Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

p-Gruppi di ordine "piccolo"

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.
Marta Morigi
Correlatore:
Chiar.mo Prof.
Libero Verardi

Presentata da:
Pietro Gagliardo

II Sessione
2014/2015

Indice

Introduzione

Il concetto di gruppo è sicuramente una delle idee centrali della matematica e la teoria dei gruppi è uno dei rami più antichi dell'algebra moderna. Le sue origini si ritrovano nei lavori di Lagrange (1736-1813), Ruffini (1765-1822) e Galois (1811-1832) e riguardano la teoria algebrica delle equazioni. Tuttavia molte delle idee fondamentali della teoria dei gruppi sono state introdotte da questi primi matematici e dai loro successori, Cauchy (1789-1857), Sylow (1832-1918), Jordan (1838-1922) tra gli altri.
Il mio lavoro si concentrerà in principal modo sui p-gruppi *finiti*, vale a dire su quei gruppi che hanno un numero di elementi corrispondente ad una potenza di un numero primo p, spaziando prima nel concettualizzare le definizioni generali di *gruppo* e rappresentarne le proprietà generali, per poi sviluppare il significato di *p-gruppo* e darne una più chiara interpretazione tramite degli esempi, distinguendo i casi in cui ci si trova via via di fronte a gruppi abeliani e non, oppure a gruppi ciclici e non ciclici.
Verranno classificati i vari casi in cui la cardinalità del gruppo sia p^2, p^3 per concludere con i tre *Teoremi di Sylow* che sono molto utili per risolvere vari tipi di problemi di natura combinatoria riguardanti appunto i gruppi finiti e sottolineano l'importanza dello studio dei p-gruppi finiti, in quanto costituenti di tutti gli altri gruppi finiti; il primo teorema garantisce l'esistenza di sottogruppi di un gruppo finito aventi come ordine una potenza di un numero primo, il secondo teorema mette in risalto la relazione di coniugio tra i p-sottogruppi di Sylow dello stesso ordine, infine il terzo teorema mostra le proprietà di congruenza e divisibilità del numero dei p-sottogruppi che in alcuni casi particolari ci consentono di sapere con precisione il loro numero.
Infine si fa accenno al *teorema fondamentale sui gruppi abeliani finiti* che illustra in che modo i gruppi possono essere rappresentati tramite prodotto di p-gruppi ciclici e ci offre un modo per illustrare al meglio la *struttura* del gruppo.

Capitolo 1

Notazioni e Prerequisiti

1.1 Gruppi: alcune proprietà generali

Definizione 1.1 (Gruppo)**.** Un *Gruppo* è un monoide in cui ogni elemento è invertibile. Quindi sia $(G, *)$ un insieme dotato di operazione; è un gruppo se:

1. l'operazione è associativa;
2. $\exists\ 1_G$ tale che $a * 1_G = \ 1_G * a \ = a$, $\forall\ a \in G$;
3. $\forall\ a \in M \ \ \exists\ b \in G$ tale che $a * b = b * a = 1_M$.

Definizione 1.2 (Ordine di un gruppo)**.** Sia $(G, *)$ un gruppo *finito*, chiamiamo *ordine* di G la sua *cardinalità*, che si indica con $|G|$.

Definizione 1.3 (Sottogruppo)**.** Un *sottogruppo* $(S, *)$ di un gruppo G è un sottoinsieme non vuoto di G tale che sia esso stesso un gruppo rispetto alla *medesima operazione* di G, e si indica con $S \leq G$.
Quindi un sottoinsieme S di un gruppo G è un sottogruppo se e solo se:

1. $1_G \in S$;

2. S è chiuso rispetto all'operazione di G, ossia $\forall\ a, b \in S$ si ha $a * b \in S$;

3. S è chiuso rispetto agli inversi, ossia $\forall\ a \in S$, si ha che $a^{-1} \in S$.

Definizione 1.4 (Sottogruppo ciclico)**.** Sia X un sottoinsieme di G. Si definisce *Sottogruppo generato da* X il più piccolo sottogruppo di G contenente X e coincide con l'intersezione di tutti i sottogruppi di G che contengono X. Si indica con $\langle X \rangle$.

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H \tag{1.1}$$

.

Se $X = \{g\} \subseteq G$ allora $\langle g \rangle = \{\ g^i \mid i \in \mathbb{Z}\}$, che prende il nome di *sottogruppo ciclico* generato dall'elemento g.

Definizione 1.5 (Ordine di un elemento)**.** Se $(G, *)$ è un gruppo e $g \in G$, definiamo *ordine* o *periodo* di g il più piccolo intero positivo r, se esiste, tale che $g^r = 1_G$ e lo indichiamo con $o(g) = r$. Se tale intero non esiste allora diciamo che g ha *ordine* infinito.

Definizione 1.6. Un gruppo G si dice *ciclico* se esiste un elemento $g \in G$ tale che $G = \langle g \rangle$.

Proposizione 1.1.1. *Ogni sottogruppo di un gruppo G, ciclico, è anch'esso ciclico.*

Proposizione 1.1.2. *Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n, allora $\forall\ k$ tale che $k|n$ esiste uno e un solo sottogruppo di G che abbia ordine proprio k.*

Definizione 1.7 (classe laterale)**.** Sia $(G, *)$ gruppo e H sottogruppo. Definiamo la relazione di *congruenza destra* modulo H:

$$a\ \varrho_d\ b \longleftrightarrow a * b^{-1} \in H \tag{1.2}$$

e *congruenza sinistra* modulo H:

$$a\ \varrho_s\ b \longleftrightarrow b^{-1} * a \in H \tag{1.3}$$

che *ripartiscono* il gruppo G in *classi di equivalenza*:

$$Ha = \{h * a \mid h \in H\} \tag{1.4}$$

o, rispettivamente,

$$aH = \{a * h \mid h \in H\} \tag{1.5}$$

Proposizione 1.1.3. *Tutte le classi laterali del sottogruppo H hanno la stessa cardinalità, che è la stessa del sottogruppo H.*

Teorema 1.1.4 (Teorema di Lagrange)**.** *Sia G un gruppo finito e sia H un suo sottogruppo, allora l'ordine di H divide l'ordine di G.*

Corollario 1.1.5. *Un gruppo G che ha cardinalità un numero primo è un gruppo ciclico.*

Corollario 1.1.6. *Se G è un gruppo finito allora $\forall\ g \in G$ l'ordine di g divide l'ordine di G.*

Corollario 1.1.7. *Se $|G| = n$ allora $g^n = 1_G$, $\forall\ g \in G$.*

Definizione 1.8. Il *minimo* m tale che $\forall\ g \in G$, $g^m = 1_G$, si dice *esponente* di G. Questo è un divisore di $|G|$ ed è il *mcm* degli ordini degli elementi di G.

Definizione 1.9. Se ϱ è una relazione di equivalenza, è detta *compatibile* con l'operazione del gruppo G, se vale che:

$$g_1\ \varrho\ g_2, \quad g_3\ \varrho\ g_4 \quad \Longrightarrow \quad g_1 g_3\ \varrho\ g_2 g_4;$$

Proposizione 1.1.8. *Sia $H \leq G$, e siano ϱ_d e ϱ_s le relazioni di congruenza destra e sinistra modulo H, condizione necessaria e sufficiente affinché ϱ_d o ϱ_s siano compatibili con l'operazione è che valga:*

$$\varrho_d = \varrho_s \quad \textit{ossia} \quad Hx = xH \quad \forall\ x \in G$$

Definizione 1.10. Un sottogruppo H di un gruppo G si dice *normale* in G se $\forall\ x \in G$ vale:

$$Hx = xH. \tag{1.6}$$

e si scrive $H \lhd G$

Proposizione 1.1.9. *Sia G un gruppo e ϱ una relazione d'equivalenza compatibile con l'operazione. Allora il sottogruppo $H = \{x\ \in G |\ x\ \varrho\ 1_G\}$ è un sottogruppo normale di G e risulta che $\varrho\ =\ \varrho_d\ = \varrho_s$ modulo H.*

.

Definizione 1.11 (Gruppo abeliano)**.** Un gruppo G è abeliano se vale la proprietà *commutativa*.

Osservazione 1. Ogni sottogruppo di un gruppo *abeliano* G è *normale*.

Definizione 1.12 (Elementi coniugati)**.** Due elementi di un gruppo G si dicono *coniugati* se esiste $g \in G$ tale che:

$$y = gxg^{-1}. \tag{1.7}$$

Corollario 1.1.10. *Il coniugio è una relazione di equivalenza in G, infatti, $\forall\ x, y, z \in G$, posto $e = 1_G$:*

Dimostrazione. 1. è *riflessiva*: $\forall\ x \in G, \quad x = e^{-1}xe$;

2. è *simmetrica*: Se x è coniugato a y, cioè $y = g^{-1}xg$, moltiplicando a sinistra e a destra rispettivamente per g e g^{-1} otteniamo $gyg^{-1} = x$. Essendo $g \in G$ allora $\exists\ h \in G$ tale che $h = g^{-1}$ e $h^{-1} = g$; quindi sostituendo otteniamo $h^{-1}yh = x$, cioè y è coniugato a x;

3. è *transitiva*: se x è coniugato a y, allora $y = g^{-1}xg$; y è coniugato a z, allora $z = h^{-1}yh$; sostituendo la y nella seconda equazione otteniamo che:

$$z = h^{-1}g^{-1}xgh = (gh)^{-1}xgh$$

dove $gh \in G$, quindi x è coniugato a z.

□

Quindi esiste un partizione del gruppo G in classi di equivalenza dette *classi di coniugio*:

$$[x]_G = \{\ gxg^{-1} |\ g \in G\} \tag{1.8}$$

Definizione 1.13 (sottogruppo coniugato)**.** Sia $H \leq G$ chiamiamo *sottogruppo coniugato di H* l'insieme:

$$xHx^{-1} = \{\ xhx^{-1}\ |\ h \in H\}. \tag{1.9}$$

Si dimostra che xHx^{-1} è a sua volta un *sottogruppo* di G.

Osservazione 2. Si ha $xHx^{-1} = H, \forall\, x \in G$ se e solo se H è un sottogruppo normale.

Definizione 1.14 (gruppo quoziente)**.** Sia $H \lhd G$, definiamo *gruppo quoziente* l'insieme:

$$G/H = \{xH \mid x \in G\}. \tag{1.10}$$

con l'operazione:

1. $xH \cdot yH = xyH$, (che è *ben definita* se e solo se $H \lhd G$)
2. $1_{G/H} = H$
3. $(xH)^{-1} = x^{-1}H$

Osservazione 3. G/H lo si può rappresentare come l'insieme dei laterali, indifferentemente destri o sinistri di H in G.

Definizione 1.15 (Isomorfismo)**.** Definiamo *isomorfismo* una funzione f tra due gruppi $(G, *)$ *e* $(H, \cdot)$ tale che questa risulti *biettiva* e valga:

$$f(x * y) = f(x) \cdot f(y) \qquad \forall\, x,\ y \in G. \tag{1.11}$$

Definizione 1.16 (Automorfismo)**.** Sia G un gruppo. Un *automorfismo* di G è un *isomorfismo* di G in sé. Gli automorfismi costituiscono un gruppo rispetto alla composizione, denotato con $Aut(G)$

Definizione 1.17 (Automorfismo interno)**.** Le funzioni $T_g : G \longrightarrow G$, tali che $\forall\, x \in G$, $T_g(x) = gxg^{-1}$, sono automorfismi particolari, che definiamo *automorfismi interni.*

Definizione 1.18. Denotiamo l'insieme di tutti gli automorfismi interni di un gruppo G con $\mathcal{I}(G)$. Esso risulta essere un sottogruppo *normale* del gruppo $Aut(G)$.

Definizione 1.19 (Centro)**.** Sia G un gruppo. Chiamiamo *centro* del gruppo G l'insieme:

$$Z(G) = \{\ g \in G \mid gx = xg \quad \forall\, x \in G\} \tag{1.12}$$

Osservazione 4. Il *centro* è un sottogruppo *normale* di G e G è *abeliano* $\iff Z(G) = G$.

Si ha che $x \in Z(G) \iff [x]_G = \{x\}$, infatti, $\forall\, g \in G$:

$$gxg^{-1} = x \iff gx = xg \iff x \in Z(G).$$

Definizione 1.20 (centralizzante)**.** Sia G un gruppo. Definiamo *centralizzante* di un elemento $g \in G$ l'insieme degli elementi che *commutano* con l'elemento g stesso:

$$Z(g) = \{\ x \in G \mid gx = xg\} \tag{1.13}$$

dove $Z(g)$ è un sottogruppo di G.

Notiamo che esiste una relazione tra $|Z(g)|$ e la lunghezza della classe di coniugio di g. Si ha infatti, per i gruppi *finiti*:

$$|G| = |Z(g)| \cdot |[g]_G|$$

Dimostrazione. $\forall\, h = ygy^{-1} \in [g]_G$, consideriamo il laterale $Z(g)y$; la relazione che associa ad h il laterale $Z(g)y$ è una *biiezione* tra $[g]_G$ e $\{yZ(g) \mid y \in G\}$. Infatti $\forall\, y_1, y_2 \in G$ si ha: $y_1 g y_1^{-1} = y_2 g y_2^{-1} \iff (y_2^{-1}y_1)g(y_2^{-1}y_1)^{-1} = g \iff y_2^{-1}y_1 \in Z(g) \iff y_1 \in y_2 Z(g) \iff y_1 Z(g) = y_2 Z(g)$.
Questo verso $\Longrightarrow$ ci dice che la relazione è una *funzione*.
Quest'altro $\Longleftarrow$ ci dice che la funzione è *iniettiva*.
La suriettività è ovvia, quindi $|[g]_G| = |\{yZ(g) \mid y \in G\}| = |G|/|Z(g)|$, da cui l'asserto. In particolare, $|[g]_G|$ divide $|G|$. □

Nota 1. $Z(G) = \bigcap_{g \in G} Z(g)$.

Proposizione 1.1.11. *$G/Z(G)$ non può essere ciclico a meno che il gruppo non sia abeliano.*

Dimostrazione. Supponiamo per assurdo che $G/Z(G)$ sia ciclico e quindi generato da un elemento, quindi $G/Z(G) = \langle gZ(G)\rangle$. Fissiamo $a \notin Z(G)$ e sia $b \in G$ un elemento generico. Si ha che esistono $n, m \in \mathbb{N}$ tale che $aZ = g^n Z$ e $bZ = g^m Z$. Dunque esisteranno $z_1, z_2 \in Z(G)$ tale che $a = g^n z_1$ e $b = g^m z_2$. Risulta evidente che $ab = g^n z_1 g^m z_2 = g^m z_2 g^n z_1 = ba$, Quindi a commuta con b, $\forall b \in G$, e dunque $a \in Z(G)$ contro l'ipotesi che avevamo fatto inizialmente. Da ciò segue che $G/Z(G)$ è ciclico $\iff$ è banale. □

Infine,

Definizione 1.21. Dati due gruppi $(H, \star)$ e $(K, \cdot)$, Definiamo *prodotto diretto esterno* la struttura $(H \times K, *)$ dove sul loro prodotto cartesiano $H \times K$ definiamo *l'operazione* tale che:

1. $\forall\ h_1, h_2 \in H,\ \forall\ k_1, k_2 \in K,\ (h_1, k_1) * (h_2, k_2) = (h_1 \star h_2, k_1 \cdot k_2)$;
2. *l'unità* $1_{G\times H} = (1_H, 1_K)$;
3. *l'inverso* $(h, k)^{-1} = (h^{-1}, k^{-1})$.

Osservazione 5. Se H e K sono *abeliani* allora anche $H \times K$ è abeliano, e viceversa.

Proposizione 1.1.12. *Siano H e K due gruppi ciclici rispettivamente di ordine n e m. Allora $H \times K$ è ciclico se e solo se $MCD(n, m) = 1$.*

Inoltre, se G è un gruppo con due sottogruppi normali H, K tali che $H \cap K = \{1_G\}$ e $G = HK$, (ossia $\forall\ g \in G$, esistono $h \in H, k \in K$ tali che $g = hk$), allora G risulta isomorfo al prodotto diretto $H \times K$. Tale isomorfismo associa ad ogni g la coppia $(h, k) \in H \times K$ tale che $g = hk$. (Tale coppia si può dimostrare che è unica e che se $g_1 = h_1k_1$, $g_2 = h_2k_2$ allora $g_1g_2 = (h_1h_2)(k_1k_2)$).
G in tal caso si dice *prodotto diretto interno* di H e K.

Capitolo 2

p-gruppi

2.1 Concetto di p-gruppo, proprietà

In questo capitolo vedremo alcune proprietà dei gruppi finiti aventi per ordine la potenza di un *primo*. Il seguente teorema costituisce un premessa interessante.

Teorema 2.1.1 (Teorema di Cauchy)**.** *Sia G un gruppo tale che $|G| = n$ e sia p un numero primo tale che $p|n$. Allora esiste $g \in G$ tale che $g^p = 1_G$.*

Dunque l'*esistenza* di un elemento di *periodo p primo* ci garantisce che il sottogruppo da esso generato, $\langle g \rangle = P$, ha ordine p. Tale teorema ci conduce a poter definire i cosiddetti *p-gruppi*.

Definizione 2.1 (p-gruppo)**.** Sia p un numero *primo*. Si definisce *p-gruppo* un gruppo che ha come ordine una *potenza* di p.

Teorema 2.1.2. *Un gruppo finito G è un p-gruppo, con p primo $\iff$ ogni suo elemento ha per ordine una potenza di p.*

Dimostrazione. Sia $|G| = p^n \implies \forall\, x \in G$, $|x| = p^k$ con $k \leq n$, per il teorema di Lagrange. Viceversa, se $\forall\, x \in G$ la cardinalità di x è una potenza di p, allora non può esistere un primo $q \neq p$ che divida $|G|$, perché, per il teorema di Cauchy, in G ci sarebbe un elemento di ordine q. □

Sappiamo già che se $|G| = p$ allora G è ciclico, e c'è a meno di isomorfismi un solo gruppo d'ordine p. Il problema è studiare i gruppi di ordine p^α, con $\alpha > 1$.

Lemma 2.1.3. *Sia p un numero primo e $N \trianglelefteq G$.*

1. *Se G è un p-gruppo allora G/N è un p-gruppo;*

2. *Se N e G/N sono p-gruppi allora G è un p-gruppo*

Dimostrazione. 1. Essendo G un p-gruppo allora esiste un $h > 0$ per cui vale che $g^{p^h} = e$ $\forall g \in G$, con e elemento neutro di G. Sia p^n il periodo di g e consideriamo gN; avremo che $(gN)^{p^n} = g^{p^n}N = eN = N$. Quindi anche gN ha come periodo una potenza di p, per cui G/N è un p-gruppo.
2. Sia $gN \in G/N$, in quanto p-gruppo esiste $h > 0$ tale che $g^{p^h}N = (gN)^{p^h} = N$, quindi $g^{p^h} \in N$; essendo anche N un p-gruppo, esiste $k > 0$ tale che $(g^{p^{h+k}}) = (g^{p^h})^{p^k} = e$. Quindi per un generico $g \in G$ questo avrà come periodo una potenza di p e quindi anche G è un p-gruppo. □

Teorema 2.1.4. *Sia G un p-gruppo finito. Allora il centro $Z(G)$ è non banale.*

Dimostrazione. Supponiamo che G abbia ordine p^α, vale a dire $|G| = p^\alpha$ e consideriamo la partizione del gruppo G in *classi coniugate*. Per quanto visto nel capitolo precedente la cardinalità di ognuna di questa classi deve dividere l'ordine del gruppo G; ciò vuol dire che la cardinalità di ciascuna classe $[x]_G$ deve essere o 1 oppure un divisore di p^α, cioè deve essere una potenza di p. Sappiamo che il centro di G è costituito da tutti quegli elementi che commutano con ogni altro elemento di G e quindi è costituito da *tutte* quelle classi che possiedono solamente un elemento. Dunque se il centro $Z(G)$ fosse banale allora l'ordine di G sarebbe *congruo* a 1 modulo p che contraddice l'ipotesi che la cardinalità di G sia p^α. □

Corollario 2.1.5. *Sia G un gruppo di ordine p^n allora $\forall\, h \in \mathbb{N}, h < n$, esiste un sottogruppo normale di ordine p^h.*

Dimostrazione. Sia G un gruppo di ordine n e procediamo per induzione su n. Per $n = 0$ basta considerare il caso $G = \{e\}$. Per $n > 0$ considero il centro di G che è un p-sottogruppo non banale di G tale per cui p divide l'ordine del centro, quindi esiste

un elemento $g \in Z(G)$ tale che $p = |g|$. Si osserva che il sottogruppo generato da g è *normale* in G, così che $G/\langle g \rangle$ è un p-gruppo di ordine p^{n-1}. Per induzione, poiché $N \trianglelefteq G$ e $\langle g \rangle \leq N \iff N/\langle g \rangle \trianglelefteq G/\langle g \rangle$ il corollario risulta dimostrato perché per ogni $k < n-1$ esiste un sottogruppo normale di $G/\langle g \rangle$ di ordine p^k ove $|N| = p^{k+1}$ e $N \trianglelefteq G$. □

Osservazione 6. Per cui si può osservare che per un p-gruppo finito il *teorema di Lagrange* è invertibile

Lemma 2.1.6. *Un gruppo G è abeliano $\iff$ esiste H sottogruppo di $Z(G)$ tale che G/H sia ciclico.*

Teorema 2.1.7. *Un gruppo G di ordine p^2 è abeliano.*

Dimostrazione. Considerando che $Z(G)$ di G è non banale, allora il centro di G avrà cardinalità o p oppure p^2. Supponiamo che abbia cardinalità p e consideriamo $x \notin Z(G)$. Consideriamo il *centralizzante* di x, $Z(x) = \{g \in G \mid gx = xg\}$ che contiene *propriamente* $Z(G)$, cioè $Z(G) \subsetneq Z(x)$. Allora per il teorema di Lagrange deve coincidere con il gruppo G stesso, il che è un assurdo perché allora dovrebbe appartenere anche al centro di G. Nel caso in cui il centro abbia p^2 elementi coincide con il gruppo G stesso. Quindi G è in ogni caso *abeliano.* □

Considerando sempre un gruppo G finito di ordine p^2 possiamo dire ancora:

Proposizione 2.1.8. *Sia G un gruppo finito di ordine p^2 allora:*

1. *o G è ciclico, e in tal caso $G \cong \mathbb{Z}_{p^2}$*
2. *oppure G è isomorfo al prodotto diretto di due sottogruppi ciclici di ordine p, e in tal caso $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$*

Dimostrazione. Sia G un gruppo di ordine p^2. Se G è ciclico allora sarà isomorfo a $\mathbb{Z}_{p^2}$. Altrimenti, se G non è ciclico, consideriamo un elemento di G diverso dall'unità, $g \neq 1_G$. Per il teorema di Lagrange sappiamo che $o(g)|p^2$ con $o(g) \neq p^2$. Dunque $o(g)$ deve per forza essere uguale a p, vale a dire $|\langle g \rangle| = p$. Sia $h \in G - \langle g \rangle$, allora l'ordine di h dovrà essere anch'esso p. Consideriamo ora $H = \langle g \rangle\langle h \rangle = \{g^n h^m \mid n, m \in \mathbb{Z}\}$. Essendo G abeliano in quanto di ordine p^2, H è un sottogruppo di G e quindi $|H|||G|$ e H contiene

strettamente $\langle g \rangle$, dunque la cardinalità di H sarà maggiore di p e dovendo dividere p^2 non può che essere proprio uguale a p^2, cioè $H = G$.
Consideriamo ora l'applicazione

$$f : \langle g \rangle \times \langle h \rangle \longrightarrow G \tag{2.1}$$

$$(g^n, h^m) \longmapsto g^n h^m$$

Questo è un omomorfismo suriettivo di gruppi moltiplicativi, dove per ogni $(g^n, h^m) \in \langle g \rangle \times \langle h \rangle$ si ha:

$$(g^n, h^m) \in kerf \Longleftrightarrow g^n h^m = 1_G \Longrightarrow g^{-n} = h^m \Longrightarrow h^m \in \langle g \rangle$$

Supposti m e p coprimi, allora esistono $s, t \in \mathbb{Z}$ tali che $sp + tm = 1$. Dunque $h = h^{sp+tm} = (h^p)^s (h^t)^m \in \langle g \rangle$, che contraddice il modo in cui era stato scelto h. Dunque $p|m$ e allora $h^m = 1_G$ da cui $g^n = 1_G$. Quindi abbiamo provato che il nucleo di f è uguale a $\{(1_G, 1_G)\}$. Per cui f risulta essere un isomorfismo e $G = \langle g \rangle \times \langle h \rangle$. Poichè $\langle g \rangle \times \langle h \rangle = \mathbb{Z}_p \times \mathbb{Z}_p$ la tesi risulta essere verificata. □

2.2 Esempi

Nel caso sia $\alpha = 2$ e dunque $|G| = p^2$, sappiamo già essere abeliano. Dobbiamo distinguere i casi in cui il gruppo è ciclico e quando non lo è.

Consideriamo $p = 2$, allora in questo caso avremo un gruppo d'ordine *quattro*, e un gruppo di tale ordine o è ciclico o è di *Klein*, vale a dire un gruppo in cui ogni elemento al quadrato dà l'elemento neutro. Sappiamo già che l'ordine di un elemento deve dividere l'ordine del gruppo, quindi un elemento di G avrà ordine o due o quattro
Nel primo caso esiste un elemento di ordine *quattro*, quindi il gruppo G sarà generato da un elemento, cioè $G = \langle a \rangle = \{1, a, a^2, a^3\}$ che sarà isomorfo a $\mathbb{Z}_4 = \{[0], [1], [2], [4]\}$.
Nel secondo caso, se nessun elemento avrà ordine quattro, vuol dire che ogni elemento avrà ordine due, tranne l'unità. Quindi G non sarà ciclico e $\forall a \in G$ avremo che $o(a) = 2$, con $a \neq 1$. In questo caso qui risulterà $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ che prende il nome di

gruppo di Klein. Tale gruppo ha ordine quattro e contiene ben tre sottogruppi di ordine due: $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, $\langle(1,1)\rangle$, e fa parte dei cosiddetti *p-gruppi abeliani elementari*.

Considerando $p = 3$ otteniamo un gruppo G di cardinalità 9, e in tal caso distinguiamo due casi. Il primo in cui $G \cong \mathbb{Z}_{3^2} = \mathbb{Z}_9$, *ciclico* generato da tutti quegli interi *coprimi* con 9, vale a dire $G = \langle[1]\rangle = \langle[2]\rangle = \langle[4]\rangle = \langle[5]\rangle = \langle[7]\rangle$, ed ha un unico sottogruppo di ordine 3, precisamente $\langle[3]\rangle = \langle[6]\rangle$. Il secondo in cui $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, non *ciclico* in cui ogni sottogruppo del tipo $\langle(a,b)\rangle$, con $a, b \in \mathbb{Z}_3$ ha cardinalità 3. Anche questo gruppo fa parte dei cosiddetti *abeliani elementari*.
Identiche considerazioni si possono fare per $G \cong \mathbb{Z}_{5^2}$, *ciclico* con cardinalità 25, e $G \cong \mathbb{Z}_5 \times \mathbb{Z}_5$, *non ciclico* e *abeliano elementare*

Nel caso sia $\alpha = 3$ e dunque $|G| = p^3$; gli *unici* gruppi *abeliani* di tale ordine sono:

1. $G = \mathbb{Z}_{p^3} = \{a \in \mathbb{Z} \mid a^{p^3} = 1\} = \langle a \mid a^{p^3} = 1\rangle$ che è un gruppo *ciclico*;

2. $G = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p = \{(a,b,c) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \mid a^p = b^p = c^p = 1,\ ab = ba,\ ac = ca,\ bc = cb\} = (\mathbb{Z}_p)^3$, che è un gruppo *non ciclico*, ma è abeliano elementare;

3. e infine $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_p = \{(a,b) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_p \mid a^{p^2} = b^p = 1,\ ab = ba\}$ anch'esso non ciclico.

Non ce ne sono altri, infatti se $\exists g \in G$ tale che $|g| = p^3$, allora G è ciclico; se $\forall\ g \in G$, $|g| = p$, allora è abeliano elementare. Nell'ultimo caso, consideriamo un elemento $a \in G$, tale che $|\langle a\rangle| = p^2$ e prendiamo un $b \notin \langle a\rangle$. Se $|b| = p$ allora $G = \langle a\rangle \times \langle b\rangle$. Invece, se $|b| = p^2$ allora $\langle a\rangle \cap \langle b\rangle \neq \{1_G\}$, altrimenti si avrebbe che $|G| = p^4$. Quindi, sarà $\langle a\rangle \cap \langle b\rangle = \langle a^p\rangle = \langle b^p\rangle \Rightarrow a^p \in \langle b^p\rangle \Rightarrow \exists\ k$ tale che $a^p = (b^p)^k$, con $MCD(k,p) = 1$; avremo che $1_G = a^p(b^{pk})^{-1} = a^p(b^{-k})^p = (ab^{-k})^p$. Considerato $c = ab^{-k}$, $|c| = p$ e $c \notin \langle a\rangle$, avremo che $G = \langle a\rangle \times \langle c\rangle$ e siamo nel caso $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$.

Per quanto riguarda i gruppi *non abeliani*, consideriamo un caso particolare per $p = 2$, dunque $|G| = 8$. Prima

Definizione 2.2. Definiamo *Gruppo diedrale* D_n il gruppo dei movimenti rigidi che mutano in sé un poligono regolare di n lati.

Esso possiede n *rotazioni* attorno al centro del poligono, corrispondenti agli angoli: $k\frac{2\pi}{n}$, con $k = \{1, 2, \ldots, n\}$. Inoltre D_n possiede n *ribaltamenti* o *simmetrie assiali* rispetto agli n assi di simmetria del poligono, dove se n è dispari, questi assi di simmetria sono le bisettrici degli angoli del poligono, se invece $n = 2k$ è pari sono le k bisettrici e i k assi. In definitiva avremo che $|D_n| = 2n$.

Proposizione 2.2.1. *Sia r la rotazione di $2\pi/n$ attorno al centro di un poligono regolare e s un qualunque ribaltamento. Allora il gruppo diedrale D_n è generato da r e s e risulta:*

$$D_n = \langle r, s\rangle = \{id, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

Nel nostro caso prendiamo in esame il gruppo **diedrale** $G = D_4$, con $|D_4| = 8 = 2^3$. Avremo che:

$$D_4 = \langle r, s\rangle = \{id, r, s, r^2, rs, r^3, r^2s, sr\}.$$

dove, numerando i vertici del quadrato da 1 a 4 in senso antiorario, $r = (1234)$ rappresenta la rotazione di $\pi/2$ antioraria, mentre $s = (12)(34)$ la simmetria rispetto ad un asse. Tale gruppo contiene quattro rotazioni, di ampiezze $k\cdot 2\pi/4$, con $k = \{0, 1, 2, 3\}$, intorno all'origine, e quattro simmetrie assiali rispetto agli assi e alle diagonali.

Il gruppo D_4 presenta tre sottogruppi d'ordine 4, che risultano essere *normali*, in quanto la loro cardinalità divide a metà la cardinalità del nostro gruppo, e *abeliani*. Uno *ciclico*, generato dalla rotazione r:

$$\langle r\rangle = \{id, r, r^2, r^3\}.$$

e due non ciclici, corrispondenti rispettivamente ai gruppi di simmetria del rettangolo e del rombo:

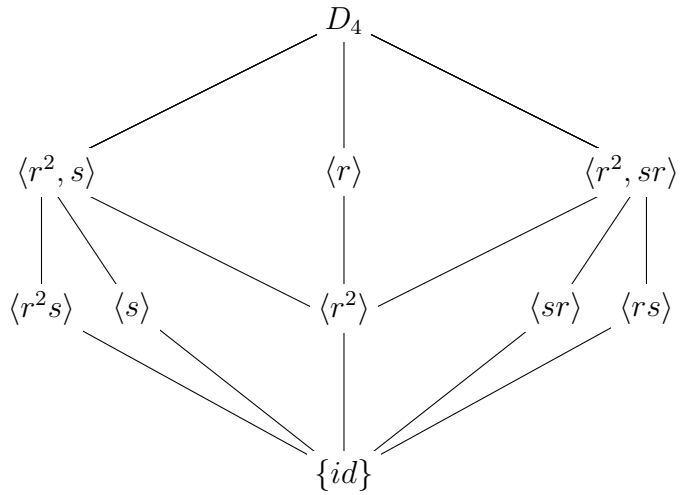
$$\langle r^2, s\rangle = \{id, r^2, s, r^2s\}.$$

$$\langle r^2, rs\rangle = \{id, r^2, rs, sr\}.$$

L'intersezione dei tre sottogruppi d'ordine 4 è il sottogruppo:

$$\langle r^2 \rangle \ = \ \{id, r^2\}.$$

i cui elementi commutano con tutti gli altri e rappresenta il *centro* del gruppo $Z(D_4)$, dove $|D_4/Z(D_4)| \ = \ 4$ e non è *ciclico*. Gli altri sottogruppi $\langle r^2 s \rangle$, $\langle s \rangle$, $\langle sr \rangle$, $\langle rs \rangle$ hanno ordine 2 e non sono normali in D_4. Questo è il diagramma:



Sempre per $p = 2$ possiamo considerare il gruppo dei *quaternioni*, definito in questo modo:

$$Q_8 \ = \ \{1, \ -1, \ i, \ j, \ k, \ -i, \ -j, \ -k\}$$

dove:

$$i^2 \ = \ j^2 \ = \ k^2 \ = -1$$

$$ij \ = \ k, \quad ji \ = \ -k$$

$$ik \ = \ -j, \quad ki \ = \ j$$

$$jk \ = \ i, \quad kj \ = \ -i$$

Tale gruppo è appunto non *abeliano* e generato da i, j, k e inoltre risulta essere il più piccolo gruppo non abeliano in cui tutti i sottogruppi sono normali(gruppi del genere prendono il nome di *hamiltoniani*).

Q_8 è chiuso rispetto al prodotto, che è ben definito, e lo si può rappresentare anche con 8 matrici di ordine 2 o sul campo complesso oppure sul campo $\mathbb{Z}_3$.
Supponiamo di volerlo rappresentare su $\mathbb{Z}_3$, allora definisco:

$$Q_8 = \left\{ \boldsymbol{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_3,\ ad - bc = 1 \right\}$$

e tale che $\forall\ A \in Q_8,\ A^4 = I_2$.
Siano:

$$\boldsymbol{a} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \qquad \boldsymbol{b} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \qquad \boldsymbol{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Notiamo che:
$a^2 = b^2 = (ab)^2$
$a^4 = b^4 = id$
$ba = (ab)^3$.

Dunque:

$$Q_8 = \{id,\ a,\ b,\ a^2,\ ba,\ a^3,\ ab,\ b^3\}$$

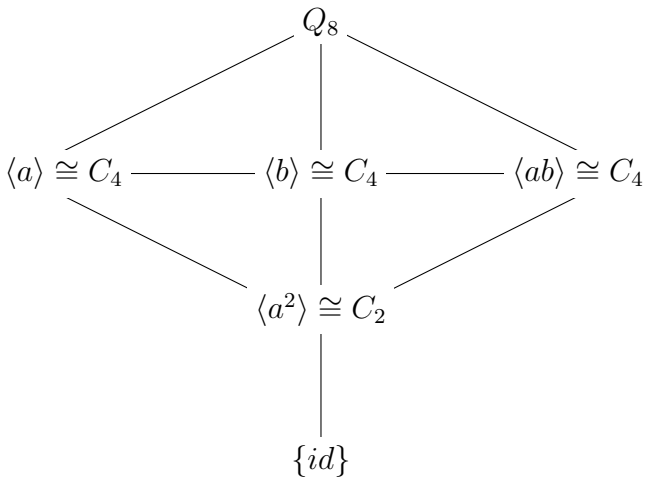
Tale gruppo ha un solo sottogruppo di ordine 2, costituito da $\{id,\ a^2\}$ e tre sottogruppi ciclici di ordine 4, ovvero:

$$\langle a \rangle = \{id,\ a,\ a^2,\ a^3\}$$

$$\langle b \rangle = \{id,\ b^2,\ a^2,\ b^3\}$$

$$\langle ab \rangle = \{id,\ a^2,\ ba,\ ab\}$$

Questi sono tutti sottogruppi normali, infatti il loro ordine è metà di quello del gruppo, e, insieme ai gruppi banali, id e Q_8 stesso, sono i soli sottogruppi di Q_8.
Il centro del gruppo è costituito dagli elementi id e a^2, che sono gli unici che commutano con tutti gli altri. Insieme ai gruppi banali, id e Q_8 stesso, sono gli unici sottogruppi di Q_8.
Detto C_k il gruppo ciclico d'ordine k il reticolo dei sottogruppi di Q_8 è il seguente:



Nel caso $p > 2$ possiamo illustrare due tipologie di gruppi *non abeliani*, uno in cui ogni elemento non banale del gruppo ha ordine p, e l'altro in cui esiste un elemento di ordine p^2.
Nel primo caso possiamo rappresentare il gruppo G nel modo seguente:

$$G = \left\{ \begin{pmatrix} \mathbf{1} & \boldsymbol{a} & \boldsymbol{b} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\},$$

dotato dell'operazione prodotto; ha ordine p^3 ed è appunto non abeliano.

L'espressione del prodotto di due matrici è data da

$$\begin{pmatrix} \mathbf{1} & \boldsymbol{a} & \boldsymbol{b} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{1} & \boldsymbol{x} & \boldsymbol{y} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{z} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \boldsymbol{a+x} & \boldsymbol{b+y+az} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{z+c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

Mentre l'inversa di una matrice $A = \begin{pmatrix} \mathbf{1} & \boldsymbol{a} & \boldsymbol{b} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$ è:

$$\boldsymbol{A^{-1}} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

Infatti, riprendendo l'espressione del prodotto

$$\begin{pmatrix} \mathbf{1} & \boldsymbol{a+x} & \boldsymbol{b+y+az} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{z+c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} = I_3 \iff \begin{cases} x+a=0 \\ y+az+b=0 \\ z+c=0 \end{cases} \iff \begin{cases} x=-a \\ y=ac-b \\ z=-c \end{cases}$$

Inoltre l'ordine di una generica matrice $A \in G$ è p, cioè $\forall\ A \in G$, $A^p = I_3$. Dimostriamolo per induzione su n:

$$A^2 = \begin{pmatrix} \mathbf{1} & \boldsymbol{2a} & \boldsymbol{2b+ac} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{2c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}, A^3 = \begin{pmatrix} \mathbf{1} & \boldsymbol{3a} & \boldsymbol{3b+3ac} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{3c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}, \ldots, A^n = \begin{pmatrix} \mathbf{1} & \boldsymbol{na} & \boldsymbol{nb+\binom{n}{2}ac} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{nc} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}.$$

Per $n = p$ allora:

$$A^p = \begin{pmatrix} \mathbf{1} & \boldsymbol{pa} & \boldsymbol{pb+\binom{p}{2}ac} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{pc} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

Il centro del gruppo è rappresentato da

$$Z(G) = \left\{ \begin{pmatrix} \mathbf{1} & \mathbf{0} & \boldsymbol{b} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \mid b \in \mathbb{Z}_p \right\}$$

Infatti verifica la condizione

$$\begin{pmatrix} \mathbf{1} & \boldsymbol{a} & \boldsymbol{b} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{1} & \mathbf{0} & \boldsymbol{z} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \boldsymbol{z} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{1} & \boldsymbol{a} & \boldsymbol{b} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{c} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

per ogni matrice $A \in G$.

Nel secondo caso, possiamo rappresentare G come un gruppo generato da due elementi, a e b, tali che $o(a) = p^2$ e $o(b) = p$, in questo modo:

$$G \;=\; \langle a, b \rangle \;=\; \{(a, b) \mid a^{p^2} = b^p = 1,\ ba^{p+1} = ab\}$$

Provando a costruire tale gruppo, prendiamo un elemento a tale che $|a| = p^2$, e prendiamo un elemento $b \notin \langle a \rangle$ e tale che $|b| = p$. Dobbiamo trovare un intero k che verifichi la condizione $b^{-1}ab = a^k$, dove k deve essere diverso da 1, altrimenti si avrebbe $ab = ba$ e quindi G sarebbe abeliano.
Verifichiamo che tale proprietà è verificata per $k = p + 1$, infatti:

$$a^{(p+1)^p} = a^{p^p + \binom{p}{1}p^{p-1} + \cdots + \binom{p}{p-1}p + 1} = a^{p^p} \cdot a^{\binom{p}{1}p^{p-1}} \cdot \ldots \cdot a^{\binom{p}{p-1}p} \cdot a$$

Notiamo che $\binom{p}{1}, \ldots, \binom{p}{p-1}$ sono tutti multipli di p, e $p^{p-1}, \ldots, p$ sono tutte potenze di p, quindi i loro prodotti sono multipli di $p^2 = |a|$, per cui

$$a^{p^p + \binom{p}{1}p^{p-1} + \cdots + \binom{p}{p-1}p + 1} = \underbrace{a^{p^p + \binom{p}{1}p^{p-1} + \cdots + \binom{p}{p-1}p}}_{=1} \cdot a = a$$

per cui abbiamo trovato un k che verifica la condizione $ba^k = ab$ e costruito il gruppo G generato da due elementi, dove $\langle a \rangle$ è normale in G e isomorfo a $\mathbb{Z}_{p^2}$ e $\langle b \rangle$ con cardinalità p.

Nota 2.
$b^{-1}ab = a^{p+1} \Longrightarrow \forall\ n,\ (b^{-1})^2 a (b)^2 \;=\; b^{-1}(a^{p+1})b \;=\; a^{(p+1)^2} \Longrightarrow\ b^{-n}ab^n \;=\; a^{(p+1)^n}$, (per induzione su n). Per $n = p$ si ha $b^p \;=\; 1$, quindi $b^{-p}ab^p \;=\; a$, ma, come visto, si ha anche $a^{(p+1)^p} \;=\; a$; quindi la condizione $ba^{p+1} \;=\; ab$ è ben posta. Il gruppo ottenuto è detto "prodotto semidiretto" di $\langle a \rangle$ per $\langle b \rangle$.
Si può dimostrare infine che ogni gruppo non abeliano di ordine p^3 è isomorfo ad uno di questi due gruppi di esponente p o p^2.

Capitolo 3

Conclusioni e Teoremi di Sylow

3.1 Teoremi di Sylow

Abbiamo visto con il teorema di *Lagrange* che ogni sottogruppo ha ordine un divisore dell'ordine del gruppo stesso. In questo capitolo vedremo se sia possibile "invertire" tale teorema, ovvero prendendo un intero positivo che divide l'ordine del gruppo, ci chiediamo sotto quali condizioni esiste un sottogruppo che abbia ordine quell'intero. Ciò in generale non vale, ma si ottengono significativi risultati se si studiano i numeri primi.

Definizione 3.1. Preso P un *p-sottogruppo* di un gruppo finito G, questo prende il nome di *p-sottogruppo di Sylow* se la sua cardinalità è la potenza *massima* di p che divide la cardinalità di G.

Enunciamo ora i teoremi di Sylow.

Teorema 3.1.1 (Primo teorema di Sylow)**.**
Sia G un gruppo finito e p un numero primo che divide l'ordine di G. Allora G ha un p-sottogruppo di Sylow.

A tal proposito enunciamo pure:

Proposizione 3.1.2. *Sia G un gruppo finito tale che la sua cardinalità sia mp^n e $MCD(p, m) = 1$. Allora nel gruppo G esistono p-sottogruppi di ordine $p, p^2, \ldots, p^n$.*

Da questo segue il teorema di *Cauchy* citato nel capitolo precedente: il sottogruppo d'ordine p è generato da un elemento d'ordine p.

Teorema 3.1.3 (Secondo teorema di Sylow)**.**
Sia G un gruppo finito tale che la sua cardinalità sia mp^n, allora:

1. *se H è un p-gruppo, con p^h elementi e $h < n$, allora è contenuto in un p-sottogruppo di Sylow;*

2. *due qualunque p-sottogruppi di Sylow di G sono coniugati.*

Teorema 3.1.4 (Terzo teorema di Sylow)**.**
Sia G un gruppo finito e p un primo che divide l'ordine di G. Se n_p è il numero dei p-sottogruppi di Sylow di G ed S è uno di questi p-sottogruppi, allora:

$$n_p | [G : S] \quad e \quad n_p \equiv 1 \ (mod\ p) \tag{3.1}$$

dove $[G : S]$ è il numero dei laterali destri (o sinistri) $= \frac{|G|}{|S|}$.
Questi teoremi sottolineano l'importanza dello studio dei p-gruppi, in quanto costituenti di tutti gli altri gruppi finiti.

3.2 Classificazione dei gruppi abeliani finiti

In questa sezione daremo un accenno e proveremo in parte il *teorema fondamentale sui gruppi abeliani finiti*, secondo cui dato comunque un intero positivo n, saremo in grado di stabilire quanti sono e chi sono i gruppi abeliani finiti di ordine n e allo stesso modo stabilire se gruppi abeliani dello stesso ordine sono isomorfi o meno.
Abbiamo già detto che un *p-gruppo* è un gruppo che ha come ordine un potenza di p e che ogni suo elemento ha ordine una potenza di p.

Osservazione 7. Nel caso finito si può definire *p-gruppo* un gruppo tale che ogni suo elemento ha come ordine una potenza di p, come visto nel capitolo precedente.

Teorema 3.2.1. *Sia G un gruppo abeliano finito. Per ogni primo p tale che $p||G|$ poniamo*

$$\Sigma_p = \{\ x \in G |\ x \text{ ha come ordine una potenza di } p\}$$

Allora

1. *ogni Σ_p è un sottogruppo di G (che è un p-sottogruppo di G);*
2. *G è prodotto diretto di tutti i Σ_p, al variare di p tra tutti i divisori primi di $|G|$.*

Dimostrazione. (cenno)
Avremo

$$\Sigma_p \ = \ \{x \in G \mid x^{p^s} = 1_G \text{ per qualche } s\}.$$

Considerando che G è abeliano, il primo punto è banale.
Per il secondo punto, sia $x \in G$ tale che $o(x) = n \mid |G|$. Sia $n \ = \ p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, con p_i distinti e $\alpha_i \geq 1$, per ogni $i \ = \ 1, \ldots, r$. Ponendo $q_i \ = \ n/(p_1^{\alpha_1})$ risulterà che $MCD(q_1, q_2, \ldots, q_r) = 1$. Esisteranno quindi k_i interi tali che

$$1 \ = \ k_1 q_1 + k_2 q_2 + \cdots + k_r q_r$$

Allora

$$x \ = \ x^1 \ = \ x^{k_1 q_1 + k_2 q_2 + \cdots + k_r q_r} \ = \ x^{k_1 q_1} x^{k_2 q_2} \cdots x^{k_r q_r}.$$

Ora, $(x^{q_i})^{p_i^{\alpha_i}} \ = \ x^n \ = \ 1$, $\forall\ i = 1, \ldots, r$; quindi $x^{q_i} \in \Sigma_{p_i} \Longrightarrow x^{q_i k_i} \in \Sigma_{p_i}$. Quindi ogni $x \in G$ si scrive come prodotto di elementi di Σ_{p_i}, cioè

$$G \ = \ \Sigma_{p_1} \Sigma_{p_2} \cdots \Sigma_{p_k}$$

□

Proseguendo otteniamo che $G \ = \ \Sigma_{p_1} \times \Sigma_{p_2} \times \cdots \times \Sigma_{p_k}$ dove

$$\Sigma_{p_i} \ = \ \{x \in G \mid x^{p_i^{s_i}} \ = \ 1_G \text{ per qualche } s_i\}$$

e ognuno dei Σ_{p_i} prende il nome di *componente primaria* di G

Provando a studiare i singoli fattori Σ_{p_i} vediamo che Σ_p risulta essere prodotto diretto di gruppi ciclici, infatti sussiste il seguente:

Teorema 3.2.2. *Sia Σ_p un p-gruppo abeliano finito. Allora Σ_p è un prodotto diretto di gruppi ciclici(di ordine una potenza di p)*

Dunque risulterà che

$$\Sigma_p \cong \langle s_1 \rangle \times \langle s_2 \rangle \times \cdots \times \langle s_t \rangle$$

Per cui ogni gruppo abeliano finito G è prodotto diretto di gruppi ciclici i cui ordini sono potenze dei primi che compaiono nella fattorizzazione di $n = |G|$.
Se $n = p_1^{\alpha_1} p_1^{\alpha_1} \cdots p_1^{\alpha_1}$, allora

$$G = \underbrace{\mathbb{Z}_{p_1^{a_{1,1}}} \times \mathbb{Z}_{p_1^{a_{1,2}}} \times \cdots \mathbb{Z}_{p_1^{a_{1,s}}}}_{\Sigma_{p_1}} \times \underbrace{\mathbb{Z}_{p_2^{a_{2,1}}} \times \mathbb{Z}_{p_2^{a_{2,2}}} \times \cdots \mathbb{Z}_{p_2^{a_{2,t}}}}_{\Sigma_{p_2}} \times \cdots \times \underbrace{\cdots}_{\Sigma_{p_k}}$$

dove gli interi $a_{i,j}$ sono tali che $\sum_j a_{i,j} = \alpha_i$ per ogni $i = 1, \ldots, k$, e sono ordinati in modo tale che $a_{i,j(i)} \geq \cdots a_{i,2} \geq a_{i,1} \geq 0$ e questi prendono il nome di *invarianti* di Σ_{p_i}; invece gli interi $p_i^{a_{i,j}}$ che compaiono nella decomposizione si chiamano *divisori elementari* di G.
Tali interi determinano univocamente il gruppo G e a loro volta sono univocamente determinati dal gruppo G, nel senso che due gruppi abeliani dello stesso ordine sono isomorfi se e solo se hanno gli stessi divisori elementari e gli stessi invarianti. Quanto detto, è il senso del *Teorema fondamentale sui gruppi abeliani finiti*, che spiega come tale fattorizzazione è unica, nel senso che se due gruppi abeliani finiti sono isomorfi, allora hanno gli stessi *divisori elementari*. In più ci offre quindi la *struttura* di tutti i gruppi abeliani finiti.

Quindi, dato un intero N, per contare quanti sono i gruppi abeliani che hanno N come ordine, si deve vedere in quanti modi si riesce a fattorizzare ogni Σ_p come prodotto di gruppi ciclici(di ordine potenze di p). Vale a dire si deve "contare" in quanti modi si può scrivere

$$\Sigma_p = \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_s}}.$$

Si deve avere

$$|\Sigma_p| = p^n = p^{n_1} p^{n_2} \cdots p^{n_s} = p^{n_1+n_2+\cdots+n_s}.$$

Quindi si tratta di contare in quanti modi si può scrivere n come somma di $n_1+n_2+\cdots+n_s$, con $n_1 \geq n_2 \geq \cdots \geq n_s$; tale numero coincide con il numero di partizioni di n, che lo indichiamo con $p(n)$. Dunque ogni Σ_p si può scrivere in $p(n)$ modi come prodotti di gruppi ciclici. Quindi procediamo fattorizzando per prima N come prodotto di potenze di primi distinti:

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

con $p_i^{\alpha_i} = |\Sigma_{p_i}|$. Successivamente si contano gli invarianti di ogni Σ_{p_i}, vale a dire contare il numero $p(\alpha_i)$ di partizioni di ogni α_i. Dunque il numero totale di gruppi abeliani non isomorfi di ordine $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ è dato da:

$$p(\alpha_1)p(\alpha_2)\cdots p(\alpha_k)$$

Per esempio, prendendo il *p-sottogruppo* Σ_2, questo ha cardinalità 4 e ha due diverse fattorizzazioni che sono:

$$\mathbb{Z}_{2^2} \qquad\qquad \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Inoltre per tali gruppi il *teorema di Lagrange* si "inverte", cioè:

Corollario 3.2.3. *Se m divide l'ordine di un gruppo abeliano finito G, allora G contiene un sottogruppo di ordine m.*

3.3 Funzione di Eulero

La *funzione di Eulero* $\varphi(n)$ è un funzione molto importante per quanto riguarda la teoria dei numeri, questa è definita come il numero degli interi compresi tra 1 ed n, $\forall\ n \in \mathbb{Z}^+$, che sono coprimi con n stesso e deve il suo nome al matematico *Leonhard Euler* che la descrisse per primo.
Riguardo la teoria dei numeri $\varphi(n)$ rappresenta la cardinalità del gruppo moltiplicativo degli interi di modulo n.
Ciò, combinato al teorema di Lagrange, dimostra il *teorema di Eulero*:

Teorema 3.3.1 (Teorema di Eulero)**.** *Se x è un numero coprimo con n allora:*

$$x^{\varphi(n)} \equiv 1 \ (mod\ n) \tag{3.2}$$

Un espressione formale della funzione è:

$$\varphi(n) = n \prod (1 - 1/p_i) \tag{3.3}$$

ove ogni p_i divide n e rappresentano tutti i *primi* che compongono la fattorizzazione di n.
Nel caso specifico sia $n = p^k$ avremo:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) \tag{3.4}$$

Dimostrazione. Per poter dimostrare l'equazione bisogna trovare tutti gli interi $n \leq p^k$ tale che $MCD(n, p^k) \neq 1$. Quindi n deve avere dei fattori in comuni con p^k; essendo p un numero primo allora la fattorizzazione di n deve contenere dei multipli di una potenza di p e tutti i possibili valori saranno $p, 2p, \ldots, p^{k-1}p$. Tutti questi non sono coprimi con p^k e saranno esattamente p^{k-1} valori. Notiamo che tutti i numeri minori o uguali a p^k sono proprio p^k e dunque i restanti numeri primi con p^k minori di p^k sono esattamente $p^k - p^{k-1}$.
Dunque avremo che $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$. □

Ciò vale $\forall\ k > 0$ in particolare quindi per $k = 2$:

$$\varphi(p^2) = p^2 - p = p(p-1). \tag{3.5}$$

Dove risulterà che $\varphi(p^2)$ è pari al numero dei generatori del gruppo ciclico D_{p^2} così come di $\mathbb{Z}_{p^2}$.

Si dimostra pure che se G è ciclico e la sua cardinalità è p^2 allora $|Aut(G)| = p(p-1) = \varphi(p^2)$.
Allora per il teorema di *Cauchy* esiste $f \in Aut(G)$, tale che $|f| = p$ e si ha, posto $G = \langle a \rangle$, $f(a) = a^{p+1}$ come visto nel capitolo precedente. La costruzione del gruppo d'ordine p^3 non abeliano e di esponente p^2 fa uso di questo automorfismo f, identificato col coniugio rispetto all'altro generatore b: $b^{-1}ab = f(a) = a^{p+1}$

Bibliografia

[1] A. Machì. *Introduzione alla Teoria dei Gruppi*. Feltrinelli, 1974.

[2] G. M. Piacentini Cattaneo. *Algebra. Un approccio algoritmico*. Zanichelli, 1996.

[3] D. J. S. Robinson. *A Course in the Theory of Groups*. Springer-Verlag, 1996.

[4] E. Sernesi. *Geometria I*, Bollati Boringhieri, Torino, 1989.

[5] A. Vistoli: *Note di Algebra*. Bologna, 1993/94