Corso di Algebra - a.a. 2006-2007

Prova scritta del 31.1.2007

1. Sia G un gruppo, α un automorfismo di G e $H = \{g \in G : \alpha(g) = g\}$.
   (a) Dimostrare che H è un sottogruppo di G.
   (b) Dimostrare che, se $H = \{1\}$ e $G \neq \{1\}$, allora α non è un automorfismo interno.
2. Dire per quali valori di n il gruppo alterno A_n contiene elementi di ordine 4.
3. Sia $f : A \to B$ un omomorfismo di anelli.
   (a) Dimostrare che se $a \in A^*$, allora $f(a) \in B^*$. Dedurre che $f|_{A^*}$ induce un omomorfismo di gruppi $f^* : A^* \to B^*$.
   (b) Fornire un esempio in cui f è suriettivo ma f^* non lo è.
4. Sia K un campo e sia n un intero ≥ 1. Indichiamo con I l'ideale in $K[X]$ generato da X^n, con A l'anello $K[X]/I$, e con λ la classe di X in A.
   (a) L'anello A è un dominio?
   (b) L'ideale $A\lambda$ è massimale?
   (c) descrivere tutti gli ideali di A.
5. Dimostrare che il polinomio $P(X) = X^3 + 3X - 2$ è irriducibile in $\mathbb{Q}[X]$. Detta α una sua radice, determinare il grado di $\alpha^2 + 1$ su $\mathbb{Q}$.

Soluzioni

1. (a) H non è vuoto perchè $\alpha(1) = 1$. Se $\alpha(g) = g$ e $\alpha(g') = g'$, allora
   $$\alpha(g^{-1}g') = \alpha(g)^{-1}\alpha(g') = g^{-1}g'$$
   Quindi H è un sottogruppo di G.
   (b) Se α è l'automorfismo interno $g \mapsto \gamma g \gamma^{-1}$, due sono i casi possibili. O $\gamma = 1$, e allora $H = G \neq \{1\}$, oppure $\gamma \neq 1$. In questo secondo caso $\gamma \in H$ perchè $\gamma\gamma\gamma^{-1} = \gamma$, e quindi $H \neq \{1\}$.
2. Sia σ un elemento di ordine 4 di A_n, e sia $\sigma = \sigma_1 \cdots \sigma_h$ la sua decomposizione in cicli disgiunti. L'ordine di ognuno dei σ_i deve dividere 4, e quindi può essere solo 2 o 4. In particolare tutti i σ_i sono permutazioni dispari, e dunque h è pari. D'altra parte almeno uno dei σ_i deve avere ordine 4. Ne segue che $n \geq 6$. Viceversa, se $n \geq 6$, A_n contiene sempre un elemento di ordine 4, ad esempio il prodotto di due cicli disgiunti, uno di ordine 4 e uno di ordine 2.
3. (a) Se $a \in A^*$ c'è a' tale che $aa' = a'a = 1$. Applicando f a queste uguaglianze si ottiene che $f(a)f(a') = f(a')f(a) = f(1) = 1$. Quindi $f(a)$ è invertibile.

(b) Esempio: $A = \mathbb{Z}$, $B = \mathbb{Z}/p\mathbb{Z}$, dove p è un primo > 3, e $f(n) =$ classe di n modulo p. L'omomorfismo f è suriettivo, ma f^* no perchè $\mathbb{Z} = \{1, -1\}$ ma $(\mathbb{Z}/p\mathbb{Z})^*$ ha $p - 1 > 2$ elementi.

4. Indichiamo con $\varphi : K[X] \to A$ l'omomorfismo passaggio al quoziente.

   (a) Se $n = 1$, $A \cong K$ è un campo. Se $n > 1$, $\lambda \neq 0$ ma $\lambda^n = 0$. Quindi λ è un divisore di zero e A non è un dominio.

   (b) $A\lambda = \varphi((X))$, quindi $A/A\lambda \cong K[X]/(X)$ per i teoremi di isomorfismo. D'altra parte $K[X]/(X)$ è isomorfo a K, che è un campo, quindi $A\lambda$ è massimale.

   (c) Gli ideali propri sono $A\lambda, A\lambda^2, \ldots, A\lambda^n = \{0\}$. In primo luogo A è un dominio a ideali principali perchè è quoziente di un dominio a ideali principali ($K[X]$). Un elemento non nullo $f \in A$ è un polinomio in λ a coefficienti in K, e quindi possiamo scrivere $f = \lambda^h q$, dove $q = a - b\lambda$, con $a \in K$, $a \neq 0$ e $b \in K[X]$. Per concludere basta mostrare che q è invertibile, e quindi che f è associato a λ^h. Dato che $q = a(1 - (b/a)\lambda)$, e a è invertibile, si può supporre che $a = 1$. Ora notiamo che

$$
\begin{aligned}
&(1 - b\lambda)(1 + b\lambda) = 1 - b^2\lambda^2 \\
&(1 - b^2\lambda^2)(1 + b^2\lambda^2) = 1 - b^4\lambda^4 \\
&\ldots \\
&(1 - b^{2^{k-1}}\lambda^{2^{k-1}})(1 + b^{2^{k-1}}\lambda^{2^{k-1}}) = 1 - b^{2^k}\lambda^{2^k}
\end{aligned}
$$

   Se k è abbastanza grande $2^k \geq n$, quindi $\lambda^{2^k} = 0$ e il lato destro dell'ultima uguaglianza vale 1. Ciò significa che

$$(1 + b\lambda)(1 + b^2\lambda^2) \ldots (1 + b^{2^{k-1}}\lambda^{2^{k-1}})$$

   è l'inverso di $1 - b\lambda$.

5. Il polinomio $P(X)$ non ha radici razionali. Infatti una tale radice dovrebbe essere intera e dovrebbe dividere il termine noto; potrebbe quindi essere uguale solo a ± 1, ± 2. Si verifica direttamente che nessuno di questi valori è una radice. Poiché $P(X)$ ha grado 3 e non ha radici, è irriducibile. Se $\alpha^2 + 1$ appartenesse a $\mathbb{Q}$, α sarebbe radice di un polinomio di secondo grado a coefficienti razionali. Questo è impossibile perchè il polinomio minimo di α è $P(X)$. Dunque il grado di $\alpha^2 + 1$ su $\mathbb{Q}$ è strettamente maggiore di 1. D'altra parte questo grado divide $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, ed è quindi pari a 3.