Compitino di Algebra 1
8 febbraio 2022

Cognome e nome: .....

Numero di matricola: ..... Aula: .....

IMPORTANTE: Non si possono consultare libri e appunti. Non si possono usare calcolatrici, computer o altri dispositivi elettronici. Non si può scrivere con la matita. Ogni passaggio va motivato.

Esercizio 1.

1. Dimostrare che per $n = 2, 3, 4$ se H è un sottogruppo di indice n in S_n allora H è isomorfo a S_{n-1}.

2. Sia $n \geq 2$. Dato $i \in \{1, 2, .., n\}$ sia $Fix(i)$ il sottogruppo di S_n dato dagli elementi che lasciano fisso i. Dimostrare che i sottogruppi $Fix(i)$, al variare di i in $\{1, .., n\}$ sono tutti coniugati fra loro.

3. Dimostrare che anche per ogni $n \geq 5$ se H è un sottogruppo di indice n in S_n allora H è isomorfo a S_{n-1}.

4. Dimostrare che in S_6 esiste un sottogruppo di indice 6 non coniugato ai sottogruppi $Fix(i)$. [Può essere utile considerare i 5-Sylow...]

1) In generale è andato bene. Segnalo che nel caso $n = 4$ un sottogruppo di indice 4 di S_4 ha 6 elementi. Sappiamo che un gruppo di cardinalità 6 è isomorfo a $\mathbb{Z}_6$ o a S_3. Poiché però in S_4 non ci sono elementi di ordine 6 (né 6-cicli né prodotti di (vari) 2-cicli e (vari) 3-cicli disgiunti), i sottogruppi in questione sono isomorfi a S_3. [Noto che esistono e sono i $Fix(i)$.]

2) È andato abbastanza bene.

Un modo di risolverlo era osservare direttamente che

$$(i,j)\ \mathrm{Fix}(i)\ (i,j) = \mathrm{Fix}(j)$$

Infatti se $\tau \in \mathrm{Fix}(i)$ allora se si applica $(i,j)\cdot\tau(i,j)$ a j si ottiene j. Dunque

$$(i,j)\,\tau\,(i,j) \in \mathrm{Fix}(j).$$

Allora $(i,j)\ \mathrm{Fix}(i)\ (i,j) \subseteq \mathrm{Fix}(j)$

e l'uguaglianza segue per motivi di cardinalità

$$\left(|\mathrm{Fix}(i)| = |(i,j)\ \mathrm{Fix}(i)\ (i,j)| = |\mathrm{Fix}\, j|\right).$$

Più raffinatamente si poteva dire così:

Considero l'azione di S_n su $X=\{1,2,\dots,n\}$.

C'è un'unica orbita, uguale a X stesso.

Lo stabilizzatore di $i \in X$ è $\mathrm{Fix}(i)$.

Lo stabilizzatore di $j \in X$ è $\mathrm{Fix}(j)$.

Due stabilizzatori di due elementi di una stessa orbita sono, come sappiamo dalla teoria, coniugati fra loro.

3) Sia ora $n \geq 5$ e sia H un sottogruppo di indice n.

Facciamo agire S_n su S_n/H da sinistra.
Questo ci dà l'omomorfismo

$$\Gamma : S_n \longrightarrow Bij\left(S_n/H\right) \cong S_n$$

Su $\ker\Gamma$ sappiamo due cose:

A) $\ker\Gamma \trianglelefteq S_n$

B) $\ker\Gamma \leq H$. ← vale tutte le volte che un gruppo G agisce su G/H nel modo standard.

Visto che $n \geq 5$, la A) ci lascia tre sole scelte per $\ker\Gamma$:

$$\ker\Gamma = \begin{cases} \{e\} \\ \{A_n\} \\ \{S_n\} \end{cases}$$

NO perché $|A_n| = \frac{n!}{2}$ e $|H| = (n-1)!$ e dato che $n \geq 5$ $\frac{n!}{2} > (n-1)!$ che contraddice $\ker\Gamma \leq H$.

NO perché l'azione non è banale.

Allora Γ è INIETTIVA.
Dunque $\Gamma(H)$ è un s. gruppo isomorfo ad H e giace in $Bij\left(S_n/H\right) \cong S_n$.

Che sottogruppo è $\Gamma(H)$? Poiché nell'azione da sinistra se $h \in H$ vale che $h \cdot H = H$, gli elementi di $\Gamma(H)$ sono biiezioni in $Big(S_n/H)$ che fissano la classe laterale H.
Dunque, identificando $Big(S_n/H)$ con S_n, sono biiezioni che fissano un elemento, diciamo 1.
Allora $\Gamma(H) < Fix(1)$ e per ragioni di cardinalità $\Gamma(H) = Fix(1)$ che è isomorfo a S_{n-1}.
Dunque H è ISOMORFO a S_{n-1}.

4) Sia X l'insieme dei 5-Sylow di S_5.
(Il suggerimento diceva di considerare i 5-Sylow, ho dato comunque un punto a chi ha studiato i 5-Sylow di S_6, ma la cosa rilevante era considerare quelli di S_5). Come si vede facilmente, $|X| = 6$.
Sappiamo per Sylow II che S_5 agisce su X per coniugio formando un'unica orbita.
Questo dà un omomorfismo:

$$\varphi : S_5 \longrightarrow Big(X) \cong S_6$$

Come sopra, sappiamo che $\ker \varphi \triangleleft S_5$

dunque

$$\ker \varphi = \begin{cases} \{e\} \\ A_5 \\ S_5 \end{cases}$$

NO perché sarebbe $|\mathrm{Im}\,\varphi| = 2$ dunque le orbite prodotte in X dall'azione dovrebbero avere cardinalità che divide 2, ma sappiamo che c'è un'unica orbita di cardinalità 6.

NO perché l'azione sarebbe banale

Allora φ è iniettiva e $\varphi(S_5) = H$ è un sottogruppo di S_6 di cardinalità $5!$ e dunque di indice 6. Dato che l'azione di H su $\{1,2,3,4,5,6\}$ produce un'unica orbita, non c'è nessun i fissato da tutti gli elementi di H, e dunque H è diverso da $\mathrm{Fix}(i)$ per ogni i. Dato che i coniugati dei $\mathrm{Fix}(i)$ sono ancora dei $\mathrm{Fix}(j)$, H non è coniugato a nessuno dei $\mathrm{Fix}(i)$.

Esercizio 2 (Miscellanea). 1. Esibire un generatore v_1 del sottogruppo $H = \{4x + 6y = 0\}$ di $\mathbb{Z}^2$. Esibire elementi v_2, v_3, v_4 di $\mathbb{Z}^2$ tali che per ogni $i = 2, 3, 4$ il sottogruppo (v_1, v_i) ha indice i in $\mathbb{Z}^2$. È possibile trovare v_4 tale che $\mathbb{Z}^2/(v_1, v_4)$ sia isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$?

2. Sia G un gruppo abeliano finito e sia n un intero positivo che divide $|G|$. Dimostrare che esiste un sottogruppo K di G di ordine n. Dimostrare che le soluzioni dell'equazione $x^n = e$ sono un multiplo di n.

3. Trovare un polinomio $f(x) \in \mathbb{Z}_2[x]$ tale che $K = \mathbb{Z}_2[x]/(f(x))$ sia una estensione di Galois di $\mathbb{Z}_2$ con gruppo di Galois isomorfo a $\mathbb{Z}_5$.

1) In sintesi: generatore $\begin{pmatrix} -3 \\ 2 \end{pmatrix}$ oppure $\begin{pmatrix} 3 \\ -2 \end{pmatrix}$

(non ce ne sono ALTRI!).

Per v_i basta scegliere un vettore $\begin{pmatrix} a \\ b \end{pmatrix}$ tale che

$$\det \begin{pmatrix} -3 & a \\ 2 & b \end{pmatrix} = \pm i$$

Dunque per esempio $v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$v_4 = \begin{pmatrix} -2 \\ 2 \end{pmatrix}$

Dato che quando si crea la forma di Smith $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ vale che $d_1 = MCD$ dei coefficienti di $\begin{pmatrix} -3 & a \\ 2 & b \end{pmatrix}$ allora $d_1 = 1$. Questo mostra che non è

possibile che $\mathbb{Z}^2/(v_1, v_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

2) Come sappiamo G è prodotto dei suoi p-Sylow.

Sia $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ | $|G| = p_1^{\beta_1} \cdots p_k^{\beta_k} \cdots p_s^{\beta_s}$

Dunque il p_1-Sylow N_{p_1} di G ha $p_1^{\beta_1}$ elementi con $\beta_1 \geq \alpha_1$. Per Sylow I ∞ che esiste in N_{p_1} un n-gruppo H_1 tale che $|H_1| = p_1^{\alpha_1}$.

Ripetendo per ogni $i = 1, \ldots, k$ trovo che

$H = H_1 H_2 H_3 \cdots H_k$ è un n-gruppo di G di cardinalità n.

Per la seconda parte, si osserva subito che

$$S = \{x \in G \mid x^n = e\}$$ è un n-gruppo di G dato che G è abeliano.

Inoltre il n-gruppo H di cardinalità n trovato sopra è contenuto in S visto che l'ordine di ogni suo elemento divide n per un corollario del Teo di Lagrange.

Allora $n = |H| \mid |S|$ per il teo di Lagrange.

3) Come sappiamo, una estensione di $\mathbb{F}_2$ di grado 5 è una estensione di Galois con gruppo di Galois isomorfo a $\mathbb{Z}/5$ (generato dall'automorfismo di Frobenius F).

Basta dunque trovare un polinomio $f(x) \in \mathbb{Z}/2[x]$ IRRIDUCIBILE di grado 5.

Bisogna che

1) non abbia radici, dunque $f(0) \neq 0$, $f(1) \neq 0$.
2) non sia divisibile per x^2+x+1, che è l'unico polinomio IRRID di grado 2 in $\mathbb{Z}/2[x]$.

NOTATE che ogni fattorizzazione in irriducibili di un polinomio di grado 5 (che non è IRRID) include sempre o un polinomio IRRID di grado 1 o un polinomio IRRID di grado 2.

Con poche verifiche si trova per esempio che

$$x^5+x^4+x^3+x^2+1 \quad \text{è irriducibile in } \mathbb{Z}/2[x].$$

Esercizio 3. Si consideri il campo di spezzamento K su $\mathbb{Q}$ del polinomio $x^8 - 9$.

1. Calcolare $[K : \mathbb{Q}]$.

2. Descrivere il gruppo di Galois $Aut(K/\mathbb{Q})$ ed esibire dei generatori.

Punto 1. Le radici di $x^8 - 9$ sono della forma $\sqrt[8]{9}\zeta_8^i$ con $i = 0, 1, \ldots, 7$. Si osservi che $\sqrt[8]{9} = \sqrt[4]{3}$ e quindi $K = \mathbb{Q}(\sqrt[4]{3}, \zeta_8)$. Sappiamo che $\zeta_8 = \cos(\pi/4)+i\sin(\pi/4) = (\sqrt{2}+i\sqrt{2})/2$. Vediamo che $\mathbb{Q}(\sqrt[4]{3}, \zeta_8) = \mathbb{Q}(\sqrt{2}, i, \sqrt[4]{3})$. Il contenimento $\subseteq$ segue dal fatto che ζ_8 è uguale a $\sqrt{2}(1 + i)/2$. Il contenimento $\supseteq$ segue dal fatto che $i = \zeta_8^2$ e che $\sqrt{2} = 2\zeta_8/(1 + i)$. Quindi $K = \mathbb{Q}(\sqrt{2}, i, \sqrt[4]{3})$.

Calcoliamo ora il grado. Il polinomio $x^4 - 3$ è irriducibile per Eisenstein e quindi $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}$ ha grado 4. Supponiamo per assurdo che $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{3})$. Allora $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ è un campo di grado 4 (visto che $3/2$ non è un quadrato in $\mathbb{Q}$) ed è contenuto in $\mathbb{Q}(\sqrt[4]{3})$. Ma visto che entrambi i campi hanno grado 4 devono essere uguali, ma una estensione è di Galois e l'altra no, il che è assurdo. Quindi $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{3})$. Dunque, $[\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[4]{3})] = 2$. Inoltre $[\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i) : \mathbb{Q}(\sqrt{2}, \sqrt[4]{3})] = 2$ perché i è complesso e il campo base è reale. Quindi,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i) : \mathbb{Q}(\sqrt{2}, \sqrt[4]{3})]\cdot[\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}), \mathbb{Q}(\sqrt[4]{3})]\cdot[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 16.$$

Nota: In molti avete dato per scontato che $\sqrt{2}$ non appartiene a $\mathbb{Q}(\sqrt[4]{3})$ o a $\mathbb{Q}(\sqrt[4]{3}, i)$. Questo non è affatto ovvio, andava dimostrato. □

Punto 2. Sia $K_1 = \mathbb{Q}(\sqrt{2})$ e $K_2 = \mathbb{Q}(\sqrt[4]{3}, i)$. Il campo K_1 è di Galois su $\mathbb{Q}$ e ha grado 2. Il campo K_2 è di Galois (è cds di $x^4 - 3$) e ha grado 8. Se $[K_1 \cap K_2 : \mathbb{Q}] = 2$, allora $K_1 \subseteq K_2$ e quindi $K = K_2$. Questo è assurdo per motivi di grado (abbiamo visto $[K : \mathbb{Q}] = 16$) e concludiamo che $[K_1 \cap K_2 : \mathbb{Q}] = 1$. Per i teoremi di Galois abbiamo

$$\mathrm{Gal}(K : \mathbb{Q}) \cong \mathrm{Gal}(K/K_1) \times \mathrm{Gal}(K/K_2) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}).$$

Il gruppo $\mathrm{Gal}(K_1/\mathbb{Q})$ ha ordine 2 ed è generato da σ tale che $\sigma(\sqrt{2}) = -\sqrt{2}$. Il gruppo $\mathrm{Gal}(K_2/\mathbb{Q})$ ha ordine 8, non è abeliano perché contiene una sottoestensione non di Galois $(\mathbb{Q}(\sqrt[4]{3}))/\mathbb{Q})$ ed è contenuto in S_4. Quindi è necessariamente D_4. Sia $r \in \mathrm{Gal}(K_2/\mathbb{Q})$ tale che $r(i) = i$ e $r(\sqrt[4]{3}) = i\sqrt[4]{3}$ e

sia $s \in \mathrm{Gal}(K_2/\mathbb{Q})$ tale che $s(i) = -i$ e $s(\sqrt[4]{3}) = \sqrt[4]{3}$. Si vede facilmente che $\mathrm{Gal}(K_2/\mathbb{Q})$ è generato da r e s. Quindi

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times D_4$$

ed è generato da $(\sigma, 1)$, $(1, r)$ e $(1, s)$. Per essere precisi, i tre generatori sono

$$\sigma_1 = \begin{cases} \sqrt{2} \to -\sqrt{2} \\ i \to i \\ \sqrt[4]{3} \to \sqrt[4]{3} \end{cases} \qquad \sigma_2 = \begin{cases} \sqrt{2} \to \sqrt{2} \\ i \to -i \\ \sqrt[4]{3} \to \sqrt[4]{3} \end{cases} \qquad \sigma_3 = \begin{cases} \sqrt{2} \to \sqrt{2} \\ i \to i \\ \sqrt[4]{3} \to i\sqrt[4]{3} \end{cases}$$

□

Visto che alcuni hanno risolto il punto 1 usando un'altra via, faccio vedere velocemente come si poteva risolvere l'esericizo 1 in modo alternativo.

Dimostrazione alternativa punto 1. Sia E il cds di $x^4 - 3$ e F il cds di $x^4 + 3$. Visto che $x^8 - 9 = (x^4 - 3)(x^4 + 3)$ abbiamo $K = EF$. Notiamo che i e $\sqrt{3}$ appartengono sia a E che a F. Quindi $[E \cap F : \mathbb{Q}]$ è almeno 4 e divide 8, cioè il grado di E.

Se fosse 8, avremmo che $E = F$, vediamo che è assurdo. Come visto prima abbiamo $\sqrt{2} \in EF$ e se avessimo $E = F$ avremmo $\sqrt{2} \in E$. Sappiamo che $\mathrm{Gal}(E/\mathbb{Q}) = D_4$ e i sottogruppi di ordine 4 (e quindi di indice 2) sono 3, quello generato da r, quello generato da r^2 e s e quello generato da sr e r^2. Quindi ci sono 3 campi E' tali che $[E' : \mathbb{Q}] = 2$ e $E' \subseteq E$. Visto che $\sqrt{3}$ e i appartengono a E abbiamo che le tre sottoestensioni di E di grado 2 sono $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$. Ma $\sqrt{2}$ non appartiene a nessuno di questi campi e quindi $\sqrt{2} \notin E$. Concludiamo che $[E \cap F : \mathbb{Q}] \neq 8$.

Allora, $[E \cap F : \mathbb{Q}] = 4$ e $[E : E \cap F] = [E : \mathbb{Q}]/[E \cap F : \mathbb{Q}] = 8/4 = 2$. Allo stesso modo $[F : E \cap F] = 2$. Quindi,

$$\begin{aligned} [K : \mathbb{Q}] &= [EF : \mathbb{Q}] = [EF : E \cap F] \cdot [E \cap F : \mathbb{Q}] \\ &= [E : E \cap F] \cdot [F : E \cap F] \cdot [E \cap F : \mathbb{Q}] \\ &= 16. \end{aligned}$$

□