Algebra 2 (Schoof) 1^o esonero 20 novembre 2017, ore 14:00–16:00.

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. Sia G un gruppo e sia $H \subset G$ un sottogruppo con $[G:H] = n$. Dimostrare che H contiene un sottogruppo N, normale in G, con la proprietà che $[G:N]$ divide $n!$.
2. Sia ϕ l'unico omomorfismo suriettivo da $\mathbf{Z}_4$ ad $\mathrm{Aut}(\mathbf{Z}_3)$. Sia B il prodotto semidiretto $\mathbf{Z}_3 \rtimes \mathbf{Z}_4$ associato a ϕ. Determinare gli elementi di ordine 2 di B.
3. Dimostrare che un gruppo G di cardinalità 1500 non può essere semplice.
4. Dire se il polinomio $X^3 + 2$ è irriducibile o meno come elemento degli anelli $\mathbf{Q}[X]$ e $\mathbf{Z}_p[X]$ per $p = 3$, 5 e 7 rispettivamente.
5. Dimostrare che in un PID (dominio ad ideali principali) ogni ideale primo non nullo è massimale.
6. Sia p un numero primo. Consideriamo l'azione lineare naturale del gruppo
$$G = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{Z}_p \}$$
sullo spazio vettoriale $X = \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p$. Quante orbite ci sono?

Soluzioni.

1. Questo è l'esercizio 4 del foglio 1.
2. Questo è l'esercizio 4 del foglio 3.
3. Si ha che $1500 = 5^3 \cdot 12$. Sia P un 5-sottogruppo di Sylow. Se P è normale, allora G non è semplice. Se no, allora ci sono sei 5-sottogruppi di Sylow di G. L'azione, tramite coniugio, di G sull'insieme dei 5-sottogruppi di Sylow induce un omomorfismo $\phi : G \longrightarrow S_6$ che non è banale. Il nucleo di ϕ è quindi un sottogruppo normale non banale di G.
4. Sia $f = X^3 + 2$. In $\mathbf{Z}_3[X]$ si ha che $f = (X-1)^3$ e quindi f è riducibile. Il polinomio f ha lo zero $\overline{2} \in \mathbf{Z}_5$ ed è quindi riducibile in $\mathbf{Z}_5[X]$. Invece f non ha zeri in $\mathbf{Z}_7$ ed è irriducible in $\mathbf{Z}_7[X]$. Ne segue che f è anche irriducibile come elemento di $\mathbf{Z}[X]$ e quindi, per il lemma di Gauss, anche in $\mathbf{Q}[X]$.
5. Sia P un ideale primo di R. Allora $P = (\pi)$ per qualche elemento primo π del PID R. Supponiamo che esista un ideale I con $P \subset I \subset R$. Allora anche I è principale ed è generato da $\alpha \in R$, diciamo. Questo implica che esiste $\beta \in R$ con $\alpha\beta = \pi$. Il fatto che π è irriducibile implica che uno degli elementi α, β è invertibile. Nel primo caso abbiamo che $I = R$ e nel secondo caso $I = P$. Concludiamo che P è un ideale massimale.
6. Siano $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ i vettori della base canonica di X. I punti fissi dell'azione di G sono i p punti della retta $\mathbf{Z}_p\mathbf{e}_1$. Ce ne sono p. L'orbita di un vettore del tipo $\alpha\mathbf{e_2}$ con $\alpha \in \mathbf{Z}_p^*$, sono i vettori $\lambda\mathbf{e}_1 + \alpha\mathbf{e_2}$ con $\lambda \in \mathbf{Z}_p$. Si tratta di $p-1$ orbite di lunghezza p. Infine, l'orbita di un vettore del tipo $\alpha\mathbf{e_3}$ con $\alpha \in \mathbf{Z}_p^*$, sono i vettori $\lambda\mathbf{e}_1 + \mu\mathbf{e}_2 + \alpha\mathbf{e_3}$ con $\lambda, \mu \in \mathbf{Z}_p$. Si tratta di $p-1$ orbite di lunghezza p^2.

   Poiché $p + (p-1)p + p^2(p-1) = p^3 = \#X$, abbiamo determinato tutte le orbite. Ci sono quindi $p + (p-1) + (p-1) = 3p-2$ orbite.