UNIVERSITÀ DEGLI STUDI DI BARI

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

CORSO DI LAUREA IN MATEMATICA

ESERCIZIARIO DI ALGEBRA 1

Autore:

Dott. Francesco Sasso

Introduzione

Questo eserciziario nasce dalla necessità di mettere a disposizione degli studenti alcune tipologie di esercizi di Algebra, specificando altresì comuni pratiche di risoluzione degli stessi. L'opera che leggete si basa sulle lezioni di Algebra 1 del corso di Laurea Triennale in Matematica dell'Università degli Studi di Bari. Tali lezioni, tenute annualmente dalla Prof.ssa Margherita Barile, sono reperibili in formato PDF al link [1] (vedasi la Bibliografia). Non voglio ora fare una distinzione di sorta, ma in base a quanto premesso, il seguente eserciziario è rivolto in primis agli studenti impegnati a superare l'esame scritto del suddetto corso. Ciononostante, spero sia una lettura gradita anche a un pubblico più vasto. Specifico inoltre che gli esercizi qui presenti sono stati opportunamente selezionati tra le tracce d'esame del corso, anch'esse presenti in [1].
Questo eserciziario non deve essere scambiato per un manuale pratico di risoluzione degli esercizi d'esame. Gli svolgimenti che vi vengono proposti non sono gli unici possibili, e spesso non sono nemmeno i più semplici. Alcuni di essi includono nozioni avanzate, non contenute nel programma di esame. Essi vanno intesi come una palestra di approfondimento dei concetti, in quanto costringono il lettore a comprendere, di questi ultimi, tutti gli aspetti numerici, strutturali, combinatori, compresi i meno evidenti. La sfida lanciata con queste note vuole essere un invito a prendere familiarità con oggetti astratti, costruiti formalmente, e che vanno manipolati sulla base delle proprietà di cui godono, prescritte dalle definizioni o dedotte tramite i teoremi.
Il primo passo per superare le difficoltà è riconoscere ed accettare, per intero e senza paura, la complessità del problema che si ha di fronte.
Detto questo, non mi resta che augurare a tutti voi un buono studio e rivolgere, agli studenti impegnati nel superamento dell'esame di Algebra 1, un beneaugurante in bocca al lupo.

Dott. Francesco Sasso

Indice

Capitolo 1

Premesse

Il fine di questo capitolo, lo diciamo subito, è quello di mettere sullo stesso piano la teoria e la pratica. Le ragioni di quest'asserzione risulteranno senza dubbio più chiare nel seguito.

1.1 Sui metodi risolutivi

È del tutto lecito, soprattutto per uno studente alle prime armi, chiedersi se esista un metodo meccanico attraverso cui riuscire a risolvere le diverse tipologie di problemi. La speranza di chi se lo chiede è quella di quozientare opportunamente l'insieme degli esercizi, in modo da ottenere un numero "sufficientemente piccolo" delle cosiddette tipologie, e che per ciascuna tipologia possa essere applicato questo fantomatico ragionamento meccanico a cui prima accennavamo.
È bene chiarire sin da subito che, per quanto riguarda l'Algebra, questa speranza va disillusa. Lo studente che si accinge alla risoluzione deve quindi mettersi l'anima in pace, e soprattutto deve sapere che gli esercizi proposti sono realizzati in modo che egli possa mettere in pratica gli strumenti provenienti dalla teoria, ragion per cui è vivamente consigliato uno studio della stessa che sia quanto più accurato possibile, e tutto ciò prima di cominciare con la pratica.
Se ciò sarà stato fatto, ci si renderà presto conto di come possano esistere diverse strade che conducano alla risoluzione di uno stesso problema, e anzi di più: in alcuni casi potrà risolversi lo stesso esercizio sia con risultati provenienti dall'Algebra che con risultati provenienti da altre discipline, quale è ad esempio l'Analisi. Si lascia quindi una certa libertà di ragionamento al risolutore, che deve convincere l'esaminatore di aver compreso a pieno gli insegnamenti e di saperli maneggiare con cura e, magari, con la fantasia che contraddistingue il bravo matematico.
Illustriamo adesso due esercizi che mettano in luce quanto detto sopra, in modo da togliere il dubbio a chi ancora credesse nell'esistenza di un metodo meccanico che ci tolga dagli impicci.

- Esercizio 1.1.1: Si consideri il polinomio

$$f(x) = x^{9604} + 5x^3 - 18x^2 - 20x + 30 \in \mathbb{Z}[x].$$

Provare che $f(x)$ non ha radici multiple in $\mathbb{Z}$.

Di questo esercizio proponiamo due distinti svolgimenti.

Svolgimento 1: Supponiamo per assurdo che α sia radice multipla di $f(x)$ in $\mathbb{Z}$, da ciò segue, per il Teorema di Ruffini e per il Lemma di Gauss, che $(x-\alpha)^2$ divide $f(x)$ in $\mathbb{Z}[x]$, ossia:

$$\exists g(x) \in \mathbb{Z}[x] \text{ tale che } f(x) = (x-\alpha)^2 \cdot g(x)$$

Sappiamo inoltre, da una nota proposizione, che

$$\exists r, s \in \mathbb{Z} \text{ tali che } r \mid 30, s \mid 1 \text{ e } \alpha = \tfrac{r}{s}$$

il che può essere riassunto dicendo che $\alpha \in \{r \in \mathbb{Z} \mid r \mid 30\}$, motivo per il quale fattorizziamo il termine noto di $f(x)$, osservando che $30 = 2 \cdot 3 \cdot 5$. Indichiamo ora con $\overline{f}_i(x), \overline{g}_i(x)$ le riduzioni modulo i di $f(x), g(x)$ in $\mathbb{Z}_i[x]$ con $i \in \{2,3,5\}$. Abbiamo allora che:

$$\overline{f}_i(x) = (x - [\alpha]_i)^2 \cdot \overline{g}_i(x) \qquad i \in \{2,3,5\}$$

ragion per cui $[\alpha]_i$ è radice multipla di $\overline{f}_i(x)$ in $\mathbb{Z}_i$, con $i \in \{2,3,5\}$. In particolare $[\alpha]_3$ è radice multipla di $\overline{f}_3(x)$ in $\mathbb{Z}_3$. Andiamo quindi alla ricerca delle radici di $\overline{f}_3(x)$ in $\mathbb{Z}_3$. Osserviamo che:

$$\overline{f}_3(x) = x^{9604} - x^3 + x = x \cdot (x^{9603} - x^2 + [1]_3) = x \cdot \overline{h}_3(x)$$

dove $\overline{h}_3(x) = x^{9603} - x^2 + [1]_3$. Proviamo che $\overline{h}_3(x)$ non ha radici in $\mathbb{Z}_3$. Anzitutto è immediato verificare che $[0]_3$ non è radice di $\overline{h}_3(x)$. Consideriamo ora $\beta \in \mathbb{Z}_3$ con $\beta \neq [0]_3$. Allora sfruttando il teorema di Eulero, si ha che:

$$\overline{h}_3(\beta) = \beta^{9603} - \beta^2 + [1]_3 = \beta^{4801 \cdot 2 + 1} - \beta^2 + [1]_3 = \beta - [1]_3 + [1]_3 = \beta \neq [0]_3$$

e dunque $\overline{h}_3(x)$ non ha radici in $\mathbb{Z}_3$. Ne deduciamo quindi che l'unica radice di $\overline{f}_3(x)$ in $\mathbb{Z}_3$ è $[0]_3$, e che tale radice è semplice in quanto $\overline{h}_3(x)$ è privo di radici in $\mathbb{Z}_3$. In definitiva $\overline{f}_3(x)$ non possiede radici multiple in $\mathbb{Z}_3$, ma prima avevamo detto che $[\alpha]_3$ era una radice multipla di $\overline{f}_3(x)$ in $\mathbb{Z}_3$. Siamo quindi pervenuti a un assurdo, derivato dall'aver supposto che $f(x)$ avesse una radice multipla in $\mathbb{Z}$. Di conseguenza $f(x)$ non possiede radici multiple in $\mathbb{Z}$.

Svolgimento 2: Stavolta adottiamo una strategia diversa. Anziché agire per assurdo, faremo vedere esplicitamente che $f(x)$ non ha radici multiple in $\mathbb{Z}$ dimostrando che $f(x)$ non possiede radici in $\mathbb{Z}$. Per far ciò utilizzeremo un ragionamento più analitico che algebrico. Anzitutto, è immediato verificare che $f(0) \neq 0, f(1) \neq 0, f(-1) \neq 0$. Consideriamo quindi $\alpha \in \mathbb{Z}$, con $|\alpha| \geq 2$, e facciamo vedere che $f(\alpha) > 0$. Ciò equivale a provare che:

$$-5\alpha^3 + 18\alpha^2 + 20\alpha - 30 < \alpha^{9604} \qquad (1)$$

Proviamo quindi la (1). Ovviamente si ha che:

$$-5\alpha^3 + 18\alpha^2 + 20\alpha - 30 \leq 5\,|\alpha|^3 + 18\,|\alpha|^2 + 20\,|\alpha| + 30$$

e siccome $max\{5, 18, 20\} < 30$, allora:

$$5\,|\alpha|^3 + 18\,|\alpha|^2 + 20\,|\alpha| + 30 < 30(|\alpha|^3 + |\alpha|^2 + |\alpha| + 1)$$

ora, tenuto conto che $2 \leq |\alpha|$, si ha che $max\{|\alpha|^2, |\alpha|, 1\} < |\alpha|^3$, e quindi

$$30(|\alpha|^3 + |\alpha|^2 + |\alpha| + 1) < 30(|\alpha|^3 + |\alpha|^3 + |\alpha|^3 + |\alpha|^3) = 120\,|\alpha|^3 = 2^3 \cdot 3 \cdot 5\,|\alpha|^3$$

e ricordandosi nuovamente che $2 \leq |\alpha|$, deduciamo che $2^3 \leq |\alpha|^3$, $3 < 2^3 \leq |\alpha|^3$, e inoltre $5 < 2^3 \leq |\alpha|^3$, ragion per cui:

$$2^3 \cdot 3 \cdot 5\,|\alpha|^3 < |\alpha|^3 \cdot |\alpha|^3 \cdot |\alpha|^3 \cdot |\alpha|^3 = |\alpha|^{12} < |\alpha|^{9604} = \alpha^{9604}$$

e quindi riassumendo il tutto si ha che:

$$-5\alpha^3 + 18\alpha^2 + 20\alpha - 30 < \alpha^{9604}$$

ossia abbiamo provato la (1). Possiamo ora raccogliere le suddette informazioni per dire che effettivamente $f(x)$ non possiede radici in $\mathbb{Z}$, e quindi a maggior ragione non ha radici multiple in $\mathbb{Z}$.

- Esercizio 1.1.2: Si consideri il polinomio

$$f(x) = x^4 + 8270 \cdot 14876^{100}x^3 + 15413^{798543}x + 2 \cdot 27584^{81} \in \mathbb{Z}[x].$$

1. Provare che la riduzione modulo 3 di $f(x)$ si decompone in $\mathbb{Z}_3[x]$ nel prodotto di fattori lineari.
2. Determinare una fattorizzazione in $\mathbb{Z}_5[x]$ della riduzione di $f(x)$ modulo 5.
3. Provare che $f(x)$ non ha radici intere divisibili per 6.

La parte interessante dello svolgimento riguarda in realtà i soli punti 1. e 3., per la cui risoluzione agiremo adottando due distinti ragionamenti che fanno leva su diversi risultati provenienti dalla teoria algebrica.

Svolgimento

1. Denotiamo con $\overline{f}(x)$ la riduzione modulo 3 di $f(x)$, cioè:

   $$\overline{f}(x) = x^4 + \overline{8270} \cdot \overline{14876}^{100}x^3 + \overline{15413}^{798543}x + \overline{2} \cdot \overline{27584}^{81} \in \mathbb{Z}_3[x]$$

   Dove, ovviamente, col soprassegno si indica la classe di congruenza modulo 3. Sfruttando il teorema di Fermat e la definizione di classe di congruenza, si deduce in modo semplice che:

   $$\overline{f}(x) = x^4 + \overline{2}x^3 + \overline{2}x + \overline{1}$$

   Per fattorizzare $\overline{f}(x)$ in $\mathbb{Z}_3[x]$, per prima cosa andiamo alla ricerca di eventuali sue radici in $\mathbb{Z}_3$. A tal proposito, ci si rende rapidamente conto che $\overline{f}(\overline{1}) = \overline{0}$, ossia $\overline{1}$ è una radice di $\overline{f}(x)$ in $\mathbb{Z}_3$. Possiamo allora applicare il teorema di Ruffini per dire che $(x - \overline{1})$ divide $\overline{f}(x)$ in $\mathbb{Z}_3[x]$; e in effetti, dalla seguente divisione euclidea:

$$\begin{array}{rrrr|rr} x^4 & +\overline{2}x^3 & +\overline{2}x & +\overline{1} & x & -\overline{1} \\ \cline{5-6} -x^4 & +x^3 & & & x^3 & +\overline{2} \\ \cline{1-4} & & \overline{2}x & +\overline{1} & & \\ & & -\overline{2}x & +\overline{2} & & \\ \cline{3-4} & & & \overline{0} & & \end{array}$$

ci si accorge che:

$$\overline{f}(x) = (x - \overline{1})(x^3 + \overline{2})$$

Ovviamente $(x - \overline{1})$ è irriducibile, e resta quindi da decomporre in $\mathbb{Z}_3[x]$ il fattore $\overline{g}(x) = (x^3 + \overline{2})$. A tal fine, si può agire in più di un modo:

(a) si potrebbe agire come al solito, cercando cioè eventuali radici di $\overline{g}(x)$ in $\mathbb{Z}_3$. Stavolta, essendo $deg(g(x)) \leq 3$, l'eventuale assenza di radici in $\mathbb{Z}_3$ implicherebbe, per il 2° corollario al teorema di Ruffini, l'irriducibilità di $\overline{g}(x)$ in $\mathbb{Z}_3[x]$. Se invece è presente una radice, si sfrutta il teorema di Ruffini così come fatto in precedenza;

(b) altrimenti possiamo fare affidamento, in questo particolarissimo caso, al teorema di Fermat e al teorema binomiale di Newton in $\mathbb{Z}_p$ (con p generico numero primo positivo). Cerchiamo di spiegare meglio ciò che intendiamo. Sappiamo, dal teorema binomiale di Newton, che:

$$\forall a, b \in \mathbb{Z} : \qquad (a + b)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^{p-k} b^k$$

tenuto quindi conto che

$$\forall k = 1, ..., p - 1 : \qquad p \mid \left(\frac{p!}{k!(p-k)!} \right)$$

si deduce che:

$$\forall a, b \in \mathbb{Z}_p : \qquad (a + b)^p = a^p + b^p$$

Possiamo allora dire, nel nostro caso, che:

$$\overline{g}(x) = x^3 + \overline{2} = x^3 + \overline{2}^3 = (x + \overline{2})^3$$

dove si sono per l'appunto impiegati il teorema di Fermat (nella seconda uguaglianza) e il teorema binomiale di Newton in $\mathbb{Z}_3$ (nella terza uguaglianza), ottenendo in tal modo la fattorizzazione di $\overline{g}(x)$ in $\mathbb{Z}_3[x]$;

Si ha quindi la seguente decomposizione di $\overline{f}(x)$ in fattori irriducibili in $\mathbb{Z}_3[x]$:

$$\overline{f}(x) = (x - \overline{1})(x + \overline{2})^3$$

2. Denotiamo stavolta con $\hat{f}(x)$ la riduzione di $f(x)$ modulo 5, ossia:

$$\hat{f}(x) = x^4 + \overline{8270} \cdot \overline{14876}^{100} x^3 + \overline{15413}^{798543} x + \overline{2} \cdot \overline{27584}^{81} \in \mathbb{Z}_5[x]$$

Dove stavolta col soprassegno si indica la classe di congruenza modulo 5. Sfruttando il teorema di Fermat e la definizione di classe di congruenza, si deduce in modo semplice che:

$$\hat{f}(x) = x^4 + \overline{2}x + \overline{3}$$

Per fattorizzare $\hat{f}(x)$ in $\mathbb{Z}_5[x]$, per prima cosa andiamo alla ricerca di eventuali sue radici in $\mathbb{Z}_5$. A tal proposito, ci si rende rapidamente conto che $\hat{f}(\overline{3}) = \overline{0}$, ossia $\overline{3}$ è una radice di $\hat{f}(x)$ in $\mathbb{Z}_5$. Possiamo allora applicare il teorema di Ruffini per dire che $(x - \overline{3})$ divide $\hat{f}(x)$ in $\mathbb{Z}_5[x]$; e in effetti, dalla seguente divisione euclidea:

$$\begin{array}{rrrrr|l}
x^4 & & & +\overline{2}x & +\overline{3} & x \quad -\overline{3} \\
\cline{6-6}
-x^4 & +\overline{3}x^3 & & & & x^3 \quad +\overline{3}x^2 \quad +\overline{4}x \quad +\overline{4} \\
\cline{1-2}
 & \overline{3}x^3 & & +\overline{2}x & +\overline{3} & \\
 & -\overline{3}x^3 & +\overline{4}x^2 & & & \\
\cline{2-4}
 & & \overline{4}x^2 & +\overline{2}x & +\overline{3} & \\
 & & -\overline{4}x^2 & +\overline{2}x & & \\
\cline{3-5}
 & & & \overline{4}x & +\overline{3} & \\
 & & & -\overline{4}x & +\overline{2} & \\
\cline{4-5}
 & & & & \overline{0} &
\end{array}$$

ci si accorge che:

$$\hat{f}(x) = (x - \overline{3})(x^3 + \overline{3}x^2 + \overline{4}x + \overline{4})$$

Ovviamente $(x - \overline{3})$ è irriducibile, e resta quindi da decomporre in $\mathbb{Z}_3[x]$ il fattore $\hat{g}(x) = (x^3 + \overline{3}x^2 + \overline{4}x + \overline{4})$. Come prima, cerchiamo eventuali radici di $\hat{g}(x)$ in $\mathbb{Z}_5$, trovando subito che $\hat{g}(\overline{3}) = \overline{0}$, e quindi riapplicando il teorema di Ruffini si ha che $(x - \overline{3})$ divide $\hat{g}(x)$ in $\mathbb{Z}_5[x]$, e dividendo si ottiene che:

$$\begin{array}{rrrr|l}
x^3 & +\overline{3}x^2 & +\overline{4}x & +\overline{4} & x \quad -\overline{3} \\
\cline{5-5}
-x^3 & +\overline{3}x^2 & & & x^2 \quad +x \quad +\overline{2} \\
\cline{1-2}
 & x^2 & +\overline{4}x & +\overline{4} & \\
 & -x^2 & +\overline{3}x & & \\
\cline{2-3}
 & & \overline{2}x & +\overline{4} & \\
 & & -\overline{2}x & +\overline{6} & \\
\cline{3-4}
 & & & \overline{0} &
\end{array}$$

Dunque $\hat{g}(x) = (x - \overline{3}) \cdot \hat{h}(x)$, dove $\hat{h}(x) = (x^2 + x + \overline{2})$. Resta quindi da fattorizzare $\hat{h}(x)$ in $\mathbb{Z}_5[x]$. A tal fine osserviamo che, siccome $\hat{h}(x)$ non ha radici in $\mathbb{Z}_5$ e $deg(\hat{h}(x)) \leq 3$, allora per il 2° corollario al teorema di Ruffini $\hat{h}(x)$ è irriducibile in $\mathbb{Z}_5[x]$. Si ha quindi la seguente decomposizione di $\hat{f}(x)$ in fattori irriducibili in $\mathbb{Z}_5[x]$:

$$\hat{f}(x) = (x - \overline{3})^2(x^2 + x + \overline{2})$$

3. Supponiamo per assurdo che α sia una radice intera di $f(x)$ divisibile per 6. Essendo $f(x)$ polinomio monico a coefficienti interi, allora da una nota proposizione sappiamo che necessariamente α divide il termine noto di $f(x)$. Abbiamo allora che:

$$6 \mid \alpha \quad \wedge \quad \alpha \mid [2 \cdot (27584)^{81}]$$

da cui segue subito che $6 \mid [2 \cdot (27584)^{81}]$, e quindi $3 \mid (27584)^{81}$, ovvero dev'essere $[27584^{81}]_3 = [0]_3$, cioè $[27584]_3^{81} = [0]_3$, e siccome $[27584]_3 = [2]_3$, allora si avrà $[2]_3^{81} = [0]_3$.
Tuttavia $[2]_3 \neq [0]_3$, e siccome $\mathbb{Z}_3$ è integro, allora $[2]_3^{81} \neq [0]_3$, in contraddizione con quanto detto in precedenza. L'assurdo è derivato dall'aver supposto che $f(x)$ avesse radici intere divisibili per 6; pertanto $f(x)$ non può avere radici intere divisibili per 6.
Avremmo anche potuto agire nel modo seguente: supponiamo per assurdo che α sia una radice intera di $f(x)$ divisibile per 6, si ha allora che:

$$[\alpha]_6 = [0]_6 \qquad \wedge \qquad f(\alpha) = 0.$$

Sappiamo dal Teorema cinese del resto che la seguente applicazione è un isomorfismo di anelli:

$$\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3 : [x]_6 \mapsto ([x]_2, [x]_3).$$

Notiamo quindi che:

$$f(\alpha) = 0 \Rightarrow [f(\alpha)]_6 = [0]_6 \Rightarrow \phi([f(\alpha)]_6) = \phi([0]_6) \Rightarrow$$

$$\Rightarrow ([f(\alpha)]_2, [f(\alpha)]_3) = ([0]_2, [0]_3) \Rightarrow [f(\alpha)]_3 = [0]_3.$$

Inoltre dall'altra ipotesi fatta su α, si ricava che:

$$[\alpha]_6 = [0]_6 \Rightarrow \phi([\alpha]_6) = \phi([0]_6) \Rightarrow ([\alpha]_2, [\alpha]_3) = ([0]_2, [0]_3) \Rightarrow [\alpha]_3 = [0]_3$$

Da quanto stabilito sopra, possiamo ora osservare che:

$$[0]_3 = [f(\alpha)]_3 = \overline{f}([\alpha]_3) = \overline{f}([0]_3)$$

ovvero si ha che $[0]_3$ è radice di $\overline{f}(x)$ in $\mathbb{Z}_3$, ma questo è assurdo in quanto nel punto 1. avevamo ricavato che $\overline{f}(x) = (x - [1]_3)(x + [2]_3)^3$.

1.2 Un esempio di come nasce un esercizio

È nostro intento, adesso, dare un esempio di come si possa concepire un esercizio; ossia vogliamo per un momento immedesimarci non nel semplice risolutore, che risponde senza domandarsi, ma bensì in colui che partorisce il quesito, giacché più importanti delle risposte sono senz'altro le domande.
Il punto di partenza è ciò che già ci è noto, e spesso il ricercatore cerca di accoppiare le sue conoscenze per scoprire qualcosa di nuovo. In quest'ottica, cercheremo infatti di fondere alcune delle nostre conoscenze per mettere a punto quello che per alcuni potrà sembrare un esercizio, mentre per altri una vera e propria proposizione (e a dir la verità si fa fatica a comprendere il senso di questa distinzione).
Il risultato principale che siamo intenzionati a utilizzare è un teorema che abbiamo finora tralasciato, ovvero il Criterio di Eisenstein. La prima conclusione cui questo criterio ci conduce è il fatto che, in $\mathbb{Q}[x]$, esistono polinomi irriducibili di qualsiasi grado. Basta infatti considerare:

$$f(x) = x^n + p_1 \qquad (1)$$

con n un qualunque intero positivo e p_1 un qualunque numero primo.
Adesso, sappiamo che se un polinomio in $\mathbb{Z}[x]$ ammette una riduzione modulo p (con p primo) irriducibile in $\mathbb{Z}_p[x]$, allora è esso stesso irriducibile in $\mathbb{Q}[x]$. Il viceversa però non è vero. Quindi, per quel che ne sappiamo, il polinomio definito nella (1) potrebbe benissimo ammettere una riduzione modulo p che sia riducibile. In particolare, dal Teorema di Ruffini sappiamo, in parole povere, che se un polinomio ammette radici e ha grado strettamente maggiore di uno, allora è riducibile. Dunque il polinomio definito dalla (1) potrebbe ammettere una riduzione modulo p che abbia almeno una radice in $\mathbb{Z}_p$.
Detto questo, sarebbe quanto meno curioso se il polinomio $f(x)$, che è irriducibile in $\mathbb{Q}[x]$ (e l'irriducibilità è, intuitivamente, la condizione più distante dall'avere delle radici), ammettesse una riduzione modulo p_2, che denotiamo $\overline{f}(x)$, che abbia il maggior numero possibile di radici in $\mathbb{Z}_{p_2}$, ossia la cui funzione di valutazione sia quanto più vicina possibile alla funzione nulla.
Ci accorgiamo subito che non esiste un primo p_2 tale che $\overline{f}(x)$ abbia funzione di valutazione nulla, ossia tale che $\overline{f}(x)$ abbia in $\mathbb{Z}_{p_2}$ esattamente p_2 radici distinte. Infatti, se ciò fosse vero, allora avremmo che $\overline{f}([0]_{p_2}) = [0]_{p_2}$, ossia che $[p_1]_{p_2} = [0]_{p_2}$, e quindi avremmo che $p_1 = p_2$, e dunque che $\overline{f}(x) = x^n$. Ma allora $\overline{f}([1]_{p_2}) = [1]_{p_2} \neq [0]_{p_2}$, ovvero $[1]_{p_2}$ non è radice di $\overline{f}(x)$, e pertanto $\overline{f}(x)$ non ha esattamente p_2 radici distinte in $\mathbb{Z}_{p_2}$.
Andiamo allora alla ricerca di un primo p_2 tale che $\overline{f}(x)$ abbia in $\mathbb{Z}_{p_2}$ esattamente $p_2 - 1$ radici distinte. In questo caso, le speranze sono notevolmente maggiori. Ora, supponiamo che un tale p_2 esista. Si osserva subito che tra le $p_2 - 1$ radici distinte non può esserci $[0]_{p_2}$, altrimenti avremmo di nuovo che $p_1 = p_2$, e quindi che $\overline{f}(x) = x^n$, ma allora $\overline{f}(x)$ avrebbe una unica radice (sebbene di molteplicità n), che sarebbe appunto $[0]_{p_2}$, e questo risulterebbe assurdo. Di conseguenza, avendo $\overline{f}(x)$ esattamente $p_2 - 1$ radici distinte in $\mathbb{Z}_{p_2}$, e non essendo $[0]_{p_2}$ una radice di $\overline{f}(x)$, allora:

$$\forall \alpha \in \mathbb{Z}_{p_2} - \{[0]_{p_2}\} : \qquad \overline{f}(\alpha) = [0]_{p_2}$$

ovvero si ha che

$$\forall \alpha \in \mathbb{Z}_{p_2} - \{[0]_{p_2}\} : \qquad \alpha^n + [p_1]_{p_2} = [0]_{p_2} \qquad (2)$$

e quindi

$$\forall \alpha \in \mathbb{Z}_{p_2} - \{[0]_{p_2}\} : \qquad \alpha^n = -[p_1]_{p_2}$$

ovvero si deve avere che per ogni $\alpha \in \mathbb{Z}_{p_2}$ non nullo, la quantità α^n deve essere costante. Questo risultato ci ricorda palesemente il Teorema di Eulero, che applicato in $\mathbb{Z}_{p_2}$ ci dice che:

$$\forall \alpha \in \mathbb{Z}_{p_2} - \{[0]_{p_2}\} : \qquad \alpha^{p_2 - 1} = [1]_{p_2}$$

e quindi, se consideriamo $k \in \mathbb{N} - \{0\}$, abbiamo che:

$$\forall \alpha \in \mathbb{Z}_{p_2} - \{[0]_{p_2}\} : \qquad \alpha^{k \cdot (p_2 - 1)} = [1]_{p_2} \qquad (3)$$

per tale ragione, poniamo $n = k \cdot (p_2 - 1)$, e vediamo se questa scelta è compatibile col nostro fine.
Siccome devono valere la (2) e la (3), allora necessariamente:

$$[1 + p_1]_{p_2} = [0]_{p_2}$$

ossia si deve avere che $p_2 \mid (1 + p_1)$. Ebbene, questa condizione si può verificare per infiniti p_2 e p_1 numeri primi. Infatti, mi basta scegliere un qualunque numero primo positivo p_1 (per il Teorema di Euclide ne esistono infiniti), e sfruttando il Teorema fondamentale dell'Aritmetica si ha sicuramente che esiste un numero primo positivo p_2 tale che $p_2 \mid (1+p_1)$. Detto questo, abbiamo che, considerati p_1, p_2 numeri primi positivi tali che $p_2 \mid (1 + p_1)$ (e di tali coppie ne esistono infinite), e dato $k \in \mathbb{N} - \{0\}$, si ha che il polinomio:

$$f(x) := x^{k \cdot (p_2 - 1)} + p_1$$

è irriducibile in $\mathbb{Q}[x]$, mentre la sua riduzione modulo p_2, indicata con $\overline{f}(x)$, ha in $\mathbb{Z}_{p_2}$ esattamente $p_2 - 1$ radici distinte.
In conclusione, abbiamo provato che esistono infinite coppie (n, p) tali che esista un polinomio a coefficienti interi $f(x)$ con $deg(f) = n$, che sia irriducibile in $\mathbb{Q}[x]$, e la cui riduzione modulo p ammetta esattamente $p - 1$ radici distinte in $\mathbb{Z}_p$.
A questo punto, possiamo decidere a nostro piacimento come enunciare l'esercizio (o a seconda dei punti di vista la proposizione). Possiamo decidere di spaventare il risolutore in modi diversi, a seconda di come l'esercizio viene posto:

- Esercizio 1.2.1 (enunciato amichevole): Sia p_1 un primo positivo e sia n un intero positivo. Consideriamo il polinomio:

$$f(x) = x^n + p_1$$

Determinare un intero positivo n e un primo positivo p_2 tali che la riduzione di $f(x)$ modulo p_2 abbia in $\mathbb{Z}_{p_2}$ esattamente $p_2 - 1$ radici distinte.

- Esercizio 1.2.2 (enunciato poco amichevole): Determinare un intero positivo n e un primo positivo p per i quali esista un polinomio a coefficienti interi che sia irriducibile in $\mathbb{Q}[x]$, che abbia grado n, e la cui riduzione modulo p abbia in $\mathbb{Z}_p$ esattamente $p - 1$ radici distinte.

- Esercizio 1.2.3 (enunciato brutale): Provare che esistono infinite coppie (n, p) di interi positivi, con p primo, per le quali esista un polinomio a coefficienti interi che sia irriducibile in $\mathbb{Q}[x]$, che abbia grado n, e la cui riduzione modulo p abbia in $\mathbb{Z}_p$ esattamente $p-1$ radici distinte.

In conclusione si noti che, per partorire quest'esercizio, si è fatto cenno, nell'ordine, ai seguenti risultati teorici:

1. Criterio di Eisenstein;

2. Irriducibilità e riduzione modulo p;
3. Lemma di Gauss;
4. Teorema di Ruffini;
5. Teorema di Eulero;
6. Teorema di Euclide;
7. Teorema fondamentale dell'Aritmetica;

Tutto questo per rimarcare nuovamente che esercizi e proposizioni (o pratica e teoria) sono sostanzialmente la stessa cosa.

1.3 Un esempio di generalizzazione

Stefan Banach, noto matematico polacco vissuto nel secolo scorso, disse una volta una cosa buona e giusta:

"I buoni matematici riescono a vedere le analogie tra le cose. I grandi matematici riescono a vedere le analogie tra le analogie."

Questa opinione è senz'altro degna di essere abbracciata dai più, e sintetizza in sé l'importanza di saper generalizzare (o equivalentemente estendere) un qualcosa che sembra ripetersi uguale in circostanze tuttavia diverse. L'obiettivo che ci prefiggiamo in questa sezione è proprio fornire un esempio di questo genere. Consideriamo gli esercizi seguenti:

- Esercizio 1.3.1: Contare i 4-cicli di S_7.

- Esercizio 1.3.2: Contare gli elementi di S_8 che hanno struttura ciclica (3,2,1,1,1).

- Esercizio 1.3.3: Contare gli elementi di S_9 che hanno struttura ciclica (4,4,1).

- Esercizio 1.3.4: Contare gli elementi di S_{25} che hanno struttura ciclica (6,5,5,4,3,2).

Balza subito agli occhi che questi esercizi, seppur diversi, sono molto simili tra loro. Ad alcuni parrà però che abbiano un grado di difficoltà crescente, ma vedremo che non è così. Cerchiamo ora di cogliere le analogie tra i suddetti esercizi. Ci accorgiamo, in particolare, che tutti loro possono essere enunciati attraverso la seguente domanda:

"In S_n quante permutazioni si contano che abbiano una ben prefissata struttura ciclica?"

Ci proponiamo allora di realizzare un percorso logico mediante il quale dare una risposta. Per rispondere al quesito procederemo per gradi, illustrando alcuni risultati preliminari, il primo dei quali è la:

- Proposizione 1: Sia $n \in \mathbb{N} - \{0\}$, e sia X un insieme avente cardinalità n. Denotato con

$$S(X) := \{\tau : X \to X \mid \sigma \text{ è bigettiva}\}$$

si ha allora che $(S(X), \circ)$ è un gruppo isomorfo a S_n.
Per provare questo risultato, si sfrutta il fatto che esiste $f : \{1, ..., n\} \to X$ applicazione bigettiva, per definire l'applicazione:

$$\phi : S_n \to S(X) : \sigma \mapsto \phi(\sigma) = f \circ \sigma \circ f^{-1}$$

la quale si prova essere un omomorfismo di gruppi invertibile, il cui inverso è l'applicazione:

$$\psi : S(X) \to S_n : \tau \mapsto \psi(\tau) = f^{-1} \circ \tau \circ f$$

Proseguiamo ora fornendo un risultato che ci è già noto e che riguarda gli l-cicli di S_n:

- Proposizione 2: Sia $n \in \mathbb{N} - \{0\}$, e sia $l \in \{2, ..., n\}$. Allora in S_n si contano in totale

$$\frac{1}{l} \cdot \frac{n!}{(n-l)!} \qquad (0)$$

l-cicli.
La dimostrazione formale di questo risultato risulta molto, forse troppo, elaborata. Cerchiamo perciò di fornire un ragionamento euristico che ci conduca alla tesi. Cominciamo col dire che gli l-cicli di S_n possono essere rappresentati in forma di l-uple di elementi di $\{1, ..., n\}$, e queste l-uple devono avere elementi tutti distinti tra loro. Cominciamo quindi a contare tutte le possibili l-uple di elementi di $\{1, ..., n\}$ aventi componenti tutte distinte. Queste sono del tipo:

$$(a_1, ..., a_l)$$

dove:

- a_1 viene scelto arbitrariamente nell'insieme $\{1, ..., n\}$, e quindi si contano n possibili scelte per a_1;
- una volta scelto a_1, la componente a_2 può essere scelta arbitrariamente nell'insieme $\{1, ..., n\} - \{a_1\}$, e quindi, per ogni fissato a_1, si contano $n - 1$ possibili scelte per a_2;
- una volta scelti a_1, a_2, la componente a_3 può essere scelta arbitrariamente nell'insieme $\{1, ..., n\} - \{a_1, a_2\}$, e quindi, per ogni fissati a_1, a_2, si contano $n - 2$ possibili scelte per a_3;
  ...
- una volta scelti $a_1, ..., a_{l-1}$, la componente a_l può essere scelta arbitrariamente nell'insieme $\{1, ..., n\} - \{a_1, ..., a_{l-1}\}$, e quindi, per ogni fissati $a_1, ..., a_{l-1}$, si contano $n - (l - 1)$ possibili scelte per a_l;

Si contano allora $n(n-1)\cdots(n-(l-1)) = \frac{n!}{(n-l)!}$ l-uple di elementi di $\{1, ..., n\}$ aventi componenti tutte distinte.

Adesso occorre effettuare una sorta di operazione di quozientamento. Infatti, dato un l-ciclo di S_n del tipo $(a_1, ..., a_l)$, sappiamo che valgono le seguenti relazioni:

$$(a_1, ..., a_l) = (a_2, ..., a_l, a_1) = (a_3, ..., a_l, a_1, a_2) = \cdots = (a_l, a_1, ..., a_{l-1})$$

ovvero per ogni dato l-ciclo, questo si identifica con altre $(l-1)$ l-uple di elementi di $\{1, ..., n\}$ aventi componenti tutte distinte; cioè col suddetto algoritmo abbiamo finito col contare ogni l-ciclo per l volte; di conseguenza in S_n si contano $\frac{1}{l} \cdot \frac{n!}{(n-l)!}$ l-cicli.
Il passo successivo consta nel determinare il numero di permutazioni di S_n aventi una particolare struttura ciclica, ragion per cui diamo la seguente:

- Proposizione 3: Sia $n \in \mathbb{N} - \{0\}$, e siano $l_1, l_2 \in \{2, ..., n\}$ tali che $l_1 > l_2$, $n \geq l_1 + l_2$. Allora in S_n si contano:

$$\frac{1}{l_1} \cdot \frac{n!}{(n-l_1)!} \cdot \frac{1}{l_2} \cdot \frac{(n-l_1)!}{(n-l_1-l_2)!} = \frac{1}{l_1 l_2} \cdot \frac{n!}{(n-l_1-l_2)!}$$

permutazioni aventi struttura ciclica

$$(l_1, l_2, \underbrace{1, ..., 1}_{(n-l_1-l_2)-volte})$$

Anche in questo caso la dimostrazione formale risulta elaborata, ma possiamo comunque fornire l'intuizione alla base del ragionamento. Si considera la generica permutazione di S_n avente la suddetta struttura. Allora essa potrà rappresentarsi nella forma:

$$(a_1, ..., a_{l_1})(b_1, ..., b_{l_2})$$

dove:

- $(a_1, ..., a_{l_1})$ viene scelto arbitrariamente nell'insieme degli l-cicli di S_n, e quindi per la Proposizione 2 si contano $\frac{1}{l_1} \cdot \frac{n!}{(n-l_1)!}$ possibili scelte per $(a_1, ..., a_{l_1})$;
- una volta scelto $(a_1, ..., a_{l_1})$, il ciclo $(b_1, ..., b_{l_2})$ può essere scelto arbitrariamente tra gli l_2-cicli di $S(\{1, ..., n\} - \{a_1, ..., a_{l_1}\})$, e siccome per la Proposizione 1 si ha che $S(\{1, ..., n\} - \{a_1, ..., a_{l_1}\})$ è isomorfo a S_{n-l_1}, allora $(b_1, ..., b_{l_2})$ può vedersi come un generico l_2-ciclo di S_{n-l_1}, e quindi, sfruttando nuovamente la Proposizione 2 abbiamo che, per ogni fissato $(a_1, ..., a_{l_1})$ si contano $\frac{1}{l_2} \cdot \frac{(n-l_1)!}{(n-l_1-l_2)!}$ possibili scelte per $(a_1, ..., a_{l_1})$;

quindi in totale in S_n abbiamo

$$\frac{1}{l_1} \cdot \frac{n!}{(n-l_1)!} \cdot \frac{1}{l_2} \cdot \frac{(n-l_1)!}{(n-l_1-l_2)!} = \frac{1}{l_1 l_2} \cdot \frac{n!}{(n-l_1-l_2)!}$$

permutazioni aventi struttura ciclica

$$(l_1, l_2, \underbrace{1, ..., 1}_{(n-l_1-l_2)-volte})$$

Cerchiamo ora di generalizzare ulteriormente il risultato precedente dando la seguente:

- Proposizione 4 Sia $n \in \mathbb{N} - \{0\}$, e siano $l_1, ..., l_m \in \{2, ..., n\}$ tali che $l_1 > \cdots > l_m$, $l_1 + \cdots + l_m \leq n$. Allora in S_n si contano

$$\frac{1}{l_1 \cdots l_m} \frac{n!}{(n - (l_1 + \cdots + l_m))!} \qquad (1)$$

permutazioni aventi struttura ciclica

$$(l_1, ..., l_m, \underbrace{1, ..., 1}_{(n-(l_1+\cdots+l_m))-volte})$$

La dimostrazione di questo risultato ricalca quella precedente, ragion per cui viene lasciato al lettore il compito di dedurla.
Osseviamo che, per la validità del suddetto risultato, è di vitale importanza l'ipotesi che sia $l_1 > \cdots > l_m$, ossia che $l_1, ..., l_m$ siano tutti distinti, e il perché lo capiamo con la seguente:

- Proposizione 5: Sia $n \in \mathbb{N} - \{0\}$, e sia $l \in \{2, ..., n\}$. Consideriamo $h \in \mathbb{N} - \{0\}$, e supponiamo che $hl \leq n$. Allora in S_n si contano

$$\frac{1}{h!} \cdot \frac{1}{l^h} \cdot \frac{n!}{(n - hl)!} \qquad (2)$$

permutazioni aventi struttura ciclica

$$(\underbrace{l, ..., l}_{h-volte}, \underbrace{1, ..., 1}_{(n-hl)-volte})$$

Notiamo che la (2) coinciderebbe con la (1) se non fosse presente il fattore $\frac{1}{h!}$. Cerchiamo quindi di giustificare la presenza di questo fattore. La questione è questa: la dimostrazione di quest'ultimo risultato si scinde in due, un po' come quella della Proposizione 2. Nella prima parte si contano tutte le sequenze del tipo:

$$(a_1^1, ..., a_l^1)(a_1^2, ..., a_l^2) \cdots (a_1^l, ..., a_l^l)$$

dove gli l-cicli sono a due a due disgiunti. Si ricavano allora $\frac{1}{l^h} \cdot \frac{n!}{(n-hl)!}$ elementi di questo tipo. Nella seconda parte, ci si rende conto, sfruttando la commutatività dei cicli disgiunti, di aver contato ogni prodotto per $h!$ volte, e che quindi in S_n si contano

$$\frac{1}{h!} \cdot \frac{1}{l^h} \cdot \frac{n!}{(n - hl)!}$$

permutazioni aventi struttura ciclica

$$(\underbrace{l, ..., l}_{h-volte}, \underbrace{1, ..., 1}_{(n-hl)-volte})$$

Sulla base di tutti questi risultati possiamo infine concludere il paragrafo dando la seguente:

- Proposizione 6: Sia $n \in \mathbb{N} - \{0\}$, e siano $l_1, ..., l_m \in \{1, ..., n\}$ ed $h_1, ..., h_m \in \mathbb{N} - \{0\}$. Facciamo le seguenti ipotesi:

1. $l_1 > \cdots > l_m \geq 1$;
2. $h_1 l_1 + \cdots + h_m l_m = n$;

allora in S_n si contano:

$$n! \cdot \left(\prod_{i=1}^{m} \frac{1}{h_i!} \cdot \left(\frac{1}{l_i} \right)^{h_i} \right) \qquad (3)$$

permutazioni aventi struttura ciclica:

$$(\underbrace{l_1, ..., l_1}_{h_1 - volte}, ..., \underbrace{l_m, ..., l_m}_{h_m - volte})$$

Per provarlo, si consiglia di far leva sui metodi di ragionamento impiegati in precedenza, e anzi si intravede proprio qui la possibilità di mettere in pratica gli insegnamenti dati, in modo tale da farli propri. Si consiglia poi di verificare che la (3) risulta effettivamente essere una generalizzazione della (0), cioè di far vedere che quando $(h_1, m, l_m) = (1, 2, 1)$ otteniamo che la (3) e la (0) coincidono.
A conclusione del nostro ragionamento, si invita il lettore a osservare che, in virtù di quanto detto, gli esercizi all'inizio di questa sezione non solo sembrano uguali, ma hanno perfino lo stesso grado di difficoltà, e per risolverli risulta ora sufficiente applicare la formula (3).

1.4 Un altro esempio di generalizzazione

Come nella precedente sezione, vogliamo adesso fornire un ulteriore esempio di generalizzazione. Stavolta consideriamo i seguenti esercizi:

- Esercizio 1.4.1: Contare in S_4 le permutazioni che lasciano fisso 1.

- Esercizio 1.4.2: Contare in S_7 le permutazioni che mandano 1 in 5.

- Esercizio 1.4.3: Contare in S_{32} le permutazioni i cui quadrati mandano 1 in 24.

Anche in tal caso si notano delle analogie. Infatti tali esercizi possono essere messi in questa forma:

"Quante sono le permutazioni di S_n che mandano un elemento in un altro?"

Cerchiamo però di formalizzare in modo opportuno la nostra richiesta, e la relativa risposta, nella seguente:

- Proposizione 7: Sia $n \in \mathbb{N} - \{0\}$, e siano $a, b \in \{1, ..., n\}$, $k \in \mathbb{N} - \{0\}$. Supponiamo che $a \neq b$. Allora in S_n si contano $(n-d) \cdot (n-2)!$ permutazioni σ tali che $\sigma^k(a) = b$, dove d è la cardinalità dell'insieme:

$$Div_+(k) := \{h \in \mathbb{N} \mid h \mid k\}$$

Anche in tal caso cerchiamo di capire come giungere alla tesi sintetizzando quelle che sono le idee alla base della dimostrazione. Anzitutto si considera la generica permutazione $\sigma \in S_n$ tale che $\sigma^k(a) = b$. Si considera quindi la decomposizione in cicli disgiunti di σ, che sarà del tipo:

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$$

Non si lede la generalità se si suppone che γ_1 sia il ciclo associato all'orbita di a, e quindi anche all'orbita di b. Si pone poi $\sigma_1 := \gamma_2 \circ \cdots \circ \gamma_s$, in modo che sia $\sigma = \gamma_1 \circ \sigma_1$. Sia quindi l la lunghezza del ciclo γ_1. Di conseguenza γ_1 potrà rappresentarsi nel modo seguente:

$$\gamma_1 = (a_1, ..., a_l)$$

dove $(a_1, ..., a_l)$ è una l-upla di elementi tutti distinti di $\{1, ..., n\}$ che contiene sia a che b. Fissiamo la scrittura del ciclo γ_1, stabilendo, ad esempio, che l'elemento a compaia in prima posizione, ossia $a = a_1$. Osserviamo che, una volta fissata la posizione di a, il valore di k determina univocamente la posizione di b nella scrittura di γ_1. Detto questo, indichiamo con

$$\tau_1 = (b_1, ..., b_{l-2})$$

la $(l-2)$-upla ottenuta da γ_1 eliminando da essa a e b. Facciamo le seguenti considerazioni:

1. notiamo che $l \in \{1, ..., n\} - Div_+(k)$, infatti se per assurdo fosse $l \in Div_+(k)$, allora si otterrebbe che $\sigma^k(a) = a$, e che quindi $a = b$, in contraddizione con l'ipotesi. Viceversa, se l non è un divisore di k, allora si può provare che esiste un ciclo γ_1 con la proprietà richiesta. Quindi possiamo scegliere l in $(n-d)$ modi distinti;

2. dopo aver fissato l, abbiamo che γ_1 risulta automaticamente determinato una volta che è noto τ_1, e quest'ultima è una generica $(l-2)$-upla di elementi tutti distinti di $\{1, ..., n\} - \{a, b\}$, e rifacendoci alla dimostrazione della Proposizione 2, possiamo dire che le $(l-2)$-uple di elementi tutti distinti di $\{1, ..., n\} - \{a, b\}$ sono in totale $\frac{(n-2)!}{(n-2-(l-2))!} = \frac{(n-2)!}{(n-l)!}$, e quindi per ogni fissato l, posso selezionare γ_1 in $\frac{(n-2)!}{(n-l)!}$ modi distinti;

3. una volta fissati l e γ_1, abbiamo che σ_1 è una generica permutazione di $S(\{1, ..., n\} - \{a_1, ..., a_l\})$, e quindi può essere scelta in $(n-l)!$ modi distinti;

Da quanto detto sopra, ricaviamo infine che in S_n si contano $(n-d) \cdot \frac{(n-2)!}{(n-l)!} \cdot (n-l)! = (n-d) \cdot (n-2)!$ permutazioni σ tali che $\sigma^k(a) = b$. Notiamo come il risultato ottenuto sia indipendente dalla lunghezza l del ciclo γ_1.

Giunti qui, diamo un'altra celebre citazione, a opera di un altro celebre matematico, di

nome Paul Erdös:

"Togliere le ipotesi a un teorema è un esercizio che aiuta il matematico a mantenersi giovane"

Ora, siccome vogliamo indubbiamente restare giovani, possiamo sfruttare questo elisir di lunga vita chiedendoci cosa accade togliendo alla Proposizione 7 l'ipotesi secondo cui $a \neq b$, ragion per cui diamo la seguente:

- Proposizione 8: Sia $n \in \mathbb{N} - \{0\}$, e siano $a \in \{1, ..., n\}$, $k \in \mathbb{N} - \{0\}$. Allora in S_n si contano $d \cdot (n-1)!$ permutazioni σ tali che $\sigma^k(a) = a$, dove d è la cardinalità dell'insieme:

$$Div_+(k) := \{h \in \mathbb{N} \mid h \mid k\}$$

Per provare la tesi cominciamo col decomporre in cicli disgiunti la generica $\sigma \in S_n$ tale che $\sigma^k(a) = a$. Come prima si ha:

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$$

Non si lede la generalità se si suppone che γ_1 sia il ciclo associato all'orbita di a. Si pone poi $\sigma_1 := \gamma_2 \circ \cdots \circ \gamma_s$, in modo che sia $\sigma = \gamma_1 \circ \sigma_1$. Sia quindi l la lunghezza del ciclo γ_1. È semplice verificare che:

$$\sigma^k(a) = a \iff l \in Div_+(k)$$

Inoltre appare evidente che γ_1 potrà rappresentarsi nella forma: $\gamma_1 = (a_1, ..., a_l)$ e possiamo supporre $a_1 = a$. In virtù di quanto detto, si osserva quanto segue:

1. notiamo che $l \in Div_+(k)$, quindi possiamo scegliere l in d modi distinti;

2. dopo aver fissato l, abbiamo che γ_1 risulta automaticamente determinato una volta che è noto $(a_2, ..., a_l)$, e quest'ultima è una generica $(l-1)$-upla di elementi tutti distinti di $\{1, ..., n\} - \{a\}$, e rifacendoci alla dimostrazione della Proposizione 2, possiamo dire che le $(l-1)$-uple di elementi tutti distinti di $\{1, ..., n\} - \{a\}$ sono in totale $\frac{(n-1)!}{(n-1-(l-1))!} = \frac{(n-1)!}{(n-l)!}$, e quindi per ogni fissato l, posso selezionare γ_1 in $\frac{(n-1)!}{(n-l)!}$ modi distinti;

3. una volta fissati l e γ_1, abbiamo che σ_1 è una generica permutazione di $S(\{1, ..., n\} - \{a_1, ..., a_l\})$, e quindi può essere scelta in $(n-l)!$ modi distinti;

Da quanto detto sopra, ricaviamo infine che in S_n si contano $d \cdot \frac{(n-1)!}{(n-l)!} \cdot (n-l)! = d \cdot (n-1)!$ permutazioni σ tali che $\sigma^k(a) = a$.

In conclusione, si osserva come anche stavolta gli esercizi all'inizio della sezione non solo sono simili, ma hanno pure lo stesso grado di difficoltà, e per risolverli risulta sufficiente applicare le precedenti proposizioni.
Si nota pure come, in queste ultime due sezioni, si sono ottenuti dei teoremi a partire da alcuni esercizi simili tra loro, mentre tre sezioni fa avevamo dedotto un esercizio a partire da alcuni teoremi. Stiamo dicendo tutto ciò per sottolineare ancora una volta questo strano

intreccio tra teoria e pratica, che oramai dovrebbe essere così fitto da rendere indistinguibili le due cose.

1.5 Applicazione delle precedenti generalizzazioni

Cerchiamo ora di finalizzare i nostri precedenti sforzi fornendo alcuni esercizi in cui applicare i risultati di cui alle precedenti due sezioni, ovviamente coadiuvati da opportuni teoremi a noi già noti.

- Esercizio 1.5.1: Sia n un intero maggiore di 1, e sia H l'insieme delle permutazioni di S_n che non lasciano fisso l'elemento 1.

1. Determinare la cardinalità di H.
2. Provare che H non è contenuto in nessun sottogruppo proprio di S_n.
3. Per $n = 6$, determinare la cardinalità dell'insieme delle permutazioni dispari appartenenti ad H.

Svolgimento

1. Cominciamo con l'osservare che

$$H = \{\sigma \in S_n \mid \sigma(1) \neq 1\} \qquad \complement_{S_n}(H) = \{\sigma \in S_n \mid \sigma(1) = 1\}$$

e risultano ovvie le relazioni seguenti:

$$S_n = H \cup \complement_{S_n}(H) \qquad \emptyset = H \cap \complement_{S_n}(H)$$

ragion per cui si ottiene che $|S_n| = |H| + \left|\complement_{S_n}(H)\right|$ e quindi in particolare si ha che:

$$|H| = |S_n| - \left|\complement_{S_n}(H)\right|$$

Detto questo, è noto dalla teoria che $|S_n| = n!$, e quindi non ci resta che determinare la cardinalità di $\complement_{S_n}(H)$ per dedurre quella di H. Per farlo possiamo usufruire della Proposizione 8, oppure possiamo ragionare come di seguito riportato. Consideriamo $\sigma \in \complement_{S_n}(H)$, allora $\sigma(1) = 1$, e pertanto σ avrà la seguente rappresentazione matriciale:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 1 & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix}$$

dove $\begin{pmatrix} 2 & 3 & ... & n \\ \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix} \in S(\{2, ..., n\})$, essendo $S(\{2, ..., n\})$ l'insieme delle bigezioni da $\{2, ..., n\}$ a $\{2, ..., n\}$, il quale risulta bigettivo a S_{n-1}. Tenuto conto di questo, risulta semplice verificare che la seguente applicazione è bigettiva:

$$\psi : \complement_{S_n}(H) \to S(\{2, ..., n\}) : \sigma \mapsto \psi(\sigma) = \begin{pmatrix} 2 & 3 & ... & n \\ \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix}$$

e che quindi $\left|\complement_{S_n}(H)\right| = |S(\{2,...,n\})| = |S_{n-1}| = (n-1)!$
Possiamo adesso affermare che:

$$|H| = |S_n| - \left|\complement_{S_n}(H)\right| = n! - (n-1)! = (n-1)! \cdot n - (n-1)! = (n-1)! \cdot (n-1)$$

2. Sia G un sottogruppo di S_n contenente H. Ovviamente $G \subset S_n$, e quindi se proviamo che $S_n \subset G$, avremo provato che $G = S_n$, ovvero che G non è sottogruppo proprio di S_n. Consideriamo quindi $\sigma \in S_n$. Si distinguono due casi:

   (a) $\sigma \in H$, allora siccome $H \subset G$, ne deduciamo che $\sigma \in G$;

   (b) $\sigma \notin H$, allora $\sigma(1) = 1$. Osserviamo quindi quanto segue:

   $$\sigma = \sigma \cdot id = \sigma \cdot ((1,2) \cdot (2,1)) = (\sigma \cdot (1,2)) \cdot (2,1) = \sigma_1 \cdot \sigma_2$$

   dove $\sigma_1 = \sigma \cdot (1,2)$, mentre $\sigma_2 = (2,1)$.Si nota che:

   $$\sigma_1(1) = \sigma(2) \neq \sigma(1) = 1 \qquad \sigma_2(1) = 2 \neq 1$$

   ossia $\sigma_1, \sigma_2 \in H$, ed essendo $H \subset G$, allora $\sigma_1, \sigma_2 \in G$, e siccome G è un sottogruppo di S_n, allora $\sigma_1 \cdot \sigma_2 \in G$, ovvero $\sigma \in G$;

   data l'arbitrarietà impiegata, ne segue che $S_n \subset G$, e dunque $G = S_n$.

3. Sia σ una permutazione dispari di S_6. Allora σ avrà una e una sola delle seguenti strutture cicliche:

   $$(6), (4,1,1), (3,2,1), (2,1,1,1,1), (2,2,2)$$

   ragion per cui distinguiamo i casi seguenti:

   (a) σ ha struttura (6). Allora è ovvio che σ non lascia fisso 1, cioè che $\sigma \in H$. Dunque in H vi sono tutte le permutazioni di S_6 con struttura (6), ossia tutti i 6-cicli di S_6, e in S_6 ci sono $\frac{1}{6} \cdot \frac{6!}{(6-6)!} = 5! = 120$ 6-cicli;

   (b) σ ha struttura $(4,1,1)$, ossia σ è un 4-ciclo di S_6. In S_6 si contano $\frac{1}{4} \cdot \frac{6!}{(6-4)!}$ 4-cicli, ma quanti di questi lasciano fisso 1? I 4-cicli che lasciano fisso 1 sono del tipo:

   $$(1)(a_1)(a_2,...,a_5)$$

   dove $a_1 \in \{1,...,6\} - \{1\}$, mentre $(a_2,...,a_5) \in S(\{1,...,6\} - \{1,a_1\}) \simeq S_4$, cioè posso vedere $(a_2,...,a_5)$ come un generico 4-ciclo di S_4; quindi posso scegliere a_1 in 5 modi distinti, e per ciascuna di queste scelte posso selezionare $(a_2,...,a_5)$ in $\frac{1}{4} \cdot \frac{4!}{(4-4)!} = 3!$ modi diversi. Dunque si hanno $5 \cdot (3!)$ 4-cicli di S_6 che lasciano fisso 1. Quindi i 4-cicli di S_6 che non lasciano fisso 1 (e che quindi appartengono ad H) sono $\frac{1}{4} \cdot \frac{6!}{(6-4)!} - 5 \cdot (3!) = 60$;

   (c) σ ha struttura (3,2,1). Da una nota formula, sappiamo che in S_6 si contano $6! \cdot \frac{1}{3} \cdot \frac{1}{2} = 120$ permutazioni aventi struttura (3,2,1), ma quante di queste lasciano

fisso 1? Le permutazioni aventi struttura ciclica (3,2,1) che fissano 1 sono del tipo:

$$(1)(a_1, a_2)(a_3, a_4, a_5)$$

dove $(a_1, a_2) \in S(\{1, ..., 6\} - \{1\}) \simeq S_5$, cioè posso vedere (a_1, a_2) come un generico 2-ciclo di S_5; d'altra parte si nota subito che il ciclo (a_3, a_4, a_5) appartiene a $S(\{1, ..., 6\} - \{1, a_1, a_2\}) \simeq S_3$, ossia posso vedere (a_3, a_4, a_5) come un 3-ciclo di S_3; quindi posso scegliere (a_1, a_2) in $\frac{1}{2} \cdot \frac{5!}{(5-2)!}$ distinti, e per ciascuna di queste scelte posso selezionare (a_3, a_4, a_5) in $\frac{1}{3} \cdot \frac{3!}{(3-3)!}$. Di conseguenza si contano in totale $\frac{1}{2} \cdot \frac{5!}{(5-2)!} \cdot \frac{1}{3} \cdot \frac{3!}{(3-3)!} = 20$ permutazioni di S_6 aventi struttura ciclica (3,2,1) e che lasciano fisso 1. Dunque sono $120 - 20 = 100$ le permutazioni di S_6 che non lasciano fisso 1, e che pertanto appartengono ad H;

(d) σ ha struttura (2,1,1,1,1), e se si suppone che σ non fissi 1, cioè che σ appartenga ad H, si ricava che σ si decompone in cicli disgiunti nel modo seguente:

$$(1, a_1)$$

dove $a_1 \in \{1, ..., 6\} - \{1\}$, e quindi si contano, in H, 5 permutazioni aventi struttura (2,1,1,1,1);

(e) σ ha struttura (2,2,2). Allora è semplice verificare che σ non fissa 1. Da una nota formula, sappiamo che ci sono $6! \cdot \frac{1}{3!} \cdot \frac{1}{2^3} = 15$ permutazioni di S_6 che hanno struttura ciclica (2,2,2);

Da quanto visto sopra, deduciamo che la cardinalità dell'insieme delle permutazioni dispari appartenenti ad H è

$$120 + 60 + 100 + 5 + 15 = 300$$

e abbiamo quindi risolto il problema.

- Esercizio 1.5.2:

1. Determinare il numero delle permutazioni $\sigma \in S_5$ tali che $\sigma^4(1) = 2$.
2. Dimostrare che, per ogni intero n non divisibile per 5, esiste un 5-ciclo $\sigma \in S_5$ tale che $\sigma^n(1) = 2$.

Svolgimento

1. Sfruttando la Proposizione 7 si deduce subito che in S_5 si contano

$$(5 - |Div_+(4)|) \cdot (5 - 2)! = (5 - 3) \cdot 3! = 12$$

permutazioni σ tali che $\sigma^4(1) = 2$;

2. È semplice provare la tesi per $n \in \{1, ..., 4\}$. Sia ora $n \in \mathbb{Z}$ non divisibile per 5. Allora, per il lemma di divisione Euclidea:

$$\exists | q, r \in \mathbb{Z} \text{ tali che } n = 5q + r \text{ e } 0 \leq r < 5$$

e siccome n non è divisibile per 5, allora $r \in \{1, ..., 4\}$, e quindi per quanto detto in precedenza

$$\exists \sigma \in S_5 \text{ tale che } \sigma \text{ sia un 5-ciclo e } \sigma^r(1) = 2$$

poiché σ è un 5-ciclo, allora $\circ(\sigma) = 5$, pertanto:

$$\sigma^n(1) = \sigma^{5q+r} = \sigma^{5q}(\sigma^r(1)) = \sigma^{\circ(\sigma)q}(\sigma^r(1)) = \sigma^r(1) = 2$$

e quindi la tesi è vera per ogni intero n non divisibile per 5.

- Esercizio 1.5.3: Si consideri la seguente permutazione di S_{16}:

$$\alpha = (1, 7, 2, 13)(3, 14, 6, 10, 4)(8, 12)(5, 11)(9, 16, 15)$$

1. Determinare tutti gli elementi dell'insieme:

$$H = \{\sigma \in \langle \alpha \rangle \mid \sigma^2(1) = 2 \text{ e } \sigma^3(3) = 4\}.$$

2. Determinare un sottogruppo K di $\langle \alpha \rangle$ avente ordine 3 e provare che ogni sottogruppo di S_{16} contenente $H \cup K$ contiene anche $\langle \alpha \rangle$.

Questo esercizio costituisce una interessante variante del problema associato alla domanda: "quante permutazioni di S_n mandano un elemento in un altro?".

Svolgimento

1. Osserviamo quanto segue:

$$\begin{aligned} H &= \{\sigma \in \langle \alpha \rangle \mid \sigma^2(1) = 2, \quad \sigma^3(3) = 4\} \\ &= \{\alpha^k \mid k \in \mathbb{Z}, \quad \alpha^{2k}(1) = 2, \quad \alpha^{3k}(3) = 4\} \end{aligned}$$

tenuto conto che $o(\alpha) = 60$ e che:

$$\begin{aligned} &min\{s \in \mathbb{N} \mid \alpha^s(1) = 2\} = 2 \qquad min\{s \in \mathbb{N}^* \mid \alpha^s(2) = 2\} = 4 \\ &min\{s \in \mathbb{N} \mid \alpha^s(3) = 4\} = 4 \qquad min\{s \in \mathbb{N}^* \mid \alpha^s(4) = 4\} = 5 \end{aligned}$$

possiamo allora dire che:

$$\begin{aligned} H &= \{\alpha^k \mid 0 \leq k \leq 59, \quad 2k \equiv 2 \ mod \ 4, \quad 3k \equiv 4 \ mod \ 5\} \\ &= \{\alpha^k \mid 0 \leq k \leq 59, \quad k \equiv 1 \ mod \ 2, \quad k \equiv 3 \ mod \ 5\} \end{aligned}$$

sfruttando infine il Teorema cinese del resto, si ottiene:

$$\begin{aligned} H &= \{\alpha^k \mid 0 \leq k \leq 59, \quad k \equiv 3 \ mod \ 10\} \\ &= \{\alpha^k \mid 0 \leq k \leq 59, \quad \exists h \in \mathbb{Z} : \ k - 3 = 10h\} \\ &= \{\alpha^k \mid k \in \{3, 13, 23, 33, 43, 53\}\} \end{aligned}$$

2. Siccome i sottogruppi di un gruppo ciclico sono ciclici, allora neccessariamente K è ciclico, e poiché è contenuto in $\langle\alpha\rangle$, allora esso sarà generato da una potenza di α, cioè:

$$\exists k \in \{0, 1, ..., 59\} \text{ tale che } K = \langle\alpha^k\rangle$$

Dove si è tenuto conto che $o(\alpha) = 60$. Ora, giacché K ha ordine 3, allora deve essere $o(\alpha^k) = 3$. Notiamo che α ha struttura ciclica (5,4,3,2,2), di conseguenza si ha una unica orbita avente cardinalità un multiplo di 3, e siccome questa orbita è associata a un 3-ciclo, allora necessariamente α^k è un 3-ciclo. Per ottenere una potenza di α che sia un 3-ciclo, occorre eliminare le orbite che hanno cardinalità diversa da 3. Il modo più naturale per farlo è considerare, nel nostro caso, un multiplo di (5,4,2,2) che non sia un multiplo di 3 (altrimenti elimineremmo anche l'orbita 3-ciclica). Abbiamo quindi il sistema seguente:

$$\begin{cases} k \equiv 0 & mod\ 4 \\ k \equiv 0 & mod\ 5 \\ k \not\equiv 0 & mod\ 3 \\ k \in \{0, 1, ..., 59\} \end{cases}$$

il cui insieme delle soluzioni è $\{20, 40\}$. Notiamo adesso che $\langle\alpha^{20}\rangle = \langle\alpha^{40}\rangle$, ragion per cui vi è un unico sottogruppo di $\langle\alpha\rangle$ avente ordine 3, che sarebbe il sottostante:

$$K = \langle\alpha^{20}\rangle = \langle\alpha^{40}\rangle = \{id, \alpha^{20}, \alpha^{40}\}$$

Consideriamo ora G un sottogruppo di S_{16} contenente $H \cup K$. Per provare che G contiene $\langle\alpha\rangle$ è sufficiente far vedere che $\alpha \in G$. A tal proposito, facendo leva sul teorema di Lagrange, notiamo quanto segue:

$$\alpha = \alpha^{61} = \alpha^{40+21} = \alpha^{40+3\cdot 7} = \alpha^{40}(\alpha^3)^7$$

dove $\alpha^{40} \in K \subset G$, e $\alpha^3 \in H \subset G$; quindi, essendo G un gruppo, dall'equazione precedente ricaviamo subito che $\alpha \in G$.

1.6 Il problema della buona positura

Ricorre spesso in ambito matematico chiedersi se una data relazione tra strutture sia effettivamente una funzione, in tal caso si parla di verificare che la funzione sia ben posta. Restringendoci al nostro campo, cerchiamo di suggerire un possibile metodo per determinare quando una funzione è ben posta. Cerchiamo in un certo qual modo di generalizzare il nostro ragionamento, ragion per cui consideriamo B_1, B_2 strutture algebriche dello stesso tipo (cioè entrambi gruppi, o entrambi anelli, o entrambi campi), e sia poi $\{\phi_a\}_{a\in S}$ una generica famiglia di relazioni tra B_1 e B_2. Si sottolinea il fatto che, per il momento, per ogni $a \in S$ risulta che ϕ_a è una relazione tra B_1 e B_2, il che significa formalmente che ϕ_a è

un sottoinsieme di $B_1 \times B_2$; ciononostante, adoperando un abuso di notazione, si indicherà ϕ_a come solitamente si indicano le funzioni tra B_1 e B_2, cioè $\phi_a : B_1 \to B_2$, anche se a priori non sappiamo se si tratta o meno di una funzione. Il nostro obiettivo è quello di capire per quali a in S risulta in effetti che ϕ_a sia una funzione ben posta. Una buona idea risolutiva potrebbe essere quella di intraprendere il seguente percorso logico:

1. anzitutto dichiariamo l'insieme degli $a \in S$ tali che ϕ_a è una funzione:

$$S_0 := \{a \in S \mid \phi_a \text{ è una funzione ben posta}\};$$

2. dopodiché fissiamo un elemento $a_1 \in S_0$, e sfruttando la buona positura di ϕ_{a_1}, andiamo alla ricerca di una condizione che necessariamente dev'essere soddisfatta da a_1, ossia di un predicato p che deve essere verificato da a_1, cioè $p(a_1)$;

3. definiamo l'insieme degli $a \in S$ tali che a verifica il predicato (o equivalentemente la proprietà) p:

$$S_1 := \{a \in S \mid p(a)\};$$

4. tenuto conto della generalità del ragionamento di cui al punto 2., possiamo subito dire che $S_0 \subset S_1$, che tradotto vuol dire che $p(a)$ è una condizione necessaria affinché ϕ_a sia una funzione ben posta;

5. terminiamo poi il nostro ragionamento facendo vedere che $p(a)$, oltre a essere condizione necessaria, è pure condizione sufficiente affinché ϕ_a sia una funzione ben posta. In termini insiemistici, ciò significa provare che $S_1 \subset S_0$;

Riassumendo, si ha che $S_0 = S_1$, ovvero abbiamo caratterizzato la buona positura mediante la seguente:
- *Proposizione*: sia $a \in S$. Allora:

$$\phi_a \text{ è una funzione ben posta } \iff p(a)$$

Ovviamente il passo successivo è chiedersi come determinare il predicato p, la qual cosa varia da caso a caso, e quindi non è possibile effettuare una ulteriore generalizzazione che ci indichi una sola strada per ricavare p.

Cerchiamo ora di mettere in pratica il suddetto ragionamento proponendo alcuni esercizi che chiariranno meglio quanto è stato detto.

- Esercizio 1.6.1: Sia n un intero maggiore di 1 e sia x un intero tale che $1 \leq x \leq 11$. Si consideri l'applicazione:

$$\phi : \mathbb{Z}_n \to U(\mathbb{Z}_{12})$$

tale che, per ogni intero $a \geq 0$:

$$\phi([a]_n) = ([x]_{12})^a$$

1. Determinare tutte le coppie (n, x) per le quali ϕ è un omomorfismo di gruppi ben definito.

2. Determinare tutte le coppie (n, x) per le quali ϕ è un monomorfismo di gruppi.

Svolgimento

1. Consideriamo l'insieme seguente:

   $$S_0 := \{(n, x) \in \mathbb{N} \times \{1, ..., 11\} \mid n \geq 2 \text{ e } \phi \text{ è un omomorfismo di gruppi ben posto}\}$$

   Fissiamo $(n, x) \in S_0$. Per prima cosa, notiamo che:

   $$\phi([1]_n) = ([x]_{12})^1 = [x]_{12} \in U(\mathbb{Z}_{12})$$

   quindi essendo $1 \leq x \leq 11$, e $U(\mathbb{Z}_{12}) = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$, se ne deduce che $x \in \{1, 5, 7, 11\}$.
   Consideriamo ora $a, b \geq 0$, e supponiamo $[a]_n = [b]_n \wedge a \geq b$. Osserviamo quindi quanto segue:

   $$(n, x) \in S_0 \Rightarrow \phi([a]_n) = \phi([b]_n) \Rightarrow ([x]_{12})^a = ([x]_{12})^b \Rightarrow ([x]_{12})^{a-b} = [1]_{12}$$

   pertanto $o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid (a - b)$; tenuto conto che $[a]_n = [b]_n$, cioè che $n \mid (a - b)$, ne deduciamo che:

   $$\exists h \in \mathbb{Z} : a - b = nh$$

   Data l'arbitrarietà di $h \in \mathbb{Z}$, scelto $h = 1$, si ha $a - b = n$, e dunque $o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid n$. Detto ciò, definiamo:

   $$S_1 := \{(n, x) \in \mathbb{N} \times \{1, ..., 11\} \mid n \geq 2, x \in \{1, 5, 7, 11\} \quad \wedge \quad o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid n\}$$

   Tenuto conto che:

   $$o_{U(\mathbb{Z}_{12})}([5]_{12}) = o_{U(\mathbb{Z}_{12})}([7]_{12}) = o_{U(\mathbb{Z}_{12})}([11]_{12}) = 2$$

   Possiamo allora esplicitare l'insieme S_1 come segue:

   $$S_1 := \{(n, 1) \in \mathbb{N} \times \{1\} \mid n \geq 2\} \cup \{(2 \cdot k, x) \in \mathbb{N} \times \{5, 7, 11\} \mid k \in \mathbb{N} - \{0\}\}$$

   Abbiamo appena provato che $S_0 \subset S_1$. Facciamo ora vedere che $S_1 \subset S_0$, ragion per cui fissiamo $(n, x) \in S_1$.
   Siccome $x \in \{1, 5, 7, 11\}$, allora $[x]_{12} \in U(\mathbb{Z}_{12})$, e quindi:

   $$\forall m \in \mathbb{N} : ([x]_{12})^m \in U(\mathbb{Z}_{12})$$

Siano ora $a, b \geq 0$, e supponiamo $[a]_n = [b]_n \wedge a \geq b$. Allora:

$$\exists h \in \mathbb{Z} : a - b = nh$$

Siccome $o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid n$, allora $o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid nh$, cioè $o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid (a-b)$, di conseguenza si ha $([x]_{12})^{a-b} = [1]_{12}$, ossia $([x]_{12})^a = ([x]_{12})^b$, e dunque ϕ è ben definito.
Siano ora $a, b \geq 0$ generici. Allora:

$$\phi([a]_n + [b]_n) = \phi([a+b]_n) = ([x]_{12})^{a+b} = ([x]_{12})^a([x]_{12})^b = \phi([a]_n)\phi([b]_n)$$

pertanto ϕ è un omomorfismo di gruppi, dunque $(n, x) \in S_0$.
Data l'arbitrarietà impiegata, segue che $S_1 \subset S_0$ e perciò, mettendo assieme le informazioni già note, si ha: $S_0 = S_1$.

2. Consideriamo l'insieme seguente:

$$S_2 := \{(n, x) \in S_1 \mid Ker\phi = \{[0]_n\}\}$$

Fissiamo $(n, x) \in S_2$. Notiamo che $Ker\phi = \{[0]_n\}$, e inoltre:

$$\begin{aligned} Ker\phi &= \{[a]_n \in \mathbb{Z}_n \mid a \geq 0 \quad \wedge \quad ([x]_{12})^a = [1]_{12}\} \\ &= \{[a]_n \in \mathbb{Z}_n \mid a \in \{0, ..., n-1\} \quad \wedge \quad o_{U(\mathbb{Z}_{12})}([x]_{12}) \mid a\} \end{aligned}$$

Ora, sappiamo che $x \in \{1, 5, 7, 11\}$, e siccome

$$o_{U(\mathbb{Z}_{12})}([1]_{12}) = 1,\ o_{U(\mathbb{Z}_{12})}([5]_{12}) = o_{U(\mathbb{Z}_{12})}([7]_{12}) = o_{U(\mathbb{Z}_{12})}([11]_{12}) = 2$$

allora $o_{U(\mathbb{Z}_{12})}([x]_{12}) \in \{1, 2\}$. Proviamo che $o_{U(\mathbb{Z}_{12})}([x]_{12}) = 2$. Se per assurdo fosse $o_{U(\mathbb{Z}_{12})}([x]_{12}) = 1$, allora avremmo $[x]_{12} = [1]_{12}$, e di conseguenza risulterebbe che $Ker\phi = \mathbb{Z}_n$, ma ciò sarebbe assurdo. Di conseguenza $o_{U(\mathbb{Z}_{12})}([x]_{12}) = 2$.
Proviamo ora che $n = 2$. Se fosse $n \neq 2$, allora avremmo $n > 2$, e si nota subito che in tal caso $[2]_n \in Ker\phi$ e $[2]_n \neq [0]_n$, ma ciò risulterebbe assurdo. Di conseguenza $n = 2$.
Detto ciò, definiamo:

$$S_3 := \{(n, x) \in S_1 \mid n = 2 \quad \wedge \quad o_{U(\mathbb{Z}_{12})}([x]_{12}) = 2\}$$

Abbiamo appena provato che $S_2 \subset S_3$. Vogliamo ora provare che $S_3 \subset S_2$, la qual cosa è immediata da verificare una volta notato che:

$$S_3 = \{(2, x) \mid x \in \{5, 7, 11\}\}$$

e da qui è semplice ricondurci alla soluzione.

- Esercizio 1.6.2: Sia $f(x) \in \mathbb{Z}_7[x]$ un polinomio non costante. Si consideri l'applicazione

$$\phi : \mathbb{Z}_7[x]_{/(f(x))} \to \mathbb{Z}_{56}$$

definita nel modo seguente: per ogni polinomio $a[x] \in \mathbb{Z}_7[x]$, tale che

$$a(x) = \sum_{i=0}^{n} [a_i]_7 x^i \qquad \text{(con } n \in \mathbb{N}\text{, ed } a_i \in \mathbb{Z}\text{, per ogni } i\text{)},$$

si pone $\phi([a(x)]_f) = [8a_0]_{56}$.

1. Determinare l'insieme dei polinomi $f(x) \in \mathbb{Z}_7[x]$ per i quali ϕ è un omomorfismo ben definito.
2. Determinare l'insieme dei polinomi $f(x) \in \mathbb{Z}_7[x]$ per i quali ϕ è un monomorfismo di anelli, precisandone la cardinalità.
3. Nel caso in cui $f(x) = x^3 + x^2 + x$, determinare il nucleo di ϕ, precisandone la cardinalità.

Svolgimento

1. Cominciamo definendo

   $$S := \{f(x) \in \mathbb{Z}_7[x] \mid \phi \text{ è un omomorfismo di anelli ben posto}\}$$

   e consideriamo $f(x) \in S$. Siano quindi $a(x), b(x) \in \mathbb{Z}_7[x]$ tali che $[a(x)]_f = [b(x)]_f$. Possiamo supporre:

   $$a(x) = \sum_{i=0}^{m} [a_i]_7 x^i \qquad b(x) = \sum_{i=0}^{n} [b_i]_7 x^i$$

   Siccome $f(x) \in S$, allora $\phi([a(x)]_f) = \phi([b(x)]_f)$, ovvero risulta che $[8a_0]_{56} = [8b_0]_{56}$, cioè $56 \mid 8(a_0 - b_0)$, e quindi $7 \mid (a_0 - b_0)$. Ora, siccome $[a(x)]_f = [b(x)]_f$, allora:

   $$\exists q(x) \in \mathbb{Z}_7[x] \text{ tale che } a(x) - b(x) = f(x)q(x)$$

   Adesso, data l'arbitrarietà di $a(x), b(x)$ e quindi di $q(x)$, possiamo supporre:

   $$a(x), b(x) \in \mathbb{Z}_7[x] \text{ tali che } a(x) - b(x) = f(x) \qquad (\text{ossia } q(x) = [1]_7)$$

   inoltre è lecito rappresentare $f(x)$ come:

   $$f(x) = \sum_{i=0}^{s} [f_i]_7 x^i$$

   sfruttando quindi il principio di identità dei polinomi, si ricava in particolare che $[a_0]_7 - [b_0]_7 = [f_0]_7$, cioè $[a_0 - b_0]_7 = [f_0]_7$, e siccome $7 \mid (a_0 - b_0)$, allora possiamo concludere che $[f_0]_7 = [0]_7$. In virtù di ciò, poniamo:

   $$S_1 := \left\{ f(x) = \sum_{i=0}^{s} [f_i]_7 x^i \mid [f_0]_7 = [0]_7 \right\}$$

Si è provato che $S \subset S_1$.
Proviamo ora che $S_1 \subset S$. Per far ciò fissiamo $f(x) \in S_1$, e siano $a(x), b(x) \in \mathbb{Z}_7[x]$ tali che $[a(x)]_f = [b(x)]_f$, con

$$a(x) = \sum_{i=0}^{m} [a_i]_7 x^i \qquad b(x) = \sum_{i=0}^{n} [b_i]_7 x^i$$

Proviamo la buona positura di ϕ. Sappiamo che:

$$\phi([a(x)]_f) = [a_0]_{56} \qquad \phi([b(x)]_f) = [b_0]_{56}$$

dato che $[a(x)]_f = [b(x)]_f$, si ricava che

$$\exists q(x) \in \mathbb{Z}_7[x] \text{ tale che } a(x) - b(x) = f(x)q(x)$$

Il termine noto di $f(x)q(x)$ è $[f_0]_7[q_0]_7 = [0]_7$, e quindi il termine noto di $a(x) - b(x)$ è $[a_0 - b_0]_7 = [0]_7$, pertanto $7 \mid (a_0 - b_0)$, e dunque $56 \mid 8(a_0 - b_0)$, ossia $[a_0]_{56} = [b_0]_{56}$, cioè $\phi([a(x)]_f) = \phi([b(x)]_f)$, per cui ϕ è ben posta.
Proviamo ora che ϕ è un omomorfismo di anelli. Siano $[c(x)]_f, [d(x)]_f \in \mathbb{Z}_7[x]_{/(f(x))}$. Allora:

$$\phi([c(x)]_f + [d(x)]_f) = [8(c_0 + d_0)]_{56} = [8c_0]_{56} + [8d_0]_{56} = \phi([c(x)]_f) + \phi([d(x)]_f)$$

$$\phi([c(x)]_f \cdot [d(x)]_f) = [8c_0 d_0]_{56} = [64c_0 d_0]_{56} = \phi([c(x)]_f) \cdot \phi([d(x)]_f)$$

Quindi ϕ è un omomorfismo di anelli, e dunque $f(x) \in S$.
Si è dunque provato che $S = S_1$;

2. Definiamo l'insieme:

$$S_2 := \{f(x) \in \mathbb{Z}_7[x] \mid \phi \text{ è un monomorfismo di anelli}\}$$

Ovviamente $S_2 \subset S$. Consideriamo ora $f(x) \in S$, con

$$f(x) = \sum_{i=0}^{n} [f_i]_7 x^i$$

Sappiamo dalla teoria che

$$\mathbb{Z}_7[x]_{/(f(x))} = \left\{[[a_{n-1}]_7 x^{n-1} + ... + [a_0]_7]_f \mid a_{n-1}, ..., a_0 \in \{0, ..., 6\}\right\}$$

osserviamo inoltre che:

$$\begin{aligned} Ker\phi &= \{[a(x)]_f \in \mathbb{Z}_7[x]_{/(f(x))} \mid \phi([a(x)]_f) = [a_0]_{56}\} \\ &= \{[[a_{n-1}]_7 x^{n-1} + ... + [a_0]_7]_f \mid a_{n-1}, ..., a_0 \in \{0, ..., 6\}, \quad [8a_0]_{56} = [0]_{56}\} \\ &= \{[[a_{n-1}]_7 x^{n-1} + ... + [a_0]_7]_f \mid a_{n-1}, ..., a_0 \in \{0, ..., 6\}, \quad [a_0]_7 = [0]_7\} \\ &= \{[[a_{n-1}]_7 x^{n-1} + ... + [a_1]_7 x]_f \mid a_{n-1}, ..., a_1 \in \{0, ..., 6\}\} \end{aligned}$$

Di conseguenza $|Ker\phi| = 7^{n-1}$. Detto ciò, si ha che:

$$f(x) \in S_2 \iff \phi \text{ è un monomorfismo di anelli}$$
$$\iff |Ker\phi| = 1 \iff 7^{n-1} = 1 \iff n = 1$$

Dunque possiamo dire che:

$$\begin{aligned} S_2 &= \{f(x) \in S \mid deg(f(x)) = 1\} \\ &= \{[f_1]_7 x + [f_0]_7 \mid [f_1]_7 \neq [0]_7, [f_0]_7 = [0]_7\} \\ &= \{[f_1]_7 x \mid f_1 \in \{1, ..., 6\}\} \end{aligned}$$

e quindi $|S_2| = 6$;

3. Questo punto può essere risolto prendendo spunto dal precedente, ragion per cui si lascia al lettore il compito di portarlo a termine.

Si è visto in questi esercizi come sia possibile applicare il percorso logico illustrato in origine estendendolo oltre la sola buona positura (lo abbiamo adoperato anche per vedere, ad esempio, quando una data funzione fosse un monomorfismo). Tuttavia non sempre tale ragionamento risulta efficace, e sicuramente non è l'unico che possiamo impiegare, così come si può intuire dallo svolgimento del seguente:

- Esercizio 1.6.3: Sia n un intero positivo. Si consideri l'applicazione

$$\phi_n : \mathbb{Z}_5[x] \times \mathbb{Z}_5 \to \mathbb{Z}_5 : (f(x), \alpha) \mapsto f(\alpha)^n$$

1. Determinare l'insieme degli interi positivi n per i quali ϕ_n è surgettiva.
2. Trovare un intero positivo n e un elemento β di $\mathbb{Z}_5$ in modo tale che $\phi_n^{-1}(\beta)$ sia l'insieme vuoto.

Svolgimento

1. Sia $n \in \mathbb{N}$, con $n \geq 1$. Distinguiamo i casi seguenti:
   (a) $n = 1$. Proviamo che ϕ_1 è surgettiva.
   Sia $\beta \in \mathbb{Z}_5$, e consideriamo $f(x) := \beta \in \mathbb{Z}_5[x]$, ed $\alpha := \beta \in \mathbb{Z}_5$. È allora immediato verificare che $\phi_1(f(x), \alpha) = \beta$. Data l'arbitrarietà impiegata, possiamo dunque dire che ϕ_1 è surgettiva;
   (b) $n = 2$. Proviamo che ϕ_2 non è surgettiva.
   Consideriamo l'applicazione:

$$\psi_2 : \mathbb{Z}_5 \to \mathbb{Z}_5 : x \mapsto \psi_2(x) = x^2$$

Notiamo che

$$\overline{0} \xrightarrow{\psi_2} \overline{0}, \quad \overline{1} \xrightarrow{\psi_2} \overline{1}, \quad \overline{2} \xrightarrow{\psi_2} \overline{4}, \quad \overline{3} \xrightarrow{\psi_2} \overline{4}, \quad \overline{4} \xrightarrow{\psi_2} \overline{1}$$

cioè $Im\psi_2 = \{\overline{0}, \overline{1}, \overline{4}\}$.
Siano ora $(f(x), \alpha) \in \mathbb{Z}_5[x] \times \mathbb{Z}_5$. Allora:

$$\phi_2(f(x), \alpha) = (f(\alpha))^2 = \psi_2(f(\alpha)) \in Im\psi_2$$

Data l'arbitrarietà di $(f(x), \alpha)$, segue che $Im\phi_2 \subset Im\psi_2$, ovvero abbiamo che $Im\phi_2 \subset \{\overline{0}, \overline{1}, \overline{4}\} \neq \mathbb{Z}_5$, dunque ϕ_2 non è surgettiva;

(c) $n = 3$. Proviamo che ϕ_3 è surgettiva.
Consideriamo l'applicazione:

$$\psi_3 : \mathbb{Z}_5 \to \mathbb{Z}_5 : x \mapsto \psi_3(x) = x^3$$

Notiamo che

$$\overline{0} \xrightarrow{\psi_3} \overline{0}, \quad \overline{1} \xrightarrow{\psi_3} \overline{1}, \quad \overline{2} \xrightarrow{\psi_3} \overline{3}, \quad \overline{3} \xrightarrow{\psi_3} \overline{2}, \quad \overline{4} \xrightarrow{\psi_3} \overline{4}$$

cioè $Im\psi_3 = \mathbb{Z}_5$, e si nota subito che ψ_3 è bigettiva.
Sia ora $\beta \in \mathbb{Z}_5$. Allora:

$$\exists \mid \alpha \in \mathbb{Z}_5 \text{ tale che } \beta = \psi_3(\alpha) = \alpha^3$$

ora, posto $f(x) := \alpha \in \mathbb{Z}_5[x]$, abbiamo che:

$$\phi_3(f(x), \alpha) = (f(\alpha))^3 = \alpha^3 = \psi_3(\alpha) = \beta$$

data l'arbitrarietà di β, segue allora che ϕ_3 è surgettiva;

(d) $n = 4$. Proviamo che ϕ_4 non è surgettiva.
Consideriamo $(f(x), \alpha) \in \mathbb{Z}_5[x] \times \mathbb{Z}_5$, e distinguiamo due casi:

i. $f(\alpha) = \overline{0}$, allora $\phi_4(f(x), \alpha) = \overline{0}$;
ii. $f(\alpha) \neq \overline{0}$, allora $f(\alpha) \in U(\mathbb{Z}_5)$, e tenuto conto che $|U(\mathbb{Z}_5)| = 4$, applicando il teorema di Eulero, abbiamo: $\phi_4(f(x), \alpha) = (f(\alpha))^4 = \overline{1}$;

quindi $Im\phi_4 \subset \{\overline{0}, \overline{1}\} \neq \mathbb{Z}_5$, e pertanto ϕ_4 non è surgettiva;

(e) $n \geq 5$. Allora per il lemma di divisione Euclidea:

$$\exists \mid r, q \in \mathbb{Z} \text{ tali che } n = 4q + r, \quad 0 \leq r < 4$$

Siano $(f(x), \alpha) \in \mathbb{Z}_5[x] \times \mathbb{Z}_5$, e distinguiamo due casi:

i. $f(\alpha) = \overline{0}$, allora $\phi_n(f(x), \alpha) = \overline{0}$;
ii. $f(\alpha) \neq \overline{0}$, allora possiamo applicare il teorema di Eulero per dedurre:

$$\phi_n(f(x), \alpha) = (f(\alpha))^n = (f(\alpha))^{4q+r} = (f(\alpha))^r = \phi_r(f(x), \alpha)$$

ed essendo $0 \leq r < 4$, sappiamo già se ϕ_r (e quindi ϕ_n) è surgettiva o meno;

In definitiva, abbiamo che ϕ_n è surgettiva se e solo se $MCD(n, 4) = 1$, ossia se e solo se n è dispari.

2. Tenuto conto del punto (b), si ricava immediatamente che $\phi_2^{-1}(\overline{2}) = \emptyset$.

Capitolo 2

Esercizi

2.1 Esercizi su gruppi e permutazioni

In questa sezione ci concentreremo sulla risoluzione di alcuni esercizi che vertano sulle nozioni di gruppo, con particolare attenzione al gruppo delle permutazioni. A differenza di quanto accaduto nel primo capitolo, per ogni esercizio saranno dati, prima dello svolgimento, alcuni suggerimenti utili alla risoluzione; questo per favorire un primo approccio da parte dello studente che si accinge per la prima volta a confrontarsi con questi problemi.

- Esercizio 2.1.1: Sia H un sottogruppo non abeliano di A_4.

1. Provare che H ha più di 6 elementi.
2. Provare che ogni 3-ciclo di S_4 appartiene ad H.
3. Provare che $H = A_4$.

Di questo esercizio proponiamo due distinti svolgimenti.

Suggerimenti

- Per provare il punto 1. far vedere preliminarmente che ogni gruppo con al più 5 elementi deve essere abeliano. Supporre poi per assurdo che H abbia esattamente 6 elementi, e far leva sui periodi degli stessi per dedurre una contraddizione.
- Per provare il punto 2. fare le seguenti riflessioni: poiché H ha almeno 7 elementi, se non contiene tutti i 3-cicli, ne contiene esattamente 4, insieme a tutte le permutazioni del tipo (2,2). Dalla proprietà di chiusura si deduce allora che ad H deve appartenere anche uno (e quindi l'altro) dei 3-cicli mancanti.
- Determinare tutte le possibili strutture cicliche di A_4. Tenuto conto che dai punti precedenti sappiamo che in H c'è l'applicazione id e ci sono tutti i 3-cicli, basterà allora provare che in H ci sono tutte le permutazioni aventi struttura ciclica (2,2). Per farlo, scrivere la generica permutazione con struttura (2,2) come il prodotto di due 3-cicli.

Svolgimento 1

1. Consideriamo la seguente:
   - Proposizione
   Sia G un gruppo, e supponiamo che $|G| \leq 5$. Allora G è abeliano.
   Dimostrazione
   La tesi risulta ovvia qualora $|G| = 1$. Consideriamo quindi $|G| > 1$. Supponiamo per assurdo che G non sia abeliano. Denotato $n := |G|$, possiamo porre:

   $$G = \{g_1, \ldots, g_n\}$$

   Sia G un gruppo moltiplicativo, e sia $g_n := 1_G$ l'elemento neutro del gruppo. Definiamo:

   $$m := max\{\circ(g) \mid g \in G\}$$

   Si lascia al lettore la prova che m risulta essere ben definito.
   Siccome $|G| > 1$, allora $m > 1$. Inoltre si ha che:

   $$\exists \overline{g} \in G \text{ tale che } \circ(\overline{g}) = m$$

   Non lediamo la generalità se supponiamo che $\overline{g} = g_1$. Ora, siccome stiamo supponendo che G non sia abeliano, allora G non risulta essere ciclico, e quindi $1 < \circ(g_1) < n$. Facciamo vedere che $\circ(g_1) \neq 2$. Supponiamo per assurdo che $\circ(g_1) = 2$. Allora si ha che:

   $$\forall i = 1, ..., n \qquad \circ(g_i) \leq 2$$

   e pertanto

   $$\forall i = 1, ..., n \qquad g_i = g_i^{-1}$$

   Inoltre, dalla proprietà di chiusura, si ha:

   $$\forall i, j = 1, ..., n \qquad \exists k = 1, ..., n \qquad \text{tale che} \qquad g_i \cdot g_j = g_k$$

   Detto questo, si ha allora che, presi $i, j = 1, ..., n$ risulta:

   $$g_i \cdot g_j = g_k = g_k^{-1} = (g_i \cdot g_j)^{-1} = g_j^{-1} \cdot g_i^{-1} = g_j \cdot g_i$$

   data l'arbitrarietà impiegata, segue che G è abeliano, in contraddizione col fatto che G sia non abeliano. Tale assurdo è derivato dall'aver supposto $\circ(g_1) = 2$, e pertanto si ha che $2 < \circ(g_1) < n$. Facciamo ora dei distinguo:

   (a) Supponiamo $|G| = 2$. Allora si ha che

   $$n = |G| = 2 < \circ(g_1) < n$$

   ossia $n < n$, ma questo è assurdo. L'assurdo è derivato dall'aver supposto $|G| = 2$, quindi $|G| \neq 2$.

(b) Supponiamo $|G| = 3$. Allora si ha che

$$2 < 3 \leq \circ(g_1) < n = |G| = 3$$

e quindi $3 < 3$, ma questo è assurdo. L'assurdo è derivato dall'aver supposto $|G| = 3$, quindi $|G| \neq 3$.

(c) Supponiamo $|G| = 4$. Abbiamo allora che $2 < \circ(g_1) < n = |G| = 4$, ovvero $2 < \circ(g_1) < 4$, e dunque $\circ(g_1) = 3$. Adesso, non lediamo la generalità se poniamo:

$$\langle g_1 \rangle = \{1_G, g_1, g_2\}$$

Si nota subito che $\langle g_1 \rangle, \{g_3\}$ formano una partizione di G. Di conseguenza, considerato l'elemento $g_1 \cdot g_3 \in G$, si ha una e una sola delle seguenti possibilità:

i. $g_1 \cdot g_3 \in \{g_3\}$, allora $g_1 \cdot g_3 = g_3$, e quindi $g_1 = 1_G$, ma questo è assurdo.
ii. $g_1 \cdot g_3 \in \langle g_1 \rangle$, allora $g_1 \cdot g_3 = g_1^k$, ragion per cui $g_3 = g_1^{k-1}$, ma allora $g_3 \in \langle g_1 \rangle$, e questo è assurdo.

In ogni caso si è pervenuti a un assurdo, derivato dall'aver supposto che $|G| = 4$, e quindi $|G| \neq 4$.

(d) Supponiamo $|G| = 5$. Dovendo essere $2 < \circ(g_1) < 5$, si hanno due eventualità: $\circ(g_1) = 4$ oppure $\circ(g_1) = 3$. Se $\circ(g_1) = 4$ allora come fatto nel punto (c) ci si riconduce a un assurdo. Supponiamo quindi che sia $\circ(g_1) = 3$. Non lediamo la generalità ponendo:

$$\langle g_1 \rangle = \{1_G, g_1, g_2\}$$

Definiamo ora:

$$l := max\{\circ(g) \mid g \in G - \langle g_1 \rangle\}$$

quindi:

$$\exists \hat{g} \in G - \langle g_1 \rangle \text{ tale che } \circ(\hat{g}) = l$$

Non lediamo la generalità se supponiamo che $\hat{g} = g_3$. Ovviamente si ha che $1 < \circ(g_3) \leq \circ(g_1) = 3$, e quindi si hanno due casi:

i. $\circ(g_3) = 3$. Allora risulta semplice provare che:

$$\langle g_3 \rangle = \{1_G, g_3, g_4\}$$

in particolare, si ha che $\langle g_1 \rangle, \{g_3, g_4\}$ formano una partizione di G. A questo punto, consideriamo l'elemento $g_1 \cdot g_3 \in G$. Se $g_1 \cdot g_3 \in \langle g_1 \rangle$, allora $g_3 \in \langle g_1 \rangle$, ma ciò è assurdo. Se invece $g_1 \cdot g_3 \in \{g_3, g_4\}$, allora $g_1 \cdot g_3 \in \langle g_3 \rangle$, e quindi $g_1 \in \langle g_3 \rangle$, ma ciò è assurdo. In ogni caso si è pervenuti a un assurdo, derivato dall'aver supposto $\circ(g_3) = 3$, quindi $\circ(g_3) \neq 3$.

ii. $\circ(g_3) = 2$. Allora risulta semplice provare che $\circ(g_4) = 2$. Si ha dunque che $\langle g_1 \rangle, \{g_3\}, \{g_4\}$ formano una partizione di G. Si verifica, come fatto in precedenza, che necessariamente:

$$g_3 \cdot g_1, g_1 \cdot g_3 \in \langle g_4 \rangle \qquad g_4 \cdot g_1, g_1 \cdot g_4 \in \langle g_3 \rangle$$

e siccome $\circ(g_3) = \circ(g_4) = 2$, allora si ha per forza di cose che:

$$g_3 \cdot g_1 = g_1 \cdot g_3 = g_4 \qquad g_4 \cdot g_1 = g_1 \cdot g_4 = g_3$$

Detto questo, notiamo che:

$$g_3 \cdot g_1 = g_4 \Rightarrow g_1 = g_3^{-1} \cdot g_4 \Rightarrow g_1 = g_3 \cdot g_4$$

e analogamente

$$g_4 \cdot g_1 = g_3 \Rightarrow g_1 = g_4^{-1} \cdot g_3 \Rightarrow g_1 = g_4 \cdot g_3$$

pertanto abbiamo che:

$$g_4 \cdot g_3 = g_3 \cdot g_4 = g_1$$

in particolare abbiamo provato che g_1, g_3, g_4 commutano, e da qui risulta semplice verificare che G è abeliano, ma ciò è assurdo. Tale assurdo è derivato dall'aver supposto che $\circ(g_3) = 2$, quindi $\circ(g_3) \neq 2$.

In ogni caso siamo pervenuti a un assurdo. Tale assurdo è derivato dall'aver supposto che $|G| = 5$, e quindi $|G| \neq 5$.

In ogni caso siamo pervenuti a un assurdo. Tale assurdo è derivato dall'aver supposto che G non fosse abeliano, e quindi G deve essere abeliano. □

Adesso, siccome H è un gruppo non abeliano, in base alla suddetta proposizione possiamo dire che $|H| \geq 6$. Ora, notiamo che $H < A_4$, e che gli elementi di A_4 ammettono una e una sola delle seguenti strutture cicliche: (1,1,1,1), (2,2) o (3,1). Tenuto conto che in S_4 si contano 3 elementi aventi struttura ciclica (2,2), e che c'è un unico elemento avente struttura ciclica (1,1,1,1), allora necessariamente in H deve essere presente un elemento con struttura (3,1). Cerchiamo quindi di nominare i 3-cicli di S_4. Denotiamo:

$$\{1, ..., 4\} = \{a_1, ..., a_4\}$$

e osserviamo che i 3-cicli di S_4 sono 8, che sarebbero i seguenti:

$$\begin{aligned} c_1 &= (a_1, a_2, a_3) & d_1 &= c_1^{-1} = (a_1, a_3, a_2) \\ c_2 &= (a_1, a_2, a_4) & d_2 &= c_2^{-1} = (a_1, a_4, a_2) \\ c_3 &= (a_2, a_3, a_4) & d_3 &= c_3^{-1} = (a_2, a_4, a_3) \\ c_4 &= (a_1, a_3, a_4) & d_4 &= c_4^{-1} = (a_1, a_4, a_3) \end{aligned}$$

Si osserva in particolare che:

$$\begin{aligned} c_1 &= c_2 \cdot c_3 \\ c_2 &= c_4 \cdot c_1 \\ c_3 &= c_1 \cdot c_4 \\ c_4 &= c_3 \cdot c_2 \end{aligned}$$

In base a questo, segue subito che se H contiene tre 3-cicli, allora li contiene tutti. Adesso, supponiamo per assurdo che $|H| = 6$. Possiamo porre:

$$H = \{h_1, ..., h_6\}$$

dove $h_6 := 1_H$ è l'elemento neutro di H, ossia la permutazione id. Sappiamo che H contiene almeno un 3-ciclo, che possiamo supporre essere h_1, e per fissare le idee possiamo considerare $h_1 = c_1$. Dunque in H c'è anche il 3-ciclo $h_1^{-1} = c_1^{-1} = d_1$, e non lediamo la generalità se scriviamo $h_2 = d_1$. Quindi in H ci sono almeno due distinti 3-cicli. Supponiamo per assurdo che non ce ne siano altri. Allora avremmo che h_3, h_4, h_5 sono tutti gli elementi di S_4 aventi struttura ciclica (2,2). In particolare, possiamo considerare:

$$h_3 = (a_1, a_2)(a_3, a_4)$$

ma allora, per la proprietà di chiusura di H rispetto alla composizione, si ha che:

$$h_1 \cdot h_3 = (a_1, a_3, a_4) = c_4 \in H$$

e dunque in H si contano almeno tre distinti 3-cicli (che sarebbero c_1, d_1, c_4), ma questo è assurdo. Tale assurdo è derivato dall'aver supposto che H non avesse tre distinti 3-cicli, e quindi H contiene almeno tre distinti 3-cicli, e dunque per quanto stabilito in precedenza, contiene tutti i 3-cicli di S_4, e siccome i 3-cicli di S_4 sono 8, allora sicuramente H ha più di 6 elementi.

2. Vedasi il punto precedente.

3. Sappiamo dai punti precedenti che H contiene tutti i 3-cicli di S_4, ed è ovvio che contenga anche l'identità di S_4, cioè l'unica permutazione di S_4 con struttura (1,1,1,1). Per provare che $H = A_4$, resta quindi da provare che H contiene tutte le permutazioni di S_4 aventi struttura (2,2). Consideriamo quindi la generica permutazione di S_4 avente struttura (2,2). Allora questa sarà del tipo:

$$(a_1, a_2)(a_3, a_4)$$

dove $\{a_1, ..., a_4\} = \{1, ..., 4\}$. Osserviamo quindi che:

$$\begin{aligned}(a_1, a_2)(a_3, a_4) &= (a_1, a_2)((a_2, a_3)(a_2, a_3))(a_3, a_4) \\ &= ((a_1, a_2)(a_2, a_3))((a_2, a_3)(a_3, a_4)) \\ &= (a_1, a_2, a_3)(a_2, a_3, a_4)\end{aligned}$$

dove (a_1, a_2, a_3) e (a_2, a_3, a_4), essendo 3-cicli di S_4, sono elementi di H, e siccome H è un sottogruppo, allora $(a_1, a_2)(a_3, a_4) \in H$. Data l'arbitrarietà impiegata, segue subito che H contiene tutte le permutazioni di S_4 aventi struttura ciclica (2,2), e dunque $H = A_4$.

Proponiamo ora un ragionamento diverso.

Suggerimenti

- Per risolvere il punto 1., considerare il fatto che in H ci sono almeno due elementi che non commutano. Far vedere che H ha cardinalità strettamente maggiore di 4 (in quanto i gruppi con cardinalità minore o uguale a 4 sono tutti abeliani). Ricordarsi del fatto che $H \subset A_4$, e cercare di capire quali sono le possibili strutture cicliche degli elementi di H. Provare che in H c'è almeno un 3-ciclo, e poi far vedere la tesi nel caso in cui ci sono due 3-cicli che non commutano, oppure un 3-ciclo e una permutazione con struttura (2,2) che non commutano.

- Sfruttare il fatto che $|H| \geq 7$ per provare che in H ci sono almeno tre 3-cicli, e osservare che i 3-cicli di S_4 sono tutte e sole le permutazioni di S_4 che hanno un unico punto fisso.

- Ricordarsi nuovamente di tutte le possibili strutture cicliche di A_4. Tenuto conto che dai punti precedenti sappiamo che in H c'è l'applicazione id e ci sono tutti i 3-cicli, basterà allora provare che in H ci sono tutte le permutazioni aventi struttura ciclica (2,2). Per farlo, scrivere la generica permutazione con struttura (2,2) come il prodotto di due 3-cicli.

Svolgimento 2

1. Essendo H un gruppo non abeliano, allora:

$$\exists \sigma, \tau \in H \text{ t.c. } \sigma\tau \neq \tau\sigma \quad \text{(I)}$$

ragion per cui $\{id, \sigma, \tau, \sigma\tau, \tau\sigma\} \subset H$. Proviamo che $| \{id, \sigma, \tau, \sigma\tau, \tau\sigma\} | = 5$:

   (a) ovviamente $| \{id, \sigma, \tau\} | = 3$, altrimenti avremmo che $\sigma\tau = \tau\sigma$, in contraddizione con la (I);

   (b) proviamo che $\sigma\tau \notin \{id, \sigma, \tau\}$:

      i. se fosse $\sigma\tau = id$, allora $\sigma = \tau^{-1}$, quindi $\sigma\tau = \tau^{-1}\tau = \tau\tau^{-1} = \tau\sigma$, che sarebbe assurdo;

      ii. se fosse $\sigma\tau = \sigma$, allora $\tau = id$, che sarebbe assurdo;

      iii. se fosse $\sigma\tau = \tau$, allora $\sigma = id$, che sarebbe assurdo;

      quindi $\sigma\tau \notin \{id, \sigma, \tau\}$;

   (c) proviamo che $\tau\sigma \notin \{id, \sigma, \tau, \sigma\tau\}$:

      i. come in ii. si prova che $\tau\sigma \notin \{id, \sigma, \tau\}$;

      ii. inoltre dalla (I) sappiamo che $\sigma\tau \neq \tau\sigma$;

      quindi $\tau\sigma \notin \{id, \sigma, \tau, \sigma\tau\}$;

   Dai punti precedenti, segue allora che $| \{id, \sigma, \tau, \sigma\tau, \tau\sigma\} | = 5$.
   Ora, notiamo che $H < A_4$, e che gli elementi di A_4 ammettono una e una sola delle seguenti strutture cicliche: (1,1,1,1), (2,2) o (3,1). Vogliamo provare che almeno uno tra σ e τ ha struttura (3,1). Per farlo, supponiamo per assurdo che σ e τ non abbiano

struttura (3,1). Allora, poiché $\sigma, \tau \notin \{id\}$, ne segue che necessariamente σ e τ hanno struttura (2,2). Notiamo che in S_4 gli elementi che hanno struttura (2,2) sono:

$$(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$$

ed è immediato far vedere che questi elementi commutano fra loro (infatti tali elementi sono contenuti nel gruppo di Klein il quale, essendo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, risulta abeliano). Dunque pure σ e τ commutano, ma ciò è assurdo in virtù della (I). Pertanto uno tra σ e τ ha struttura (3,1).
Non lediamo la generalità se supponiamo che τ abbia struttura (3,1), e che quindi $o(\tau) = 3$. Abbiamo allora che $\{id, \sigma, \tau, \sigma\tau, \tau\sigma, \tau^2\} \subset H$, inoltre è semplice far vedere che $\tau^2 \notin \{id, \sigma, \tau, \sigma\tau, \tau\sigma\}$. Infatti:

(a) se fosse $\tau^2 = id$, avremmo $o(\tau) \leq 2 < 3 = o(\tau)$, che sarebbe assurdo;

(b) se fosse $\tau^2 = \sigma$, avremmo $\sigma\tau = \tau^2\tau = \tau\tau^2 = \tau\sigma$, che sarebbe assurdo;

(c) se fosse $\tau^2 = \tau$, avremmo $\tau = id$, che sarebbe assurdo;

(d) se fosse $\tau^2 = \sigma\tau$, avremmo $\sigma = \tau$, che sarebbe assurdo;

(e) se fosse $\tau^2 = \tau\sigma$, avremmo $\sigma = \tau$, che sarebbe assurdo;

dunque $\tau^2 \notin \{id, \sigma, \tau, \sigma\tau, \tau\sigma\}$, e quindi per quanto già visto precedentemente si deduce che $| \{id, \sigma, \tau, \sigma\tau, \tau\sigma, \tau^2\} | = 6$.
Detto questo, distinguiamo due casi:

(a) σ ha struttura (3,1). Allora $\{id, \sigma, \tau, \sigma\tau, \tau\sigma, \tau^2, \sigma^2\} \subset H$, e ha elementi tutti distinti. Per provarlo, mi basta far vedere che $\sigma^2 \notin \{id, \sigma, \tau, \sigma\tau, \tau\sigma, \tau^2\}$, la qual cosa si dimostra identicamente a quanto fatto in precedenza. Se ne deduce quindi che $|H| \geq 7$, ossia è verificata la tesi;

(b) σ ha struttura (2,2). Come prima, si prova che $\tau^2\sigma \notin \{id, \sigma, \tau, \tau\sigma, \tau^2\}$. Resta da provare che $\tau^2\sigma \neq \sigma\tau$, seguirà che $\{id, \sigma, \tau, \sigma\tau, \tau\sigma, \tau^2, \tau^2\sigma\}$ è un sottoinsieme di H avente 7 elementi distinti, e sarà vera la tesi.
Supponiamo per assurdo che $\tau^2\sigma = \sigma\tau$.
Notiamo che $o(\tau) = mcm(3,1) = 3$, e $o(\sigma) = mcm(2,2) = 2$, da cui si deduce che $\tau^2 = \tau^{-1}$, e $\sigma = \sigma^{-1}$. Dunque:

$$\tau^2\sigma = \sigma\tau \Rightarrow \tau^{-1}\sigma = \sigma^{-1}\tau \Rightarrow (\sigma^{-1}\tau)^{-1} = \sigma^{-1}\tau \Rightarrow (\sigma\tau)^{-1} = \sigma\tau$$

ragion per cui $o(\sigma\tau) \leq 2$. Detto ciò, tenuto conto che τ ha struttura (3,1) e che σ ha struttura (2,2), abbiamo che:

$$\sigma = (a_1, a_2)(a_3, a_4) \qquad \tau = (b_1, b_2, b_3)$$

dove $a_i, b_j \in \{1, ..., 4\}$, $| \{b_1, ..., b_3\} | = 3$, $| \{a_1, ..., a_4\} | = 4$. In particolare, si nota che

$$\{b_1, ..., b_3\} \subset \{a_1, ..., a_4\}$$

e non lediamo la generalità se supponiamo $b_1 = a_1$, $b_2 = a_2$ (il lettore cerchi di capire il perché la generalità non viene lesa). Si hanno allora due casi:

i. $b_3 = a_3$, allora:

$$\sigma\tau = (a_2, a_4, a_3)$$

e quindi $o(\sigma\tau) = 3$;

ii. $b_3 = a_4$, allora:

$$\sigma\tau = (a_2, a_3, a_4)$$

e quindi $o(\sigma\tau) = 3$;

pertanto $o(\sigma\tau) \leq 2 < 3 = o(\sigma\tau)$, ma ciò è assurdo. Di conseguenza deduciamo che $\tau^2\sigma \neq \sigma\tau$.

2. Vogliamo provare che in H sono contenuti tutti i 3-cicli di S_4. Per far questo, è sufficiente provare che

$$\forall b \in \{1, ..., 4\} : \exists \psi \in H \text{ 3-ciclo tale che } \psi(b) = b \qquad (1)$$

Si lascia al lettore la prova che (1) è condizione sufficiente affinché H contenga tutti i 3-cicli di S_4. Per dimostrarlo, si può far leva sui seguenti risultati (anche loro da provare come semplici esercizi):

$$\psi \in S_4 \text{ è un 3-ciclo} \iff \psi \in S_4 \text{ ha un solo punto fisso} \qquad (2)$$

$$\forall b \in \{1, ..., 4\} : |\{\psi \in S_4 \mid \psi(a) = a \text{ e } \psi \text{ è un 3-ciclo}\}| = 2 \qquad (3)$$

Cerchiamo quindi di provare la (1). Cominciamo sfruttando il fatto che $|H| \geq 7$, ragion per cui in H ci sono almeno tre 3-cicli (infatti gli elementi di H hanno struttura (1,1,1,1), (2,2) o (3,1), e in S_4 si conta un solo elemento con struttura (1,1,1,1), e tre elementi con struttura (2,2)). Inoltre questi 3-cicli non possono avere tutti lo stesso punto fisso in comune (in quanto vale la (3)). Detto questo, poniamo:

$$\{a_1, ..., a_4\} = \{1, ..., 4\}$$

e in virtù di quanto stabilito, non lediamo la generalità supponendo che in H ci sia un 3-ciclo che fissa a_4, e un 3-ciclo che fissa a_3. Sotto queste ipotesi, si lascia al lettore la verifica che:

$$\langle (a_1, a_2, a_3) \rangle \subset H \qquad \langle (a_1, a_2, a_4) \rangle \subset H \qquad (4)$$

Abbiamo adesso tutti gli elementi utili a verificare la (1). Fissiamo $b \in \{a_1, ..., a_4\}$ e distinguiamo i casi seguenti:

(a) $b = a_1$. Vogliamo determinare un 3-ciclo di H che fissa a_1. Per farlo, cerchiamo di sfruttare la (4). Notiamo che:

$$(a_4, a_2, a_1)(a_1, a_2, a_3) = (a_2, a_3, a_4)$$

dove $(a_4, a_2, a_1) \in \langle (a_1, a_2, a_4) \rangle$, mentre $(a_1, a_2, a_3) \in \langle (a_1, a_2, a_3) \rangle$, e dunque posto $\psi := (a_2, a_3, a_4)$, abbiamo che ψ è un 3-ciclo di H che fissa a_1;

(b) $b = a_2$. Vogliamo determinare un 3-ciclo di H che fissa a_2. Per farlo, cerchiamo di sfruttare la (4). Notiamo che:

$$(a_4, a_1, a_2)(a_2, a_1, a_3) = (a_1, a_3, a_4)$$

dove $(a_4, a_1, a_2) \in \langle (a_1, a_2, a_4) \rangle$, mentre $(a_2, a_1, a_3) \in \langle (a_1, a_2, a_3) \rangle$, e dunque posto $\psi := (a_1, a_3, a_4)$, abbiamo che ψ è un 3-ciclo di H che fissa a_2;

(c) $b = a_3$. Allora posto $\psi := (a_1, a_2, a_4)$, abbiamo subito che ψ è un 3-ciclo di H che fissa a_3;

(d) $b = a_4$. Allora posto $\psi := (a_1, a_2, a_3)$, abbiamo subito che ψ è un 3-ciclo di H che fissa a_4;

Data l'arbitrarietà di b, abbiamo quindi dedotto la (1), e pertanto H contiene tutti i 3-cicli di S_4.

3. Vedasi lo svolgimento precedente.

Facciamo ora alcune riflessioni su quest'ultimo esercizio:

1. Cerchiamo di fare mente locale, riassumendo i punti salienti che ci hanno condotto alla soluzione del problema. Per la risoluzione del punto 1., abbiamo in buona sostanza sfruttato il fatto che H fosse contenuto in A_4 per dire che i suoi elementi avevano struttura (1,1,1,1), (2,2) o (3,1). Dopodiché, si è fatto leva sulla non commutatività di H per provare che in H c'era almeno un 3-ciclo, e infine, componendo opportunamente le permutazioni e valutando i loro periodi, abbiamo dedotto che H aveva almeno 7 elementi. Nel successivo punto, abbiamo utilizzato questo risultato per dire che in H c'erano almeno 3 distinti 3-cicli, e in pratica abbiamo provato che se H conteneva 3 distinti 3-cicli, allora li conteneva tutti, e anzi di più: abbiamo proprio dedotto che $H = A_4$. Abbiamo sottolineato questo punto per una ragione precisa, che sarebbe la seguente: uno stesso esercizio può essere riformulato in modi decisamente differenti gli uni dagli altri. Infatti, il precedente esercizio ammette la seguente riformulazione equivalente:
- Esercizio: Sia H un sottogruppo di A_4, e supponiamo che in esso ci siano 3 distinti 3-cicli di S_4.
Provare che $H = A_4$.
Quindi esercizi apparentemente molto diversi possono in realtà essere identici;

2. Si nota subito una certa laboriosità nel nostro ragionamento, dovuta soprattutto al fatto che abbiamo impiegato i soli strumenti provenienti dal corso di Algebra 1. Andando avanti con gli studi, però, acquisiremo finalmente alcune nozioni senz'altro più potenti. Ad esempio si fornirà una nuova formulazione del teorema di Lagrange, secondo cui un sottogruppo di un gruppo finito ha ordine (cioè numero di elementi), che divide l'ordine del gruppo. Adoperando questo risultato, avremmo potuto liquidare in modo alquanto semplice gli ultimi due punti del precedente esercizio. Infatti: sappiamo che $H < A_4$, quindi per il teorema di Lagrange: $|H| \mid |A_4|$, ed è noto che $|A_4| = \frac{|S_4|}{2} = \frac{4!}{2} = 12$, ragion per cui $|H| \in \{1, 2, 3, 4, 6, 12\}$. Sappiamo però dal primo

punto che $|H| \geq 7$, quindi $|H| = 12 = |A_4|$, e dunque $H = A_4$, e siccome A_4 contiene tutti i 3-cicli di S_4, allora anche H contiene tutti i 3-cicli di S_4;

- Esercizio 2.1.2: Si considerino le seguenti permutazioni di S_{12}:

$$\alpha = (1, 2, 3) \qquad \beta = (4, 5, 6, 7, 8)$$

Inoltre sia γ una permutazione di A_{12} avente periodo 4. Infine, sia H un sottogruppo di A_{12} al quale appartengono α, β, γ.

1. Provare che H non è ciclico.
2. Dire se H può essere abeliano.

Di questo esercizio proponiamo addirittura tre distinti svolgimenti.

Suggerimenti

- Per provare il punto 1. ragionare per assurdo, utilizzando il teorema di Lagrange e i periodi degli elementi coinvolti nell'esercizio.
- Per provare il punto 2. ragionare per assurdo facendo vedere che, se H fosse abeliano, allora necessariamente la permutazione γ lascerebbe fissi gli elementi $1, ..., 8$. Per far questo, sfruttare il fatto che γ commuta con α e β, e cercare di capire come possono essere fatte le orbite di γ.

Svolgimento 1

1. Supponiamo per assurdo che H sia ciclico. Si ha quindi che

   $$\exists \sigma \in H \text{ tale che } H = \langle \sigma \rangle$$

   Se ne deduce che:

   $$\exists k_1, k_2, k_3 \in \{1, ..., \circ(\sigma)\} \text{ tali che } \alpha = \sigma^{k_1}, \beta = \sigma^{k_2}, \gamma = \sigma^{k_3}$$

   Abbiamo pertanto che

   $$\circ(\alpha) = \circ(\sigma^{k_1}) = \frac{\circ(\sigma)}{MCD(\circ(\sigma), k_1)}$$
   $$\circ(\beta) = \circ(\sigma^{k_2}) = \frac{\circ(\sigma)}{MCD(\circ(\sigma), k_2)}$$
   $$\circ(\gamma) = \circ(\sigma^{k_3}) = \frac{\circ(\sigma)}{MCD(\circ(\sigma), k_3)}$$

   e quindi, tenuto conto che $\circ(\alpha) = 3, \circ(\beta) = 5, \circ(\gamma) = 4$, ricaviamo che

   $$\circ(\sigma) = 3 \cdot MCD(\circ(\sigma), k_1)$$
   $$\circ(\sigma) = 5 \cdot MCD(\circ(\sigma), k_2)$$
   $$\circ(\sigma) = 4 \cdot MCD(\circ(\sigma), k_3)$$

ossia 3,5,4 dividono $\circ(\sigma)$, e siccome 3,5,4 sono a due a due coprimi, allora $3 \cdot 5 \cdot 4$ divide $\circ(\sigma)$, ovvero $60 \mid \circ(\sigma)$. Detto questo, sia:

$$\sigma = \gamma_1 \cdot ... \cdot \gamma_r$$

la decomposizione in cicli disgiunti di σ, e denotiamo con l_i la lunghezza del ciclo γ_i, dove $i = 1, ..., r$. Notiamo che:

$$\circ(\sigma) = mcm(l_1, ..., l_r)$$

dove, a meno di permutare i cicli, si ha:

$$\sum_{i=1}^{r} l_i = 12 \qquad l_1 \geq ... \geq l_r \geq 1$$

Siccome $5 \mid \circ(\sigma)$, allora $\exists i = 1, ..., r$ tale che $5 \mid l_i$.
Siccome $4 \mid \circ(\sigma)$, allora $\exists j = 1, ..., r$ tale che $4 \mid l_j$.
Siccome $3 \mid \circ(\sigma)$, allora $\exists k = 1, ..., r$ tale che $3 \mid l_k$.
Proviamo che i, j, k sono tutti distinti.
Se fosse $i = j$, allora avremmo che $5 \cdot 4 \mid l_i$, ovvero $20 \mid l_i$, per cui risulterebbe $l_i \geq 20 > 12 \geq l_i$, che sarebbe assurdo.
Se fosse $i = k$, allora avremmo che $5 \cdot 3 \mid l_i$, ovvero $15 \mid l_i$, per cui risulterebbe $l_i \geq 15 > 12 \geq l_i$, che sarebbe assurdo.
Se fosse $j = k$, allora avremmo che $4 \cdot 3 \mid l_j$, ovvero $12 \mid l_j$, per cui risulterebbe $l_j \geq 12 \geq l_j$, dunque dovrebbe essere $l_j = 12$, e pertanto $r = 1$ e $j = 1$, ossia $\sigma = \gamma_1$, ovvero σ sarebbe un 12-ciclo, ovvero σ sarebbe dispari, ma ciò contraddirebbe il fatto che $\sigma \in H < A_{12}$.
Dunque i, j, k sono a due a due distinti, e inoltre $l_i \geq 5, l_j \geq 4, l_k \geq 3$, pertanto:

$$12 = 5 + 4 + 3 \leq l_i + l_j + l_k \leq \sum_{h=1}^{r} l_h = 12$$

di conseguenza:

$$l_1 = l_i = 5 \qquad l_2 = l_j = 4 \qquad l_3 = l_k = 3 \qquad r = 3$$

Dunque σ ha struttura (5,4,3), ma allora σ è dispari, e questo è assurdo. Tale assurdo è derivato dall'aver supposto che H fosse ciclico, e pertanto H non può essere ciclico.

2. Ragioniamo per assurdo, supponendo che H sia abeliano. Possiamo scrivere

$$\alpha = (a_{[0]_3}, a_{[1]_3}, a_{[2]_3}) \qquad \beta = (b_{[0]_5}, b_{[1]_5}, b_{[2]_5}, b_{[3]_5}, b_{[4]_5})$$

dove si pone:

$$a_{[i]_3} = i + 1 \qquad i = 0, ..., 2$$
$$b_{[j]_5} = j + 4 \qquad j = 0, ..., 4$$

Il particolare uso notazionale delle classi di congruenza modulo 3 e modulo 5 come pedici (anziché degli usuali numeri naturali) è dettata da una particolare ragione. Il lettore, continuando a leggere lo svolgimento, cerchi di capire il perché di questa scelta.
Facciamo ora le seguenti osservazioni:

(a) Fissiamo $i = 0, ..., 2$ e sia $k := \gamma(a_{[i]_3})$. Proviamo che $k \in \{a_{[0]_3}, a_{[1]_3}, a_{[2]_3}\}$. Supponiamo per assurdo che $k \notin \{a_{[0]_3}, a_{[1]_3}, a_{[2]_3}\}$. Allora:

$$\gamma(\alpha(a_{[i]_3})) = \alpha(\gamma(a_{[i]_3})) = \alpha(k) = k$$

dove la prima uguaglianza segue dal fatto che H è abeliano, mentre l'ultima uguaglianza deriva dall'ipotesi $k \notin \{a_{[0]_3}, a_{[1]_3}, a_{[2]_3}\}$. Pertanto $\gamma(\alpha(a_{[i]_3})) = \gamma(a_{[i]_3})$, e data l'ingettività di γ segue che $\alpha(a_{[i]_3}) = a_{[i]_3}$. Ma questo è assurdo in quanto, essendo $i \in \{0, ..., 2\}$, risulta $\alpha(a_{[i]_3}) = a_{[i+1]_3} \neq a_{[i]_3}$. Tale assurdo è derivato dall'aver supposto $k \notin \{a_{[0]_3}, a_{[1]_3}, a_{[2]_3}\}$. Dunque $k \in \{a_{[0]_3}, a_{[1]_3}, a_{[2]_3}\}$.

(b) Fissato $j = 0, ..., 4$ e posto $k := \gamma(b_{[j]_5})$ si prova, analogamente al punto precedente, che $k \in \{b_{[0]_5}, ..., b_{[4]_5}\}$.

Prima di proseguire col nostro ragionamento, ricordiamo che, presi in considerazione $n \in \mathbb{N} - \{0\}, \sigma \in S_n, a \in \{1, ..., n\}$, si definisce orbita dell'elemento a rispetto alla permutazione σ il seguente insieme:

$$\Omega_{(\sigma,a)} := \{\sigma^m(a) \mid m \in \mathbb{Z}\}$$

In base a quanto precedentemente stabilito, abbiamo che

(1) $\forall i = 0, ..., 2 \qquad \Omega_{(\gamma, a_{[i]_3})} \subset \{a_{[0]_3}, ..., a_{[2]_3}\}$

(2) $\forall j = 0, ..., 4 \qquad \Omega_{(\gamma, b_{[j]_5})} \subset \{b_{[0]_5}, ..., b_{[4]_5}\}$

Adesso, tenuto conto che le orbite di γ formano una partizione di $\{1, ..., 12\}$, che $\circ(\gamma) = 4$ e che

(3) $\forall c = 1, ..., 12 \qquad |\Omega_{(\gamma,c)}| \mid \circ(\gamma)$

abbiamo allora dalla (1) e dalla (2) che:

$$\exists \hat{i} \in \{0, ..., 2\} \text{ tale che } |\Omega_{(\gamma, a_{[\hat{i}]_3})}| = 1$$
$$\exists \hat{j} \in \{0, ..., 4\} \text{ tale che } |\Omega_{(\gamma, b_{[\hat{j}]_5})}| = 1$$

ragion per cui risulta che

(4) $\gamma(a_{[\hat{i}]_3}) = a_{[\hat{i}]_3} \qquad \gamma(b_{[\hat{j}]_5}) = b_{[\hat{j}]_5}$

Detto questo, notiamo che:

$$\gamma(a_{\hat{[i+1]_3}}) = \gamma(\alpha(a_{\hat{[i]_3}})) = \alpha(\gamma(a_{\hat{[i]_3}})) = \alpha(a_{\hat{[i]_3}}) = a_{\hat{[i+1]_3}}$$

dunque iterando il ragionamento abbiamo che:

$$\gamma(a_{\hat{[i+2]_3}}) = a_{\hat{[i+2]_3}}$$

In definitiva, si è provato che

$$(5) \qquad \forall i = 0, ..., 2 \qquad \gamma(a_{[i]_3}) = a_{[i]_3}$$

In modo analogo, si prova che:

$$(6) \qquad \forall j = 0, ..., 4 \qquad \gamma(b_{[j]_5}) = b_{[j]_5}$$

Di conseguenza si ha che:

$$(7) \qquad \forall c = 1, ..., 8 \qquad \gamma(c) = c$$

da questo e dal fatto che $\circ(\gamma) = 4$, se ne deduce che, necessariamente, γ è un 4-ciclo, e pertanto $\gamma \notin A_{12}$, ma questo è assurdo. Tale assurdo è derivato dall'aver supposto che H fosse abeliano. Possiamo allora concludere che H non può essere abeliano.

Proponiamo ora uno svolgimento alternativo.

Suggerimenti

- Per provare il punto 1., basta risolvere il punto 2.
- Per risolvere il punto 2. si suppone per assurdo la commutatività e si effettuano considerazioni sul periodo del prodotto $\alpha\beta\gamma$. Se l'n-esima potenza di tale prodotto è uguale a id, allora γ^{-n} appartiene al sottogruppo ciclico generato dal prodotto $\alpha\beta$, il cui ordine è 15. Ma allora il periodo di γ^{-n}, che divide 4, divide anche 15, e quindi è 1. Dunque n è multiplo di 4. Poiché allora $(\alpha\beta)^n = id$, n è anche multiplo di 15. Se ne deduce che il periodo del prodotto $\alpha\beta\gamma$ è un multiplo di 60. Tuttavia, in A_{12} non esiste un elemento il cui periodo sia multiplo di 60.

Svolgimento 2

1. Per provare che H non è ciclico, è sufficiente provare che H non è abeliano (ricordiamo infatti che ogni gruppo ciclico è abeliano).
2. Proviamo che H non può essere abeliano. Supponiamo per assurdo che lo sia, e consideriamo la permutazione $\sigma := \alpha\beta\gamma$. Ovviamente $\sigma \in A_{12}$. Poniamo $n := \circ(\sigma)$. Dunque:

$$\sigma^n = id \Rightarrow (\alpha\beta\gamma)^n = id \Rightarrow (\alpha\beta)^n\gamma^n = id \Rightarrow (\alpha\beta)^n = \gamma^{-n} \Rightarrow \gamma^{-n} \in \langle\alpha\beta\rangle$$

dove nella seconda implicazione si è fatto uso della presunta abelianità di H.
Adesso, poiché $\gamma^{-n} \in \langle \alpha\beta \rangle$, allora si ha che $\circ(\gamma^{-n}) \mid \circ(\alpha\beta)$, ossia $\circ(\gamma^{-n}) \mid 15$.
Notiamo pure che $\gamma^{-n} \in \langle \gamma \rangle$, e pertanto $\circ(\gamma^{-n}) \mid \circ(\gamma)$, ovvero $\circ(\gamma^{-n}) \mid 4$.
Ne segue che $\circ(\gamma^{-n}) \mid MCD(15,4)$, cioè $\circ(\gamma^{-n}) \mid 1$, e quindi $\circ(\gamma^{-n}) = 1$, ragion per cui $\gamma^{-n} = id$, e dunque $\circ(\gamma) \mid n$, ossia $4 \mid n$.
Sappiamo inoltre che $(\alpha\beta)^n = \gamma^{-n} = id$, per cui $\circ(\alpha\beta) \mid n$, ovvero $15 \mid n$.
Ne segue che $mcm(4,15) \mid n$, cioè $60 \mid n$, quindi $60 \mid \circ(\sigma)$.
Detto questo, sia:

$$\sigma = \gamma_1 \cdot ... \cdot \gamma_r$$

la decomposizione in cicli disgiunti di σ, e denotiamo con l_i la lunghezza del ciclo γ_i, dove $i = 1, ..., r$. Notiamo che:

$$\circ(\sigma) = mcm(l_1, ..., l_r)$$

dove, a meno di permutare i cicli, si ha:

$$\sum_{i=1}^{r} l_i = 12 \qquad l_1 \geq ... \geq l_r \geq 1$$

Siccome $5 \mid \circ(\sigma)$, allora $\exists i = 1, ..., r$ tale che $5 \mid l_i$.
Siccome $4 \mid \circ(\sigma)$, allora $\exists j = 1, ..., r$ tale che $4 \mid l_j$.
Siccome $3 \mid \circ(\sigma)$, allora $\exists k = 1, ..., r$ tale che $3 \mid l_k$.
Proviamo che i, j, k sono tutti distinti.
Se fosse $i = j$, allora avremmo che $5 \cdot 4 \mid l_i$, ovvero $20 \mid l_i$, per cui risulterebbe $l_i \geq 20 > 12 \geq l_i$, che sarebbe assurdo.
Se fosse $i = k$, allora avremmo che $5 \cdot 3 \mid l_i$, ovvero $15 \mid l_i$, per cui risulterebbe $l_i \geq 15 > 12 \geq l_i$, che sarebbe assurdo.
Se fosse $j = k$, allora avremmo che $4 \cdot 3 \mid l_j$, ovvero $12 \mid l_j$, per cui risulterebbe $l_j \geq 12 \geq l_j$, dunque dovrebbe essere $l_j = 12$, e pertanto $r = 1$ e $j = 1$, ossia $\sigma = \gamma_1$, ovvero σ sarebbe un 12-ciclo, ovvero σ sarebbe dispari, ma ciò contraddirebbe il fatto che $\sigma \in H < A_{12}$.
Dunque i, j, k sono a due a due distinti, e inoltre $l_i \geq 5, l_j \geq 4, l_k \geq 3$, pertanto:

$$12 = 5 + 4 + 3 \leq l_i + l_j + l_k \leq \sum_{h=1}^{r} l_h = 12$$

di conseguenza:

$$l_1 = l_i = 5 \qquad l_2 = l_j = 4 \qquad l_3 = l_k = 3 \qquad r = 3$$

Dunque σ ha struttura (5,4,3), ma allora σ è dispari, e questo è assurdo. Tale assurdo è derivato dall'aver supposto che H fosse abeliano, e pertanto H non può essere abeliano.

Proponiamo ora un ulteriore svolgimento.

Suggerimenti

- Per provare il punto 1., basta risolvere il punto 2.
- Sfruttare il fatto che se $\sigma, \tau \in S_n$, e se

$$\sigma = (a_1^1, ..., a_{r_1}^1) \cdots (a_1^h, ..., a_{r_h}^h)$$

è la decomposizione di σ in cicli disgiunti (compresi i cicli di lunghezza 1). Allora:

$$\tau\sigma\tau^{-1} = (\tau(a_1^1), ..., \tau(a_{r_1}^1)) \cdots (\tau(a_1^h), ..., \tau(a_{r_h}^h)).$$

Agire quindi per assurdo, supponendo che H sia abeliano. In tal caso, far vedere che γ ha come punti fissi $1, ..., 8$ (per provarlo, far leva sul risultato di cui sopra e sulle strutture di α e β) e cercare da qui di dedurre l'assurdo.

Svolgimento 3

1. Per provare che H non è ciclico, è sufficiente provare che H non è abeliano (ricordiamo infatti che ogni gruppo ciclico è abeliano).
2. Proviamo che H non può essere abeliano. Cominciamo col dare il seguente risultato teorico:
   - Proposizione: siano $\sigma, \tau \in S_n$, e sia

$$\sigma = (a_1^1, ..., a_{r_1}^1)...(a_1^h, ..., a_{r_h}^h)$$

la decomposizione di σ in cicli disgiunti (compresi i cicli di lunghezza 1). Allora:

$$\tau\sigma\tau^{-1} = (\tau(a_1^1), ..., \tau(a_{r_1}^1)) \cdots (\tau(a_1^h), ..., \tau(a_{r_h}^h)) \qquad (i)$$

Dimostrazione
Si osserva che:

$$\tau\sigma\tau^{-1}(\tau(a_1^1)) = \tau(\sigma(a_1^1)) = \tau(a_2^1)$$

e analogamente si prova che le permutazioni a primo e secondo membro della (i) coincidono su tutti gli altri elementi. □
Detto ciò, supponiamo per assurdo che H sia abeliano. Allora, poiché $\alpha, \beta, \gamma \in H$, se ne deduce che:

(a) $\alpha\gamma = \gamma\alpha$, cioè $\gamma\alpha\gamma^{-1} = \alpha$, per cui sfruttando la proposizione data si ottiene che:

$$\gamma\alpha\gamma^{-1} = (\gamma(1), \gamma(2), \gamma(3)) = (1, 2, 3) = \alpha$$

pertanto γ avrà la forma seguente:

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & 9 \\ i_1 & i_2 & i_3 & j_4 & \cdots & j_{12} \end{pmatrix}$$

dove:

i. $(i_1, i_2, i_3) \in \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\} \subset \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$;

ii. $j_4, ..., j_{12} \in \{4, ..., 12\}$;

di conseguenza:

$$\gamma = \gamma_1 \sigma_1 \qquad (ii)$$

dove:

i. $\gamma_1 \in \{id, (1,2,3), (1,3,2)\} \subset S_{12}$;

ii. $\sigma_1 \in \{\sigma \in S_{12} \mid \sigma(i) = i \text{ per ogni } i \in \{1,2,3\}\}$;

(b) $\beta\gamma = \gamma\beta$, cioè $\gamma\beta\gamma^{-1} = \beta$, per cui sfruttando la proposizione data si ottiene che:

$$\gamma\beta\gamma^{-1} = (\gamma(4), ..., \gamma(8)) = (4, ..., 8) = \beta$$

pertanto, tenuto conto di (ii), si ha:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & 8 & 9 & \cdots & 12 \\ 1 & 2 & 3 & k_4 & \cdots & k_8 & j_9 & \cdots & j_{12} \end{pmatrix}$$

dove:

i. $(k_4, ..., k_8)$ è una quintupla di numeri interi appartenente al seguente insieme:

$$\{(4,5,6,7,8), (5,6,7,8,4), (6,7,8,4,5), (7,8,4,5,6), (8,4,5,6,7)\};$$

ii. $j_9, ..., j_{12} \in \{9, ..., 12\}$;

di conseguenza:

$$\gamma = \gamma_1 \gamma_2 \sigma_2 \qquad (iii)$$

dove:

i. $\gamma_2 \in \{id, (4,5,6,7,8), (4,6,8,5,7), (4,7,5,8,6), (4,8,7,6,5)\} \subset S_{12}$;

ii. $\sigma_2 \in \{\sigma \in S_{12} \mid \sigma(i) = i \text{ per ogni } i \in \{1, ..., 8\}\}$;

Facciamo adesso le seguenti considerazioni:

(a) $\gamma_1 = id$. Infatti: supponiamo per assurdo che $\gamma_1 \neq id$. Allora γ_1 è un 3-ciclo facente parte della decomposizione in cicli disgiunti di γ (infatti γ_1 è disgiunto sia da γ_2 che da σ_2, e γ_2 è disgiunto da σ_2, quindi γ_1 e γ_2 sono disgiunti dai cicli di cui si compone σ_2). Di conseguenza $l(\gamma_1) / \circ(\gamma)$, cioè $3/4$, ma questo è assurdo. Dunque $\gamma_1 = id$;

(b) $\gamma_2 = id$. Infatti: supponiamo per assurdo che $\gamma_2 \neq id$. Allora γ_2 è un 5-ciclo facente parte della decomposizione in cicli disgiunti di γ. Di conseguenza $l(\gamma_2) / \circ(\gamma)$, ovvero $5/4$, ma questo è assurdo. Dunque $\gamma_2 = id$;

Abbiamo perciò che:

$$\gamma = \sigma_2 = \begin{pmatrix} 1 & \cdots & 8 & 9 & \cdots & 12 \\ 1 & \cdots & 8 & j_9 & \cdots & j_{12} \end{pmatrix} \qquad (iv)$$

e quindi si hanno le seguenti possibili strutture cicliche per σ_2 (e quindi per γ):

$$(1,1,1,1), (2,1,1), (2,2), (3,1), (4)$$

tuttavia, sappiamo che $\circ(\gamma) = 4$, quindi l'unica struttura che mi può rendere vera la (vi) è (4), ma allora γ sarebbe un 4-ciclo, e quindi $\gamma \notin A_{12}$, ma ciò è in contraddizione con l'ipotesi $\gamma \in A_{12}$. Si è quindi giunti a un assurdo, derivato dall'aver supposto che H fosse abeliano, e pertanto H non può essere abeliano.

- Esercizio 2.1.3: Siano date, in S_{18}, le seguenti permutazioni:

- $\sigma = (1,2,3)(5,6)(7,8,9)(10,11)(12,13,14,15,16,17,18)$
- $\tau = (1,2,3,4)(5,6,7)(8,9,10)(11,12,13)(14,15,16,17,18)$

1. Determinare un sottogruppo H, abeliano e non ciclico, di S_{18} tale che $H \cap \langle\sigma\rangle$ e $H \cap \langle\tau\rangle$ non siano il sottogruppo banale.
2. Determinare un sottogruppo ciclico di S_{18} verificante la proprietà del punto precedente.

Suggerimenti

- Per provare il punto 1., osservare che $H \cap \langle\sigma\rangle$ è un gruppo ciclico generato da una potenza di σ, che chiamiamo r. Analogamente $H \cap \langle\tau\rangle$ è un gruppo ciclico generato da una potenza di τ, che chiamiamo s. Si consideri quindi l'insieme:

$$\langle r, s\rangle := \{r^{n_1}s^{m_1}\cdots r^{n_l}s^{m_l} \mid n_i, m_i \in \mathbb{Z}\}$$

  Provare che tale insieme è un sottogruppo di S_{18}, e tale gruppo è sicuramente abeliano se $rs = sr$. Ricordarsi quindi che tra i gruppi abeliani non ciclici a noi noti, c'è il gruppo di Klein (isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$), quindi fare in modo che $\langle r, s\rangle$ sia isomorfo a tale gruppo (occorre quindi scegliere opportunamente le suddette potenze di σ e τ). Basterà poi porre $H := \langle r, s\rangle$.

- Il punto 2. risulta in verità più semplice del precedente. Anche qui il sottogruppo può essere generato da opportune potenze di σ e τ.

Svolgimento

1. Facciamo le seguenti osservazioni:
   (a) $H < S_{18}$, quindi $H \cap \langle\sigma\rangle$ è un gruppo (perché è intersezione di gruppi). Inoltre $H \cap \langle\sigma\rangle < \langle\sigma\rangle$, e siccome $\langle\sigma\rangle$ è ciclico, allora $H \cap \langle\sigma\rangle$ è ciclico, e sarà generato da una potenza di σ, cioè:

   (1) $\quad H \cap \langle\sigma\rangle = \langle\sigma^k\rangle \qquad$ con $k \in \{0, ..., \circ(\sigma) - 1\}$ opportuno.

   Ora, siccome $H \cap \langle\sigma\rangle$ non è banale, allora $k \neq 0$;
   (b) analogamente al punto precedente, si ricava che

   (2) $\quad H \cap \langle\tau\rangle = \langle\tau^h\rangle \qquad$ con $h \in \{1, ..., \circ(\tau) - 1\}$ opportuno.

Ora, i punti precedenti ci suggeriscono di considerare

(3) $\quad H = \langle \sigma^k, \tau^h \rangle \qquad$ con $k \in \{1, ..., \circ(\sigma) - 1\}, h \in \{1, ..., \circ(\tau) - 1\}$ opportuni.

Vogliamo che H sia abeliano, ragion per cui occorre che sia:

(4) $\quad \sigma^k \tau^h = \tau^h \sigma^k$

Si richiede anche che H non sia ciclico. Tra i gruppi abeliani non ciclici ricordiamo il gruppo di Klein (il quale risulta uguale, a meno di isomorfismi, al gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$). Vediamo quindi se è possibile scegliere (h, k) in modo che H sia isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Affinché ciò sia vero, è necessario che gli elementi di H non abbiano periodo maggiore di 2 e quindi, in particolare, che σ^k e τ^h abbiano esattamente periodo 2 (in quanto deve valere la (3)). Inoltre, per far valere la (4), è sufficiente che i cicli di σ^k e di τ^h siano a due a due disgiunti. Seguendo tali direttive, consideriamo:

(5) $\quad (h, k) = (30, 21)$

allora posto:

(6) $\quad r := \sigma^k = \sigma^{21} = (5, 6)(10, 11) \qquad s := \tau^h = \tau^{30} = (1, 3)(2, 4)$

abbiamo che, definito:

(7) $\quad H := \langle r, s \rangle = \{r^{n_1} s^{m_1} \cdots r^{n_l} s^{m_l} \mid n_i, m_i \in \mathbb{Z}\}$

risulta che H è un sottogruppo di S_{18} (il lettore lo verifichi adoperando, ad esempio, la caratterizzazione dei sottogruppi). Inoltre H è abeliano in quanto $rs = sr$, e inoltre:

$$\begin{aligned} H &= \langle r, s \rangle \\ &= \{r^{n_1} s^{m_1} \cdots r^{n_l} s^{m_l} \mid n_i, m_i \in \mathbb{Z}\} \\ &= \{r^n s^m \mid n, m \in \mathbb{Z}\} \\ &= \{r^n s^m \mid n, m \in \{0, 1\}\} \\ &= \{id, r, s, rs\} \end{aligned}$$

dove la terza uguaglianza è dovuta al fatto che $rs = sr$, mentre la quarta uguaglianza segue dal fatto che $\circ(r) = \circ(s) = 2$. Notiamo pure che:

$$H \cap \langle \sigma \rangle = \{id, r\} \qquad H \cap \langle \tau \rangle = \{id, s\}$$

non sono banali. A questo punto, ci resta solo da provare che H non è ciclico. A tal fine è sufficiente provare che H è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Per questo definiamo l'applicazione $\phi : H \to \mathbb{Z}_2 \times \mathbb{Z}_2$ che opera come segue:

$$id \mapsto ([0]_2, [0]_2), \quad r \mapsto ([1]_2, [0]_2), \quad s \mapsto ([0]_2, [1]_2), \quad rs \mapsto ([1]_2, [1]_2)$$

è semplice verificare che ϕ è un isomorfismo di gruppi.

2. Resta valido il ragionamento di cui al punto 1. fino alla (4). Stavolta però vogliamo che H sia ciclico. Allora il modo migliore di agire è quello di fare in modo che σ^k, τ^h siano cicli disgiunti le cui lunghezze siano coprime tra loro. A tal fine, consideriamo:

   (8) $\quad (h,k) = (15,6)$

   e siano:

   (9) $\quad r := \sigma^k = \sigma^6 = (12,18,17,16,15,14,13) \qquad s := \tau^h = \tau^{15} = (1,4,3,2)$

   Abbiamo che, posto:

   (10) $\quad H := \langle r,s\rangle = \{r^{n_1}s^{m_1}\cdots r^{n_l}s^{m_l} \mid n_i, m_i \in \mathbb{Z}\}$

   risulta che H è abeliano in quanto $rs = sr$. Inoltre:

   $$\{id, r\} \subset H \cap \langle\sigma\rangle \qquad \{id, s\} \subset H \cap \langle\tau\rangle$$

   e quindi $H \cap \langle\sigma\rangle$ e $H \cap \langle\tau\rangle$ non sono banali. Resta da verificare che H è ciclico. A questo scopo, si consideri:

   (11) $\quad t := rs = (1,4,3,2)(12,18,17,16,15,14,13)$

   Siccome $t \in \langle r,s\rangle$, allora $\langle t\rangle \subset H$. Inoltre si ha:

   (12) $\quad r = t^8, \quad s = t^{21}$

   cioè $r, s \in \langle t\rangle$, quindi $H \subset \langle t\rangle$. Pertanto $H = \langle t\rangle$, ovvero H è ciclico.

- Esercizio 2.1.4: Si considerino le seguenti permutazioni di S_{13}:

$$\alpha = (1,2,3,4,5)(6,7,8,9)(10,11,12,13)$$

$$\beta = (1,2,3,4)(5,6,7,8,9)(10,11)(12,13)$$

1. Provare che $\langle\alpha\rangle \cap \langle\beta\rangle$ è il sottogruppo banale.
2. Sia H un sottogruppo di S_{13} al quale appartengono α e β. Determinare, in H, un sottogruppo commutativo e non ciclico.

Suggerimenti

- Per risolvere il punto 1., ragionare sulle orbite di α e β, in particolare notare le differenze tra l'orbita di 5 rispetto ad α e l'orbita di 5 rispetto a β.

- Prendere di nuovo in considerazione il fatto che un tale sottogruppo può essere generato da una coppia di elementi di H che commutino tra loro e, in particolare, da opportune potenze di α e di β.

Svolgimento

1. Il nostro obiettivo è provare che $\langle\alpha\rangle \cap \langle\beta\rangle = \{id\}$. Ovviamente $\{id\} \subset \langle\alpha\rangle \cap \langle\beta\rangle$, quindi ci resta soltanto da verificare che $\langle\alpha\rangle \cap \langle\beta\rangle \subset \{id\}$. Per questo motivo fissiamo $\gamma \in \langle\alpha\rangle \cap \langle\beta\rangle$, ragion per cui:

$$\exists h, k \in \mathbb{Z} \text{ tali che} \quad \gamma = \alpha^h \quad \wedge \quad \gamma = \beta^k$$

Tenuto conto che $\circ(\alpha) = \circ(\beta) = 20$, non lediamo affatto la generalità supponendo che $h, k \in \{0, ..., 19\}$.
Prima di proseguire col nostro ragionamento, ricordiamo che, presi in considerazione $n \in \mathbb{N} - \{0\}, \sigma \in S_n, a \in \{1, ..., n\}$, si definisce orbita dell'elemento a rispetto alla permutazione σ il seguente insieme:

$$\Omega_{(\sigma,a)} := \{\sigma^m(a) \mid m \in \mathbb{Z}\}$$

Detto questo, si osserva immediatamente che:

$$5 \in \Omega_{(\alpha,1)} \cap \Omega_{(\beta,9)} \qquad \wedge \qquad \Omega_{(\alpha,1)} \neq \Omega_{(\beta,9)}$$

Inoltre, tenuto conto che $|\Omega_{(\alpha,1)}| = |\Omega_{(\beta,9)}| = 5$, si lascia al lettore la semplice verificare che, per ogni $i \in \{1, 5\}$ e per ogni $j \in \{5, 9\}$:

$$\Omega_{(\alpha^h,i)} = \Omega_{(\alpha,i)} \iff MCD(h, 5) = 1$$

$$\Omega_{(\beta^k,j)} = \Omega_{(\beta,j)} \iff MCD(k, 5) = 1$$

Supponiamo adesso che $MCD(h, 5) = MCD(k, 5) = 1$; si ha quindi, in base a quanto già detto, che:

$$\Omega_{(\alpha,1)} = \Omega_{(\alpha^h,1)} = \Omega_{(\alpha^h,5)} = \Omega_{(\gamma,5)} = \Omega_{(\beta^k,5)} = \Omega_{(\beta^k,9)} = \Omega_{(\beta,9)}$$

si è dunque stabilito che $\Omega_{(\alpha,1)} = \Omega_{(\beta,9)}$, ma ciò è in contraddizione col fatto che $\Omega_{(\alpha,1)} \neq \Omega_{(\beta,9)}$. L'assurdo deriva dall'aver supposto $MCD(h, 5) = MCD(k, 5) = 1$, di conseguenza abbiamo che $MCD(h, 5) \neq 1$ oppure $MCD(k, 5) \neq 1$, e siccome 5 è un numero primo, allora ciò equivale a dire che $5 \mid h$ oppure $5 \mid k$. Distinguiamo quindi i casi seguenti:

   (a) $5 \mid h \quad \wedge \quad \neg(5 \mid k)$, allora $h \in \{0, 5, 10, 15\}$, e si ha che:

$$5 = \alpha^h(5) = \gamma(5) = \beta^k(5) \in \{6, 7, 8, 9\}$$

   e quindi ho un assurdo;

   (b) $5 \mid k \quad \wedge \quad \neg(5 \mid h)$, allora analogamente al caso precedente ricaviamo un assurdo;

(c) $5 \mid h \quad \wedge \quad 5 \mid k$, allora $h, k \in \{0, 5, 10, 15\}$. Si distinguono allora i casi seguenti:

i. $h \neq 0 \quad \wedge \quad k \neq 0$, allora:

$$\gamma(4) = \alpha^h(4) = 4 \neq \beta^k(4) = \gamma(4)$$

e quindi ho un assurdo;

ii. $h = 0 \quad \wedge \quad k \neq 0$, allora:

$$\gamma = \alpha^h = id \neq \beta^k = \gamma$$

e quindi ho un assurdo;

iii. $h \neq 0 \quad \wedge \quad k = 0$, allora come nel punto precedente si deduce un assurdo;

iv. $h = 0 \quad \wedge \quad k = 0$, allora si ottiene che $\gamma = id$;

L'unico caso in cui non si incorre in contraddizioni è quello in cui $h = k = 0$, e quindi ne segue che necessariamente $\gamma = id$. Data l'arbitrarietà nella scelta di $\gamma \in \langle\alpha\rangle \cap \langle\beta\rangle$, possiamo allora dire che $\langle\alpha\rangle \cap \langle\beta\rangle \subset \{id\}$, e che quindi $\langle\alpha\rangle \cap \langle\beta\rangle$ è il sottogruppo banale.

2. Osserviamo che il più piccolo sottogruppo di S_{13} contenente α e β è il gruppo generato da α e β, che sarebbe il seguente:

$$\langle\alpha, \beta\rangle := \{\alpha^{r_1}\beta^{s_1} \cdots \alpha^{r_m}\beta^{s_m} \mid m \in \mathbb{N} - \{0\} \quad r_i, s_i \in \mathbb{Z} \quad i = 1, ..., m\}$$

Si consiglia al lettore di verificare quanto segue:

$$\langle\alpha, \beta\rangle = \bigcap_{\{\alpha,\beta\} \subset G < S_{13}} G$$

Abbiamo quindi che $\langle\alpha, \beta\rangle \subset H$. Il nostro fine è determinare, in H, un sottogruppo commutativo e non ciclico. Per far questo, in virtù di quanto detto, è sufficiente determinare un sottogruppo commutativo e non ciclico di $\langle\alpha, \beta\rangle$, ed è questo ciò che faremo.
Sia K il nostro ipotetico sottogruppo di $\langle\alpha, \beta\rangle$ che sia commutativo e non ciclico. Ora, il modo più intuitivo di agire, per definire K, è supporre che esso sia generato da una coppia di elementi, che chiamiamo γ e δ, i quali devono, per forza di cose, commutare tra loro e appartenere a $\langle\alpha, \beta\rangle$. Si richiede inoltre che K non sia ciclico, e quindi non devo poter esprimere γ come una potenza di δ e viceversa. Adesso, la cosa più naturale è fare in modo che γ sia una potenza di α (cioè che $\gamma \in \langle\alpha\rangle$), che δ sia una potenza di β (cioè che $\delta \in \langle\beta\rangle$), e che i cicli di γ siano disgiunti da quelli di δ (in modo da assicurare che γ e δ commutino tra loro). Una buona scelta, in questo senso, è la seguente:

$$\gamma := \alpha^5 = (6, 7, 8, 9)(10, 11, 12, 13) \qquad \delta := \beta^{10} = (1, 3)(2, 4)$$

e quindi posto $K := \langle \gamma, \delta \rangle$, si ha che:

$$\begin{aligned} K &= \langle \gamma, \delta \rangle \\ &= \{\gamma^{r_1}\delta^{s_1} \cdots \gamma^{r_m}\delta^{s_m} \mid m \in \mathbb{N} - \{0\} \quad r_i, s_i \in \mathbb{Z} \quad i = 1, ..., m\} \\ &= \{\gamma^r \delta^s \mid r, s \in \mathbb{Z}\} \\ &= \{\gamma^r \delta^s \mid r \in \{0, ..., \circ(\gamma) - 1\}, s \in \{0, ..., \circ(\delta) - 1\}\} \\ &= \{\gamma^r \delta^s \mid r \in \{0, 1, 2, 3\}, s \in \{0, 1\}\} \end{aligned}$$

Data la scelta di γ e δ, è ovvio che K sia un sottogruppo commutativo di $\langle \alpha, \beta \rangle$. Resta da provare che K non è ciclico. Si è già visto che $|K| = 8$, inoltre è semplice far vedere che:

$$\circ(\gamma^r \delta^s) \leq 4 \qquad \forall r \in \{0, 1, 2, 3\}, s \in \{0, 1\}$$

ragion per cui K non può esser ciclico.
Alternativamente, avremmo potuto considerare le permutazioni:

$$\sigma := \alpha^{10} = (6, 8)(7, 9)(10, 12)(11, 13) \qquad \tau := \beta^{10} = (1, 3)(2, 4)$$

e costruire, a partire da queste, un opportuno sottogruppo di H che risulti abeliano e non ciclico. Infatti si nota subito che σ e τ commutano, e inoltre:

$$\sigma\tau = \tau\sigma = (1, 3)(2, 4)(6, 8)(7, 9)(10, 12)(11, 13)$$

Di conseguenza:

$$\circ(\sigma) = \circ(\tau) = \circ(\sigma\tau) = 2$$

Tenuto conto di questo poniamo:

$$L := \{id, \sigma, \tau, \sigma\tau\}$$

Si verifica che L risulta essere un sottogruppo di H. Infatti L è contenuto in H in quanto σ e τ sono rispettivamente potenze di α e β, che per ipotesi appartengono ad H che sappiamo essere un sottogruppo di S_{13}. Oltretutto L contiene la permutazione id ed è chiuso rispetto all'operazione di inversione, ossia di ogni elemento contiene il suo inverso, e ciò in quanto ogni suo elemento ha periodo al più 2, e quindi ogni elemento di L coincide col suo inverso. Inoltre L è chiuso rispetto al prodotto, e per provarlo basta considerare la seguente tabella moltiplicativa:

$\cdot$	id	σ	τ	$\sigma\tau$
id	id	σ	τ	$\sigma\tau$
σ	σ	id	$\sigma\tau$	τ
τ	τ	$\sigma\tau$	id	σ
$\sigma\tau$	$\sigma\tau$	τ	σ	id

Inoltre L è abeliano (in quanto σ e τ commutano tra loro) e non può essere ciclico, in quanto ha cardinalità 4 mentre ogni suo elemento ha periodo al più 2.

- Esercizio 2.1.5: Sia data la seguente permutazione di S_{17}:

$$\alpha = (1,2,3,4,5)(6,7,8,9,10,11)(12,13,14,15,16,17)$$

Per ogni intero positivo n, sia $K_n = \{\sigma \in \langle\alpha\rangle \mid \circ(\sigma) \text{ divide } n\}$.

1. Provare che, per ogni n, K_n è un sottogruppo di S_{17}.
2. Determinare $|K_{18396}|$.
3. Determinare tutti gli n per i quali $|K_n| = 2$.

Suggerimenti

- Provare il punto 1. facendo uso della caratterizzazione dei sottogruppi.
- Per provare il punto 2. provare che

  $$\sigma \in K_{18396} \iff \sigma \in \langle\alpha\rangle \text{ e inoltre } \circ(\sigma) \text{ divide } MCD(\circ(\alpha), 18396)$$

  e ricordarsi che:

  $$\circ(\alpha^h) = \frac{\circ(\alpha)}{MCD(h, \circ(\alpha))}.$$

- Per provare il punto 3. si ragiona in modo simile al punto precedente.

Svolgimento

1. Sia n un intero positivo. Proviamo che K_n è un sottogruppo di S_{17} facendo uso della caratterizzazione dei sottogruppi:
   (a) Anzitutto $K_n \neq \emptyset$, infatti: $id \in \langle\alpha\rangle$ e in più $\circ(id) = 1$, per cui $\circ(id)$ divide n, e dunque $id \in K_n$.
   (b) Consideriamo $\sigma, \tau \in K_n$, e facciamo vedere che $\sigma\tau^{-1} \in K_n$. Infatti: siccome $\sigma, \tau \in \langle\alpha\rangle$, allora:

   $$\exists h, k \in \mathbb{Z} \text{ tali che } \sigma = \alpha^h,\ \tau = \alpha^k$$

   Abbiamo quindi che:

   $$\sigma\tau^{-1} = \alpha^h(\alpha^k)^{-1} = \alpha^{h-k} \in \langle\alpha\rangle$$

   Dunque ci resta solo da provare che $\circ(\sigma\tau^{-1})$ divide n, e ciò accade, per una nota proposizione, se e soltanto se $(\sigma\tau^{-1})^n = id$. Basta quindi verificare quest'ultima condizione, e in effetti:

   $$(\sigma\tau^{-1})^n = (\alpha^{h-k})^n = \alpha^{n(h-k)} = \alpha^{nh}\alpha^{-nk} = (\alpha^h)^n(\alpha^k)^{-n} = \sigma^n\tau^{-n}$$

   Adesso, siccome $\circ(\sigma)$ e $\circ(\tau)$ dividono n, allora per la sopracitata proposizione si ha che $\sigma^n = \tau^n = id$, e quindi:

   $$(\sigma\tau^{-1})^n = \sigma^n\tau^{-n} = \sigma^n(\tau^n)^{-1} = id \cdot id^{-1} = id$$

   da quanto premesso, possiamo ora dire che $\sigma\tau^{-1} \in K_n$.

In base ai suddetti punti e alla caratterizzazione dei sottogruppi, concludiamo che K_n è un sottogruppo di S_{17}.

2. Verifichiamo quanto segue:

$$\sigma \in K_{18396} \iff \sigma \in \langle\alpha\rangle \text{ e inoltre } \circ(\sigma) \text{ divide } MCD(\circ(\alpha), 18396)$$

Infatti:

(a) Supponiamo $\sigma \in K_{18396}$ e verifichiamo, sotto tale ipotesi, che $\sigma \in \langle\alpha\rangle$ e che inoltre $\circ(\sigma)$ divide $MCD(\circ(\alpha), 18396)$.

i. Siccome $\sigma \in K_{18396}$, allora $\sigma \in \langle\alpha\rangle$, di conseguenza $\sigma = \alpha^h$, con h un opportuno numero intero. Sappiamo allora, da un noto risultato, che:

$$\circ(\sigma) = \circ(\alpha^h) = \frac{\circ(\alpha)}{MCD(h, \circ(\alpha))}$$

da cui si deduce che $\circ(\sigma)$ divide $\circ(\alpha)$.

ii. Siccome $\sigma \in K_{18396}$, allora $\circ(\sigma)$ divide 18396.

Abbiamo quindi che $\circ(\sigma)$ divide sia $\circ(\alpha)$ che 18396, e quindi dividerà anche il $MCD(\circ(\alpha), 18396)$.
In definitiva, si ha che $\sigma \in \langle\alpha\rangle$ e che inoltre $\circ(\sigma)$ divide $MCD(\circ(\alpha), 18396)$.

(b) Supponiamo ora che $\sigma \in \langle\alpha\rangle$ e che inoltre $\circ(\sigma)$ divide $MCD(\circ(\alpha), 18396)$. Allora risulta immediato, sotto tali ipotesi, verificare che $\sigma \in K_{18396}$.

Adesso, in base a quanto provato, necessitiamo di conoscere il $MCD(\circ(\alpha), 18396)$. A tal fine, si osserva che:

$$\circ(\alpha) = mcm(5, 6, 6) = 30 = 2 \cdot 3 \cdot 5 \qquad 18396 = 2^2 \cdot 3^2 \cdot 7 \cdot 73$$

ragion per cui:

$$MCD(\circ(\alpha), 18396) = 2 \cdot 3 = 6$$

Consideriamo adesso $\sigma \in \langle\alpha\rangle$, e quindi

$$\exists h = 0, ..., 29 \text{ tale che } \sigma = \alpha^h$$

Sappiamo allora che:

$$\circ(\sigma) = \circ(\alpha^h) = \frac{\circ(\alpha)}{MCD(h, \circ(\alpha))}$$

e di conseguenza:

$$\circ(\sigma) \text{ divide } MCD(\circ(\alpha), 18396) \iff \tfrac{\circ(\alpha)}{MCD(h,\circ(\alpha))} \text{ divide } MCD(\circ(\alpha), 18396) \iff$$

$$\iff \left(\tfrac{30}{MCD(h,30)}\right) \mid 6 \iff \tfrac{30}{MCD(h,30)} \in \{1, 2, 3, 6\} \iff h \in \{0, 5, 10, 15, 20, 25\}$$

Pertanto, in virtù di quanto stabilito in precedenza, otteniamo che:

$$K_{18396} = \{\alpha^h \mid h \in \{0, 5, 10, 15, 20, 25\}\}$$

e quindi $|K_{18396}| = 6$.

3. Così come fatto nel punto precedente, si prova che:

$$\sigma \in K_n \iff \sigma \in \langle\alpha\rangle \text{ e inoltre } \circ(\sigma) \text{ divide } MCD(\circ(\alpha), n)$$

ragion per cui risulta che

$$\sigma \in K_n \iff \sigma = \alpha^h, \text{ con } h \in \{1, ..., \circ(\alpha)\}, \text{ e inoltre } \circ(\sigma) \text{ divide } MCD(\circ(\alpha), n)$$

Detto questo, ricordiamo che

$$(1) \qquad \forall h = 1, ..., \circ(\alpha): \qquad \circ(\alpha^h) = \tfrac{\circ(\alpha)}{MCD(\circ(\alpha), h)}$$

Ricordiamo pure che $MCD(\circ(\alpha), n) \mid n$ e che $MCD(\circ(\alpha), n) \mid \circ(\alpha)$, e siccome $\circ(\alpha) = 30$, allora si hanno i seguenti possibili casi:

(a) $MCD(\circ(\alpha), n) = 30$, ossia $MCD(\circ(\alpha), n) = \circ(\alpha)$, quindi $\circ(\alpha) \mid n$, e di conseguenza dalla (1) si deduce subito che

$$\forall h = 1, ..., \circ(\alpha): \qquad \circ(\alpha^h) \mid n$$

per cui $K_n = \langle\alpha\rangle$, e in particolare $|K_n| > 2$.

(b) $MCD(\circ(\alpha), n) = 15$. Sfruttando la (1), troviamo che $\circ(\alpha^2) = \circ(\alpha^4) = \circ(\alpha^8) = 15$, dunque $\circ(\alpha^2), \circ(\alpha^4), \circ(\alpha^8)$ dividono il $MCD(\circ(\alpha), n)$, e dunque per transitività dividono n. Ne segue che $\alpha^2, \alpha^4, \alpha^8 \in K_n$, e perciò $|K_n| > 2$.

(c) $MCD(\circ(\alpha), n) = 10$. Sfruttando la (1), troviamo che $\circ(\alpha^3) = \circ(\alpha^9) = \circ(\alpha^{21}) = 10$, dunque $\circ(\alpha^3), \circ(\alpha^9), \circ(\alpha^{21})$ dividono il $MCD(\circ(\alpha), n)$, e dunque per transitività dividono n. Ne segue che $\alpha^3, \alpha^9, \alpha^{21} \in K_n$, e perciò $|K_n| > 2$.

(d) $MCD(\circ(\alpha), n) = 6$. Sfruttando la (1), troviamo che $\circ(\alpha^5) = \circ(\alpha^{25}) = 6$ e inoltre $\circ(\alpha^{30}) = 1$, dunque $\circ(\alpha^5), \circ(\alpha^{25}), \circ(\alpha^{30})$ dividono il $MCD(\circ(\alpha), n)$, e dunque per transitività dividono n. Ne segue che $\alpha^5, \alpha^{25}, \alpha^{30} \in K_n$, e perciò $|K_n| > 2$.

(e) $MCD(\circ(\alpha), n) = 5$. Sfruttando la (1), troviamo che $\circ(\alpha^6) = \circ(\alpha^{12}) = \circ(\alpha^{18}) = 5$, dunque $\circ(\alpha^6), \circ(\alpha^{12}), \circ(\alpha^{18})$ dividono il $MCD(\circ(\alpha), n)$, e dunque per transitività dividono n. Ne segue che $\alpha^6, \alpha^{12}, \alpha^{18} \in K_n$, e perciò $|K_n| > 2$.

(f) $MCD(\circ(\alpha), n) = 3$. Sfruttando la (1), troviamo che $\circ(\alpha^{10}) = \circ(\alpha^{20}) = 3$ e inoltre $\circ(\alpha^{30}) = 1$, dunque $\circ(\alpha^{10}), \circ(\alpha^{20}), \circ(\alpha^{30})$ dividono il $MCD(\circ(\alpha), n)$, e dunque per transitività dividono n. Ne segue che $\alpha^{10}, \alpha^{20}, \alpha^{30} \in K_n$, e perciò $|K_n| > 2$.

(g) $MCD(\circ(\alpha), n) = 2$. Sfruttando la (1), troviamo che l'unico elemento di $\langle\alpha\rangle$ avente periodo 2 è α^{15}, ed è ovvio che l'unico elemento di $\langle\alpha\rangle$ avente periodo 1 è α^{30}. Quindi α^{15}, α^{30} sono gli unici elementi di $\langle\alpha\rangle$ che dividono il $MCD(\circ(\alpha), n)$, e dunque per transitività dividono n. Ne segue che $K_n = \{\alpha^{15}, \alpha^{30}\}$, per cui $|K_n| = 2$.

(h) $MCD(\circ(\alpha), n) = 1$. Allora è semplice verificare che $K_n = \{\alpha^{30}\}$, e quindi $|K_n| < 2$.

In base a quanto detto, segue che $|K_n| = 2$ se e soltanto se $MCD(\circ(\alpha), n) = 2$.

A proposito di quest'ultimo esercizio, facciamo una riflessione: il punto 2. può essere interessante in quanto oggetto di spunto per un altro tipo di generalizzazione, che sarebbe la seguente: determinare la cardinalità di K_n al variare dell'intero positivo n.

2.2 Esercizi su omomorfismi e divisibilità

In questa sezione sposteremo la nostra attenzione su esercizi riguardanti la nozione di omomorfismo tra strutture (peraltro già incontrata quando abbiamo affrontato il problema della buona positura) e quella di divisibilità tra numeri interi. Come nella precedente sezione, ciascun esercizio sarà corredato da opportuni suggerimenti.

- Esercizio 2.2.1:

1. Determinare tutte le soluzioni dell'equazione $x^3 = x$ in $\mathbb{Z}_{303}$.
2. Determinare tutte le soluzioni dell'equazione $x^3 = x$ in $\mathbb{Z}_{404}$.

Suggerimenti

- Per la risoluzione di entrambi i punti, tenere conto che le soluzioni volute sono radici di opportuni polinomi a coefficienti in un anello, e non in un campo. Per determinare queste radici, servirà risolvere un sistema di congruenze lineari, e quindi ci sarà da rispolverare il teorema Cinese del resto.

Svolgimento

1. Anzitutto definiamo:

$$f_{303}(x) = x^3 - x \in \mathbb{Z}_{303}[x] \qquad H_{303} := \{\alpha \in \mathbb{Z}_{303} \mid f_{303}(\alpha) = [0]_{303}\}$$

Ovviamente l'insieme delle soluzioni dell'equazione $x^3 = x$ in $\mathbb{Z}_{303}$ coincide con H_{303}. È immediato verificare che:

$$f_{303}(x) = x(x + [1]_{303})(x - [1]_{303})$$

Saremmo quindi tentati di dire che $H_{303} = \{[0]_{303}, [1]_{303}, [-1]_{303}\}$. Purtroppo questo è inesatto, e ciò in quanto $\mathbb{Z}_{303}$ non è un campo; infatti 303 non è primo, poiché ha la seguente fattorizzazione: $303 = 3 \cdot 101$. Definiamo quindi:

$$f_i(x) = x^3 - x \in \mathbb{Z}_i[x] \qquad H_i := \{\alpha \in \mathbb{Z}_i \mid f_i(\alpha) = [0]_i\} \qquad i \in \{3, 101\}$$

Ovviamente, fissato $i \in \{3, 101\}$, risulta che:

$$f_i(x) = x(x + [1]_i)(x - [1]_i) \qquad i \in \{3, 101\}$$

e stavolta, essendo $\mathbb{Z}_i$ un campo, si ha effettivamente che $H_i = \{[0]_i, [1]_i, [-1]_i\}$. In particolare, si nota subito che $H_3 = \mathbb{Z}_3$.
Consideriamo ora $\alpha \in \{0, ..., 302\}$, e osserviamo quanto segue:

$$[\alpha]_{303} \in H_{303} \iff 303 \mid (\alpha^3 - \alpha) \iff 3 \cdot 101 \mid (\alpha^3 - \alpha) \iff$$
$$3 \mid (\alpha^3 - \alpha) \quad \wedge \quad 101 \mid (\alpha^3 - \alpha) \iff [\alpha]_3 \in H_3 \quad \wedge \quad [\alpha]_{101} \in H_{101} \iff$$
$$[\alpha]_3 \in \mathbb{Z}_3 \quad \wedge \quad [\alpha]_{101} \in \{[0]_{101}, [1]_{101}, [-1]_{101}\} \iff$$
$$\alpha \equiv 0 \ mod\ 101 \quad \vee \quad \alpha \equiv 1 \ mod\ 101 \quad \vee \quad \alpha \equiv -1 \ mod\ 101 \iff$$
$$\alpha \in \{0, 101, 202\} \cup \{1, 102, 203\} \cup \{100, 201, 302\}$$

Di conseguenza abbiamo che:

$$H_{303} = \{[\alpha]_{303} \mid \alpha \in \{0, 101, 202, 1, 102, 203, 100, 201, 302\}\}.$$

Avremmo anche potuto risolvere l'esercizio facendo leva sul Teorema cinese del resto, in base al quale si ha il seguente isomorfismo di anelli:

$$\phi : \mathbb{Z}_{303} \to \mathbb{Z}_3 \times \mathbb{Z}_{101} : [x]_{303} \mapsto ([x]_3, [x]_{101})$$

Sfruttando tale isomorfismo, otteniamo che

$$[\alpha]_{303} \in H_{303} \iff [\alpha]^3_{303} = [\alpha]_{303} \iff \phi([\alpha]^3_{303}) = \phi([\alpha]_{303}) \iff$$
$$([\alpha]^3_3, [\alpha]^3_{101}) = ([\alpha]_3, [\alpha]_{101}) \iff [\alpha]_3 \in H_3 \quad \wedge \quad [\alpha]_{101} \in H_{101}$$

e da qui in poi possiamo facilmente concludere l'esercizio così come fatto sopra.

2. Ragioniamo analogamente al punto precedente, tenendo però conto che questa volta $404 = 4 \cdot 101$. Definiamo quanto segue:

$$f_i(x) = x^3 - x \in \mathbb{Z}_i[x] \qquad H_i := \{\alpha \in \mathbb{Z}_i \mid f_i(\alpha) = [0]_i\} \qquad i \in \{4, 101, 404\}$$

Ovviamente l'insieme delle soluzioni dell'equazione $x^3 = x$ in $\mathbb{Z}_{404}$ coincide con H_{404}. Altrettanto ovvio il fatto che sia:

$$f_i(x) = x(x + [1]_i)(x - [1]_i) \qquad i \in \{4, 101, 404\}$$

in virtù di ciò, è immediato verificare che:

$$H_4 = \{[0]_4, [1]_4, [3]_4\} \qquad H_{101} = \{[0]_{101}, [1]_{101}, [-1]_{101}\}$$

Agendo quindi come nel punto precedente si prova che, dato $\alpha \in \{0, ..., 403\}$, risulta:

$$[\alpha]_{404} \in H_{404} \iff [\alpha]_4 \in H_4 \quad \wedge \quad [\alpha]_{101} \in H_{101}$$

notiamo quindi che:

(a) $[\alpha]_4 \in H_4$ se e soltanto se:

$$\alpha \in \{4k \mid k \in \{0, ..., 100\}\} \cup \{4k+1 \mid k \in \{0, ..., 100\}\} \cup \{4k+3 \mid k \in \{0, ..., 100\}\};$$

(b) $[\alpha]_{101} \in H_{101}$ se e soltanto se

$$\alpha \in \{0, 101, 202, 303\} \cup \{1, 102, 203, 304\} \cup \{100, 201, 302, 403\};$$

Ragion per cui possiamo concludere che:

$$[\alpha]_{404} \in H_{404} \iff \alpha \in \{0, 101, 303, 1, 203, 304, 100, 201, 403\}.$$

- Esercizio 2.2.2:

1. Determinare tutti i numeri interi positivi n per i quali 77 divide $4^{n^2+n+13} - 1$.
2. Determinare un primo dispari p tale che, per ogni intero positivo n, p non divida il numero $4^{n^2+n+13} - 1$.

Suggerimenti

- Per provare il punto 1., determinare il periodo di $[4]_{77}$ in $U(\mathbb{Z}_{77})$, che chiamiamo m, e far vedere che i nostri n, modulo m, sono radici di un opportuno polinomio in $\mathbb{Z}_m[x]$.
- Scegliere un primo p in modo che $[4]_p \in U(\mathbb{Z}_p)$, porre $m := \circ_{U(\mathbb{Z}_p)}([4]_p)$, considerare il polinomio
$$\overline{f}_m(x) = x^2 + x + [13]_m \in \mathbb{Z}_m[x]$$
e fare in modo che tale polinomio non abbia alcuna radice in $\mathbb{Z}_m$ scegliendo opportunamente p.

Svolgimento

1. Sia $n \in \mathbb{N}$. Procederemo attraverso una sequenza di equivalenze. Si ha che 77 divide $4^{n^2+n+13} - 1$ sse $[4^{n^2+n+13} - 1]_{77} = [0]_{77}$ sse $[4]_{77}^{n^2+n+13} = [1]_{77}$; tenuto conto che $MDC(4, 77) = 1$, e che quindi $[4]_{77} \in U(\mathbb{Z}_{77})$, abbiamo che $[4]_{77}^{n^2+n+13} = [1]_{77}$ sse $\circ_{U(\mathbb{Z}_{77})}([4]_{77}) \mid (n^2 + n + 13)$; tenuto conto che $\circ_{U(\mathbb{Z}_{77})}([4]_{77}) = 15$, possiamo dire, in base a quanto già dedotto, che $77 \mid (4^{n^2+n+13} - 1)$ sse $15 \mid (n^2 + n + 13)$, e ciò accade sse $[n^2 + n + 13]_{15} = [0]_{15}$ sse $[n]_{15}^2 + [n]_{15} + [13]_{15} = [0]_{15}$; di conseguenza, posto $\overline{f}_{15}(x) = x^2 + x + [13]_{15} \in \mathbb{Z}_{15}[x]$, abbiamo che 77 divide $4^{n^2+n+13} - 1$ sse $\overline{f}_{15}([n]_{15}) = [0]_{15}$ sse $[n]_{15}$ è radice di $\overline{f}_{15}(x)$ in $\mathbb{Z}_{15}$. Possiamo determinare le radici di $\overline{f}_{15}(x)$ facendo uso del Teorema cinese del resto, così come fatto nell'Esercizio 2.2.1. Si ricaverà allora che le radici di $\overline{f}_{15}(x)$ in $\mathbb{Z}_{15}$ sono $[0]_{15}, [13]_{15}$, e quindi riassumendo il nostro ragionamento abbiamo che 77 divide $4^{n^2+n+13} - 1$ sse $[n]_{15} = [1]_{15}$ oppure $[n]_{15} = [13]_{15}$. In definitiva l'insieme degli $n \in \mathbb{N}$ per i quali 77 divide $4^{n^2+n+13} - 1$ è il seguente
$$A = \{n \in \mathbb{N} \mid [n]_{15} = [1]_{15} \quad \vee \quad [n]_{15} = [13]_{15}\}$$

2. Sia p un primo dispari positivo. Possiamo subito dire che $MCD(p,4)=1$, e che quindi $[4]_p \in U(\mathbb{Z}_p)$. Definiamo $m := \circ_{U(\mathbb{Z}_p)}([4]_p)$, e consideriamo il seguente polinomio:

$$\overline{f}_m(x) = x^2 + x + [13]_m \in \mathbb{Z}_m[x]$$

Ragionando come fatto nel punto precedente, risulta semplice verificare che:

$$\exists n \in \mathbb{N} \text{ tale che } p \mid (4^{n^2+n+13} - 1) \iff \overline{f}_m(x) \text{ ha almeno una radice in } \mathbb{Z}_m$$

Negando la suddetta equivalenza si ottiene allora che:

$$\forall n \in \mathbb{N} : \neg(p \mid (4^{n^2+n+13} - 1)) \iff \overline{f}_m(x) \text{ non ha alcuna radice in } \mathbb{Z}_m$$

Il nostro obiettivo è quindi quello di determinare un primo dispari positivo p in modo che $\overline{f}_m(x)$ non abbia alcuna radice in $\mathbb{Z}_m$, essendo $m := \circ_{U(\mathbb{Z}_p)}([4]_p)$. Cominciamo allora con il determinare un intero m per il quale $\overline{f}_m(x)$ non abbia alcuna radice in $\mathbb{Z}_m$. Procedendo per tentativi, si trova che $m = 2$ è una buona scelta, in quanto $\overline{f}_2(x) = x^2 + x + [1]_2$ non ha radici in $\mathbb{Z}_2$. Fatto questo, non ci resta che determinare un primo dispari positivo p in modo che $\circ_{U(\mathbb{Z}_p)}([4]_p) = 2$. Procedendo per tentativi, si trova che $p = 5$ è una buona scelta, in quanto $\circ_{U(\mathbb{Z}_5)}([4]_5) = 2$. Pertanto abbiamo dedotto che 5 è un primo dispari tale che, per ogni intero positivo n, 5 non divide $4^{n^2+n+13} - 1$.

- Esercizio 2.2.3: Siano $a, b \in \mathbb{Z}, m, n \in \mathbb{N} - \{0, 1\}$. Si consideri:

$$\phi^{a,b}_{m,n} : \mathbb{Z}_{mn} \to \mathbb{Z}_n \times \mathbb{Z}_m : [x]_{mn} \mapsto \phi^{a,b}_{m,n}([x]_{mn}) = ([ax]_n, [bx]_m)$$

1. Determinare tutti gli interi a, b per i quali $\phi^{a,b}_{14,15}(\mathbb{Z}_{210})$ ha cardinalità 10.
2. Determinare tutti gli interi a, b per i quali $\phi^{a,b}_{2,3}$ è un omomorfismo di anelli.
3. Determinare $(\phi^{2,35}_{3,14})^{-1}([1]_3, [1]_{14})$.

Suggerimenti

- Per risolvere il punto 1., ricordare che se $\phi : G_1 \to G_2$ è un omomorfismo di gruppi, e se $G_1 = \langle g \rangle$, allora $\phi(G_1) = \langle \phi(g) \rangle$. Detto questo, risulterà poi sufficiente ricordarsi della relazione che intercorre tra l'ordine di un gruppo ciclico e il periodo di un suo generatore.
- Il punto 2. è un problema di buona positura risolubile come già visto in una precedente sezione.
- Il punto 3. consiste nella risoluzione di un opportuno sistema di congruenze lineari, che può o meno avere soluzione.

Svolgimento

1. Anzitutto si lascia al lettore la semplice verifica che $\phi^{a,b}_{m,n}$ è ben posta ed è un omomorfismo di gruppi per qualsivoglia scelta di $a, b \in \mathbb{Z}, m, n \in \mathbb{N} - \{0, 1\}$. Scegliamo adesso $a, b \in \mathbb{Z}$. Il gruppo $(\mathbb{Z}_{210}, +)$ è generato da $[1]_{210}$, cioè $\mathbb{Z}_{210} = \langle [1]_{210} \rangle$, e quindi gli elementi di $\mathbb{Z}_{210}$ sono del tipo $k[1]_{210}$, con $k \in \mathbb{Z}$. Notiamo quindi che, se $k > 0$, allora:

$$\begin{aligned}\phi^{a,b}_{14,15}(k[1]_{210}) &= \phi^{a,b}_{14,15}(\underbrace{[1]_{210} + ... + [1]_{210}}_{k-volte}) \\ &= \underbrace{\phi^{a,b}_{14,15}([1]_{210}) + ... + \phi^{a,b}_{14,15}([1]_{210})}_{k-volte} \\ &= k\phi^{a,b}_{m,n}([1]_{210})\end{aligned}$$

Si lascia al lettore la semplice verifica che se $k \leq 0$, allora $\phi^{a,b}_{14,15}(k[1]_{210}) = k\phi^{a,b}_{m,n}([1]_{210})$. Di conseguenza $\phi^{a,b}_{14,15}(\mathbb{Z}_{210}) = \langle \phi^{a,b}_{14,15}([1]_{210}) \rangle$, ed essendo $\phi^{a,b}_{14,15}([1]_{210}) = ([a]_{14}, [b]_{15})$, allora $\phi^{a,b}_{14,15}(\mathbb{Z}_{210}) = \langle ([a]_{14}, [b]_{15}) \rangle$.
Poniamo $c := ([a]_{14}, [b]_{15})$. Vogliamo che $|\phi^{a,b}_{14,15}(\mathbb{Z}_{210})| = 10$, cioè che $\langle c \rangle$ sia un sottogruppo di ordine 10 di $\mathbb{Z}_{14} \times \mathbb{Z}_{15}$, ovvero che c sia un elemento periodico di periodo 10 in $\mathbb{Z}_{14} \times \mathbb{Z}_{15}$. Notiamo che:

$$\circ_{\mathbb{Z}_{14} \times \mathbb{Z}_{15}}(c) = \circ_{\mathbb{Z}_{14} \times \mathbb{Z}_{15}}([a]_{14}, [b]_{15}) = mcm(\circ_{\mathbb{Z}_{14}}([a]_{14}), \circ_{\mathbb{Z}_{15}}([b]_{15}))$$

occorre quindi imporre che $mcm(\circ_{\mathbb{Z}_{14}}([a]_{14}), \circ_{\mathbb{Z}_{15}}([b]_{15})) = 10 = 2 \cdot 5$. Notiamo che, per il teorema di Lagrange, si ha che:
- $\circ_{\mathbb{Z}_{14}}([a]_{14}) \mid |\mathbb{Z}_{14}|$, cioè $\circ_{\mathbb{Z}_{14}}([a]_{14}) \in \{1, 2, 7, 14\}$;
- $\circ_{\mathbb{Z}_{15}}([b]_{15}) \mid |\mathbb{Z}_{15}|$, cioè $\circ_{\mathbb{Z}_{15}}([b]_{15}) \in \{1, 3, 5, 15\}$;
in considerazione di ciò, si ha che:

$$mcm(\circ_{\mathbb{Z}_{14}}([a]_{14}), \circ_{\mathbb{Z}_{15}}([b]_{15})) = 2 \cdot 5 \iff (\circ_{\mathbb{Z}_{14}}([a]_{14}), \circ_{\mathbb{Z}_{15}}([b]_{15})) = (2, 5)$$

occorre quindi determinare gli elementi di $\mathbb{Z}_{14}$ aventi periodo 2, e gli elementi di $\mathbb{Z}_{15}$ aventi periodo 5.
- è immediato verificare che $[7]_{14}$ è l'unico elemento di $\mathbb{Z}_{14}$ avente periodo 2;
- è inoltre semplice vedere che $[3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}$ sono gli elementi di $\mathbb{Z}_{15}$ aventi periodo 5;
dunque l'insieme degli interi (a, b) tali che $\phi^{a,b}_{14,15}(\mathbb{Z}_{210})$ abbia cardinalità 10, è il seguente:

$$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid [a]_{14} = [7]_{14} \quad \wedge \quad [b]_{15} \in \{[3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}\}.$$

2. Definiamo l'insieme:

$$S_0 := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \phi^{a,b}_{2,3} \text{ è un omomorfismo di anelli}\}$$

e fissiamo un elemento $(a,b) \in S_0$. Siano ora $x, y \in \mathbb{Z}$. Allora, essendo $\phi_{2,3}^{a,b}$ un omomorfismo di anelli, si ha che:

$$\phi_{2,3}^{a,b}([x]_6 \cdot [y]_6) = \phi_{2,3}^{a,b}([x]_6) \cdot \phi_{2,3}^{a,b}([y]_6)$$

ovvero risulta:

$$([axy]_2, [bxy]_3) = ([a^2xy]_2, [b^2xy]_3)$$

da cui deduciamo immediatamente che:

$$([a]_2 \cdot [a-1]_2 \cdot [xy]_2, [b]_3 \cdot [b-1]_3 \cdot [xy]_3) = ([0]_2, [0]_3) \qquad (1)$$

Data l'arbitrarietà di $x.y \in \mathbb{Z}$, possiamo sceglierli, in particolare, in modo che:

$$[xy]_2 \neq [0]_2 \qquad [xy]_3 \neq [0]_3$$

con questa scelta, tenuto conto che $\mathbb{Z}_2, \mathbb{Z}_3$ sono campi, dalla (1) otteniamo allora che:

$$([a]_2 \cdot [a-1]_2, [b]_3 \cdot [b-1]_3) = ([0]_2, [0]_3)$$

ragion per cui:

$$[a]_2 \in \{[0]_2, [1]_2\} \quad \wedge \quad [b]_3 \in \{[0]_3, [1]_3\}.$$

Posto

$$S_1 := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid [a]_2 \in \{[0]_2, [1]_2\} \quad \wedge \quad [b]_3 \in \{[0]_3, [1]_3\}\}$$

si è provato che $S_0 \subset S_1$.
Si lascia ora al lettore la semplice verifica che $S_1 \subset S_0$, e che quindi $S_0 = S_1$.

3. Si osserva quanto segue:

$$\begin{aligned}(\phi_{3,14}^{2,35})^{-1}([1]_3, [1]_{14}) &= \{[x]_{42} \mid \phi_{3,14}^{2,35}([x]_{42}) = ([1]_3, [1]_{14})\} \\ &= \{[x]_{42} \mid ([2x]_3, [35x]_{14}) = ([1]_3, [1]_{14})\} \\ &= \{[x]_{42} \mid 2x \equiv 1 \ mod \ 3 \ \wedge \ 35x \equiv 1 \ mod \ 14\}\end{aligned}$$

valutiamo quindi l'insieme delle soluzioni del seguente sistema di congruenze lineari nell'incognita x:

$$\begin{cases} 2x \equiv 1 \ mod \ 3 \\ 35x \equiv 1 \ mod \ 14 \\ x \in \{0, ..., 41\} \end{cases}$$

Tenuto conto che $MCD(35, 14)$ non divide 1, segue che la congruenza $35x \equiv 1 \ mod \ 14$ non ha soluzione, e dunque il precedente sistema non ha soluzione, e pertanto:

$$(\phi_{3,14}^{2,35})^{-1}([1]_3, [1]_{14}) = \emptyset.$$

- Esercizio 2.2.4: Determinare l'insieme dei numeri interi n tali che 12 divide il numero

1. $1 + \sum_{i=1}^{11} n^i$
2. $5 + \sum_{i=1}^{11} n^i$

Suggerimenti

- Entrambi i punti si risolvono allo stesso modo, tenendo cioè conto che gli n cercati sono, modulo 12, gli zeri di un particolare polinomio a coefficienti in $\mathbb{Z}_{12}$. Si consiglia però di distinguere il caso di radici invertibili in $\mathbb{Z}_{12}$ (per poter sfruttare in modo opportuno il teorema di Eulero) dal caso di radici non invertibili in $\mathbb{Z}_{12}$.

Svolgimento

1. Definiamo l'insieme:
$$S := \left\{ n \in \mathbb{Z} \mid 12 \mid \left(1 + \sum_{i=1}^{11} n^i \right) \right\}$$
Consideriamo poi il polinomio:
$$f(x) := [1]_{12} + \sum_{i=1}^{11} x^i \in \mathbb{Z}_{12}[x]$$
È immediato verificare che $S = \{n \in \mathbb{Z} \mid f([n]_{12}) = [0]_{12}\}$, ragion per cui ci limiteremo a considerare $n \in \{0, ..., 11\}$. Distinguiamo due casi:
   (a) $[n]_{12} \in U(\mathbb{Z}_{12})$, quindi $n \in \{1, 5, 7, 11\}$. Ovviamente:
   $$|U(\mathbb{Z}_{12})| = \phi(12) = \phi(2^2 \cdot 3) = \phi(2^2) \cdot \phi(3) = 2 \cdot (2-1) \cdot (3-1) = 4$$
   dove ϕ è la funzione di Eulero. Poniamo ora:
   $$g(x) := [3]_{12} \cdot (x^3 + x^2 + x + [1]_{12}) \in \mathbb{Z}_{12}[x]$$
   Osserviamo che, essendo $[n]_{12} \in U(\mathbb{Z}_{12})$, possiamo sfruttare il teorema di Eulero per dire che
   $$f([n]_{12}) = g([n]_{12})$$
   e quindi le radici invertibili di $f(x)$ coincidono con le radici invertibili di $g(x)$. Detto questo, è immediato verificare che
   $$\forall \alpha \in U(\mathbb{Z}_{12}) : \qquad g(\alpha) = [0]_{12}$$
   e quindi $\{n \in \mathbb{Z} \mid [n]_{12} \in U(\mathbb{Z}_{12})\} \subset S$;
   (b) $[n]_{12} \notin U(\mathbb{Z}_{12})$. Facciamo un'ulteriore distinzione:
      i. $n \in \{0, 2, 4, 6, 8, 10\}$. Allora n è pari, e quindi $1 + \sum_{i=1}^{11} n^i$ è dispari, ragion per cui 12 non può dividere $1 + \sum_{i=1}^{11} n^i$, e dunque $n \notin S$;

ii. $n \in \{3, 9\}$. Allora supposto per assurdo che $n \in S$, si ha che

$$12 \mid \left(1 + \sum_{i=1}^{11} n^i\right)$$

e quindi

$$3 \mid \left(1 + \sum_{i=1}^{11} n^i\right) \quad \wedge \quad 3 \mid \sum_{i=1}^{11} n^i$$

ragion per cui $3 \mid 1$, ma questo è assurdo;

Da quanto detto segue che $S = \{n \in \mathbb{Z} \mid [n]_{12} \in U(\mathbb{Z}_{12})\}$.

2. Ragionando analogamente al punto precedente, si deduce che:

$$\nexists n \in \mathbb{Z} : \quad 12 \mid \left(5 + \sum_{i=1}^{11} n^i\right).$$

2.3 Esercizi sui polinomi

In questa sezione ci concentreremo invece sulla risoluzione di problemi che vertano sulla nozione di polinomio, cercando di comprendere quando e come poterli fattorizzare e come poterne determinare le radici. Inoltre, nel caso delle classi di congruenza modulo un polinomio, vedremo quali sono le condizioni di invertibilità e come determinare gli inversi. Come nelle precedenti due sezioni, ogni esercizio riporterà alcuni utili suggerimenti, per chi volesse cominciare a vedersela da solo.

- Esercizio 2.3.1: Sia n un intero maggiore di 1.

1. Provare che il polinomio $f(x) = x^{2n} - 2x^{2n-4} - 2^{n-1}$ possiede in $\mathbb{Q}[x]$ un fattore irriducibile di grado 2.

2. Provare che la riduzione di $f(x)$ modulo 7 ha almeno due radici in $\mathbb{Z}_7$.

Suggerimenti

- Per risolvere il punto 1., capire quale legame intercorre tra il polinomio $f(x)$ e il polinomio
$$h(x) := x^n - 2x^{n-2} - 2^{n-1} \in \mathbb{Q}[x]$$
provare poi che per ogni intero positivo $n > 1$ risulta $h(2) = 0$, e sfruttare infine il teorema di Ruffini per decomporre opportunamente $h(x)$ e, quindi, $f(x)$.

- Per risolvere il punto 1., si può sfruttare il punto precedente, ammesso e non concesso di essere stati in grado di decomporre $f(x)$ seguendo le suddette direttive.

Svolgimento

1. Osserviamo subito che

$$f(x) = x^{2n} - 2x^{2n-4} - 2^{n-1} = (x^2)^n - 2(x^2)^{n-2} - 2^{n-1}$$

Definendo il polinomio:

$$h(x) := x^n - 2x^{n-2} - 2^{n-1} \in \mathbb{Q}[x]$$

È immediato verificare che $h(2) = 0$, cioè che 2 è radice in $\mathbb{Q}$ di $h(x)$. Ci si potrebbe chiedere come abbiamo fatto a capire che 2 è una radice di $h(x)$. Molto semplicemente, si è adottato un ragionamento di questo tipo: mi slego dalla generalità di $h(x)$ dovuta alla presenza di n, per considerare alcuni casi particolari. Si considera perciò il caso $n = 2$, e capisco che in tal caso 2 è radice di $h(x)$, poi considero $n = 3$, e anche qui mi accorgo che 2 è radice di $h(x)$, poi considero $n = 4$, e di nuovo osservo che 2 è radice di $h(x)$. A questo punto sorge spontanea una domanda: "non è che, per caso, 2 è radice di $h(x)$ per ogni $n \in \mathbb{N} - \{0, 1\}$?" La risposta è affermativa in quanto, fissato $n \in \mathbb{N}$:

$$h(2) = 2^n - 2 \cdot 2^{n-2} - 2^{n-1} = 2^n - 2^{n-1} - 2^{n-1} = 2^n - 2 \cdot 2^{n-1} = 2^n - 2^n = 0$$

Quindi per il teorema di Ruffini: $(x - 2) \mid h(x)$ in $\mathbb{Q}[x]$, ossia:

$$\exists a(x) \in \mathbb{Q}[x] \text{ tale che } h(x) = (x - 2) \cdot a(x)$$

Definiamo ora i polinomi $b(x) := a(x^2) \in \mathbb{Q}[x]$, $k(x) := x^2 - 2 \in \mathbb{Q}[x]$. si osserva subito che:

$$f(x) = h(x^2) = (x^2 - 2) \cdot a(x^2) = k(x) \cdot b(x)$$

Possiamo allora dire che il polinomio $k(x)$ divide $f(x)$ in $\mathbb{Q}[x]$. Risulta poi ovvio che $k(x)$ sia irriducibile in $\mathbb{Q}[x]$, in quanto ha grado 2 e non ha radici in $\mathbb{Q}$, ragion per cui possiamo applicare il secondo corollario al teorema di Ruffini per dedurre appunto l'irriducibilità di $k(x)$ in $\mathbb{Q}[x]$.

2. Sia $\overline{f}_7(x)$ la riduzione modulo 7 di $f(x)$ in $\mathbb{Z}_7[x]$, e sia $\overline{k}_7(x)$ la riduzione modulo 7 di $k(x)$ in $\mathbb{Z}_7[x]$. Siccome $k(x) \mid f(x)$, allora $\overline{k}_7(x) \mid \overline{f}_7(x)$, e in particolare le radici in $\mathbb{Z}_7$ di $\overline{k}_7(x)$ sono radici in $\mathbb{Z}_7$ di $\overline{f}_7(x)$. Osserviamo allora che:

$$\overline{k}_7(x) = x^2 - [2]_7 \in \mathbb{Z}_7[x]$$

e che in particolare $\overline{k}_7([3]_7) = [0]_7$, e $\overline{k}_7([4]_7) = [0]_7$. Quindi $[3]_7, [4]_7$ sono radici distinte di $\overline{f}_7(x)$ in $\mathbb{Z}_7$.

- Esercizio 2.3.2: Sia p un numero primo positivo e dispari. Per ogni intero positivo n sia:

$$f_n(x) = x^n + x + 1 \in \mathbb{Z}[x]$$

e sia $\bar{f}_n(x)$ la sua riduzione modulo p.

1. Provare che esistono infiniti interi positivi n non divisibili per p per i quali $\bar{f}_n(x)$ ha in $\mathbb{Z}_p$ una sola radice.

2. Provare che esistono infiniti interi positivi n divisibili per p per i quali $\bar{f}_n(x)$ ha in $\mathbb{Z}_p$ una sola radice.

Suggerimenti

- I due quesiti ammettono un processo risolutivo pressoché identico, che si basa sostanzialmente su una corretta applicazione del Teorema di Eulero.

Svolgimento

1. Sappiamo che p è un numero dispari, primo e positivo, quindi $p > 2$, e in particolare $\overline{-2} = \overline{p-2} \in U(\mathbb{Z}_p)$. Ora, dal Teorema di Eulero sappiamo che:

$$\forall \alpha \in U(\mathbb{Z}_p): \qquad \alpha^{p-1} = \overline{1}$$

ragion per cui definiamo l'insieme:

$$S_0 := \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}, MCD(k,p) = 1 \text{ t.c. } n = k(p-1)\}$$

è ovvio che S_0 sia un insieme infinito. Considero ora $n \in S_0$, allora $n = k(p-1)$, con $k \in \mathbb{N}$ e $MCD(k,p) = 1$. Sia ora $\alpha \in U(\mathbb{Z}_p)$, allora:

$$\overline{f}_n(\alpha) = \alpha^{k(p-1)} + \alpha + \overline{1} = \overline{1} + \alpha + \overline{1} = \alpha + \overline{2} \tag{2.1}$$

Tenuto quindi conto che $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$ e che $\overline{f}_n(\overline{0}) \neq \overline{0}$, essendo vera la (1), ne segue che l'unica radice di $\overline{f}_n(x)$ in $\mathbb{Z}_p$ è $\overline{-2}$.
Infine, siccome $MCD(k,p) = 1$, allora $\neg(p \mid n)$. Infatti: se fosse vero che $p \mid n$, allora $p \mid k(p-1)$, e siccome $MCD(k,p) = 1$, allora $p \mid (p-1)$, ma ciò risulterebbe assurdo.

2. È sufficiente considerare l'insieme:

$$S_1 := \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \text{ t.c. } n = kp(p-1)\}$$

e ragionare in modo analogo a quanto fatto in (a).

- Esercizio 2.3.3:

1. Provare che il polinomio

$$f(x) = x^{1002} + 75x^{1001} + 42x^{1000} - 36x^{999} + 17x^{202} + 31x^{201} - 10x^{11} + 9x^2 + 21x + 210 \in \mathbb{Z}[x]$$

non ha radici intere di molteplicità maggiore di uno.

2. sia p un intero positivo primo. Determinare una fattorizzazione in $\mathbb{Z}_p[x]$ del polinomio $g(x) = x^{2p} + [4]_p x^p + [4]_p$.

3. Determinare un numero intero a tale che, per ogni numero primo $p > 2$, il polinomio $h(x) = x^{2p} + [4]_p x^p + [a]_p$ abbia in $\mathbb{Z}_p$ due radici distinte.

Suggerimenti

- Per risolvere il punto 1. si può agire per assurdo, tenendo conto che le radici razionali di $f(x)$ devono essere intere e devono dividere il termine noto di $f(x)$, che la nozione di radice multipla implica una particolare decomposizione di $f(x)$, e che questa nuova decomposizione può essere confrontata con $f(x)$ attraverso il principio di identità dei polinomi.
- Per risolvere il punto 2., osservare preliminarmente che $g(x)$ è il quadrato di un binomio, per poi sfruttare il teorema binomiale di Newton in $\mathbb{Z}_p$ e il teorema di Fermat per dedurre la fattorizzazione di $g(x)$.
- Per risolvere il punto 3., considerare la sostituzione $y = x^p$, imporre che $h(y)$ abbia due radici distinte, sfruttare il teorema di Ruffini e il principio di identità dei polinomi per ricavare una opportuna scelta di tali radici, e infine far leva sul teorema di Fermat per dire che queste radici di $h(y)$ sono pure radici di $h(x)$.

Svolgimento

1. Supponiamo per assurdo che $r \in \mathbb{Z}$ sia una radice multipla di $f(x)$. Allora tenuto conto del Teorema di Ruffini e del Teorema di Gauss, si ha che:

$$\exists g(x) \in \mathbb{Z}[x] \text{ tale che } f(x) = (x-r)^2 \cdot g(x) = (x^2 + 2rx + r^2) \cdot g(x)$$

ovviamente per il teorema sul grado, si ha che $deg(g(x)) = deg(f(x)) - 2 = 1000$, e quindi è lecito scrivere:

$$g(x) = \sum_{i=0}^{1000} a_i x^i.$$

Sfruttando allora il principio di identità dei polinomi si ottiene che $r^2 a_0 = 210$, cioè $r^2 \mid 210$, e siccome $210 = 2 \cdot 3 \cdot 5 \cdot 7$, allora necessariamente $r \in \{-1, 1\}$. Tuttavia $f(-1) \neq 0, f(1) \neq 0$. Siamo quindi pervenuti a un assurdo, derivato dall'aver supposto che $f(x)$ avesse radici multiple in $\mathbb{Z}$, quindi $f(x)$ non ha radici multiple in $\mathbb{Z}$.

2. Si osserva subito che:

$$g(x) = x^{2p} + [4]_p x^p + [4]_p = (x^p)^2 + [2]_p \cdot [2]_p x + [2]_p^2 = (x^p + [2]_p)^2$$

inoltre, dal teorema binomiale sappiamo che:

$$\forall a, b \in \mathbb{Z} : \qquad (a+b)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^{p-k} b^k$$

tenuto quindi conto che

$$\forall k = 1, ..., p-1 : \qquad p \mid \left(\frac{p!}{k!(p-k)!} \right)$$

si deduce che:

$$\forall a, b \in \mathbb{Z}_p : \qquad (a+b)^p = a^p + b^p.$$

Pertanto, ricordando che per il teorema di Fermat: $[2]_p = [2]_p^p$, per quanto stabilito sopra si ha che:

$$g(x) = (x + [2]_p)^{2p}$$

la quale è la decomposizione di $g(x)$ in $\mathbb{Z}_p[x]$.

3. Sappiamo che

$$h(x) = x^{2p} + [4]_p x^p + [a]_p$$

sia quindi $y = x^p$. Allora

$$h(y) = y^2 + [4]_p y + [a]_p$$

Imponiamo che $h(y)$ abbia due radici distinte; allora dette α_1, α_2 tali radici, si ha che:

$$h(y) = (y - \alpha_1)(y - \alpha_2) = y^2 - (\alpha_1 + \alpha_2)y + \alpha_1\alpha_2$$

e quindi per il principio di identità dei polinomi si ha che:

$$\begin{cases} -(\alpha_1 + \alpha_2) = [4]_p \\ \alpha_1\alpha_2 = [a]_p \end{cases}$$

Tenuto conto che $\alpha_1 \neq \alpha_2$, una possibile scelta è $\alpha_1 = -[1]_p, \alpha_2 = -[3]_p$, e quindi $[a]_p = [3]_p$. A questo punto, sfruttando il teorema di Fermat, è semplice dedurre che

$$h(\alpha_1) = [0]_p \qquad h(\alpha_2) = [0]_p$$

dove $\alpha_1 = -[1]_p, \alpha_2 = -[3]_p, [a]_p = [3]_p$.

- Esercizio 2.3.4:

1. Sia $f(x) = x^5 + 5^{1313}x^4 + 3^{212}x^3 + 2^{44}x^2 + 3^{115}x + 7^{33} \in \mathbb{Z}[x]$. Provare che $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

2. Sia p un numero primo positivo, e sia

$$g(x) = x^{p^5} + x^{p^4} - x^{p^3} - x^{p^2} + x^{2p+1} - x^{2p} - x + [1]_p \in \mathbb{Z}_p[x].$$

Trovare tutte le radici di $g(x)$ in $\mathbb{Z}_p$, e provare che nessuna di esse è semplice.

Suggerimenti

- Per risolvere il punto 1. basta determinare un numero primo $p > 0$ in modo che la riduzione modulo p di $f(x)$ risulti irriducibile in $\mathbb{Z}_p[x]$.

- Per risolvere il punto 2. osservare che

$$\begin{aligned} g(x) &= x^{p^5} + x^{p^4} - x^{p^3} - x^{p^2} + x^{2p+1} - x^{2p} - x + [1]_p \\ &= (x^{p^2} - x)^{p^3} + (x^{p^2} - x)^{p^2} + (x + \overline{1})^p (x - \overline{1})^{p+1} \\ &= h(x)^{p^3} + h(x)^{p^2} + k(x) \end{aligned}$$

  e studiare singolarmente $h(x)$ e $k(x)$.

Svolgimento

1. Per verificare l'irriducibilità di $f(x)$ in $\mathbb{Q}[x]$ è sufficiente determinare un numero primo $p > 0$ in modo che la riduzione modulo p di $f(x)$ risulti irriducibile in $\mathbb{Z}_p[x]$. Procedendo per tentativi, potremmo cominciare considerando $p = 2$. In tal caso, sfruttando tra gli altri il teorema di Fermat, ricaviamo che la riduzione modulo p di $f(x)$ è:

$$\overline{f}(x) = x^5 + x^4 + x^3 + x + \overline{1} \in \mathbb{Z}_2[x]$$

   Ora, siccome $\overline{f}(\overline{0}) \neq \overline{0}$ e $\overline{f}(\overline{1}) \neq \overline{0}$, allora $\overline{f}(x)$ non ha radici in $\mathbb{Z}_2$. Se ne deduce, dato il grado di $f(x)$, che l'unica decomposizione ancora possibile è del tipo:

$$\overline{f}(x) = (x^3 + ax^2 + bx + c)(x^2 + dx + e)$$

   da cui, sfruttando il principio di identità dei polinomi, si ottiene il sistema:

$$\begin{cases} d = \overline{1} & (1) \\ e + ad + b = \overline{1} & (2) \\ ae + bd + c = \overline{0} & (3) \\ be + dc = \overline{1} & (4) \\ ce = \overline{1} & (5) \end{cases}$$

   Dalla (5) si ha che $(c, e) = (\overline{1}, \overline{1})$ (ricordiamo che in $\mathbb{Z}_2$: $\overline{1} = -\overline{1}$).
   Andando a sostituire $(c, e, d) = (\overline{1}, \overline{1}, \overline{1})$ nella (4) si ha $b = \overline{0}$, andando poi a sostituire nella (3) si ottiene che $a = \overline{1}$, sostituendo infine nella (2) si ricava che $\overline{0} = \overline{1}$, ma ciò è assurdo.
   Ne segue che $\overline{f}(x)$ è irriducibile in $\mathbb{Z}_2[x]$, e quindi $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

2. Si osserva quanto segue:

$$\begin{aligned} g(x) &= x^{p^5} + x^{p^4} - x^{p^3} - x^{p^2} + x^{2p+1} - x^{2p} - x + [1]_p \\ &= (x^{p^2} - x)^{p^3} + (x^{p^2} - x)^{p^2} + (x + \overline{1})^p (x - \overline{1})^{p+1} \\ &= h(x)^{p^3} + h(x)^{p^2} + k(x) \end{aligned}$$

   dove

$$h(x) = x^{p^2} - x, \qquad k(x) = (x + \overline{1})^p (x - \overline{1})^{p+1}$$

Sfruttando il teorema di Fermat si deduce che

$$\forall \alpha \in \mathbb{Z}_p : \qquad h(\alpha) = \overline{0}$$

da cui segue che l'insieme delle radici di $g(x)$ coincide con l'insieme delle radici di $k(x)$, e siccome l'insieme delle radici di $k(x)$ è $\{-\overline{1}, \overline{1}\}$, allora l'insieme delle radici di $g(x)$ in $\mathbb{Z}_p$ è $\{-\overline{1}, \overline{1}\}$. Vogliamo ora provare che queste radici non sono semplici. Siccome $-\overline{1}, \overline{1}$ sono radici di $h(x)$, allora per il teorema di Ruffini segue che:

$$\exists l(x) \in \mathbb{Z}_p[x] \text{ tale che } h(x) = (x+\overline{1})(x-\overline{1})l(x)$$

ragion per cui:

$$\begin{aligned} g(x) &= h(x)^{p^3} + h(x)^{p^2} + k(x) \\ &= ((x+\overline{1})(x-\overline{1})l(x))^{p^3} + ((x+\overline{1})(x-\overline{1})l(x))^{p^2} + k(x) \\ &= (x+\overline{1})^{p^3}(x-\overline{1})^{p^3} l(x)^{p^3} + (x+\overline{1})^{p^2}(x-\overline{1})^{p^2} l(x)^{p^2} + (x+\overline{1})^p (x-\overline{1})^{p+1} \\ &= (x+\overline{1})^p (x-\overline{1})^p m(x) \end{aligned}$$

dove

$$m(x) = \left[((x+\overline{1})(x-\overline{1}))^{p^3-p} l(x)^{p^3} + ((x+\overline{1})(x-\overline{1}))^{p^2-p} l(x)^{p^2} + (x-\overline{1}) \right]$$

e quindi $-\overline{1}, \overline{1}$ non sono radici semplici di $g(x)$.

- Esercizio 2.3.5: Sia $f(x) = x^8 + 2x^7 + 3x^6 + 2x^5 + 3x^4 + 4x^3 + 6x^2 + 4x + 2 \in \mathbb{R}[x]$.

1. Sia ω una radice cubica complessa e non reale di 1. Provare che ω è una radice multipla di $f(x)$.
2. Determinare una fattorizzazione di $f(x)$ in $\mathbb{R}[x]$.
3. Determinare una fattorizzazione in $\mathbb{Z}_3[x]$ della riduzione di $f(x)$ modulo 3.

Suggerimenti

- Per risolvere i primi due punti, ricordarsi delle formule di De Moivre, del teorema fondamentale dell'Algebra, e del fatto che se ho una radice complessa di un polinomio in $\mathbb{R}[x]$ di molteplicità m, allora anche il suo complesso coniugato è radice dello stesso polinomio con la stessa molteplicità.
- Per risolvere il terzo punto, sfruttare la decomposizione ottenuta nel primo punto.

Svolgimento

1. Sappiamo, dalle formule di De Moivre, che le radici cubiche di 1 sono le seguenti:

$$\omega_k := e^{i\frac{2k\pi}{3}} \qquad k = 0, ..., n-1$$

In particolare, le radici cubiche complesse e non reali di 1 sono:

$$\omega := \omega_1 = e^{i\frac{2\pi}{3}} = cos\left(\frac{2\pi}{3}\right) + isin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$\overline{\omega} = \omega_2 = e^{i\frac{4\pi}{3}} = cos\left(\frac{4\pi}{3}\right) + isin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Ora, poiché $f(x)$ è un polinomio a coefficienti in $\mathbb{R}$, allora è immediato verificare che ω è radice di molteplicità k di $f(x)$ in $\mathbb{C}$ se e solo se $\overline{\omega}$ è radice di molteplicità k di $f(x)$ in $\mathbb{C}$. Adesso, vogliamo provare che ω è radice multipla di $f(x)$; cioè se k è la presunta molteplicità di ω, allora vogliamo provare che $k \geq 2$; per far questo, è sufficiente verificare che $(x-\omega)^2 \mid f(x)$. In virtù di quanto sopra accennato, noi faremo un qualcosa di meglio: proveremo che $[(x-\omega)(x-\overline{\omega})]^2 \mid f(x)$.
Osserviamo che:

$$(x-\omega)(x-\overline{\omega}) = x^2 - 2\mathbb{R}e(\omega)x + |\omega|^2 = x^2 + x + 1$$

di conseguenza:

$$[(x-\omega)(x-\overline{\omega})]^2 = (x^2+x+1)^2 = x^4 + 2x^3 + 3x^2 + 2x + 1$$

ragion per cui effettuiamo la seguente divisione Euclidea:

x^8	$+2x^7$	$+3x^6$	$+2x^5$	$+3x^4$	$+4x^3$	$+6x^2$	$+4x$	$+2$	x^4	$+2x^3$	$+3x^2$	$+2x$	$+1$
$-x^8$	$-2x^7$	$-3x^6$	$-2x^5$	$-x^4$					x^4	$+2$			
				$2x^4$	$+4x^3$	$+6x^2$	$+4x$	$+2$					
				$-2x^4$	$-4x^3$	$-6x^2$	$-4x$	-2					
								0					

Poiché il resto è nullo, si ha che $[(x-\omega)(x-\overline{\omega})]^2 \mid f(x)$, e inoltre:

$$f(x) = g(x)^2 \cdot h(x)$$

dove:

$$g(x) := x^2 + x + 1 \qquad h(x) := x^4 + 2$$

2. Risulta semplice verificare che $g(x)$ non possiede radici in $\mathbb{R}$, e siccome il suo grado è minore o uguale a 3, possiamo allora applicare un noto corollario al teorema di Ruffini per asserire l'irriducibilità di $g(x)$ in $\mathbb{R}[x]$. A questo punto ci rimane soltanto da determinare una fattorizzazione di $h(x)$ in fattori irriducibili in $\mathbb{R}[x]$. Per far questo, possiamo agire in più modi:

   (a) Osserviamo che $h(x)$ non ha radici in $\mathbb{R}$, infatti:

   $$\forall \alpha \in \mathbb{R}: \qquad h(\alpha) > 0$$

   inoltre $h(x)$, avendo $deg(h(x)) \geq 3$, non può essere irriducibile in $\mathbb{R}[x]$. Pertanto:

$$\exists b, c, d, e \in \mathbb{R} \text{ tali che } h(x) = (x^2 + bx + c)(x^2 + dx + e)$$

Sviluppando il prodotto e sfruttando il principio di identità dei polinomi, si ottiene il sistema:

$$\begin{cases} ce = 2 & (1) \\ be + cd = 0 & (2) \\ e + bd + c = 0 & (3) \\ b + d = 0 & (4) \end{cases}$$

Dalla (4) si ha che $d = -b$, e andando a sostituire nella (2) deduciamo che $d(c - e) = 0$, e quindi si hanno due possibilità:

i. $d = 0$, allora abbiamo il sistema:

$$\begin{cases} ce = 2 \\ e + c = 0 \end{cases}$$

il quale non ammette soluzione reale;

ii. $c - e = 0$, allora abbiamo il sistema:

$$\begin{cases} c^2 = 2 \\ 2c - b^2 = 0 \end{cases}$$

il quale ha come unica soluzione $(c, b) = (\sqrt{2}, \sqrt{2\sqrt{2}})$, e andando a sostituire nelle precedenti equazioni ricaviamo che:

$$(b, c, d, e) = \left(\sqrt{2\sqrt{2}}, \sqrt{2}, -\sqrt{2\sqrt{2}}, \sqrt{2}\right)$$

Da quanto detto, ricaviamo infine la seguente fattorizzazione di $h(x)$ in fattori irriducibili in $\mathbb{R}[x]$:

$$h(x) = \left(x^2 + \sqrt{2\sqrt{2}}x + \sqrt{2}\right)\left(x^2 - \sqrt{2\sqrt{2}}x + \sqrt{2}\right)$$

(b) Oppure possiamo agire come segue: decomponiamo $h(x)$ in $\mathbb{C}[x]$, ossia determiniamo tutte le radici di $h(x)$ in $\mathbb{C}$ (ricordiamo infatti che per il teorema fondamentale dell'algebra $\mathbb{C}$ è un campo algebricamente chiuso), e poi le accoppiamo opportunamente per dedurre la decomposizione di $h(x)$ in $\mathbb{R}[x]$. Detto questo, osserviamo che le radici di $h(x)$ in $\mathbb{C}$ sono:

$$\alpha_k := \sqrt[4]{2} e^{i\frac{(2k+1)\pi}{4}} \qquad k = 0, ..., 3$$

in particolare, notiamo che:

$$\alpha_0 = \sqrt[4]{2}e^{i\frac{\pi}{4}} = \sqrt[4]{2}\left(cos\left(\frac{\pi}{4}\right) + isin\left(\frac{\pi}{4}\right)\right) = \sqrt[4]{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$$

$$\alpha_1 = \sqrt[4]{2}e^{i\frac{3\pi}{4}} = \sqrt[4]{2}\left(cos\left(\frac{3\pi}{4}\right) + isin\left(\frac{3\pi}{4}\right)\right) = \sqrt[4]{2}\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$$

$$\alpha_3 = \overline{\alpha_0} \qquad \alpha_2 = \overline{\alpha_1}$$

Detto questo, si ha che:

$$\begin{aligned} h(x) &= (x-\alpha_0)(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \\ &= (x-\alpha_0)(x-\overline{\alpha_0})(x-\alpha_1)(x-\overline{\alpha_1}) \\ &= (x^2 - 2\mathbb{R}e(\alpha_0)x + |\alpha_0|^2)(x^2 - 2\mathbb{R}e(\alpha_1)x + |\alpha_1|^2) \\ &= \left(x^2 + \sqrt{2\sqrt{2}}x + \sqrt{2}\right)\left(x^2 - \sqrt{2\sqrt{2}}x + \sqrt{2}\right) \end{aligned}$$

risultato, questo, del tutto analogo a quello trovato in precedenza.

3. Sia $\overline{f}(x)$ la riduzione di $f(x)$ modulo 3. Notiamo che, in base a quanto già visto, risulta:
$$\overline{f}(x) = \overline{g}(x)^2 \cdot \overline{h}(x)$$
dove $\overline{g}(x), \overline{h}(x)$ sono rispettivamente le riduzioni modulo 3 di $g(x), h(x)$. Restano quindi da determinare le decomposizioni in $\mathbb{Z}_3[x]$ di $\overline{g}(x)$ e $\overline{h}(x)$, la qual cosa viene lasciata per esercizio al lettore (risulta infatti sufficiente l'utilizzo opportuno del teorema di Ruffini, dei suoi corollari, e della divisione Euclidea).

- Esercizio 2.3.6: Si consideri in $\mathbb{Z}_3[x]$ il polinomio $f(x) = x^4 + \overline{2}$.

1. Si dica se l'anello $B = \mathbb{Z}_3[x]_{/(\overline{f})}$ è un campo e se ne determini l'ordine.
2. Si provi che $[x]$ è invertibile in B e si trovi il suo inverso.

Suggerimenti

- Per risolvere il primo punto, ricordarsi i risultati teorici sulle congruenze modulo un polinomio.
- Per risolvere il secondo punto, determinare il $MCD(x, \overline{f})$ e i relativi coefficienti di Bézout.

Svolgimento

1. Sappiamo, da un noto risultato, che l'anello B è un campo se e soltanto se il polinomio $\overline{f}(x)$ è irriducibile in $\mathbb{Z}_3[x]$. Si osserva che, nel nostro caso, il polinomio $\overline{f}(x)$ ha almeno una radice in $\mathbb{Z}_3$ (si ha infatti che $\overline{f}(\overline{1}) = \overline{0}$), quindi per il teorema di Ruffini si deduce subito che $x - \overline{1}$ divide $\overline{f}(x)$ in $\mathbb{Z}_3[x]$, e pertanto $\overline{f}(x)$ è riducibile in $\mathbb{Z}_3[x]$; da quanto premesso, si può adesso concludere che l'anello B non è un campo. Risulta altresì noto che, in generale, se $p > 0$ è primo e $\overline{g}(x) \in \mathbb{Z}_p[x]$, allora l'anello $\mathbb{Z}_p[x]_{/(\overline{g})}$ ha ordine $p^{deg(\overline{g})}$; quindi nel nostro caso possiamo stabilire che B ha ordine 3^4.

2. Sia $\overline{g}(x) \in \mathbb{Z}_3[x]$. Da una nota proposizione sappiamo che $[\overline{g}]$ è invertibile in B se e soltanto se $MCD(\overline{f}, \overline{g}) = \overline{1}$. Supponiamo adesso che $MCD(\overline{f}, \overline{g}) = \overline{1}$, allora dall'identità di Bézout sappiamo che

$$\exists | \overline{u}, \overline{v} \in \mathbb{Z}_3[x] \text{ tali che } \overline{u} \cdot \overline{f} + \overline{v} \cdot \overline{g} = \overline{1}$$

e quindi $\overline{f} \mid (\overline{v} \cdot \overline{g} - \overline{1})$, cioè

$$\overline{v} \cdot \overline{g} \equiv \overline{1} \qquad mod\ \overline{f}$$

e pertanto $[\overline{v}] = [\overline{g}]^{-1}$. Sappiamo che $\overline{u}, \overline{v}$ si dicono coefficienti di Bézout del $MCD(\overline{f}, \overline{g})$. La cosa che ci interessa, è che l'identità di Bézout vale per ogni massimo comune divisore, e che i relativi coefficienti possono essere ricavati (assieme al massimo comune divisore) attraverso un semplice algoritmo. Tale algoritmo vale in ogni dominio Euclideo, e quindi in particolare vale in $\mathbb{Z}$ e in $K[x]$, dove K è un campo. Consideriamo $A = \mathbb{Z}$, oppure $A = K[x]$ con K campo. Sia 0 l'elemento neutro della somma, e 1 l'elemento neutro del prodotto di A. Consideriamo $a, b \in A$. Vogliamo determinare un massimo comune divisore di (a, b) e i relativi coefficienti di Bézout. Per farlo, poniamo:

$$X_0 = 1 \qquad Y_0 = 0 \qquad U_0 = 0 \qquad V_0 = 1$$

e poi definiamo:

$$A_0 = X_0 \cdot a + Y_0 \cdot b \qquad B_0 = U_0 \cdot a + V_0 \cdot b$$

Sia ora $i \in \mathbb{N}$, e supponiamo di avere definito $X_i, Y_i, U_i, V_i, q_i, A_i, B_i$. Per il lemma di divisione Euclidea sappiamo che:

$$\exists | q_{i+1}, r_{i+1} \in A \text{ tali che } A_i = B_i \cdot q_{i+1} + r_{i+1}, \text{ e } r_{i+1} = 0 \text{ oppure } 0 < \nu(r_{i+1}) < \nu(B_i)$$

dove ν è il valore assoluto se $A = \mathbb{Z}$, mentre $\nu = deg$ nel caso in cui $A = K[x]$.
Definiamo ora:

$$X_{i+1} = U_i \qquad Y_{i+1} = V_i \qquad U_{i+1} = X_i - U_i \cdot q_{i+1} \qquad V_{i+1} = Y_i - V_i \cdot q_{i+1}$$

$$A_{i+1} = B_i \qquad B_{i+1} = r_{i+1}$$

Si osserva in particolare che

$$A_i = X_i \cdot a + Y_i \cdot b \qquad B_i = U_i \cdot a + V_i \cdot b$$

e si può provare che:

$$MCD(A_{i+1}, B_{i+1}) = MCD(A_i, B_i)$$

Adesso, tenuto conto che:

$$B_i = 0 \text{ oppure } 0 < \nu(B_{i+1}) < \nu(B_i)$$

se ne deduce che il seguente insieme è non vuoto:

$$\{i \in \mathbb{N} \mid B_i = 0\}$$

e dunque possiamo definire:

$$j := min\,\{i \in \mathbb{N} \mid B_i = 0\}$$

allora si può dimostrare che A_j è un massimo comune divisore di (a, b) (ma non il solo), e inoltre:

$$A_j = X_j \cdot a + Y_j \cdot b$$

cioè X_j, Y_j sono i coefficienti di Bézout del massimo comune divisore A_j (rimarchiamo che il massimo comune divisore non è unico).
Applichiamo ora questo algoritmo nel nostro caso, cioè con:

$$A = \mathbb{Z}_3[x] \qquad a = \overline{f} \qquad b = x$$

con questi dati, il suddetto algoritmo viene riassunto nella seguente tabella:

i	q_i	A_i	B_i	X_i	Y_i	U_i	V_i
0		$\overline{f}$	x	$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{1}$
1	x^3	x	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{1}$	$-x^3$
2	$-x$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$-x^3$	x	$\overline{1} - x^4$

e dunque un massimo comune divisore di $(\overline{f}, x)$ è:

$$\overline{2} = \overline{1} \cdot \overline{f} - x^3 \cdot x$$

e siccome $\overline{2} \in U(\mathbb{Z}_3)$, allora:

$$\overline{2}^{-1} \cdot \overline{2} = \overline{2}^{-1} \cdot (\overline{1} \cdot \overline{f} - x^3 \cdot x)$$

per cui, essendo $\overline{2}^{-1} = \overline{2}$, sviluppando i calcoli abbiamo che:

$$\overline{1} = \overline{2} \cdot \overline{f} + x^3 \cdot x$$

Di conseguenza: $\overline{f} \mid (x^3 \cdot x - \overline{1})$, cioè

$$x^3 \cdot x \equiv \overline{1} \qquad mod\ \overline{f}$$

e pertanto $[x]$ è invertibile e $[x]^{-1} = [x^3]$.

2.4 Due esercizi molto significativi

Per concludere, diamo ora un paio di esercizi dai molteplici significati. Il primo ci consentirà di porci alcune importanti domande, alle quali si darà risposta durante il corso di Algebra 2 (e da questo punto di vista tale esercizio ci apre la porta della Teoria dei Campi). Il secondo, invece, mette in relazione risultati teorici provenienti da diverse "branche" della Matematica, in particolare l'Algebra e la Geometria, e ci fa capire come nessuna materia risulta essere a sè stante. Per entrambi questi esercizi non daremo suggerimenti.

- Esercizio 2.4.1: Dire se può esistere un campo avente esattamente 9 elementi, e in caso affermativo determinarne un esempio.

Svolgimento

Risulta noto, in generale, che se $p > 0$ è primo e $f(x) \in \mathbb{Z}_p[x]$, allora l'anello $\mathbb{Z}_p[x]_{/(f)}$ ha ordine $p^{deg(f)}$. Inoltre sappiamo, in generale, che se K è un campo, e se $f(x) \in K[x]$, allora $K[x]_{/(f)}$ è un campo se e soltanto se $f(x)$ è irriducibile in $K[x]$. Vogliamo sapere se può esistere un campo avente esattamente 9 elementi. Osserviamo che $9 = 3^2$. Cerchiamo quindi di accoppiare i precedenti risultati al fine di rispondere (positivamente) al quesito. Nella fattispecie, ci basterà determinare un polinomio $f(x) \in \mathbb{Z}_3[x]$, che sia irriducibile in $\mathbb{Z}_3$ e che abbia $deg(f) = 2$. Avremo allora che $\mathbb{Z}_3[x]_{/(f)}$ sarà un campo con 9 elementi. Adesso, per un noto corollario al teorema di Ruffini, sappiamo che i polinomi irriducibili in $\mathbb{Z}_3[x]$ aventi grado 2 sono tutti e soli i polinomi di grado 2 in $\mathbb{Z}_3[x]$ che non abbiano radici in $\mathbb{Z}_3$. Cerchiamo quindi un polinomio $f(x) \in \mathbb{Z}_3[x]$ che non abbia radici in $\mathbb{Z}_3$ e che abbia grado 2. Per trovarlo, si può procedere per tentativi. Risulta semplice far vedere che

$$f(x) = x^2 + [1]_3 \in \mathbb{Z}_3[x]$$

è adatto al nostro scopo. Dunque si ha effettivamente che esiste un campo avente esattamente 9 elementi, e $\mathbb{Z}_3[x]_{/(f)}$ ne è un esempio.

In base ai risultati richiamati, sorgono spontanee alcune domande:

1. Dato un primo $p > 0$ e un numero naturale $n > 0$, esiste sempre un campo avente p^n elementi?
2. Dato un campo finito con ordine m, esistono un primo p e un numero naturale n tali che $m = p^n$?
3. Se le risposte ai precedenti quesiti sono positive, possiamo dire che, a meno di isomorfismi di campi, esiste un unico campo finito con p^n elementi?
4. Se le risposte ai precedenti quesiti sono positive, quale sarebbe il significato algebrico di p e geometrico di n?

Se siete impazienti e ambiziosi, potete provare a rispondere alle suddette (difficili) domande da soli. Male che vada potrete comunque attendere il prossimo corso di Algebra 2 per

togliervi i dubbi.

- Esercizio 2.4.2: Provare che $\mathbb{R}$ è un $\mathbb{Q}$-spazio vettoriale, e determinare la $dim_{\mathbb{Q}}(\mathbb{R})$.

Svolgimento

Si lascia al lettore la prova che $\mathbb{R}$ è un $\mathbb{Q}$-spazio vettoriale. Dimostriamo adesso che $dim_{\mathbb{Q}}(\mathbb{R}) = \infty$. Consideriamo $n \in \mathbb{N}$, $n > 1$, con n dispari. Per il Criterio di Eisenstein esiste un polinomio $f(x) \in \mathbb{Z}[x]$ che sia irriducibile in $\mathbb{Q}[x]$ e che abbia grado n. Adesso, sappiamo che:

$$\mathbb{Q}[x]_{/(f)} = \{[q_{n-1}x^{n-1} + ... + q_0] \mid q_{n-1}, ..., q_0 \in \mathbb{Q}\}$$

In base a questo, si lascia al lettore la verifica che $\mathbb{Q}[x]_{/(f)}$ è un $\mathbb{Q}$-spazio vettoriale con $dim_{\mathbb{Q}}(\mathbb{Q}[x]_{/(f)}) = n$. Adesso, essendo $n > 1$ un numero dispari, sicuramente esiste α radice di $f(x)$ in $\mathbb{R}$. Definiamo ora l'applicazione:

$$\phi : \mathbb{Q}[x]_{/(f)} \to \mathbb{R} : [g(x)] \mapsto \phi(x) = g(\alpha)$$

Si lascia al lettore la prova che ϕ è un omomorfismo di $\mathbb{Q}$-spazi vettoriali ben definito. Adesso, dal teorema del rango sappiamo che:

$$dim_{\mathbb{Q}}(Im\phi) + dim_{\mathbb{Q}}(Ker\phi) = dim_{\mathbb{Q}}(\mathbb{Q}[x]_{/(f)})$$

Notiamo che $dim_{\mathbb{Q}}(Ker\phi) = 0$. Infatti, se $[g] \in Ker\phi$, allora $g(\alpha) = 0$, dunque per il teorema di Ruffini $(x - \alpha)$ divide $g(x)$ in $\mathbb{R}[x]$. Sappiamo pure che $f(\alpha) = 0$, e dunque sempre per il teorema di Ruffini si ha che $(x - \alpha)$ divide $f(x)$ in $\mathbb{R}[x]$. Pertanto $(x - \alpha)$ divide il $MCD(f, g)$ in $\mathbb{R}[x]$. Si lascia ora al lettore la prova che se $a, b \in \mathbb{Q}[x]$, allora:

$$MCD(a, b) = 1 \text{ in } \mathbb{Q}[x] \iff MCD(a, b) = 1 \text{ in } \mathbb{R}[x]$$

Adesso, siccome sappiamo che $MCD(f, g) \neq 1$ in $\mathbb{R}[x]$, per quanto sopra segue immediatamente che $MCD(f, g) \neq 1$ in $\mathbb{Q}[x]$, cioè $[g] \notin U(\mathbb{Q}[x]_{/(f)})$, e questo in quanto:

$$U(\mathbb{Q}[x]_{/(f)}) = \{[h] \mid MCD(f, h) = 1\}$$

Ora, essendo $f(x)$ irriducibile in $\mathbb{Q}[x]$, allora $\mathbb{Q}[x]_{/(f)}$ risulta essere un campo, e quindi $U(\mathbb{Q}[x]_{/(f)}) = \mathbb{Q}[x]_{/(f)} - \{[0]\}$. Di conseguenza $[g] = [0]$, e pertanto $Ker\phi = \{[0]\}$.
In base a quanto detto, si ha che $dim_{\mathbb{Q}}(Im\phi) = n$, e siccome $Im\phi$ è un $\mathbb{Q}$-sottospazio vettoriale di $\mathbb{R}$, allora $dim_{\mathbb{Q}}(\mathbb{R}) \geq dim_{\mathbb{Q}}(Im\phi)$, ovvero $dim_{\mathbb{Q}}(\mathbb{R}) \geq n$. Data l'arbitrarietà di n, segue allora che $dim_{\mathbb{Q}}(\mathbb{R}) = \infty$.

L'esercizio, ora completo, ci fa capire come in realtà la Matematica non si componga di diverse branche (dando l'idea che ognuna non abbia a che fare con le altre) bensì si compone di idee, e che l'unione di queste idee è la sua vera forza.

Bibliografia

[1] M. Barile, Dispense di Algebra, http://www.dm.uniba.it/∼barile/Rete/indice.htm