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

Prova scritta del 27.2.2015

1. Siano p e q due numeri primi e sia G un gruppo di ordine pq.
   (a) Siano H e K sottogruppi di G tali che $\{1\} \subsetneq H \subsetneq K$. Dimostrare che $K = G$.
   (b) Dimostrare che se $Z(G) \neq \{1\}$ allora G è abeliano.
2. Sia G un gruppo e $n \geq 2$ un intero. Dimostrare che le seguenti condizioni sono equivalenti:
   (a) G contiene un sottogruppo di indice 2;
   (b) esiste un omomorfismo suriettivo da G a $\mathbb{Z}/2\mathbb{Z}$;
   (c) esiste un omomorfismo da G a S_n la cui immagine non è contenuta in A_n.
3. Siano $f, g\colon A \to B$ omomorfismi di anelli.
   (a) Dimostrare che $A' = \{a \in A : f(a) = g(a)\}$ è un sottoanello di A.
   (b) Dimostrare che se A è un campo anche A' lo è.
   (c) Dimostrare che se $A = \mathbb{Q}$ allora $A' = A$.
4. Sia I un ideale di $\mathbb{Z}[X]$ tale che $2 \in I$.
   (a) Dimostrare che esiste $p(X) \in \mathbb{Z}[X]$ tale che $I = (2, p(X))$.
   (b) Verificare che $(2, X^4 + X^2 + 1)$ non è un ideale primo di $\mathbb{Z}[X]$.
   (c) Verificare che $(2, X^4 + X^3 + X^2 + X + 1)$ è un ideale massimale di $\mathbb{Z}[X]$.

Soluzioni

1. (a) Indicando con m l'ordine di H e con n l'ordine di K, per il teorema di Lagrange si ha $m \mid n \mid pq$, e per ipotesi $1 < m < n$. Ne segue che necessariamente $m = p$ o $m = q$ e $n = pq$, e quindi $K = G$.

   (b) Posto $H = Z(G)$, G è abeliano se e solo se $H = G$. Supponendo per assurdo $H \neq G$, sia $a \in G \setminus H$ e sia $K = \{g \in G : ag = ga\}$ il centralizzante di a. Chiaramente $H \subseteq K$ e $a \in K$, dunque $H \subsetneq K$; inoltre $H \neq \{1\}$ per ipotesi e H e K sono sottogruppi di G. Per la prima parte si ottiene allora $K = G$, il che implica $a \in Z(G) = H$, assurdo.

2. (a) $\implies$ (b) Sia H un sottogruppo di G di indice 2. Poiché H è normale, G/H è un gruppo di ordine 2 e la proiezione naturale $\pi\colon G \to G/H$ è un omomorfismo suriettivo. Dato che ogni gruppo di ordine 2 è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, esiste un isomorfismo $\phi\colon G/H \to \mathbb{Z}/2\mathbb{Z}$. Allora $\phi \circ \pi\colon G \to \mathbb{Z}/2\mathbb{Z}$ è un omomorfismo suriettivo perché composizione di omomorfismi suriettivi.

   (b) $\implies$ (c) Sia $f\colon G \to \mathbb{Z}/2\mathbb{Z}$ un omomorfismo suriettivo. Scelto $\sigma \in S_n \setminus A_n$ di ordine 2 (per esempio $\sigma = (1, 2)$), la funzione $g\colon \mathbb{Z}/2\mathbb{Z} \to S_n$ definita da $g(\bar{0}) = (1)$ e $g(\bar{1}) = \sigma$ è un omomorfismo (iniettivo) con immagine $I = \{(1), \sigma\}$. Allora $g \circ f\colon G \to S_n$ è un omorfismo con immagine I, dunque non contenuta in A_n.

   (c) $\implies$ (a) Sia $h\colon G \to S_n$ un omomorfismo con immagine non contenuta in A_n. Essendo A_n un sottogruppo normale di indice 2 di S_n, $G' = S_n/A_n$ è un gruppo di ordine 2 e la proiezione naturale $p\colon S_n \to G'$ è un omomorfismo suriettivo con nucleo A_n. Ne segue che $p \circ h\colon G \to G'$ è un omomorfismo suriettivo (altrimenti la sua immagine sarebbe costituita dal solo elemento neutro di G', e quindi l'immagine di h sarebbe contenuta in A_n). Per il primo teorema di isomorfismo si ottiene $G' \cong G/H$ con $H = \ker(p \circ h)$ e H è un sottogruppo (normale) di G di indice 2 perché $\#(G/H) = \#G' = 2$.

3. (a) Dati $a_1, a_2 \in A'$ (cioè elementi di A tali che $f(a_i) = g(a_i)$ per $i = 1, 2$), essendo f e g omomorfismi di anelli si ha

$$f(a_1 - a_2) = f(a_1) - f(a_2) = g(a_1) - g(a_2) = g(a_1 - a_2)$$
$$f(a_1 a_2) = f(a_1) f(a_2) = g(a_1) g(a_2) = g(a_1 a_2)$$

e quindi $a_1 - a_2, a_1 a_2 \in A'$; inoltre $f(1_A) = 1_B = g(1_A)$, per cui anche $1_A \in A'$. Ciò dimostra che A' è un sottoanello di A.

(b) Se A è un campo, A' è un anello commutativo non banale perché sottoanello di A che lo è. Per dimostrare che A' è un campo resta dunque da verificare che $a^{-1} \in A'$ per ogni $a \in A' \setminus \{0\}$. Poiché $a \in A^*$ e f e g sono omomorfismi di anelli, $f(a), g(a) \in B^*$ e $f(a^{-1}) = f(a)^{-1} = g(a)^{-1} = g(a^{-1})$, per cui $a^{-1} \in A'$.

(c) Per il punto precedente basta dimostrare che se un sottoanello A' di $\mathbb{Q}$ è un campo, allora $A' = \mathbb{Q}$. Infatti $1 \in A'$ e A' è in particolare un sottogruppo di $\mathbb{Q}$, per cui $A' \supseteq \mathbb{Z}$, che è il sottogruppo generato da 1. Inoltre $n^{-1} \in A'$ per ogni $n \in \mathbb{Z} \setminus \{0\} \subseteq A' \setminus \{0\}$ perché A' è un campo. Preso allora $q \in \mathbb{Q}$, per definizione esistono $m, n \in \mathbb{Z}$ con $n \neq 0$ tali che $q = mn^{-1}$, e si conclude che $q \in A'$ perché $m, n^{-1} \in A'$ e A' è un sottoanello di $\mathbb{Q}$.

4. (a) Posto $A = \mathbb{Z}[X]$ e $J = (2)$, l'ipotesi $2 \in I$ implica chiaramente $J \subseteq I$. Essendo $A/J \cong \mathbb{Z}/2\mathbb{Z}[X]$ un dominio a ideali principali (perché $\mathbb{Z}/2\mathbb{Z}$ è un campo), l'ideale I/J di A/J è principale. Esiste dunque $p \in A$ tale che I/J è generato da $\bar{p} = p + J$, da cui segue che $I = (2, p)$. Infatti, sia I che $(2, p)$ sono ideali di A contenenti J e (nella corrispondenza biunivoca tra ideali di A contententi J e ideali di A/J) entrambi corrispondono a I/J.

(b) Usando la notazione del punto precedente con $p = X^4 + X^2 + 1$, I è primo (rispettivamente massimale) se e solo se A/I è un dominio (rispettivamente un campo). Per il terzo teorema di isomorfismo $A/I \cong (A/J)/(I/J)$, dunque I è primo (rispettivamente massimale) in A se e solo se $I/J = (\bar{p})$ è primo (rispettivamente massimale) in A/J. Poiché $p \notin J$, risulta $\bar{p} \neq 0$ e quindi, essendo A/J un dominio a ideali principali, I/J è primo se e solo se I/J è massimale se e solo se $\bar{p}$ è irriducibile. Ora, nell'isomorfismo tra A/J e $\mathbb{Z}/2\mathbb{Z}[X]$, $\bar{p}$ corrisponde a p, visto come polinomio a coefficienti in $\mathbb{Z}/2\mathbb{Z}$. Si tratta perciò di dimostrare che p non è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$, e in effetti si ha $p = (X^2 + X + 1)^2$.

(c) Ragionando come nel punto precedente, basta dimostrare che $p = X^4 + X^3 + X^2 + X + 1$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$. Per questo, basta osservare che p non ha radici (perché $p(0) = p(1) = 1$) e non è divisibile per l'unico polinomio irriducibile di secondo grado di $\mathbb{Z}/2\mathbb{Z}[X]$, cioè $X^2 + X + 1$ (perché $p = X^2(X^2 + X + 1) + X + 1$, il che mostra che il resto della divisione di p per $X^2 + X + 1$ è $X + 1$).