1. Sottogruppi del prodotto diretto di due gruppi

Osserviamo che in generale un sottogruppo del prodotto diretto di due gruppi non é il prodotto diretto dei due sottogruppi. Per esempio se G è un gruppo non banale allora il sottogruppo diagonale $D =< (1,1) >= \{x,x) \mid x \in G\}$ é un sottogruppo di $G \times G$ che non é il prodotto diretto di due sottogruppi di G (infatti $(x,y) \notin D$ se $x \neq y$). Osserviamo che $D \cong G \cong \{1\} \times G \leq G \times G$. Quindi ci si chiede se esista $A \leq H \times K$ tale che $A \ncong A_1 \times A_2$ con $A_1 \leq H$ e $A_2 \leq K$. Il seguente esempio mostra che questo capita.

Esempio 1.1. Consderiamo l'omomorfismo suriettivo

$$f : S_3 \times S_3 \to \{\pm 1\} \cong \mathbb{Z}_2,\ (f,g) \mapsto sgn(f \circ g).$$

Allora il suo nucleo $H = Ker f < S_3 \times S_3$ non è isomorfo al prodotto diretto di due sottogruppi di S_3. Infatti $|H| = 18$ (per il primo teorema di isomorfismo e per Lagrange) e quindi se fosse isomorfo al prodotto diretto di due sottogruppi di S_3 l'unica possibilità (a meno dell'ordine) sarebbe $H \cong A_3 \times S_3$. Osserviamo ora che $((12),(123)) \in A_3 \times S_3$ é un elemento di ordine 6 mentre H non ha elementi di ordine 6; se ci fosse un elemento di ordine 6 in $H < S_3 \times S_3$ dovrebbe essere (a meno dell'ordine) della forma (τ,σ) con τ trasposizione e σ 3-ciclo. Ma $f(\tau \circ \sigma) = sgn(\tau \circ \sigma) = -1$ e quindi $(\tau,\sigma) \notin H$.

Se i gruppi sono finiti e di cardinalita coprime fra loro allora vale il seguente risultato.

Teorema 1.2. *Siano H e K due gruppi tali che $|H| = m$ e $|K| = n$ con $(m,n) = 1$. Allora per ogni $A \leq H \times K$ esistono $A_1 \leq H$ e $A_2 \leq K$ tali che $A = A_1 \times A_2$.*

Proof. Siano $A_1 := p_1(A)$ e $A_2 := p_2(A)$ (dove p_i sono le proezioni canoniche). Allora $A \subseteq A_1 \times A_2$ e quindi

$$|A|\,|\,|A_1 \times A_2| = |A_1||A_2|. \tag{1}$$

Siccome $|A|\,|\,|H \times K| = mn$ segue che $|A| = ab$ con $a|m$ e $b|n$. Ora $|A_1|\,|m$ (per Lagrange) e $|A_1|\,|\,|A| = ab$ (per un corollario del primo teorema di isomorfismo). Quindi $|A_1|\,|(m,ab) = a$ (in quanto $a|m$, $b|n$ e $(m,n) = 1$). Analogamente $|A_2|\,|b$. Quindi

$$|A_1 \times A_2| = |A_1||A_2|\,|\,ab. \tag{2}$$

La (1) e (2) danno $|A| = ab = |A_1 \times A_2|$ da cui $A = A_1 \times A_2$. $\square$