Corso di Algebra 1 - a.a. 2017-2018

Prova scritta del 19/06/2018

1. Dato un gruppo G, sia

$$N := \{a \in G : \langle a \rangle \text{ è normale in } G\}$$

   (a) Dimostrare che $N = G$ se e solo se ogni sottogruppo di G è normale.

   (b) Dimostrare che $\langle a \rangle \subseteq N$ per ogni $a \in N$.

   (c) Dimostrare che N non è un sottogruppo di G se $G = \mathbb{Z}/3\mathbb{Z} \times D_3$.

2. Trovare, se esiste, $\sigma \in G$ tale che $\sigma(1,2,3)\sigma^{-1} = (2,3,4)$ in ciascuno dei seguenti casi:

   (a) $G = S_4$;

   (b) $G = A_4$;

   (c) $G = A_5$.

3. Nell'anello $\mathbb{Z}^{\mathbb{Z}}$ delle funzioni da $\mathbb{Z}$ a $\mathbb{Z}$ si consideri il sottoinsieme

$$I := \{f \in \mathbb{Z}^{\mathbb{Z}} : f(n) \in n\mathbb{Z} \text{ per ogni } n \in \mathbb{Z}\}.$$

   (a) Dimostrare che I è un ideale di $\mathbb{Z}^{\mathbb{Z}}$.

   (b) Dimostrare che l'immagine di $f \in \mathbb{Z}^{\mathbb{Z}}$ nell'anello quoziente $\mathbb{Z}^{\mathbb{Z}}/I$ è invertibile se e solo se $\mathrm{mcd}(n, f(n)) = 1$ per ogni $n \in \mathbb{Z}$.

   (c) Esiste un omomorfismo di anelli $\mathbb{Z}^{\mathbb{Z}}/I \to \mathbb{Z}$?

4. Dati due numeri primi p e q, si consideri il polinomio $f := X^p - pX - q$.

   (a) Dimostrare che, se $p = q$, allora f è irriducibile in $\mathbb{Z}[X]$.

   (b) Dimostrare che, se $p = 2$ o $p = 3$, allora esiste unico q tale che f sia riducibile in $\mathbb{Z}[X]$.

   (c) Esistono p e q tali che f sia irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$?

Soluzioni

1. (a) È ovvio che, se ogni sottogruppo di G è normale, in particolare $\langle a\rangle$ è normale per ogni $a \in G$, cioè $N = G$. Viceversa, supponiamo $N = G$ e sia H un sottogruppo di G. Per ogni $g \in G$ e per ogni $a \in H$ si ha $gag^{-1} \in \langle a\rangle$ (perché $a \in N = G$, quindi $\langle a\rangle$ è normale in G). D'altra parte, $\langle a\rangle \subseteq H$ (essendo $a \in H$ e H sottogruppo di G), e dunque $gag^{-1} \in H$, il che dimostra che H è normale in G.

   (b) Va dimostrato che $a^n \in N$ (cioè che $\langle a^n\rangle$ è normale in G) per ogni $a \in N$ e per ogni $n \in \mathbb{Z}$. In effetti per ogni $g \in G$ esiste $i \in \mathbb{Z}$ tale che $gag^{-1} = a^i$ (perché $\langle a\rangle$ è normale in G). Se ne deduce che per ogni $k \in \mathbb{Z}$

   $$g(a^n)^k g^{-1} = ga^{nk}g^{-1} = (gag^{-1})^{nk} = (a^i)^{nk} = a^{ink} = (a^n)^{ik} \in \langle a^n\rangle,$$

   e quindi $\langle a^n\rangle$ è normale in G.

   (c) Basta trovare $a, b \in N$ tali che $ab \notin N$. Si può prendere per esempio $a := (\overline{1}, 1)$ e $b := (\overline{0}, R)$. Risulta infatti $\langle a\rangle = \mathbb{Z}/3\mathbb{Z} \times \{1\}$ e $\langle b\rangle = \{\overline{0}\} \times \langle R\rangle$, ed entrambi sono normali in G, dato che $\mathbb{Z}/3\mathbb{Z}$, $\{\overline{0}\}$ sono normali in $\mathbb{Z}/3\mathbb{Z}$, che $\{1\}$, $\langle R\rangle$ sono normali in D_3, e che (come è immediato verificare) in un prodotto di gruppi il prodotto di sottogruppi normali è normale. Invece

   $$\langle ab\rangle = \langle(\overline{1}, R)\rangle = \{(\overline{0}, 1), (\overline{1}, R), (\overline{2}, R^2)\}$$

   non è normale in G, in quanto $g := (\overline{0}, S) \in G$ è tale che

   $$gabg^{-1} = (\overline{0}, S)(\overline{1}, R)(\overline{0}, S)^{-1} = (\overline{1}, SRS^{-1}) = (\overline{1}, R^2) \notin \langle ab\rangle.$$

2. Ricordiamo preliminarmente che $\sigma(1, 2, 3)\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$ per ogni $\sigma \in S_n$.

   (a) Si può prendere $\sigma = (1, 4)$. Infatti

   $$(1, 4)(1, 2, 3)(1, 4)^{-1} = (4, 2, 3) = (2, 3, 4).$$

   (b) Non esiste $\sigma \in A_4$ tale che $\sigma(1, 2, 3)\sigma^{-1} = (2, 3, 4)$. Per vederlo basta osservare che il 3-ciclo $(2, 3, 4)$ può essere scritto in 3 modi (cioè anche come $(3, 4, 2)$ o $(4, 2, 3)$) e che corrispondentemente ci sono 3 soluzioni σ di tale equazione in S_4, date da

   $$\begin{aligned}
   &\sigma(1) = 2 \quad \sigma(2) = 3 \quad \sigma(3) = 4 \quad (\text{e quindi } \sigma(4) = 1),\\
   &\sigma(1) = 3 \quad \sigma(2) = 4 \quad \sigma(3) = 2 \quad (\text{e quindi } \sigma(4) = 1),\\
   &\sigma(1) = 4 \quad \sigma(2) = 2 \quad \sigma(3) = 3 \quad (\text{e quindi } \sigma(4) = 1).
   \end{aligned}$$

Le soluzioni sono dunque $(1,2,3,4)$, $(1,3,2,4)$ e (come già visto nel punto precedente) $(1,4)$, e sono tutte in $S_4 \setminus A_4$.

(c) Si può prendere $\sigma = (1,4,5)$. Infatti

$$(1,4,5)(1,2,3)(1,4,5)^{-1} = (4,2,3) = (2,3,4).$$

3. (a) Chiaramente I contiene la funzione identicamente nulla, per cui $I \neq \emptyset$. Se $f, g \in I$ e $h \in \mathbb{Z}^{\mathbb{Z}}$, allora $(f+g)(n) = f(n) + g(n) \in n\mathbb{Z}$ e $(fh)(n) = f(n)h(n) \in n\mathbb{Z}$ (essendo $n\mathbb{Z}$ un ideale di $\mathbb{Z}$) per ogni $n \in \mathbb{Z}$, il che dimostra che $f+g, fh \in I$.

(b) Indicando con $\mathbf{1}$ l'elemento neutro moltiplicativo di $\mathbb{Z}^{\mathbb{Z}}$ (definito da $\mathbf{1}(n) := 1$ per ogni $n \in \mathbb{Z}$), l'immagine $\overline{f} \in \mathbb{Z}^{\mathbb{Z}}/I$ di $f \in \mathbb{Z}^{\mathbb{Z}}$ è invertibile se e solo se esiste $g \in \mathbb{Z}^{\mathbb{Z}}$ tale che $\overline{f}\overline{g} = \overline{\mathbf{1}}$. Tale uguaglianza equivale a $fg - \mathbf{1} \in I$, cioè $f(n)g(n) - 1 \in n\mathbb{Z}$ per ogni $n \in \mathbb{Z}$. Dunque $\overline{f}$ è invertibile se e solo se, per ogni $n \in \mathbb{Z}$, esistono $x, y = g(n) \in \mathbb{Z}$ tali che $nx + f(n)y = 1$, e questa equazione ha soluzione se e solo se $\mathrm{mcd}(n, f(n)) = 1$.

(c) Sì. Infatti $\alpha\colon \mathbb{Z}^{\mathbb{Z}} \to \mathbb{Z}$ definito da $\alpha(f) := f(0)$ è un omomorfismo di anelli, dato che

$$\alpha(f+g) = (f+g)(0) = f(0) + g(0) = \alpha(f) + \alpha(g),$$
$$\alpha(fg) = (fg)(0) = f(0)g(0) = \alpha(f)\alpha(g)$$

e $\alpha(\mathbf{1}) = 1$. Inoltre $I \subseteq \ker(\alpha)$ (se $f \in I$, allora $\alpha(f) = f(0) = 0$, cioè $f \in \ker(\alpha)$). Per il teorema di omomorfismo, α induce allora un omomorfismo di anelli $\mathbb{Z}^{\mathbb{Z}}/I \to \mathbb{Z}$ (definito da $\overline{f} \mapsto \alpha(f)$).

4. (a) Se $p = q$, $f = X^p - pX - p$ è irriducibile in $\mathbb{Z}[X]$ per il criterio di Eisenstein relativo al primo p.

(b) Essendo di grado 2 o 3, in entrambi i casi f è riducibile in $\mathbb{Z}[X]$ (o equivalentemente in $\mathbb{Q}[X]$) se e solo se ha una radice razionale, che può assumere solo i valori $\pm 1, \pm q$. Inoltre 1 non può mai essere radice perché $f(1) = 1 - p - q < 0$.

Se $p = 2$ (per cui $f = X^2 - 2X - q$), risulta $f(-1) = 3 - q$ (quindi -1 è radice se e solo se $q = 3$), $f(q) = q^2 - 3q = q(q-3)$ (quindi q è radice se e solo se $q = 3$) e $f(-q) = q^2 + q > 0$ (quindi $-q$ non è mai radice). Si conclude allora che, se $p = 2$, f è riducibile se e solo se $q = 3$.

Se $p = 3$ (per cui $f = X^3 - 3X - q$), risulta $f(-1) = 2 - q$ (quindi -1 è radice se e solo se $q = 2$), $f(q) = q^3 - 4q = q(q-2)(q+2)$

(quindi q è radice se e solo se $q = 2$) e $f(-q) = -q^3 + 2q = q(2 - q^2) < 0$ (quindi $-q$ non è mai radice). Si conclude allora che, se $p = 3$, f è riducibile se e solo se $q = 2$.

(c) No. Infatti $f = X^p - \overline{q} \in \mathbb{Z}/p\mathbb{Z}[X]$ ha sempre la radice $\overline{q}$ (per il piccolo teorema di Fermat).