Corso di Algebra 1 - a.a. 2015-2016

Prova scritta del 14.6.2016

1. Sia G un gruppo e, per ogni numero primo p, sia

$$G_p := \{g \in G \,:\, g^{p^n} = 1 \text{ per qualche } n \in \mathbb{N}\}.$$

   (a) Dimostrare che $G_p \cap G_q = \{1\}$ se p e q sono primi distinti.

   (b) Dimostrare che se G contiene elementi non banali di ordine finito, allora esiste un primo p tale che $G_p \neq \{1\}$.

   (c) Dimostrare che se G è abeliano, allora G_p è un sottogruppo di G per ogni primo p.

2. Sia G un gruppo e consideriamo la seguente relazione $\mathcal{R}$ su G: dati $g, h \in G$ definiamo

$$g \,\mathcal{R}\, h \iff g = xhx \text{ per qualche } x \in G.$$

   (a) Dimostrare che se G è abeliano, allora $\mathcal{R}$ è una relazione di equivalenza su G.

   (b) Dimostrare che $1 \,\mathcal{R}\, g$ se e solo se $g = y^2$ per qualche $y \in G$.

   (c) Stabilire se $1 \,\mathcal{R}\, g$ quando $G = S_6$ e $g = (12)(3456)$.

   (d) Determinare le classi di $\mathcal{R}$-equivalenza quando $G = \mathbb{Z}/5\mathbb{Z}$ e quando $G = \mathbb{Z}/4\mathbb{Z}$.

3. Sia A un anello commutativo, B un suo sottoanello e $b \in B$.

   (a) Dimostrare che $Bb \subseteq Ab \cap B$.

   (b) Dimostrare che $Bb = Ab \cap B$ se $A = B[X]$.

   (c) Fornire un esempio in cui $Bb \subsetneq Ab \cap B$.

4. Si consideri il polinomio $p(X) = X^3 + aX + 1 \in \mathbb{Z}[X]$, con $a > 0$. Dire per ciascuna delle seguenti affermazioni se è vera o falsa.

   (a) p è irriducibile su $\mathbb{Z}$.

   (b) Se p è irriducibile su $\mathbb{Z}/3\mathbb{Z}$, allora $a \equiv 2 \mod 3$.

   (c) Se $p - 2X$ è riducibile su $\mathbb{Z}$, allora $(p-2X)^3 - 3X + 2$ è riducibile su $\mathbb{Z}$.

Soluzioni

1. Preliminarmente osserviamo che $g \in G_p$ se e solo se $\mathrm{ord}(g) = p^m$ per qualche $m \in \mathbb{N}$. Infatti, se $\mathrm{ord}(g) = p^m$, allora $g^{p^m} = 1$ e quindi $g \in G_p$. Viceversa, se $g \in G_p$, allora esiste $n \in \mathbb{N}$ tale che $g^{p^n} = 1$. Ciò implica che $\mathrm{ord}(g) \mid p^n$, e dunque $\mathrm{ord}(g) = p^m$ per qualche $0 \leq m \leq n$.

   (a) Per quanto appena detto, $g \in G_p \cap G_q$ se e solo se $\mathrm{ord}(g)$ è una potenza sia di p che di q, e chiaramente questo succede se e solo se $\mathrm{ord}(g) = 1 = p^0 = q^0$. Dato che in un gruppo l'elemento neutro è l'unico elemento di ordine 1, concludiamo che $G_p \cap G_q = \{1\}$.

   (b) Se $1 \neq a \in G$ ha ordine n, deve essere $n > 1$, per cui esiste un primo p tale che $p \mid n$. Posto $b := a^{\frac{n}{p}}$, risulta $\mathrm{ord}(b) = p$ (perché $b \neq 1$ e $b^p = a^n = 1$), e quindi $b \in G_p$.

   (c) Chiaramente $1 \in G_p$. Dati $a, b \in G_p$, per definizione esistono $m, n \in \mathbb{N}$ tali che $a^{p^m} = b^{p^n} = 1$. Indicando con l il massimo tra m e n e tenendo conto che G è abeliano, si ottiene

   $$(ab^{-1})^{p^l} = a^{p^l} b^{-p^l} = (a^{p^m})^{p^{l-m}} (b^{p^n})^{-p^{l-n}} = 1^{p^{l-m}} 1^{-p^{l-n}} = 1,$$

   il che dimostra che $ab^{-1} \in G_p$.

2. (a) Osserviamo che, anche senza assumere che G sia abeliano, $\mathcal{R}$ risulta riflessiva (cioè $g \mathcal{R} g$ per ogni $g \in G$) e simmetrica (cioè $g \mathcal{R} h$ implica $h \mathcal{R} g$). Infatti $g = 1g1$ e, se $g = xhx$ (con $x \in G$), allora $h = x^{-1}gx^{-1}$. La commutatività di G serve invece per dimostrare che $\mathcal{R}$ è transitiva (cioè $g \mathcal{R} h$ e $h \mathcal{R} k$ implica $g \mathcal{R} k$). Se infatti $g = xhx$ e $h = yky$ (con $x, y \in G$), si ottiene

   $$g = xhx = xykyx = xykxy.$$

   (b) Per quanto visto al punto precedente, $1 \mathcal{R} g$ se e solo se $g \mathcal{R} 1$, e per definizione questo succede se e solo se $g = y1y = y^2$ per qualche $y \in G$.

   (c) In questo caso non vale $1 \mathcal{R} g$. Supponendo per assurdo che $1 \mathcal{R} g$, per il punto precedente esiste $y \in S_6$ tale che $g = y^2$. Posto $a := y(1)$, si ha

   $$2 = g(1) = y^2(1) = y(y(1)) = y(a),$$

   e questo implica $a \neq 1$ (altrimenti $1 = a = y(1) = y(a) = 2$) e $a \neq 2$ (altrimenti $y(1) = a = 2 = y(a) = y(2)$, contro l'iniettività

di y). Analogamente, posto $b := y(2)$, si trova $y(b) = 1$ con $b \neq 1, 2$. Deve essere inoltre $a \neq b$ (altrimenti $1 = y(b) = y(a) = 2$), e quindi $y|_{\{1,2,a,b\}} = (1, a, 2, b)$. Indicando con c e d gli altri due elementi di $\{1, \ldots, 6\}$, necessariamente $y = (1, a, 2, b)z$ con $z = 1$ o $z = (c, d)$. In ogni caso, tenendo presente che cicli disgiunti commutano, si ottiene l'assurdo

$$y^2 = \big((1, a, 2, b)z\big)^2 = (1, a, 2, b)^2 z^2 = (1, a, 2, b)^2 = (1, 2)(a, b) \neq g.$$

(d) Quando G è un gruppo abeliano additivo, si ha $g \mathcal{R} h$ se e solo se $g - h = 2x$ per qualche $x \in G$. Ora, in $\mathbb{Z}/n\mathbb{Z}$ gli elementi della forma $2x$ sono: tutti se n è dispari; quelli della forma $\overline{a}$ con a pari se n è pari. Ne segue che c'è una sola classe di $\mathcal{R}$-equivalenza in $\mathbb{Z}/5\mathbb{Z}$, mentre ce ne sono due in $\mathbb{Z}/4\mathbb{Z}$, cioè $\{\overline{0}, \overline{2}\}$ e $\{\overline{1}, \overline{3}\}$.

3. (a) Per definizione un elemento di Bb è della forma cb con $c \in B$. Essendo B un sottoanello di A, si ha $cb \in Ab$ e $cb \in B$, cioè $cb \in Ab \cap B$.

(b) Per il punto precedente basta dimostrare che $B[X]b \cap B \subseteq Bb$. Dato $c \in B[X]b \cap B$, esiste $p = \sum_{i=0}^{n} b_i X^i \in B[X]$ tale che $pb = c \in B$. Poiché $pb = \sum_{i=0}^{n} (b_i b) X^i$, deve essere $b_i b = 0$ per $i > 0$ e $b_0 b = c$. L'ultima uguaglianza dimostra che $c \in Bb$.

(c) Se $A = \mathbb{Q}$, $B = \mathbb{Z}$ e $b = 2$, risulta $Ab = \mathbb{Q}2 = \mathbb{Q}$ (perché $2 \in \mathbb{Q}^*$), e dunque

$$Bb = \mathbb{Z}2 = 2\mathbb{Z} \subsetneq Ab \cap B = \mathbb{Q}2 \cap \mathbb{Z} = \mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}.$$

4. (a) Vera. Essendo primitivo, p è irriducibile su $\mathbb{Z}$ se e solo se lo è su $\mathbb{Q}$, e questo succede se e solo se p non ha radici in $\mathbb{Q}$ (perché $\deg(p) = 3$). D'altra parte le eventuali radici razionali di p possono essere solo 1 e -1, ma nessuno di questi due valori è radice di p, visto che $p(1) = 2 + a > 0$ e $p(-1) = a > 0$.

(b) Vera. Se p è irriducibile su $\mathbb{Z}/3\mathbb{Z}$, allora non ha radici in $\mathbb{Z}/3\mathbb{Z}$, e in particolare $\overline{0} \neq p(\overline{1}) = \overline{2 + a}$ e $\overline{0} \neq p(\overline{-1}) = \overline{a}$. Le due disuguaglianze implicano $\overline{a} = \overline{2}$, cioè $a \equiv 2 \mod 3$.

(c) Falsa. Per $a = 2$

$$p - 2X = X^3 + 1 = (X + 1)(X^2 - X + 1)$$

è riducibile, ma

$$(p - 2X)^3 - 3X + 2 = (X^3 + 1)^3 - 3X + 2 = X^9 + 3X^6 + 3X^3 - 3X + 3$$

è irriducibile per il criterio di Eisenstein relativo al primo 3.