui $S = P$ è l'unico punto fisso, dunque tutte le altre orbite hanno ordine un divisore diverso da 1 dell'ordine di P, e quindi $n_p \equiv 1 \pmod{p}$. □

6.8. Applicazioni dei teoremi di Sylow

6.8.1. Gruppi di ordine 15. Sia G un gruppo di ordine 15. Ha un 3-sottogruppo di Sylow T e un 5-sottogruppo di Sylow C.

Abbiamo $n_3 \mid 5$ e $n_3 \equiv 1 \pmod{3}$, dunque $n_3 = 1$.

Abbiamo $n_5 \mid 3$ e $n_5 \equiv 1 \pmod{5}$, dunque $n_5 = 1$.

Dunque T e C sono unici, dunque normali, e dunque $G \cong T \times C$, che è ciclico di ordine 15.

6.8.1. Osservazione. Questo per la verità lo sapevamo già fare. Per il Lemma di Cauchy, G ha sottogruppi T di ordine 3, e C di ordine 5. Ora C è normale in G, perché ha indice il più piccolo primo che divide l'ordine del gruppo. Dato che $|\,T\,| = 3 \nmid 4 = |\,\mathrm{Aut}(C)\,|$, l'unico prodotto semidiretto di C mediante T è quello diretto.

6.8.2. Gruppi di ordine pq, con p, q primi distinti. Si tratta di una generalizzazione del caso dei gruppi di ordine 15.

Siano $p > q$ primi, e G un gruppo di ordine pq. Sia P un p-sottogruppo di Sylow, e Q un q-sottogruppo di Sylow.

Si ha $n_p \mid q$ e $n_p \equiv 1 \pmod{p}$. Dunque se fosse $n_p > 1$ si avrebbe $n_p \geq 1 + p > p > q$, Ne segue che $n_p = 1$, dunque $P \trianglelefteq G$.

Si ha $n_q \mid p$, e $n_q \equiv 1 \pmod{q}$. Se $n_q = 1$, allora come nel caso dei gruppi di ordine 15 si ha che G è ciclico. Se invece $n_q > 1$, allora $n_q = p$, e dunque $p \equiv 1 \pmod{q}$, ovvero $q \mid p - 1$. Se ora vale quest'ultima divisibilità, allora nel gruppo $U(\mathbf{Z}/p\mathbf{Z})$ delle unità di $\mathbf{Z}/p\mathbf{Z}$, che ha ordine $\varphi(p) = p - 1$, c'è per il Lemma di Cauchy un elemento β di ordine q. Sia $P = \langle\, a \,\rangle$ e $Q = \langle\, b \,\rangle$. Se $\psi : Q \to \mathrm{Aut}(P)$ è il morfismo

$$b \mapsto (a \mapsto a^\beta),$$

allora otteniamo che G è il prodotto semidiretto di P mediante Q dato dalla presentazione

$$\left\langle\, a, b : a^p, b^q, b^{-1}ab = a^\beta \,\right\rangle.$$

Tutti questi prodotti semidiretti sono fra loro isomorfi. Per un fatto che abbiamo citato senza dimostrazione, $U(\mathbf{Z}/p\mathbf{Z})$ è ciclico, e dunque i suoi elementi di

ordine q sono tutti e soli i β^i, per $i = 1, 2, \ldots, q-1$. Consideriamo il prodotto semidiretto $Q \ltimes_{\psi_i} P$, ove $\psi_i(b) = \beta^i$, per $i = 1, 2, \ldots, q-1$. Notiamo che $\alpha_i : b \mapsto b^i$ determina un automorfismo di Q, per $i = 1, 2, \ldots, q-1$.

Affermo che

$$\Theta : Q \ltimes_{\psi_i} P \to Q \ltimes_{\psi_1} P$$
$$(h, k) \mapsto (h^{\alpha_i}, k)$$

è un isomorfismo. è chiaro che è una biiezione. Calcoliamo dapprima

$$\Theta((h_1, k_1) \cdot (h_2, k_2)) = \Theta(h_1 h_2, k_1^{\psi_i(h_2)} k_2) = ((h_1 h_2)^{\alpha_i}, k_1^{\beta^{ij}} k_2),$$

se $h_2 = b^j$, e poi

$$\Theta(h_1, k_1) \cdot \Theta(h_2, k_2) = (h_1^{\alpha_i}, k_1) \cdot (h_2^{\alpha_i}, k_2) = (h_1^{\alpha_i} h_2^{\alpha_i}, k_1^{\psi(h_2^{\alpha_i})} k_2),$$

e ora basta notare che $(h_1 h_2)^{\alpha_i} = h_1^{\alpha_i} h_2^{\alpha_i}$, e che

$$\psi(h_2^{\alpha_i}) = \psi(b^{ji}) = \beta^{ji}.$$

6.8.2. Osservazione. Vale un discorso analogo a quello dell'Osservazione 6.8.1.

6.8.3. Gruppi di ordine p^2q.

6.8.3. Proposizione. *Se p, q sono primi distinti, allora in un gruppo di ordine p^2q c'è un sottogruppo di Sylow normale.*

Supponiamo che i p-sottogruppi di Sylow non siano normali. Devo far veder che c'è un solo q-sottogruppo di Sylow. Per il terzo teorema di Sylow, $n_p = q \equiv 1 \pmod{p}$. In particolare, $p \mid q-1$, e dunque $p < q$.

Se i p-sottogruppi di Sylow hanno a due a due intersezione 1, allora essi esauriscono (omettendo l'identità) $q(p^2-1) = p^2q - q$ elementi. Resta dunque lo spazio per esattamente un q-sottogruppo di Sylow.

Se ci sono due p-sottogruppi di Sylow X, Y, che abbiano intersezione $N = X \cap Y$ di ordine p, allora il normalizzante di N contiene sia X che Y (dato che i gruppi di ordine p^2 sono abeliani), dunque $N_G(N) = G$, e $N \trianglelefteq G$. Sia Q un q-sottogruppo di Sylow di G. Allora NQ in G ha indice p, il più piccolo primo che divide $|\, G \,|$, e dunque $NQ \trianglelefteq G$. Per la stessa ragione $Q \trianglelefteq NQ$, dunque Q è unico di ordine q in NQ, e dunque normale in G.

6.8.4. Un gruppo di ordine 45 è abeliano. $n_5 \mid 9$ e $n_5 \equiv 1 \pmod{5}$ implica $n_5 = 1$, dunque c'è un unico 5-sottogruppo di Sylow C.

Si ha $n_3 \mid 5$ e $n_3 \equiv 1 \pmod{3}$, dunque c'è anche un unico 3-sottogruppo di Sylow T. Il risultato segue dal Lemma 6.3.3.

L'argomento generale sarebbe che se p, q sono primi distinti, e valgono

$$p \nmid q-1, q \nmid p^2-1,$$

allora ogni gruppo di ordine p^2q è abeliano.

Si può vedere abbastanza facilmente, usando i prodotti semidiretti di gruppi ciclici e qualcos'altro, che se anche una sola di queste due condizioni non vale, allora c'è un gruppo non abeliano di ordine p^2q:

- Se $p \mid q-1$, c'è un gruppo non abeliano di ordine pq, e poi basta fare un prodotto diretto con un gruppo di ordine p.
- Stessa cosa,a ruoli scambiati, se $q \mid p-1$.
- Se invece $q \mid p+1$, si vede nell'Esercizio 6.8.4 seguente che il gruppo degli automorfismi del gruppo abeliano $H = C_p \times C_p$ ha un elemento di ordine p^2-1, dunque un elemento di ordine $p+1$, dunque un elemento di ordine q; ne segue che si può fare un prodotto semidiretto ma non diretto di H per C_q.

6.8.4. Esercizio. *Sia $H = C_p \times C_p$. Allora H ha un automorfismo di ordine p^2-1.*

(Suggerimento: Sia F il campo con p^2 elementi. Sappiamo che per ogni $a \in F$ vale $pa = 0$, dunque il gruppo additivo K di F non è ciclico, e quindi è isomorfo ad H, per il teorema di struttura dei gruppi abeliani finiti. Ora sappiamo (anche se per la verità ad Algebra non abbiamo visto una dimostrazione) che il gruppo moltiplicativo $F^\star$ è ciclico, dunque esiste un elemento α di periodo moltiplicativo p^2-1. Ne segue che K ha l'automorfismo $x \mapsto x\alpha$ di ordine p^2-1.)

6.9. Gruppi di ordine 12, 24 e 30

6.9.1. Lemma. *Sia G un gruppo finito, q un primo. Supponiamo che G abbia k sottogruppi di ordine p. Allora G ha $k(q-1)$ elementi di ordine q.*

Dimostrazione. Per il Teorema di Lagrange, l'intersezione di due sottogruppi distinti di ordine q ha ordine 1. □

6.9.2. Esercizio. *In un gruppo di ordine 12 si ha $n_2 = 1$ o $n_3 = 1$.*

Naturalmente segue dalla Proposizione 6.8.3, ma lo rivediamo come applicazione del Lemma.

Dimostrazione. Supponiamo che sia $n_3 > 1$. Per i Teoremi di Sylow si ha $n_3 = 4$. Dunque per il Lemma 6.9.1 ci sono $4 \cdot 2 = 8$ elementi di ordine 3. Ne avanzano giusto $12 - 8 = 4$ per fare un unico 2-sottogruppo di Sylow. □

6.9.3. Esercizio.

(1) Mostrate che in un gruppo abeliano di ordine 12 si ha $n_2 = n_3 = 1$.
(2) Mostrate che in A_4 si ha $n_2 = 1$ e $n_3 = 4$.
(3) Mostrate che in $S_3 \times C_2$ si ha $n_3 = 1$ e $n_2 = 3$.

6.9.4. Esercizio. *Si mostri che in un gruppo G di ordine 30 si ha $n_3 = n_5 = 1$, e c'è un sottogruppo ciclico di ordine 15.*

Premettiamo il

6.9.5. Lemma. *Sia G un gruppo finito di ordine ab, con $\gcd(a,b) = 1$. Se G ha un sottogruppo normale di ordine a, allora esso è unico del suo ordine, e contiene tutti gli elementi di ordine un divisore di a. In particolare, N contiene ogni sottogruppo di ordine un divisore di a.*

DIMOSTRAZIONE. Sia N un sottogruppo normale di ordine a. Dato che G/N ha ordine b, si ha che N contiene tutte le b-sime potenze. D'altra parte esistono u, v tali che $au + bz = 1$.

Se $y \in G$ è tale che $| y | \mid a$ (in particolare se $y \in N$), allora

$$y = y^1 = y^{au+bz} = (y^z)^b$$

appartiene a N. Inoltre ogni elemento di N è una b-sima potenza, dunque N è l'insieme delle b-sime potenze, e dunque unico (e caratteristico).

Se $H \leq G$ ha ordine un divisore di a, allora ogni suo elemento ha ordine un divisore di a, e dunque $H \leq N$. □

Una dimostrazione alternativa del Lemma si può ottenere considerando che se $H \leq G$ ha ordine un divisore di a, allora $HN/N \cong H/H \cap N$ ha ordine che divide da un lato $| G/N | = b$ e dall'altro $| H |$, un divisore di a. Dunque $| HN/N | = 1$, cioè $H \leq N$.

DIMOSTRAZIONE DELL'ESERCIZIO 6.9.4. Se fosse $n_3, n_5 > 1$, allora sarebbe $n_3 = 10$ e $n_5 = 6$, dunque ci sarebbero $2 \cdot 10 + 4 \cdot 6 = 44$ elementi di ordine 3 o 5, troppi.

Dunque o $n_3 = 1$ o $n_5 = 1$, cioè o un 3-sottogruppo di Sylow o un 5-sottogruppo di Sylow deve essere normale. Ma allora, se T è un 3-sottogruppo di Sylow, e C è un 5-sottogruppo di Sylow, si ha $CT \leq G$, un gruppo di ordine 15 che è ciclico per quanto visto nella sottosezione 6.8.1.

Per il Lemma 6.9.5, tutti i 3- e 5-sottogruppi di Sylow sono contenuti in CT, e dunque $n_3 = n_5 = 1$. □

6.9.6. ESERCIZIO. *Sia G un gruppo di ordine 24. Si mostri che G ha un sottogruppo normale di ordine 4 o 8.*

DIMOSTRAZIONE. Sia D un 2-sottogruppo di Sylow di G. Dato che $| G : D | = 3$, il Lemma 6.11.1 implica che G ha un sottogruppo normale K tale che

$$3 \text{ divide } | G : K |, \text{ che divide } 3! = 6,$$

sicché $| K | \in \{ 8, 4 \}$. □

6.9.7. ESERCIZIO.

- *Si mostri che un gruppo abeliano di ordine 24 ha sottogruppi normali di ordine $4, 8$. (E anche di ordine 2, per la verità.)*
- *Si mostri che S_4 ha un sottogruppo normale di ordine 4, ma non ha sottogruppi normali di ordine 2 o 8.*
- *(Piuttosto complicato) Si trovi un gruppo di ordine 24 che ha un sottogruppo normale di ordine 8, ma non un sottogruppo normale di ordine 4.*

6.10. L'argomento di Frattini

6.10.1. LEMMA. *Sia G un gruppo che agisce sull'insieme Ω.*
Sia $H \leq G$ transitivo su Ω.
Allora $G = G_\alpha H$ per ogni $\alpha \in \Omega$.

DIMOSTRAZIONE. Dato che H è transitivo, per ogni $g \in G$ esisterà $h \in H$ tale che $(\alpha^g)^h = \alpha$. Dunque $gh \in G_\alpha$, e $g \in G_\alpha H$. □

6.10.2. TEOREMA. *Sia G un gruppo finito, p un primo che ne divide l'ordine, e sia P un p-sottogruppo di Sylow di G.*

Se $M \geq N_G(P)$, allora $N_G(M) = M$. In particolare

$$N_G(N_G(P)) = N_G(P).$$

DIMOSTRAZIONE. Sia Ω l'insieme dei p-sottogruppi di Sylow di G contenuti in M. (Fra questi naturalmente c'è P.) Questi saranno dunque i p-sottogruppi di Sylow di M.

$N_G(M)$ agisce su Ω, dato che coniuga un p-sottogruppo di Sylow di M in un altro tale sottogruppo. Per il secondo teorema di Sylow, M agisce transitivamente su Ω. Dunque

$$N_G(M) = N_{N_G(M)}(P)M \leq N_G(P)M = M.$$

□

6.10.3. DEFINIZIONE. Un gruppo G si dice *nilpotente* se per ogni $H < G$ si ha $H < N_G(H)$. (Intendo inclusioni strette.)

6.10.4. LEMMA. *Un p-gruppo finito è nilpotente.*

DIMOSTRAZIONE. Sia $H < G$. Se $Z(G) \not\leq H$, allora $H < HZ(G) \leq N_G(H)$. Se $Z(G) \leq H$, si passa al quoziente $G/Z(G)$ e si procede per induzione (si veda l'esercizio seguente). □

6.10.5. ESERCIZIO. *Sia G un gruppo, $K \trianglelefteq G$ e $K \leq H \leq G$.*

Allora

$$N_{G/K}(H/K) = N_G(H)/K.$$

6.10.6. TEOREMA. *Sia G un gruppo finito. Sono equivalenti:*

(1) G è nilpotente,

(2) G ha un unico p-sottogruppo di Sylow per ogni primo p che ne divida l'ordine, e

(3) G è prodotto diretto di p-gruppi (per primi p distinti).

DIMOSTRAZIONE. Solo un cenno. Se G è nilpotente, e P è un p-sottogruppo di Sylow, allora $N_G(N_G(P)) = N_G(P)$, e dunque $N_G(P) = G$. □

6.11. Gruppi piccoli

In questa sezione (in costruzione) vogliamo mostrare che i gruppi di ordine < 60 o sono abeliani o hanno un sottogruppo normale proprio non banale, ovvero non sono semplici. Ricordiamo che A_5 è un gruppo semplice di ordine 60.

Cominciamo con un risultato che generalizza un argomento dell'Esercizio 6.9.6.

6.11.1. LEMMA. *Sia G un gruppo, e $H \leq G$ con $|\, G : H \,| = k > 1$.*

Allora G ha un sottogruppo $N \leq H$ normale (che 'e dunque proprio, cioè diverso da G) tale che

$$k \quad \textit{divide} \quad |\, G : N \,| \quad \textit{divide} \quad k!$$

DIMOSTRAZIONE. Facciamo agire G per moltiplicazione a destra sull'insieme

$$\Omega = \{\, Ha : a \in G \,\}$$

delle k classi laterali destre di H in G. Dunque $(Ha)^g = H(ag)$.

Chiaramente l'azione è transitiva, perché l'orbita di H è

$$H^G = \{\, H^a : a \in G \,\} = \{\, Ha : a \in G \,\}.$$

In effetti lo stabilizzatore $G_H = \{\, a \in G : Ha = H \,\} = H$ ha proprio indice $k = |\,\Omega\,|$, come segue dal Teorema Orbita/Stabilizzatore.

Ora il nucleo di un'azione qualsiasi di un gruppo G sull'insieme Ω è il sottogruppo normale

$$\{\, g \in G : \alpha^g = \alpha \text{ per ogni } \alpha \in \Omega \,\} = \bigcap \{\, G_\alpha : \alpha \in \Omega \,\},$$

che è il nucleo del morfismo

$$\begin{aligned} G &\to S(\Omega) \\ g &\mapsto (x \mapsto x^g). \end{aligned}$$

Nel nostro caso dunque il nucleo N è un sottogruppo di H, e dunque è un sottogruppo proprio, e G/N è isomorfo a un sottogruppo di $S(\Omega) \cong S_k$, e quest'ultimo è un gruppo di ordine $k!$, da cui $|\,G : N\,| \le k!$. □

Una conseguenza immediata è

6.11.2. PROPOSIZIONE. *Sia G un gruppo finito, e $H \le G$.*
Se $|\,G : H\,| = p$ è il più piccolo primo che divide l'ordine di G, allora $H \trianglelefteq G$.

Il caso $p = 2$ lo conosciamo già.

DIMOSTRAZIONE. Per il Lemma precedente, esiste un sottogruppo normale $K \le H$ tale che $p \mid |\,G : K\,| \mid p!$. D'altra parte per Lagrange $|\,G : K\,| \mid |\,G\,|$. Dato che p divide una volta sola $p!$, e gli altri primi che dividono $p!$ sono più piccoli di p, si ha

$$p \mid |\,G : K\,| \mid \gcd(p!, |\,G\,|) = p,$$

dunque $|\,G : K\,| = p$, e dato che $K \le H$ si ha $K = H \trianglelefteq G$. □

6.11.3. ESERCIZIO. *Nel caso del Lemma, lo stabilizzatore della classe Hg è*

$$G_{Hg} = \{\, a \in G : Hga = Hg \,\} = \left\{\, a \in G : gag^{-1} \in H \,\right\} = g^{-1}Hg,$$

e il nucleo è

$$\bigcap \left\{\, g^{-1}Hg : g \in G \,\right\},$$

il più grande sottogruppo normale di G che sia contenuto in H.

Nel trattare i gruppi di ordine < 60, terremo conto innanzitutto dei seguenti fatti.

(1) Un gruppo di ordine 1, o di ordine un primo, è ciclico, e quindi abeliano
(2) Un gruppo G di ordine una potenza $p^n > p$ di un numero primo ha centro $Z(G) \neq \{\, 1 \,\}$. Se $a \in Z(G)$ è un elemento di ordine p, che esiste ad esempio per il Lemma di Cauchy, allora $\langle\, a \,\rangle$ è un sottogruppo normale di G diverso da $\{\, 1 \,\}$ e G.

(3) Un gruppo G di ordine pq, ove $p > q$ sono primi, ha un sottogruppo normale di ordine p.
(4) Un gruppo G di ordine p^2q, ove p, q sono primi distinti, ha un p-sottogruppo di Sylow normale, o un q-sottogruppo di Sylow normale.

Useremo i Teoremi di Sylow, e alcune volte il Lemma 6.9.1.

Comnciamo dunque a vedere gli ordini rimasti.

$|\,G\,| = 24$**.** Sia D un 2-sottogruppo di Sylow. Dato che D ha indice 3, per il Lemma 6.11.1 G ha un sottogruppo normale proprio di indice $\leq 3! = 6 < 24$, dunque proprio.

$|\,G\,| = 30$**.** Abbiamo visto che G ha sottogruppi normali di ordine $3, 5, 15$.

$|\,G\,| = 36$**.** Sia T un 3-sottogruppo di Sylow. Dato che T ha indice 4, per il Lemma 6.11.1 G ha un sottogruppo normale proprio di indice $\leq 4! = 24 < 36$, dunque proprio.

$|\,G\,| = 40$**.** Deve essere $n_5 = 1$, dunque un 5-sottogruppo di Sylow è normale.

$|\,G\,| = 42$**.** Deve essere $n_7 = 1$, dunque un 7-sottogruppo di Sylow è normale.

$|\,G\,| = 48$**.** Sia D un 2-sottogruppo di Sylow. Dato che D ha indice 3, per il Lemma 6.11.1 G ha un sottogruppo normale proprio di indice $\leq 3! = 6 < 48$, dunque proprio.

$|\,G\,| = 54$**.** Un 3-sottogruppo di Sylow ha indice 2, ed è quindi normale.

$|\,G\,| = 56$**.** Deve essere $n_7 = 1, 8$. Se fosse $n_7 = 8$, allora ci sono $6 \cdot 8 = 48$ elementi di ordine 7, e ne rimangono giusto 8 per un unico 2-sottogruppo di Sylow, che è dunque normale.

6.12. Gruppi semplici di ordine 60

Vogliamo far vedere che se G è semplice di ordine 60, allora $G \cong A_5$. (Ad ognuno dei passi seguenti, si può verificare che le condizioni trovate sono soddisfatte in A_5.)

Abbiamo $n_5 = 1, 6$, dunque $n_5 = 6$, $N_G(C)$ ha ordine 10, dove C è un 5-sottogruppo di Sylow. Ci sono dunque $6 \cdot 4 = 24$ elementi di ordine 5.

Abbiamo $n_3 = 1, 4, 10$. Se fosse $n_3 = 4$, allora $N_G(T)$, ove T è un 3-sottogruppo di Sylow, avrebbe indice 4, e dunque G avrebbe un sottogruppo normale proprio di indice ≤ 24. Dunque $n_3 = 10$, e ci sono $2 \cdot 10 = 20$ elementi di ordine 3.

n_2 può essere $1, 3, 5, 15$. Come al solito, 3 è troppo piccolo.

Per escludere 15, mostriamo che l'intersezione di due 2-sottogruppi di Sylow D_1, D_2 distinti è banale. Supponiamo che $D_1 \cap D_2 = A = \langle\, a \,\rangle$ abbia ordine 2. Allora $C_G(a)$ ha ordine un multiplo proprio di 4.

Se $C_G(a)$ ha ordine 20, allora ha indice 3, troppo basso. Se $C_G(a)$ ha ordine 12, sia T un 3-sottogruppo di Sylow di $C_G(a)$. Allora AT è un sottogruppo di $C_G(a)$ di indice 2, dunque normale in $C_G(a)$. Ma T è unico del suo ordine in AT, dunque è normale in $C_G(a)$, contro il fatto che $N_G(T)$ ha ordine 6.

Se dunque $n_2 = 15$, allora ci sono $3 \cdot 15 = 45$ elementi di ordine una potenza di 2, troppi tenendo conto che ho già contato $24 + 20$ elementi di ordine 3 e 5.

Dunque $n_2 = 5$, e se D è un 2-sottogruppo di Sylow, allora $N_G(D)$ ha ordine 12.

6.12.1. Osservazione (Il paragrafo seguente non gioca un ruolo nella dimostrazione). Mostriamo ora che D non è ciclico. Se fosse D ciclico, allora $N_G(D)$, di ordine 12, è prodotto semidiretto di D mediante T di ordine 3. Ma dato che $\gcd(\varphi(4), 3) = \gcd(2, 3) = 1$, $N_G(D)$ verrebbe abeliano, dunque $N_G(T)$ ha ordine almeno 12, una contraddizione.

Ora faccio agire G per coniugio sull'insieme Ω dei 2-sottogruppi di Sylow (ovvero equivalentemente, per il Teorema Orbita-Stabilizzatore, per moltiplicazione a destra sulle classi laterali di $N_G(D)$).

Questo mi fornisce un morfismo f di G in S_5. Dato che G agisce transitivamente su Ω, f non ha nucleo G, dunque il nucleo è 1, e f è iniettivo (in alternativa, $N_G(D)$ è un sottogruppo proprio, per il Lemma 6.11.1 il nucleo è un sottogruppo normale proprio di G, dunque per la semplicità di G il nucleo è 1, e di nuovo f è iniettivo.) L'immagine di f è dunque un sottogruppo di S_5 di ordine 60.

Affermo che l'unico sottogruppo di S_5 di ordine 60 è proprio A_5, e dunque $f(G) = A_5$, e f è un isomorfismo fra G e A_5.

Se, procedendo per assurdo, H fosse un altro sottogruppo di S_5 di ordine 60, e dunque di indice 2 e normale in S_5, allora $HA_5 > A_5$, e dunque $HA_5 = S_5$. (Questo perché

$$2 = |\, S_5 : A_5 \,| = |\, S_5 : HA_5 \,| \cdot |\, HA_5 : A_5 \,|$$

e dunque se $|\, HA_5 : A_5 \,| > 1$ deve essere $|\, S_5 : HA_5 \,| = 1$.) Ne segue che

$$2 = |\, S_5 : H \,| = |\, HA_5 : H \,| = |\, A_5 : H \cap A_5 \,|\,,$$

da cui seguirebbe che $H \cap A_5$ è un sottogruppo normale di A_5 di indice 2, contro la semplicità di A_5.

Un'alternativa un po' più laboriosa per vedere che $F(G) = A_5$, ma che illustra un argomento di qualche interesse, consiste nel mostrare che ogni elemento di G va sotto f in una permutazione pari. ne segue $f(G) \leq A_5$, e dunque $f(G) = A_5$, dato che G e A_5 hanno lo stesso ordine.

Chiaramente gli elementi di ordine 3 e 5 vanno in cicli della stessa lunghezza, e dunque pari. Resta solo da vedere che un 2-elemento vada in un elemento pari. Dato che D non è ciclico, ogni elemento $1 \neq x \in D$ è di ordine 2. Voglio vedere che $f(x) = (st)(uv)$, per s, t, u, v distinti, ovvero che $f(x)$ ha un unico punto fisso.

Sia $D^a = (D^a)^x = D^{ax}$, dunque $axa^{-1} \in N_G(D)$, ma x è un elemento di ordine 2, e D è l'unico 2-sottogruppo di Sylow di $N_G(D)$, dunque $x \in D \cap a^{-1}Da$, e l'unico punto fisso è D.

In alternativa, sia $N_G(D)ax = N_G(D)a$, dunque $axa^{-1} \in N_G(D)$. Dato che D è l'unico 2-sottogruppo di Sylow di $N_G(D)$, deve essere $axa^{-1} \in D$, ovvero $x \in D \cap a^{-1}Da$, e questo è possibile solo se $D = a^{-1}Da$, ovvero $a \in N_G(D)$, ovvero $N_G(D)a = N_G(D)$. Dunque l'unico punto fisso di $f(x)$ è $N_G(D)$.

Bibliografia

[Car13] A. Caranti, *Quasi-inverse endomorphisms*, J. Group Theory **16** (2013), no. 5, 779–792. MR 3101012

[CM19] A. Caranti and S. Mattarei, *Note di algebra per un corso da 12 crediti*, `http://www.science.unitn.it/~caranti/Didattica/Algebra/static/Note/Algebra.pdf`, 2019.

[Gor80] Daniel Gorenstein, *Finite groups*, second ed., Chelsea Publishing Co., New York, 1980. MR 569209

[Gou89] Edouard Goursat, *Sur les substitutions orthogonales et les divisions régulières de l'espace*, Ann. Sci. École Norm. Sup. (3) **6** (1889), 9–102. MR 1508819

[Gra97] Andrew Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276. MR 1483922

[HN52] Graham Higman and B. H. Neumann, *Groups as groupoids with one law*, Publ. Math. Debrecen **2** (1952), 215–221. MR 0057866 (15,284a)

[Hup67] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967. MR 0224703 (37 #302)

[Luc78a] Edouard Lucas, *Theorie des Fonctions Numeriques Simplement Periodiques*, Amer. J. Math. **1** (1878), no. 2, 184–196. MR 1505161

[Luc78b] ———, *Theorie des Fonctions Numeriques Simplement Periodiques*, Amer. J. Math. **1** (1878), no. 4, 289–321. MR 1505176

[Luc78c] ———, *Theorie des Fonctions Numeriques Simplement Periodiques. [Continued]*, Amer. J. Math. **1** (1878), no. 3, 197–240. MR 1505164

[Mac12] Antonio Machì, *Groups*, Unitext, vol. 58, Springer, Milan, 2012, An introduction to ideas and methods of the theory of groups. MR 2987234

[ML98] Saunders Mac Lane, *Categories for the working mathematician*, second ed., Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998. MR 1712872

[Rob96] Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR 1357169 (96f:20001)

[Rot95] Joseph J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR 1307623

[Ser16] Jean-Pierre Serre, *Finite groups: an introduction*, Surveys of Modern Mathematics, vol. 10, International Press, Somerville, MA; Higher Education Press, Beijing, 2016, With assistance in translation provided by Garving K. Luli and Pin Yu. MR 3469786