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

Prova scritta del 13.7.2016

1. Sia G un gruppo e $\mathrm{Aut}(G)$ il suo gruppo degli automorfismi. Dato $g \in G$, sia
$$H_g := \{\phi \in \mathrm{Aut}(G) \,:\, \phi(g) = g\}.$$
   (a) Dimostrare che H_g è un sottogruppo di $\mathrm{Aut}(G)$.
   (b) Dimostrare che H_g è normale in $\mathrm{Aut}(G)$ se e solo se $H_g \subseteq H_{\psi(g)}$ per ogni $\psi \in \mathrm{Aut}(G)$.
   (c) Stabilire se $H_{(1,2,3)}$ è normale in $\mathrm{Aut}(S_3)$.

2. Sia $n > 1$ un intero e $f\colon \mathbb{Z}/n\mathbb{Z}^* \to \mathbb{Z}/n\mathbb{Z}$ un omomorfismo di gruppi.
   (a) Dimostrare che se n è primo allora f è banale.
   (b) Dimostrare che se f è iniettivo allora n è pari.
   (c) Dimostrare che f non è iniettivo se $n = 8$.

3. Sia A un anello commutativo con un unico ideale I tale che $I \neq \{0\}$ e $I \neq A$.
   (a) Dimostrare che I è un ideale principale.
   (b) Dimostrare che A non è un dominio.
   (c) Può essere $A = \mathbb{Z}/n\mathbb{Z}$ per qualche intero positivo n?

4. (a) Sia A un anello commutativo e $p \in A[X]$. Dimostrare che l'ideale (X, p) è primo (rispettivamente massimale) in $A[X]$ se e solo se l'ideale $(p(0))$ è primo (rispettivamente massimale) in A.
   (b) Stabilire per ciascuno dei seguenti ideali se è primo e/o massimale in $\mathbb{R}[X, Y]$:
   - $I_1 = (X, Y + 1)$;
   - $I_2 = (X, Y^2 + 1)$;
   - $I_3 = (X, Y^2 + X^3)$;
   - $I_4 = (XY - 1)$.

Soluzioni

1. (a) Chiaramente $\mathrm{id}_G \in H_g$. Se $\phi, \psi \in H_g$ allora anche $\phi \circ \psi \in H_g$ perché $(\phi \circ \psi)(g) = \phi(\psi(g)) = \phi(g) = g$. Inoltre, se $\phi \in H_g$ allora $\phi^{-1} \in H_g$ perché $\phi^{-1}(g) = \phi^{-1}(\phi(g)) = g$.

   (b) H_g è normale in $\mathrm{Aut}(G)$ se e solo se $\psi \circ \phi \circ \psi^{-1} \in H_g$ per ogni $\phi \in H_g$ e per ogni $\psi \in \mathrm{Aut}(G)$. Inoltre, per definizione, $\psi \circ \phi \circ \psi^{-1} \in H_g$ se e solo se $g = (\psi \circ \phi \circ \psi^{-1})(g)$. Essendo ψ^{-1} iniettivo, tale uguaglianza vale se e solo se

   $$\psi^{-1}(g) = \psi^{-1}((\psi \circ \phi \circ \psi^{-1})(g)) = \phi(\psi^{-1}(g)),$$

   che, di nuovo per definizione, è verificata se e solo se $\phi \in H_{\psi^{-1}(g)}$. Ciò dimostra che H_g è normale se e solo se $H_g \subseteq H_{\psi^{-1}(g)}$ per ogni $\psi \in \mathrm{Aut}(G)$, e per concludere basta osservare che ogni elemento di $\mathrm{Aut}(G)$ è della forma ψ^{-1} per un unico $\psi \in \mathrm{Aut}(G)$.

   (c) Per il punto precedente $H_{(1,2,3)}$ è normale in $\mathrm{Aut}(S_3)$ se e solo se $H_{(1,2,3)} \subseteq H_{\psi((1,2,3))}$ per ogni $\psi \in \mathrm{Aut}(S_3)$. Poiché un automorfismo preserva l'ordine degli elementi, $\psi((1,2,3))$ ha ordine 3, e quindi $\psi((1,2,3))$ può essere solo $(1,2,3)$ o $(1,3,2)$. Ovviamente $H_{(1,2,3)} \subseteq H_{(1,2,3)}$, e basta allora verificare se $H_{(1,2,3)} \subseteq H_{(1,3,2)}$. In effetti, dato $\phi \in H_{(1,2,3)}$ (cioè tale che $\phi((1,2,3)) = (1,2,3)$), si ha

   $$\phi((1,3,2)) = \phi((1,2,3)^{-1}) = \phi((1,2,3))^{-1} = (1,2,3)^{-1} = (1,3,2)$$

   (cioè $\phi \in H_{(1,3,2)}$), e dunque $H_{(1,2,3)}$ è normale in $\mathrm{Aut}(S_3)$.

2. (a) Dato $g \in \mathbb{Z}/n\mathbb{Z}^*$, per il teorema di Lagrange si ha $\mathrm{ord}(g) \mid \varphi(n) = n-1$ (perché n è primo) e $\mathrm{ord}(f(g)) \mid n$. D'altra parte, essendo f un omomorfismo, $\mathrm{ord}(f(g)) \mid \mathrm{ord}(g)$, e dunque $\mathrm{ord}(f(g)) \mid (n-1)$. Ne segue che $\mathrm{ord}(f(g)) \mid \mathrm{mcd}(n-1, n) = 1$. Ciò dimostra che $f(g) = \overline{0}$, per cui f è l'omomorfismo banale.

   (b) Se f è iniettivo, l'immagine di f è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ isomorfo a $\mathbb{Z}/n\mathbb{Z}^*$, e quindi $\varphi(n) \mid n$ per il teorema di Lagrange. Per concludere che n è pari basta allora dimostrare che $\varphi(n) \nmid n$ se n è dispari. Se $n = \prod_{i=1}^{k} p_i^{a_i}$ con $k \geq 1$ (perché $n > 1$), i p_i primi distinti e gli $a_i > 0$, risulta $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$, da cui $(p_1 - 1) \mid \varphi(n)$. Ora, se n è dispari, anche p_1 lo è, e allora $p_1 - 1$ è pari. Se ne deduce che $\varphi(n)$ è pari e pertanto $\varphi(n) \nmid n$.

(c) Come osservato nel punto precedente, se f fosse iniettivo l'immagine di f sarebbe un sottogruppo di $\mathbb{Z}/8\mathbb{Z}$ isomorfo a $\mathbb{Z}/8\mathbb{Z}^*$. Questo non è possibile perché ogni sottogruppo di un gruppo ciclico è ciclico, mentre $\mathbb{Z}/8\mathbb{Z}^*$ è un gruppo non ciclico di ordine 4 (è infatti immediato verificare che $g^2 = \overline{1}$ per ogni $g \in \mathbb{Z}/8\mathbb{Z}^*$).

3. (a) Preso $0 \neq a \in I$, si ha $a \in (a) \subseteq I$. In particolare $(a) \neq 0$ e $(a) \neq A$, e quindi, per l'unicità di I, deve essere $I = (a)$, cioè I è principale.

   (b) Come visto nel punto precedente, scelto $0 \neq a \in I$, vale $I = (a)$. Posso supporre $a^2 \neq 0$ (altrimenti è ovvio che A non è un dominio), e quindi anche $I = (a^2)$. Ne segue che $a \in (a^2)$, cioè esiste $b \in A$ tale che $a = a^2b$. Perciò $a(1-ab) = 0$, il che dimostra che A non è un dominio, dato che $a \neq 0$ per ipotesi e $1 - ab \neq 0$ perché $a \notin A^*$ (altrimenti si avrebbe $I = A$).

   (c) Gli ideali di $\mathbb{Z}/n\mathbb{Z}$ sono tutti e soli della forma $d\mathbb{Z}/n\mathbb{Z}$ con d intero positivo tale che $d \mid n$. Pertanto $\mathbb{Z}/n\mathbb{Z}$ ha la proprietà richiesta se e solo se esiste unico $1 < d < n$ tale che $d \mid n$. È chiaro che questo succede se (e solo se) $n = p^2$ con p un numero primo (e in tal caso $d = p$).

4. (a) Per il terzo teorema di isomorfismo per anelli

$$A[X]/(X, p) \cong (A[X]/(X))/(\overline{p}).$$

   Ora, $A[X]/(X) \cong A$ e l'isomorfismo è indotto dall'omomorfismo di valutazione $A[X] \to A$, $f \mapsto f(0)$, per cui la classe $\overline{p}$ di p in $A[X]/(X)$ corrisponde a $p(0) \in A$. Si ottiene allora $A[X]/(X, p) \cong A/(p(0))$, e dunque si conclude che (X, p) è primo (rispettivamente massimale) in $A[X]$ se e solo se $A[X]/(X, p)$ è un dominio (rispettivamente un campo) se e solo se $A/(p(0))$ è un dominio (rispettivamente un campo) se e solo se $(p(0))$ è primo (rispettivamente massimale) in A.

   (b) Per il punto precedente I_1 è primo (rispettivamente massimale) in $\mathbb{R}[X, Y] \cong \mathbb{R}[Y][X]$ se e solo se $(Y + 1)$ è primo (rispettivamente massimale) in $\mathbb{R}[Y]$. Poiché $\mathbb{R}[Y]$ è un dominio a ideali principali e $Y + 1$ è irriducibile in $\mathbb{R}[Y]$ (avendo grado 1), si conclude che I_1 è primo e massimale. Analogamente I_2 è primo e massimale perché $Y^2 + 1$ è irriducibile in $\mathbb{R}[Y]$ (avendo grado 2 e non avendo radici), mentre I_3 non è né primo né massimale perché Y^2 (cioè $Y^2 + X^3$ valutato in $X = 0$) è ovviamente riducibile in $\mathbb{R}[Y]$.

Essendo $\mathbb{R}[X,Y]$ un dominio a fattorizzazione unica, I_4 è primo se e solo se $XY-1$ è irriducibile (o 0). Chiaramente $XY-1 \neq 0$ e $XY-1 \notin \mathbb{R}[X,Y]^* = \mathbb{R}^*$. Se poi $XY-1 = qr$, a meno di scambiare q e r posso supporre che i gradi rispetto a X di q e r siano rispettivamente 1 e 0. Dunque esistono $f,g,h \in \mathbb{R}[Y]$ tali che $q = fX+g$ e $r = h$, cioè $fh = Y$ e $gh = 1$. L'ultima uguaglianza mostra che $r = h \in \mathbb{R}[Y]^* = \mathbb{R}[X,Y]^*$; pertanto $XY-1$ è irriducibile e I_4 è primo. Invece I_4 non è massimale perché per esempio

$$I_4 \subsetneq (X-1, Y-1) \subsetneq \mathbb{R}[X,Y].$$

Infatti $XY-1 = (X-1)Y+(Y-1) \in (X-1,Y-1)$, e ciò implica che $I_4 \subseteq (X-1,Y-1)$. D'altra parte è facile vedere che $X-1 \notin I_4$ (il che dimostra che $I_4 \neq (X-1,Y-1)$): altrimenti esisterebbe $f \in \mathbb{R}[X,Y]$ tale che $X-1 = (XY-1)f$, e necessariamente il grado rispetto a X di f sarebbe 0, cioè $f \in \mathbb{R}[Y]$, il che darebbe l'assurdo $Yf = 1$ e $f = 1$. Infine $(X-1,Y-1) \neq \mathbb{R}[X,Y]$ perché $f(1,1) = 0$ per ogni $f \in (X-1,Y-1)$, e quindi $1 \notin (X-1,Y-1)$.