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

Prova scritta del 22.9.2016

1. Stabilire per quali dei seguenti valori di n esise una soluzione dell'equazione
$$13x + 8y = n$$
con $x, y \in \mathbb{N}$. Determinare inoltre quando una tale soluzione è unica.
   (a) $n = 73$
   (b) $n = 83$
   (c) $n = 125$

2. Sia G un gruppo e $H \subseteq G$ un sottogruppo. Un sottogruppo K di G si dice *complementare* di H se $HK = G$ e $H \cap K = \{1\}$.
   (a) Determinare tutti i sottogruppi di $\mathbb{Z}$ che ammettono un complementare.
   (b) Per $n \geq 2$, trovare un complementare di A_n in S_n.
   (c) Per quali valori di n è vero che ogni complementare di A_n in S_n è generato da una trasposizione?

3. Siano A e B due anelli e $f\colon A \to B$ un omomorfismo di gruppi additivi tale che anche $f|_{A^*}\colon A^* \to B^*$ sia un omomorfismo di gruppi moltiplicativi.
   (a) Dimostrare che, se A è un campo, allora f è un omomorfismo di anelli.
   (b) Dimostrare che, se $A = \mathbb{Z}/n\mathbb{Z}$ per qualche $n > 0$, allora f è un omomorfismo di anelli.
   (c) Fornire un esempio in cui $A = B = K[X]$ (con K campo) e f non è un omomorfismo di anelli.

4. Stabilire in quali dei seguenti anelli commutativi ogni ideale primo è massimale:
   (a) $\mathbb{Z}$
   (b) $\mathbb{Z}/18\mathbb{Z}$
   (c) $\mathbb{Q}[X]/(X^2 - 1)$
   (d) $\mathbb{Z}[X]/(X^2 - 1)$

Soluzioni

1. Poiché $\mathrm{mcd}(13, 8) = 1$, l'equazione $13x + 8y = n$ ha sempre soluzioni in $\mathbb{Z}$. Inoltre, se (x_0, y_0) è una soluzione, ogni soluzione è della forma

$$\begin{cases} x = x_0 + 8k \\ y = y_0 - 13k \end{cases}$$

con $k \in \mathbb{Z}$. Essendo $1 = -3 \cdot 13 + 5 \cdot 8$, si può scegliere per esempio $x_0 = -3n$, $y_0 = 5n$. Si tratta poi di stabilire se esiste e se è unico $k \in \mathbb{Z}$ tale che $x, y \geq 0$. Con questa scelta di x_0 e y_0 risulta $x \geq 0$ se e solo se $k \geq \frac{3n}{8}$ e $y \geq 0$ se e solo se $k \leq \frac{5n}{13}$, e quindi i k cercati sono gli interi che verificano

$$\frac{3n}{8} \leq k \leq \frac{5n}{13}.$$

   (a) Per $n = 73$ si ottiene

$$\frac{219}{8} = 27 + \frac{3}{8} \leq k \leq \frac{365}{13} = 28 + \frac{1}{13},$$

   che ha un'unica soluzione $k = 28$ (corrispondente a $x = 5$ e $y = 1$).

   (b) Per $n = 83$ si ottiene

$$\frac{249}{8} = 31 + \frac{1}{8} \leq k \leq \frac{415}{13} = 31 + \frac{12}{13},$$

   che non ha soluzioni.

   (c) Per $n = 125$ si ottiene

$$\frac{375}{8} = 46 + \frac{7}{8} \leq k \leq \frac{625}{13} = 48 + \frac{1}{13},$$

   che ha due soluzioni $k = 47$ (corrispondente a $x = 1$ e $y = 14$) e $k = 48$ (corrispondente a $x = 9$ e $y = 1$).

2. (a) Si osservi intanto che, essendo $\mathbb{Z}$ un gruppo additivo, la condizione di complementarietà diventa $H + K = \mathbb{Z}$ e $H \cap K = \{0\}$. È allora facile vedere che gli unici sottogruppi di $\mathbb{Z}$ che ammettono un complementare sono quelli banali, cioè $\{0\}$ e $\mathbb{Z}$. Infatti, è chiaro che $\mathbb{Z}$ è un complementare di $\{0\}$ e $\{0\}$ è un complementare di $\mathbb{Z}$. D'altra parte, se H è un sottogruppo non banale di $\mathbb{Z}$, allora $H = n\mathbb{Z}$ per qualche $n \geq 2$. Dato un qualunque sottogruppo K di $\mathbb{Z}$, si ha $K = m\mathbb{Z}$ per qualche $m \in \mathbb{N}$. Se $H \cap K = \{0\}$, deve essere $m = 0$ (altrimenti $0 < nm \in H \cap K$), ma allora $H + K = n\mathbb{Z} + \{0\} = n\mathbb{Z} \neq \mathbb{Z}$, e quindi K non è un complementare di H.

(b) Il sottogruppo K generato da una trasposizione σ di S_n (per esempio, $\sigma = (1,2)$) è un complementare di A_n. Infatti, $K = \{1, \sigma\}$ (perché σ ha ordine 2) e $A_n \cap K = \{1\}$ (perché σ è dispari). Inoltre, tenendo conto che $\#A_n = \frac{n!}{2}$ si ha

$$\#(A_n K) = \frac{\#A_n \cdot \#K}{\#(A_n \cap K)} = n! = \#S_n,$$

per cui $A_n K = S_n$.

(c) Se K è un complementare di A_n, risulta (sempre assumendo $n \geq 2$)

$$\#K = \frac{\#(A_n K) \cdot \#(A_n \cap K)}{\#A_n} = \frac{\#S_n \cdot \#\{1\}}{\#A_n} = 2.$$

Poiché ogni gruppo di ordine 2 è ciclico, esiste $\sigma \in S_n$ di ordine 2 tale che $K = \langle\sigma\rangle = \{1, \sigma\}$; inoltre σ è dispari, dato che $A_n \cap K = \{1\}$. Viceversa, lo stesso argomento del punto precedente mostra che ogni sottogruppo generato da una permutazione dispari di ordine 2 è un complementare di A_n. Si tratta quindi di stabilire per quali $n \geq 2$ le uniche permutazioni dispari di ordine 2 in S_n sono le trasposizioni. Ora, $\sigma \in S_n$ ha ordine 2 se e solo se σ è un prodotto (non vuoto) di trasposizioni disgiunte, e un tale prodotto è dispari se e solo se il numero di trasposizioni è dispari. È chiaro allora che un elemento di questa forma che non sia una trasposizione esiste in S_n se e solo se $n \geq 6$ (nel qual caso si può prendere per esempio $\sigma = (1,2)(3,4)(5,6)$), e dunque i valori cercati sono $2 \leq n \leq 5$.

3. (a) f verifica $f(a+b) = f(a) + f(b)$ per ogni $a, b \in A$ (perché è un omomorfismo additivo) e $f(1) = 1$ (perché $f|_{A^*}$ è un omomorfismo), per cui resta da verificare che $f(ab) = f(a)f(b)$ per ogni $a, b \in A$. Per ipotesi tale uguaglianza vale se $a, b \in A^* = A \setminus \{0\}$, per cui rimane da considerare il caso $a = 0$ o $b = 0$, che però segue subito dal fatto che $f(0) = 0$ (dato che f è un omomorfismo additivo) e che $x0 = 0x = 0$ in ogni anello.

(b) Indicando con $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la proiezione al quoziente (che è un omomorfismo di anelli), $g := f \circ \pi\colon \mathbb{Z} \to B$ è un omomorfismo di gruppi additivi (in quanto composizione di omomorfismi) tale che $g(1) = 1$. Tenendo conto che un omomorfismo di gruppi da $\mathbb{Z}$ verso un qualunque gruppo è univocamente determinato dall'immagine di 1 e che esiste un unico omomorfismo di anelli da $\mathbb{Z}$ verso qualunque anello, ne segue che g è un omomorfismo di anelli (l'unico

da $\mathbb{Z}$ a B). Per ogni $m \in n\mathbb{Z}$ si ha $g(m) = f(\pi(m)) = f(\overline{0}) = 0$, cioè $n\mathbb{Z} \subseteq \ker(g)$. Per il teorema di omomorfismo per anelli esiste allora un unico omomorfismo di anelli $h\colon \mathbb{Z}/n\mathbb{Z} \to B$ tale che $h \circ \pi = g = f \circ \pi$. Essendo π suriettivo, tale uguaglianza implica $f = h$, e perciò f è un omomorfismo di anelli.

(c) Sia $f\colon K[X] \to K[X]$ definito da $f(\sum_i a_i X^i) := a_0 + a_1 X$. Allora f è un omomorfismo di gruppi additivi perché

$$f(\sum_i a_i X^i + \sum_i b_i X^i) = f(\sum_i (a_i + b_i) X^i) = a_0 + b_0 + (a_1 + b_1)X$$
$$= a_0 + a_1 X + b_0 + b_1 X = f(\sum_i a_i X^i) + f(\sum_i b_i X^i)$$

per ogni $\sum_i a_i X^i, \sum_i b_i X^i \in K[X]$. Inoltre, essendo $K[X]^* = K^*$, risulta $f|_{K[X]^*} = \mathrm{id}_{K[X]^*}$, che è ovviamente un omomorfismo. D'altra parte f non è un omomorfismo di anelli perché per esempio $0 = f(X^2) \neq f(X)f(X) = X^2$.

4. (a) $\{0\}$ è primo ma non massimale in $\mathbb{Z}$, dato che $\mathbb{Z}$ è un dominio ma non un campo.

(b) In $\mathbb{Z}/18\mathbb{Z}$ ogni ideale primo è massimale. Infatti, ponendo $A = \mathbb{Z}$ e $I = 18\mathbb{Z}$, si può osservare più in generale che in A/I ogni ideale primo è massimale se A è un dominio a ideali principali e I è un ideale non nullo di A. Per dimostrare questo, ricordiamo intanto che gli ideali di A/I sono tutti e soli della forma J/I con J ideale di A tale che $I \subseteq J$. Inoltre J/I è primo (rispettivamente massimale) in A/I se e solo se J è primo (rispettivamente massimale) in A: tenendo conto che $(A/I)/(J/I) \cong A/J$ per il terzo teorema di isomorfismo, ciò segue subito dal fatto che un ideale è primo (rispettivamente massimale) se e solo se l'anello quoziente è un dominio (rispettivamente un campo). Per concludere basta dunque ricordare che in un dominio a ideali principali un ideale non nullo è primo se e solo se è massimale.

(c) In $\mathbb{Q}[X]/(X^2 - 1)$ ogni ideale primo è massimale, e si può dimostrare usando lo stesso argomento del punto precedente (con $A = \mathbb{Q}[X]$ e $I = (X^2 - 1)$).

(d) $(X - 1)/(X^2 - 1)$ è primo ma non massimale in $\mathbb{Z}[X]/(X^2 - 1)$. Infatti, $(\mathbb{Z}[X]/(X^2 - 1))/((X - 1)/(X^2 - 1)) \cong \mathbb{Z}[X]/(X - 1)$ per il terzo teorema di isomorfismo, e $\mathbb{Z}[X]/(X - 1) \cong \mathbb{Z}$ è un dominio ma non un campo.