Algebra 1 (Schoof) 2^o appello 11 febbraio 2020, ore 10:00–12:00.

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. Il teorema di Bézout dice che per ogni due interi non nulli n, m esistono $a, b \in \mathbf{Z}$ con $an + bm = \mathrm{mcd}(n, m)$. Dimostrare che $\mathrm{mcd}(a, b) = 1$.
2. Sia $H \subset \mathbf{Z}_{32}^*$ il sottogruppo generato da $\overline{7}$. Determinare l'ordine dell'elemento $\overline{3}H$ del gruppo quoziente $\mathbf{Z}_{32}^*/H$.
3. Sia G un gruppo e siano H, H' due sottogruppi normali di G con la proprietà che G/H e G/H' sono abeliani. Dimostrare che $G/(H \cap H')$ è abeliano.
4. Sia $I \subset \mathbf{Z}[X]$ l'ideale generato dai polinomi $X^2 - 1$ e $X^2 + 1$. Quanti sono gli elementi invertibili dell'anello quoziente $\mathbf{Z}[X]/I$?
5. Sia $A \subset \mathbf{R}$ l'anello $\{a + b\sqrt{3} : a, b \in \mathbf{Z}\}$. Quanti omomorfismi di anelli $A \longrightarrow \mathbf{Z}_9$ ci sono?
6. Sia $f \in \mathbf{R}[X]$ un polinomio non nullo e sia A l'anello quoziente $\mathbf{R}[X]/(f)$. Dimostrare che A è un dominio se e solo se è un campo.

Soluzioni.

1. Sia $d = \mathrm{mcd}(n, m)$. Abbiamo quindi che $a(n/d) + b(m/d) = 1$. Ora, se d' è un divisore comune di a e b, allora d' divide $a(n/d) + b(m/d) = 1$.
2. Si ha che $H = \{\overline{1}, \overline{7}, \overline{17}, \overline{23}\}$. L'ordine di $\overline{3}H$ divide quindi $[\mathbf{Z}_{32}^* : H] = 4$. Poiché ne $\overline{3}$, ne $\overline{9}$ appartengono ad H, l'ordine di $\overline{3}H$ in $\mathbf{Z}_{32}^*/H$ è 4.
3. Questo è l'esercizio 6 del foglio 7.
4. Questo è l'esercizio 6 del foglio 14.
5. L'anello A è isomorfo a $\mathbf{Z}[X]/(X^2-3)$. Un omorfismo $f : \mathbf{Z}[X]/(X^2-3) \longrightarrow \mathbf{Z}_9$ è determinato dall'elemento $f(X) \in \mathbf{Z}_9$. Abbiamo che $f(X)^2 = 3$ in $\mathbf{Z}_9$. Questo è impossibile e non ci sono quindi omomorfismi.
6. Osserviamo che A è uno spazio vettoriale su $\mathbf{R}$ di dimensione uguale al grado di f. Supponiamo che A sia un dominio. Sia $a \neq 0$ in A. Allora l'applicazione $g : A \longrightarrow A$ data dalla moltiplicazione per a è un'applicazione lineare iniettiva. Poiché A ha dimemsione finita, g è anche suriettiva e quindi esiste $b \in A$ tale che $g(b) = ab = 1$. Ne segue che a è invertibile.