Corso di Algebra 1 - a.a. 2023-2024

Prova scritta del 18/09/2024

1. Diciamo che un gruppo G *ha abbastanza sottogruppi normali* se per ogni sottogruppo H di G tale che $H \neq G$ esiste un sottogruppo normale H' di G tale che $H \subseteq H' \neq G$.

   (a) Dimostrare che D_3 non ha abbastanza sottogruppi normali.

   (b) Dimostrare che, se G ha abbastanza sottogruppi normali e K è un sottogruppo normale di G, allora anche G/K ha abbastanza sottogruppi normali.

   (c) Dimostrare che ogni sottogruppo H di G è normale in $Z(G)H$.

   (d) Dimostrare che, se $G/Z(G)$ ha abbastanza sottogruppi normali, allora anche G ha abbastanza sottogruppi normali.

2. Sia K un campo e sia $f \in K[X]$ un polinomio monico con $\deg(f) > 0$.

   (a) Dimostrare che gli unici ideali di $K[X]/(f)$ sono quelli banali se e solo se f è irriducibile in $K[X]$.

   (b) Dimostrare che $K[X]/(f)$ ha un solo ideale non banale se e solo se f è il quadrato di un polinomio irriducibile in $K[X]$.

   (c) Supponendo $f \in \mathbb{Z}[X]$ e $\deg(f) = 4$, dimostrare che f è irriducibile in $\mathbb{Q}[X]$ se esistono due numeri primi p e q con le seguenti proprietà (indicando con $\overline{f}$ l'immagine di f in $\mathbb{Z}/p\mathbb{Z}[X]$ o in $\mathbb{Z}/q\mathbb{Z}[X]$):
      - $\overline{f}$ non è irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$ e non ha radici in $\mathbb{Z}/p\mathbb{Z}$;
      - $\overline{f}$ ha una sola radice in $\mathbb{Z}/q\mathbb{Z}$ e tale radice ha molteplicità 1.

   (d) Stabilire se $\mathbb{Q}[X]/(X^4 - X^2 + 2X + 3)$ è un campo.

Soluzioni

1. (a) Per esempio $H := \langle S \rangle = \{1, S\}$ è un sottogruppo non normale di D_3 (perché $RSR^{-1} = R^2S \notin H$). D'altra parte, se $H < H' < D_3$ e $H' \neq D_3$, deve essere $H' = H$ (e quindi H' non è normale in D_3): infatti, per il teorema di Lagrange, si ha

$$2 = \#H \mid \#H' \mid \#D_3 = 6$$

e $\#H' < 6$, da cui segue $\#H' = 2$.

(b) Ogni sottogruppo di G/K è della forma H/K con $K < H < G$, e ovviamente $H/K \neq G/K$ se e solo se $H \neq G$. In tal caso, per l'ipotesi su G, esiste $H' \neq G$ tale che $H < H' \lhd G$. Ne segue che $H/K < H'/K \lhd G/K$ e $H'/K \neq G/K$, il che dimostra che G/K ha abbastanza sottogruppi normali.

(c) Si osservi che $Z(G)H < G$ perché $H < G$ e $Z(G) \lhd G$, e chiaramente $H < Z(G)H$. Va dimostrato che $aha^{-1} \in H$ per ogni $a \in Z(G)H$ e per ogni $h \in H$. Per definizione esistono $c \in Z(G)$ e $k \in H$ tali che $a = ck$, e dunque

$$aha^{-1} = ckh(ck)^{-1} = ckhk^{-1}c^{-1} = khk^{-1}cc^{-1} = khk^{-1} \in H$$

(per la penultima uguaglianza si è usato che $c \in Z(G)$, e la conclusione segue dal fatto che $h, k \in H$).

(d) Sia $H < G$ tale che $H \neq G$ e sia $\tilde{H} := Z(G)H$. Se $\tilde{H} = G$, allora (per il punto precedente) $H \lhd \tilde{H} = G$, per cui $H' = H$ è tale che $H < H' \lhd G$ con $H' \neq G$. Se invece $\tilde{H} \neq G$, tenendo conto che $Z(G) < \tilde{H}$, si ha $\tilde{H}/Z(G) < G/Z(G)$ con $\tilde{H}/Z(G) \neq G/Z(G)$. Per l'ipotesi su $G/Z(G)$ esiste quindi $\tilde{H}/Z(G) < K \lhd G/Z(G)$ con $K \neq G/Z(G)$. D'altra parte esiste (unico) $Z(G) < H' \lhd G$ tale che $K = H'/Z(G)$. Inoltre da $\tilde{H}/Z(G) < K = H'/Z(G)$ segue $\tilde{H} < H'$ e da $K = H'/Z(G) \neq G/Z(G)$ segue $H' \neq G$. Dato che $H < \tilde{H}$, si conclude che $H < H' \lhd G$ con $H' \neq G$. Pertanto G ha abbastanza sottogruppi normali.

2. Gli ideali di $K[X]/(f)$ sono tutti e soli della forma $I/(f)$ con I ideale di $K[X]$ tale che $(f) \subseteq I$. Essendo $K[X]$ un dominio a ideali principali, per ogni ideale I di $K[X]$ esiste, unico a meno di associati, $g \in K[X]$ tale che $I = (g)$; inoltre $(f) \subseteq (g)$ se e solo se $g \mid f$. Dunque gli ideali di $K[X]/(f)$ sono in corrispondenza biunivoca con i divisori monici di f.

(a) Tenendo conto che $f \neq 0$ e $f \notin K[X]^* = K^*$ (dato che $\deg(f) > 0$), per definizione f è irriducibile se e solo se gli unici divisori monici di f sono quelli banali (cioè 1 e f), se e solo se gli unici ideali di $K[X]/(f)$ sono quelli banali.

(b) $K[X]/(f)$ ha un solo ideale non banale se e solo se f ha un solo divisore monico non banale. Essendo $K[X]$ un dominio a fattorizzazione unica (perché a ideali principali), è chiaro che, se $f = g^2$ con $g \in K[X]$ monico irriducibile, allora f ha un solo divisore monico non banale (cioè g). Se invece $f = g^i$ con $i > 2$ o nella fattorizzazione di f compaiono due polinomi monici irriducibili distinti g e h, allora f ha almeno due divisori monici non banali (g e g^2 nel primo caso, g e h nel secondo). Infine, per il punto precedente, f non ha divisori monici non banali se è irriducibile.

(c) Essendo monico (quindi primitivo), f è irriducibile in $\mathbb{Q}[X]$ se e solo se lo è in $\mathbb{Z}[X]$. Supponendo per assurdo che f non sia irriducibile, esistono allora $g, h \in \mathbb{Z}[X]$ monici tali che $f = gh$ con $\deg(g) = 1$ e $\deg(h) = 3$ o $\deg(g) = \deg(h) = 2$. Poiché $\overline{f} = \overline{g}\overline{h}$ in $\mathbb{Z}/p\mathbb{Z}[X]$ e in $\mathbb{Z}/q\mathbb{Z}[X]$, l'ipotesi su p implica che non può essere $\deg(\overline{g}) = 1$, mentre l'ipotesi su q implica che non può essere $\deg(\overline{g}) = \deg(\overline{h}) = 2$ (l'unica radice semplice di $\overline{f}$ deve essere l'unica radice semplice di $\overline{g}$ o di $\overline{h}$, che quindi non può avere grado 2). Considerato che $\deg(g) = \deg(\overline{g})$ e $\deg(h) = \deg(\overline{h})$ si ottiene pertanto un assurdo.

(d) Sì, $\mathbb{Q}[X]/(f)$ è un campo quando $f = X^4 - X^2 + 2X + 3$. In effetti $\mathbb{Q}[X]/(f)$ è un campo se e solo se f è irriducibile in $\mathbb{Q}[X]$ (dato che $\mathbb{Q}[X]$ è un dominio a ideali principali), e si può verificare che f è irriducibile utilizzando il punto precedente con $p = 2$ e $q = 3$. Infatti

$$\overline{f} = X^4 + X^2 + \overline{1} = (X^2 + X + \overline{1})^2$$

(con $X^2 + X + \overline{1}$ irriducibile perché di secondo grado e senza radici) in $\mathbb{Z}/2\mathbb{Z}[X]$ e

$$\overline{f} = X^4 - X^2 - X = X(X^3 - X - \overline{1})$$

(con $X^3 - X - \overline{1}$ irriducibile perché di terzo grado e senza radici) in $\mathbb{Z}/3\mathbb{Z}[X]$.