Corso di Algebra 1 - a.a. 2014-2015

Prova scritta del 16.6.2015

1. Sia G il gruppo $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ e $\mathrm{Aut}(G)$ il suo gruppo degli automorfismi.
   (a) Stabilire se esiste $f \in \mathrm{Aut}(G)$ tale che $f((\bar{3}, \bar{0})) = (\bar{1}, \bar{0})$.
   (b) Stabilire se esiste $f \in \mathrm{Aut}(G)$ tale che $f((\bar{1}, \bar{0})) = (\bar{1}, \bar{1})$.
   (c) Determinare l'ordine di $\mathrm{Aut}(G)$.

2. (a) Dimostrare che gli elementi di S_5 di ordine 6 sono tutti coniugati alla permutazione $(1, 2)(3, 4, 5)$.
   (b) Contare gli elementi di ordine 6 in S_5.
   (c) Contare i sottogruppi ciclici di ordine 6 in S_5.

3. Sia A un sottoanello di $\mathbb{Q}$.
   (a) Dimostrare che $\mathbb{Z} \subseteq A$.
   (b) Dati $m, n \in \mathbb{Z}$ tali che $n \neq 0$ e $\mathrm{mcd}(m, n) = 1$, dimostrare che se $\frac{m}{n} \in A$ allora anche $\frac{1}{n} \in A$.
   (c) Dimostrare che per ogni ideale I di A esiste $k \in \mathbb{Z}$ tale che $I \cap \mathbb{Z} = k\mathbb{Z}$ e $I = kA$.

4. Sia A un anello e $P = X^4 - 6X^3 + 9X^2 + 6X + 15 \in A[X]$. Stabilire se l'anello quoziente $A[X]/(P)$ è un dominio e/o un campo in ciascuno dei seguenti casi:
   (a) $A = \mathbb{Z}/2\mathbb{Z}$;
   (b) $A = \mathbb{Q}$;
   (c) $A = \mathbb{Z}$.

Soluzioni

1. Ricordiamo preliminarmente che, per ogni intero positivo n e per ogni gruppo H, gli omomorfismi iniettivi da $\mathbb{Z}/n\mathbb{Z}$ a H sono in corrispondenza biunivoca con gli elementi di H di ordine n. Poiché una funzione tra due insiemi con n elementi è iniettiva se e solo se è suriettiva, ne segue che gli automorfismi di $\mathbb{Z}/n\mathbb{Z}$ sono in corrispondenza biunivoca con gli elementi di $\mathbb{Z}/n\mathbb{Z}$ di ordine n, e per la precisione a $\bar{h} \in \mathbb{Z}/n\mathbb{Z}$ di ordine n corrisponde l'automorfismo che manda $\bar{a}$ in $\bar{a}\bar{h}$. Ricordando inoltre che per $\bar{h} \in \mathbb{Z}/n\mathbb{Z}$ si ha $\mathrm{ord}(\bar{h}) = \frac{n}{\mathrm{mcd}(n,h)}$, si trova $\mathrm{ord}(\bar{h}) = n$ se e solo se $\mathrm{mcd}(n,h) = 1$ se e solo se $\bar{h} \in \mathbb{Z}/n\mathbb{Z}^*$. Se ne deduce che $\#\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \#\mathbb{Z}/n\mathbb{Z}^* = \varphi(n)$.

   (a) È sufficiente trovare $f_1 \in \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ e $f_2 \in \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z})$ tali che $f_1(\bar{3}) = \bar{1}$ e $f_2(\bar{0}) = \bar{0}$, perché poi

$$\begin{aligned} f = f_1 \times f_2 \colon G &\to G \\ (\bar{a}, \bar{b}) &\mapsto (f_1(\bar{a}), f_2(\bar{b})) \end{aligned}$$

   è chiaramente un automorfismo di G che verifica $f((\bar{3}, \bar{0})) = (\bar{1}, \bar{0})$. Prendendo come f_1 l'automorfismo di $\mathbb{Z}/7\mathbb{Z}$ corrispondente a $\bar{5} \in \mathbb{Z}/7\mathbb{Z}^*$ e come f_2 un qualunque automorfismo di $\mathbb{Z}/11\mathbb{Z}$ (per esempio l'identità), si ha in effetti $f_1(\bar{3}) = \bar{3}\cdot\bar{5} = \bar{1}$ e $f_2(\bar{0}) = \bar{0}$. Pertanto esiste $f \in \mathrm{Aut}(G)$ con la proprietà richiesta.

   (b) Dati $\bar{a} \in \mathbb{Z}/7\mathbb{Z}$ e $\bar{b} \in \mathbb{Z}/11\mathbb{Z}$ vale

$$\mathrm{ord}_G((\bar{a}, \bar{b})) = \mathrm{mcd}(\mathrm{ord}_{\mathbb{Z}/7\mathbb{Z}}(\bar{a}), \mathrm{ord}_{\mathbb{Z}/11\mathbb{Z}}(\bar{b})),$$

   quindi $\mathrm{ord}_G((\bar{1}, \bar{0})) = \mathrm{mcd}(7, 1) = 7$ e $\mathrm{ord}_G((\bar{1}, \bar{1})) = \mathrm{mcd}(7, 11) = 77$. Poiché un automorfismo preserva l'ordine degli elementi, concludiamo che non esiste $f \in \mathrm{Aut}(G)$ tale che $f((\bar{1}, \bar{0})) = (\bar{1}, \bar{1})$.

   (c) Essendo $\mathrm{mcd}(7, 11) = 1$ per il teorema cinese del resto $G \cong \mathbb{Z}/77\mathbb{Z}$, e dunque $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbb{Z}/77\mathbb{Z})$. Da quanto detto sopra segue allora

$$\#\mathrm{Aut}(G) = \#\mathrm{Aut}(\mathbb{Z}/77\mathbb{Z}) = \varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60.$$

2. (a) L'ordine di $\sigma \in S_5$ è il minimo comune multiplo delle lunghezze dei cicli che compaiono nella decomposizione di σ come prodotto di cicli disgiunti. Poiché S_5 non contiene 6-cicli, $\mathrm{ord}(\sigma) = 6$

se e solo se σ è il prodotto di una trasposizione e di un 3-ciclo disgiunti. Ricordando che due permutazioni sono coniugate se e solo se hanno lo stesso tipo di decomposizione come prodotto di cicli disgiunti, otteniamo che gli elementi di S_5 di ordine 6 sono tutti e soli quelli coniugati a $(1,2)(3,4,5)$.

(b) Per quanto visto sopra gli elementi di S_5 di ordine 6 sono quelli della forma $(a,b)(c,d,e)$ con a,b,c,d,e distinti. Poiché ci sono $\binom{5}{2} = 10$ modi di scegliere $\{a,b\} \subset \{1,2,3,4,5\}$ e, per ogni tale scelta, ci sono due permutazioni del tipo cercato (cioè $(a,b)(c,d,e)$ e $(a,b)(c,e,d)$), gli elementi di ordine 6 in S_5 sono $10 \cdot 2 = 20$.

(c) Ogni gruppo ciclico di ordine 6 contiene esattamente 2 elementi di ordine 6: un tale gruppo è isomorfo a $\mathbb{Z}/6\mathbb{Z}$, i cui elementi di ordine 6 sono $\bar{1}$ e $\bar{5}$. Inoltre ogni elemento di ordine 6 appartiene a un unico sottogruppo ciclico di ordine 6 (quello da lui generato). Dunque il numero di sottogruppi ciclici di ordine 6 in S_5 è la metà del numero di elementi di ordine 6 in S_5, cioè, per il punto precedente, 10.

3. (a) Per definizione di sottoanello $1 \in A$ e A è un sottogruppo (additivo) di $\mathbb{Q}$, quindi A contiene il sottogruppo di $\mathbb{Q}$ generato da 1, che è $\mathbb{Z}$.

(b) Dato che $\mathrm{mcd}(m,n) = 1$, esistono $a,b \in \mathbb{Z}$ tali che $1 = am + bn$. Dividendo per n si trova $\frac{1}{n} = a\frac{m}{n} + b \in A$ (usando il punto (a) e il fatto che A è chiuso rispetto a somma e prodotto).

(c) $I \cap \mathbb{Z}$ è un sottogruppo di $\mathbb{Q}$ (perché intersezione di sottogruppi) contenuto in $\mathbb{Z}$, dunque è anche un sottogruppo di $\mathbb{Z}$. Se ne deduce che esiste $k \in \mathbb{Z}$ tale che $I \cap \mathbb{Z} = k\mathbb{Z}$, e resta da dimostrare che $I = kA$. Chiaramente $kA \subseteq I$ perché $k \in I$ e I è un ideale di A. Viceversa, dato $x \in I$, esistono $m,n \in \mathbb{Z}$ tali che $n \neq 0$, $\mathrm{mcd}(m,n) = 1$ e $x = \frac{m}{n}$. Per il punto (a) $n \in A$, quindi $m = nx \in I$ (essendo I un ideale di A). Dunque $m \in I \cap \mathbb{Z}$, e per definizione di k esiste $c \in \mathbb{Z}$ tale che $m = kc$. Si ottiene allora $x = \frac{m}{n} = k\frac{c}{n} \in kA$ perché $\frac{c}{n} \in A$ (dato che $c \in A$ per il punto (a), $\frac{1}{n} \in A$ per il punto (b) e A è chiuso rispetto al prodotto).

4. Se A è un anello commutativo, l'anello quoziente $A[X]/(P)$ è un dominio (rispettivamente un campo) se e solo se l'ideale (P) è primo (rispettivamente massimale) in $A[X]$. Se A (e quindi $A[X]$) è un dominio a fattorizzazione unica e $P \neq 0$, l'ideale principale (P) è primo se e solo se l'elemento P di $A[X]$ è irriducibile. Se inoltre A è un campo

(e quindi $A[X]$ è un dominio a ideali principali), (P) è primo se e solo se (P) è massimale. Osservando che i tre anelli considerati sono tutti domini a fattorizzazione unica e che i primi due sono anche campi, otteniamo i seguenti risultati.

(a) Dato che $P = X^4 + X^2 + 1 = (X^2 + X + 1)^2 \in \mathbb{Z}/2\mathbb{Z}[X]$ non è irriducibile, $\mathbb{Z}/2\mathbb{Z}[X]/(P)$ non è né un dominio né un campo.

(b) P è irriducibile in $\mathbb{Z}[X]$ per il criterio di Eisenstein relativo al primo 3. Essendo $\mathbb{Q}$ il campo dei quozienti di $\mathbb{Z}$, ne segue che P è irriducibile anche in $\mathbb{Q}[X]$, e dunque $\mathbb{Q}[X]/(P)$ è sia un dominio che un campo.

(c) Come visto nel punto precedente, P è irriducibile in $\mathbb{Z}[X]$, dunque $\mathbb{Z}[X]/(P)$ è un dominio. D'altra parte (P) non è massimale in $\mathbb{Z}[X]$ perché per esempio l'ideale $I = (P, 3)$ verifica verifica $(P) \subsetneq I \subsetneq \mathbb{Z}[X]$. Infatti $3 \in I \setminus (P)$ (dato che per ogni $Q \in \mathbb{Z}[X]$ si ha $PQ = 0$ se $Q = 0$, e altrimenti $\deg(PQ) = \deg(P) + \deg(Q) \geq 4$, essendo $\mathbb{Z}$ un dominio) e $1 \in \mathbb{Z}[X] \setminus I$ (perché ogni elemento di I è della forma $PQ + 3R$ con $Q, R \in \mathbb{Z}[X]$, e dunque il suo termine noto è un multiplo di 3). Si conclude quindi che $\mathbb{Z}[X]/(P)$ non è un campo.