**ALGEBRA 1 - Quarto appello scritto**

8 luglio 2021

soluzioni

1. Determinare quanti siano gli elementi di ordine $3$ nel gruppo moltiplicativo $\mathbb{Z}/(35)^\times$.

   *Soluzione:*

   Il gruppo $\mathbb{Z}/(35)^\times$ ha ordine $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$ ed è abeliano. Possiede pertanto un unico (poiché normale!) 3-Sylow che contiene tutti gli elementi il cui ordine è una potenza di $3$.

   Dalla fattorizzazione $24 = 2^3 \cdot 3$, si conclude subito che tale 3-Sylow ha ordine $3$, e contiene quindi l'identità del gruppo e due elementi di ordine $3$. In conclusione, gli elementi di ordine $3$ nel gruppo moltiplicativo $\mathbb{Z}/(35)^\times$ sono esattamente due.

   Chiaramente, è possibile calcolare il numero degli elementi di ordine $3$ anche risolvendo la congruenza $x^3 \equiv 1 \mod 35$, dopo averla magari separata in congruenze modulo $5$ e $7$ attraverso il Teorema cinese dei resti.

2. Mostrare che un gruppo di ordine $45$ è necessariamente abeliano. Esibire un tale gruppo che non sia ciclico.

   *Soluzione:* Se $|G| = 45 = 3^2 \cdot 5$, il Teorema di Sylow ci spiega che il numero dei 3-Sylow di $G$ è congruo ad $1$ modulo $5$ e divide $45$; inevitabilmente, il 3-Sylow $P$ è allora unico. Allo stesso modo si vede che anche il $5$-Sylow $Q$ è unico, e quindi normale.

   Poiché $|P| = 9, |Q| = 5$, l'intersezione $P \cap Q$ ha ordine $1$ per il Teorema di Lagrange, e $G$ è prodotto diretto dei sottogruppi normali $P$ e $Q$. Di conseguenza, $G$ è isomorfo a $P \times Q$.

   Ora, un gruppo di ordine primo è necessariamente ciclico, e quindi $Q \simeq \mathrm{C}_5$. Un gruppo il cui ordine è il quadrato di un primo è sempre abeliano, e quindi $P$ è abeliano, ed è isomorfo a $\mathrm{C}_9$ oppure a $\mathrm{C}_3 \times \mathrm{C}_3$. In ogni caso, $G$ è abeliano in quanto prodotto diretto di gruppi abeliani. Più precisamente, $G$ è isomorfo a $\mathrm{C}_5 \times \mathrm{C}_9 \simeq \mathrm{C}_{45}$ nel primo caso, e a $\mathrm{C}_5 \times (\mathrm{C}_3 \times \mathrm{C}_3) \simeq \mathrm{C}_{15} \times \mathrm{C}_3$ nel secondo.

   Tale gruppo non può essere ciclico poiché non possiede elementi di ordine $45$.

3. Sia $A$ un anello commutativo con unità. Mostrare che il sottoinsieme

$$N = \{a \in A \,|\, a^n = 0 \text{ per qualche } n \in \mathbb{N}\}$$

è un ideale di $A$. Calcolare $N$ quando $A = \mathbb{Z}/(12)$.

*Soluzione:* $N$ è non vuoto in quanto $0 \in N$. Assorbe inoltre la moltiplicazione per elementi di $A$ in quanto

$$a \in A, x \in N \implies (ax)^n = a^n x^n = a^n 0$$

non appena $x^n = 0$; in particolare $(-x)^n = ((-1)x)^n = 0$. Rimane da mostrare che $N$ sia chiuso rispetto alla somma. In effetti, se $x^m = y^n = 0$, allora

$$(x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n}$$

e in nessun termine della sommatoria è possibile che l'esponente $i$ sia inferiore a $m$ e contemporaneamente l'esponente $m+n-i$ sia inferiore a $n$, dal momento che la loro somma è $m+n$. Pertanto $(x+y)^{m+n} = 0$[1].

E' importante notare che abbiamo utilizzato la formula della potenza del binomio, che vale per la commutatività del prodotto (siamo in un anello commutativo!).

Quando $A = \mathbb{Z}/(12)$, gli elementi di $N$ sono quegli $\overline{x}, x \in \mathbb{Z}$, che soddisfano $x^n \equiv 0 \mod 12$, cioè quegli interi una cui potenza è multipla di 12: per il Teorema di fattorizzazione unica, questi sono esattamente i multipli di 6 e quindi $N = (\overline{6}) = \{\overline{0}, \overline{6}\}$.

[1] L'esponente $m+n$ non è ottimale. La dimostrazione funziona anche con $m+n-1$

4. Dire per quali valori naturali di $n > 1$ l'applicazione

$$\mathbb{Z}[i] \ni a + bi \mapsto a + b \in \mathbb{Z}/(n)$$

sia un omomorfismo di anelli.

*Soluzione:* Indichiamo con $\phi$ l'applicazione data. Affinché $\phi$ sia un omomorfismo di anelli deve valere

$$ac + ad + bc - bd = \phi((ac - bd) + (ad + bc)i) = \phi((a + bi)(c + di)) \equiv$$
$$\equiv \phi(a + bi)\phi(c + di) = (a + b)(c + d) = ac + ad + bc + bd \mod n$$

o in altre parole $2bd \equiv 0 \mod n$ per ogni scelta di $a, b, c, d \in \mathbb{Z}$. Poiché possiamo scegliere $b = d = 1$, questo forza $2 \equiv 0 \mod n$ e quindi $n|2 \implies n = 2$. Viceversa, se $n = 2$, allora $2bc$ è sicuramente congruo a $0$ modulo $2$.

In conclusione, l'unica scelta di $n$ che può rendere l'applicazione un omomorfismo di anelli è $n = 2$. Lascio a voi la verifica che se $n = 2$ tutte le altre proprietà di un omomorfismo sono soddisfatte.

5. Sia $\alpha$ una radice complessa del polinomio $x^4 + x + 1 \in \mathbb{Q}[x]$.

   - Calcolare $[\mathbb{Q}(\alpha) : \mathbb{Q}]$;
   - Calcolare $[\mathbb{Q}(\alpha^2) : \mathbb{Q}]$.

   *Soluzione:* Il polinomio $f(x) = x^4 + x + 1$ è sicuramente irriducibile in $\mathbb{Q}[x]$. In effetti, le sue uniche possibili radici razionali sono $\pm 1$ per un criterio visto a lezione, e si vede subito che non soddisfano il polinomio.

   Per quanto riguarda la possibilità che si spezzi nel prodotto di due polinomi di grado 2, possiamo innanzitutto supporre, per il Lemma di Gauss, che tali polinomi abbiano coefficienti interi. Allora, da $x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$ si ottiene

$$\begin{cases} a + c = 0 \\ b + d + ac = 0 \\ ad + bc = 1 \\ bd = 1. \end{cases}$$

   Dalla prima si ricava $c = -a$, che sostituito nella terza fornisce $a(d-b) = 1$. Tuttavia $bd = 1$ ha le sole soluzioni intere $b = d = \pm 1$ e quindi $d - b = 0$, da cui un assurdo.

   Una volta stabilita l'irriducibilità di $f(x)$ su $\mathbb{Q}$, otteniamo che $f(x)$ è il polinomio minimo di $\alpha$ su $\mathbb{Q}$ e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ coincide con il grado di $f(x)$ e deve valere $4$.

   Per quanto riguarda il secondo punto, osserviamo che $(\alpha^2)^2 = \alpha^4 = -(1 + \alpha)$ e quindi $\alpha = -(\alpha^2)^2 - 1$. In altre parole, $\alpha \in \mathbb{Q}(\alpha^2)$ e quindi $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha^2)$. L'inclusione opposta è ovvia, e quindi $\mathbb{Q}(\alpha)$ coincide con $\mathbb{Q}(\alpha^2)$. Pertanto $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4$.