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

Prova scritta del 17/01/2023

1. Sia G un gruppo e sia D il sottoinsieme di G costituito dagli elementi di ordine dispari.

   (a) Dato $a \in G$, dimostrare che $a \in D$ se e solo se esiste un intero dispari k tale che $a^k = 1$.

   (b) Dimostrare che, se G è abeliano, allora D è un sottogruppo di G.

   (c) Dimostrare che, se G è abeliano finito, allora l'ordine di ogni elemento di G/D è una potenza di 2.

   (d) Nel caso in cui $G = S_n$ (con n intero positivo), dimostrare che D è un sottogruppo di G se e solo se $n \leq 3$.

2. Per ogni intero n siano $f_n := X^4 + 2X^2 + nX + 1$ e $A_n := \mathbb{Q}[X]/(f_n)$.

   (a) Dimostrare che A_n è un campo se e solo se $\mathbb{Z}[X]/(f_n)$ è un dominio.

   (b) Dimostrare che, se n è dispari, allora A_n è un campo.

   (c) Dimostrare che A_0 ha un solo ideale massimale ma non è un campo.

   (d) Dimostrare che esiste un campo K tale che $A_4 \cong \mathbb{Q} \times K$.

Soluzioni

1. (a) Se $a \in D$, allora per definizione $\mathrm{ord}(a)$ è un intero dispari e $a^{\mathrm{ord}(a)} = 1$. Viceversa, se k è un intero dispari tale che $a^k = 1$, allora $\mathrm{ord}(a) \mid k$. Poiché ogni divisore di un numero dispari è dispari, ciò dimostra che $\mathrm{ord}(a)$ è dispari, cioè $a \in D$.

   (b) $1 \in D$ perché $\mathrm{ord}(1) = 1$. Dati $a, b \in D$, siano h e k interi dispari tali che $a^h = b^k = 1$. Si ha allora

   $$(ab^{-1})^{hk} = a^{hk}(b^{-1})^{hk} = (a^h)^k(b^k)^{-h} = 1^k 1^{-h} = 1$$

   (la prima uguaglianza usa l'ipotesi G abeliano), quindi $ab^{-1} \in D$ grazie al punto precedente e al fatto che hk è dispari.

   (c) Dato $a \in G$ sia $\bar{a} := aD \in G/D$. Poiché $\#G < \infty$, anche $\mathrm{ord}(\bar{a}) < \infty$. Dunque esistono (unici per il teorema fondamentale dell'aritmetica) $l, m \in \mathbb{N}$ con m dispari tali che $\mathrm{ord}(\bar{a}) = 2^l m$, e va dimostrato $m = 1$. Posto $b := a^{2^l}$, si ha $b^m = a^{2^l m}$, e dunque

   $$\overline{b^m} = \overline{a^{2^l m}} = \bar{a}^{2^l m} = \bar{1},$$

   per cui $b^m \in D$. Esiste allora k dispari tale che $b^{mk} = (b^m)^k = 1$, da cui segue (essendo mk dispari) $b \in D$ per il primo punto. Pertanto $\bar{a}^{2^l} = \bar{b} = \bar{1}$, da cui si deduce $\mathrm{ord}(\bar{a}) = 2^l m \mid 2^l$, e quindi $m = 1$.

   (d) Ricordando che l'ordine di un m-ciclo è m, D è un sottogruppo di G per $n \leq 3$ perché $D = \{(1)\}$ per $n = 1, 2$ e $D = A_3 = \{(1), (1,2,3), (1,3,2)\}$ per $n = 3$. Invece D non è un sottogruppo di G per $n > 3$ perché in quel caso $(1,2,3), (1,2,4) \in D$, ma $(1,2,3)(1,2,4) = (1,3)(2,4) \notin D$ (avendo ordine 2).

2. (a) A_n è un campo se e solo se l'ideale (f_n) è massimale in $\mathbb{Q}[X]$. Poiché $\mathbb{Q}[X]$ è un dominio a ideali principali (essendo $\mathbb{Q}$ un campo), questo è vero se e solo se f_n è irriducibile in $\mathbb{Q}[X]$. D'altra parte $\mathbb{Z}[X]/(f_n)$ è un dominio se e solo se l'ideale (f_n) è primo in $\mathbb{Z}[X]$. Poiché $\mathbb{Z}[X]$ è un dominio a fattorizzazione unica (essendolo $\mathbb{Z}$), questo è vero se e solo se f_n è irriducibile in $\mathbb{Z}[X]$. La conclusione segue allora dal fatto che f_n (che è primitivo in $\mathbb{Z}[X]$) è irriducibile in $\mathbb{Q}[X]$ se e solo se lo è in $\mathbb{Z}[X]$.

(b) Per n dispari f_n è irriducibile in $\mathbb{Z}[X]$ (quindi A_n è un campo per quanto visto nel punto precedente) perché $\overline{f_n} = X^4 + X + \bar{1}$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$. Infatti è immediato verificare che $\overline{f_n}$ non ha radici in $\mathbb{Z}/2\mathbb{Z}$ e non è divisibile per $X^2 + X + \bar{1}$, che è l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}/2\mathbb{Z}[X]$.

(c) Poiché $f_0 = (X^2 + 1)^2$ non è irriducibile in $\mathbb{Q}[X]$, sempre per quanto visto nel primo punto A_0 non è un campo. Inoltre gli ideali di A_0 sono tutti e soli della forma $I/(f_0)$ con I ideale di $\mathbb{Q}[X]$ tale che $(f_0) \subseteq I$. Essendo $\mathbb{Q}[X]$ un dominio a ideali principali, deve esistere $g \in \mathbb{Q}[X]$ tale che $I = (g)$, e la condizione $(f_0) \subseteq (g)$ equivale a $g \mid f$. Tenendo conto che $X^2 + 1$ è irriducibile in $\mathbb{Q}[X]$ (in quanto di secondo grado e senza radici razionali), a meno di associati gli unici divisori di f_0 sono $(X^2+1)^i$ per $i = 0, 1, 2$. Se ne deduce che gli unici ideali di A_0 sono $(1)/(f_0) = A_0$, $(X^2+1)/(f_0)$ e $(f_0)/(f_0) = \{\bar{0}\}$. Chiaramente da ciò segue che $(X^2 + 1)/(f_0)$ è l'unico ideale massimale di A_0.

(d) Per il criterio della radice razionale le eventuali radici razionali di f_n possono essere solo 1 o -1. In effetti $f_4(-1) = 0$ e risulta $f_4 = (X + 1)g$ con $g = X^3 - X^2 + 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (perché di terzo grado e senza radici razionali, dato che $g(1) \neq 0 \neq g(-1)$). Essendo $X + 1$ e g irriducibili e non associati, si ha $\mathrm{mcd}(X + 1, g) = 1$, e quindi gli ideali $(X + 1)$ e (g) sono coprimi nel dominio a ideali principali $\mathbb{Q}[X]$. Grazie al teorema cinese del resto per anelli commutativi si ottiene allora

$$A_4 = \mathbb{Q}[X]/(f_4) = \mathbb{Q}[X]/(X+1)(g) \cong \mathbb{Q}[X]/(X+1) \times \mathbb{Q}[X]/(g),$$

e per concludere basta osservare che $\mathbb{Q}[X]/(X + 1) \cong \mathbb{Q}$ e che $\mathbb{Q}[X]/(g)$ è un campo (dato che g è irriducibile).