Corso di Algebra - a.a. 2007-2008

Prova scritta del 27.2.2008

1. Sia G un gruppo finito e D il sottoinsieme di G costituito dagli elementi di ordine dispari.
   (a) Dimostrare che, se G è abeliano, D è un sottogruppo di G.
   (b) Dire se D è un sottogruppo nel caso in cui G è il gruppo simmetrico S_4.
2. Consideriamo $\mathbb{Z}$ come sottogruppo additivo di $\mathbb{Q}$. Mostrare che:
   (a) ogni elemento di $\mathbb{Q}/\mathbb{Z}$ ha ordine finito;
   (b) per ogni $x \in \mathbb{Q}/\mathbb{Z}$ e per ogni intero positivo n esiste $y \in \mathbb{Q}/\mathbb{Z}$ tale che $x = ny$;
   (c) per ogni intero positivo n esiste un unico sottogruppo di $\mathbb{Q}/\mathbb{Z}$ di ordine n, e questo sottogruppo è ciclico.
3. Sia A un anello commutativo con la proprietà che per ogni $a \in A$ esiste un intero $n > 1$ tale che $a^n = a$.
   (a) Dimostrare che, se A è un dominio d'integrità, allora A è un campo.
   (b) Dimostrare che ogni ideale primo di A è massimale.
4. Sia A un dominio, e sia $\varphi : A[X] \to A[X]$ un omomorfismo di anelli tale che $\varphi(a) = a$ per ogni $a \in A$. Mostrare che, se φ è un automorfismo, allora $\varphi(X)$ è della forma $aX + b$, dove $a \in A^\times$, $b \in A$.
5. Sia K un campo, p un numero primo e L il campo di spezzamento del polinomio $f = X^p - 1$ su K.
   (a) Dimostrare che esiste una radice α di f tale che $L = K(\alpha)$.
   (b) Determinare $[L : K]$ nel caso $K = \mathbb{Z}/2\mathbb{Z}$ e $p = 5$.

Soluzioni

1. (a) 1_G ha ordine 1, e quindi appartiene a D. Se $a, b \in D$, ci sono interi dispari h e k tali che $a^h = b^k = 1$. Dato che G è abeliano, $(ab^{-1})^{hk} = a^{hk}b^{-hk} = (a^h)^k(b^k)^{-h} = 1^k 1^{-h} = 1$. Dunque l'ordine di ab divide hk, e quindi è dispari.
   (b) No: (1 2 3) e (2 3 4) hanno ordine 3, ma (2 3 4)(1 2 3) = (1 3)(2 4) ha ordine 2.
2. Indichiamo con $\alpha : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ l'omomorfismo quoziente, e poniamo $G = \mathbb{Q}/\mathbb{Z}$.
   (a) Se $x \in G$, $x = \alpha(y)$ per qualche $y \in \mathbb{Q}$. Scriviamo $y = a/b$, dove a, b sono interi e $b \neq 0$. Allora $bx = b\alpha(a/b) = \alpha(b \cdot a/b) = \alpha(a) = 0$ in G.
   (b) Dato $x = \alpha(a/b)$, dove a, b sono interi e $b \neq 0$, poniamo $y = \alpha(a/nb)$. Allora $ny = \alpha(n \cdot a/nb) = \alpha(a/b) = x$.

(c) Sia $x = \alpha(q)$ un elemento di G, e supponiamo che $nx = 0$. Questo equivale a dire che $nq \in \mathbb{Z}$. Quindi $q \in \frac{1}{n}\mathbb{Z}$. Sia ora H un sottogruppo finito di G, e sia n il suo ordine. Poiché $nx = 0$ per ogni elemento x di H, segue da quanto detto che $H \subset \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Quest'ultimo gruppo ha ordine n, e quindi è uguale ad H. Inoltre è ciclico. Ne segue che tutti i sottogruppi finiti di G sono ciclici e della forma $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. In particolare, per ogni $n > 0$ esiste uno e un solo sottogruppo di G di ordine n, e cioè $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

3. (a) $a^n = a$ equivale ad $a(a^{n-1} - 1) = 0$. Se $a \neq 0$, dato che A è un dominio, ne segue che $a^{n-1} = 1$, cioè che a ha come inverso a^{n-2}.

   (b) Se P è un ideale primo in A, A/P è un dominio. Se $a \in A$ e $\overline{a}$ indica la sua classe in A/P, da $a^n = a$ segue che $\overline{a}^n = \overline{a}$. Per il punto precedente, A/P è un campo, e quindi P è massimale.

4. Poniamo $f = \varphi(X)$. Sia $P = \sum a_i X^i$ un elemento di $A[X]$. Dato che φ è un omomorfismo si ha

$$\varphi(P) = \sum \varphi(a_i) f^i = \sum a_i f^i \,.$$

   In particolare, se $f \in A$, anche $\varphi(P)$ appartiene ad A; in questo caso, dunque, φ non può essere suriettivo. D'ora in poi supponiamo che f non sia nullo e abbia grado $d > 0$. Sia p il grado di P. Il termine di grado più alto di f è della forma cX^d, dove $c \neq 0$. Ne segue che il termine di grado più alto di $\varphi(P)$ è $a_p c^p X^{pd}$, che non è nullo perchè A non ha divisori di zero. Quindi $\varphi(P)$ ha grado pd. Se φ è suriettivo, c'è un P tale che $\varphi(P) = X$. Ciò implica che $pd = 1$, il che accade solo quando $p = d = 1$. Dunque P è della forma $aX + b$, con $a, b \in A$. Ma allora

$$X = \varphi(P) = a_1 aX + a_1 b + a_0 \,, \tag{1}$$

   e quindi a è invertibile con inverso a_1.

   (NB: vale anche il viceversa. Se $f = aX + b$, con $a \in A^\times$, esiste Q tale che $\varphi(Q) = X$; infatti, in base alla (1), basta porre $Q = b_1 X + b_0$, dove b_1 è l'inverso di a e $b_0 = -b_1 b$. A questo punto, se $R = \sum c_i X^i$ è un qualsiasi elemento di $A[X]$, si ha che

$$R = \varphi(\sum c_i Q^i) \,.$$

   Dunque φ è suriettiva. Dato che f ha grado 1, $\varphi(P)$ non può essere nullo a meno che P non sia una costante. Ma allora, per ipotesi, $\varphi(P) = P$, e $\varphi(P)$ è nullo se e solo se $P = 0$.)

5. (a) Se 1 è l'unica radice di f, ovviamente $L = K = K(1)$. Altrimenti esiste $1 \neq \alpha \in L$ tale che $f(\alpha) = 0$, e osservo che anche $f(\alpha^i) = 0$ per ogni intero i. Essendo $\alpha^p = 1$ e $\alpha \neq 1$, l'ordine di α nel gruppo moltiplicativo L^* è p. Dunque i p elementi α^i per $0 \leq i < p$ sono distinti e sono tutte le radici di f. Allora, per definizione,

$$L = K(\alpha^0, \alpha^1, \ldots, \alpha^{p-1}) = K(\alpha).$$

   (b) $f = (X - 1)g$ con $g = X^4 + X^3 + X^2 + X + 1$. g è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$ perché non ha radici (infatti $g(0) = g(1) = 1$) e non è divisibile per l'unico polinomio irriducibile di secondo grado, cioè $X^2 + X + 1$ (in quanto $g = X^2(X^2 + X + 1) + X + 1$). g è quindi il polinomio minimo di una sua qualunque radice α, e per la parte (a) si ha

$$[L : K] = [K(\alpha) : K] = \deg(g) = 4.$$

Altra soluzione:

(a) Se K ha caratteristica p, $f = (X-1)^p$, quindi $K = L = K[1]$. Se K non ha caratteristica p, $f' = pX^{p-1}$ non ha zeri in comune con f, che quindi ha p radici distinte in L. Sia G l'insieme di queste radici. Dato che G è chiuso rispetto al prodotto, è un sottogruppo di $L^\times$. Poiché G ha ordine primo, è ciclico; se α è un suo generatore, $L = K[\alpha]$, perchè quest'ultimo campo contiene tutte le potenze di α, cioè tutte le radici di f.

(b) $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$. Il polinomio $P = X^4 + X^3 + X^2 + X + 1$ è irriducibile. Infatti non ha radici in K e dunque, se fosse riducibile, dovrebbe essere il quadrato dell'unico polinomio irriducibile di secondo grado in $K[X]$, cioè di $X^2 + X + 1$. Ma in questo caso $X^5 - 1$ avrebbe radici multiple, contro quanto osservato nel punto precedente. Quindi il polinomio minimo di α è P, e $[L : K] = 4$.