Corso di Algebra 1 - a.a. 2013-2014

Prova scritta del 23.6.2014

1. Dato un intero positivo n, sia $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la funzione definita da $f(a) = \overline{2a+1}$.
   (a) Dimostrare che l'immagine di f è contenuta in $\mathbb{Z}/n\mathbb{Z}^*$ se e solo se n è una potenza di 2.
   (b) Determinare i valori di n per cui f è un omomorfismo di gruppi da $\mathbb{Z}$ a $\mathbb{Z}/n\mathbb{Z}^*$.

2. Sia G il gruppo $S_3 \times A_4$.
   (a) Esistono in G elementi di ordine 12?
   (b) Dimostrare che G contiene un sottogruppo isomorfo a $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Sia A un anello tale che ogni sottogruppo additivo di A è un ideale.
   (a) Dimostrare che se $f\colon B \to A$ è un omomorfismo di anelli, allora f è suriettivo.
   (b) Dimostrare che A è isomorfo (come anello) a $\mathbb{Z}$ o a $\mathbb{Z}/n\mathbb{Z}$ per qualche intero positivo n.

4. Sia P il polinomio $X^3 + 2X + 1$.
   (a) Dimostrare che P è irriducibile in $\mathbb{Q}[X]$.
   (b) Esiste un'estensione di campi $\mathbb{Q} \subset K$ di grado 2 tale che P sia riducibile in $K[X]$?

Soluzioni

1. (a) Poiché $\mathbb{Z}/n\mathbb{Z}^* = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} : \mathrm{mcd}(n,k) = 1\}$, l'immagine di f è contenuta in $\mathbb{Z}/n\mathbb{Z}^*$ se e solo se $\mathrm{mcd}(n, 2a+1) = 1$ per ogni $a \in \mathbb{Z}$. Essendo $2a+1$ sempre dispari, questa condizione è chiaramente verificata se n è una potenza di 2. Viceversa, se n non è una potenza di 2 esiste un numero primo dispari p che divide n, e allora per $a = (p-1)/2$ si ha $\mathrm{mcd}(n, 2a+1) = \mathrm{mcd}(n,p) = p \neq 1$.

   (b) Per la prima parte possiamo considerare f come una funzione da $\mathbb{Z}$ a $\mathbb{Z}/n\mathbb{Z}^*$ se e solo se n è una potenza di 2. Con questa ipotesi, per definizione f è un omomorfismo di gruppi se e solo se $f(a+b) = f(a)f(b)$ per ogni $a, b \in \mathbb{Z}$. Dato che

$$f(a+b) = \overline{2(a+b)+1} = \overline{2a+2b+1},$$
$$f(a)f(b) = (\overline{2a+1})(\overline{2b+1}) = \overline{4ab+2a+2b+1},$$

   vale $f(a+b) = f(a)f(b)$ se e solo se $\overline{4ab} = \overline{0}$, cioè se e solo se $n \mid 4ab$. Quest'ultima condizione è soddisfatta per ogni $a, b \in \mathbb{Z}$ se e solo se $n \mid 4$ (visto che $4ab = 4$ per $a = b = 1$), cioè se e solo se $n = 1, 2$ o 4. Essendo 1, 2 e 4 potenze di 2, questi sono tutti e soli i valori per cui f risulta un omomorfismo da $\mathbb{Z}$ a $\mathbb{Z}/n\mathbb{Z}^*$.

2. (a) La risposta è negativa. Infatti, poiché G è un prodotto diretto di gruppi, l'ordine di un elemento, cioè di una coppia del tipo (a,b) con $a \in S_3$ e $b \in A_4$, è il minimo comune multiplo degli ordini di a e b nei rispettivi gruppi. Ma in S_3 ci sono solo elementi di ordine $1, 2$ e 3, e così anche in A_4; perciò il minimo comune multiplo non può mai essere 12.

   (b) La tesi è equivalente a trovare un elemento x di ordine 6 e uno y di ordine due che commutino tra loro ma non abbiano potenze in comune a parte l'identità (nel nostro caso, basta quindi che y non sia una potenza di x, perché e e y sono le uniche potenze di y). Infatti a quel punto x e y genererebbero due sottogruppi abeliani di G, di ordine rispettivamente 6 e 2, la cui intersezione sarebbe solo l'identità e i cui elementi commuterebbero tutti tra loro: quindi tutti gli elementi del tipo (x^k, y^h) con $k = 0, \ldots, 5$ e $h = 0, 1$ costituirebbero il sottogruppo cercato.

   Ma, per quanto detto al punto precedente, gli elementi di ordine 6 sono quelle coppie (a,b) in cui o a è un 3-ciclo e b una doppia trasposizione, o a è una trasposizione e b è un 3-ciclo; mentre per

quelli di ordine 2 ci sono 3 casi, cioè quando a è una trasposizione e $b = e$, quando b è una doppia trasposizione e $a = e$, o a è una trasposizione e b una doppia trasposizione.

Allora possiamo scegliere $x = (a, b)$ del primo tipo tra quelli di ordine 6 e $y = (c, d)$ del secondo tipo tra quelli di ordine 2 (cioè con $c = e$) in modo però che b sia diverso da d: ad esempio, potremmo porre $x = ((123), (12)(34))$ e $y = (e, (13)(24))$. Chiaramente x e y commutano, infatti

$$xy = (a, b)(e, d) = (a, bd) = (a, db) = (e, d)(a, b) = yx,$$

dove abbiamo usato il fatto che le doppie trasposizioni b e d commutano in A_4. Inoltre, se fosse $x^k = y$ per qualche k, ciò vorrebbe dire che $a^k = e$ e $b^k = d$; ma a sua volta b ha ordine 2 quindi le sue uniche potenze in A_4 sono e e se stesso, e noi abbiamo scelto d diverso da entrambe. Quindi y non è una potenza di x e questi elementi generano in G il sottogruppo cercato [è facile anche convincersi che questa scelta è di fatto l'unica possibile tra i casi che abbiamo esaminato].

Alternativamente, basta osservare che $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: prendendo allora il sottogruppo C dei 3-cicli in S_3 e quello V delle doppie trasposizioni in A_4 è chiaro che $C \times V < G$ ha le caratteristiche richieste (e con questa descrizione è anche ovvio che si tratta di un sottogruppo normale, poiché C e V lo sono rispettivamente in S_3 e in A_4).

3. (a) Essendo $f(B)$ un sottoanello (e quindi in particolare un sottogruppo additivo) di A, l'ipotesi su A implica che $f(B)$ è un ideale di A. Inoltre $1_A = f(1_B) \in f(B)$, per cui $f(B) = A$ (un ideale che contiene 1 è tutto l'anello), cioè f è suriettivo.

   (b) Per la prima parte l'unico omomorfismo di anelli $f\colon \mathbb{Z} \to A$ (definito da $f(n) = n1_A$) è suriettivo. Dal primo teorema di isomorfismo segue allora che A è isomorfo a $\mathbb{Z}/\ker(f)$. Per concludere basta osservare che $\ker(f)$ è un ideale di $\mathbb{Z}$, dunque $\ker(f) = \{0\}$ (nel qual caso A è isomorfo a $\mathbb{Z}$) o $\ker(f) = n\mathbb{Z}$ per qualche intero positivo n.

4. (a) Un polinomio di grado 3 riducibile su un campo deve avere una radice in esso. Ma per il criterio della radice razionale, le uniche possibili radici per P in $\mathbb{Q}$ sarebbero 1 o -1, che non lo soddisfano; quindi P è irriducibile in $\mathbb{Q}[x]$.

(b) La risposta è negativa. Supponiamo infatti per assurdo che una tale estensione K esista: allora, come già detto, P dovrebbe avere una radice in K, che chiamiamo α. Ma poiché P è irriducibile, esso sarebbe anche il polinomio minimo di α su $\mathbb{Q}$ e quindi l'estensione di $\mathbb{Q}$ con α avrebbe grado pari al grado di P, cioè 3: questo però porta ad un assurdo, perché avremmo $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$, quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ dovrebbe dividere $[K : \mathbb{Q}] = 2$.