Corso di Algebra 1 - a.a. 2022-2023

Prova scritta del 04/07/2023

1. Sia G il gruppo $D_3 \times D_3$.
   (a) Quanti elementi di ordine 6 ci sono in G?
   (b) Dimostrare che nessun sottogruppo ciclico di ordine 6 di G è normale.
   (c) Trovare un sottogruppo normale H di G tale che $H \cong G/H$.
   (d) Trovare un sottogruppo di ordine 6 non ciclico e non normale di G.

2. Indicando con f il polinomio $15X^4 + 10X^3 + 2X^2 + X - 4$, per ogni numero primo p sia $A_p := \mathbb{Z}/p\mathbb{Z}[X]/(f)$.
   (a) Dimostrare che A_5 è un campo.
   (b) Dimostrare che ogni ideale non banale di A_3 è massimale.
   (c) Trovare un ideale non banale e non primo di A_2.
   (d) Determinare il più piccolo valore di p tale che esiste un omomorfismo di anelli $A_p \to \mathbb{Z}/p\mathbb{Z}$.

Soluzioni

1. (a) Poiché $\mathrm{ord}((a,b)) = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b))$ per ogni $a, b \in D_3$ e in D_3 ci sono solo elementi di ordine 1, 2 e 3, si ha $\mathrm{ord}((a,b)) = 6$ se e solo se $\mathrm{ord}(a) = 3$ e $\mathrm{ord}(b) = 2$ o $\mathrm{ord}(a) = 2$ e $\mathrm{ord}(b) = 3$. Dato che in D_3 ci sono 2 elementi di ordine 3 (R e R^2) e 3 elementi di ordine 2 (S, RS e R^2S), si conclude che in G ci sono $2 \cdot 3 + 3 \cdot 2 = 12$ elementi di ordine 6.

   (b) Un sottogruppo ciclico di ordine 6 di G è della forma

$$\langle (a,b) \rangle = \{(a,b)^k = (a^k, b^k) \,:\, k \in \mathbb{Z}\}$$

   con $(a,b) \in G$ di ordine 6. Per quanto visto nel punto precedente deve essere $a = R^i$ con $i = 1, 2$ e $b = R^j S$ con $j = 1, 2, 3$, o viceversa. Supponendo di essere nel primo caso (l'altro è del tutto analogo), $\langle (a,b) \rangle$ non è normale perché $(R^i, R^j S) = (a,b) \in \langle (a,b) \rangle$, mentre

$$(1,S)(R^i, R^j S)(1,S)^{-1} = (R^i, SR^j S S^{-1}) = (R^i, R^{-j} S) \notin \langle (a,b) \rangle$$

   (infatti $R^{-j}S$ è diverso sia da $1 = (R^j S)^k$ per k pari che da $R^j S = (R^j S)^k$ per k dispari).

   (c) Si può prendere $H = D_3 \times \{1\}$. Infatti

$$\begin{aligned} f \colon G &\to D_3 \\ (a,b) &\mapsto b \end{aligned}$$

   è un omomorfismo suriettivo con $\ker(f) = H$. Dunque H è un sottogruppo normale di G e, per il primo teorema di isomorfismo, $D_3 = \mathrm{im}(f) \cong G/\ker(f) = G/H$. Infine $H \cong G/H$ perché chiaramente anche $H \cong D_3$.

   (d) Sia $K := \{(a,a) \,:\, a \in D_3\}$. Allora K è un sottogruppo di G isomorfo a D_3 (quindi di ordine 6 e non ciclico): infatti $K = \mathrm{im}(g)$, dove

$$\begin{aligned} g \colon D_3 &\to G \\ a &\mapsto (a,a) \end{aligned}$$

   è un omomorfismo iniettivo. Infine K non è normale perché per esempio $(R,R) \in K$, ma

$$(1,S)(R,R)(1,S)^{-1} = (R, SRS^{-1}) = (R, R^{-1}) \notin K.$$

2. Ricordiamo preliminarmente che $\mathbb{Z}/p\mathbb{Z}[X]$ è un dominio a ideali principali (perché $\mathbb{Z}/p\mathbb{Z}$ è un campo, essendo p primo). Dunque, dato $g \in \mathbb{Z}/p\mathbb{Z}[X]$, si ha che g è irriducibile se e solo se (g) è primo se e solo (g) è massimale. Inoltre gli ideali di $A_p = \mathbb{Z}/p\mathbb{Z}[X]/(f)$ sono tutti e soli della forma $I/(f)$ con I ideale di $\mathbb{Z}/p\mathbb{Z}[X]$ tale che $(f) \subseteq I$. Poiché I è principale, esiste (unico a meno di associati) $g \in \mathbb{Z}/p\mathbb{Z}[X]$ tale che $I = (g)$, e la condizione $(f) \subseteq I$ equivale a $g \mid f$. Quindi gli ideali di A_p sono in corrispondenza biunivoca con i divisori di f, a meno di associati. Chiaramente gli ideali banali corrispondono ai divisori banali 1 e f. D'altra parte, poiché (se $g \mid f$) $A_p/((g)/(f)) \cong \mathbb{Z}/p\mathbb{Z}[X]/(g)$ per il terzo teorema di isomorfismo per anelli, l'ideale $(g)/(f)$ è primo (o massimale) in A_p se e solo se (g) è primo (o massimale) in $\mathbb{Z}/p\mathbb{Z}[X]$ se e solo se g è irriducibile.

   (a) $f = 2X^2 + X + 1$ in $\mathbb{Z}/5\mathbb{Z}[X]$. È immediato verificare che f non ha radici in $\mathbb{Z}/5\mathbb{Z}$ e quindi (dato che $\deg(f) = 2$) è irriducibile. Allora (f) è massimale e pertanto A_5 è un campo.

   (b) $f = X^3 - X^2 + X - 1 = (X - 1)(X^2 + 1)$ in $\mathbb{Z}/3\mathbb{Z}[X]$, con X^2+1 è irriducibile perché di secondo grado e senza radici in $\mathbb{Z}/3\mathbb{Z}$. Dunque gli unici divisori non banali di f (a meno di associati), cioè $X - 1$ e $X^2 + 1$, sono irriducibili. Come spiegato all'inizio, ciò implica che gli ideali non banali di A_3 sono massimali.

   (c) $f = X^4 + X = X(X + 1)(X^2 + X + 1)$ in $\mathbb{Z}/2\mathbb{Z}[X]$. Allora per esempio $X^2 + X = X(X + 1)$ è un divisore non banale e non irriducibile di f, e quindi $(X^2 + X)/(f)$ è un ideale non banale e non primo di A_2.

   (d) Il valore cercato è $p = 2$. Infatti si può considerare per esempio l'omomorfismo di anelli

$$\begin{aligned} \alpha\colon \mathbb{Z}/2\mathbb{Z}[X] &\to \mathbb{Z}/2\mathbb{Z} \\ g &\mapsto g(\bar{0}) \end{aligned}$$

   Poiché $f \in \ker(\alpha)$ (cioè $f(\bar{0}) = \bar{0}$), e quindi $(f) \subseteq \ker \alpha$, per il teorema di omomorfismo per anelli esiste un omomorfismo di anelli $\beta\colon A_2 = \mathbb{Z}/2\mathbb{Z}[X]/(f) \to \mathbb{Z}/2\mathbb{Z}$ (ed è unico tale che $\beta(g + (f)) = \alpha(g)$ per ogni $g \in \mathbb{Z}/2\mathbb{Z}[X]$).