Corso di Algebra 1 – a.a. 2011-2012

Prova scritta del 20.6.2012

1. Sia G un gruppo e sia a un elemento di G. Dimostrare che, se m e n sono due interi primi tra loro e $a^m = 1$, allora esiste $b \in G$ tale che $a = b^n$.

2. Esistono omomorfismi suriettivi dal gruppo alterno A_4 al gruppo simmetrico S_3?

3. Per ogni numero primo p indichiamo con $\mathbb{F}_p$ il campo $\mathbb{Z}/(p)$. Consideriamo gli anelli

$$A = \mathbb{F}_5[X]/(X^3 + X^2 + 2)\ , \quad B = \mathbb{F}_7[X]/(X^3 + X^2 + 2)\,,$$

dove X è una indeterminata su $\mathbb{F}_5$ o su $\mathbb{F}_7$, rispettivamente.

L'anello A è un dominio? È un campo? Stesse domande per B.

4. Sia A l'insieme dei numeri razionali della forma $a/3^k$, dove a e k sono interi e $k \geq 0$.

   (a) Mostrare che A è un sottoanello di $\mathbb{Q}$.

   (b) Mostrare che A è un dominio a ideali principali.

   (c) Trovare gli ideali primi e massimali di A.

Soluzioni

1. Ci sono interi h e k tali che $hn + km = 1$. Allora

$$a = a^1 = a^{hn+km} = (a^h)^n (a^m)^k = (a^h)^n$$

Quindi basta porre $b = a^h$.

2. Se $\alpha : A_4 \to S_3$ è un omomorfismo, il suo nucleo è un sottogruppo normale di A_4. Il solo sottogruppo normale non banale di A_4, che indichiamo con K, ha ordine 4 e ha come elementi l'identità e i prodotti di due trasposizioni disgiunte. D'altra parte $\ker \alpha \neq \{1\}$ perché A_4 ha 12 elementi e S_3 ne ha solo 6. Inoltre $\alpha(A_4) \simeq A_4/\ker \alpha$. Quindi $\alpha(A_4)$ consta di un solo elemento, quando α è l'omomorfismo banale, oppure di 3 quando $\ker \alpha = K$. In ogni caso α non può essere suriettivo.

3. Il polinomio $X^3 + X^2 + 2$ non ha radici in $\mathbb{F}_5$. Dato che ha grado 3 ne segue che è irriducibile. Visto che $\mathbb{F}_5[X]$ è a ideali principali questo implica che l'ideale generato da $X^3 + X^2 + 2$ è primo e massimale. Quindi A è un campo e , a maggior ragione, un dominio.

   Il numero 2 è una radice di $X^3 + X^2 + 2$ modulo 7. Quindi $X^3 + X^2 + 2$ non è irriducibile in $\mathbb{F}_7[X]$ e l'ideale che esso genera non è primo. Ne segue che B non è un dominio e, a maggior ragione, non è un campo.

4. (a) $1 \in A$. Inoltre, se $a/3^k$, $b/3^h \in A$,

$$\frac{a}{3^k} - \frac{b}{3^h} = \frac{3^h a - 3^k b}{3^{h+k}} \in A\,, \quad \frac{a}{3^k}\frac{b}{3^h} = \frac{ab}{3^{h+k}} \in A\,.$$

(b) Sia I un ideale di A. L'intersezione $I \cap \mathbb{Z}$ è un ideale in $\mathbb{Z}$, quindi principale, generato da $a \in \mathbb{Z}$. Chiaramente $Aa \subset I$. Viceversa, se $b \in I$ c'è un intero positivo k tale che $3^k b \in \mathbb{Z}$, e quindi $3^k b \in I \cap \mathbb{Z}$. Ne segue che $3^k b = ca$ per qualche intero c e quindi $b = (c/3^k)a \in Aa$. Dunque $I = Aa$.

(c) Dato che A è a ideali principali gli ideali primi di A diversi dall'ideale nullo (che è primo) sono massimali. Quindi basta trovare gli ideali primi non nulli. Abbiamo visto che un tale ideale è generato da un intero $a \neq 0$. Inoltre $I \cap \mathbb{Z}$ è primo in $\mathbb{Z}$ e quindi a è un numero primo. D'altra parte $a \neq 3$ dato che 3 è invertibile in A. Viceversa, mostriamo che, se b è un numero primo diverso da 3, allora Ab è primo. Per questo basta vedere che b è irriducibile. Se $b = c/3^h \cdot d/3^k = cd/3^{h+k}$, dove c e d non sono divisibili per 3, allora $b = cd$ e quindi $c = \pm 1$ o $d = \pm 1$. Questo significa che $c/3^h$ o $d/3^k$ è invertibile e conclude la dimostrazione.