Corso di Algebra 1 - a.a. 2016-2017

Prova scritta del 15.6.2017

1. Sia G un gruppo con un unico sottogruppo H tale che $\{1\} \neq H \neq G$.
   (a) Dimostrare che ogni elemento di $G \setminus H$ è un generatore di G.
   (b) Dimostrare che G è isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ per qualche numero primo p.

2. (a) Sia n un intero positivo e sia $f\colon \mathbb{Z}/15\mathbb{Z} \to S_n$ un omomorfismo di gruppi. Dimostrare che l'immagine di f è contenuta in A_n.
   (b) Quanti sono gli omomorfismi da $\mathbb{Z}/15\mathbb{Z}$ a S_5?
   (c) Per quali valori di n esiste un omomorfismo iniettivo da $\mathbb{Z}/15\mathbb{Z}$ a S_n?

3. Sia A un anello, B un suo sottoanello e $f\colon A \to B$ un omomorfismo di anelli tale che $f(b) = b$ per ogni $b \in B$.
   (a) Dimostrare che $\ker(f)$ è un ideale primo di A se e solo se B è un dominio.
   (b) Dimostrare che, se A è un campo, allora $B = A$.
   (c) È vero che, se B è un campo, allora $B = A$?

4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss.
   (a) Dimostrare che 29 non è irriducibile in $\mathbb{Z}[i]$.
   (b) Dimostrare che $\mathbb{Z}[i]/(29)$ è isomorfo come anello a $\mathbb{Z}/29\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z}$.
   (c) Quanti sono gli elementi non invertibili di $\mathbb{Z}[i]/(29)$?

Soluzioni

1. (a) Dato $a \in G \setminus H$, il sottogruppo $\langle a \rangle$ generato da a non può essere né $\{1\}$ né H (perché $a \notin H$), dunque necessariamente $\langle a \rangle = G$, cioè G è generato da a.

   (b) Essendo un gruppo ciclico per il punto precedente, G deve essere isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/n\mathbb{Z}$ per qualche intero positivo n. Non può essere $G \cong \mathbb{Z}$ perché $\mathbb{Z}$ ha infiniti sottogruppi non banali (quelli della forma $m\mathbb{Z}$ con $m > 1$). D'altra parte i sottogruppi non banali di $\mathbb{Z}/n\mathbb{Z}$ sono quelli della forma $d\mathbb{Z}/n\mathbb{Z}$ con d divisore di n tale che $1 < d < n$, per cui sono in corrispondenza biunivoca con i divisori (positivi) non banali di n. Ne segue che $G \cong \mathbb{Z}/n\mathbb{Z}$ con n che ha un unico divisore non banale. Per concludere basta allora osservare che, se n ha un unico divisore non banale, allora $n = p^2$ per qualche primo p. Infatti, se n fosse divisibile per due primi distinti p e q, avrebbe almeno due divisori non banali (cioè p e q), mentre p^k (con $k > 0$) ha esattamente $k - 1$ divisori non banali (cioè p^i con $0 < i < k$).

2. (a) Per ogni $a \in \mathbb{Z}/15\mathbb{Z}$ si ha $\operatorname{ord}(f(a)) \mid \operatorname{ord}(a) \mid 15$, dunque $\operatorname{ord}(f(a))$ è dispari. Dato che l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei cicli che compaiono nella sua decomposizione come prodotto di cicli disgiunti, $f(a)$ deve essere prodotto di cicli (disgiunti) di lunghezza dispari. Tali cicli sono elementi di A_n, e quindi lo stesso vale per $f(a)$.

   (b) In generale per ogni intero positivo m e per ogni gruppo G gli omomorfismi da $\mathbb{Z}/m\mathbb{Z}$ a G sono in corrispondenza biunivoca con gli elementi di G il cui ordine divide m (la corrispondenza si ottiene associando all'omomorfismo $f\colon \mathbb{Z}/m\mathbb{Z} \to G$ l'elemento $f(\overline{1}) \in G$). Nel nostro caso gli omomorfismi cercati sono dunque tanti quanti gli elementi di S_5 il cui ordine divide 15. In S_5 non ci sono elementi di ordine 15, gli elementi di ordine 5 sono i 5-cicli, quelli di ordine 3 sono i 3-cicli e l'elemento neutro è l'unico di ordine 1. Dato che in generale in S_n il numero di k-cicli (con $k \leq n$) è $\binom{n}{k}(k-1)!$, in S_5 i 5-cicli sono $4! = 24$ e i 3 cicli sono $\binom{5}{3}2! = 20$. Quindi il numero richiesto è $24 + 20 + 1 = 45$.

   (c) Attraverso la corrispondenza biunivoca illustrata nel punto precedente, gli omomorfismi iniettivi da $\mathbb{Z}/m\mathbb{Z}$ a G corrispondono agli elementi di G di ordine m. Perciò esiste un omomorfismo iniettivo da $\mathbb{Z}/15\mathbb{Z}$ a S_n se e solo se S_n contiene elementi di ordine

15, e questo succede se e solo se $n \geq 8$. Infatti, in S_n con $n \geq 8$ l'elemento $(1,2,3,4,5)(6,7,8)$ ha ordine 15. D'altra parte, nella decomposizione in cicli disgiunti di una permutazione di ordine 15 deve comparire un 15-ciclo (quindi $n \geq 15$) oppure sia un 5-ciclo che un 3-ciclo (quindi $n \geq 5+3=8$).

3. (a) Essendo f suriettivo, per il primo teorema di isomorfismo per anelli $B = \mathrm{im}(f) \cong A/\ker(f)$. Dunque B è un dominio se e solo se $A/\ker(f)$ è un dominio se e solo se $\ker(f)$ è primo.

   (b) $\ker(f) = \{0\}$ (quindi f è iniettivo) perché un campo ha solo gli ideali banali e $1 \notin \ker(f)$ (dato che $f(1) = 1 \neq 0$). Per ogni $a \in A$ si ha $f(a) = f(f(a))$ (perché $f(a) \in B$), quindi $a = f(a) \in B$ per l'iniettività di f.

   (c) No: un controesempio è dato da $A = B[X]$ e $f\colon B[X] \to B$ definito da $f(\sum_i b_i X^i) = b_0$.

4. (a) Un numero primo p non è irriducibile in $\mathbb{Z}[i]$ se esistono $a, b \in \mathbb{Z}$ tali che $p = a^2 + b^2$, perché allora $p = (a+bi)(a-bi)$ e $a \pm bi \notin \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ (visto che deve essere $a, b \neq 0$). In particolare $29 = 5^2 + 2^2$ non è irriducibile in $\mathbb{Z}[i]$.

   (b) Da $29 = (5+2i)(5-2i)$ segue $(29) = I_1 I_2$ con $I_1 = (5+2i)$ e $I_2 = (5-2i)$. Poiché I_1 e I_2 sono due ideali coprimi di $\mathbb{Z}[i]$ (infatti $I_1 + I_2$ contiene sia $10 = 5 + 2i + 5 - 2i$ che $29 = (5+2i)(5-2i)$, e quindi anche $3 \cdot 10 - 29 = 1$), per il teorema cinese del resto

   $$\mathbb{Z}[i]/(29) \cong \mathbb{Z}[i]/I_1 \times \mathbb{Z}[i]/I_2.$$

   Resta allora da dimostrare che $\mathbb{Z}[i]/I_j \cong \mathbb{Z}/29\mathbb{Z}$ per $j = 1, 2$. Indicando con $f_j\colon \mathbb{Z} \to \mathbb{Z}[i]/I_j$ l'(unico) omomorfismo di anelli, ottenuto come composizione dell'inclusione di $\mathbb{Z}$ in $\mathbb{Z}[i]$ e della proiezione al quoziente da $\mathbb{Z}[i]$ a $\mathbb{Z}[i]/I_j$, per il primo teorema di isomorfismo per anelli basta dimostrare che f_j è suriettivo e $\ker(f_j) = 29\mathbb{Z}$. f_j è suriettivo se per ogni $a, b \in \mathbb{Z}$ esiste $c \in \mathbb{Z}$ tale che $a + bi \in c + I_j$. Assumendo $j = 1$ (il caso $j = 2$ è del tutto simile), questo è vero perché (essendo $\mathrm{mcd}(5,2) = 1$) esistono $m, n \in \mathbb{Z}$ tali che $b = 5m + 2n$, e pertanto $(n+mi)(5+2i) = 5n - 2m + bi$, il che dimostra

   $$a + bi = a - 5n + 2m + (n+mi)(5+2i) \in a - 5n + 2m + I_1.$$

   Infine $29 \in \ker(f_j)$ perché $29 = (5+2i)(5-2i) \in I_j$, per cui $29\mathbb{Z} \subseteq \ker(f_j)$. D'altra parte $29\mathbb{Z}$ è un ideale massimale di $\mathbb{Z}$ (perché 29

è primo) e $1 \notin \ker(f_j)$ (dato che $1 \notin I_j$ perché $5 \pm 2i \notin \mathbb{Z}[i]^*$), perciò deve essere $\ker(f_j) = 29\mathbb{Z}$.

(c) Per il punto precedente gli elementi non invertibili di $\mathbb{Z}[i]/(29)$ sono tanti quanti gli elementi non invertibili di $\mathbb{Z}/29\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z}$, cioè (tenendo conto che $(A \times B)^* = A^* \times B^*$ per ogni coppia di anelli A e B e che $\mathbb{Z}/29\mathbb{Z}$ è un campo perché 29 è primo)

$$\begin{aligned}
&\#(\mathbb{Z}/29\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z}) - \#(\mathbb{Z}/29\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z})^* \\
&\qquad = \#(\mathbb{Z}/29\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z}) - \#(\mathbb{Z}/29\mathbb{Z}^* \times \mathbb{Z}/29\mathbb{Z}^*) \\
&\qquad\qquad = 29^2 - 28^2 = (28+1)^2 - 28^2 = 2 \cdot 28 + 1 = 57.
\end{aligned}$$