AL210 - Appunti integrativi - 4

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

Azioni di gruppi

Se G è un gruppo moltiplicativo con elemento neutro e e X è un insieme, un'*azione* di G su X è un'applicazione

$$\mathfrak{a} : G \times X \longrightarrow X\,; \quad (g, x) \mapsto g(x)$$

tale che:

(az1) $\mathfrak{a}(e, x) = e(x) = x$, per ogni $x \in X$;

(az2) $\mathfrak{a}(g, \mathfrak{a}(h, x)) = \mathfrak{a}(g, h(x)) = g(h(x)) = gh(x) = \mathfrak{a}(gh, x)$, per ogni $x \in X$ e g, $h \in G$.

Se G agisce su X e $x \in X$, l'insieme $St(x) := \{g \in G\,;\ g(x) = x\}$ si chiama lo *stabilizzatore* di x. Si vede facilmente che $St(x)$ è un sottogruppo di G. Se poi Y è un sottoinsieme di X, poniamo $St(Y) := \bigcap_{y \in Y} St(y)$ e diciamo che il gruppo $St(Y)$ è lo stabilizzatore di Y.

Dato $x \in X$, l'azione di G su X definisce anche l'insieme $\mathcal{O}(x) := \{g(x)\,;\ g \in G\}$. Questo sottoinsieme di X si chiama l'*orbita* di x.

Si dice che l'azione di G è *transitiva*, o che G *agisce transitivamente* o ancora che G è *transitivo* su X, se $\mathcal{O}(x) = X$ per ogni $x \in X$, cioè se esiste un'unica orbita. In altre parole, G è transitivo su X se comunque scelti x, $y \in X$, esiste $g \in G$ tale che $g(x) = y$.

Notiamo che per la proprietà (az2), se $y = g(x) \in \mathcal{O}(x)$, abbiamo $h(y) = (hg)(x) \in O(x)$ e quindi $\mathcal{O}(y) \subseteq \mathcal{O}(x)$. D'altra parte, se $y = g(x)$, allora $x = (g^{-1}g)x = g^{-1}(y) \in \mathcal{O}(y)$. Quindi, se $y \in \mathcal{O}(x)$ risulta $\mathcal{O}(y) = \mathcal{O}(x)$.

Proposizione 1. *Se G è un gruppo che agisce sull'insieme X, la famiglia delle orbite degli elementi di X costituisce una partizione di X.*

Dimostrazione. Poiché $x = e(x) \in \mathcal{O}(x)$, le orbite ricoprono X.

Se poi $x \in \mathcal{O}(y) \cap \mathcal{O}(z)$, allora $h(y) = x = g(z)$ per qualche h, $g \in G$; da cui $y = h^{-1}g(z) \in \mathcal{O}(z)$ (e $z = g^{-1}h(y) \in \mathcal{O}(y)$). Perciò $\mathcal{O}(y) = \mathcal{O}(z)$. □

Il gruppo $\mathcal{T}(X)$ delle applicazioni biunivoche di X in sé (o *trasformazioni* di X) agisce in modo naturale su X, tramite l'azione

$$\mathcal{T}(X) \times X \longrightarrow X\,; \quad (f, x) \mapsto f(x),$$

per ogni $f \in \mathcal{T}(X)$, $x \in X$.

Il prossimo risultato mostra che se G agisce su X, G individua un sottogruppo di $\mathcal{T}(X)$.

Proposizione 2. *Sia G un gruppo e sia $\mathfrak{a}$ un'azione di G sull'insieme X. Allora:*

(a) Per ogni $g \in G$, la corrispondenza

$$\varphi_g : X \longrightarrow X\,; \quad x \mapsto \mathfrak{a}(g,x) = g(x)$$

è biunivoca.

(b) L'applicazione

$$\psi : G \longrightarrow \mathcal{T}(X)\,; \quad g \mapsto \varphi_g$$

è un omomorfismo di gruppi.

Dimostrazione. (a) basta osservare che $\varphi_{g^{-1}}$ è l'applicazione inversa di φ_g.

(b) Segue dal fatto che $\varphi_{gh}(x) = gh(x) = g(h(x)) = \varphi_g\varphi_h(x)$, per ogni g, $h \in G$ e $x \in X$. □

Il nucleo dell'omomorfismo ψ definito nella Proposizione 2 (b) è dato dagli elementi $g \in G$ tali che $\psi(g) = id_X$, cioè tali che $g(x) = x$, per ogni $x \in X$; quindi $\mathrm{Ker}(\psi) = St(X)$ è lo stabilizzatore di X. Questo sottogruppo di G si chiama il *nucleo dell'azione*.

Si dice che l'azione di G su X è *fedele*, o che G *agisce fedelmente* su G, se il suo nucleo è banale, cioè se G è isomorfo ad un sottogruppo di $\mathcal{T}(X)$.

Poiché si ha un isomorfismo

$$\overline{\psi} : \frac{G}{St(X)} \longrightarrow \mathrm{Im}(\psi)\,, \quad gSt(X) \mapsto \varphi_g,$$

il gruppo quoziente $G/St(X)$ agisce fedelmente su X con l'azione definita da

$$(\frac{G}{St(X)}, X) \longrightarrow X\,; \quad (gSt(X), x) \mapsto g(x).$$

Esempi 3. **(1)** Se G agisce su X, anche ogni sottogruppo H di G agisce su X per *restrizione*. L'orbita di questa azione di H si chiama anche una H-orbita e verrà indicata con $\mathcal{O}_H(x)$.

In particolare, se A è una struttura algebrica, ogni gruppo di automorfismi di A, essendo un sottogruppo di $\mathcal{T}(X)$, agisce in modo naturale su A.

(2) Il gruppo delle permutazioni $\mathbf{S}_n$ agisce naturalmente su un insieme $X := \{1, \ldots, n\}$ con n elementi.

Un sottogruppo H di $\mathbf{S}_n$ si dice *transitivo* se la sua azione naturale su X è transitiva. Questo significa che, comunque scelti $i, j \in X$, esiste $\alpha \in H$ tale che $\alpha(i) = j$. Chiaramente $\mathbf{S}_n$ è transitivo.

Se $\sigma \in \mathbf{S}_n$ e $H := \langle\sigma\rangle$ l'H-orbita di un elemento $x \in X$ è $\mathcal{O}_H(x) = \{\sigma(x), \ldots, \sigma^m(x) = x\}$, dove m è l'ordine di σ. Quindi le orbite degli elementi di X corrispondono ai cicli disgiunti di σ.

(3) Se G agisce su X, allora G agisce anche sull'insieme $\mathcal{P}(X)$ delle parti (o dei sottoinsiemi) di X:

$$G \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)\,; \quad (g, Y) \mapsto g(Y) := \{g(y), y \in Y\}.$$

Se H è un sottogruppo di G, risulta

$$H \subseteq St(Y) \Leftrightarrow h(y) \in Y, \text{per ogni } h \in H \Leftrightarrow \mathcal{O}_H(Y) \subseteq Y.$$

Dunque $H \subseteq St(Y)$ se e soltanto se Y è unione di H-orbite.

(4) Ogni gruppo G agisce su se stesso per moltiplicazione sinistra

$$G \times G \longrightarrow G\,; \quad (g, x) \mapsto gx.$$

Poiché se $x \in G$ si ha $\mathcal{O}(x) = \{gx\,; g \in G\} = G$, l'azione è transitiva.

Inoltre $St(G) = \{g \in G\,;\ gx = x, \text{ per ogni } x \in G\}$ è il sottogruppo banale (e). Quindi l'azione è fedele e, per il Teorema 2(b), G è isomorfo ad un sottogruppo di $\mathcal{T}(G)$. Questa proprietà è stata dimostrata da A. Cayley, nel 1854.

(5) Anche ogni sottogruppo H di G agisce per moltiplicazione sinistra su G:

$$H \times G \longrightarrow G\,; \quad (h, x) \mapsto hx.$$

L'orbita di un elemento x rispetto a questa azione di H è $\mathcal{O}_H(x) := \{hx\,; h \in H\} = Hx$, cioè la classe laterale destra di x rispetto ad H. In questo modo, ritroviamo che le classi laterali destre di H formano una partizione di G (Proposizione 1).

(6) Se F è un campo, il gruppo $\mathbf{S}_n$, $n \geq 2$, agisce sull'anello dei polinomi in n indeterminate $F[\mathbf{X}] := F[X_1, \ldots, X_n]$ (e sul campo delle funzioni razionali $F(\mathbf{X})$) ponendo

$$\mathbf{S}_n \times F[\mathbf{X}] \longrightarrow F[\mathbf{X}]\,; \quad (\sigma, f(\mathbf{X})) \mapsto f^\sigma(\mathbf{X}) := f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

In questo caso, l'applicazione

$$\varphi_\sigma : F[\mathbf{X}] \longrightarrow F[\mathbf{X}]\,, \quad f(\mathbf{X}) \mapsto f^\sigma(\mathbf{X})$$

è un automorfismo e l'applicazione

$$\psi : \mathbf{S}_n \longrightarrow \mathrm{Aut}(F[\mathbf{X}])\,; \quad \sigma \mapsto \varphi_\sigma$$

è iniettiva. Quindi $\mathbf{S}_n$ agisce fedelmente (ma non transitivamente) su $F[\mathbf{X}]$.

Proposizione 4. *Sia G un gruppo che agisce sull'insieme X. Allora, per ogni $x \in X$, l'applicazione definita da*

$$gSt(x) \mapsto g(x)$$

è un'applicazione biiettiva tra l'insieme delle classi laterali sinistre dello stabilizzatore $St(x)$ e l'orbita $\mathcal{O}(x)$ di x.

In particolare, se G è finito, si ha $|\mathcal{O}(x)| = [G : St(x)]$ e

$$|G| = |\mathcal{O}(x)||St(x)|.$$

Dimostrazione. Basta osservare che $g(x) = h(x)$ se e soltanto se $g^{-1}h(x) = x$, cioè $g^{-1}h \in St(x)$. □

Il seguente corollario è immediato.

Corollario 5. *Se G agisce su X e $Y \subseteq X$, $g(y) = h(y)$ per ogni $y \in Y$ se e soltanto se $gSt(Y) = hSt(Y)$.*

Il coniugio e l'equazione delle classi

Ogni gruppo G agisce su se stesso per *coniugio* ponendo

$$G \times G \longrightarrow G\,; \quad (g, x) \mapsto g(x) := gxg^{-1}.$$

L'elemento gxg^{-1} si chiama il *coniugato* di x rispetto a g. L'orbita di $x \in G$ sotto questa azione si chiama la *classe di coniugio* di x e verrà indicata con $cl(x)$, perciò $cl(x) = \{gxg^{-1}\,;\ g \in G\}$. Dunque le classi di coniugio formano una partizione di G (Proposizione 1).

Lo stabilizzatore di x in G rispetto al coniugio si chiama il *centralizzante* di x e si indica con $C(x)$:

$$C(x) := \{g \in G\,;\ gxg^{-1} = x\} = \{g \in G\,;\ gx = xg\}.$$

Si verifica facilmente che l'applicazione

$$\gamma_g : G \longrightarrow G\,; \quad x \mapsto gxg^{-1}$$

è un automorfismo di G: esso si chiama l'*automorfismo interno definito da g*. Quindi, per la Proposizione 2(b), si ha un'omomorfismo di gruppi

$$\psi : G \longrightarrow \mathrm{Aut}(G) \subseteq \mathcal{T}(X)\,; \quad g \mapsto \gamma_g$$

il cui nucleo è lo stabilizzatore di G, ovvero l'intersezione di tutti i centralizzanti. Il nucleo di ψ si indica con $Z(G)$ e si chiama il *centro* di G:

$$Z(G) := \{g \in G\,;\ gx = xg,\ \text{per ogni } x \in G\}.$$

L'immagine di ψ, ovvero il sottogruppo di $\mathrm{Aut}(G)$ formato da tutti gli automorfismi interni di G, si denota con $\mathrm{Int}(G)$. Allora $\mathrm{Int}(G)$ è canonicamente isomorfo al gruppo quoziente $G/Z(G)$ ed agisce fedelmente su G ponendo

$$\mathrm{Int}(G) \times G \longrightarrow G\,; \quad (\gamma_g, x) \mapsto \gamma_g(x) = gxg^{-1}.$$

Notiamo che G è abeliano se e soltanto se $G = Z(G)$. Inoltre

$$cl(x) = \{x\} \quad \Leftrightarrow \quad G = C(x) \quad \Leftrightarrow \quad x \in Z(G).$$

Allora, se G è un gruppo finito e Λ è un sistema completo di rappresentanti delle classi di coniugio, si ha

$$\sum_{x \in \Lambda \cap Z(G)} |cl(x)| = |Z(G)|.$$

Da cui,

$$|G| = \sum_{x \in \Lambda} |cl(x)| = |Z(G)| + \sum_{x \in \Lambda \setminus Z(G)} |cl(x)|$$

ed usando la Proposizione 4

$$|G| = |Z(G)| + \sum_{x \in \Lambda \setminus Z(G)} [G : C(x)].$$

Quest'ultima espressione viene chiamata l'*Equazione delle Classi* di G.

Esempi 6. (1) Se $\sigma := (a_1, \ldots, a_m) \in \mathbf{S}_n$ è un m-ciclo, risulta $\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_m))$. Quindi due permutazioni sono coniugate se e soltanto se hanno la stessa struttura ciclica.

(2) Verifichiamo l'equazione delle classi per il gruppo $\mathbf{A}_5$. Notiamo che i 5-cicli di $\mathbf{S}_5$ si ripartiscono in due classi di coniugio in $\mathbf{A}_5$. Infatti essi sono tutti coniugati in $\mathbf{S}_5$ ed il loro numero è $5!/5 = 24$. Quindi il centralizzante in $\mathbf{S}_5$ di un 5-ciclo σ, avendo ordine 5, è $C(\sigma) = \langle\sigma\rangle$. Poiché $C(\sigma) \subseteq \mathbf{A}_5$ ed ha indice 12 in $\mathbf{A}_5$, i coniugati di σ in $\mathbf{A}_5$ sono 12. I 3-cicli di $\mathbf{S}_5$ sono $5!/3 = 20$ e sono tutti coniugati in $\mathbf{S}_5$. Quindi il centralizzante in $\mathbf{S}_5$ di un 3-ciclo γ è un sottogruppo $C(\gamma)$ di ordine 6, necessariamente isomorfo a $\mathbf{S}_3$. Ne segue che il centralizzante di γ in $\mathbf{A}_5$ è $C(\gamma) \cap \mathbf{A}_5 = \langle\gamma\rangle$. Poiché $\langle\gamma\rangle$ ha indice 20 in $\mathbf{A}_5$, i 3-cicli sono tutti coniugati in $\mathbf{A}_5$. In modo analogo si vede che gli elementi di $\mathbf{A}_5$ del tipo $(ab)(cd)$, che sono 15, sono tutti coniugati in $\mathbf{A}_5$. Infine l'identità è autoconiugata. In definitiva, l'equazione delle classi per $\mathbf{A}_5$ dice che

$$60 = |\mathbf{A}_5| = 12 + 12 + 20 + 15 + 1.$$

Ricordiamo che il gruppo alterno $\mathbf{A}_5$ è isomorfo al gruppo delle isometrie dell'icosaedro (o *gruppo icosaedrale*). L'icosaedro ha 20 facce triangolari, 30 spigoli e 12 vertici: ai 24 5-cicli di $\mathbf{A}_5$ corrispondono le rotazioni dell'icosaedro il cui asse passa per un vertice, ai 20 3-cicli le rotazioni il cui asse passa per il centro di una faccia ed infine agli elementi di tipo $(ab)(cd)$ le rotazioni il cui asse passa per il punto medio di uno spigolo. Inoltre, per dualità, $\mathbf{A}_5$ è anche isomorfo al gruppo delle isometrie del dodecaedro.

Un gruppo G agisce per coniugio anche sull'insieme dei suoi sottogruppi, ponendo

$$g(H) := \gamma_g(H) = gHg^{-1} := \{ghg^{-1}\,;\ h \in H\},$$

per ogni sottogruppo $H \subseteq G$. Lo stabilizzatore di H si chiama il *normalizzante* di H in G, esso è il sottogruppo

$$N(H) := \{g \in G\,;\ gHg^{-1} = H\}.$$

Per definizione, un sottogruppo H di G è normale in G se $gHg^{-1} = H$, per ogni $g \in G$, cioè se $N(H) = G$. In generale $N(H)$ è il più grande sottogruppo di G in cui H è normale.

Proposizione 7. *Sia H un sottogruppo del gruppo G e sia $N(H)$ il suo normalizzante. Allora*

(a) $H \subseteq N(H)$ e H è normale in $N(H)$;

(b) Se H' è un sottogruppo di G contenente H e H è normale in H', allora $H' \subseteq N(H)$;

(c) Se G è finito, il numero dei sottogruppi di G coniugati ad H è uguale all'indice del normalizzante $[G : N(H)]$.

Dimostrazione. (a) e (b) seguono direttamente dalla definizione di $N(H)$. (c) segue dalla Proposizione 4. □

Per finire mostriamo che, data una qualsiasi azione di G su X, gli stabilizzatori di due elementi che appartengono alla stessa orbita sono coniugati.

Proposizione 8. *Sia G un gruppo che agisce sull'insieme X. Allora, per ogni $g \in G$ e $x \in X$, si ha*

$$S(gx) = gSt(x)g^{-1}.$$

Dimostrazione. Sia $h \in St(x)$. Allora $ghg^{-1}(g(x)) = g(x)$; quindi $gSt(x)g^{-1} \subseteq S(gx)$. Viceversa, se $s(g(x)) = sg(x) = g(x)$, si ha $g^{-1}sg \in St(x)$ e quindi $s \in gSt(x)g^{-1}$. □

Esempi 9. (1) Se $N(H)$ è il normalizzante di H di G, per ogni $g \in G$, risulta $N(gHg^{-1}) = gN(H)g^{-1}$.

p-gruppi finiti

Se $p \geq 2$ è un numero primo, un gruppo di ordine uguale ad una potenza di p si chiama un *p-gruppo finito*. Usando l'Equazione delle Classi, possiamo ottenere utili informazioni su questi gruppi.

Proposizione 10. *Un p-gruppo finito ha centro non banale.*

Dimostrazione. Sia G un p-gruppo finito. Se G è abeliano, allora $G = Z(G)$. Se no, esistono rappresentanti delle classi di coniugio che non appartengono a

$Z(G)$. Per tali elementi g, l'indice del centralizzante $[G : C(g)]$ è diverso da 1 e quindi è diviso da p. Consideriamo l'equazione delle classi di G:

$$|G| = |Z(G)| + \sum_{g \in \Lambda \setminus Z(G)} [G : C(g)],$$

dove al solito Λ è un sistema completo di rappresentanti per le classi di coniugio di G. Poiché p divide $|G|$ e divide anche tutti gli addendi $[G : C(g)]$ in cui $g \in \Lambda \setminus Z(G)$, allora p divide $|Z(G)|$, cioè $Z(G) \neq \langle e \rangle$. □

Corollario 11. *Un p-gruppo di ordine p^2 è abeliano.*

Dimostrazione. Per la Proposizione 10, $Z(G) \neq \langle e \rangle$. Se $Z(G) \neq G$, allora $|Z(G)| = p$. D'altra parte, dato $g \in G \setminus Z(G)$, si ha $G \supsetneq C(g)$ e dunque anche $|C(g)| = p$. Questo è impossibile perché $C(g) \supsetneq Z(G)$. □

I teoremi di Sylow

Il Teorema di Lagrange per i gruppi finiti asserisce che l'ordine di ogni sottogruppo divide l'ordine del gruppo. Ma, se d è un divisore positivo dell'ordine del gruppo, non esistono necessariamente sottogruppi di ordine d.

Esempi 12. Il gruppo alterno $\mathbf{A}_4$ ha ordine 12 ma non ha sottogruppi di ordine 6. Infatti, si osservi che $\mathbf{A}_4$ contiene tutti i 3-cicli di $\mathbf{S}_4$, che sono 8. Dunque un eventuale suo sottogruppo H di ordine 6 non può contenere tutti i 3-cicli. D'altra parte H, avendo indice 2, è normale in $\mathbf{A}_4$. Allora si può scrivere $\mathbf{A}_4/H = \{H, aH\}$, dove a è un 3-ciclo che non sta in H. Poiché la classe aH ha ordine 2, si ha che $(aH)^2 = a^2H = H$. Dunque $a^2 = a^{-1} \in H$. Poiché H è un gruppo e $a \notin H$, questo è impossibile.

Nel seguito di questo paragrafo daremo alcune condizioni di sufficienza affinché un gruppo finito abbia un sottogruppo di un certo ordine ammissibile. In particolare mostreremo che ogni gruppo finito ha un p-sottogruppo massimale per ogni divisore primo p del suo ordine. Questo risultato, che è fondamentale nella Teoria dei Gruppi finiti, è stato dimostrato da L. Sylow nel 1872. Nel 1845, A. L. Cauchy aveva precedentemente dimostrato che, se p divide l'ordine di G, allora G ha almeno un elemento, e quindi un sottogruppo, di ordine p.

Lemma 13. *Sia X un insieme con $n := p^s m$ elementi, dove $s \geq 1$ e p è un primo che non divide m. Il numero dei sottoinsiemi di X che hanno p^s elementi è il coefficiente binomiale*

$$N := \binom{n}{p^s} = \frac{n(n-1)\dots(n-k)\dots(n-p^s+1)}{p^s(p^s-1)\dots(p^s-k)\dots 1};$$

inoltre p non divide N.

Dimostrazione. È noto che il numero dei sottoinsiemi di X con p^s elementi è N.

Per mostrare che p non divide N, osserviamo che se p divide il fattore $(n-k)$ del numeratore, allora p divide k e quindi divide anche il fattore (p^s-k) del denominatore. Inoltre scrivendo $k = p^e h$, con p che non divide h, si ha che $e < s$. Quindi p^e divide sia $(n-k)$ che (p^s-k), ma p^{e+1} non li divide. In conclusione, p non divide N. □

Teorema 14 (Primo Teorema di Sylow, 1872)**.** *Sia G un gruppo finito di ordine $p^s m$, dove $s \geq 1$ e p è un primo che non divide m. Allora G ha un sottogruppo di ordine p^s.*

Dimostrazione. Sia $\mathcal{X}$ l'insieme dei sottoinsiemi di G che hanno p^s elementi. Dimostriamo che uno di questi sottoinsiemi è un sottogruppo.

Facciamo agire G su $\mathcal{X}$ per moltiplicazione sinistra:

$$G \times \mathcal{X} \longrightarrow G\,; \quad (g, Y) \mapsto gY.$$

Poiché le orbite $\mathcal{O}$ di questa azione formano una partizione di $\mathcal{X}$ (Proposizione 1), si ha $N = |\mathcal{X}| = \sum |\mathcal{O}|$. Siccome poi p non divide N, p non divide l'ordine di qualche orbita $\mathcal{O}$. Supponiamo che $\mathcal{O} = \mathcal{O}(U)$ sia l'orbita del sottoinsieme U di G e sia $St(U)$ lo stabilizzatore di U.

Osserviamo ora che $|St(U)|$ divide $|U| = p^s$ e quindi è una potenza di p. Infatti, posto $H := St(U)$, come visto nell'Esempio 3(3), U è unione disgiunta di H-orbite rispetto alla moltiplicazione sinistra, ma una H-orbita è una classe laterale destra di H (Esempio 3(5)) e quindi ha la stessa cardinalità di $H := St(U)$. Ne segue che che $|St(U)|$ divide $|U|$.

Per la Proposizione 4, otteniamo $p^s m = |G| = |St(U)||\mathcal{O}(U)|$, dove $|St(U)|$ è una potenza di p e p non divide $|\mathcal{O}(U)|$. Quindi $|St(U)| = p^s$ e perciò $St(U)$ è il sottogruppo cercato. □

Se $|G| = p^s m$, dove $s \geq 1$ e p è un primo che non divide m, un sottogruppo di G di ordine p^s, esistente per il Teorema 14, si chiama un *p-sottogruppo di Sylow*, o semplicemente un *p-Sylow* di G.

Sylow dimostrò importanti proprietà di questi sottogruppi, utili ad esempio per studiare la classificazione e la struttura dei gruppi finiti. Per completezza enunciamo quelli che vanno sotto il nome di Secondo e Terzo Teorema di Sylow.

Teorema 15 (Secondo Teorema di Sylow)**.** *Sia G un gruppo finito. Allora*

(a) *Ogni p-sottogruppo di G è contenuto in un p-sottogruppo di Sylow;*

(b) *Tutti i p-sottogruppi di Sylow di G sono coniugati.*

Teorema 16 (Terzo Teorema di Sylow)**.** *Sia G un gruppo finito di ordine $p^s m$, dove $s \geq 1$ e p è un primo che non divide m. Allora il numero dei p-sottogruppi di Sylow di G divide m ed è congruo a 1 modulo p.*

Esempi 17. (1) Poiché tutti i p-Sylow di un gruppo G sono coniugati, il loro numero uguaglia l'indice del normalizzante di uno qualsisi di essi (Proposizione 4).

(2) Il gruppo $\mathbf{S}_4$ ha ordine $24 = 2^3 3$. Esso ha perciò 4 3-Sylow, ciclici di ordine 3, e 3 2-Sylow, diedrali di ordine 8. Il normalizzante del 3-Sylow $\langle (abc) \rangle$ ha ordine 6, quindi è il sottogruppo $\langle (abc), (ab) \rangle$, isomorfo ad $\mathbf{S}_3$. Il normalizzante di un 2-Sylow H ha ordine 8 e quindi coincide con H.

(3) I p-Sylow di $\mathbf{S}_p$ sono tutti e soli i sottogruppi di ordine p; il loro numero è $(p-2)!$.

Notiamo che questi p-Sylow sono ciclici e tutti tra loro coniugati (Secondo Teorema di Sylow). Poiché un p-ciclo genera un p-Sylow, ogni elemento di ordine p di $\mathbf{S}_p$ è un p-ciclo.

(4) Un gruppo abeliano ha un unico p-Sylow, per ogni divisore primo p del suo ordine. Infatti tutti i sottogruppi di un gruppo abeliano sono normali e quindi autoconiugati.

Corollario 18 (L. Cauchy, 1845)**.** *Sia G un gruppo finito. Se p è un primo che divide l'ordine di G, allora G ha un elemento, ovvero un sottogruppo ciclico, di ordine p.*

Dimostrazione. Sia H un p-Sylow di G e sia $x \in H$. L'ordine di x è uguale a una potenza p^n. Se $n \geq 2$, allora $x^{p^{n-1}}$ è un elemento di G di ordine p. □

Corollario 19. *Un p-gruppo G di ordine p^n, $n \geq 1$, ha un sottogruppo G_k di ordine p^k per $k = 0, \ldots, n$. Inoltre G_k è normale in G_{k+1} per $0 \leq k < n$.*

Dimostrazione. Procediamo per induzione su k. Se $k = 1$, allora il sottogruppo cercato è $H := \langle e \rangle$. Sia allora $k > 1$ e supponiamo che l'asserzione sia vera per i gruppi di ordine p^{k-1}.

Per la Proposizione 10, il centro $Z(G)$ è non banale; dunque $Z(G) \neq \langle e \rangle$ ha ordine p^s con $1 \leq s \leq k-1$. Per il Teorema di Cauchy, $Z(G)$ ha un sottogruppo N di ordine p e questo è un sottogruppo normale di G (perché $gn = ng$ per ogni $g \in G$ e $n \in N \subseteq Z(G)$). Consideriamo il gruppo quoziente G/N. Questo gruppo ha ordine p^{k-1}, perciò ha un sottogruppo normale di ordine p^{k-2} per l'ipotesi induttiva. Tale sottogruppo è della forma H/N, dove H è un sottogruppo normale di G ed inoltre $|H| = |H/N||N| = p^{k-2}p = p^{k-1}$. Dunque H è il sottogruppo cercato. □

Corollario 20. *Sia G un gruppo finito. Se p è primo e p^k divide l'ordine di G, $1 \leq k$, G ha un sottogruppo di ordine p^k.*

Dimostrazione. Segue dal Primo Teorema di Sylow (Teorema 14) e il Corollario 19. □

Gruppi abeliani finiti

Vogliamo mostrare in questo paragrafo che ogni gruppo abeliano finito è prodotto diretto di p-gruppi ciclici, il cui ordine è univocamente determinato.

Prima dimostriamo che il Teorema di Lagrange "si inverte" per i gruppi abeliani.

Proposizione 21. *Sia G un gruppo abeliano finito di ordine $n \geq 2$. Se m è un divisore positivo di n, allora G ha un sottogruppo di ordine m.*

Dimostrazione. Procediamo per induzione sull'ordine di G. Se $|G| = 2$, il teorema è trivialmente vero. Sia dunque $|G| > 2$ e supponiamo che il teorema sia vero per ogni gruppo abeliano di ordine strettamente minore di $|G|$. Consideriamo un divisore primo p di m. Allora p divide $|G|$ e, per il Teorema di Cauchy, G ha un sottogruppo H di ordine p. Il gruppo quoziente G/H è abeliano e ha ordine strettamente minore di $|G|$. Inoltre m/p divide tale ordine. Perciò, per l'ipotesi induttiva, G/H ha un sottogruppo di ordine m/p. Questo sottogruppo è della forma K/H, dove K è un sottogruppo di G e, poiché $|K| = |K/H||H| = (m/p)p = m$, K è il sottogruppo cercato. □

Ogni gruppo abeliano finito ha un unico p-sottogruppo di Sylow, per ogni divisore p del suo ordine (Esempio 17(4)). Questo sottogruppo è un p-gruppo abeliano, che è costituito da tutti gli elementi di G di ordine uguale ad una potenza di p e che si chiama la *p-esima componente* del gruppo. Mostriamo che un gruppo abeliano finito è prodotto diretto delle sue p-esime componenti.

Lemma 22. *Sia G un gruppo abeliano di ordine $n = ab$, con $\mathrm{MCD}(a, b) = 1$. Allora G è prodotto diretto di due sottogruppi di ordine a e b rispettivamente. Inoltre G è ciclico se e soltanto se questi due sottogruppi sono ciclici.*

Dimostrazione. Siano H e K due sottogruppi di G di ordine a e b rispettivamente, esistenti per la Proposizione 21. Se $\mathrm{MCD}(a, b) = 1$, si ha che $H \cap K = \{e\}$ e quindi che il sottogruppo HK di G ha ordine $ab = n$. Perciò $G = HK$ è prodotto diretto di H e K.

Se H e K sono ciclici, generati da x e y rispettivamente, il prodotto xy ha ordine ab (perché $xy = yx$) e genera $G = HK$. Viceversa, se G è ciclico, anche tutti i suoi sottogruppi lo sono. □

Proposizione 23. *Ogni gruppo abeliano finito è il prodotto diretto delle sue p-esime componenti.*

Dimostrazione. Sia $n = p_1^{e_1} \dots p_m^{e_m}$ l'ordine di G, dove $p_1, \dots, p_m$ sono numeri primi distinti. Indichiamo con P_i la p_i-esima componente di G, $i = 1, \dots, m$. Poiché P_1 ha ordine $p_1^{e_1}$ e $\mathrm{MCD}(n/p_1^{e_1}, p_1^{e_1}) = 1$, per il Lemma 22, G è prodotto diretto di P_1 ed un sottogruppo H_1 di ordine $n_1 := n/p_1^{e_1}$. Dal momento che $P_2 \subseteq H_1$ è anche la p_2-esima componente di H_1 e $\mathrm{MCD}(n_1/p_2^{e_2}, p_2^{e_2}) = 1$, proseguendo in questo modo si ottiene che G è prodotto diretto dei suoi sottogruppi P_i. □

Corollario 24. *Ogni gruppo abeliano il cui ordine è un prodotto di numeri primi distinti è ciclico.*

Dimostrazione. Le p-sime componenti di G hanno ordine primo e perciò sono gruppi ciclici. Allora G, come prodotto diretto di gruppi ciclici di ordini coprimi è ciclico (Lemma 22 e Proposizione 23). □

Per la proposizione 23, per conoscere i gruppi abeliani finiti, basta conoscere i p-gruppi abeliani finiti.

Proposizione 25. *Ogni p-gruppo abeliano finito è un prodotto diretto di sottogruppi ciclici.*

Dimostrazione. Sia G un p-gruppo abeliano finito e sia $g \in G$ un elemento di ordine massimo $n := p^m$. Se G non è ciclico, $G \neq C := \langle g \rangle$. Sia $H \subseteq G$ un sottogruppo del massimo ordine possibile tale che $C \cap H = \{e\}$. Poiché G è abeliano, HC è un sottogruppo di G isomorfo al prodotto diretto $H \times C$. Mostriamo che $G = HC$. Poiché H è un p-gruppo di ordine inferiore a quello di G, potremo poi concludere per induzione sull'ordine.

Supponiamo che $HC \neq G$ e sia $x \in G \setminus HC$. Poiché l'ordine di x è uguale ad una potenza di p al più uguale ad $n := p^m$, si ha $x^n = e \in HC$. Allora esiste $s \leq m$ tale che $x^{p^s} \in HC$ e $y := x^{p^{s-1}} \notin HC$. Poiché $y^p \in HC$, possiamo scrivere $y^p = hg^t$, con $h \in H$ e $t \in \mathbb{Z}$. Notando che $y^n = (hg^t)^{n/p} = e$, vediamo che $g^{tn/p} \in C \cap H = \{e\}$. Da cui otteniamo che p divide t (perché g ha ordine $n := p^m$) e, scrivendo $t = pk$, che $y^p = hg^{pk}$. Allora $(yg^{m-k})^p = h \in H$ ma, dal momento che $y \notin HC$, $z := yg^{m-k} \notin H$. Ne segue che $H \subsetneq \langle H, z \rangle$ e, per la massimalità di H, $C \cap \langle H, z \rangle \neq \{e\}$. Sia $g^a \in \langle H, z \rangle$, $g^a \neq e$, e scriviamo $g^a = uz^b = uy^b g^{b(n-k)}$, con $u \in H$ e $a, b \in \mathbb{Z}$. Ora $y^b = u^{-1} g^{a+bk} \in HC$ e $y^p \in HC$. Inoltre p non divide b, altrimenti $z^b = (yg^{m-k})^{pc} = h^c \in H$, da cui $g^a \in H$ e $g^a = e$. In conclusione, scrivendo $1 = b\alpha + p\beta$, otteniamo $y = y^{b\alpha} y^{p\beta} \in HC$, in contraddizione con la scelta $y \notin HC$. □

La decomposizione di un p-gruppo finito nel prodotto diretto di sottogruppi ciclici non è unica, ad esempio un gruppo di Klein è prodotto diretto di due qualsiasi suoi sottogruppi propri. Mostriamo che tuttavia gli ordini delle componenti sono univocamente determinati.

Proposizione 26. *Sia G un p-gruppo abeliano finito. Se G è prodotto diretto di gruppi ciclici di ordine $p^{a_1}, \ldots, p^{a_k}$, con $a_1 \geq a_2 \geq \cdots \geq a_k \geq 1$, la succesione di interi $(a_1, \ldots, a_k)$ è univocamente determinata.*

Dimostrazione. Supponiamo che G abbia ordine p^n e procediamo per induzione sull'ordine di G. Poiché G è abeliano, l'insieme $G^p := \{g^p \,;\; g \in G\}$ è un sottogruppo proprio di G ed inoltre, se H è un sottogruppo ciclico di G di ordine p^a, H^p è un sottogruppo cilico di H di ordine p^{a-1}. Supponiamo che G si possa scrivere in due modi diversi come prodotto di p-gruppi ciclici e siano

$$(a_1, \ldots, a_k), \quad (b_1, \ldots, b_h)$$

le relative successioni di interi, con $a_1 \geq \cdots \geq a_k \geq 1$, $b_1 \geq \cdots \geq b_h \geq 1$ e $a_1 + \cdots + a_k = n = b_1 + \cdots + b_k$. Allora anche G^p si può scrivere in due modi diversi come prodotto di p gruppi ciclici le cui successioni di interi relative sono

$$(a_1 - 1, \ldots, a_r - 1), \quad (b_1 - 1, \ldots, b_s - 1)$$

dove $r \leq h$, $s \leq k$ e $a_i = p = b_j$ per $r < i \leq h$, $s < j \leq k$. Poiché l'ordine di G^p è strettamente minore di quello di G, per l'ipotesi induttiva, otteniamo $r = s$ e $a_i = b_i$ per $1 \leq i \leq r$. Dunque

$$a_1 + \cdots + a_r + (k - r)p = n = a_1 + \cdots + a_r + (h - r)p$$

da cui $h = k$ e $a_i = b_i$ per $1 \leq i \leq h$. □

Un p-gruppo G di ordine p^n che è isomorfo al prodotto diretto di gruppi ciclici di ordine $p^{a_1}, \ldots, p^{a_k}$ con $a_1 \geq \cdots \geq a_k$, si dice *di tipo* $(p^{a_1}, \ldots, p^{a_k})$ e le potenze $p^{a_1}, \ldots, p^{a_k}$ si chiamano i *divisori elementari* di G.

Una succesione di interi $(a_1, \ldots, a_k)$ tale che $a_1 \geq \cdots \geq a_k$ e $a_1 + \cdots + a_k = n$ si chiama una *partizione di* n.

Corollario 27. *Il numero delle classi di isomorfismo dei p-gruppi abeliani finiti di ordine p^n è uguale al numero delle partizioni di n.*

Esempi 28. Ogni p-gruppo di ordine p^2 è abeliano (Corollario 11), quindi è ciclico oppure è isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.

Un gruppo abeliano di ordine $2^3 = 8$ è isomorfo ad uno dei gruppi $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Possiamo finalmente enunciare il teorema di classificazione dei gruppi abeliani finiti.

Teorema 29 (Teorema di struttura dei gruppi abeliani finiti)**.** *Sia G un gruppo abeliano di ordine $n = p_1^{e_1} \ldots p_m^{e_m}$, dove $p_1, \ldots, p_m$ sono numeri primi distinti. Allora G è prodotto diretto di p_i-sottogruppi ciclici, di ordine univocamente determinato.*

Dimostrazione. G è prodotto diretto delle sue p-esime componenti, che sono p_i-gruppi abeliani univocamente determinati (Proposizione 23). A loro volta, le p_i-esime componenti di G sono prodotto diretto di p_i-gruppi ciclici, i cui ordini sono i loro divisori elementari e quindi sono univocamente determinati (Proposizioni 25 e 26). □

Il gruppo delle unità di $\mathbb{Z}_n$

Per $n \geq 2$, indichiamo con $\mathcal{U}(\mathbb{Z}_n)$ l'insieme degli elementi invertibili dell'anello $\mathbb{Z}_n$ delle classi resto modulo n. Questo insieme è un gruppo moltiplicativo di ordine $\varphi(n)$, dove $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ è la funzione di Eulero.

Per il Teorema Cinese dei Resti, se $n = p_1^{e_1} \ldots p_m^{e_m}$ è la fattorizzazione di n in numeri primi distinti, $\mathbb{Z}_n$ è isomorfo al prodotto diretto di anelli $\mathbb{Z}_{p_1^{e_1}} \times$

$\cdots \times \mathbb{Z}_{p_m^{e_m}}$ e quindi $\mathcal{U}(\mathbb{Z}_n)$ è isomorfo al prodotto diretto di gruppi moltiplicativi $\mathcal{U}(\mathbb{Z}_{p_1^{e_1}}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{p_m^{e_m}})$ (Esempio **??** (2)). Quindi per determinare la struttura di $\mathcal{U}(\mathbb{Z}_n)$ basta considerare il caso in cui n sia potenza di un numero primo p.

Teorema 30. (a) *$\mathcal{U}(\mathbb{Z}p^m)$ è un gruppo ciclico di ordine $p^{m-1}(p-1)$, per ogni primo $p \neq 2$ e $m \geq 1$.*

(b) *$\mathcal{U}(\mathbb{Z}_{2^m}) = \langle \overline{-1}, \overline{5} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$, per ogni $m \geq 3$,*

(c) *$\mathcal{U}(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\} \cong \mathbb{Z}_2$.*

Dimostrazione. (a) Sia $p \neq 2$ e $G := \mathcal{U}(\mathbb{Z}p^m)$. Se $m = 1$, $G := \mathcal{U}(\mathbb{Z}_p) = \mathbb{F}_p^*$ è ciclico di ordine $p-1$, essendo un sottogruppo finito del gruppo moltiplicativo di un campo. Se $m \geq 2$, G ha ordine $\varphi(p^m) = p^{m-1}(p-1)$. Poiché $\mathrm{MCD}(p^{m-1}, p-1) = 1$, G è prodotto diretto di un sottogruppo P di ordine p^{m-1} (la sua p-esima componente) e di un sottogruppo H di ordine $p-1$. Basterà allora mostrare che P e H sono gruppi ciclici (Lemma 22).

Notiamo che H è costituito esattamente dagli elementi di G il cui ordine divide $p-1$, perché $G = PH$ e $P \cap H = \{e\}$. Se $a \in \mathbb{Z}$ è tale che $a \equiv 1 \mod p^m$, allora $a \equiv 1 \mod p$. Perciò, se la classe di a modulo p genera il gruppo $\mathcal{U}(\mathbb{Z}_p)$, anche la classe di a modulo p^m ha ordine $p-1$ in G e quindi genera H.

Mostriamo ora che la classe di $b := 1+p$ modulo p^m ha ordine p^{m-1} e quindi genera P. Per questo, basterà verificare che $b^{p^{m-2}} \not\equiv 1 \mod p^m$. Infatti, per induzione su $n \geq 0$, applicando la formula del binomio si vede che

$$b^{p^n} := (1+p)^{p^n} \equiv 1 + p^{n+1} \mod p^{n+2}.$$

(b) Il gruppo $\mathcal{U}(\mathbb{Z}_{2^m})$ ha ordine $\varphi(2^m) = 2^{m-1}$, quindi è un 2-gruppo. Per induzione su $m \geq 3$, applicando la formula del binomio, si ha

$$5^{2^{m-3}} = (1+4)^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m.$$

Poiché $5^{2^{m-3}} \equiv 2^{m-1} + 1 \not\equiv 1 \mod 2^m$, allora $\overline{5}$ ha ordine 2^s per $m-2 \leq s \leq m-1$. Inoltre $\overline{-1}$ ha ordine 2. Mostriamo che $\langle \overline{-1} \rangle \cap \langle \overline{5} \rangle = \overline{1}$. Supponiamo che $\overline{5}^t \in \langle \overline{-1} \rangle \cap \langle \overline{5} \rangle$, ovvero $5^t \equiv -1 \mod 2^m$. Poiché $m \geq 3$, allora $5^t \equiv -1 \mod 4$, ma questo è impossibile perché $5 \equiv 1 \mod 4$. Allora $\langle \overline{-1}, \overline{5} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$ è un sottogruppo di $\mathcal{U}(\mathbb{Z}_{2^m})$ di ordine uguale almeno a 2^{m-1} e quindi coincide con tutto $\mathcal{U}(\mathbb{Z}_{2^m})$.

(c) è immediato. □