Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 15-04-2020

Sottogruppi di indice piccolo

$\#G = n$ e $H < G$ tale che $[G : H]$ sia il più piccolo numero primo che divide $n \implies H \triangleleft G$.

Dimostrazione.

$K := \ker(L\colon G \to S(G/H)) \triangleleft G$ tale che $K \subseteq H$.

$p := [G : H]$ e $m := [H : K] \implies$ per il teorema di Lagrange

$$[G : K] = \frac{\#G}{\#K} = \frac{\#G}{\#H}\frac{\#H}{\#K} = [G : H][H : K] = pm \mid n.$$

Per il primo teorema di isomorfismo $G/K \cong \mathrm{im}(L) < S(G/H)$, quindi (sempre per il teorema di Lagrange)

$$pm = \#(G/K) = \#\,\mathrm{im}(L) \mid \#S(G/H) = [G : H]! = p! = (p-1)!p.$$

$m \mid n$, $m \mid (p-1)! \implies m \mid \mathrm{mcd}(n, (p-1)!) = 1 \implies m = 1$ $\implies H = K \triangleleft G$. □

Esempi

$H < G \implies H \triangleleft G$ in ciascuno dei seguenti casi:

- $\#G = pqr$ con $p < q < r$ primi e $\#H = qr$;
- $\#G = p^2q$ con $p < q$ primi e $\#H = pq$;
- $\#G = p^n$ (p primo, $n > 0$) e $\#H = p^{n-1}$;
- $\#G = p^2$ (p primo).

Esercizio

$\#G = p^2$, G non ciclico $\implies$

- $\exists\, H, K \triangleleft G$ distinti tali che $\#H = \#K = p$;
- $H \cap K = \{1\}$;
- $HK = G$;
- $G \cong C_p \times C_p$.

Richiami sul prodotto di sottogruppi

$H, K < G$.

- $HK := \{ab : a \in H,\ b \in K\} < G \iff HK = KH$.
- $H \triangleleft G$ o $K \triangleleft G \implies HK < G$.
- $H, K \triangleleft G \implies HK \triangleleft G$.
- $ab = ba\ \forall\, a \in H$ e $\forall\, b \in K \implies$ la funzione

$$H \times K \to HK \qquad (a, b) \mapsto ab$$

è un omomorfismo suriettivo di gruppi, e è un isomorfismo $\iff H \cap K = \{1\}$.

- $H, K \triangleleft G$ e $H \cap K = \{1\} \implies HK \cong H \times K$.
- H e K finiti $\implies$

$$\#(HK) = \frac{(\#H)(\#K)}{\#(H \cap K)}.$$

Descrizione delle orbite di un'azione

Proposizione

Sia X un G-insieme. Allora $\forall\, x \in X$ la funzione

$$f : G/\mathrm{Stab}(x) \to Gx \qquad \bar{a} := a\mathrm{Stab}(x) \mapsto ax$$

è un isomorfismo di G-insiemi.

Dimostrazione.

f è ben definita: $\overline{a'} = \bar{a}$ (cioè $a' = ab$ con $b \in \mathrm{Stab}(x)$) $\implies$
$a'x = (ab)x = a(bx) = ax$.

f è un morfismo di G-insiemi: $\forall\, g, a \in G$
$f(g\bar{a}) = f(\overline{ga}) = (ga)x = g(ax) = gf(\bar{a})$.

f è suriettiva: $\forall\, a \in G\ ax = f(\bar{a})$.

f è iniettiva: $a, a' \in G$ tali che $f(\bar{a}) = f(\overline{a'})$ (cioè $ax = a'x$) $\implies$
$x = a^{-1}ax = a^{-1}a'x \implies a^{-1}a' \in \mathrm{Stab}(x) \implies \bar{a} = \overline{a'}$. □

Conseguenze

Sia X un G-insieme.

- X è omogeneo $\iff$ $X \cong G/H$ per qualche $H < G$.
- $\#(Gx) = [G : \mathrm{Stab}(x)]\ \forall\, x \in X$.
- $\#[a] = [G : C(a)]$ (con $[a] := \{gag^{-1} : g \in G\}$) $\forall\, a \in G$.
- $\#[H] = [G : N(H)]$ (con $[H] := \{gHg^{-1} : g \in G\}$) $\forall\, H < G$.
- X finito, $X = \coprod_{i=1}^{n} Gx_i \implies \#X = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$.
- G finito, $G = \coprod_{i=1}^{n} [a_i] \implies \#G = \sum_{i=1}^{n} [G : C(a_i)]$.
  Posso supporre che esista $0 \leq m \leq n$ tale che $a_i \in Z(G)$ ($\iff \#[a_i] = [G : C(a_i)] = 1$) $\iff i > m$. Si ottiene allora l'equazione delle classi:

$$\#G = \#Z(G) + \sum_{i=1}^{m} [G : C(a_i)]$$

(con $1 < [G : C(a_i)] \mid \#G\ \forall\, i = 1, \ldots, m$).

Centro di un p-gruppo

Definizione

Sia p un numero primo. Un p-gruppo è un gruppo (finito) il cui ordine è una potenza di p.

Proposizione

$G \neq \{1\}$ *p-gruppo* $\implies Z(G) \neq \{1\}$.

Dimostrazione.

Per l'equazione delle classi

$$\#Z(G) = \#G - \sum_{i=1}^{m} [G : C(a_i)].$$

Per ipotesi $\#G = p^n$ per qualche $n > 0$ e $[G : C(a_i)] = p^{n_i}$ con $0 < n_i \leq n$; in particolare $p \mid \#G$ e $p \mid [G : C(a_i)]$ $\forall\, i = 1, \ldots, m$. Allora $p \mid \#Z(G)$, e quindi $Z(G) \neq \{1\}$. □

Sottogruppi normali di un p-gruppo

Corollario

$\#G = p^n \implies \forall\, m$ *tale che* $0 \leq m \leq n\ \exists\, H \triangleleft G$ *tale che* $\#H = p^m$. *In particolare* G *è semplice* $\iff n = 1 \iff G \cong C_p$.

Dimostrazione.

Per induzione su n: $n = 0$ ovvio.

Se $n > 0$, posso supporre $m > 0$. Per la Proposizione precedente $\#Z(G) = p^{n'}$ con $0 < n' \leq n$. Esiste $K < Z(G)$ tale che $\#K = p$ (perché $p \mid \#Z(G)$ e $Z(G)$ è abeliano). Poiché $K \triangleleft G$ ($\forall\, g \in G$ e $\forall\, a \in K$ si ha $gag^{-1} = a \in K$), $\overline{G} := G/K$ è un gruppo tale che

$$\#\overline{G} = \frac{\#G}{\#K} = \frac{p^n}{p} = p^{n-1}.$$

Per l'ipotesi induttiva esiste $\overline{H} \triangleleft \overline{G}$ tale che $\#\overline{H} = p^{m-1}$; inoltre $\exists!\, H \triangleleft G$ tale che $\overline{H} = H/K$, per cui

$$\#H = (\#\overline{H})(\#K) = p^{m-1}p = p^m.$$

Gruppi di ordine p^2

Lemma

Un gruppo G è abeliano $\iff$ $G/Z(G)$ è ciclico.

Dimostrazione.

$\implies$ $Z(G) = G \implies \overline{G} := G/Z(G) = \{\bar{1}\}$ è ciclico.

$\impliedby$ $\overline{G} = \langle \bar{g} \rangle$ (con $g \in G$) $\implies \forall\, a \in G\ \exists\, n \in \mathbb{Z}$ tale che $\bar{a} = \bar{g}^n$ $\implies \exists\, b \in Z(G)$ tale che $a = g^n b \implies a \in C(g)$ (perché $g, b \in C(g)$) $\implies C(g) = G \implies g \in Z(G) \implies \bar{g} = \bar{1}$ $\implies \overline{G} = \langle \bar{1} \rangle = \{\bar{1}\} \implies Z(G) = G \implies G$ abeliano.

□

Corollario

$\#G = p^2 \implies G$ *abeliano (quindi* $G \cong C_{p^2}$ *o* $G \cong C_p^2$*).*

Dimostrazione.

Per la Proposizione $1 < \#Z(G) \mid p^2 \implies \#Z(G) = p$ o $p^2 \implies$ $\#(G/Z(G)) = p$ o $1 \implies G/Z(G)$ ciclico $\implies G$ abeliano. □

Esercizio

1. G gruppo, $a \in G \implies C(a) \triangleleft N(\langle a \rangle)$; $\mathrm{ord}(a) = m \implies N(\langle a \rangle)/C(a)$ è isomorfo a un sottogruppo di $\mathbb{Z}/m\mathbb{Z}^*$.
2. $1 < m \leq n$, $\sigma \in S_n$ m-ciclo $\implies C(\sigma) \cong C_m \times S_{n-m}$ e $N(\langle \sigma \rangle)/C(\sigma) \cong \mathbb{Z}/m\mathbb{Z}^*$.

Esercizio

1. G gruppo, $a \in G \implies C(a) \triangleleft N(\langle a \rangle)$; $\mathrm{ord}(a) = m \implies N(\langle a \rangle)/C(a)$ è isomorfo a un sottogruppo di $\mathbb{Z}/m\mathbb{Z}^*$.
2. $1 < m \leq n$, $\sigma \in S_n$ m-ciclo $\implies C(\sigma) \cong C_m \times S_{n-m}$ e $N(\langle \sigma \rangle)/C(\sigma) \cong \mathbb{Z}/m\mathbb{Z}^*$.

Osservazione

Due elementi di S_n sono coniugati $\iff$ hanno lo stesso tipo di decomposizione come prodotto di cicli disgiunti.
In particolare i coniugati di un m-ciclo sono tutti e soli gli m-cicli.
Gli m-cicli di S_m sono $(m-1)!$ (ogni tale m-ciclo può essere scritto in modo unico come $(a_1, \ldots, a_{m-1}, m)$ con $\{a_1, \ldots, a_{m-1}\} = \{1, \ldots, m-1\}$).
Quindi gli m-cicli di S_n sono

$$(m-1)!\binom{n}{m} = \frac{(m-1)!n!}{m!(n-m)!} = \frac{n!}{m(n-m)!}.$$

Dimostrazione di 1

- $C(a) \subseteq N(\langle a \rangle)$: $b \in C(a) \implies \langle a \rangle \subseteq C(b) \implies b \in N(\langle a \rangle)$.
- $C(a) \triangleleft N(\langle a \rangle)$: $g \in N(\langle a \rangle)$ e $b \in C(a) \implies$ $c := gbg^{-1} \in C(a)$ perché $g^{-1}ag \in \langle a \rangle \subseteq C(b)$, quindi $cac^{-1} = gbg^{-1}agb^{-1}g^{-1} = gg^{-1}agg^{-1} = a$, cioè $c \in C(a)$.
- Se $\mathrm{ord}(a) = m$, la funzione

  $f : N(\langle a \rangle) \to \mathbb{Z}/m\mathbb{Z}^* \qquad g \mapsto \bar{i}$ con $i \in \mathbb{Z}$ tale che $gag^{-1} = a^i$

  è ben definita perché $a^i = a^{i'} \iff i \equiv i' \mod m$ e $\mathrm{mcd}(m, i) = 1$ (dato che $\mathrm{ord}(gag^{-1}) = \mathrm{ord}(a)$).
- f omomorfismo: $g, h \in N(\langle a \rangle)$ con $f(g) = \bar{i}$ e $f(h) = \bar{j} \implies$

  $(gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = ga^jg^{-1} = (gag^{-1})^j = (a^i)^j = a^{ij}$,

  cioè $f(gh) = \overline{ij} = \bar{i}\bar{j} = f(g)f(h)$.
- $\ker(f) = C(a)$: $f(g) = \bar{1} \iff gag^{-1} = a \iff g \in C(a)$.
- Quindi $N(\langle a \rangle)/C(a) = N(\langle a \rangle)/\ker(f) \cong \mathrm{im}(f) < \mathbb{Z}/m\mathbb{Z}^*$ per il primo teorema di isomorfismo.

Dimostrazione di 2

- Posso supporre $\sigma = (n-m+1, \ldots, n)$.
- $H_1 := \langle \sigma \rangle < C(\sigma)$ e $H_1 \cong C_m$.
- $H_2 := \{\tau \in S_n \,:\, \tau(i) = i \;\forall\, i > n-m\} < C(\sigma)$ e $H_2 \cong S_{n-m}$.
- $H_1 \cap H_2 = \{1\}$ e $\tau_1\tau_2 = \tau_2\tau_1 \;\forall\, \tau_1 \in H_1$ e $\forall\, \tau_2 \in H_2$, quindi

$$H := H_1H_2 < C(\sigma) \quad \text{e} \quad H \cong H_1 \times H_2 \cong C_m \times S_{n-m}.$$

- Poiché

$$\frac{n!}{m(n-m)!} = \#[\sigma] = [S_n : C(\sigma)] = \frac{n!}{\#C(\sigma)},$$

$\#C(\sigma) = m(n-m)! = \#H \implies C(\sigma) = H \cong C_m \times S_{n-m}$.

- Poiché C_m ha $\varphi(m) = \#\mathbb{Z}/m\mathbb{Z}^*$ generatori,

$$\frac{\#[\sigma]}{\varphi(m)} = \#[\langle\sigma\rangle] = [S_n : N(\langle\sigma\rangle)] = \frac{[S_n : C(\sigma)]}{[N(\langle\sigma\rangle) : C(\sigma)]},$$

da cui segue $[N(\langle\sigma\rangle) : C(\sigma)] = \varphi(m)$, e dunque $N(\langle\sigma\rangle)/C(\sigma) \cong \mathbb{Z}/m\mathbb{Z}^*$ per il punto 1.