Corso di Algebra 1 - a.a. 2013-2014

Prova scritta del 23.1.2014

1. Trovare le soluzioni del sistema di congruenze

$$\begin{cases} x^2 \equiv 1 \mod 45 \\ x \equiv 34 \mod 75 \end{cases}$$

2. Sia G un gruppo, n un intero positivo e $H_n = \{g^n : g \in G\}$.
   (a) Dimostrare che, se G è abeliano, H_n è un sottogruppo di G.
   (b) Trovare un n tale che H_n non è un sottogruppo di G nel caso in cui $G = D_5$.

3. Sia p un numero primo e consideriamo gli anelli $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e $B = \mathbb{Z}/p\mathbb{Z}[X]/(X^2)$.
   (a) Dimostrare che A e B sono isomorfi come gruppi additivi.
   (b) A e B sono isomorfi anche come anelli?

4. Sia $1 \neq \alpha \in \mathbb{C}$ tale che $\alpha^3 = 1$.
   (a) Trovare il polinomio minimo di α su $\mathbb{Q}$.
   (b) Determinare $[\mathbb{Q}(\alpha^2) : \mathbb{Q}]$ e $[\mathbb{Q}(\alpha^2 + \alpha) : \mathbb{Q}]$.

Soluzioni

1. Per il teorema cinese del resto il sistema dato è equivalente al sistema

$$\begin{cases} x^2 \equiv 1 \mod 9 \\ x^2 \equiv 1 \mod 5 \\ x \equiv 34 \mod 3 \\ x \equiv 34 \mod 25 \end{cases}$$

Si verifica direttamente che la prima congruenza è soddisfatta se e solo se $x \equiv \pm 1 \mod 9$ e la seconda se e solo se $x \equiv \pm 1 \mod 5$. Segue che il sottosistema formato dalla prima e dalla terza congruenza è equivalente a $x \equiv 1 \mod 9$, mentre quello formato dalla seconda e dalla quarta è equivalente a $x \equiv 9 \mod 25$. In altre parole ci siamo ridotti a risolvere il sistema

$$\begin{cases} x \equiv 1 \mod 9 \\ x \equiv 9 \mod 25 \end{cases}$$

Per il teorema cinese del resto tale sistema ha un'unica soluzione modulo $9 \cdot 25 = 225$, che si trova facilmente essere $x \equiv 109 \mod 225$.

2. (a) Innanzitutto, se e è l'identità di G, $e^n = e \in H_n$. Se poi $h \in H_n$, e cioè esiste un $g \in G$ tale che $g^n = h$,

$$h^{-1} = (g^n)^{-1} = (g^{-1})^n \in H_n;$$

infine, se $h_1, h_2 \in H_n$, con $h_1 = g_1^n$ e $h_2 = g_2^n$, e se G è abeliano

$$h_1 h_2 = g_1^n g_2^n = (g_1 g_2)^n \in H_n.$$

(b) Gli elementi di D_5 sono 10 e si dividono in tre classi a seconda dell'ordine: l'identità, le simmetrie (che sono 5 e hanno ordine 2) e le rotazioni (che sono 4 e hanno ordine 5). È quindi immediato vedere che per ogni n pari H_n è esattamente l'insieme delle rotazioni, più naturalmente l'identità (le simmetrie elevate ad una potenza pari danno l'identità, mentre le rotazioni si permutano tra di loro). Si vede altrettanto facilmente che $H_3 = G$; quindi il primo valore "interessante" per n è 5. In tal caso, le rotazioni danno l'identità, mentre le simmetrie vengono mandate in se stesse, perciò H_5 coincide con il sottoinsieme delle simmetrie più l'identità; però questo non è un sottogruppo, il che può essere verificato direttamente o derivato ad esempio dal fatto che $\#H_5 = 6$ che non è un divisore di 10.

3. (a) Indicando con $\overline{f}$ la classe laterale $f + (X^2) \in B$ di $f \in \mathbb{Z}/p\mathbb{Z}[X]$, per ogni $b \in B$ esistono unici $c_0, c_1 \in \mathbb{Z}/p\mathbb{Z}$ tali che $b = \overline{c_0 + c_1 X}$ (se $b = \overline{f}$, $c_0 + c_1 X$ è il resto della divisione di f per X^2). Ciò significa che la funzione

$$\begin{aligned} \gamma \colon A &\to B \\ (c_0, c_1) &\mapsto \overline{c_0 + c_1 X} \end{aligned}$$

è biunivoca. Inoltre

$$\begin{aligned} \gamma((c_0, c_1)+(d_0, d_1)) = \gamma((c_0+d_0, c_1+d_1)) &= \overline{c_0 + d_0 + (c_1 + d_1)X} \\ = \overline{c_0 + c_1 X} + \overline{d_0 + d_1 X} &= \gamma((c_0, c_1)) + \gamma((d_0, d_1)), \end{aligned}$$

cioè γ è anche un omomorfismo (e pertanto un isomorfismo) di gruppi additivi.

(b) A e B non sono isomorfi come anelli. Infatti in B si ha $\overline{X} \neq 0$ e $\overline{X}^2 = \overline{X^2} = 0$, mentre in A vale $a^2 = 0$ se e solo se $a = 0$.

4. (a) Poiché $\alpha^3 - 1 = 0$, α soddisfa il polinomio $X^3 - 1$. Perciò il polinomio minimo di α, $p_\alpha(X)$, deve essere un divisore di $X^3 - 1 = (X - 1)(X^2 + X + 1)$. Naturalmente α non soddisfa $X - 1$ per ipotesi; inoltre $X^2 + X + 1$, avendo grado 2 senza avere radici razionali, è irriducibile. Perciò $p_\alpha(X) = X^2 + X + 1$.

(b) Abbiamo visto che $\alpha^2 + \alpha + 1 = 0$; ma allora

$$(\alpha^2)^2 + (\alpha^2) + 1 = \alpha^4 + \alpha^2 + 1 = \alpha + \alpha^2 + 1 = 0,$$

perché $\alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot 1 = \alpha$; cioè α^2 è in realtà l'altra radice di $p_\alpha(X)$. Ne deriva che $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = \deg(p_\alpha) = 2$.
Inoltre, $\alpha^2 + \alpha = -1$, perciò $\mathbb{Q}(\alpha^2 + \alpha) = \mathbb{Q}(-1) = \mathbb{Q}$ e di conseguenza $[\mathbb{Q}(\alpha^2 + \alpha) : \mathbb{Q}] = 1$.