Algebra 1 (Schoof) 4^o appello 14 settembre 2015, ore 16:00–18:00.

COGNOME ..... *NOME* .....

Risolvere gli esercizi negli spazi predisposti. Accompagnare le risposte con spiegazioni *chiare ed essenziali.* Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 5 punti.

1. Scrivere il polinomio $(X^2+1)(Y^2+1)(Z^2+1)$ come polinomio nei polinomi simmetrici elementari $s_1, s_2, s_3 \in \mathbf{Z}[X, Y, Z]$.
2. Dimostrare che l'ideale (X, Y) dell'anello $\mathbf{Q}[X, Y]$ non è principale.
3. Sia G un gruppo e sia H il sottogruppo generato dagli elementi g^2 con $g \in G$.
   (a) Dimostrare che H è un sottogruppo normale di G
   (b) Dimostare che per ogni $x \in G/H$ l'elemento x^2 è l'elemento neutro di G/H.
4. Sia Q_4 il gruppo dei quaternioni di cardinalità 8. Quanti omomorfismi $Q_4 \longrightarrow \mathbf{Z}_4$ ci sono?
5. Sia R l'anello $\mathbf{Z}[X]/(2X)$ e sia I l'ideale di R generato dall'elemento $1 + 1 = 2$.
   (a) Dimostrare che R/I è un dominio.
   (b) Determinare $\#R^*$.
6. Sia $p > 2$ un numero primo e sia q una potenza di p. Sia a un elemento invertibile dell'anello $\mathbf{Z}_q$. Dimostrare che il polinomio $X^2 - a$ ha al più due zeri in $\mathbf{Z}_q$.

Soluzioni.

1. Questo è l'esercizio 6 del foglio 15.
2. Questo è l'esercizio 2 del foglio 11.
3. Per ogni $x, y \in G$ l'elemento $yx^2y^{-1} = (yxy^{-1})^2$ è un quadrato. Questo implica che il coniugio di un prodotto di quadrati è anche un prodotto di quadrati. E quindi H è normale. La parte (b) segue dal fatto che per ogni $x \in G$, l'elemento x^2 sta in H. La sua classe è quindi banale in G/H.
4. Visto che $\mathbf{Z}_4$ è commutativo, un omomorfismo $f : Q_4 \longrightarrow \mathbf{Z}_4$ si fattorizza via il gruppo quoziente $P = Q_4/[Q_4, Q_4]$. Poiché P è isomorfo al gruppo di Klein V_4, l'immagine di f è contenuta nell'unico sottogruppo di ordine 2 di $\mathbf{Z}_4$. Il numero di omomorfismi cercato e quindi uguale al numero di omomorfismi $g : V_4 \longrightarrow \mathbf{Z}_2$. Si ha che g è banale oppure g è suriettivo con nucleo di ordine 2. Poiché V_4 ha tre sottogruppi di ordine 2, ci sono quattro omomorfismi.
5. L'anello R/I è isomorfo al dominio $\mathbf{Z}_2[X]$. Per (b): Sia $f \in R^*$. Allora esiste $g \in R$, con $f \cdot g = 1$ in R. Questa relazione vale anche modulo I, vale a dire nell'anello quoziente $\mathbf{Z}_2[X]$. Visto che $\mathbf{Z}_2[X]^* = \mathbf{Z}_2^* = \{1\}$, vediamo che i termini noti di f e di g sono dispari, mentre gli altri coefficienti sono pari. Dal fatto che $f \cdot g = 1$ in R, segue che il termine noto di f è ± 1, mentre gli altri coefficienti sono in $2\mathbf{Z}$. In altre parole, $f = \pm 1$ in R. La cardinalità di R^* è quindi 2.
6. Se $X^2 - a$ non ha nessuno zero in $\mathbf{Z}_q$, non c'è niente da dimostrare. Sia quindi $b \in \mathbf{Z}$ uno zero modulo q. Abbiamo quindi che $X^2 - a = X^2 - b^2 = (X + b)(X - b) \pmod q$. Ora, se $c \in \mathbf{Z}$ è uno zero di $X^2 - a$ in $\mathbf{Z}_q$, si ha che q divide $(c+b)(c-b)$. Se p divide sia $c+b$ che $c-b$, allora p divide la differenza $2b$. Contraddizione, perché $2b$ è invertibile in $\mathbf{Z}_q$. Quindi, q divide $c+b$ oppure $c - b$ e ci sono quindi al più due possibilità per c: si ha che $c \equiv \pm b \pmod q$.