Esercitazione n. 1

26/09/2016

Argomenti. Esercizi sui monoidi e sulle potenze degli elementi di un gruppo.

Esercizio 1 *Sia* $M = \mathbb{N}^{\mathbb{N}} = \{\varphi | \varphi : \mathbb{N} \longrightarrow \mathbb{N}\}$. *Allora* M *è un monoide rispetto l'operazione di composizione di funzioni. Sia* f *l'elemento di* M *definito da* $f(n) = 2n$, *per ogni* $n \in \mathbb{N}$. *Si mostri che* f *ha infiniti inversi sinistri. Quanti sono gli inversi destri di* f*?*

Esercizio 2 *Sia* M *un monoide e si fissi un suo elemento* m. *Si provi che* m *è invertibile in* M *se e solo se l'applicazione* $f_m : M \longrightarrow M$ *definita ponendo per ogni* $x \in M$ $f_m(x) = m \cdot x$ *è biunivoca.*

Esercizio 3 *Sia* G *l'insieme così definito*

$$G = \{(a, b) | a, b \in \mathbb{R}, a \neq 0\}.$$

Si provi che ponendo, per ogni $(a, b), (c, d) \in G$,

$$(a, b) * (c, d) = (ac, bc + d)$$

si definisce un'operazione interna su G, *rispetto alla quale* G *è un gruppo non-abeliano.*

Esercitazione n. 2

29/09/2016

Argomenti. Gruppo Generale Lineare e Speciale Lineare. Gruppi diedrali d'ordine $2n$.

Sia $n \in \mathbb{N}$, $n \geq 2$ e sia $\mathbb{F}$ un campo qualsiasi. Una matrice quadrata $n \times n$ ad entrate in $\mathbb{F}$ è una tabella del tipo

$$A = (a_{ij})_{i,j} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

dove per ogni $i, j = 1, 2, \dots, n$, $a_{ij} \in \mathbb{F}$. L'insieme delle matrici quadrate d'ordine n su $\mathbb{F}$ si denota con $M_n(\mathbb{F})$. Questo è un anello rispetto alle usuali operazioni di somma e prodotto (riga-per-colonna) di matrici. È ben noto che se V è uno spazio vettoriale di dimensione n sul campo $\mathbb{F}$, fissata una base per V, l'anello degli endomorfismi di V, $\mathrm{End}(V)$, è isomorfo come anello a $M_n(\mathbb{F})$.
Un altro fatto ben noto è che una matrice $A \in M_n(\mathbb{F})$ è invertibile se e solo se il suo determinante $\det(A)$ è non nullo. Denotiamo con

$$\mathrm{GL}_n(\mathbb{F}) := \{A \in M_n(\mathbb{F}) | \det(A) \neq 0\}$$

l'insieme di tutte e sole le matrici quadrate $n \times n$ invertibili.

Proposizione 1. *Rispetto l'operazione di prodotto riga-per-colonna,* $\mathrm{GL}_n(\mathbb{F})$ *è un gruppo non commutativo.*

Dimostrazione. Innanzitutto osserviamo che il prodotto di matrici è un'operazione ben definita su $\mathrm{GL}_n(\mathbb{F})$. Ovvero che presi due arbitrari elementi, A e B, di $\mathrm{GL}_n(\mathbb{F})$ anche $A \cdot B \in \mathrm{GL}_n(\mathbb{F})$ (cioè $\det(A \cdot B) \neq 0$ se $\det(A) \neq 0$ e $\det(B) \neq 0$). Questo è vero per il noto Teorema di Binet, che asserisce che

$$\det(A \cdot B) = \det(A) \det(B).$$

Il prodotto di matrici è inoltre associativo (vd. Algebra 1) e ammette come elemento neutro la matrice identità I_n. Infine per ogni matrice $A \in \mathrm{GL}_n(\mathbb{F})$, se

indichiamo con

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} \overline{A}_{11} & \overline{A}_{21} & \dots & \overline{A}_{n1} \\ \overline{A}_{12} & \overline{A}_{22} & \dots & \overline{A}_{n2} \\ \vdots & \vdots & \dots & \vdots \\ \overline{A}_{1n} & \overline{A}_{2n} & \dots & \overline{A}_{nn} \end{pmatrix}$$

(dove $\overline{A}_{ij}$ indica il complemento algebrico di A relativo alla posizione i, j, ovvero $\overline{A}_{ij} = (-1)^{i+j}$ volte il determinante del minore di A ottenuto cancellando la riga $i-$esima e la colonna $j-$esima) si ha che A^{-1} è l'inversa di A. Dunque $\mathrm{GL}_n(\mathbb{F})$ è un gruppo. $\mathrm{GL}_n(\mathbb{F})$ non è commutativo poiché, ad esempio già per $n = 2$,

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

□

Definizione 1. $\mathrm{GL}_n(\mathbb{F})$ viene detto *gruppo generale lineare su* $\mathbb{F}$.

Esercizio 1. *Siano n ed $\mathbb{F}$ come sopra, si provi che il sottoinsieme*

$$\mathrm{SL}_n(\mathbb{F}) := \{A \in M_n(\mathbb{F}) | \det(A) = 1\} \subset \mathrm{GL}_n(\mathbb{F})$$

è un sottogruppo di $\mathrm{GL}_n(\mathbb{F})$.

Dimostrazione. Utilizzo il criterio per sottogruppi, ovvero provo che $\mathrm{SL}_n(\mathbb{F})$ è non vuoto e che presi comunque A e B in $\mathrm{SL}_n(\mathbb{F})$, l'elemento $A \cdot B^{-1} \in \mathrm{SL}_n(\mathbb{F})$. Osservo che $\det(I_n) = 1$ e quindi $I_n \in \mathrm{SL}_n(\mathbb{F}) \neq \varnothing$. Siano ora A e B due arbitrari elementi di $\mathrm{SL}_n(\mathbb{F})$, per il Teorema di Binet si ha

$$\det(A \cdot B^{-1}) = (\det(A))(\det(B^{-1})) = \det(A) \cdot \frac{1}{\det(B)} = 1 \cdot 1 = 1,$$

quindi $A \cdot B^{-1} \in \mathrm{SL}_n(\mathbb{F})$. □

Definizione 2. $\mathrm{SL}_n(\mathbb{F})$ viene detto *gruppo speciale lineare su* $\mathbb{F}$.

Esercizio 2. *Sia G un gruppo e siano $a, b \in G$. Provare che se $ab = ba$, allora per ogni naturale n vale $(ab)^n = a^n b^n$.*
Mostrare con un esempio che se $ab \neq ba$ questo può non essere vero.

Svolgimento. Il primo punto è immediato e si fa per induzione su n. Limitiamoci a mostrare un esempio quando a e b sono due elementi di un gruppo che non commutano. Prendiamo $G = GL(2, \mathbb{Z}_2)$, il gruppo delle matrici invertibili 2×2 sul campo $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$. Siano

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Allora abbiamo che $A^2 = B^2 = Id$ e

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

quindi

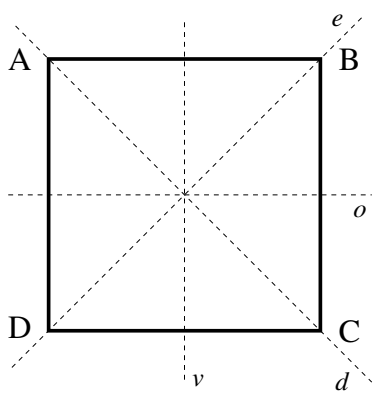
$$(AB)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

che è ben diverso da

$$A^2B^2 = Id \cdot Id = Id.$$

□

Gruppi diedrali.
Indichiamo con Q il quadrato in figura.



Consideriamo l'insieme

$$G := \{\text{simmetrie di } Q\},$$

ovvero G è l'insieme costituito da tutti i movimenti rigidi del quadrato Q che sono realizzabili nello spazio 3−dimensionale.
È evidente che date due simmetrie (α e β) di Q è possibile comporle (facendo, ad esempio, prima α e poi β), ottenendo in tal modo un'altra simmetria di Q. Quest'operazione di composizione è altresì associativa, e l'insieme G risulta essere un gruppo rispetto alla composizione (l'elemento neutro di G è la simmetria che non fa nulla, lasciando fisso il quadrato Q).
Vediamo ora di analizzare alcune particolari simmetrie. Siano

ρ :=la rotazione di Q di 90° in senso antiorario,
σ :=il ribaltamento di Q lungo l'asse verticale v.

ρ e σ sono due elementi di G. Mostriamo che ρ e σ non commutano, ovvero mostriamo che $\rho \circ \sigma \neq \sigma \circ \rho$.
Facendo la composizione $\rho \circ \sigma$ si ottiene il seguente effetto sui vertici di Q:

$$A \xrightarrow{\sigma} B \xrightarrow{\rho} A$$
$$B \xrightarrow{\sigma} A \xrightarrow{\rho} D$$
$$C \xrightarrow{\sigma} D \xrightarrow{\rho} C$$
$$D \xrightarrow{\sigma} C \xrightarrow{\rho} B$$

mentre $\sigma \circ \rho$ produce

$$A \xrightarrow{\rho} D \xrightarrow{\sigma} C$$
$$B \xrightarrow{\rho} A \xrightarrow{\sigma} B$$
$$C \xrightarrow{\rho} B \xrightarrow{\sigma} A$$
$$D \xrightarrow{\rho} C \xrightarrow{\sigma} D$$

pertanto $\rho \circ \sigma \neq \sigma \circ \rho$, ed il gruppo G non è pertanto un gruppo abeliano.
Calcoliamo ora l'ordine di G. Consideriamo un lato di Q, ad esempio il lato AB. Un elemento di G "rigira" il quadrato, dopodiché AB andrà a finire in uno dei 4 lati possibili di Q. In quella posizione potrà avere solamente 2 orientamenti possibili. Pertanto per il lato in questione ci saranno solamente $4 \cdot 2 = 8$ alternative. Una volta stabilita l'immagine di AB il resto del quadrato Q è automaticamente fissato, in quanto si tratta di movimenti rigidi che non alterano la forma, né le proporzioni di Q. In tal modo si è pertanto provato che $|G| \leq 8$. In realtà $|G|$ è esattamente 8 e i suoi elementi sono qui sotto elencati:

- l'identità , 1_G, ovvero la rotazione antioraria di $0°$.
- $\rho =$ la rotazione antioraria di $90°$,
- $\rho^2 = \rho \circ \rho =$ la rotazione antioraria di $180°$,
- $\rho^3 =$ la rotazione antioraria di $270°$,
- i quattro ribaltamenti lungo gli assi v, o e lungo le diagonali d, e.

Esercizio 3. *Con le notazioni di sopra si mostri che nel gruppo G valgono le seguenti leggi:*

$$\rho^4 = 1_G, \quad \sigma^2 = 1_G, \quad \rho\sigma = \sigma\rho^3.$$

(Suggerimento. Si consideri il comportamento di tali simmetrie sui vertici di Q.)

Esercizio 4. *Sia n un intero, $n \geq 3$, e sia P_n un poligono regolare di n lati. Detto G l'insieme delle simmetrie di P_n, si mostri che G è un gruppo (non abeliano) d'ordine $2n$.*

Definizione 3. Il gruppo G di tutte le simmetrie di P_n viene chiamato *gruppo diedrale* d'ordine $2n$, e si denota col simbolo D_{2n}.

Esercitazione n. 3

03/10/2016

Argomenti. $GL(n,p)$. Gruppi d'ordine 6. Esercizi sugli ordini degli elementi di un gruppo.

Sia p un numero primo e sia $\mathbb{F}_p$ un campo d'ordine p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Indichiamo con $GL(n,p)$ il gruppo generale lineare sul campo $\mathbb{F}_p$, ovvero l'insieme delle matrici invertibili di grado n a coefficienti in $\mathbb{F}_p$,

$$G = \left\{ A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \middle| a_{ij} \in \mathbb{F}_p,\ \det(A) \neq 0 \right\},$$

con l'operazione prodotto (riga-per-colonna) fra matrici.
Poiché le entrate di ogni matrice si possono scegliere in un numero finito di modi, $GL(n,p)$ è un gruppo finito. Proviamo che il suo ordine è dato dalla formula

$$|G| = (p^n - 1)(p^n - p^{n-1}) \dots (p^n - p^{n-1}). \tag{1}$$

Una matrice quadrata è invertibile se e solo se le sue colonne sono linearmenti indipendenti. Vediamo pertanto quante sono le possibili scelte di n colonne linearmente indipendenti sul campo $\mathbb{F}_p$. Ragioniamo in questo modo: la prima colonna si può scegliere in esattamente $p^n - 1$ modi, infatti ci sono esattamente n entrate e per ognuna di queste p scelte fra gli elementi di $\mathbb{F}_p$, quindi a priori p^n possibilità, bisogna però togliere la colonna costituita di soli zeri, quindi risulta $p^n - 1$ scelte per la prima colonna. Un volta fissata la prima colonna, per la seconda, dovendo essere linearmente indipendente dalla prima, le scelte possibili sono $p^n - p$ (abbiamo infatti tolto ora i multipli, secondo $\mathbb{F}_p$ della prima colonna). Passando alla terza si ha che da p^n va tolto il numero delle colonne lin. dip. con le prime due, ovvero il numero delle $\mathbb{F}_p$-combinazioni lineari possibili di due colonne, tale numero è p^2, quindi si hanno $p^n - p^2$ scelte per la terza colonna. Procedendo in questo modo al passo i-esimo da p^n dovremmo togliere il numero di combinazioni lineari (a coefficienti in $\mathbb{F}_p$) delle precedenti $i-1$ colonne, ovvero la quantità $p^i - 1$, quindi per la i-esima colonna le scelte possibili saranno $p^n - p^{i-1}$. In questo modo si ottiene la formula (1).

Esercizio 1. *Sia $G = GL(2,2)$. Si calcoli l'ordine di G, si determinino tutti i suoi elementi e si scriva la tavola di moltiplicazione di G. Fare la stessa cosa col gruppo diedrale D_6. Confrontare le due tavole di moltiplicazione.*

Svolgimento. Per la formula appena vista l'ordine di G è dato da

$$|G| = (2^2 - 1)(2^2 - 2) = 6.$$

G contiene l'elemento $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Calcolando le potenze di A, abbiamo

$$A^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{e} \quad A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id,$$

pertanto A è un elemento d'ordine tre. Sia $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Un rapido conto mostra che B ha ordine due. Al momento abbiamo quindi trovato quattro elementi distinti di G, ne mancano altri due. Questi sono le matrici

$$C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad D = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

il cui ordine è facile vedere essere due in entrambi i casi. Pertanto abbiamo che

$$G = \left\{ Id, A, A^2, B, C, D \right\}.$$

Determiniamo ora la tavola di moltiplicazione di G. Disponiamo gli elementi di G in modo ordinato lungo una riga e una colonna e poniamo nel posto di coordinate (g, h) della matrice l'elemento di G dato dal prodotto gh (al variare di g, h in G). Andremo a provare che si ottiene la seguente tabella

$GL(2,2)$	Id	A	A^2	B	C	D
Id	Id	A	A^2	B	C	D
A	A	A^2	Id	C	D	B
A^2	A^2	Id	A	D	B	C
B	B	D	C	Id	A^2	A
C	C	B	D	A	Id	A^2
D	D	C	B	A^2	A	Id

Infatti abbiamo che

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = C,$$

e

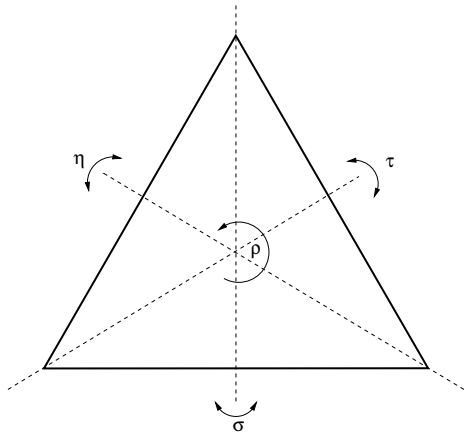
$$A^2B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = D.$$

Da ciò segue anche che

$$AC = A(AB) = A^2B = D \quad \text{e} \quad A^2D = A(AC) = AB = C,$$

il che completa le prime tre righe. Con astuzie simili si determinano le restanti righe.

Passiamo ora al gruppo D_6. Ricordiamo che D_6 è costituito dai movimenti rigidi del triangolo equilatero.



Gli elementi di D_6 sono pertanto la rotazione antioraria ρ di $2\pi/3$, il suo quadrato ρ^2, i ribaltamenti σ, τ e η lungo le bisettrici degli angoli, oltre ovviamente all'identità. Pertanto

$$D_6 = \left\{ id, \rho, \rho^2, \sigma, \tau, \eta \right\},$$

e gli ordini degli elementi sono rispettivamente: $1, 3, 3, 2, 2, 2$. Calcolando la tavola di moltiplicazione di D_6 si ottiene la seguente tabella

D_6	id	ρ	ρ^2	σ	τ	η
id	id	ρ	ρ^2	σ	τ	η
ρ	ρ	ρ^2	id	τ	η	σ
ρ^2	ρ^2	id	ρ	η	σ	τ
σ	σ	η	τ	id	ρ^2	ρ
τ	τ	σ	η	ρ	id	ρ^2
η	η	τ	σ	ρ^2	ρ	id

Confrontando le due tabelle si vede che sono molto simili, anzi sono esattamente la stessa tabella una volta effettuate le seguenti sostituzioni

$$Id \longmapsto id,\ A \longmapsto \tau,\ B \longmapsto \sigma,\ C \longmapsto \tau,\ D \longmapsto \eta.$$

$\square$

Esercitazione n. 4

(06/10/2016)

Argomenti. Esercizi sulle classi laterali destre e sinistre e sull'indice di un sottogruppo in un gruppo. Alcune applicazioni del Teorema di Lagrange.

Esempio 1 *Trovare un esempio di un gruppo G ed un suo sottogruppo H tale per cui le classi laterali destre e sinistre di H non coincidano.*
Se G è un gruppo abeliano può accadere un simil fatto?

Dimostrazione. Sia $G = D_8$ il gruppo diedrale d'ordine 8, definito nelle lezioni precedenti. Utilizzando le stesse notazioni, poniamo $H := \langle \sigma \rangle$ il sottogruppo generato da σ. Allora H è un sottogruppo d'ordine 2, poiché $\sigma^2 = 1_G$ e $H = \{1_G, \sigma\}$. Cosideriamo la classe laterale sinistra di H contenente la rotazione ρ, ovvero la classe che si denota ρH. Abbiamo che

$$\rho H = \rho \{1_G, \sigma\} = \{\rho 1_G, \rho\sigma\} = \{\rho, \rho\sigma\}.$$

Similmente per la classe laterale destra contenente ρ abbiamo

$$H\rho = \{1_G, \sigma\} \rho = \{1_G \rho, \sigma\rho\} = \{\rho, \sigma\rho\}.$$

Pertanto se fosse $\rho H = H\rho$, allora necessariamente si avrebbe $\rho\sigma = \sigma\rho$, cosa che abbiamo visto essere falsa.
Ovviamente nel caso di gruppi abeliani questo non può accadere, e classi laterali destre e sinistre coincidono in quanto, per un qualunque $K \leq G$ e $g \in G$ vale:

$$gK := \{gk | k \in K\} = \{kg | k \in K\} =: Kg.$$

□

Esercizio 1 *Sia $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ e sia P l'insieme dei numeri razionali positivi. Si provi che P è un sottogruppo del gruppo moltiplicativo $(\mathbb{Q}^*, \cdot, 1)$, si determini l'indice $[\mathbb{Q}^* : P]$ e si esibisca un sistema di rappresentanti per le classi laterali sinistre di P in $\mathbb{Q}^*$.*

Dimostrazione. Utilizzo il criterio per sottogruppi. Osservo che $P \neq \varnothing$ poiché ad esempio $1 \in P$. Inoltre presi $a, b \in P$, $ab^{-1} = \frac{a}{b} > 0$, ovvero $ab^{-1} \in P$. Dunque $P \leq \mathbb{Q}^*$.

Ricordo che l'indice $[\mathbb{Q}^* : P]$ è definito come il numero di classi laterali sinistre distinte di P. Ora preso un qualunque numero razionale q, possono accadere solo due situazioni:
o $q > 0$ e dunque $q \in P$,
oppure $q < 0$ e quindi $q = (-1) \cdot |q| \in -1P$ (essendo $|q| \in P$). Ne segue che P ha indice 2 in $\mathbb{Q}^*$ e un sistema di rappresentanti per le classi laterali sinistre di P è l'insieme $\{1, -1\}$. $\square$

Esercizio 2 *Sia* $H := \left\{\frac{m}{7^i} | m \in \mathbb{Z}, i = 0, 1\right\} \subset \mathbb{Q}$. *Si provi che* H *è un sottogruppo del gruppo additivo* $(\mathbb{Q}, +, 0)$ *contenente* $\mathbb{Z}$. *Si calcoli l'indice* $[H : \mathbb{Z}]$ *e si esibisca un opportuno sistema di rappresentanti.*

Dimostrazione. Preso un arbitrario z in $\mathbb{Z}$ poiché $z = \frac{z}{7^0}$, z appartiene ad H, quindi $\mathbb{Z}$ è contenuto in H. Mostro che H è un sottogruppo di $\mathbb{Q}$. Siano $\frac{m}{7^i}$ e $\frac{n}{7^j}$ due elementi di H, allora

$$\frac{m}{7^i} - \frac{n}{7^j} = \frac{*}{7^{max\{i,j\}}}$$

che pertanto è ancora un elemento di H. Pertanto per il criterio dei sottogruppi $H \leq \mathbb{Q}$. Troviamo ora un sistema di rappresentanti per le classi laterali sinistre di $\mathbb{Z}$ in H. Significa "confrontare gli elementi di H rispetto $\mathbb{Z}$". Sia $h = \frac{m}{7^i}$ un arbitrario elemento di H. Se $i = 0$ allora l'elemento $h \in \mathbb{Z}$, altrimenti $i = 1$ ed in tal caso detti q ed r il quoziente ed il resto della divisione di m per 7, si ha che

$$h = \frac{m}{7} = \frac{7q + r}{7} = q + \frac{r}{7} \in \frac{r}{7} + \mathbb{Z},$$

ovvero h appartiene ad uno dei laterali

$$\left\{\mathbb{Z} = 0 + \mathbb{Z}, \frac{1}{7} + \mathbb{Z}, \frac{2}{7} + \mathbb{Z}, \frac{3}{7} + \mathbb{Z}, \frac{4}{7} + \mathbb{Z}, \frac{5}{7} + \mathbb{Z}, \frac{6}{7} + \mathbb{Z}\right\}.$$

È facile poi vedere che questi sono tutti distinti, infatti se fosse

$$\frac{r_1}{7} + \mathbb{Z} = \frac{r_2}{7} + \mathbb{Z}$$

allora necessariamente

$$\frac{r_1}{7} - \frac{r_2}{7} \in \mathbb{Z},$$

cioè $r_1 - r_2$ deve essere divisibile per 7, il che è assurdo se r_1 ed r_2 sono due elementi distinti dell'insieme $\{0, 1, 2, 3, 4, 5, 6\}$. Dunque $[H : \mathbb{Z}] = 7$. $\square$

Ricordiamo il Teorema di Lagrange dimostrato a lezione.

Teorema 1 *Sia* G *un gruppo finito e sia* H *un suo sottogruppo. Allora*

$$|G| = |H|\,[G : H],$$

dove $[G : H]$ *denota l'indice di* H *in* G, *ovvero il numero di classi laterali destre (o sinistre) distinte di* H *in* G. *In particolare, si ha che l'ordine di* H *divide quello di* G.

Esercizio 3 *Siano H e K due sottogruppi di un gruppo finito G. Si provi che se $(|H|, |K|) = 1$ allora $H \cap K = \{1_G\}$ (cioè H e K si intersecano banalmente).*

Dimostrazione. Sappiamo che $H \cap K$ è un sottogruppo di G e che è contenuto sia in H che in K. Pertanto $H \cap K$ è un sottogruppo sia di H che di K. Per il teorema di Lagrange in quanto sottogruppo di H, $|H \cap K|$ divide $|H|$; similmente in quanto sottogruppo di K, $|H \cap K|$ divide anche $|K|$. Ora per ipotesi $|H|$ e $|K|$ non hanno fattori comuni, quindi l'unica possibilità è che sia $|H \cap K| = 1$, ovvero $H \cap K$ è il sottogruppo banale $\{1_G\}$. $\square$

Esercitazione n. 5

10/10/2016

Argomenti. Lemma di Poincaré. Esercizi sui sottogruppi normali e i quozienti di gruppi.

Proposizione 1. *Sia G un gruppo arbitrario e siano A e B due suoi sottogruppi di indice finito. Allora*

1. *Se $A \leq B$, $[G : A] = [G : B][B : A]$* (Formula del prodotto).
2. *In generale vale $[G : A \cap B] \leq [G : A][G : B]$* (Lemma di Poincaré).

Dimostrazione. 1. Siano $[G : B] = n$ e $[B : A] = m$ e siano $Bg_1, Bg_2, \ldots, Bg_n$ e $Ab_1, Ab_2, \ldots, Ab_m$ rispettivamente le classi laterale destre distinte di G modulo B e di B modulo A. Consideriamo le nm classi destre di G modulo A

$$A(b_i g_j), \quad i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m. \tag{1}$$

Mostriamo che esse sono tutte distinte.
Se

$$A(b_i g_j) = A(b_r g_s)$$

allora l'elemento $b_i g_j g_s^{-1} b_r^{-1} \in A$ e poiché $A \leq B$, $b_i g_j g_s^{-1} b_r^{-1} = \tilde{b} \in B$, dunque anche $g_j g_s^{-1} = b_i^{-1} \tilde{b} b_r \in B$, ovvero

$$Bg_j = Bg_s.$$

Poiché i $\{Bg_l\}_{l=1}^n$ sono laterali distinti segue $g_j = g_s$, cioè $j = s$. Ma allora si ha che $b_i b_r^{-1} \in A$, dunque $Ab_i = Ab_r$, e per gli stessi motivi di sopra si ha $b_i = b_r$, cioè $i = r$. Dunque le classi in (1) sono tutte distinte, quindi $[G : A] \geq [G : B][B : A]$.
Sia ora $g \in G$, allora $g \in Bg_i$, per qualche (unico) $i \in \{1, 2, \ldots, n\}$. Dunque $g = bg_i$, con $b \in B$. Similmente esiste un (unico) b_j ($j \in \{1, 2, \ldots, m\}$) tale che $b \in Ab_j$, cioè $b = ab_j$, per qualche $a \in A$. Ma allora

$$g = bg_i = ab_i g_j \in Ab_i g_j,$$

quindi le classi in (1) sono tutte le classi di G modulo A.

2. Consideriamo la funzione fra insiemi così definita

$$\begin{aligned} \Phi : \mathrm{Lat}(G, A \cap B) &\longrightarrow \mathrm{Lat}(G, A) \times \mathrm{Lat}(G, B) \\ (A \cap B)g &\longmapsto (Ag, Bg) \end{aligned}$$

(dove $\mathrm{Lat}(G, X)$ indica l'insieme delle classi laterali destre di G modulo il sottogruppo X). Mostriamo che Φ è una funzione ben definita e iniettiva.
<u>Φ è ben definita.</u> Se $(A \cap B)g = (A \cap B)h$, allora $gh^{-1} \in A \cap B$, dunque $gh^{-1} \in A$ e $gh^{-1} \in B$, ovvero $Ag = Ah$ e $Bg = Bh$, cioè $\Phi((A \cap B)g) = \Phi((A \cap B)h)$, come volevasi.
<u>Φ è iniettiva.</u> Siano $(Ax, Bx) = (Ay, By)$, allora $Ax = Ay$ e $Bx = By$. Pertanto $xy^{-1} \in A$ e $xy^{-1} \in B$, cioè $xy^{-1} \in A \cap B$, cioè $(A \cap B)x = (A \cap B)y$.
Ne segue che

$$|\mathrm{Lat}(G, A \cap B)| \leq |\mathrm{Lat}(G, A) \times \mathrm{Lat}(G, B)| = |\mathrm{Lat}(G, A)|\,|\mathrm{Lat}(G, B)|\,,$$

cioè

$$[G : A \cap B] \leq [G : A][G : B].$$

$\square$

Esercitazione n. 6

13/10/2016

Argomenti. Esercizi sui sottogruppi normali e i quozienti di gruppi.

Esercizio 1. *Sia S l'insieme costituito da tutte le similitudini della retta reale $\mathbb{R}$, ovvero*

$$G := \{\sigma_{a,b} : r \mapsto ar + b | a, b \in \mathbb{R}, a \neq 0\}.$$

Si provi quanto segue

1. *G è un gruppo, rispetto al prodotto $\sigma_{a,b} \cdot \sigma_{c,d} = \sigma_{c,d} \circ \sigma_{a,b}$.*
2. *Detta f l'applicazione*

$$\begin{aligned} f : G &\longrightarrow \mathbb{R}^* \\ \sigma_{a,b} &\longmapsto a \end{aligned}$$

   f è un omomorfismo suriettivo (= "epimorfismo") di gruppi.

3. *L'insieme $T := \{\sigma_{1,b} | b \in \mathbb{R}\}$ delle traslazioni è un sottogruppo normale di G.*
4. *T è isomorfo al gruppo additivo $(\mathbb{R}, +)$.*
5. *Detto $H = \{\sigma_{1,z} | z \in \mathbb{Z}\}$, provare che H è un sottogruppo* non *normale di G ed esibire un elemento $g \in G$ tale che $H^g < H$.*

Dimostrazione. 1. Siano $\sigma_{a,b}$ e $\sigma_{c,d}$ due arbitrari elementi di G. Si ha

$$\sigma_{a,b}\dot{\sigma}_{c,d} : r \longmapsto ar + b \longmapsto c(ar + b) + d = car + cb + d,$$

ovvero per ogni $r \in \mathbb{R}$, $(\sigma_{a,b} \cdot \sigma_{c,d})(r) = (\sigma_{ac,cb+d})(r)$, cioè

$$\sigma_{a,b} \cdot \sigma_{c,d} = \sigma_{ac,bc+d}. \tag{1}$$

Quindi l'operazione per gli elementi di G è ben definita. Tale composizione sappiamo già che è associativa. Mostriamo l'esistenza dell'elemento neutro e degli inversi in G. La similitudine $\sigma_{1,0}$ coincide con l'applicazione identica su

$\mathbb{R}$, ($\sigma_{1,0}(r) = r$, per ogni $r \in \mathbb{R}$), e funziona come l'identità per S, poiché da (1) si ha

$$\sigma_{a,b} \cdot \sigma_{1,0} = \sigma_{a,b} = \sigma_{1,0} \cdot \sigma_{a,b}.$$

Infine preso $\sigma_{a,b} \in G$ se si cerca un suo inverso destro $\sigma_{c,d}$ in S, dovendo essere $\sigma_{a,b} \cdot \sigma_{c,d} = \sigma_{1,0}$, da (1) si ottiene

$$\begin{cases} ac = 1 \\ bc + d = 0 \end{cases}$$

ovvero $c = a^{-1}$ e $d = -ba^{-1}$. Da ultimo si vede che l'elemento $\sigma_{a^{-1},-ba^{-1}}$ è anche inverso sinistro per $\sigma_{a,b}$. Pertanto G è un gruppo.

2. Mostriamo che l'applicazione f è un omomorfismo di gruppi.
Siano $\sigma_{a,b}$ e $\sigma_{c,d}$ due arbitrari elementi di G, abbiamo che

$$f\big(\sigma_{a,b} \cdot \sigma_{c,d}\big) = f\big(\sigma_{ac,bc+d}\big) = ac$$

che effettivamente coincide con

$$f\big(\sigma_{a,b}\big) f\big(\sigma_{c,d}\big).$$

Dunque f è omomorfismo di gruppi.
Inoltre f è suriettivo, poiché preso un qualunque $r \in \mathbb{R}^*$, ad esempio la similitudine $\sigma_{r,0} : x \mapsto rx$ è tale che $f(\sigma_{r,0}) = r$.

3. Mostriamo che T è un sottogruppo normale di G, provando che T è il nucleo di un omomorfismo fra gruppi.
Andiamo a determinare il nucleo dell'epimorfismo f del punto 2. Abbiamo che

$$\begin{aligned} \ker(f) &= \{\sigma_{a,b} \in G | f(\sigma_{a,b}) = 1\} \\ &= \{\sigma_{a,b} \in G | a = 1\} \\ &= \{\sigma_{1,b} \in G\} = T. \end{aligned}$$

Poiché nuclei di omomorfismi sono sempre sottogruppi normali, $T \trianglelefteq G$.

4. Per mostrare che T è isomorfo al gruppo $(\mathbb{R}, +)$, consideriamo l'applicazione

$$\begin{aligned} g : T &\longrightarrow \mathbb{R} \\ \sigma_{1,b} &\longmapsto b \end{aligned}$$

e mostriamo che g è un omomorfismo biunivoco.
Siano $\sigma_{1,b}$ e $\sigma_{1,d}$ arbitrariamente presi in T, allora da (1) si ha

$$g\big(\sigma_{1,b} \cdot \sigma_{1,d}\big) = g\big(\sigma_{1,b+d}\big) = b + d = g\big(\sigma_{1,b}\big) + g\big(\sigma_{1,d}\big),$$

ovvero g è omomorfismo fra gruppi.
Lasciamo per esercizio verificare che g è sia iniettivo che suriettivo.

5. È immediato verificare che H è un sottogruppo di G.
Presi arbitrariamente $g = \sigma_{a,b}$ in G, e $h = \sigma_{1,z}$ in H, abbiamo che

$$g^{-1} \cdot h \cdot g = \sigma_{a^{-1},-a^{-1}b} \cdot \sigma_{1,z} \cdot \sigma_{a,b} = \ldots = \sigma_{1,-ab+az+b}$$

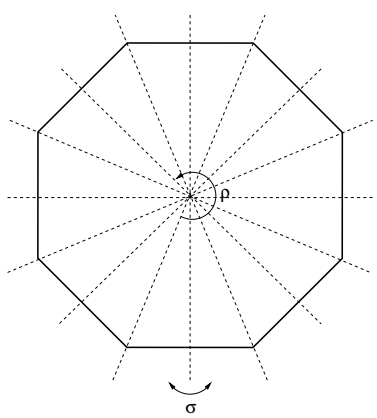
pertanto se $g = \sigma_{\pi,0}$ si ha che $g^{-1} \cdot h \cdot g = \sigma_{1,\pi z} \notin H$ e quindi H non è normale in G.
Se invece prendiamo come g l'elemento $g = \sigma_{2,0}$ otteniamo

$$H^g = g^{-1} H g = \{\sigma_{1,2z} | z \in \mathbb{Z}\}$$

che è contenuto strettamente in H. $\square$

Esercizio 2. *Sia $n \in \mathbb{N}$, $n \geq 2$ e sia D_{2n} il gruppo diedrale di ordine $2n$. Detta ρ la rotazione antioraria di $2\pi/n$ si provi che $\langle \rho \rangle$ è un sottogruppo normale d'ordine n di D_{2n}. Preso σ il ribaltamento lungo un asse mediano, si mostri che ogni elemento di D_{2n} ammette una (unica) scrittura del tipo $\rho^a \sigma^\epsilon$, al variare di $a = 0, 1, \ldots, n-1$ ed $\epsilon = 0, 1$.*

Dimostrazione. Ricordiamo che D_{2n} consiste nel gruppo dei movimenti rigidi di un poligono regolare P_n avente esattamente n lati.



La rotazione ρ è tale che

$$\rho^n = 1 = \text{identità su } P_n, \qquad \text{mentre} \qquad \rho^k \neq 1, \ \forall 0 < k < n,$$

pertanto ρ ha ordine n. In particolare detto $R := \langle \rho \rangle$, si ha che $|R| = |\rho| = n$. Dal teorema di Lagrange segue quindi che l'indice in D_{2n} di tale sottogruppo è

$$[D_{2n} : R] = \frac{|D_{2n}|}{|R|} = \frac{2n}{n} = 2,$$

ed essendo R un sottogruppo di indice 2 è necesssariamente normale in D_{2n}. Preso un elemento non appartamente a R, ad esempio il ribaltamento σ lungo l'asse verticale, si ha che

$$D_{2n} = R \sqcup R\sigma,$$

(dove il simbolo "$\sqcup$ " indica l'unione disgiunta delle due classi laterali). Un elemento di D_{2n} pertanto o appartiene ad $R = \langle \rho \rangle$, ed in tal caso è una potenza di ρ, ρ^a per un unico valore di $a \in \{0, 1, \ldots, n-1\}$, oppure appartiene alla classe $R\sigma$, ovvero è della forma $\rho^b\sigma$, anche qui per un unico valore di $b \in \{0, 1, \ldots, n-1\}$. $\square$

Esercitazione n. 7

17/10/2016

Argomenti. Classi laterali. Gruppi quoziente e omomorfismi fra gruppi.

Esercizio 1. *Sia G un gruppo e siano A e B due sottogruppi normali di G tali che $A \cap B = \{1_G\}$. Si provi che G è abeliano se e solo se G/A e G/B sono entrambi abeliani.*

Svolgimento. Vedi retro. □

Esercizio 2. *Siano G un gruppo, N un sottogruppo normale di G e g un elemento di G. Si provi quanto segue.*

1. *Se $|g| = r$ finito, allora $Ng \in G/N$ ha periodo finito che divide r.*
2. *Mostrare con degli esempi che se $|g| = \infty$, allora Ng può avere periodo sia finito sia infinito.*

Svolgimento. Vedi retro. □

Esercizio 3. *Sia $G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} | a, b \in \mathbb{Q}, a \neq 0 \right\}$ munito del prodotto così definito per ogni $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}$ in G sia:*

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} ac & ad + bc^{-1} \\ 0 & a^{-1}c^{-1} \end{pmatrix}.$$

1. *Si provi che $(G, \cdot)$ è un gruppo.*
2. *Detti $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in \mathbb{Q} \right\}$ e $K = \left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} | z \in \mathbb{Z} \right\}$, provare che $K \leq H \leq G$.*
3. *Provare che $H \trianglelefteq G$, $K \trianglelefteq H$ e che $K \ntrianglelefteq G$.*
4. *Mostrare che H è isomorfo al gruppo additivo $(\mathbb{Q}, +)$ e che G/H è isomorfo al gruppo moltiplicativo $(\mathbb{Q}^*, \cdot)$.*

Svolgimento. Vedi retro. □

17/10/2016

ES1 Poiché i quozienti di un gruppo abeliano sono gruppi abeliani, un'implicazione è ovvia.

Siano G/A e G/B abeliani e siano $x, y \in G$ arbitrari.

Poiché G/A è abeliano, abbiamo

$$xA \cdot yA = xyA = yxA = yA \cdot xA$$

cioè $y^{-1}x^{-1}yx \in A$.

Similmente $y^{-1}x^{-1}yx \in B$.

Pertanto

$$y^{-1}x^{-1}yx \in A \cap B = \{1\} \Rightarrow y^{-1}x^{-1}yx = 1 \Rightarrow xy = yx.$$

ES2 1) $(Ng)^r = Ng^r = N \cdot 1 = N \Rightarrow |Ng|$ divide r.

2) Se $G = \mathbb{Z}$ e $N = 2\mathbb{Z}$ $\quad 1 \in \mathbb{Z}$ $\quad |1| = \infty$ e $|1 + 2\mathbb{Z}| = 2$.

Se $G = GL(2, \mathbb{R})$ $\quad N = Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R}\ a \neq 0 \right\}$

allora $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ha periodo infinito in G così come l'elemento $Z(G) \cdot g \in G/Z(G)$.

$$\left((Z(G) \cdot g)^n = Z(G) \cdot \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \forall n \in \mathbb{N} \right)$$

ES3 1) Tralascio la verifica che G è un sottogruppo di $GL(2, \mathbb{Q})$ perché è standard.

2) Idem

3) Sia $\alpha = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in G$ e $\beta = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ allora

$$\alpha^{-1}\beta\alpha = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a^{-1} & a^{-1}h - b \\ 0 & a \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a^{-2}h \\ 0 & 1 \end{pmatrix}$$

Quindi se $\beta \in H$ (cioè $h \in \mathbb{Q}$) $\alpha^{-1}\beta\alpha \in H$ e quindi $H \trianglelefteq G$.

$K \not\triangleleft G$ poiché ad esempio

$$\begin{pmatrix} 2^{-1} & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 1/4 \\ 0 & 1 \end{pmatrix} \notin K.$$

Invece $K \triangleleft H$ poiché

$$\begin{pmatrix} 1 & h \\ & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \in K \qquad \forall h \in \mathbb{Q},\ \forall z \in \mathbb{Z}.$$

4) $f: H \longrightarrow \mathbb{Q}$ è un omom. ben definito, iniettivo e suriettivo.

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$$

Considero $\varphi: G \longrightarrow \mathbb{Q}^*$

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto a$$

Allora si verifica che: ① φ è omom. di gruppi.

② $\operatorname{Ker}\varphi = H$

③ $\operatorname{Im}\varphi = \mathbb{Q}^*$

Pertanto per il I teorema di omomorfismo si ha

$$G/H = G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi = \mathbb{Q}^*.$$

Esercitazione n. 8 e 9

20/10/2016

Argomenti. Esercizi sugli omomorfismi di gruppo.

Esercizio 1. *Siano G un gruppo e $a, b \in G$ tali che valga $ab = ba$. Se $|a| = r < \infty$ e $|b| = s < \infty$ e $(r, s) = 1$, si provi che $\langle a, b\rangle$ è ciclico d'ordine rs.*

Svolgimento. Osserviamo che poiché $ab = ba$ i sottogruppi $\langle a\rangle$ e $\langle b\rangle$ sono permutabili tra di loro. Ne segue che $\langle a\rangle\langle b\rangle$ è un sottogruppo di G. Inoltre poiché esso contiene sia a che b, $\langle a\rangle\langle b\rangle$ contiene il più piccolo sottogruppo di G che contiene sia a che b, ovvero $\langle a, b\rangle \leq \langle a\rangle\langle b\rangle$. Viceversa, poiché $\langle a\rangle \leq \langle a, b\rangle \geq \langle b\rangle$, allora $\langle a\rangle\langle b\rangle \leq \langle a, b\rangle$, e quindi coincidono. Per la formula dell'ordine si ha che

$$|\langle a, b\rangle| = |\langle a\rangle\langle b\rangle| = \frac{|\langle a\rangle|\,|\langle b\rangle|}{|\langle a\rangle \cap \langle b\rangle|} = \frac{r \cdot s}{|\langle a\rangle \cap \langle b\rangle|}.$$

Ora per il Teorema di Lagrange $|\langle a\rangle \cap \langle b\rangle|$ divide sia $|\langle a\rangle| = r$ che $|\langle b\rangle| = s$, ma essendo r ed s coprimi si ha necessariamente che $|\langle a\rangle \cap \langle b\rangle| = 1$, ovvero $\langle a\rangle \cap \langle b\rangle = \{1_G\}$ e $|\langle a, b\rangle| = rs$. Non ci resta che mostrare che questo gruppo è ciclico esibendo un elemento d'ordine rs. Consideriamo l'elemento ab di G e sia d il suo ordine. Abbiamo innanzitutto che

$$(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = 1_G^s 1_G^r = 1_G,$$

ovvero $d|rs$. Viceversa, da $ab^d = 1_G$ segue che $a^d b^d = 1_G$, cioè

$$a^d = b^{-d},$$

ma quest'ultimo è un elemento di $\langle a\rangle \cap \langle b\rangle = 1_G$ e quindi si ha

$$\begin{cases} a^d = 1_G \\ b^{-d} = 1_G \end{cases}$$

cioè $|a| = r|d$ e $|b| = s|d$. Essendo r ed s coprimi si ha $rs|d$, e quindi $rs = d$, ovvero $\langle a, b\rangle = \langle ab\rangle$ è ciclico d'ordine rs.

$\square$

Esercizio 2. *Sia G un gruppo finito d'ordine $|G| = 20$. Provare che se esiste un omomorfismo non-banale $\varphi : G \longrightarrow \mathbb{Z}_{15}$ allora G ammette un sottogruppo normale d'ordine 4.*

Svolgimento. Sia K il nucleo di φ. Allora K è un sottogruppo normale di G. Inoltre per il I Teorema di omomorfismo sappiamo che

$$G/K \simeq \varphi(G) \leq \mathbb{Z}_{15}.$$

Quindi per il Teorema di Lagrange otteniamo che $\frac{|G|}{|K|} = \frac{20}{|K|}$ divide 15. Ne segue che $|K| \in \{4, 20\}$, ma se K avesse ordine 20 allora sarebbe $G = K$ e pertanto φ sarebbe l'omomorfismo banale, il che è assurdo. $\square$

Esercizio 3. *Siano G ed H due gruppi e $f : G \longrightarrow H$ un omomorfismo. Si assumi che H sia abeliano. Provare che ogni sottogruppo L di G che contiene $\ker(f)$ è normale in G.*

Svolgimento. Sia $K = \ker(f)$ e sia $K \leq L \leq G$. Presi arbitrariamente $g \in G$ ed $l \in L$, abbiamo che

$$f(g^{-1}lg) = f(g^{-1})f(l)f(g) = (f(g))^{-1}f(l)f(g) = f(l)(f(g))^{-1}f(g) = f(l),$$

poiché f è un omomorfismo di gruppi, $f(G) \leq H$ ed H è abeliano. Pertanto

$$l^{-1}g^{-1}lg \in \ker(f) = K,$$

e quindi $l^{-1}g^{-1}lg \in L$ da cui segue $g^{-1}lg \in L$ e, per il criterio, $L \trianglelefteq G$. $\square$

Esercizio 4. *Siano G un gruppo, H ed N due suoi sottogruppi con $N \trianglelefteq G$ e $G = NH$. Provare quanto segue:*

1. *Esiste $f : H \longrightarrow G/N$ omomorfismo suriettivo;*
2. *Se $|H|$ è finito, vale*

$$H \simeq \frac{G}{N} \Longleftrightarrow N \cap H = \{1_G\}.$$

Svolgimento. 1. Poiché $G = NH$ ogni elemento $g \in G$ può essere scritto come

$$g = nh, \quad \text{con } n \in N, h \in H.$$

Quindi si ha che

$$\frac{G}{N} = \{Ng | g \in G\} = \{Nnh | n \in N, h \in H\} = \{Nh | h \in H\}.$$

Ora consideriamo l'applicazione

$$\begin{aligned} f : H &\longrightarrow \frac{G}{N} \\ h &\longmapsto Nh \end{aligned}$$

f è un omomorfismo di gruppi. Infatti per ogni $h_1, h_2 \in H$ abbiamo che

$$f(h_1h_2) = Nh_1h_2 = (Nh_1)(Nh_2) = f(h_1)f(h_2),$$

per come è definito il prodotto nel gruppo quoziente G/N. Inoltre f è suriettiva proprio perché $G/N = \{Nh | h \in H\}$.

2. Osserviamo che

$$\ker(f) = \left\{h \in H | Nh = \left\{1_{G/N}\right\} = N\right\} = \{h \in H | h \in N\} = H \cap N,$$

pertanto dal primo Teorema di omomorfismo, essendo f suriettiva, segue che

$$\frac{H}{H \cap N} \simeq \frac{G}{N}. \tag{1}$$

Ora se $H \cap N = 1_G$, da (1) si ha subito che $H \simeq G/N$.
Viceversa sia $H \simeq G/N$, allora

$$|H| = |G/N|.$$

D'altra parte da (1) passando alle cardinalità (che sappiamo essere finite) abbiamo che

$$|G/N| = |H| / |H \cap N|,$$

e quindi

$$|H| = |H| / |H \cap N|,$$

ovvero $|H \cap N| = 1$, cioè $H \cap N = \{1_G\}$.

□

Esercizio 5. *Per ogni $n \in \mathbb{N}$ sia*

$$U_n = \{z \in \mathbb{C} | z^n = 1\}$$

Si provi che:

1. *U_n è un sottogruppo normale di $\mathbb{C}^*$;*
2. $$\frac{\mathbb{C}^*}{U_n} \simeq \mathbb{C}^*.$$

Svolgimento. 1) Poiché $\mathbb{C}^*$ è un gruppo abeliano, basta provare che U_n è un sottogruppo di $\mathbb{C}^*$. La verifica è standard.
2) Consideriamo l'applicazione

$$\begin{aligned} \psi : \mathbb{C}^* &\longrightarrow \mathbb{C}^* \\ z &\longmapsto z^n \end{aligned}$$

Si prova agevolmente (tralasciamo la verifica) che questo è un omomorfismo di gruppi, il cui nucleo è proprio U_n. ψ è inoltre suriettivo in quanto preso arbitrariamente $\alpha \in \mathbb{C}, \alpha \neq 0$ il polinomio $x^n\alpha \in \mathbb{C}[x]$ ammette n radici, essendo $\mathbb{C}$ algebricamente chiuso). Detta allora β una radice, si ha $f(\beta) = \alpha$. $\square$

Esercizio 6. *Sia $\sigma : \mathbb{Q} \longrightarrow \mathbb{Q}$ definita da $\sigma(q) = -q$ per ogni $q \in \mathbb{Q}$.*

1. *Provare che σ è un automorfismo del gruppo additivo $(\mathbb{Q}, +, 0)$ d'ordine 2.*
2. *Dimostrare che il prodotto cartesiano $G := \mathbb{Q} \times \langle\sigma\rangle$ munito della seguente operazione*
$$(a, \alpha) \cdot (b, \beta) = (a + \alpha(b), \alpha\beta)$$
è un gruppo.
3. *Trovare il centro di G.*
4. *Per ogni sottogruppo A di $\mathbb{Q}$, provare che*
$$K(A) = \{(a, id) | a \in A\}$$
è un sottogruppo normale di G.
5. *Detto $H = \langle(0, \sigma)\rangle$, dimostrare che $G = K(\mathbb{Q}) \cdot H$.*
6. *Calcolare*
$$\left| \frac{G/K(\mathbb{Z})}{K(\mathbb{Q})/K(\mathbb{Z})} \right|.$$

Svolgimento.
1) Abbiamo che $\sigma(a + b) = -(a + b) = -a - b = \sigma(a) + \sigma(b)$, per ogni $a, b \in \mathbb{Q}$. Inoltre $\sigma^2(a) = \sigma(-a) = -(-a) = a = id(a)$, quindi $|\sigma| = 2$.

2) Presi tre arbitrari elementi di G, abbiamo che

$$\begin{aligned} (a, \alpha) \cdot \Big((b, \beta) \cdot (c, \gamma) \Big) &= (a, \alpha) \cdot (b + \beta(c), \beta\gamma) = (a + \alpha(b + \beta(c)), \alpha(\beta\gamma)) \\ &= (a + \alpha(b) + \alpha\beta(c), \alpha\beta\gamma) \\ \Big((a, \alpha) \cdot (b, \beta) \Big) \cdot (c, \gamma) &= (a, \alpha(b), \alpha\beta) \cdot (c, \gamma) = (a + \alpha(b) + \alpha\beta(c)), (\alpha\beta)\gamma)) \\ &= (a + \alpha(b) + \alpha\beta(c), \alpha\beta\gamma) \end{aligned}$$

Pertanto il prodotto è associativo.
Si vede poi che l'elemento $(0, id)$ è l'unità per G e che l'inverso del generico (a, α) è

$$(a, \alpha)^{-1} = \begin{cases} (-a, id) & \text{se } \alpha = id \\ (a, \sigma) & \text{se } \alpha = \sigma \end{cases}$$

3) Sia $(x, \eta) \in Z(G)$, allora da $(x, \eta)(0, \sigma) = (0, \sigma)(x, \eta)$ abbiamo che

$$x = \sigma(x)$$

cioè $x = -x$, ovvero $x = 0$. Ora, da $(0, \eta)(1, id) = (1, id)(0, \eta)$ segue

$$0 + \eta(1) = 1 + id(0)$$

cioè $\eta(1) = 1$, e quindi $\eta = id$. Deduciamo così che $Z(G) = \{(0, id)\}$ è il sottogruppo banale di G.

4) Siano $(a, id), (b, id) \in K(A)$. Allora

$$(a, id)(b, id)^{-1} = (a, id)(-b, id) = (a - b, id \in K(A)$$

poiché $a - b \in A$ essendo A un sottogruppo di $\mathbb{Q}$.
Presi arbitrariamente $(b, \beta) \in G$ e $(a, id) \in K(A)$, abbiamo che

$$(b, \beta)^{-1}(a, id)(b, \beta) = (\pm a, id) \in K(A)$$

(tralascio i conti). Ne segue che $K(A) \trianglelefteq G$.

5) Per ogni $(a, \alpha) \in G$ si ha che

$$(a, \alpha) = (a, id)(0, \alpha) \in K(A)H,$$

dunque $G = K(A)H$.

6) Applicando il III Teorema di omomorfismo di gruppi otteniamo che

$$\left| \frac{G/K(\mathbb{Z})}{K(\mathbb{Q})/K(\mathbb{Z})} \right| = \left| \frac{G}{K(\mathbb{Q})} \right| = 2.$$

$\square$

Esercitazione n. 10

24/10/2016

Argomenti. Omomorfismi e Teoremi di omomorfismi di gruppo.

Esercizio 1. *Si provi che il gruppo additivo* $(\mathbb{Z}[X], +)$ *dei polinomi a coefficienti interi è isomorfo al gruppo moltiplicativo* $(\mathbb{Q}_{>0}, \cdot)$.

Svolgimento. Fissiamo un qualunque ordinamento dell'insieme $\mathbb{P} = \{p_0, p_1, \ldots\}$ dei numeri primi e consideriamo l'applicazione $\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Q}_{>0}$ definita ponendo

$$\phi(a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0) = p_0^{a_0} \cdot p_1^{a_1} \cdot \ldots \cdot \cdot p_n^{a_n}.$$

È banale ora verificare che ϕ è un isomorfismo. □

Esercizio 2. *Sia* A *un gruppo abeliano e per ogni* $n \in \mathbb{N}$ *sia* $\rho_n : A \longrightarrow A$ *definita ponendo* $\rho_n(a) = a^n$, *per ogni* $a \in A$.

1. *Provare che* ρ_n *è un omomorfismo di* A;
2. *se* $|A| < \infty$, *allora* $\rho_n \in \mathrm{Aut}\,(A)$ *se e solo se* $(n, |A|) = 1$;
3. *mostrare un esempio di gruppo infinito in cui* ρ_2 *sia iniettiva e non suriettiva;*
4. *mostrare un esempio di gruppo infinito in cui* ρ_2 *sia suriettiva non-iniettiva.*

Svolgimento. 1) Presi arbitrariamente $a, b \in A$, essendo A abeliano abbiamo che:

$$\rho_n(ab) = (ab)^n = a^n b^n = \rho_n(a)\rho_n(b).$$

2) Assumiamo che sia $(n, |A|) = 1$ e proviamo che $\rho_n \in \mathrm{Aut}\,(A)$.
Sia $a \in \ker(\rho_n)$. Allora $a^n = 1$, da cui segue che $|a|\,|n$. Poiché per il Teorema di Lagrange abbiamo anche che $|a|\,|\,|A|$, allora $|a|$ divide il massimo comune divisore $(n, |A|) = 1$ e pertanto l'omomorfismo ρ_n ha nucleo banale. Essendo ρ_n un'applicazione iniettiva da un insieme finito in s
'e, ρ_n è anche suriettiva, ovvero è un automorfismo di A.
Viceversa sia $\rho_n \in \mathrm{Aut}\,(A)$ e sia $d = (n, |A|)$. Proviamo che $d = 1$. Se fosse

$d \neq 1$, prendiamo un numero primo $p|d$ e un elemento $x \in A$ d'ordine p (un tale elemento esiste sempre, vedi lezione Prof. Puglisi). Allora poiché $p|n$ si ha

$$\rho_n(x) = x^n = 1 = \rho_n(1)$$

ed essendo ρ_n iniettiva, avremmo l'assurdo $x = 1$.

3) Basta prendere $A = \mathbb{Z}$, $\rho_2(z) = 2z$ per ogni $z \in \mathbb{Z}$ è iniettiva non suriettiva.

Sia

$$G = U_2 = \left\{ z \in \mathbb{C}^* | z^{2^t} = 1 \text{ per qualche } t \in \mathbb{N} \right\}$$

Abbiamo che U_2 è un sottogruppo di $\mathbb{C}^*$ e che $\rho_2 : U_2 \longrightarrow U_2$. Poiché ad esempio $\rho_2(1) = 1 = \rho_2(-1)$, tale applicazione non è iniettiva. È però suriettiva, perché se w è un arbitrario elemento di U_2, con $w^{2^r} = 1$, allora presa una radice h del polinomio $x^2 - y \in \mathbb{C}[x]$, che sappiamo sempre esistere poiché $\mathbb{C}$ è algebricamente chiuso, abbiamo che $\rho_2(h) = w$ e $h^{2^{r+1}} = w^{2^r} = 1$, quindi h è una retroimmagine in U_2 dell'elemento w. $\square$

Esercitazione n. 11

27/10/2016

Argomenti. Prodotto diretto (esterno ed interno) di gruppi.

Vengono introdotte le nozioni di prodotto diretto interno ed esterno di gruppi, come nelle dispense del corso (pagg. 53–55).

Esercizio 1. *Sia A un gruppo abeliano finito. Si provi che*

$$A = P \times D$$

dove $P = \{a \in A \mid |a| = 2^m$ per qualche $m \in \mathbb{N}\}$ e $D = \{a \in A \mid |a|$ è dispari$\}$.

Svolgimento. Sia a un arbitrario elemento di A e sia $|a| = 2^k d$ con $k \in \mathbb{N}$ e $(2, d) = 1$. Esistono allora $\alpha, \beta \in \mathbb{Z}$ tali che $1 = 2^k\alpha + d\beta$. Pertanto

$$a = a^{2^k\alpha + d\beta} = a^{2^k\alpha} a^{d\beta},$$

ed è immediato accorgersi che $a^{2^k\alpha}$ ha ordine dispari che divide d, mentre $a^{d\beta}$ ha ordine un divisore di 2^k e quindi una potenza di 2. Data la geniricità con cui si è scelto $a \in A$, ne segue che

$$A = DP = PD.$$

È banale che P e D sono normali in A, poiché questo è un gruppo abeliano. Dalle definizioni di P e D si ha pure immediatamente che $P \cap D = \{1_A\}$. $\square$

Esercizio 2. *Sia A un gruppo abeliano e sia $\alpha \in \mathrm{Aut}\,(A)$ tale che $\alpha^2 = id$. Provare quanto segue.*

1. *Gli insiemi $C = \{a \in A | \alpha(a) = a\}$ e $D = \left\{a \in A | \alpha(a) = a^{-1}\right\}$ sono sottogruppi di A.*
2. *Per ogni $a \in A$ vale che $\alpha(a^{-1})a \in D$.*
3. *$A^2 = \left\{a^2 | a \in A\right\}$ è contenuto in CD.*
4. *Se A è finito e di ordine dispari, allora $A = C \times D$.*

Svolgimento. 1) Tralascio questa verifica perché è immediata.

2)

$$\alpha(\alpha(a^{-1})a) = \alpha^2(a^{-1})\alpha(a) = a^{-1}\alpha(a) = (\alpha(a^{-1})a)^{-1}$$

essendo $\alpha^2 = id$, e quindi $\alpha(a^{-1})a \in D$.

3)

$$a^2 = a\alpha(a)\alpha(a^{-1})a \in CD$$

poiché in modo simile a quanto fatto al punto 2) abbiamo che $a\alpha(a) \in C$.

4) Essendo $|A|$ finito d'ordine dispari, l'applicazione $f : A \longrightarrow A$ che associa ad ogni a in A, $f(a) = a^2$ è iniettiva. Pertanto è pure suritettiva, cioè $A = A^2$. Il risultato segue ora dal punto precedente. $\square$

Esercitazione n. 12

03/11/2016

Argomenti. Esercizi sui gruppi di permutazione.

Esercizio 1 *Nel gruppo simmetrico S_8 si considerino i seguenti elementi*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 2 & 3 & 8 & 1 & 7 & 6 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 7 & 8 & 1 & 5 & 3 & 2 \end{pmatrix}$$

Scrivere σ, τ e $\sigma\tau$ come prodotto di cicli disgiunti. Calcolare gli ordini di σ, τ e $\sigma\tau$. Calcolare $\tau^{-1}\sigma\tau$ e il suo ordine.

Dimostrazione. Si ha

$$\begin{aligned} \sigma &= (1586)(243) \\ \tau &= (165)(248)(37), \end{aligned}$$

mentre

$$\sigma\tau = (1586)(243)(165)(248)(37) = (285)(347).$$

Ora l'ordine di una permutazione è il minimo comune multimo delle lunghezze dei suoi cicli disgiunti, detto esplicitamente, una volta scritta la generica permutazione π come prodotto di cicli disgiunti

$$\pi = \pi_1\pi_2 \dots \pi_h,$$

se ogni ciclo π_i è un m_i ciclo (i.e. $\pi_i = (a_1 a_2 \dots a_{m_i})$), allora

$$|\pi| = m.c.m.(m_1, m_2, \dots, m_h).$$

Pertanto $|\sigma| = 4 \cdot 3 = 12$, $|\tau| = 3 \cdot 2 = 6$, $|\sigma\tau| = 3$.
Per calcolare il coniugato di σ tramite τ, ovvero $\tau^{-1}\sigma\tau$, posso procedere in

due modi. O, "brutalmente", invertire τ e moltiplicarlo per il già calcolato $\sigma\tau$, oppure in maniera più agevole, ricordarsi che $\tau^{-1}\sigma\tau$ è ancora dello stesso tipo ciclico di σ e sostituire ad ogni elemento j che compare in σ esattamente $j\tau$; così facendo si ottiene

$$\tau^{-1}\sigma\tau = (1\tau 5\tau 8\tau 6\tau)(2\tau 4\tau 3\tau) = (6125)(487).$$

Poiché il coniugio è un automorfismo del gruppo $|\tau^{-1}\sigma\tau| = |\sigma| = 12$. $\square$

Esercizio 2 *Scrivere i tipi degli elementi rispettivamente dei gruppi S_3 ed S_4 e per ciascun tipo dire quanti elementi ci sono.*

Dimostrazione. Il gruppo S_3.
S_3 ha ordine $3! = 6$ i suoi elementi non banali sono o scambi (cioè del tipo (ab)) o 3-cicli (cioè del tipo (abc)). Ci sono esattamente $\frac{3\cdot 2}{2} = 3$ scambi (infatti il primo elemento a si può scegliere in 3 modi, b in 2, e poi il tutto va diviso per 2, poiché le scritture (ab) e (ba) rappresentano lo stesso elemento di S_3). In maniera simile si calcolano i $3-$cicli. Questi sono in numero di $\frac{3\cdot 2}{3} = 3$. Aggiungendo l'elemento banale, se vogliamo l'unico elemento la struttura ciclica è vuota, si hanno 6 elementi e quindi tutti gli elementi di S_3. In pratica

$$S_3 = \{1_{S_3}, (12), (13), (23), (123), (132)\}.$$

Il gruppo S_4.
$|S_4| = 4! = 24$. Gli elementi non banali di S_4 hanno uno dei seguenti tipi

$$(ab), \quad (abc), \quad (abcd) \quad \text{e} \quad (ab)(cd).$$

Ci sono $\frac{4\cdot 3}{2} = 6$ scambi, $\frac{4\cdot 3\cdot 2}{3} = 8$ elementi del tipo (abc), $\frac{4\cdot 3\cdot 2}{4} = 6$ del tipo $(abcd)$. Gli elementi del tipo $(ab)(cd)$ vengono chiamati doppi scambi e sono in numero di

$$\frac{4\cdot 3\cdot 2}{2\cdot 2\cdot 2} = 3,$$

infatti ci sono 4 scelte per a, 3 per b, 2 per c (una per d), poi devo dividere per un primo 2, poiché (ab) lo posso scrivere in due modi, un secondo 2, poiché (cd) lo posso scrivere in due modi, ed un ultimo 2, poiché le scritture $(ab)(cd)$ e $(cd)(ab)$ rappresentano lo stesso elemento. Contando gli elementi di tutti diversi tipi si ha

$$1 + 6 + 8 + 6 + 3 = 24 = |S_4|,$$

quindi esauriamo giustamente, tutti gli elementi di S_4. $\square$

Esercizio 3 *All'interno del gruppo simmetrico S_4, si consideri il sottoinsieme*

$$V_4 := \{1_{S_4}, (12)(34), (13)(24), (14)(23)\}.$$

1. *Si mostri che V_4 è un sottogruppo normale di S_4.*
2. *Sia $H := \{\sigma \in S_4 | 4\sigma = 4\}$. Si mostri che H è un sottogruppo di S_4.*
3. $H \simeq S_3$.
4. $V_4 \cap H = \{1_{S_4}\}$
5. $S_4 = V_4 H$.
6. $S_4/V_4 \simeq S_3$.

Dimostrazione. Osserviamo preliminarmente che come insieme V_4 è l'unione dei tipi $\varnothing = \{1_{S_4}\}$ e $\{(ab)(cd)\}$. Pertanto poiché l'operazione di coniugio preserva i tipi, preso un qualsiasi $v \in V_4$ e $\sigma \in S_4$, $\sigma^{-1}v\sigma$ è dello stesso tipo di v e quindi sta in V_4. Ne consegue che basta provare che V_4 è un sottogruppo di S_4, la normalità è garantita da quanto appena detto. Ora siano $\alpha = (12)(34)$, $\beta = (13)(24)$ e $\gamma = (14)(24)$, un rapido conteggio mostra che

$$\begin{aligned} \alpha\beta = \beta\alpha = \gamma \\ \alpha\gamma = \gamma\alpha = \beta \\ \beta\gamma = \gamma\beta = \alpha \end{aligned}$$

da cui segue che V_4 è un sottogruppo di S_4.
H è un sottogruppo di S_4, infatti se σ_1 e $\sigma_2 \in H$, allora $4\sigma_2 = 4$ e quindi pure $4\sigma_2^{-1} = 4$, pertanto $4\sigma_1\sigma_2^{-1} = 4\sigma_2^{-1} = 4$, ovvero $\sigma_1\sigma_2^{-1} \in H$, e $H \leq S_4$.
Inoltre gli elementi di H sono

$$H = \{1_{S_4}, (12), (13), (23), (123), (132)\},$$

da cui segue subito che $H \simeq S_3$.
È evidente che l'unità è l'unico elemento di V_4 che fissa 4, pertanto

$$V_4 \cap H = \{1_{S_4}\}.$$

Essendo $V_4 \trianglelefteq S_4$, V_4H è un sottogruppo di S_4, il cui ordine è

$$|V_4H| = \frac{|V_4|\,|H|}{|V_4 \cap H|} = 4 \cdot 6 = 24 = |S_4|\,,$$

pertanto $V_4H = S_4$.
Infine applicando il secondo Teorema di omomorfismo si ha

$$\frac{S_4}{V_4} = \frac{V_4H}{V_4} \simeq \frac{H}{V_4 \cap H} \simeq H \simeq S_3.$$

$\square$

Esercitazione n. 13

07/11/2016

Argomenti. Esercizi sui gruppi di permutazione.

Esercizio 1 *1. Si scriva lelemento* (123) *di* S_3 *come prodotto di scambi in due modi diversi.*

2. Si scrivano tutti gli elementi del gruppo A_4*.*

Svolgimento. 1. Abbiamo che

$$(123) = (12)(13) = (12)(12)^{(23)} = (12)(23)(12)(23).$$

2.

$$A_4 = \{id, (123), (132), (124), (142), (134), (143), (234), (243), \\ (12)(34), (13)(24), (14)(23)\}.$$

L'esempio che segue mostra che in generale il Teorema di Lagrange non è invertibile.

Esercizio 2 *Il gruppo alterno* A_4 *d'ordine 12 non possiede sottogruppi d'ordine 6.*

Svolgimento. Supponiamo che A_4 ammetta un sottogruppo H d'ordine 6. Allora H ha indice 2 in A_4, quindi H è normale in A_4. Anche il sottogruppo V_4 d'ordine 4 è normale in A_4, pertanto si ha che il sottogruppo $H \cap V_4$ è normale in A_4. Ora tale sottogruppo ha ordine 2. Infatti abbiamo che

$$|HV_4| = \frac{6 \cdot 4}{|H \cap V_4|} \leq 12,$$

da cui segue necessariamente che $H \cap V_4$ ha ordine 2. Ma allora $H \cap V_4$ oltre all'unità contiene un solo elemento d'ordine 2, cioè del tipo $(ab)(cd)$, ovvero $H \cap V_4$ è uno fra i tre sottogruppi

$$\langle (12)(34) \rangle \,, \quad \langle (13)(24) \rangle \,, \quad \langle (14)(23) \rangle \,.$$

Ora una rapida verifica[1] mostra che nessuno di questi tre sottogruppi è normale in A_4, il che contraddice quanto precedentemente osservato.

Esercizio 3 *Si mostri che per $n \geq 3$ il centro di S_n è il sottogruppo banale.*

Dimostrazione. Sia π un elemento non banale di $Z(S_n)$. Allora esiste un certo $i \in \{1, 2, \ldots, n\}$ appartenente al supporto di π, ovvero tale che $i\pi = j$, per qualche $j \neq i$ ($j \in \{1, 2, \ldots, n\}$). Ora poiché $n \geq 3$ esiste un k diverso da i e da j in $\{1, 2, \ldots, n\}$. Possiamo pertanto considerare la trasposizione $\alpha = (ik) \in S_n$. Facciamo

$$\pi^{-1}\alpha\pi = \alpha^{\pi}.$$

Da un lato si ha che

$$\alpha^{\pi} = \alpha = (ik),$$

essendo $\pi \in Z(S_n)$. D'altra parte, per la regola del coniugio

$$\alpha^{\pi} = (ik)^{\pi} = (i\pi\, k\pi) = (j\, k\pi),$$

Dunque

$$(ik) = (j\, k\pi),$$

che è assurdo, essendo j diverso sia da i che da k. Se ne conclude che $Z(S_n) = \{1\}$. $\square$

Esercizio 4 *Sia G un gruppo qualsiasi e sia $Z(G)$ il centro di G. Si mostri che se il gruppo quoziente $G/Z(G)$ è un gruppo ciclico allora G è abeliano, dunque $G/Z(G) = \{1\}$.*

Dimostrazione. Poiché $G/Z(G)$ è ciclico sia $G/Z(G) = \langle Z(G)x \rangle$. Ma allora ogni elemento $g \in G$ si può scrivere come $g = cx^a$, per un opportuno $c \in Z(G)$ e $a \in \mathbb{Z}$. Ne segue che

$$G = Z(G) \cdot \langle x \rangle \,.$$

[1] Ad esempio: $\langle (12)(34) \rangle \ntrianglelefteq A_4$, poiché $(12)(34)^{(123)} = (23)(14) \notin \langle (12)(34) \rangle$.

Ora presi g_1, g_2 arbitrari in G, esistono $c_1, c_2 \in Z(G)$ ed $a, b \in \mathbb{Z}$ tali che $g_1 = c_1 x^a$ e $g_2 = c_2 x^b$. Dunque

$$g_1 g_2 = c_1 x^a c_2 x^b = c_1 c_2 x^a x^b = c_2 c_1 x^{a+b} = c_2 c_1 x^b x^a = c_2 x^b c_1 x^a = g_2 g_1,$$

ovvero g_1 e g_2 commutano. Data la genericità con cui sono stati scelti g_1 e g_2, abbiamo provato che G è abeliano, dunque $G = Z(G)$. $\square$

Esercizio 5 *Nel gruppo simmetrico S_6 si consideri la permutazione*

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$$

Si scriva τ come prodotto di cicli disgiunti e si calcoli l'ordine del di τ e del suo centralizzante in S_6. Si determinino due sottogruppi propri, H e K, di $C = C_{S_6}(\tau)$ tali che $C = K \cdot H$, $|C : K| = 2$ e $H \cap K = \{1_{S_6}\}$.

Svolgimento. Abbiamo che

$$\tau = (135)(264)$$

ha ordine tre. Poiché il centralizzante di un elemento del gruppo coincide con lo stabilizzatore dell'azione di coniugio si ha che

$$|C_{S_6}(\tau)| = \frac{|S_6|}{|(\tau)^{S_6}|} = \frac{6!}{|(\tau)^{S_6}|},$$

doce $(\tau)^{S_6}$ indica la classe di coniugio in S_6 di τ. Ora gli elementi di S_6 coniugati a τ sono tutti e soli quelli aventi lo stesso tipo di τ, ovvero sono tutti e soli quelli della forma

$$(abc)(def),$$

di questi in S_6 ce ne sono esattamente $\frac{6!}{3 \cdot 3 \cdot 2} = 5 \cdot 4 \cdot 2 = 40$. Pertanto $|C_{S_6}(\tau)| = 6!/40 = 18$.
Fra gli elementi di S_6 che commutano con $(135)(264)$ ci sono sicuramente (135) e (264) e quindi il sottogruppo da loro generati, ovvero il sottogruppo d'ordine 9

$$K := \langle (135) \rangle \cdot \langle (264) \rangle \simeq C_3 \times C_3.$$

K ha indice 2 in $C_{S_6}(\tau)$ quindi è normale. Ora un altro elemento che commuta con τ è

$$(12)(36)(54).$$

questo genera un sottogruppo, H, d'ordine due e pertanto si ha che

$$C_{S_6}(\tau) = K \cdot H$$

e $H \cap K = \{id\} = \{1_{S_6}\}$.

Esercitazione n. 14

10/11/2016

Argomenti. Esercizi sui gruppi di permutazione.

Esercizio 1. *Mostrare che il gruppo S_n è generato dalle due permutazioni* (12) *e* $(123\dots n)$.

Dimostrazione. Sia K il sottogruppo generato da (12) e $(123\dots n)$. Sappiamo che ogni permutazione puoò essere scritta come prodotto di cicli, pertanto per provare l'enunciato occorre e basta mostrare che ogni ciclo (ab) appartiene a K. Osserviamo inoltre che se $b = 1$, $(ab) = (1a)$, mentre se $b \neq 1$ si ha $(ab) = (ba) = (1a)^{(1b)}$. Questa osservazione ci consente di limitare ulteriormente le nostre ricerche, ci basta infatti adesso provare che ogni ciclo della forma $(1a)$, al variare di $a = 2, 3, \dots, n$, appartiene a K. È ovvio dalla definizione di K che $(12) \in K$. Inoltre si ha

$$(12)^{(123\dots n)} = (23) \in K$$

e dunque pure

$$(12)^{(23)} = (13) \in K.$$

Ma ora abbiamo anche che

$$(13)^{(123\dots n)} = (24) \in K,$$

da cui segue

$$(12)^{(24)} = (14) \in K.$$

Procedendo per induzione e assumendo d'aver provato che $(1i) \in K$, si ha

$$(1i)^{(123\dots n)} = (2\,i+1) \in K,$$

da cui segue

$$(12)^{(2\,i+1)} = (1\,i+1) \in K.$$

Quindi ogni $(1a) \in K$ e, per i ragionamenti sopra descritti, $K = S_n$. $\square$

Introduciamo il *gruppo dei Quaternioni* Q_8.
Siano i, j e k tre elementi distinti e definiamo i prodotti tra questi come

$$i^2 = j^2 = k^2 = -1,$$

$$
\begin{aligned}
ij &= k, \qquad ji = -k,\\
jk &= i, \qquad kj = -i,\\
ki &= j, \qquad ik = -j,
\end{aligned}
$$

sia inoltre 1 l'elemento neutro rispetto a tale prodotto e sia

$$Q_8 := \{1, -1, i, j, k, -i, -j, -k\}.$$

Allora Q_8 con il prodotto così definito è un gruppo non commutativo d'ordine 8, detto *Gruppo dei quaternioni*.

Dimostrazione. Il prodotto è ben definito in Q_8, inoltre una verifica diretta (che omettiamo) mostra che è anche associativo. L'elemento 1 è l'unità del gruppo.
L'elemento -1 ha ordine 2. Mentre da $i^2 = j^2 = k^2 = -1$ si ricava subito che i, j e k hanno periodo quattro e che

$$i^3 = i^{-1} = -i, \quad j^3 = j^{-1} = -j, \quad k^3 = k^{-1} = -k.$$

Q_8 non è abeliano poiché ad esempio $k = ij \neq ji = -k$. □

Esercizio 2. *Trovare e descrivere tutti i sottogruppi di Q_8. Mostrare che essi sono tutti ciclici e normali in Q_8 (anche se Q_8 non è abeliano)*

Dimostrazione. Per il Teorema di Lagrange ogni sottogruppo proprio non banale di Q_8 ha ordine due o quattro. Per quanto detto sopra -1 è l'unico elemento di Q_8 di periodo due, ne segue che esiste un solo sottogruppo d'ordine 2 ed è $\langle -1 \rangle = \{1, -1\}$. Esso è normale in Q_8, e poiché l'elemento -1 commuta con ogni elemento di Q_8, i.e.

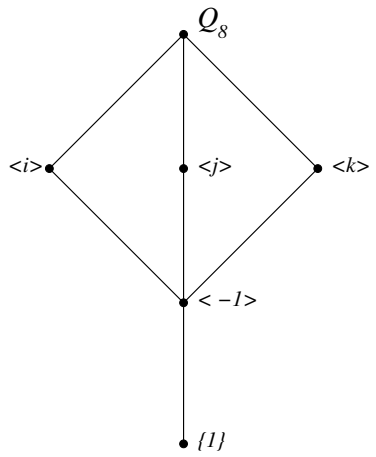
$$-1 \cdot i = -i = i \cdot -1, \quad -1 \cdot j = -j = j \cdot -1, \quad -1 \cdot k = -k = k \cdot -1,$$

il sottogruppo $\langle -1 \rangle$ è contenuto nel centro $Z(Q_8)$. Poiché i, j e k hanno periodo 4 i sottogruppi

$$
\begin{aligned}
\langle i \rangle &= \left\{1, i, -1 = i^2, -i = i^3\right\}\\
\langle j \rangle &= \left\{1, j, -1 = j^2, -j = j^3\right\}\\
\langle k \rangle &= \left\{1, k, -1 = k^2, -k = k^3\right\}
\end{aligned}
$$

hanno ordine 4, ovvero indice due in Q_8. Essendo ogni sottogruppo d'indice due normale, essi sono normali in Q_8. Non ci sono altri sottogruppi ed il reticolo dei sottogruppi di Q_8 è il seguente □

Esercizio 3. *Si trovi un sottogruppo del gruppo simmetrico S_8 che è isomorfo a Q_8.*



Dimostrazione. Occorre trovare un sottogruppo non abeliano d'ordine 8 in cui ci sono tre elementi d'ordine quattro che generano tre sottogruppi ciclici distinti e tali che hanno lo stesso quadrato. Prendiamo

$$a = (1234)(5678).$$

È evidente che $|a| = 4$ e che

$$a^2 = (13)(24)(57)(68).$$

Ricomponendo i fattori in modo diverso, si vede che questo è anche il quadrato dell'elemento

$$b = (1537)(2846).$$

Ora faccio ab, ottengo

$$ab = (1234)(5678)(1537)(2846) = (1836)(2745) =: c.$$

Ovviamente si ha $c^2 = a^2 = b^2 = (13)(24)(57)(68)$, inoltre

$$bc = (1537)(2846)(1836)(2745) = (1234)(5678) = a$$

e

$$ca = (1836)(2745)(1234)(5678) = (1537)(2846) = b.$$

Pertanto detto $H := \{1, a^2, a, b, c, a^3, b^3, c^3\}$, l'applicazione

$$\begin{aligned} \varphi : Q_8 &\longrightarrow H \\ 1 &\longmapsto 1_{S_4} \\ -1 &\longmapsto a^2 \\ i &\longmapsto a \\ j &\longmapsto b \\ k &\longmapsto c, \end{aligned}$$

induce l'isomorfismo voluto. □

Esercitazione n. 15

14/11/2016

Argomenti. Esercizi sui gruppi di permutazione.

Esercizio 1. *Sia* $G := \langle g \rangle$ *un gruppo ciclico d'ordine 9, si provi che* $\mathrm{Aut}\,(G)$ *è ciclico d'ordine 6.*

Dimostrazione. Incominciamo con l'osservare che ogni automorfismo α del gruppo ciclico $\langle g \rangle$ è in modo unico determinato dalla scelta dell'elemento $\alpha(g)$. Infatti una volta stabilita l'immagine di g tramite α, ovvero $\alpha(g) =: x$, il generico elemento g^k di $\langle g \rangle$ avrà immagine tramite α

$$\alpha(g^k) = (\alpha(g))^k = x^k,$$

essendo α un omomorfismo. Pertanto se α e β sono due automorfismi di $\langle g \rangle$ tali per cui $\alpha(g) = \beta(g)$, allora per ogni g^k, $\alpha(g^k) = \beta(g^k)$, cioè $\alpha \equiv \beta$. Ora se α è un automorfismo e g un generatore di $\langle g \rangle$, $\alpha(g)$ deve anch'esso essere un generatore di $\langle g \rangle$ (poiché ad esempio $|\alpha(g)| = |g| = |\langle g \rangle|$). Ne segue che gli automorfismi di $\langle g \rangle$ sono in corrispondenza biounivoca con i generatori di $\langle g \rangle$, ovvero

$$|\mathrm{Aut}\,(\langle g \rangle)| = |\{\text{generatori di } \langle g \rangle\}|\,.$$

Nel nostro caso $G := \langle g \rangle$ è ciclico d'ordine 9, pertanto $|\mathrm{Aut}\,(G)| = \varphi(9) = 6$, dove φ è la funzione di Eulero. Da ultimo mostriamo che esiste un elemento di $\mathrm{Aut}\,(G)$ d'ordine esattamente 6, il che prova che si tratta di un gruppo ciclico d'ordine 6. Considero l'automorfismo δ così definito

$$\delta(g) = g^2,$$

e quindi $\delta(g^k) = (\delta(g))^k = g^{2k}$ per ogni $k = 0, 1, 2, \ldots, 8$. Osservo che, poiché $(2, 9) = 1$, g^2 è un generatore per $\langle g \rangle$ e quindi δ è effettivamente un automorfismo di G. Inoltre si ha che

$$\delta^2 :\ g \xrightarrow[\delta]{} g^2 \xrightarrow[\delta]{} g^4, \qquad \text{ovvero } \delta^2(g) = g^4$$

$$\delta^3 :\ g \xrightarrow[\delta]{} g^2 \xrightarrow[\delta]{} g^4 \xrightarrow[\delta]{} g^8 = g^{-1}, \qquad \text{ovvero } \delta^3(g) = g^{-1}$$

e quindi $\delta^i(g) \neq g$ per ogni i compreso tra 2 e 5; ne segue che $|\delta| = 6$ e $\mathrm{Aut}\,(G) = \langle \delta \rangle$ è ciclico d'ordine 6. $\square$

Esercizio 2. *Sia $G = A \times B$ il prodotto diretto di due suoi sottogruppi A e B. Si mostri che il centro di G è il prodotto diretto del centro di A per quello di B, in termini*

$$Z(G) = Z(A) \times Z(B).$$

Dimostrazione. Incominciamo col provare che sia $Z(A)$ che $Z(B)$ stanno nel centro di G. Siano $x \in Z(A)$ e $g \in G = A \times B$ arbitrari, allora scritto $g = ab$ (con $a \in A$ e $b \in B$), si ha che

$$xg = xab = axb = abx = gx,$$

poiché x commuta con a (essendo $x \in Z(A)$ e $a \in A$) e x commuta con b (essendo $x \in A$ e $b \in B$, ed il prodotto è diretto). Pertanto x commuta con ogni elemento di G, e quindi $x \in Z(G)$, ovvero $Z(A) \leq Z(B)$. Similmente si prova che $Z(B) \leq Z(G)$. Ora essendo ogni sottogruppo del centro un sottogruppo normale del gruppo, i sottogruppi $Z(A)$ e $Z(B)$ sono in particolare sottogruppi permutabili, quindi $Z(A)Z(B)$ è un sottogruppo di G tale che $Z(A)Z(B) \leq Z(G)$. Viceversa sia ora $y \in Z(G)$ e scrivamo y in modo unico come $y = a'b'$, con $a' \in A$ e $b' \in B$. Ora per ogni $a \in A$ abbiamo che $ya = ay$, ovvero

$$a'b'a = aa'b'$$

ma b' ed a commutano, quindi da sopra a sinistra si ha

$$a'ab' = aa'b',$$

semplificando per b' a destra otteniamo

$$a'a = aa',$$

e questo vale per ogni scelta di $a \in A$, cioè a' è un elemento di $Z(A)$. Similmente si prova che $b' \in Z(B)$, e pertanto $g = a'b' \in Z(A)Z(B)$, cioè $Z(G) = Z(A)Z(B)$. Da ultimo osserviamo che il prodotto $Z(A)Z(B)$ è diretto. È ovvio che $Z(A)$ e $Z(B)$ sono normali in $Z(G)$ (ad esempio poiché $Z(G)$ è un sottogruppo abeliano) reata da verificare che $Z(A) \cap Z(B) = \{1\}$, ma

$$Z(A) \cap Z(B) \leq A \cap B = \{1\}.$$

$\square$

17/10/2016

ES 1. Poiché i quozienti di un gruppo abeliano sono gruppi abeliani, un'implicazione è ovvia.

Siano G/A e G/B abeliani e siano $x, y \in G$ arbitrari.

Poiché G/A è abeliano, abbiamo

$$xA \cdot yA = xyA = yxA = yA \cdot xA$$

cioè $y^{-1}x^{-1}yx \in A$.

Similmente $y^{-1}x^{-1}yx \in B$.

Pertanto

$$y^{-1}x^{-1}yx \in A \cap B = \{1\} \Rightarrow y^{-1}x^{-1}yx = 1 \Rightarrow xy = yx.$$

ES 2 1) $(Ng)^r = Ng^r = N \cdot 1 = N \Rightarrow |Ng|$ divide r.

2) Se $G = \mathbb{Z}$ e $N = 2\mathbb{Z}$ $\quad 1 \in \mathbb{Z}$ $\quad |1| = \infty$ e $|1 + 2\mathbb{Z}| = 2$.

Se $G = GL(2, \mathbb{R})$ $\quad N = Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R}\ a \neq 0 \right\}$

allora $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ha periodo infinito in G così come l'elemento $Z(G) \cdot g \in G/Z(G)$.

$$\left((Z(G) \cdot g)^n = Z(G) \cdot \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \forall n \in \mathbb{N} \right)$$

ES 3 1) Tralascio la verifica che G è un sottogruppo di $GL(2, \mathbb{Q})$ perché è standard.

2) Idem

3) Sia $\alpha = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in G$ e $\beta = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ allora

$$\alpha^{-1}\beta\alpha = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a^{-1} & a^{-1}h - b \\ 0 & a \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a^{-2}h \\ 0 & 1 \end{pmatrix}$$

Quindi se $\beta \in H$ (cioè $h \in \mathbb{Q}$) $\alpha^{-1}\beta\alpha \in H$ e quindi $H \trianglelefteq G$.

$K \not\triangleleft G$ perché ad esempio

$$\begin{pmatrix} 2^{-1} & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 1/4 \\ 0 & 1 \end{pmatrix} \notin K.$$

Invece $K \triangleleft H$ perché

$$\begin{pmatrix} 1 & h \\ & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \in K \qquad \forall h \in \mathbb{Q},\ \forall z \in \mathbb{Z}.$$

4) $f: H \longrightarrow \mathbb{Q}$ è un omom. ben definito, iniettivo e suriettivo.

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$$

Considero $\varphi: G \longrightarrow \mathbb{Q}^*$

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto a$$

Allora si verifica che: ① φ è omom. di gruppi.

② $\operatorname{Ker}\varphi = H$

③ $\operatorname{Im}\varphi = \mathbb{Q}^*$

Pertanto per il I teorema di omomorfismo si ha

$$G/H = G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi = \mathbb{Q}^*.$$

Esercitazione n. 17

21/11/2016

Argomenti. Esercizi sulle azioni di gruppo e sui Teoremi di Sylow.

Esercizio 1. *Sia G il gruppo simmetrico S_3 e sia Ω l'insieme $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Si mostri che la seguente legge definisce un'azione di G su Ω*

$$\begin{aligned} G \times \Omega &\longrightarrow \Omega \\ (\sigma, (a_1, a_2, a_3)) &\longmapsto \sigma \cdot (a_1, a_2, a_3) := (a_{1\sigma^{-1}}, a_{2\sigma^{-1}}, a_{3\sigma^{-1}}). \end{aligned}$$

Si mostri che esiste un'unica orbita di lunghezza 6.

Svolgimento. Per provare che la legge dell'enunciato definisce effettivamente un'azione occorre verificare le seguenti due condizioni:

1) $\forall \sigma, \tau \in S_3$ e $\forall (a_1, a_2, a_3) \in \Omega$, vale $\sigma\tau \cdot (a_1, a_2, a_3) = \sigma \cdot (\tau \cdot (a_1, a_2, a_3))$
2) $\forall (a_1, a_2, a_3) \in \Omega$, vale $1_{S_3} \cdot (a_1, a_2, a_3) = (a_1, a_2, a_3)$.

1) Osserviamo che

$$\begin{aligned} \sigma\tau \cdot (a_1, a_2, a_3) &= (a_{1(\sigma\tau)^{-1}}, a_{2(\sigma\tau)^{-1}}, a_{3(\sigma\tau)^{-1}}) \\ &= (a_{1\tau^{-1}\sigma^{-1}}, a_{2\tau^{-1}\sigma^{-1}}, a_{3\tau^{-1}\sigma^{-1}}) \\ &= \sigma \cdot (a_{1\tau^{-1}}, a_{2\tau^{-1}}, a_{3\tau^{-1}}) \\ &= \sigma \cdot (\tau \cdot (a_1, a_2, a_3)). \end{aligned}$$

2) $1_{S_3} \cdot (a_1, a_2, a_3) = (a_{1\mathrm{id}}, a_{2\mathrm{id}}, a_{3\mathrm{id}}) = (a_1, a_2, a_3)$.

Mostriamo ora che esiste un'unica orbita di lunghezza 6.
Osserviamo che se $\mathcal{O}(\omega)$ è l'orbita contenente l'elemento $\omega \in \Omega$, per il Lemma del conteggio si ha che

$$|\mathcal{O}(\omega)| = \frac{|S_3|}{|\mathrm{Stab}_{S_3}(\omega)|} = \frac{6}{|\mathrm{Stab}_{S_3}(\omega)|}.$$

Ne segue che se esiste un'orbita, $\mathcal{O}(\omega)$, costituita da 6 elementi, allora necessariamente

$$\mathrm{Stab}_{S_3}(\omega) = \{1_{S_3}\}.$$

Ora l'azione in questione è quella che permuta le componenti di ogni terna, pertanto se un elemento $\omega = (a_1, a_2, a_3)$ ha due coordinate uguali, allora il suo stabilizzatore è certamente non banale. Ad esempio lo stabilizzatore dell'elemento $(0, 0, 1)$ contiene lo scambio $(12) \in S_3$, e così via... Ne segue che gli unici elementi a stabilizzatore nullo sono quelli del sottoinsieme

$$\Delta := \{(a_1, a_2, a_3) \in \Omega | a_1, a_2, a_3 \text{ sono tutti distinti}\}.$$

Ora è ovvio che $|\Delta| = 6$ (poiché posso scegliere a_1 in tre modi diversi, a_2 in due modi, a_3 in un solo modo). Quindi risulta che Δ coincide proprio con l'orbita dell'elemento $\omega = (0, 1, 2)$, ed essa è l'unica orbita di lunghezza 6.

Proposizione 1. *Sia G un gruppo e sia H un sottogruppo di G di indice finito $[G : H] = n$. Allora esiste un sottogruppo normale $N \trianglelefteq G$ tale che $N \leq H$ e G/N è isomorfo ad un sottogruppo del gruppo simmetrico S_n su n oggetti.*

Dimostrazione. G agisce in modo transitivo sulle classi laterali sinistre di H in G, mediante

$$\begin{aligned} G \times \mathrm{Lat}(G/H) &\longrightarrow \mathrm{Lat}(G/H) \\ (g, xH) &\longmapsto gxH \end{aligned}$$

Si vede immediatamente che questa è un'azione ben definita. Tale azione può anche essere definita tramite

$$\begin{aligned} \psi : G &\longrightarrow S_n \\ g &\longmapsto (xH \longmapsto gxH). \end{aligned}$$

Sia N il nucleo dell'azione, ovvero $N = \ker(\psi)$. Allora si ha che

$$\begin{aligned} N &= \{g \in G | gxH = xH,\ \forall xH \in \mathrm{Lat}(G/H)\} = \left\{g \in G | x^{-1}gx \in H,\ \forall x \in G\right\} = \\ &= \left\{g \in G | g \in xHx^{-1},\ \forall x \in G\right\} = \bigcap_{x \in G} xHx^{-1} =: H_G, \end{aligned}$$

detto il *nocciolo di H*. Ora è evidente che $N \leq H$ e che $N \trianglelefteq G$. Inoltre per il primo Teorema di isomorfismo G/N è isomorfo ad un sottogruppo di S_n. $\square$

Esercizio 2. *Sia G un gruppo finito e sia p il più piccolo primo che divide l'ordine di G. Se G ha un sottogruppo d'indice p, allora questo è normale in G.*

Svolgimento. Per la Proposizione precedente si ha che esiste $N \trianglelefteq G$ tale che $N \leq H \neq G$ e $G/N \lesssim S_p$. Ora $|S_p| = p!$ e per come è definito p, $(|G|, |S_p|) = p$. Ne segue che l'ordine di G/N può essere solamente p. Ovvero $[G : N] = p = [G : H]$, e poiché $N \leq H$, segue $H = N$, cioè H è normale in G.

Proposizione 2. *Sia G un gruppo finito d'ordine $|G| = p^a m$ (dove $p \nmid m$). Detto n_p il numero dei $p-$Sylow di G, abbiamo che*

1. $n_p | m$,

2. $n_p \equiv 1 \pmod{p}$,

3. Se G è semplice, allora $|G|$ divide $(n_p)!$.

Dimostrazione. La Proposizione è stata provata durante le lezioni. Ad ogni modo rivediamo i fatti salienti.
1. Sia P un $p-$sottogruppo di Sylow di G, che sappiamo esistere in virtù del primo Teorema di Sylow. Per i Teoremi di Sylow, ogni $p-$Sylow è un coniugato di P (e viceversa), ne consegue che il numero dei $p-$Sylow, n_p, coincide con il numero dei coniugati di P in G, ovvero

$$n_p = [G : N_G(P)].$$

Dalla formula del prodotto degli indici si ha che tale numero divide $[G : P] = m$.
2. È parte del secondo Teorema di Sylow.
3. G agisce per coniugio (in modo transitivo non banale) sull'inseme dei $p-$sottogruppi di Sylow di G.

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Sym}(\mathrm{Syl}_p(G)) \simeq S_{n_p} \\ g &\longmapsto (P_i \longmapsto (P_i)^g). \end{aligned}$$

Assumendo G semplice si ha che $\ker(\varphi) = \{1_G\}$, e quindi G è isomorfo ad un sottogruppo di S_{n_p}. Per Lagrange, $|G|$ divide $\left|S_{n_p}\right| = (n_p)!$. $\square$

Esercizio 3. *Sia G un gruppo d'ordine 224. Allora G non è semplice.*

Svolgimento. Sia G d'ordine $224 = 32 \cdot 7 = 2^5 \cdot 7$ e assumiamo per assurdo che G sia un gruppo semplice. Detto n_2 il numero dei $2-$sottogruppi di Sylow di G si ha che $n_2 \equiv 1 \pmod 2$ e n_2 divide 7. Pertanto ci sono solo due casi possibili: $n_2 = 1$ o $n_2 = 7$. Nel primo caso si avrebbe un unico $2-$sottogruppo di Sylow che pertanto sarebbe un sottogruppo (proprio non-banale) normale di G, il che contraddirebbe la nostra ipotesi d'assurdo. Quindi assumiamo che $n_2 = 7$. Allora per la Proposizione precedente (punto 3), $|G| = 2^5 \cdot 7$ dovrebbe dividere 7!, ma anche ciò è assurdo poiché 2^5 non divide 7!. Se ne conclude che G non è un gruppo semplice.

Esercitazione n. 18

24/11/2016

Argomenti. Esercizi sui Teoremi di Sylow.

Esercizio 1. *Ogni gruppo d'ordine* 15 *è ciclico. (Ovvero, a meno di isomorfismi, esiste un unico gruppo d'ordine* 15*.)*

Svolgimento. In tal caso l'unica possibilità per n_3 e per n_5 è $n_3 = n_5 = 1$. Dunque G ammette un unico $3-$Sylow T e un unico $5-$Sylow Q. Per ragioni d'ordine si ha $G = T \times Q$, che è ciclico in quanto prodotto diretto di due gruppi ciclici d'ordine coprimo.

Esercizio 2. *Sia G un gruppo d'ordine* 45*. Allora G è abeliano.*

Svolgimento. Osserviamo che $|G| = 3^2 \cdot 5$. sia n_3 il numero dei $3-$sottogruppi di Sylow di G. Allora n_3 è congruo ad 1 modulo 3 e n_3 divide 5. Se ne deduce che l'unica possibilità per n_3 è $n_3 = 1$. Quindi esiste un unico $3-$Sylow che chiamiamo T. Sia n_5 il numero dei $5-$Sylow. Si ha che $n_5 \equiv 1 \pmod 5$ e $n_5|9$, ne consegue che $n_5 = 1$, ovvero esiste un unico $5-$Sylow, Q. Entrambi T e Q sono normali in G, quindi QT è un sottogruppo di G. Ma

$$|QT| = \frac{|Q|\,|T|}{|Q \cap T|} = |Q|\,|T| = 5 \cdot 9 = |G|\,,$$

da cui segue che

$$G = QT \simeq Q \times T.$$

Ora Q ha ordine 5, primo, quindi Q è ciclico, in particolare abeliano. T ha ordine 3^2, poiché ogni gruppo d'ordine il quadrato d'un primo è abeliano[1], si ha che T è abeliano. Allora G essendo il prodotto diretto di due gruppi abeliani è abeliano.

Esercizio 3. *Un gruppo d'ordine* 6 *è ciclico oppure isomorfo ad S_3.*

Svolgimento. Il numero n_3 dei $3-$Sylow di G deve dividere 2 ed essere congruo ad 1 modulo 3, pertanto $n_3 = 1$, cioè G ammette un unico $3-$Sylow, T,

[1] Si provi per esercizio che se G è un gruppo d'ordine p^2, o $G \simeq C_{p^2}$, o $G \simeq C_p \times C_p$.

che pertanto è normale in G. Il numero n_2 dei $2-$Sylow dovendo dividere 3 ed essere congruo ad 1 modulo 2, è o 1 o 3. Entrambi i casi sono ammissibili. Nel primo caso G ammette un unico $2-$Sylow P che è quindi normale. Si ha che

$$G = P \times T$$

e poiché è prodotto diretto di gruppi ciclici *d'ordine coprimo*, G è ciclico d'ordine $2 \cdot 3 = 6$. Nel secondo caso G ha tre $2-$Sylow. Sia P uno di questi e consideriamo l'azione di moltiplicazione a sinistra sulle classi laterali di P in G,

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Sym}(\mathrm{Lat}(G, P)) \simeq S_3 \\ g &\longmapsto (xP \longmapsto gxP), \end{aligned}$$

Il nucleo di tale azione sappiamo essere il nocciolo di P in G, ovvero

$$\ker(\varphi) = P_G = \bigcap_{x \in G} P^x = \{1_G\},$$

poiché è un sottogruppo normale contenuto in $P \simeq C_2$ e P non è normale in G. Quindi $G \simeq \varphi(G) \leq S_3$, ed avendo lo stesso ordine di S_3 segue $G \simeq S_3$.

Esercizio 4. *Siano p e q due numeri primi e sia G un gruppo d'ordine pq. Allora G non è semplice. Se $p < q$ e $p \not| q-1$, si provi che G è commutativo, anzi ciclico.*

Svolgimento. Se $p = q$ allora G ha ordine p^2 ed è un gruppo abeliano, poiché G contiente sottogruppi d'ordine p, questi sono normali e G non può essere semplice.
Sia $p \neq q$, e supponiamo che $p < q$ (altrimenti scambiamo p con q) . Sia n_q il numero dei q-sottogruppi di Sylow di G. Allora $n_q \equiv 1 \pmod q$ e $n_q | p$. Essendo p primo si ha che o $n_q = 1$ oppure $n_q = p$. Nel secondo caso si avrebbe $p \equiv 1 \pmod q$, ovvero per qualche $n \in \mathbb{N}_{\geq 1}$, $p = 1 + qn$, il che contraddice il fatto che $p < q$. Risulta pertanto $n_q = 1$, ovvero G possiede un unico $q-$Sylow che chiamiamo Q. Essendo i $q$sottogruppi di Sylow tutti coniugati, si ha che Q è normale in G, e G non è semplice.
Assumiamo che p non divida $q-1$ e sia n_q il numero dei $p-$Sylow di G. Ora n_p divide q e $n_p \equiv 1 \pmod p$. Se fosse $n_p = q$ si avrebbe $q \equiv 1 \pmod p$, da cui $p | q-1$, il che è assurdo. Pertanto anche $n_p = 1$. G possiede allora un unico $q-$Sylow Q e un unico $p-$Sylow, P. Entrambi sono normali in G, poiché hanno ordini coprimi $P \cap Q = \{1\}$, inoltre, per ragioni d'ordine vale

$$G = PQ = P \times Q.$$

Ora P e Q hanno ordini primi, pertanto sono gruppi ciclici. Posto $P = \langle x \rangle$ e $Q = \langle y \rangle$, si ha che l'elemento xy ha ordine pq, dunque genera G.

Esercizio 5. *Siano p e q due primi distinti e sia G un gruppo d'ordine pq^2. Allora G non è semplice. Se inoltre p divide $|Z(G)|$, allora G è abeliano.*

Dimostrazione. Per assurdo sia G un gruppo semplice di tale ordine.
Se $q > p$, allora $n_q | p$ e $n_q \equiv 1 \pmod q$ implicano $n_q = 1$, dunque G ammette un unico $q-$Sylow che è normale. Assurdo
Sia $p > q$, allora, non potendo essere $n_p = 1$ né $n_p = q$, n_p è uguale a q^2. Dunque $q^2 \equiv 1 \pmod p$, cioè $p | q^2 - 1 = (q-1)(q+1)$. Ma allora, poiché p non può dividere $q - 1$ (essendo $q < p$), segue $p | q + 1$, ovvero $q + 1 = pm$ per qualche m. Ora essendo $p > q$ necessariamente di deve avere $m = 1$, cioè $p = 3$ e $q = 2$ (poiché sono entrambi dei numeri primi). G ha pertanto ordine 12 e $n_3 = 4$, $n_2 = 3$. Preso allora un $2-$Sylow P e considerata l'azione di G sui laterali sinistri di P

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Sym}(\mathrm{Lat}(G, P)) \simeq S_3 \\ g &\longmapsto (xP \longmapsto gxP), \end{aligned}$$

la semplicità di G impone $\ker(\varphi) = \{1_G\}$, ovvero G si immerge in S_3, ma ciò è assurdo poiché G ha ordine 12, mentre $|S_3| = 6$.
Assumiamo ora che p divida l'ordine del centro di G. Preso P un $p-$Sylow di $Z(G)$, $|P| = p$, quindi $P \in \mathrm{Syl}_p(G)$, ed essendo un sottogruppo del centro, $P \trianglelefteq G$. Se allora Q è un qualunque $q-$Sylow di G, si ha che $PQ \leq G$ tale che

$$|PQ| = \frac{|P|\,|Q|}{|P \cap Q|} = \frac{p \cdot q^2}{1} = |G|\,,$$

ovvero $G = PQ$. Ora se g è un arbitrario elemento di G, scritto g come $g = xy$, con $x \in P \leq Z(G)$ e $y \in Q$, si ha

$$Q^g = Q^{xy} = Q^y = Q,$$

dunque anche $Q \trianglelefteq G$ e pertanto G è il prodotto diretto (interno) $G = P \times Q$. Infine P è abeliano perché ha ordine p (primo), Q è abeliano perché ha ordine q^2 (quadrato di un primo), e pertanto G è abeliano perché prodotto diretto di due gruppi abeliani. $\square$

Esercitazione n. 19.

28/11/2016

Argomenti. Esercizi sui Teoremi di Sylow.

Esercizio 1. *Siano p e q due primi distinti e sia G un gruppo d'ordine pq^2. Allora G non è semplice. Se inoltre p divide $|Z(G)|$, allora G è abeliano.*

Dimostrazione. Per assurdo sia G un gruppo semplice di tale ordine.
Se $q > p$, allora $n_q | p$ e $n_q \equiv 1 \pmod q$ implicano $n_q = 1$, dunque G ammette un unico $q-$Sylow che è normale. Assurdo
Sia $p > q$, allora, non potendo essere $n_p = 1$ né $n_p = q$, n_p è uguale a q^2. Dunque $q^2 \equiv 1 \pmod p$, cioè $p | q^2 - 1 = (q-1)(q+1)$. Ma allora, poiché p non può dividere $q - 1$ (essendo $q < p$), segue $p | q + 1$, ovvero $q + 1 = pm$ per qualche m. Ora essendo $p > q$ necessariamente di deve avere $m = 1$, cioè $p = 3$ e $q = 2$ (poiché sono entrambi dei numeri primi). G ha pertanto ordine 12 e $n_3 = 4$, $n_2 = 3$. Preso allora un $2-$Sylow P e considerata l'azione di G sui laterali sinistri di P

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Sym}(\mathrm{Lat}(G, P)) \simeq S_3 \\ g &\longmapsto (xP \longmapsto gxP), \end{aligned}$$

la semplicità di G impone $\ker(\varphi) = \{1_G\}$, ovvero G si immerge in S_3, ma ciò è assurdo poiché G ha ordine 12, mentre $|S_3| = 6$.
Assumiamo ora che p divida l'ordine del centro di G. Preso P un $p-$Sylow di $Z(G)$, $|P| = p$, quindi $P \in \mathrm{Syl}_p(G)$, ed essendo un sottogruppo del centro, $P \trianglelefteq G$. Se allora Q è un qualunque $q-$Sylow di G, si ha che $PQ \leq G$ tale che

$$|PQ| = \frac{|P|\,|Q|}{|P \cap Q|} = \frac{p \cdot q^2}{1} = |G|\,,$$

ovvero $G = PQ$. Ora se g è un arbitrario elemento di G, scritto g come $g = xy$, con $x \in P \leq Z(G)$ e $y \in Q$, si ha

$$Q^g = Q^{xy} = Q^y = Q,$$

dunque anche $Q \trianglelefteq G$ e pertanto G è il prodotto diretto (interno) $G = P \times Q$. Infine P è abeliano perché ha ordine p (primo), Q è abeliano perché ha ordine q^2 (quadrato di un primo), e pertanto G è abeliano perché prodotto diretto di due gruppi abeliani. $\square$

Esercizio 2. *Siano p, q ed r tre numeri primi distinti (wlog.*[1] *$p > q > r$). Sia G un gruppo finito d'ordine $p \cdot q \cdot r$. Allora G non è un gruppo semplice*

Dimostrazione. Assumiamo per assurdo che G sia un gruppo semplice di tale ordine. Allora il numero n_p dei $p-$Sylow di G deve essere necessariamente qr. Poiché ogni $p-$Sylow di G contiene p elementi e due distinti $p-$Sylow si intersecano nell'unità di G, esistono in G esattamente $qr(p-1)$ elementi d'ordine p. Ora il numero dei $q-$Sylow di G può essere solamente p o pr. Nel secondo caso però G avrebbe $pr(q-1)$ elementi d'ordine q, che sommati agli elementi d'ordine p, dà un totale di

$$qr(p-1) + pr(q-1) = 2pqr - qr - pr$$

elementi d'ordine p o q. Quseti sono troppi poichè

$$2pqr - qr - pr > pqr = |G|,$$

per ogni scelta di tre primi distinti. Ne risulta che $n_q = p$, ovvero il normalizzante in G di un $q-$Sylow Q ha ordine qr, i.e. $|N_G(Q)| = qr$. Ora calcoliamo la cardinalità dell'insieme $\Omega := G \setminus \{\text{elementi d'ordine } p\}$.

$$|\Omega| = pqr - qr(p-1) = pr = |N_G(Q)|.$$

Risulta quindi che $N_G(Q)$ è l'unico sottogruppo d'ordine qr. Infatti ogni siffatto sottogruppo, per il Teorema di Sylow (Lemma di Cauchy) non può contenere elementi d'ordine p e dunque è contenuto in Ω, ma allora coincide con esso. Quindi $N_G(Q) \trianglelefteq G$, e ciò è assurdo. □

Esercizio 3. *Sia G un gruppo finito ed S un $p-$sottogruppo di Sylow di G. Sia inoltre N un sottogruppo normale di G. Allora $S \cap N$ è un $p-$sottogruppo di Sylow di N. In particolare se N è un $p-$sottogruppo normale di G, allora N è contenuto in ogni $p-$Sylow.*

Dimostrazione. È ovvio che $S \cap N$ è un $p-$sottogruppo di N, pertanto per il terzo Teorema di Sylow è contenuto in almeno un $p-$Sylow di N. Assumiamo che $S \cap N \lneq T \in \mathrm{Syl}_(N)$. Allora in particolare T è un $p-$sottogruppo di G, quindi per il terzo e secondo Teorema di Sylow, esiste un $g \in G$ tale per cui $T \leq S^g$. Ma allora

$$S \cap N \lneq T \leq S^g \cap N = (S \cap N)^g,$$

(essendo $N \trianglelefteq G$) e ciò è assurdo. □

Lemma 1 (Argomento di Frattini)**.** *Sia G un gruppo finito e sia N un sottogruppo normale di G. Se $P \in Syl_p(N)$ è un $p-$sottogruppo di Sylow di N (per qualche primo p), allora $G = N_G(P) \cdot N$.*

[1] Wlog=without loss of generality=senza perdere in generalità possiamo supporre che...

Dimostrazione. Preso un arbitrario elemento $g \in G$ il sottogruppo $P^g = g^{-1}Pg$ sta in N, essendo quest'ultimo normale in G. Inoltre $|P^g| = |P|$, quindi sia P che P^g sono due $p-$Sylow di N. Per il (secondo) Teorema di Sylow, questi sono pertanto coniugati *in* N, ovvero esiste $n \in N$ tale per cui

$$P^g = P^n.$$

Ne segue che $P^{gn^{-1}} = P$, ovvero l'elemento gn^{-1} normalizza P, i.e. $gn^{-1} \in N_G(P)$ e $g \in N_G(P)n \subseteq N_G(P) \cdot N$. Data la genericità con cui si è scelto $g \in G$, abbiamo provato che $G = N_G(P) \cdot N$, cioè la tesi. $\square$

Esercitazione n. 20

12/12/2016

Argomenti. Esercizi sulle estensioni di campi.

Esercizio 1. *Si costruisca un campo d'ordine 8 ed uno d'ordine 25. Si esibiscano inoltre dei generatori dei rispettivi gruppi moltiplicativi.*

Svolgimento.
Campo d'ordine 8. Ogni campo d'ordine 8 è isomorfo ad un quoziente dell'anello $\mathbb{Z}_2[X]$ rispetto l'ideale principale genrato da un polinomio irriducibile di grado 3 (vedi Algebra 1). Cerchiamo pertanto un polinomio $g(X) \in \mathbb{Z}_2[X]$ irriducibile di grado 3. Basta prendere un polinomio di grado 3 che non ammette radici in $\mathbb{Z}_2$. Ad esempio

$$g(X) = X^3 + X + \overline{1},$$

infatti $g(\overline{0}) = g(\overline{1}) = \overline{1}$. Detto $I := \langle g(X) \rangle$, si ha che

$$\frac{\mathbb{Z}_2[X]}{I} = \left\{ \overline{a_2}X^2 + \overline{a_1}X + \overline{a_0} + I | \overline{a_2}, \overline{a_1}, \overline{a_0} \in \mathbb{Z}_2 \right\}.$$

Quindi $\left| \frac{\mathbb{Z}_2[X]}{I} \right| = 2^3 = 8$ ed è un ("il", a meno d'isomorfismo) campo richiesto. Determiniamo ora un generatore del gruppo moltiplicativo $\frac{\mathbb{Z}_2[X]}{I}^*$. Sia $\epsilon := X + I$, allora vale

$$\begin{aligned}
\epsilon^2 &= X^2 + I, \\
\epsilon^3 &= X^3 + I = X + 1 + I = \epsilon + 1, \\
\epsilon^4 &= X^4 + I = X^2 + X + I = \epsilon^2 + \epsilon, \\
\epsilon^5 &= X^2 + X + 1 + I = \epsilon^2 + \epsilon + 1, \\
\epsilon^6 &= X^3 + X + 1 + I = \epsilon^2 + 1, \\
\epsilon^7 &= \epsilon^3 + \epsilon = 1.
\end{aligned}$$

Campo d'ordine 25. Dobbiamo cercare in $\mathbb{Z}_5[X]$ un polinomio irriducibile di grado 2, ovvero un polinomio di grado due che non ammette radici in $\mathbb{Z}_5$. Vediamo quali sono i quadrati degli elementi di $\mathbb{Z}_5$:

$$\overline{0}^2 = \overline{0}, \quad \overline{1}^2 = \overline{1}, \quad \overline{2}^2 = \overline{4}, \quad \overline{3}^2 = \overline{4}, \quad \overline{4}^2 = \overline{1}$$

Un polinomio che fa al nostro caso è quindi

$$f(X) = X^2 + \overline{2} \in \mathbb{Z}_5[X].$$

Sia $I := \langle f(X) \rangle$ si ha

$$\frac{\mathbb{Z}_5[X]}{I} = \{\overline{a_1}X + \overline{a_0} + I | \overline{a_1}, \overline{a_0} \in \mathbb{Z}_5\}.$$

Quindi $\left|\frac{\mathbb{Z}_5[X]}{I}\right| = 5^2 = 25$ ed è un ("il", a meno d'isomorfismo) campo richiesto. Un generatore del gruppo moltiplicativo è ad esempio

$$\alpha = X + \overline{1} + I.$$

Lo si verifichi. Sia $E|F$ un'estensione di campi e sia $\alpha \in E$ un elemento algebrico su F. Allora il polinomio minimo di α è in particolare un polinomio irriducibile su F (che genera l'ideale $I_\alpha := \{f \in F[X] | f(\alpha) = 0\}$). Nel caso di estensioni *di anelli* (e non necessariamente di campi) non è detto che polinomi minimi siano ancora irriducibili. Vediamo un esempio di tale situazione.

Esercizio 2. *Sia $R := M_2(\mathbb{R})$ l'anello delle matrici 2×2 sui reali e sia α la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in R$. Allora il polinomio minimo di α su $\mathbb{R}$ è $f(X) = X^2$ (dunque un polinomio non irriducibile).*

Dimostrazione. Consideriamo l'estensione di anelli $R|\mathbb{R}$, dove il campo reale è identificato con le matrici scalari $\left\{\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} | r \in R\right\}$. È evidente che $\alpha \neq 0$ e che $\alpha^2 = 0$. Quindi la tesi. □

Esercizio 3. *Sia $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{C}$.*

1. *Trovare i polinomi minimi di α su $\mathbb{R}$ e su $\mathbb{Q}$.*
2. *Mostrare che ogni radice di $f := minpol_{\mathbb{Q}}(\alpha)$ appartiene al campo $\mathbb{Q}[\alpha]$.*

Dimostrazione. Poiché $\alpha \in \mathbb{R}$ si ha che $\text{minpol}_{\mathbb{R}}(\alpha)(X) = X - \alpha$. Determiniamo ora $\text{minpol}_{\mathbb{Q}}(\alpha)$. Abbiamo che

$$\alpha^2 = 2 + \sqrt{2},$$

dunque

$$\alpha^2 - 2 = \sqrt{2},$$

da cui elevando al quadrato si ottiene

$$\alpha^4 - 4\alpha^2 + 4 = 2.$$

Ovvero α è radice del polinomio monico

$$f(X) := X^4 - 4X^2 + 2.$$

Proviamo che questo è un polinomio irriducibile in $\mathbb{Q}[X]$, mostrando così che è il polinomio minimo di α su $\mathbb{Q}$. Le radici complesse di f sono:

$$\alpha,\ -\alpha,\ \beta := \sqrt{2-\sqrt{2}} \ \text{ e } \ -\beta.$$

Questi sono tutti numeri reali <u>non</u> in $\mathbb{Q}$. In $\mathbb{R}[X]$ f si fattorizza come

$$f(X) = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta).$$

L'unica eventuale fattorizzazione propria di $f(X)$ in $\mathbb{Q}[X]$ dovrà pertanto essere del tipo: prodotto di due fattori di grado due. Ma poiché $\alpha^2 = 2+\sqrt{2} \notin \mathbb{Q}$ e $\alpha\beta = \sqrt{4-2} = \sqrt{2} \notin \mathbb{Q}$ si ha che una tale fattorizzazione non può esistere in $\mathbb{Q}[X]$. f è pertanto il polinomio minimo di α su $\mathbb{Q}$.
È evidente che la radice $-\alpha \in \mathbb{Q}[\alpha]$. Invece facendo

$$\alpha \cdot \beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{4-2} = \sqrt{2} = \alpha^2 - 2$$

si ha che

$$\beta = \frac{\alpha^2-2}{\alpha} \in \mathbb{Q}[\alpha].$$

Similmente per $-\beta$. Dunque $\mathbb{Q}[\alpha] = \mathbb{Q}[\alpha, -\alpha, \beta, -\beta]$. $\square$

Esercitazione n. 21

12/12/2016

Argomenti. Lemma di Gauss e criterio di Eisenstein. Aplicazioni. Vengono enunciati e dimostrati i Lemmi 9.12, 9.13, 9.14 e le Proposizioni 9.15, 9.18, oltre al criterio di Eisensten, delle dispense di ALGEBRA 1.

Definizione 1. *Sia* $f = a_n X^n + \ldots + \ldots a_1 X + a_0$ *un polinomio non nullo in* $\mathbb{Z}[X]$. f *si dice* primitivo *se* $MCD(a_0, a_1, \ldots, a_n) = 1$.

Lemma 1 (Lemma 9.12)**.** *Per ogni* $0 \neq f \in \mathbb{Z}[X]$ *esiste un* $d \in \mathbb{Z}$ *e un polinomio primitivo* $f_0 \in \mathbb{Z}[X]$ *tale che* $f = df_0$*, tale fattorizzazione è unica a meno del segno.*

Lemma 2 (Lemma 9.13)**.** *Per ogni* $0 \neq f \in \mathbb{Q}[X]$ *esiste un* $\gamma \in \mathbb{Q}$ *e un polinomio primitivo* $f_0 \in \mathbb{Z}[X]$ *tale che* $f = \gamma f_0$*, tale fattorizzazione è unica a meno del segno.*

Lemma 3 (Lemma 9.14)**.** *Il prodotto di polinomi interi primitivi è pimitivo.*

Proposizione 1 (Proposizione 9.15)**.** *Sia* $0 \neq f \in \mathbb{Q}[X]$ *e sia* $f = \gamma f_0$ *con* $\gamma \in \mathbb{Q}$ *e* $f_0 \in \mathbb{Z}[X]$ *primitivo. Allora* f *è irriducibile in* $\mathbb{Q}[X]$ *se e solo se* f_0 *è irriducibile in* $\mathbb{Z}[X]$.

Teorema 1 (Criterio di Eisenstein)**.** *Sia* $0 \neq f \in \mathbb{Z}[X]$ *il polinomio*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0.$$

Assumiamo che esista un primo $p \in \mathbb{Z}$ *per cui accadono i seguenti tre fatti*

1. $p \not| a_n$.
2. $p | a_i$ *per ogni* $i = 0, 1, \ldots, n-1$.
3. $p^2 \not| a_0$.

Allora $f(X)$ *è irriducibile in* $\mathbb{Q}[X]$.

Proposizione 2 (Proposizione 9.18)**.** *Sia* p *un numero primo. Allora il polinomio*

$$X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1$$

è irriducibile in $\mathbb{Q}[X]$.

Esercitazione n. 22

12/12/2016

Argomenti. Calcolo di polinomi minimi e campi di spezzamento.

Esercizio 1. *Siano a e b due numeri complessi entrambi algebrici su $\mathbb{Q}$ e tali che $|\mathbb{Q}[a] : \mathbb{Q}| = n$ e $|\mathbb{Q}[b] : \mathbb{Q}] | m$ con $M.C.D.(n, m) = 1$. Si provi che*

$$\mathbb{Q}[a] \cap \mathbb{Q}[b] = \mathbb{Q} \quad e \quad |\mathbb{Q}[a, b] : \mathbb{Q}| = n \cdot m.$$

Dimostrazione. Sia $\mathbb{L} := \mathbb{Q}[a] \cap \mathbb{Q}[b]$. Allora $\mathbb{L}$ è un campo (poiché intersezione di campi) che contiene $\mathbb{Q}$. Inoltre poiché $\mathbb{Q}[a] \supseteq \mathbb{L} \supseteq \mathbb{Q}$, dalla formula dei gradi si ha che $n = |\mathbb{Q}[a] : \mathbb{Q}|$ è divisibile per $|\mathbb{L} : \mathbb{Q}|$. Similmente $m = |\mathbb{Q}[b] : \mathbb{Q}|$ è divisibile per $|\mathbb{L} : \mathbb{Q}|$. Essendo $M.C.D.(m, n) = 1$ si ha necessariamente $|\mathbb{L} : \mathbb{Q}| = 1$, ovvero $\mathbb{L} = \mathbb{Q}$.
Ora sia $\mathbb{E} := \mathbb{Q}[a, b]$. Allora applicando la formula dei gradi si ha

$$\begin{aligned} |\mathbb{E} : \mathbb{Q}| &= |\mathbb{Q}[a, b] : \mathbb{Q}[a]| \cdot |\mathbb{Q}[a] : \mathbb{Q}| = |\mathbb{Q}[a, b] : \mathbb{Q}[a]|\, n \\ &= |\mathbb{Q}[a, b] : \mathbb{Q}[b]| \cdot |\mathbb{Q}[b] : \mathbb{Q}| = |\mathbb{Q}[a, b] : \mathbb{Q}[b]|\, m \end{aligned}$$

Dunque sia n che m dividono il grado di $\mathbb{E}$ su $\mathbb{Q}$ e poiché si tratta di due numeri coprimi abbiamo

$$nm \big| \, |\mathbb{E} : \mathbb{Q}| \, .$$

Ora $|\mathbb{E} : \mathbb{Q}[a]| = |\mathbb{Q}[a][b] : \mathbb{Q}[a]| = \deg(\min)_{\mathbb{Q}[a]}(b)$ e detto $g = \min_{\mathbb{Q}[a]}(b)$ ed $f = \min_{\mathbb{Q}}(b)$ abbiamo che $f \in \mathbb{Q}[X] \subseteq \big(\mathbb{Q}[a]\big)[X]$, dunque per definizione di polinomio minimo g divide f in $\big(\mathbb{Q}[a]\big)[X]$, in particolare $\deg(g) \leq \deg(f) = n$. Dalla formula dei gradi si ha allora che $|\mathbb{E} : \mathbb{Q}| \leq nm$, e pertanto $|\mathbb{E} : \mathbb{Q}| = nm$.
□

Esercizio 2. *Sia p un numero primo e sia $f(X) = X^p - 2 \in \mathbb{Q}[X]$. Sia $\mathbb{E}$ il campo di spezzamento di f su $\mathbb{Q}$ (in $\mathbb{C}$). Provare che*

1. *$\mathbb{E} = \mathbb{Q}[\alpha, \epsilon]$, dove $\alpha = \sqrt[p]{2}$, $\epsilon = e^{\frac{2\pi i}{p}} = \cos(\frac{2\pi}{p}) + i \sin(\frac{2\pi}{p})$.*
2. *$min_{\mathbb{Q}}(\epsilon)(X) = X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1$.*
3. *$[\mathbb{E} : \mathbb{Q}] = p(p - 1)$.*

Dimostrazione. 1. Per determinare $\mathbb{E}$ occorre calcolare le radici complesse del polinomio f. Queste scritte in forma esponenziale sono esattamente

$$X_k := \sqrt[p]{2}e^{\frac{2\pi i k}{p}}, \quad \text{al variare di } k = 0, 1, \ldots, p-1,$$

ovvero, secondo le notazioni dell'enunciato,

$$X_k := \alpha\epsilon^k, \quad \text{al variare di } k = 0, 1, \ldots, p-1. \tag{1}$$

Per definizione di campo di spezzamento abbiamo che

$$\mathbb{E} = \mathbb{Q}[X_0, X_1, \ldots X_{p-1}],$$

quindi, in virtù di (1), appare evidente che $\mathbb{E} \subseteq \mathbb{Q}[\alpha, \epsilon]$. D'altra parte $\alpha = X_0$ e $\epsilon = X_1/X_0$, dunque $\mathbb{Q}[\alpha, \epsilon] \subseteq \mathbb{E}$.
2. Il polinomio minimo di ϵ su $\mathbb{Q}$ è un polinomio a coefficienti in $\mathbb{Q}$, monico, irriducibile e tale che ammette ϵ come radice. Ora

$$\epsilon^p = (e^{\frac{2\pi i}{p}})^p = 1,$$

dunque ϵ è radice si $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1)$, inoltre $\epsilon \neq 1$, quindi è radice del polinomio ciclotomico

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1,$$

che sappiamo essere irriducibile (vd. lezione precedente), e pertanto esso è il polinomio minimo di ϵ.
3. Osserviamo innanzitutto il polinomio $f(X)$ è irriducibile in $\mathbb{Q}[X]$ per il criterio di Eisenstein al primo 2. Pertanto, essendo monico, esso è il polinomio minimo di α in $\mathbb{Q}$ e quindi $|Q[\alpha] : \mathbb{Q}| = p$. Ora $|\mathbb{Q}[\epsilon] : \mathbb{Q}| = \deg(\Phi_p(X)) = p - 1$, pertanto siamoesattamente nella situazione dell'esercizio 1 e possiamo concludere che

$$|\mathbb{E} : \mathbb{Q}| = p(p-1).$$

$\square$

Esercitazione n. 23

15/12/2016

Argomenti. Calcolo di polinomi minimi e campi di spezzamento.

Esercizio 1. *Sia* $\alpha = \sqrt{3} + \sqrt[3]{2} \in \mathbb{C}$.

1. *Provare che* $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$.
2. *Trovare il polinomio minimo di* α *in* $\mathbb{Q}$.

Dimostrazione. 1. Ovviamente $\alpha \in \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$ e quindi $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$. Viceversa osserviamo che

$$\alpha - \sqrt{3} = \sqrt[3]{2},$$

da cui elevando al cubo si ha

$$\alpha^3 - 3\alpha^2\sqrt{3} + 9\alpha - 3\sqrt{3} = 2,$$

ovvero

$$\alpha^3 + 9\alpha - 2 = 3(\alpha^2 + 1)\sqrt{3},$$

cioè

$$\sqrt{3} = \frac{\alpha^3 + 9\alpha - 2}{3(\alpha^2 + 1)} \in \mathbb{Q}[\alpha]. \tag{1}$$

Una volta garantito che $\sqrt{3} \in \mathbb{Q}[\alpha]$ da $\sqrt[3]{2} = \alpha - \sqrt{3}$ abbiamo che anche $\sqrt[3]{2} \in \mathbb{Q}[\alpha]$, e dunque $\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] \subseteq \mathbb{Q}[\alpha]$.
2. Elevando al quadrato la (1) si ottiene che α è radice del polinomio

$$h(X) = X^6 - 9X^4 - 4X^3 + 27X^2 - 36X - 23.$$

L'irriducibilità di tale polinomio è garantita dal fatto che il polinomio minimo di α su $\mathbb{Q}$ deve avere grado uguale a

$$|\mathbb{Q}[\alpha] : \mathbb{Q}| = \left|\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] : \mathbb{Q}\right| = 2 \cdot 3 = 6,$$

in virtù dell'esercizio della lezione precedente, dunque $\min_{\mathbb{Q}}(\alpha)(X) = h(X)$. $\square$

Esercizio 2. *Siano* p_1 *e* p_2 *due numeri primi distinti. Sia* $\mathbb{E}$ *l'estensione* $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}]$.

1. *Si calcoli il grado di* $\mathbb{E}$ *su* $\mathbb{Q}$.

2. *Si individuino tre campi intermedi, strettamente compresi tra* $\mathbb{Q}$ *ed* $\mathbb{E}$ *e si esibisca una base per* $\mathbb{E}$ *come spazio vettoriale su* $\mathbb{Q}$.

3. *Si mostri che* $\mathbb{E}$ *è un'estensione semplice (Suggerimento: provare che* $\mathbb{E} = \mathbb{Q}[\sqrt{p_1} + \sqrt{p_2}]$*).*

4. *Si esibisca il polinomio minimo di* $\sqrt{p_1} + \sqrt{p_2}$ *su* $\mathbb{Q}$.

5. *Si dica se* $\mathbb{E}|\mathbb{Q}$ *è un'estensione di Galois.*

6. *Si determini l'ordine ed i ltipo di isomorfismo del gruppo di Galois* $Gal(\mathbb{E}, \mathbb{Q})$.

Dimostrazione. 1. Per il criterio di Eisenstein i polinomi $X^2 - p_1$ e $X^2 - p_2$ sono irriducibili in $\mathbb{Q}$, pertanto essi sono i polinomi minimi rispettivamente di $\sqrt{p_1}$ e $\sqrt{p_2}$. In particolare si ha che $\left|\mathbb{Q}[\sqrt{p_1}] : \mathbb{Q}\right| = \left|\mathbb{Q}[\sqrt{p_2}] : \mathbb{Q}\right| = 2$. Ora dalla formula dei gradi si ha che

$$\begin{aligned} |\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}| &= |\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}[\sqrt{p_1}]|\, |\mathbb{Q}[\sqrt{p_1}] : \mathbb{Q}| = \\ &= |\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}[\sqrt{p_1}]| \cdot 2. \end{aligned}$$

Inoltre $\left|\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}[\sqrt{p_1}]\right|$ coincide con il grado del polinomio minimo, g, di $\sqrt{p_2}$ sul campo $\mathbb{Q}[\sqrt{p_1}]$; sappiamo che tale polinomio divide ogni polinomio a coefficienti in $\mathbb{Q}[\sqrt{p_1}]$ che ammette $\sqrt{p_2}$ come radice. Pertanto g divide anche $X^2 - p_2$. Ma allora si possono avere solo due casi: o g ha grado due (e quindi in tal caso $g = X^2 - p_2$), oppure g ha grado uno. In quest'ultimo caso si ha che $\left|\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}[\sqrt{p_1}]\right| = 1$, ovvero $\sqrt{p_2} \in \mathbb{Q}[\sqrt{p_1}]$. Ora il campo $\mathbb{Q}[\sqrt{p_1}]$ ha grado due su $\mathbb{Q}$ e una sua base, come spazio vettoriale su $\mathbb{Q}$, è $\left\{1, \sqrt{p_1}\right\}$. Scriviamo pertanto

$$\sqrt{p_2} = a \cdot 1 + b \cdot \sqrt{p_1}, \tag{2}$$

con $a, b \in \mathbb{Q}$. Elevando al quadrato otteniamo

$$2ab\sqrt{p_1} = p_2 - a^2 - p_1 b^2 \in \mathbb{Q},$$

che è assurdo se entrambi a e b sono non nulli. Pertanto o $b = 0$, ma ciò è assurdo perché da (2) si avrebbe $\sqrt{p_2} \in \mathbb{Q}$ che è assurdo, oppure $a = 0$, e (2) diventa

$$\sqrt{p_2} = b\sqrt{p_1}.$$

Scritto $b = \frac{r}{s}$, con $(r, s) = 1$, elevando otteniamo

$$p_2 s^2 = p_1 r^2, \tag{3}$$

Ora p_2 è un primo distinto da p_1, quindi necessariamente p_2 divide r^2, ma allora divide anche r. Scritto $r = tp_2$ (con $t \in \mathbb{Z}$), semplificando in (3) abbiamo che

$$s^2 = p_1 t^2 p_2,$$

e quindi p_2 divide anche s, il che contraddice il fatto che r ed s sono coprimi. Ne segue che $\sqrt{p_2}$ non può scriversi come combinazione lineare (a coefficienti in $\mathbb{Q}$) di 1 e $\sqrt{p_1}$, ovvero $\sqrt{p_2} \notin \mathbb{Q}[\sqrt{p_1}]$. Quindi il grado di $g = \min_{\mathbb{Q}[\sqrt{p_1}]}(\sqrt{p_2})$ è due e $g(X) = X^2 - p_2$. In particolare si ha che

$$|\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}[\sqrt{p_1}]| = 2$$

e

$$|\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] : \mathbb{Q}| = 4.$$

2. I campi $\mathbb{Q}[\sqrt{p_1}]$ e $\mathbb{Q}[\sqrt{p_2}]$ sono ovviamente campi intermedi tra $\mathbb{Q}$ ed $\mathbb{E}$ entrambi di grado due su $\mathbb{Q}$. Abbiamo già visto che sono distinti, poichè $\sqrt{p_2} \notin \mathbb{Q}[\sqrt{p_1}]$. Un terzo campo intermedio è $\mathbb{Q}[\sqrt{p_1 p_2}]$ ($\sqrt{p_1 p_2} = \sqrt{p_1}\sqrt{p_2} \in \mathbb{E}$). Esso ha ovviamente grado due su $\mathbb{Q}$ (infatti $\min_{\mathbb{Q}}(\sqrt{p_1 p_2}) = X^2 - p_1 p_2$) ed è distinto dai due precedenti (se fosse ad esempio $\mathbb{Q}[\sqrt{p_1 p_2}] = \mathbb{Q}[\sqrt{p_2}]$ si avrebbe $\sqrt{p_1} = \frac{\sqrt{p_1 p_2}}{\sqrt{p_2}} \in \mathbb{Q}[\sqrt{p_2}]$, assurdo. Similmente si prova che $\mathbb{Q}[\sqrt{p_1 p_2}] \neq \mathbb{Q}[\sqrt{p_1}]$). Una base per $\mathbb{E}$ su $\mathbb{Q}$ è costituita da $4 = |\mathbb{E} : \mathbb{Q}|$ elementi di $\mathbb{E}$ linearmente indipendenti. Ad esempio una base è data da

$$\{1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1 p_2}\} \tag{4}$$

(si ottiene moltiplicando tra loro rispettivamente un elemento di una base di $\mathbb{Q}[\sqrt{p_1}]$ su $\mathbb{Q}$, i.e. $\{1, \sqrt{p_1}\}$, con uno della base di $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}]$ su $\mathbb{Q}[\sqrt{p_1}]$, i.e. $\{1, \sqrt{p_2}\}$, vedi dimostrazione della formula del prodotto di gradi).

3. Sia $\alpha = \sqrt{p_1} + \sqrt{p_2}$, è ovvio che $\alpha \in \mathbb{E} = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}]$ e perciò $\mathbb{Q}[\alpha] \subseteq \mathbb{E}$. Viceversa proviamo che l'elemento α ha grado 4. Se così non fosse dalla formula dei gradi si avrebbe che α ha grado due su $\mathbb{Q}$ (è evidente che $\alpha \notin \mathbb{Q}$). Posto allora

$$f(X) = X^2 + uX + v$$

il polinomio minimo di α su $\mathbb{Q}$, da $f(\alpha) = 0$ si ottiene

$$p_1 + p_2 + v + u\sqrt{p_1} + u\sqrt{p_2} + 2\sqrt{p_1 p_2} = 0.$$

Ma dal fatto che (4) è una base per $\mathbb{E}$ su $\mathbb{Q}$ segue che tale condizione è impossibile. Pertanto l'elemento α ha grado 4 su $\mathbb{Q}$, cioè $\mathbb{E} = \mathbb{Q}[\sqrt{p_1} + \sqrt{p_2}]$.

4. Occorre e basta trovare un polinomio monico (a coefficienti in $\mathbb{Q}$) di grado 4 di cui α è radice. Elevando α al quadrato si ha

$$\alpha^2 = p_1 + p_2 + 2\sqrt{p_1 p_2}$$

da cui

$$2\sqrt{p_1 p_2} = \alpha^2 - p_1 - p_2$$

che elevato al quadrato fa

$$4p_1 p_2 = \alpha^4 + p_1^2 + p_2^2 - 2p_1\alpha^2 - 2p_2\alpha^2 + 2p_1 p_2.$$

Pertanto il polinomio minimo di $\sqrt{p_1} + \sqrt{p_2}$ su $\mathbb{Q}$ è

$$X^4 - 2(p_1 + p_2)X^2 + p_1^2 + p_2^2 - 2p_1p_2.$$

$\square$

Esercitazione n. 24

19/12/2016

Argomenti. Estensioni di campi e Teoria di Galois.

Esercizio 1. *Si consideri il polinomio a coefficienti interi* $f(X) := X^3 - 11$.

1. *Si determini il campo di spezzamento* $\mathbb{E}$ *di* f *su* $\mathbb{Q}$.
2. *Dire se* $\mathbb{E}|\mathbb{Q}$ *è un'estensione di Galois.*
3. *Dire se* $\mathbb{Q}[\sqrt[3]{11}]|\mathbb{Q}$ *è un'estensione normale.*
4. *Si calcoli l'ordine del gruppo di Galois* $\mathrm{Gal}(\mathbb{E}|\mathbb{Q})$.
5. *Determinare a meno di isomorfismo il gruppo in questione.*

Dimostrazione. 1. Il campo di spezzamento $\mathbb{E}$ di f è per definizione l'estensione di $\mathbb{Q}$ tramite le radici di f. Queste sono

$$x_1 := \sqrt[3]{11},\ x_2 := \sqrt[3]{11} \cdot \epsilon,\ x_3 := \sqrt[3]{11} \cdot \epsilon^2$$

dove ϵ è la radice primitiva terza $\epsilon = e^{2\pi i/3}$. Risulta che

$$\mathbb{E} = \mathbb{Q}[x_1, x_2, x_3] = \mathbb{Q}[\sqrt[3]{11}, \epsilon].$$

2. Poiché $\mathbb{E}$ è campo di spezzamento di un polinomio di $\mathbb{Q}[X]$, per il Teorema sopra richiamato, $\mathbb{E}|\mathbb{Q}$ è un'estensione finita e normale. Poiché la caratteristica di $\mathbb{Q}$ è zero, tale estensione è anche separabile. Dunque $\mathbb{E}|\mathbb{Q}$ è per definizione un'estensione di Galois.

3. Consideriamo ora l'estensione $\mathbb{Q}[\sqrt[3]{11}]|\mathbb{Q}$. Questa è sicuramente algebrica di grado tre. Ora il polinomio minimo dell'elemento $\sqrt[3]{11}$ è $X^3 - 11$. Fra le sue tre radici, $\sqrt[3]{11}$ è l'unica che sta in $\mathbb{Q}[\sqrt[3]{11}]$ (le altre due, $\sqrt[3]{11}\epsilon$ e $\sqrt[3]{11}\epsilon^2$ non sono reali, dunque non stanno in $\mathbb{Q}[\sqrt[3]{11}] \subseteq \mathbb{R}$). Pertanto tale estensione non è normale.
L'estensione $\mathbb{Q}[\epsilon]|\mathbb{Q}$ è invece normale in quanto è il campo di spezzamento del polinomio $X^2 + X + 1$ su $\mathbb{Q}$ (in $\mathbb{C}$).

4. Per il Teorema di sopra, essendo l'estensione di Galois si ha che

$$|\mathrm{Gal}(\mathbb{E}|\mathbb{Q})| = |\mathbb{E} : \mathbb{Q}|\,.$$

Inoltre

$$
\begin{aligned}
|\mathbb{E}:\mathbb{Q}| &= \left|\mathbb{Q}[\sqrt[3]{11},\epsilon]:\mathbb{Q}\right| = \left|\mathbb{Q}[\sqrt[3]{11},\epsilon]:\mathbb{Q}[\epsilon]\right| \cdot |\mathbb{Q}[\epsilon]:\mathbb{Q}| = \left|\mathbb{Q}[\sqrt[3]{11},\epsilon]:\mathbb{Q}[\epsilon]\right| \cdot 2 \\
&= \left|\mathbb{Q}[\sqrt[3]{11},\epsilon]:\mathbb{Q}[\sqrt[3]{11}]\right| \cdot \left|\mathbb{Q}[\sqrt[3]{11}]:\mathbb{Q}\right| = \left|\mathbb{Q}[\sqrt[3]{11},\epsilon]:\mathbb{Q}[\sqrt[3]{11}]\right| \cdot 3 = \\
&= 6,
\end{aligned}
$$

essendo $X^3 - 11$ il polinomio minimo di $\sqrt[3]{11}$ su $\mathbb{Q}$ e $X^2 + X + 1$ quello di ϵ su $\mathbb{Q}$. Dunque $|\mathrm{Gal}(\mathbb{E}|\mathbb{Q})| = 6$.

5. Sia $G := \mathrm{Gal}(\mathbb{E}|\mathbb{Q})$. Gli elementi di G sono automorfismi di $\mathbb{E} = \mathbb{Q}[\sqrt[3]{11},\epsilon]$ che fissano ogni elemento del sottocampo $\mathbb{Q}$. In particolare se α è un elemento di G e x_i una radice di $f = X^3 - 11$, si ha

$$(\alpha(x_i))^3 - 11 = (\alpha(x_i))^3 - \alpha(11) = \alpha((x_i)^3) - \alpha(11) = \alpha((x_i)^3 - 11) = \alpha(0) = 0,$$

ovvero $\alpha(x_i)$ è ancora una radice di f. Detto Ω l'insieme delle radici di f, abbiamo che G agisce su Ω, ovvero esiste un omomorfismo

$$
\begin{aligned}
\phi : G &\longrightarrow Sym(\Omega) \simeq S_3 \\
\alpha &\longmapsto (x_i \longmapsto \alpha(x_i))
\end{aligned}
$$

Sia K il nucleo di tale azione, cioè $K = \ker(\phi)$. Se $\alpha \in K$ allora

$$\alpha(x_1) = x_1,\ \alpha(x_2) = x_2, \quad \alpha(x_3) = x_3,$$

ma allora α è l'identità su tutto $\mathbb{E} = \mathbb{Q}[x_1, x_2, x_3]$. Quindi $K = 1$ e ϕ è un isomorfismo fra G ed il gruppo simmetrico S_3. $\square$

Esercitazione n. 25

21/12/2016

Argomenti. Estensioni di campi e Teoria di Galois.

Esercizio 1. *Sia $f(X)$ il polinomio $X^4 - X^2 + 4 \in \mathbb{Q}[X]$ e sia $\mathbb{E}$ il suo campo di spezzamento su $\mathbb{Q}$ in $\mathbb{C}$.*

1. *Provare che f è irriducibile in $\mathbb{Q}$.*
2. *Determinare $\mathbb{E}$ e il suo grado su $\mathbb{Q}$.*
3. *Mostrare che $\mathbb{E} = \mathbb{Q}[\gamma]$, dove γ è un'arbitraria radice di f.*
4. *Dire se $\mathbb{E}|\mathbb{Q}$ è un'estensione di Galois.*
5. *Determinare l'ordine e il tipo di isomorfismo del gruppo* $\mathrm{Gal}(\mathbb{E}|\mathbb{Q})$.

Svolgimento. 1. Troviamo tutte le radici complesse di $X^4 - X^2 + 4$. Notiamo che

$$X^4 - X^2 + 4 = (X^2 + 2)^2 - 5X^2 = (X^2 + 2 + \sqrt{5}X)(X^2 + 2 - \sqrt{5}X).$$

Risolvendo le equazioni $X^2 + \sqrt{5}X + 2 = 0$ e $X^2 - \sqrt{5}X + 2 = 0$ si trovano le radici di f, che sono pertanto

$$\alpha := (\sqrt{5} + i\sqrt{3})/2,\ \beta := (\sqrt{5} - i\sqrt{3})/2,\ -\alpha,\ -\beta.$$

Nessuna di queste è reale, quindi f non ha radici in $\mathbb{Q}$, ne segue che se f fosse riducibile su $\mathbb{Q}$, allora f necessariamente si spezza come il prodotto di due fattori di grado due ciascuno. Inoltre sappiamo che questi fattori devono avere uno dei seguenti tipi

$$(X - \alpha)(X + \alpha),\ \text{ oppure } (X + \pm\alpha)(X + \pm\beta),\ \text{ oppure } (X - \beta)(X + \beta).$$

Dal fatto che α^2, β^2, $\alpha + \beta$ e $\alpha - \beta$ non stanno in $\mathbb{Q}$, segue che una tale fattorizzazione con polinomi a coefficienti in $\mathbb{Q}$ non esiste. f pertanto è un polinomio irriducibile.

2. Si ha che $\mathbb{E} = \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\sqrt{5}, i\sqrt{3}]$. In particolare per la formula dei gradi abbiamo che

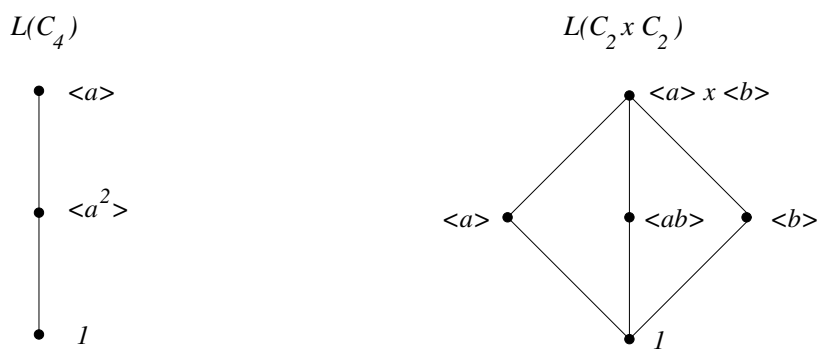
$$|\mathbb{E} : \mathbb{Q}| = \left|\mathbb{E} : \mathbb{Q}[\sqrt{5}]\right| \left|\mathbb{Q}[\sqrt{5}] : \mathbb{Q}\right| = 2 \cdot 2 = 4.$$

(Essendo $\mathbb{Q}[\sqrt{5}] \in \mathbb{R}$, l'elemento $i\sqrt{3} \notin \mathbb{Q}[\sqrt{5}]$, quindi $\min_{\mathbb{Q}[\sqrt{5}]}(i\sqrt{3}) = X^2+3$).

3. Sia γ una radice di f, allora $\mathbb{Q}[\gamma] \subseteq \mathbb{E}$. Inoltre essendo f irriducibile di grado 4 e $f(\gamma) = 0$, $|\mathbb{Q}[\gamma] : \mathbb{Q}| = 4$ e quindi coincide col grado di $\mathbb{E}$ su $\mathbb{Q}$. Ne segue che $\mathbb{Q}[\gamma] = \mathbb{E}$.

4. $\mathbb{E}$ è un'estensione finita e normale di $\mathbb{Q}$ perché campo di spezzamento di un polinomi a coefficienti razionali. Inoltre tale estensione è separabile poiché $\mathbb{Q}$ ha caratteristica zero. Dunque si tratta di un'estensione di Galois.

5. Indichiamo con G il gruppo di Galois $\mathrm{Gal}(\mathbb{E}|\mathbb{Q})$. Poiché $\mathbb{E}|\mathbb{Q}$ è di Galois, $|G| = |\mathbb{E} : \mathbb{Q}| = 4$. A meno di isomorfismo ci sono esattamente due gruppi d'ordine quattro: il ciclico C_4 e il prodotto diretto $C_2 \times C_2$. Ricordiamo che i reticoli dei sottogruppi dei gruppi in questione sono i seguenti



Utilizziamo il Teorema di corrispondenza di Galois per determinare quale dei due gruppi è G. Sappiamo che esiste una corrispondenza biunivoca tra i sottogruppi di G e i campi intermedi tra $\mathbb{Q}$ ed $\mathbb{E}$. Poiché $\mathbb{E} = \mathbb{Q}[\sqrt{5}, i\sqrt{3}]$ i campi $\mathbb{Q}[\sqrt{5}]$ e $\mathbb{Q}[i\sqrt{3}]$ sono distinti, intermedi tra $\mathbb{Q}$ ed $\mathbb{E}$ ed entrambi di grado due su $\mathbb{Q}$. Ne segue che G non è ciclico, dunque $G \simeq C_2 \times C_2$.

Esercizio 2. *Sia α il numero complesso $\alpha := \sqrt{2+\sqrt{2}}$.*

1. *Determinare il polinomio minimo di α ed il suo campo di spezzamento $\mathbb{E}$ su $\mathbb{Q}$.*

2. *Calcolare $|\mathbb{E} : \mathbb{Q}|$.*

3. *Dire se $\mathbb{Q}[\alpha]|\mathbb{Q}$ è un'estensione normale/di Galois.*

4. *Determinare ordine e tipo di isomorfismo del gruppo $\mathrm{Gal}(\mathbb{E}|\mathbb{Q})$.*

Svolgimento. 1. Per l'esercizio XX del giorno XX sappiamo che il polinomio minimo di α su $\mathbb{Q}$ è

$$f(X) := X^4 - 4X^2 + 2$$

e che le sue radici complesse sono

$$\alpha, \ -\alpha, \ \beta := \sqrt{2-\sqrt{2}} \ \text{ e } \ -\beta.$$

Pertanto $\mathbb{E} = \mathbb{Q}[\alpha, \beta]$.

2. Si ha che

$$\begin{aligned} |\mathbb{E} : \mathbb{Q}| &= |\mathbb{Q}[\alpha, \beta] : \mathbb{Q}[\alpha]| \, |\mathbb{Q}[\alpha] : \mathbb{Q}| = \\ &= \deg(\min_{\mathbb{Q}[\alpha]}(\beta)) \cdot \deg(\min_{\mathbb{Q}}(\alpha)) = \\ &= \deg(\min_{\mathbb{Q}[\alpha]}(\beta)) \cdot 4, \end{aligned}$$

essendo $\min_{\mathbb{Q}}(\alpha) = f(X)$. Ora osservo che

$$\alpha \cdot \beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{4-2} = \sqrt{2} = \alpha^2 - 2,$$

pertanto

$$\beta = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}[\alpha],$$

ma allora $\min_{\mathbb{Q}[\alpha]}(\beta) = X - \beta$ e $|\mathbb{Q}[\alpha, \beta] : \mathbb{Q}[\alpha]| = 1$, ovvero $\mathbb{E} = \mathbb{Q}[\alpha]$ ed è un'estensione di grado 4 su $\mathbb{Q}$.

3. Poiché $\mathbb{Q}[\alpha] = \mathbb{E}$ =campo di spezzamento di un polinomio a coefficienti interi, l'estensione $\mathbb{Q}[\alpha]|\mathbb{Q}$ è normale. Essa è anche separabile, essendo la caratteristica di $\mathbb{Q}$ zero. Quindi è un'estensione di Galois.

4. Sia G il gruppo di Galois dell'estensione. Si ha che $|G| = |\mathbb{E} : \mathbb{Q}| = 4$, e, come nell'esercizio precedente, utilizziamo la corrispondenza di Galois per capire di che gruppo si tratta. Sia $\mathbb{K}$ un campo intermedio, $\mathbb{Q} \subsetneqq \mathbb{K} \subsetneqq \mathbb{E} = \mathbb{Q}[\alpha]$. Allora $|\mathbb{Q}[\alpha] : \mathbb{K}| = 2$ e $|\mathbb{K} : \mathbb{Q}| = 2$. Sia $g(X)$ il polinomio minimo di α su $\mathbb{K}$. Sappiamo che $g(X)$ è un polinomio a coefficienti in $\mathbb{K}$, di grado due, tale che $g(\alpha) = 0$ e che $g(X)$ divide $f(X)$. Pertanto $g(x)$ può essere solamente uno dei seguenti polinomi

$$(X-\alpha)(X+\alpha) \ \text{ oppure } \ (X-\alpha)(X-\beta) \ \text{ oppure } \ (X-\alpha)(X+\beta).$$

Dal fatto che $\alpha^2 = 2 + \sqrt{2}$ e che $\alpha\beta = \sqrt{2}$ si ha che, qualunque cosa sia il polinomio g, il suo termine noto coinvolge l'elemento $\sqrt{2}$. Ne segue che $\sqrt{2} \in \mathbb{K}$ e quindi $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{K}$. Infine poiché $\mathbb{Q}[\sqrt{2}]$ ha grado due su $\mathbb{Q}$, esattamente quanto $\mathbb{K}$, abbiamo che $\mathbb{Q}[\sqrt{2}] = \mathbb{K}$. Dunque esiste un unico campo intermedio e per il teorema di corrispondenza esiste un unico sottogruppo di G d'ordine 2, cioè $G \simeq C_4$.

Esercizio 3. *Sia $\mathbb{E}$ un campo d'ordine 128 e sia $\mathbb{F}$ il suo sottocampo fondamentale.*

1. *Determinare il numero di campi intermedi tra $\mathbb{F}$ ed $\mathbb{E}$.*
2. *Sia f un fattore irriducibile del polinomio $x^{128} - x \in \mathbb{Z}_2[x]$. Provare che $f = x$, oppure $f = x - 1$, oppure f ha grado 7.*
3. *Determinare il numero di fattori irriducibili di $x^{128} - x$ in $\mathbb{Z}_2[x]$.*

Svolgimento. 1) Abbiamo che $|E| = 2^7$, pertanto $\mathbb{F} = \mathbb{Z}_2$; inoltre il grado $|\mathbb{E} : \mathbb{F}| = \log_2(128) = 7$, ed essendo un numero primo non ci sono campi intermedi propri non-banali tra $\mathbb{F}$ ed $\mathbb{E}$.

2) Ovviamente

$$x^{128} - x = x(x-1)(x^{126} + x^{125} + x^{124} + \ldots + x^2 + x + 1).$$

Sia $f \in \mathbb{Z}_2[x]$ un fattore irriducibile diverso da x e da $x - 1$. Ora per quanto visto a teoria, $\mathbb{E}$ è campo di spezzamento di $x^{128} - x$ su $\mathbb{F} = \mathbb{Z}_2$, ne segue che $\mathbb{E}$ contiene una radice α di f, pertanto dalla formula dei gradi segue che

$$deg(f) = deg(min_{\mathbb{F}}(\alpha)) = |\mathbb{F}[\alpha] : \mathbb{F}| \,\big|\, |\mathbb{E} : \mathbb{F}| = 7$$

e, poiché $f \notin \{x, x-1\}$, f ha grado > 1 e quindi $deg(f) = 7$.

3) Per quanto detto al punto precedente il numero di fattori irriducibili di $x^{128} - x$ è dato da

$$1 + 1 + \frac{126}{7} = 1 + 1 + 18 = 20.$$

Esercitazione n. 26

22/12/2016

Argomenti. Estensioni di campi e Teoria di Galois.

Esercizio 1. *Sia $\mathbb{E}|\mathbb{F}$ un'estensione algebrica, non necessariamente finita, e sia $G = Gal(\mathbb{E}, \mathbb{F})$. Allora G opera su $\mathbb{E}$. Provare che la G-orbita di ogni elemento $\alpha \in \mathbb{E}$ è finita.*

Svolgimento. Siano $\alpha \in \mathbb{E}$ ed f il suo polinomio minimo su $\mathbb{F}$. Poiché ogni elemento σ del guppo G fissa i coefficienti di f è immediato accorgersi che $\sigma(\alpha)$ è ancora una radice di f. Ne segue che la G-orbita

$$\alpha^G = \{\sigma(\alpha) | \sigma \in G\}$$

è costituita da radici del polinomio f. Essendo queste in numero finito, tale è la cardinalità di α^G.

Esercizio 2. *Sia*

$$f(x) = x^6 + 2x^4 + 3x^2 + 6 \in \mathbb{Z}_7[x].$$

Determinare:

1. *il numero di radici multiple di f in un suo campo di spezzamento su $\mathbb{Z}_7$,*
2. *un'estensione di $\mathbb{Z}_7$ su cui f ha almeno una radice multipla,*
3. *la fattorizzazione in fattori irriducibili di f in $\mathbb{Z}_7[x]$,*
4. *il campo di spezzamento di f su $\mathbb{Z}_7$.*

Svolgimento. 1) Facciamo la derivata formale di f nell'anello dei polinomi $\mathbb{Z}_7[x]$,

$$f' = 6x^5 + x^3 + 6x = -x(x^4 - x^2 + 1)$$

e calcoliamo il massimo comune divisore (f, f'). Applicando l'algoritmo euclideo si trova che

$$(f, f') = x^2 + 2 \neq 1.$$

Ne segue che f ha radici multiple in un'opportuna estensione di $\mathbb{Z}_7$. Le radici multiple di f sono esattamente le radici del fattore $x^2 + 2$ e pertanto sono due.

2) Consideriamo

$$\mathbb{K} = \frac{\mathbb{Z}_7[x]}{\langle x^2+2\rangle} = \left\{a_0 + a_1 x + \langle x^2+2\rangle \,|a_0, a_1 \in \mathbb{Z}_7\right\}.$$

Essendo x^2+2 irriducibile su $\mathbb{Z}_7$ (poiché di grado due e privo di radici), l'ideale principale $\langle x^2+2\rangle$ è massimale e dunque $\mathbb{K}$ è un campo. Inoltre $\mathbb{K}$ contiene un campo isomorfo a $\mathbb{Z}_7$, precisamente

$$\left\{a_0 + \langle x^2+2\rangle \,|a_0 \in \mathbb{Z}_7\right\},$$

e le radici multiple, $\pm x + \langle x^2+2\rangle$, di f.

3) Scomponiamo f ricordando che stiamo lavorando modulo 7:

$$\begin{aligned} x^6+2x^4+3x^2+6 &= x^4(x^2+2)+3(x^2+2) = (x^2+2)(x^4+3) \\ &= (x^2+2)(x^2+2)(X^2+5) = (X^2+2)^2(x^2+5) \\ &= (X^2+2)^2(x-3)(x-4). \end{aligned}$$

4) Il campo $\mathbb{K}$ del punto 2) risulta pertanto essere un campo di spezzamento di f su $\mathbb{Z}_7$.

Esercizio 3. *Descrivere la struttura del gruppo di Galois associato al polinomio X^4-2.*
Dire quanti sono i campi intermedi tra $\mathbb{Q}$ e un campo di spezzamento di tale polinomio.

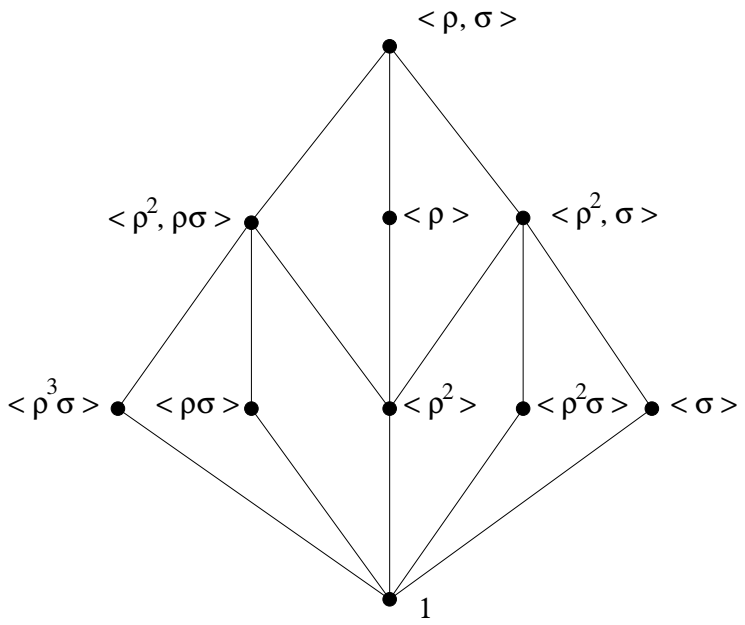
Svolgimento. Il polinomio $g(X) := X^4-2$ è irriducibile in $\mathbb{Q}[X]$ per il criterio di Eisenstein. Le sue radici complesse sono

$$\sqrt[4]{2},\ \ i\sqrt[4]{2},\ \ -\sqrt[4]{2},\ \ -i\sqrt[4]{2}.$$

Pertanto il suo campo di spezzamento (in $\mathbb{C}$ su $\mathbb{Q}$) è $\mathbb{E} = \mathbb{Q}[\sqrt[4]{2}, i]$. $\mathbb{E}|\mathbb{Q}$ è sicuramente un'estensione finita, normale e separabile, quindi un'estensione di Galois. Pertanto il gruppo $G := \mathrm{Gal}(\mathbb{E}|\mathbb{Q})$ ha ordine

$$\begin{aligned} |G| = |\mathbb{E}:\mathbb{Q}| &= \left|\mathbb{Q}[\sqrt[4]{2}, i]:\mathbb{Q}\right| = \\ &= \left|\mathbb{Q}[\sqrt[4]{2}, i]:\mathbb{Q}[\sqrt[4]{2}]\right| \left|\mathbb{Q}[\sqrt[4]{2}]:\mathbb{Q}\right| = \\ &= \deg(\min_{\mathbb{Q}[\sqrt[4]{2}]}(i)) \cdot \deg(\min_{\mathbb{Q}}(\sqrt[4]{2})) = \\ &= \deg(X^2+1)\cdot\deg(X^4-2) = 8. \end{aligned}$$

(Essendo $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathbb{R}$, il polinomio minimo di i su $\mathbb{Q}[\sqrt[4]{2}]$ è sempre X^2+1.)
Sappiamo inoltre che G agisce sull'insieme delle quattro radici di f, e che tale azione è fedele (cioè ha nucleo banale). Pertanto G è isomorfo ad un sottogruppo d'ordine 8 del gruppo simmetrico S_4. Ovvero G è isomorfo ad un 2-Sylow di S_4. I 2−Sylow di S_4 sono isomorfi al gruppo diedrale d'ordine 8 $D_8 := \langle \rho, \sigma | \rho^4 = 1,\ \sigma^2 = 1,\ \sigma^{-1}\rho\sigma = \rho^{-1}\rangle$. Il reticolo dei sottogruppi di un gruppo diedrale d'ordine 8 è il seguente.



Per il Teorema di corrispondenza di Galois esistono pertanto 10 campi intermedi tra $\mathbb{Q}$ e un campo di spezzamento di tale polinomio, esattamente tanti quanti i sottogruppi di $G \simeq D_8$ (contando pure il sottogruppo banale e l'intero gruppo).