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 $a^{-1}\cdot H\cdot a=\{a^{-1}\cdot h\cdot a\ |h\in H\}$ 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.
Osservate che un sottogruppo di un gruppo abeliano è sempre normale.

Esempio
Si consideri il gruppo $M_2(R)$ delle matrici quadrate non singolari di ordine 2 a coefficienti reali, rispetto all'usuale operazione di prodotto di matrici. Il sottoinsieme H delle matrici aventi determinante 1 costituisce un sottogruppo normale di $M_2(R)$.
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, consideriamo $C^{-1}AC$, $\det(C^{-1}AC)=\det C^{-1}\det A\det C=\det C^{-1}\det C=1$; 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 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 $(h\cdot k,e)\in\rho$ da cui $h\cdot k\in\rho_e$; inoltre per la riflessività di ρ si ha $(h^{-1},h^{-1})\in\rho$ e quindi $(h\cdot h^{-1},e\cdot h^{-1})\in\rho$ 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 $<A,\cdot>$.

Si consideri ora un qualsiasi elemento $a\in A$ e si consideri la ρ-classe 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 $b=h\cdot a$.

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 $a\cdot H=\{a\cdot h|h\in H\}$ ($H\cdot a=\{h\cdot a|h\in H\}$). I laterali vengono spesso semplicemente indicati con aH (Ha).
Nel caso in cui H sia normale il 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 allora laterali del sottogruppo normale ρ_e.

Al contrario se abbiamo un gruppo $<A,\cdot>$ e un suo qualsiasi sottogruppo normale H, la relazione ρ_H definita ponendo $(a,b)\in\rho_H$ se e solo se $a\cdot b^{-1}\in H$ è una relazione di

congruenza su <A,·> avente come ρ-classe dell'unità il sottogruppo H e come ρ-classe di a il laterale di H in avente come rappresentante a.

Pertanto i laterali di un sottogruppo normale H di un gruppo <A,·> costituiscono gli elementi del gruppo quoziente A/ρ_H (spesso indicato con A/H) e l'operazione • indotta da · 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 $H\cdot a^{-1}$.

Da quanto sopra segue immediatamente che se f è un omomorfismo del gruppo <A,·> nel gruppo <A',*>, le controimmagini dell'unità di <A',*> costituiscono un sottogruppo normale di <A,·>, essendo la classe di congruenza di ker f che contiene l'unità di <A,·>, tale sottogruppo si dice nucleo dell'omomorfosmo f. Inoltre se H è un sottogruppo normale di <A,·>, esiste sempre un epimorfismo p_H di <A,·> su <A/H,•> che è la proiezione canonica definita ponendo $p_H(a)=H\cdot a$ per ogni $a\in A$. (che legame c'è con la proiezione canonica che abbiamo definito a partire da una relazione di congruenza di <A,·>? Come viene riformulato il teorema di fattorizzazione degli omomorfisni?)

Osservate poi che se provate a dimostrare (o a rivedere negli appunti la dimostrazione) che la relazione ρ_H è una relazione di equivalenza non vi serve il fatto che H sia normale, ma utilizzate solo il fatto che H è sottogruppo. La normalità di H serve solo per provare che la relazione è una congruenza e quindi per poter definire l'operazione indotta sui laterali.
E' inoltre facile provare che le classi di equivalenza della relazione ρ_H sono i laterali destri di H in <A,·> (i laterali sinistri sono invece le classi di equivalenza della relazione $(a,b)\in\tau_H$ se e solo se $a^{-1}b\in H$). I laterali destri (o sinistri) di un qualsiasi sottogruppo H sono dunque una partizione di <A,·>; inoltre è molto facile provare che due laterali di uno stesso sottogruppo hanno la stessa cardinalità.
Da questo si ricava immediatamente una importante conseguenza:
Teorema di Lagrange: Se <A,·> è un gruppo finito di ordine n, un suo qualsiasi sottogruppo ha ordine m che divide n.

Si consideri ora un anello <A,+,·>, un sottoanello I di <A,+,·> si dice ideale di <A,+,·> se per ogni $i\in I$ e per ogni $a\in A$ si ha $i\cdot a\in I$ e $a\cdot i\in I$.
Provate che se ρ è una congruenza di <A,+,·>, la ρ-classe dello 0 è un ideale di <A,+,·> e la ρ-classe di un qualsiasi elemento a di <A,+,·>, è l'insieme $I+a=\{i+a|i\in I\}$. I+a si chiama laterale di I avente rappresentante a (notate che è il laterale del sottogruppo I nel gruppo additivo <A,+>). Viceversa se si considera un ideale I dell'anello <A,+,·>, la relazione binaria su A definita ponendo $a\rho_I b$ se e solo se $a-b\in I$ è una relazione di congruenza le cui classi sono i laterali di I in <A,+,·>. Tra i laterali di un ideale I di <A,+,·> (che sono classi di congruenza di <A,+,·>) si possono quindi definire le operazioni ⊕,• indotte rispettivamente da +,· ponendo $(I+a)\oplus(I+b)= I+(s+t)$ e $(I+s)\bullet(I+t)= I+(s\cdot t)$, rispetto a tali operazioni i laterali dell'anello <A,+,·> formano a loro volta un anello che ha per zero I e per opposto di I+a il laterale I+(-a). Tale anello sarà 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 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.