Corso di Algebra 1 - a.a. 2021-2022

Prova scritta del 14/06/2022

1. Sia G l'insieme $\mathbb{Z} \times \{\pm 1\}$ con l'operazione

$$G \times G \to G$$
$$\big((a,u),(b,v)\big) \mapsto (a+ub, uv)$$

   (a) Dimostrare che G è un gruppo.

   (b) Dimostrare che $H := \{(0,u) : u \in \{\pm 1\}\}$ e $K := \{(a,1) : a \in \mathbb{Z}\}$ sono sottogruppi di G.

   (c) Dimostrare che K è normale in G, mentre H non lo è.

   (d) Dimostrare che $K_n := \{(na,1) : a \in \mathbb{Z}\}$ è un sottogruppo normale di G e $G/K_n \cong D_n$ per ogni intero $n > 1$.

2. Sia $f \in \mathbb{Z}[X]$ monico, irriducibile e tale che $f(0) = 1$; sia inoltre $g := X^3 + 4X^2 + 6X + 4$.

   (a) Dimostrare che, dati un elemento a e un ideale I in un anello commutativo A, si ha $a + I \in (A/I)^*$ se e solo se $(a) + I = A$.

   (b) Dimostrare che $f + (g) \in (\mathbb{Q}[X]/(g))^*$.

   (c) Dimostrare che, se $\deg(f) = 1$, allora $f + (g) \in (\mathbb{Z}[X]/(g))^*$.

   (d) Fornire un esempio in cui $\deg(f) = 2$ e $f + (g) \notin (\mathbb{Z}[X]/(g))^*$.

Soluzioni

1. (a) L'operazione è associativa perché per ogni $a, b, c \in \mathbb{Z}$ e per ogni $u, v, w \in \{\pm 1\}$ si ha

$$[(a,u)(b,v)](c,w) = (a+ub, uv)(c,w) = (a+ub+uvc, uvw)$$
$$= (a+u(b+vc), uvw) = (a,u)(b+vc, vw) = (a,u)[(b,v)(c,w)].$$

L'elemento neutro è $(0,1)$, dato che

$$(a,u)(0,1) = (a+u0, u1) = (a,u) = (0+1a, 1u) = (0,1)(a,u),$$

e l'inverso di (a,u) è $(-ua, u^{-1})$ perché

$$(a,u)(-ua,u^{-1}) = (a-u^2a, uu^{-1}) = (0,1)$$
$$= (-ua+u^{-1}a, u^{-1}u) = (-ua,u^{-1})(a,u)$$

per ogni $a \in \mathbb{Z}$ e per ogni $u \in \{\pm 1\}$.

(b) H è un sottogruppo di G perché $(0,1) \in H$ e per ogni $u, v \in \{\pm 1\}$ si ha $(0,u)(0,v)^{-1} = (0,u)(0,v^{-1}) = (0,uv^{-1}) \in H$. Analogamente K è un sottogruppo di G perché $(0,1) \in K$ e per ogni $a, b \in \mathbb{Z}$ si ha $(a,1)(b,1)^{-1} = (a,1)(-b,1) = (a-b,1) \in K$.

(c) K è normale perché per ogni $(a,u) \in G$ e per ogni $(b,1) \in K$ (con $a, b \in \mathbb{Z}$ e $u \in \{\pm 1\}$) si ha

$$(a,u)(b,1)(a,u)^{-1} = (a+ub,u)(-ua,u^{-1})$$
$$= (a+ub-u^2a, uu^{-1}) = (ub,1) \in K.$$

D'altra parte H non è normale perché $(0,-1) \in H$, ma

$$(1,1)(0,-1)(1,1)^{-1} = (1,-1)(-1,1) = (2,-1) \notin H.$$

(d) La funzione $f\colon G \to D_n$, $(a,u) \mapsto R^aS^{\frac{1-u}{2}}$ è un omomorfismo perché per ogni $a, b \in \mathbb{Z}$ e per ogni $u, v \in \{\pm 1\}$ si ha (dato che in ogni caso $\frac{1-uv}{2} \equiv \frac{1-u}{2} + \frac{1-v}{2} \mod 2$)

$$f((a,u)(b,v)) = f((a+ub,uv)) = R^{a+ub}S^{\frac{1-uv}{2}}$$
$$= R^aR^{ub}S^{\frac{1-u}{2}}S^{\frac{1-v}{2}} = R^aS^{\frac{1-u}{2}}R^bS^{\frac{1-v}{2}} = f((a,u))f((b,v)).$$

Chiaramente f è suriettivo, dato che $R^a = f((a,1))$ e $R^aS = f((a,-1))$ per ogni $a \in \mathbb{Z}$. Inoltre $(a,u) \in \ker(f)$ se e solo se $R^aS^{\frac{1-u}{2}} = 1 \in D_n$ se e solo se $n \mid a$ e $u = 1$, per cui $\ker(f) = K_n$. Si conclude allora che K_n è normale in G e che $D_n = \operatorname{im}(f) \cong G/\ker(f) = G/K_n$ per il primo teorema di isomorfismo.

2. (a) Per definizione $a + I \in (A/I)^*$ se e solo se esiste $b \in A$ tale che $1 + I = (a + I)(b + I) = ab + I$. Poiché $1 + I = ab + I$ se e solo se $1 \in ab + I$, otteniamo $a + I \in (A/I)^*$ se e solo se $1 \in (a) + I$ se e solo se $(a) + I = A$.

   (b) Le possibili radici razionali di g sono $\pm 1, \pm 2, \pm 4$, e si verifica subito che l'unica radice è -2. Si trova quindi la fattorizzazione $g = g_1 g_2$ con $g_1 := X + 2$ e $g_2 := X^2 + 2X + 2$ irriducibili sia in $\mathbb{Z}[X]$ che in $\mathbb{Q}[X]$. Poiché $g_1(0) = g_2(0) = 2 \neq 1 = f(0)$, si ha $g_1, g_2 \neq f$ e pertanto (essendo tutti polinomi monici) f non è associato in $\mathbb{Q}[X]$ né a g_1 né a g_2. Per l'irriducibilità di f ne segue $\mathrm{mcd}(f, g) = 1$ in $\mathbb{Q}[X]$, e dunque (dato che $\mathbb{Q}[X]$ è un dominio a ideali principali) $(f) + (g) = (\mathrm{mcd}(f, g)) = \mathbb{Q}[X]$. Si conclude allora che $f + (g) \in (\mathbb{Q}[X]/(g))^*$ per il primo punto.

   (c) Facendo la divisione con resto in $\mathbb{Z}[X]$ di g per $f = X + 1$ si trova $g = qf + r$ con $r = g(-1) = 1$ (e $q = X^2 + 3X + 3$). Quindi $1 = r = g - qf \in (f) + (g)$ in $\mathbb{Z}[X]$, cioè $(f) + (g) = \mathbb{Z}[X]$, e si ottiene ancora $f + (g) \in (\mathbb{Z}[X]/(g))^*$ per il primo punto.

   (d) Si può prendere $f = X^2 + 1$ (che è irriducibile in $\mathbb{Z}[X]$ perché di secondo grado e senza radici razionali). Facendo la divisione con resto in $\mathbb{Z}[X]$ di g per f si trova $g = qf + r$ con $r = 5X$ (e $q = X + 4$). Poiché chiaramente $(f) + (g) = (f, g) = (f, r)$, per concludere che $f + (g) \notin (\mathbb{Z}[X]/(g))^*$ sempre per il primo punto basta dimostrare $1 \notin (f, r)$. Supponiamo per assurdo $1 \in (f, r)$, cioè $1 = fh + rk = (X^2 + 1)h + 5Xk$ con $h, k \in \mathbb{Z}[X]$. Se $h = \sum_{i \geq 0} a_i X^i$ (con $a_i \in \mathbb{Z}$ quasi tutti 0), non tutti gli a_i possono essere divisibili per 5, altrimenti lo sarebbero anche tutti i coefficienti di $1 = (X^2 + 1)h + 5Xk$. Deve allora esistere il massimo naturale n tale che a_n non è divisibile per 5, ma questo dà la contraddizione che anche il coefficiente di grado $n + 2$ di $1 = (X^2 + 1)h + 5Xk$ non è divisibile per 5.