Corso di Algebra 1 - a.a. 2009-2010

Prova scritta del 2.2.2010

1. Per quali $n \in \mathbb{N}$ vale $2^n \equiv 3^n \mod 7$?

2. Se G è un gruppo, $[G, G]$ indica il sottogruppo (normale) dei commutatori di G, cioè il sottogruppo generato dal sottoinsieme di G

$$\{aba^{-1}b^{-1} \ : \ a, b \in G\}.$$

   Dimostrare che $[D_4, D_4]$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$ e $D_4/[D_4, D_4]$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Sia $f\colon G \to G'$ un omomorfismo di gruppi.

   (a) Dimostrare che se f è suriettivo, allora $f(Z(G)) \subseteq Z(G')$.

   (b) Dimostrare che se f è un isomorfismo, allora $f(Z(G)) = Z(G')$.

4. Sia A un anello commutativo e $a \in A$ un elemento non nullo e non invertibile.

   (a) Dimostrare che se A è un dominio di integrità, allora $(a^2) \subsetneq (a)$.

   (b) Fornire un esempio in cui $(a^2) = (a)$.

5. Dire se l'ideale $(3X^2 + 4X + 1)$ in $A[X]$ è primo e/o massimale nei seguenti casi:

   (a) $A = \mathbb{Z}/3\mathbb{Z}$;

   (b) $A = \mathbb{Q}$.

Soluzioni

1. Denotando con $\bar{a}$ la classe di un intero a in $\mathbb{Z}/7\mathbb{Z}$, un naturale n verifica la congruenza data se e solo se $\bar{2}^n = \bar{3}^n$. Osservando che $\bar{2}, \bar{3} \in \mathbb{Z}/7\mathbb{Z}^*$ (perché $\mathrm{mcd}(2,7) = \mathrm{mcd}(3,7) = 1$), quest'ultima uguaglianza è equivalente a $(\bar{2}^{-1} \cdot \bar{3})^n = \bar{1}$, che è verificata se e solo se n è un multiplo dell'ordine (in $\mathbb{Z}/7\mathbb{Z}^*$) di $\bar{2}^{-1} \cdot \bar{3} = \bar{4} \cdot \bar{3} = \bar{5}$. È facile verificare che $\mathrm{ord}(\bar{5}) = 6$: per il teorema di Lagrange $\mathrm{ord}(\bar{5}) | \#(\mathbb{Z}/7\mathbb{Z}^*) = 6$ e $\mathrm{ord}(\bar{5}) > 3$ perché $\bar{5}^1 = \bar{5} \neq \bar{1}$, $\bar{5}^2 = \bar{4} \neq \bar{1}$, $\bar{5}^3 = \bar{6} \neq \bar{1}$. Dunque gli $n \in \mathbb{N}$ cercati sono i multipli di 6.

2. Indichiamo con $R^i S^j$ $(i = 0, \ldots, 3,\ j = 0, 1)$ gli elementi di D_4 e poniamo $H = [D_4, D_4]$.

   (a) Ricordando che $\mathrm{ord}(R) = 4$, $\mathrm{ord}(S) = 2$ e che vale la relazione $SR = R^{-1}S$, determiniamo il commutatore $[a,b] = aba^{-1}b^{-1}$ di due elementi $a, b \in D_4$ nei vari casi. Se $a = R^i$ e $b = R^j$,

   $$[a,b] = R^i R^j R^{-i} R^{-j} = 1.$$

   Se $a = R^i$ e $b = R^j S$,

   $$[a,b] = R^i R^j S R^{-i} S R^{-j} = R^{2i}.$$

   Se $a = R^i S$ e $b = R^j$,

   $$[a,b] = R^i S R^j S R^{-i} R^{-j} = R^{-2j}.$$

   Se $a = R^i S$ e $b = R^j S$,

   $$[a,b] = R^i S R^j S S R^{-i} S R^{-j} = R^{2i-2j}.$$

   Ne segue che l'insieme dei commutatori in D_4 è $\{1, R^2\}$, che è un sottogruppo di D_4, come è immediato verificare. Dunque $H = \{1, R^2\} \cong \mathbb{Z}/2\mathbb{Z}$.

   (b) Per ogni $a \in D_4$ si ha $a^2 \in H$ (per la precisione, $a^2 = 1$ se $a = 1$, $a = R^2$ o $a = R^i S$, mentre $a^2 = R^2$ se $a = R$ o $a = R^3$). Perciò nel gruppo quoziente $G = D_4/H$ si ha $g^2 = 1$ per ogni $g \in G$. Essendo G un gruppo di ordine $(\#D_4)/(\#H) = 8/2 = 4$, e sapendo che ogni gruppo di ordine 4 è isomorfo a $\mathbb{Z}/4\mathbb{Z}$ o a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, concludiamo che deve essere $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. (a) Bisogna dimostrare che se $a \in Z(G)$, allora $f(a) \in Z(G')$, cioè che $f(a)b' = b'f(a)$ per ogni $b' \in G'$. Essendo f suriettivo, esiste $b \in G$ tale che $f(b) = b'$, per cui usando il fatto che $ab = ba$ e che f è un omomorfismo concludiamo che

$$f(a)b' = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b'f(a).$$

   (b) Grazie alla prima parte resta da dimostrare che $Z(G') \subseteq f(Z(G))$. Dato $a' \in Z(G')$, poiché f è suriettivo esiste $a \in G$ tale che $a' = f(a)$, e basta provare che $a \in Z(G)$, cioè che $ab = ba$ per ogni $b \in G$. Usando il fatto che $a' \in Z(G')$ e che f è un omomorfismo, troviamo

$$f(ab) = f(a)f(b) = a'f(b) = f(b)a' = f(b)f(a) = f(ba),$$

   il che implica $ab = ba$ perché f è iniettivo.

4. (a) Poiché $a^2 \in (a)$, si ha $(a^2) \subseteq (a)$. Inoltre ovviamente $a \in (a)$, quindi per concludere che $(a^2) \neq (a)$ basta dimostrare che $a \notin (a^2)$. Supponendo per assurdo che $a \in (a^2)$, esisterebbe $b \in A$ tale che $a = a^2b$, cioè $a(1 - ab) = 0$. Essendo A un dominio, da ciò seguirebbe che $a = 0$ o $ab = 1$ (per cui $a \in A^*$), contro l'ipotesi.

   (b) Un esempio è dato da $A = \mathbb{Z}/6\mathbb{Z}$ e $a = \bar{3}$: infatti si ha

$$a^2 = \bar{3}^2 = \bar{9} = \bar{3} = a,$$

   e dunque $(a^2) = (a)$.

5. In entrambi i casi, essendo A un campo e quindi $A[X]$ un dominio a ideali principali, l'ideale generato da $f = 3X^2+4X+1 \neq 0$ è massimale se e solo se è primo se e solo se f è irriducibile.

   (a) $f = X + 1$ è irriducibile, dunque (f) è primo e massimale.

   (b) $f = (X+1)(3X+1)$ non è irriducibile, dunque (f) non è né primo né massimale.