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

Prova scritta del 15/02/2022

1. Sia G un gruppo e sia $a \in G$ un elemento di ordine m.
   (a) Dimostrare che, se $g \in G$ e $k \in \mathbb{Z}$ sono tali che $gag^{-1} = a^k$, allora $\mathrm{mcd}(m, k) = 1$.
   (b) Dimostrare che $N(a) := \{g \in G : gag^{-1} \in \langle a \rangle\}$ è un sottogruppo di G.
   (c) Dimostrare che la funzione $f\colon N(a) \to \mathbb{Z}/m\mathbb{Z}^*$, $g \mapsto \overline{k}$ con $k \in \mathbb{Z}$ tale che $gag^{-1} = a^k$ è ben definita ed è un omomorfismo di gruppi.
   (d) Dimostrare che, se $G = S_n$ e a è un m-ciclo (con $m \leq n$), allora f è suriettiva.

2. Dato un intero n, sia $f_n := X^4 + 6X^3 - 15X^2 + 6X + n \in \mathbb{Z}[X]$.
   (a) Trovare un intero n tale che $\mathbb{Q}[X]/(f_n)$ sia un campo.
   (b) Esiste un intero n tale che $\mathbb{Z}[X]/(2, f_n)$ sia un campo?
   (c) Dimostrare che esiste un unico intero n tale che $X^2 + 1 + (f_n)$ sia un divisore di zero in $\mathbb{Q}[X]/(f_n)$.
   (d) Determinare tutti gli ideali primi di $\mathbb{Q}[X]/(f_0)$.

Soluzioni

1. (a) Poiché $gag^{-1} = \varphi_g(a)$ con $\varphi_g\colon G \to G$, $x \mapsto gxg^{-1}$ automorfismo (interno), si ha $\mathrm{ord}(gag^{-1}) = \mathrm{ord}(a) = m$. Dunque nel nostro caso $\mathrm{ord}(a^k) = m$, ma in generale si ha anche $\mathrm{ord}(a^k) = \mathrm{ord}(a)/\mathrm{mcd}(\mathrm{ord}(a), k) = m/\mathrm{mcd}(m, k)$. Si conclude allora che $\mathrm{mcd}(m, k) = 1$.

   (b) Chiaramente $1 \in N(a)$ perché $1a1^{-1} = a \in \langle a\rangle$. Va poi dimostrato che $gg', g^{-1} \in N(a)$ per ogni $g, g' \in N(a)$. Per ipotesi esistono $k, k' \in \mathbb{Z}$ tali che $gag^{-1} = a^k$ e $g'ag'^{-1} = a^{k'}$, e pertanto

$$(gg')a(gg')^{-1} = g(g'ag'^{-1})g^{-1} = ga^{k'}g^{-1} \\ = (gag^{-1})^{k'} = (a^k)^{k'} = a^{kk'} \in \langle a\rangle,$$

   cioè $gg' \in N(a)$. Inoltre da $gag^{-1} = a^k$ segue $a = g^{-1}a^k g$. Tenendo conto che $\mathrm{mcd}(m, k) = 1$ per il punto precedente, esiste $l \in \mathbb{Z}$ tale che $kl \equiv 1 \mod m$. Dato che $\mathrm{ord}(a) = m$ si ha allora $a = a^{kl}$ e quindi

$$g^{-1}ag = g^{-1}a^{kl}g = (g^{-1}a^k g)^l = a^l \in \langle a\rangle,$$

   cioè $g^{-1} \in N(a)$.

   (c) Per definizione dato $g \in N(a)$ esiste $k \in \mathbb{Z}$ tale che $gag^{-1} = a^k$. Se poi $l \in \mathbb{Z}$ è tale che $a^k = a^l$, allora $k \equiv l \mod \mathrm{ord}(a) = m$, il che dimostra che $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ è ben definita. Inoltre $\overline{k} \in \mathbb{Z}/m\mathbb{Z}^*$ perché $\mathrm{mcd}(m, k) = 1$ per il primo punto; pertanto f risulta ben definita. Per dimostrare che f è un omomorfismo va verificato che $f(gg') = f(g)f(g')$ per ogni $g, g' \in N(a)$. Dati $k, k' \in \mathbb{Z}$ (coprimi con m) tali che $f(g) = \overline{k}$ e $f(g') = \overline{k'}$ (cioè $gag^{-1} = a^k$ e $g'ag'^{-1} = a^{k'}$) bisogna quindi dimostrare che $f(gg') = \overline{k}\,\overline{k'} = \overline{kk'}$ (cioè $(gg')a(gg')^{-1} = a^{kk'}$), il che è già stato visto nella dimostrazione del punto precedente.

   (d) Basta dimostrare che a^k è un m-ciclo per ogni $k \in \mathbb{Z}$ coprimo con m, perché poi, dato che due m-cicli sono coniugati in S_n, esiste $g \in S_n$ tale che $a^k = gag^{-1}$, cioè $\overline{k} = f(g)$. Osserviamo che in generale $\sigma \in S_n$ è un m-ciclo se e solo se esiste $M(\sigma) \subseteq \{1, \dots, n\}$ con $\#M(\sigma) = m$ tale che $\sigma(i) = i$ per $i \in \{1, \dots, n\} \setminus M(\sigma)$, mentre $\sigma^l(i) = i$ se e solo se $m \mid l$ per $i \in M(\sigma)$. Ora, essendo a un m-ciclo, esiste un tale $M(a)$, e per concludere basta dimostrare che risulta $M(a^k) = M(a)$. In effetti è ovvio che $a^k(i) = i$ per $i \in \{1, \dots, n\} \setminus M(a)$, mentre $(a^k)^l(i) = a^{kl}(i) = i$ se e solo se $m \mid kl$ se e solo se $m \mid l$ (essendo $\mathrm{mcd}(m, k) = 1$) per $i \in M(a)$.

2. (a) Si può prendere per esempio $n = 3$. Infatti f_3 è irriducibile in $\mathbb{Q}[X]$ per il criterio di Eisenstein relativo al primo 3, quindi (essendo $\mathbb{Q}[X]$ un dominio a ideali principali) (f_3) è un ideale massimale di $\mathbb{Q}[X]$ e $\mathbb{Q}[X]/(f_3)$ è un campo.

   (b) No, non esiste. Infatti
   $$\mathbb{Z}[X](2, f_n) \cong (\mathbb{Z}[X]/(2))/(\overline{f_n}) \cong \mathbb{Z}/2\mathbb{Z}[X]/(\overline{f_n})$$
   con $\overline{f_n} = X^4 + X^2 + \overline{n} \in \mathbb{Z}/2\mathbb{Z}[X]$. Poiché per n pari $\overline{f_n} = X^4 + X^2 = X^2(X+1)^2$ mentre per n dispari $\overline{f_n} = X^4 + X^2 + \overline{1} = (X^2 + X + \overline{1})^2$, in ogni caso $\overline{f_n}$ non è irriducibile, dunque $\mathbb{Z}[X](2, f_n) \cong \mathbb{Z}/2\mathbb{Z}[X]/(\overline{f_n})$ non è un campo.

   (c) Per definizione $g := X^2 + 1$ è tale che $\overline{g} := g + (f_n)$ è un divisore di zero in $\mathbb{Q}[X]/(f_n)$ se e solo se $\overline{g} \neq \overline{0}$ ed esiste $h \in \mathbb{Q}[X]$ tale che $\overline{h} \neq \overline{0}$ e $\overline{g}\overline{h} = \overline{gh} = \overline{0}$ (cioè $f_n \nmid g$, $f_n \nmid h$ e $f_n \mid gh$). Chiaramente $f_n \nmid g$, dato che $\deg(f_n) = 4 > 2 = \deg(g)$. D'altra parte g è irriducibile in $\mathbb{Q}[X]$ (perché di secondo grado e senza radici razionali), quindi condizione necessaria e sufficiente perché esista $h \in \mathbb{Q}[X]$ tale che $f_n \nmid h$ e $f_n \mid gh$ è che $g \mid f_n$. Infatti, se $g \mid f_n$, per definizione esiste $h \in \mathbb{Q}[X]$ tale che $f_n = gh$ (quindi $\deg(h) = \deg(f_n) - \deg(g) = 4 - 2 = 2$), il che dimostra che $f_n \nmid h$ e $f_n \mid gh$; se invece $g \nmid f_n$, per l'irriducibilità di g si ha $\mathrm{mcd}(f_n, g) = 1$, e dunque $f_n \mid gh$ implica $f_n \mid h$. Per concludere basta allora fare la divisione con resto di f_n per g: si trova quoziente $X^2 + 6X - 16$ e resto $n + 16$. Pertanto $g \mid f_n$ (cioè $\bar{g}$ è un divisore di zero in $\mathbb{Q}[X]/(f_n)$) se e solo se $n = -16$.

   (d) Ricordiamo che in generale, se I è un ideale di un anello A, gli ideali di A/I sono tutti e soli della forma J/I con J ideale di A contenente I; inoltre (quando A è commutativo) J/I è primo in A/I (se e solo se $(A/I)/(J/I)$ è un dominio) se e solo J è primo in A (se e solo se A/J è un dominio), dato che $(A/I)/(J/I) \cong A/J$ per il terzo teorema di isomorfismo. Nel nostro caso $A = \mathbb{Q}[X]$ (che è un dominio a ideali principali e quindi anche a fattorizzazione unica) e $I = (f_0)$, per cui gli ideali di $\mathbb{Q}[X]$ contenenti (f_0) sono tutti e soli della forma (g) con $g \in \mathbb{Q}[X]$ divisore di f_0; inoltre (g) è primo se e solo se g è irriducibile. Poiché $f_0 = X(X^3 + 6X^2 - 15X + 6)$ e entrambi i fattori sono irriducibili (il secondo sempre per il criterio di Eisenstein relativo al primo 3), si conclude che gli unici divisori irriducibili di f_0 (a meno di associati) sono X e $X^3 + 6X^2 - 15X + 6$, quindi gli unici ideali primi di $\mathbb{Q}[X]/(f_0)$ sono $(X)/(f_0)$ e $(X^3 + 6X^2 - 15X + 6)/(f_0)$.