COMPLEMENTI SULLE STRUTTURE ALGEBRICHE

Consideriamo un gruppo $< A, \cdot >$, un suo sottogruppo H si dice normale in A se per ogni $h \in H$ e per ogni $a \in A$ si ha $a^{-1} \cdot h \cdot a \in H$.
L'elemento $a^{-1} \cdot h \cdot a$ si dice anche coniugato di h mediante a, un sottogruppo di un gruppo è quindi normale se e solo se contiene i coniugati di tutti i suoi elementi.
L'insieme $a^{-1} \cdot H \cdot a = \{a^{-1} \cdot h \cdot a \mid h \in H\}$ si dice coniugato del sottogruppo H mediante a (verificare che $a^{-1} \cdot H \cdot a$ è un sottogruppo di $<A, \cdot>$), è facile allora notare che un sottogruppo è normale se e solo se contiene tutti i suoi coniugati.

N.B. Per verificare che un sottoinsieme di A sia sottogruppo normale bisogna anche verificare che sia sottogruppo.

Si osservi che un sottogruppo di un gruppo abeliano è sempre normale.

Esempio
Si consideri il gruppo generale lineare $GL(2,R)$, cioè l'insieme delle matrici quadrate non singolari di ordine 2 a coefficienti reali che risulta essere un gruppo rispetto all'usuale operazione di prodotto di matrici. Il sottoinsieme $SL(2,R)$ delle matrici aventi determinante 1 costituisce un sottogruppo normale di $GL(2,R)$, detto gruppo speciale lineare.
Siano infatti $A, B \in H$, AB e A^{-1} sono ancora matrici aventi determinante 1, dunque H è un sottogruppo. Prendiamo, ora, una qualsiasi matrice C non singolare quadrata di ordine 2 e consideriamo il prodotto $C^{-1}AC$. Risulta $\det(C^{-1}AC) = \det C^{-1} \det A \det C = \det C^{-1} \det C = 1$ dunque $C^{-1}AC \in H$.

Si consideri ora una congruenza ρ del gruppo $< A, \cdot >$. Detta e l'unità del gruppo, la classe ρ_e dell'elemento neutro è un sottogruppo normale di $< A, \cdot >$.
Infatti per ogni $h, k \in \rho_e$ si ha, per definizione di ρ-classe, $(h,e) \in \rho$ e $(k,e) \in \rho$ da cui, per definizione di congruenza, $(h \cdot k, e \cdot e) \in \rho$ e quindi $(h \cdot k, e) \in \rho$ e quindi $h \cdot k \in \rho_e$; inoltre, per la riflessività di ρ, si ha $(h^{-1}, h^{-1}) \in \rho$ e così $(h \cdot h^{-1}, e \cdot h^{-1}) \in \rho$ da cui $(e, h^{-1}) \in \rho$ e, per la simmetria di ρ, $(h^{-1}, e) \in \rho$ quindi $h^{-1} \in \rho_e$ dunque ρ_e è un sottogruppo di $< A, \cdot >$.
Inoltre per ogni $a \in A$ e per ogni $h \in \rho_e$ si ha $(a^{-1}, a^{-1}) \in \rho$, $(h,e) \in \rho$, $(a,a) \in \rho$ (perché?) e quindi $(a^{-1} \cdot h \cdot a, e) \in \rho$ da cui $a^{-1} \cdot h \cdot a \in \rho_e$ e quindi ρ_e è sottogruppo normale di $< A, \cdot >$.

Dati un gruppo $< A, \cdot >$, un suo elemento a ed un suo sottogruppo H diciamo laterale sinistro (destro) di H in $< A, \cdot >$, avente come rappresentante a, l'insieme $a \cdot H = \{a \cdot h \mid h \in H\}$ ($H \cdot a = \{h \cdot a \mid h \in H\}$). I laterali vengono spesso semplicemente indicati con aH (Ha).
Nel caso in cui H sia normale i laterali destri e sinistri aventi come rappresentanti a coincidono e richiamano semplicemente laterali di H in $<A, \cdot>$. Viceversa ogni sottogruppo in cui laterali destri e sinistri coincidono è normale.

Le classi di congruenza di una relazione di congruenza ρ su un gruppo $< A, \cdot >$ sono laterali del sottogruppo normale ρ_e. Infatti si prenda un qualsiasi elemento $a \in A$ e si consideri la ρ-classe di a, ρ_a. Un elemento b appartiene a ρ_a se e solo se esiste un $h \in \rho_e$ tale che $b = h \cdot a$. Infatti se $b = h \cdot a$, si ha $(b, h \cdot a) \in \rho$, ma $(h \cdot a, e \cdot a) \in \rho$ e dunque $(b,a) \in \rho$; viceversa da $(b,a) \in \rho$ si ottiene $(b \cdot a^{-1}, a \cdot a^{-1}) \in \rho$ cioè $(b \cdot a^{-1}, e) \in \rho$ da cui $b \cdot a^{-1} = h$, cioè $b = h \cdot a$.

Viceversa vale il seguente risultato:

Proposizione

Siano $< A, \cdot >$ un gruppo, e il suo elemento neutro ed H un suo sottogruppo. Sia ρ_H la relazione binaria su A definita ponendo $(a,b) \in \rho_H$ se e solo se $a \cdot b^{-1} \in H$. Allora ρ_H è una relazione di equivalenza su $< A, \cdot >$ tale che:

1. la ρ-classe di e coincide con il sottogruppo H;
2. la ρ-classe di un elemento $a \in A$ è il laterale destro di H in $< A, \cdot >$ avente come rappresentante a ;
3. ogni ρ-classe ha la stessa cardinalità di H.

In particolare se nella proposizione precedente H è sottogruppo normale del gruppo $< A, \cdot >$ la relazione ρ_H risulta essere una relazione di congruenza e quindi i laterali di H costituiscono gli elementi del gruppo quoziente A/ρ_H (spesso indicato con A/H) e l'operazione $\bullet$ indotta da $\cdot$ sui laterali di H è così definita: $(H \cdot a) \bullet (H \cdot b) = H \cdot (a \cdot b)$, l'unità del gruppo quoziente è H e l'inverso del laterale $H \cdot a$ è il laterale $H \cdot a^{-1}$.
Dalla proposizione segue che le classi di equivalenza della relazione ρ_H sono i laterali destri di H in $< A, \cdot >$ mentre si dimostra che i laterali sinistri sono le classi di equivalenza della relazione τ_H su A definita ponendo $(a,b) \in \tau_H$ se e solo se $a^{-1} \cdot b \in H$ (ovviamente quando H è normale le due relazioni ρ_H e τ_H coincidono). I laterali destri (o sinistri) di un qualsiasi sottogruppo H sono dunque una partizione di $< A, \cdot >$ e sempre dalla proposizione segue che due laterali di uno stesso sottogruppo hanno la stessa cardinalità. Da questo si ricava immediatamente un'importante conseguenza:

Teorema di Lagrange

Se $< A, \cdot >$ è un gruppo finito di ordine n (cioè la sua cardinalità è n), un suo qualsiasi sottogruppo ha ordine m che divide n.

N.B. Non vale in generale l'inverso del teorema di Lagrange, ovvero non è detto che dato un gruppo finito $< A, \cdot >$ di ordine n ed un divisore m di n il gruppo abbia un sottogruppo di ordine m. L'inverso del teorema di Lagrange vale invece per i gruppi abeliani, quindi un gruppo abeliano di ordine n ha per ogni divisore m di n almeno un sottogruppo di ordine m.

Sia f un omomorfismo del gruppo $< A, \cdot >$ nel gruppo $< A', * >$. Allora l'insieme delle controimmagini dell'unità di $< A', * >$ costituiscono un sottogruppo normale di $< A, \cdot >$ essendo tale insieme la classe di congruenza di $\ker f$ che contiene l'unità di $< A, \cdot >$. Tale sottogruppo si dice nucleo dell'omomorfismo f e lo denotiamo con N_f. Dal teorema di fattorizzazione degli omomorfismi per i gruppi si ricava quindi il seguente teorema:

Teorema di omomorfismo per gruppi

Siano $< A, \cdot >$ un gruppo, $< A', * >$ una struttura algebrica ed f un omomorfismo di $< A, \cdot >$ in $< A', * >$. Posto $T = f(A) \subseteq A'$, risulta:

1. $< T, * >$ è un gruppo;
2. N_f è un sottogruppo normale di $< A, \cdot >$;
3. $< A / N_f , \bullet >$ è isomorfo a $< T, * >$.

Quindi, a meno di isomorfismi, le immagini per epimorfismo di un gruppo sono i suoi gruppi quozienti che sono completamente determinati dai sottogruppi normali del gruppo stesso.

Esempio.
Le immagini per epimorfismo di $<Z,+>$ sono il gruppo stesso, il gruppo $<\{0\},+>$ ed i gruppi $<Z_n,+>$.
Osserviamo infatti che ogni sottogruppo di $<Z,+>$ è un sottogruppo normale. Inoltre i sottogruppi di $<Z,+>$ sono oltre i due sottogruppi banali $<Z,+>$ e $<\{0\},+>$ tutti e soli i sottogruppi $H_n=\{nh|h\in Z\}$ con n intero fissato maggiore di 1 (verificarlo)
Ora $<Z/\{0\},+>$ è isomorfo a $<Z,+>$, $<Z/Z,+>$ è isomorfo a $<\{0\},+>$, e $<Z/H_n,+>$ è $<Z_n,+>$.

Si consideri un anello $<A, +, \cdot>$. Un sottoanello I di $<A, +, \cdot>$ si dice ideale di $<A, +, \cdot>$ se per ogni $i\in I$ e per ogni $a\in A$ si ha $i\cdot a\in I$ ed $a\cdot i\in I$.
Si provi che se ρ è una congruenza di $<A, +, \cdot>$, la ρ-classe dello 0 è un ideale di $<A, +, \cdot>$ e la ρ-classe di un qualsiasi elemento a di $<A, +, \cdot>$, è l'insieme $I+a = \{i+a| i\in I\}$.
$I+a$ si chiama laterale dell'ideale I avente rappresentante a (si noti che è il laterale del sottogruppo I nel gruppo additivo $<A, +>$).
Viceversa se si considera un ideale I dell'anello $<A, +, \cdot>$, la relazione binaria su A definita ponendo $(a,b)\in\rho_I$ se e solo se $a-b\in I$ è una relazione di congruenza le cui classi sono i laterali di I in $<A, +, \cdot>$.
Tra i laterali di un ideale I di $<A,+,\cdot>$ (che sono classi di congruenza di $<A, +, \cdot>$) si possono quindi definire le operazioni $\oplus,\bullet$ indotte rispettivamente da $+,\cdot$ ponendo $(I+a)\oplus(I+b) = I+(a+b)$ e $(I+a)\bullet(I+b) = I+(a\cdot b)$. Rispetto a tali operazioni i laterali dell'anello $<A, +, \cdot>$ formano a loro volta un anello che ha per zero I e per opposto di $I+a$ il laterale $I+(-a)$. Tale anello viene indicato con la notazione A/I e coincide con l'anello quoziente rispetto alla congruenza indotta da I.
Poiché dal teorema di fattorizzazione degli omomorfismi sappiamo che tutte e sole le immagini di un anello mediante epimorfismi sono i suoi anelli quozienti, da quanto sopra osservato si ricava che le immagine mediante epimorfismi di un anello risultano completamente determinate quando si conoscano gli ideali dell'anello.

Facili conti permettono di verificare che gli unici ideali di un corpo sono il corpo stesso e l'insieme $\{0\}$. I due anelli quozienti del corpo sono perciò isomorfi rispettivamente ad un anello costituito da un solo elemento che funziona da zero (tale anello può essere visto come un corpo degenere in cui zero e unità coincidono e non ci sono elementi diversi dallo zero) e allo stesso corpo. Le immagini mediante epimorfismi di un corpo sono allora solo due: il corpo degenere formato dal solo zero e il corpo stesso.

Somma diretta di strutture simili.
Siano $<A_1,\Omega_1>$, $<A_2,\Omega_2>$, due strutture simili, chiamiamo somma diretta delle due strutture la struttura $<A_1\times A_2, \Omega>$, che ha per sostegno il prodotto cartesiano dei due sostegni e in cui per ogni operazione $\omega_1\in\Omega_1$ di arità n su A_1, viene introdotta una operazione ω di arità n su $A_1\times A_2$ ponendo per ogni n-upla di elementi $\left(a_1^{(1)},a_1^{(2)}\right),\ldots,\left(a_n^{(1)},a_n^{(2)}\right)\in A_1\times A_2$

$$\omega\left(\left(a_1^{(1)},a_1^{(2)}\right),\ldots,\left(a_n^{(1)},a_n^{(2)}\right)\right)=\left(\omega_1\left(a_1^{(1)},\ldots,a_n^{(1)}\right),\omega_2\left(a_1^{(2)},\ldots,a_n^{(2)}\right)\right).$$

dove ovviamente $\omega_2\in\Omega_2$ è l'operazione corrispondente alla operazione $\omega_1\in\Omega_1$.
E' facile osservare che la somma diretta di due gruppi $<A_1,\cdot>$, $<A_2,*>$, è un gruppo $<A_1\times A_2,\bullet>$, la cui unità è (e_1,e_2), dove e_1, e_2 sono rispettivamente le unità di $<A_1,\cdot>$, $<A_2,*>$, e l'inverso di un elemento (a_1,a_2) è $(a_1^{-1},\overline{a_2})$ dove $a_1^{-1},\overline{a_2}$ rappresentano rispettivamente gli inversi di a_1, a_2 in $<A_1,\cdot>$, $<A_2,*>$.
Analogamente la somma diretta di due anelli è un anello (dire come sono fatti lo zero e l'opposto di un elemento).