Algebra 1 (Schoof) 4^o appello 13 settembre 2013, ore 10:00–12:00.

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

Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Ogni esercizio vale 5 punti.

1. Il numero $p = 601$ è primo. Quante radici primitive ci sono in $\mathbf{Z}_p^*$?

2. Siano σ, τ elementi del gruppo simmetrico S_n. Dimostrare che se la permutazione $\sigma\tau$ è un prodotto di t cicli disgiunti di lunghezze $k_1, k_2, \ldots, k_t$, allora la stessa cosa vale anche per $\tau\sigma$.

3. Sia G il gruppo $\mathbf{Z}_2 \times \mathbf{Z}_8$ e sia H il sottogruppo generato dall'elemento $v = (\overline{1}, \overline{2})$. Determinare l'ordine di v e decidere se il gruppo quoziente G/H è ciclico o meno.

4. Sia R l'anello $\mathbf{Z}[X]/(X^3 - 1)$. Quanti omomorfismi *di anelli* $f : R \longrightarrow \mathbf{Z}_{11}$ ci sono?

5. Sia R l'anello $\mathbf{Z}[X, Y, Z]/(X^2 - Y, Y^2 - Z, X + Y + Z, 2)$. Determinare il numero di elementi di R.

6. Sia k un campo e sia $g(X) \in k[X]$ un polinomio non nullo. Dimostrare che ogni elemento non nullo dell'anello $k[X]/(g(X))$ o è invertibile o è un divisore di zero.

Soluzioni.

1. Questo è il primo esercizio del secondo appello.
2. Questo è il quarto esercizio del 5^o foglio.
3. Questo è la parte (c) dell'esercizio 14 del 7^o foglio.
4. Un omomorfismo di anelli $f : \mathbf{Z}[X]/(X^3 - 1) \longrightarrow \mathbf{Z}_{11}$ è determinato da $f(X)$. Poiché $X^3 - 1$ è zero, è necessario che $f(X)^3 = 1$ in $\mathbf{Z}_{11}$. In altre parole, $f(X)$ deve essere un elemento di $\mathbf{Z}_{11}^*$ di ordine un divisore di 3. Visto che 3 non divide $\#\mathbf{Z}_{11}^*$ abbiamo che $f(X) = 1$. C'è quindi un unico omomorfismo, quello dato da $f(g) = g(1)$.
5. Si ha che
$$\begin{aligned}\mathbf{Z}[X, Y, Z]/(X^2 - Y, Y^2 - Z, X + Y + Z, 2) &\cong \mathbf{Z}[X, Z]/(X^4 - Z, X + X^2 + Z, 2),\\ &\cong \mathbf{Z}[X]/(X + X^2 + X^4, 2) \cong \mathbf{Z}_2[X]/(X^4 + X^2 + X)).\end{aligned}$$
Dal fatto che $X^4 + X^2 + X$ ha grado 4 segue che l'anello ha $2^4 = 16$ elementi.
6. Sia $a \in k[X]/(g(X))$ un elemento non nullo. Allora la moltiplicazione per a è un'applicazione k-lineare ϕ da $k[X]/(g(X))$ in se stesso. Se a non è invertibile, allora 1 non è contenuto nell'immagine di ϕ e ϕ non è quindi suriettiva. Dal fatto che la k-dimensione di $k[X]/(g(X))$ è finita, segue che ϕ non è neanche iniettiva. Sia b un elemento non nullo nel nucleo di ϕ. Allora si ha che $ab = 0$. Dunque a è un divisore di zero, come richiesto.