Corso di Algebra - a.a. 2006-2007

Prova scritta del 26.2.2007

1. Sia G un gruppo, p un numero primo e A il sottoinsieme di G costituito dagli elementi il cui ordine è una potenza di p.
   (a) Dimostrare che, se G è abeliano, allora A è un sottogruppo di G.
   (b) Dimostrare che, se A è un sottogruppo di G, allora A è normale in G e nessun elemento non banale di G/A ha ordine divisibile per p.
2. Mostrare che non esistono omomorfismi non banali dal gruppo simmetrico S_4 a $\mathbb{Z}/3\mathbb{Z}$.
3. Sia A un anello commutativo. Dati due ideali I e J di A, si pone
$$I : J = \{a \in A : aJ \subset I\}.$$
   (a) Dimostrare che $I : J$ è un ideale di A che contiene I.
   (b) Dimostrare che se I è un ideale primo e J non è contenuto in I, allora $I : J = I$.
4. Mostrare che il polinomio $P(X) = X^4 + 3X^3 + 7X^2 + 2$ è irriducibile in $\mathbb{Z}[X]$.
5. Sia $K \subset L$ un'estensione algebrica di campi e sia A un sottoanello di L contenente K. Dimostrare che A è un campo.

Soluzioni

1. (a) A non è vuoto perchè contiene 1. Siano x, y elementi di A. Dunque $x^{p^h} = y^{p^k} = 1$. Sia n un intero tale che $h \leq n$, $k \leq n$. Allora
$$(xy^{-1})^{p^n} = x^{p^n} \left(y^{p^n}\right)^{-1} = 1 \cdot 1 = 1$$
   Dunque A è un sottogruppo di G.
   (b) Se $x \in A$, $x^{p^h} = 1$ per qualche h. Se $y \in G$, $(yxy^{-1})^{p^h} = yx^{p^h}y^{-1} = yy^{-1} = 1$, e dunque $yxy^{-1} \in A$. Se l'ordine modulo A di un elemento g di G è della forma pk, allora $\gamma^p \in A$, dove $\gamma = g^k$. In altre parole $\gamma^{p^{h+1}} = (\gamma^p)^{p^h} = 1$ per qualche h, cioè $g^k = \gamma \in A$. Dato che l'ordine di g modulo A è pk, questo è impossibile.
2. Supponiamo che esista un omomorfismo non banale $\varphi\colon S_4 \to \mathbb{Z}/3\mathbb{Z}$. Allora φ è suriettivo perchè $\mathbb{Z}/3\mathbb{Z}$ non ha sottogruppi non banali, e quindi il suo nucleo K deve avere ordine 8, dato che l'ordine di S_4 è 24. D'altra parte tutti gli elementi di S_4 il cui ordine non sia divisibile per 3 devono appartenere a K. Tra questi vi sono, oltre all'identità, nove elementi di ordine due (sei trasposizioni e tre prodotti di trasposizioni disgiunte); in altre parole, ben più di otto elementi. Questo assurdo mostra che φ non può esistere.
3. (a) Se $aJ \subset I$ e $bJ \subset I$, allora $(a+b)J \subset aJ + bJ \subset I$, e inoltre $caJ \subset cI \subset I$ per ogni $c \in A$. Poi $IA \subset I$ perchè I è un ideale, e quindi $IJ \subset I$, cioè $I \subset I : J$.

(b) Esiste $b \in J$ tale che $b \notin I$. Se $a \in I : J$, allora $ab \in I$. Dato che I è primo ne segue che $a \in I$.

4. La riduzione di P modulo 3 è $p(X) = X^4 + X^2 - 1$. Basta mostrare che p è irriducibile in $K[X]$, dove $K = \mathbb{Z}/3\mathbb{Z}$. Né 0 nè ± 1 è radice di p. Dunque se p fosse riducibile, dovrebbe essere prodotto di due fattori irriducibili di grado 2. D'altra parte i polinomi monici di grado 1 in $K[X]$ sono X, $X+1$ e $X-1$, i cui prodotti a due a due sono X^2, X^2+X, X^2-X, X^2-X+1, X^2-1 e X^2+X+1. Quindi i polinomi monici irriducibili di grado 2 in $K[X]$ sono $f(X) = X^2+1$, $g(X) = X^2+X-1$ e $h(X) = X^2-X-1$. Il polinomio f non divide p dato che -1 non è radice di $q(T) = T^2+T-1$. Inoltre p è diverso sia da gh, che da g^2, che da h^2, dato che questi polinomi hanno tutti e tre termine noto uguale a 1.

Altra soluzione. Se vi fosse una radice di P, questa dovrebbe dividere 2. Si verifica direttamente che $1, -1, 2, -2$ non sono radici di P. Quindi, se P non è irriducibile, è prodotto di due polinomi irriducibili di grado 2. Si può supporre che i due fattori siano monici, e il prodotto dei loro termini noti deve valere 2. Supponiamo quindi che

$$P(X) = (X^2 + aX \pm 1)(X^2 + bX \mp 2) = X^4 + (a+b)X^3 + (ab \pm 1 \mp 2)X^2 \pm (b-2a)X + 2\,,$$

dove a e b sono interi. Paragonando i coefficienti dei due lati dell'uguaglianza si ricava che $b = 2a$, e poi che $3a = 3$, cioè che $a = 1$. Ne segue che

$$7 = 2 \pm 1 \mp 2\,,$$

il che è assurdo, dato che il lato destro vale 1 con una scelta di segni, e 3 con l'altra.

5. Basta mostrare che ogni elemento non nullo di A possiede un inverso moltiplicativo in A. Se $a \in A$, l'anello $K[a]$ è un campo, dato che a è algebrico su K. Quindi, se $a \neq 0$, a possiede un inverso moltiplicativo in $K[a]$, e quindi in A, dato che $K[a] \subset A$.