Corso di Algebra 1 - a.a. 2017-2018

Prova scritta del 22/01/2018

1. Sia $(G, +)$ un gruppo abeliano additivo. Si dice che G è *divisibile* se per ogni $a \in G$ e per ogni intero positivo n esiste $b \in G$ tale che $a = nb$.
   (a) Dimostrare che se G è divisibile e H è un sottogruppo di G, allora anche G/H è divisibile.
   (b) Supponendo che G sia un sottogruppo di $\mathbb{Q}$, dimostrare che G è divisibile se e solo se $G = \{0\}$ o $G = \mathbb{Q}$.
   (c) Dimostrare che se G è divisibile e non banale, allora G è infinito.

2. Sia G un gruppo.
   (a) Dimostrare che se esiste un omomorfismo suriettivo $G \to \mathbb{Z}$, allora esiste un omomorfismo iniettivo $\mathbb{Z} \to G$.
   (b) Dimostrare che se G è finito ed esiste un omomorfismo suriettivo $G \to \mathbb{Z}/n\mathbb{Z}$ (con n intero positivo), allora esiste un omomorfismo iniettivo $\mathbb{Z}/n\mathbb{Z} \to G$.
   (c) Fornire un esempio in cui G ha ordine 8 ed esiste un omomorfismo suriettivo $G \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ma non esiste un omomorfismo iniettivo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$.

3. Siano A un dominio, B un sottoanello di A, I un ideale di A e K il campo dei quozienti di A. Siano inoltre
$$A' := \{x \in K \,:\, \exists b \in B \setminus \{0\} \text{ tale che } bx \in A\},$$
$$I' := \{x \in K \,:\, \exists b \in B \setminus \{0\} \text{ tale che } bx \in I\}.$$
   (a) Dimostrare che A' è un sottoanello di K.
   (b) Dimostrare che I' è un ideale di A'.
   (c) Dimostrare che $I' \neq A'$ se e solo se $I \cap B = \{0\}$.

4. Sia $f = X^5 - 5X^4 - 6X^3 + 4X^2 + 2X - 2$.
   (a) Fattorizzare f in $\mathbb{Z}[X]$.
   (b) Dimostrare che ogni ideale non banale di $\mathbb{Q}[X]/(f)$ è massimale.
   (c) Dimostrare che l'ideale generato da $2 + (f)$ in $\mathbb{Z}[X]/(f)$ non è banale e non è primo.

Soluzioni

1. (a) Per ogni $a \in G$ e per ogni intero positivo n esiste $b \in G$ tale che $a = nb$, dunque vale anche $a + H = nb + H = n(b + H)$, il che dimostra che G/H è divisibile.

   (b) $\{0\}$ è divisibile perché $0 = n0$ per ogni intero n. $\mathbb{Q}$ è divisibile perché per ogni $a \in \mathbb{Q}$ e per ogni intero positivo n esiste unico $b = n^{-1}a \in \mathbb{Q}$ tale che $a = nb$. Viceversa, se G è un sottogruppo divisibile di $\mathbb{Q}$, posso supporre $G \neq \{0\}$. Esiste allora $g \in G\backslash\{0\}$, e per ogni $q \in \mathbb{Q}$ esistono $m, n \in \mathbb{Z}$ con $n > 0$ tali che $g^{-1}q = n^{-1}m$, cioè $q = n^{-1}mg$. Si ha $mg \in G$ perché G è un sottogruppo di $\mathbb{Q}$, e quindi $q \in G$ perché G è divisibile. Ciò dimostra che $G = \mathbb{Q}$.

   (c) Sia $a \in G \setminus \{0\}$. Per ogni intero positivo n esiste $b \in G$ tale che $nb = a \neq 0$, dunque $\mathrm{ord}(b) \nmid n$. Se ne deduce (per il teorema di Lagrange) che $\#G \neq n$. Poiché questo vale per ogni $n > 0$, G deve essere infinito.

2. (a) Sia $f\colon G \to \mathbb{Z}$ un omomorfismo suriettivo e sia $a \in G$ tale che $f(a) = 1$. Non può essere $\mathrm{ord}(a) = m < \infty$ (se no $\mathrm{ord}(f(a)) \mid m$, mentre $\mathrm{ord}(1_{\mathbb{Z}}) = \infty$), dunque $\mathrm{ord}(a) = \infty$. Ne segue che la funzione $\mathbb{Z} \to G$ definita da $k \mapsto a^k$ è un omomorfismo iniettivo.

   (b) Sia $f\colon G \to \mathbb{Z}/n\mathbb{Z}$ un omomorfismo suriettivo e sia $a \in G$ tale che $f(a) = \overline{1}$. Posto $m := \mathrm{ord}(a)$ (necessariamente $m < \infty$ poiché G è finito), si ha $n \mid m$ perché $\mathrm{ord}(f(a)) \mid \mathrm{ord}(a)$ e $\mathrm{ord}(\overline{1}) = n$. Allora $b := a^{\frac{m}{n}} \in G$ verifica $\mathrm{ord}(b) = n$, e quindi la funzione $\mathbb{Z}/n\mathbb{Z} \to G$ definita da $\overline{k} \mapsto b^k$ è un omomorfismo iniettivo.

   (c) Sia $G := Q$ (il gruppo delle unità dei quaternioni) e $H := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il sottogruppo $\{\pm 1\}$ di Q è normale (coincide con il centro) e il gruppo quoziente $Q/\{\pm 1\}$ è isomorfo a H (perché ha ordine 4 e tutti i suoi elementi hanno ordine 1 o 2, dato che $g^2 \in \{\pm 1\}$ per ogni $g \in Q$). Dunque, componendo un isomorfismo $Q/\{\pm 1\} \to H$ con l'omomorfismo suriettivo dato dalla proiezione al quoziente $Q \to Q/\{\pm 1\}$, si ottiene un omomorfismo suriettivo $Q \to H$. Se esistesse un omomorfismo iniettivo $H \to Q$, la sua immagine sarebbe costituita da un elemento di ordine 1 e da tre elementi di ordine 2 (dato che gli omomorfismi iniettivi preservano gli ordini degli elementi), il che è impossibile perché Q contiene un solo elemento di ordine 2, cioè -1.

3. (a) $1 \in A'$ perché $1 \cdot 1 = 1 \in A$ e $1 \in B \setminus \{0\}$. Se $x_1, x_2 \in A'$, per definizione esistono $b_1, b_2 \in B \setminus \{0\}$ tali che $a_i := b_i x_i \in A$ per $i = 1, 2$. Allora $b_1 b_2 (x_1 - x_2) = b_2 a_1 - b_1 a_2 \in A$ e $b_1 b_2 x_1 x_2 = a_1 a_2 \in A$, il che dimostra che $x_1 - x_2, x_1 x_2 \in A'$, dato che $b_1 b_2 \in B \setminus \{0\}$ (essendo B un dominio).

   (b) È chiaro per definizione che $I' \subseteq A'$. $0 \in I'$ perché $1 \cdot 0 = 0 \in A$ e $1 \in B \setminus \{0\}$. Analogamente al punto precedente, se $y_1, y_2 \in I'$, esistono $b_1, b_2 \in B \setminus \{0\}$ tali che $c_i := b_i y_i \in I$ per $i = 1, 2$; ne segue che $b_1 b_2 (y_1 + y_2) = b_2 c_1 + b_1 c_2 \in I$ con $b_1 b_2 \in B \setminus \{0\}$, e quindi $y_1 + y_2 \in I'$. Infine, se $x \in A'$ e $y \in I'$, esistono $b, b' \in B \setminus \{0\}$ tali che $a := bx \in A$ e $c := b'y \in I$; si ottiene allora $bb'xy = ac \in I$ con $bb' \in B \setminus \{0\}$, per cui $xy \in I'$.

   (c) È equivalente dimostrare che $I' = A'$ se e solo se $I \cap B \neq \{0\}$. Essendo I' un ideale di A', si ha $I' = A'$ se e solo se $1 \in I'$. Per definizione di I', $1 \in I'$ se e solo se esiste $b \in B \setminus \{0\}$ tale che $b1 = b \in I$, cioè (tenendo conto che in ogni caso $0 \in I \cap B$) se e solo se $I \cap B \neq \{0\}$.

4. (a) Le eventuali radici razionali di f vanno cercate in $\{\pm 1, \pm 2\}$, ed è immediato verificare che solo -1 è radice di f. Risulta in effetti $f = (X + 1)(X^4 - 6X^3 + 4X - 2)$, e questa è la fattorizzazione completa di f, dato che il secondo fattore è irriducibile per il criterio di Eisenstein relativo al numero primo 2.

   (b) Gli ideali di $\mathbb{Q}[X]/(f)$ sono tutti e soli della forma $I/(f)$ con I ideale di $\mathbb{Q}[X]$ tale che $(f) \subseteq I$. Poiché $\mathbb{Q}[X]$ è un dominio a ideali principali (essendo $\mathbb{Q}$ un campo), per ogni ideale I di $\mathbb{Q}[X]$ esiste (unico a meno di associati) $g \in \mathbb{Q}[X]$ tale che $I = (g)$; inoltre $(f) \subseteq I$ se e solo se g divide f. Tenendo conto che, per il punto precedente, $f = f_1 f_2$ con $f_1 = X + 1$ e $f_2 = X^4 - 6X^3 + 4X - 2$ irriducibili non associati, tutti gli ideali di $\mathbb{Q}[X]$ contenenti (f) sono $(1) = \mathbb{Q}[X]$, (f_1), (f_2) e (f) stesso. Se ne deduce che gli ideali non banali di $\mathbb{Q}[X]/(f)$ sono solo $(f_1)/(f)$ e $(f_2)/(f)$. Essi sono anche massimali in $\mathbb{Q}[X]/(f)$ perché (f_1) e (f_2) sono massimali in $\mathbb{Q}[X]$ (dato che f_1 e f_2 sono irriducibili nel dominio a ideali principali $\mathbb{Q}[X]$).

   (c) L'ideale considerato coincide con $(2, f)/(f)$ in $\mathbb{Z}[X]/(f)$. Si tratta allora di dimostrare che $(f) \subsetneq (2, f) \subsetneq \mathbb{Z}[X]$ e che $(2, f)$ non è primo in $\mathbb{Z}[X]$ (infatti, se I è un ideale di $\mathbb{Z}[X]$ contenente (f), $I/(f)$ è primo in $\mathbb{Z}[X]/(f)$ se e solo se $(\mathbb{Z}[X]/(f))/(I/(f))$ è un dominio, ma, per il terzo teorema di isomorfismo, quest'ultimo

anello è isomorfo a $\mathbb{Z}[X]/I$, che è un dominio se e solo se I è primo in $\mathbb{Z}[X]$). Chiaramente $(f) \subsetneq (2, f)$ (visto che $2 \notin (f)$, cioè $f \nmid 2$) e $(2, f) \subsetneq \mathbb{Z}[X]$ (basta osservare che il termine noto di ogni elemento di $(2, f)$ è pari). Resta dunque da dimostrare che $(2, f)$ non è primo in $\mathbb{Z}[X]$, cioè che $\mathbb{Z}[X]/(2, f)$ non è un dominio. Ora, sempre per il terzo teorema di isomorfismo per anelli, si ha

$$\mathbb{Z}[X]/(2, f) \cong (\mathbb{Z}[X]/(2))/(\overline{f}) \cong \mathbb{Z}/2\mathbb{Z}[X]/(\overline{f})$$

($\overline{f}$ indica l'immagine di f in $\mathbb{Z}/2\mathbb{Z}[X]$), e quest'ultimo anello non è un dominio perché $(\overline{f})$ non è primo in $\mathbb{Z}/2\mathbb{Z}[X]$ (infatti $\overline{f} = X^5 + X^4 = X^4(X + \overline{1})$ non è irriducibile).