Algebra 2 (Schoof) 2^o appello 26 febbraio 2010, ore 11:00–13:00.

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

Accompagnare le risposte con spiegazioni *chiare ed essenziali*. Ogni esercizio vale 6 punti.

1. Per ogni $n \in \mathbf{Z}_{\geq 1}$ determinare l'ordine del centro del gruppo diedrale D_n.

   Il gruppo D_n è generato dalla rotazione R di angolo $\frac{2\pi}{n}$ intorno l'origine di $\mathbf{R}^2$ e dalla riflessione T rispetto all'asse x di $\mathbf{R}^2$. Si ha che $TR = R^{-1}T$. Il gruppo D_n ha $2n$ elementi ed è quindi commutativo se $n \leq 2$. In questi due casi il centro ha $\#D_n = 2n$ elementi.

   Adesso supponiamo che $n > 2$. Sia A un elemento del centro di D_n. Allora si ha in particolare che $AT = TA$. Questo implica che A manda i due autospazi di T in se stessi, ossia A preserva i due assi. Poichè A è una isometria, questo implica che $A = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. In altre parole, vale $A = \pm\mathrm{id}$ oppure $A = \pm T$. Poichè $n > 2$, si ha che $RT \neq TR$ e quindi $A \neq \pm T$, ma necessariamente $A = \pm\mathrm{id}$. Le matrici $\pm\mathrm{id}$ commutano con tutti gli elementi di D_n. La matrice $-\mathrm{id}$ corrisponde alle rotazioni di 180 gradi intorno all'origine ed è contenuto in D_n se e solo se n è pari. In conclusione, il centro di D_n ha due elementi quando n è pari, mentre consiste solo nell'identità quando n è dispari.

2. Dimostrare che non esiste un gruppo semplice di cardinalità 100.

   Sia G un gruppo di ordine $100 = 2^2 \cdot 5^2$. Il numero di 5-Sylow sottogruppi divide 2^2 ed è congruo ad 1 (mod 5). Di consequenza G ammette un unico 5-sottogruppo di Sylow P. Poiché P è l'unico sottogruppo di G di ordine 25, è per forza uguale ai suoi coniugati. Ne segue che P è normale in G e che G non è semplice.

3. Sia p un primo e sia $f = X^p - X + 1 \in \mathbf{Z}_p[X]$.
   (a) Dimostrare che se α è uno zero di f, anche $\alpha + 1$ è uno zero di f.
   (b) Dimostrare che per ogni zero α di f vale che $\alpha^{p^p} = \alpha$.
   (c) Dimostrare che $f = X^p - X + 1$ é irriducibile in $\mathbf{Z}_p[X]$.

   Ricordiamo che per ogni $x, y \in \overline{\mathbf{F}}_p$ vale $(x+y)^p = x^p + y^p$.
   (a) Si ha che $(\alpha+1)^p - (\alpha+1) + 1 = \alpha^p + 1 - \alpha - 1 + 1 = 0$.
   (b) Si dimostra per induzione che $\alpha^{p^i} = \alpha - i$ per $i \geq 1$.
   (c) Sia $\alpha \in \overline{\mathbf{F}}_p$ uno zero di f. Per la parte (b) abbiamo che $\mathbf{F}_p(\alpha) \subset \mathbf{F}_{p^p}$. Per la moltiplicatività del grado, $[\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ divide p. Poiché $f(x) = x^p - x + 1 = 1$ per ogni $x \in \mathbf{Z}_p$, il polinomio f non ha zeri in $\mathbf{F}_p$ e quindi non è possibile che $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = 1$. Concludiamo che il campo $\mathbf{F}_p(\alpha)$ ha grado p su $\mathbf{F}_p$ e che f è quindi irriducibile.

4. Fattorizzare il polinomio $X^4 + 1$ in fattori irriducibili
   (a) in $\mathbf{R}[X]$;
   (b) in $\mathbf{Z}_2[X]$.

   (a) Si ha che $X^4 + 1 = (X^2 + \sqrt{2}\,X + 1)(X^2 - \sqrt{2}\,X + 1)$ in $\mathbf{R}[X]$. I due fattori sono irriducibili in $\mathbf{R}[X]$, perché non ammettono zeri reali. (b) Si ha che $X^4 + 1 = (X+1)^4$ in $\mathbf{Z}_2[X]$.

5. Sia p un numero primo e sia $A = \mathbf{Z}_{p^3} \times \mathbf{Z}_p$. Sia $f : A \longrightarrow A$ l'omomorfismo dato da
$$f(a) \;=\; p^2 a \;=\; \underbrace{a + a + \ldots + a}_{p^2 \text{ volte}}, \qquad \text{per } a \in A.$$
   (a) Dimostrare che $\mathrm{im}\, f \subset \ker f$.
   (b) Quanti elementi ha il gruppo quoziente $\ker f / \mathrm{im}\, f$?

   (a) Sia $a \in \mathrm{im}\, f$. Allora $a = f(b)$ per un certo $b \in A$. Si ha che $f(a) = f(f(b)) = p^4 b = 0$ e quindi a è contenuto nel nucleo di f.
   (b) Si ha che $\ker f = \{(x, y) \in \mathbf{Z}_{p^3} \times \mathbf{Z}_p : x \equiv 0 \pmod{p}\}$ e quindi l'ordine di $\ker f$ è p^3 D'altra parte, si ha che $\mathrm{im}\, f = \{(x, 0) \in \mathbf{Z}_{p^3} \times \mathbf{Z}_p : x \equiv 0 \pmod{p^2}\}$ e quindi $\mathrm{im}\, f$ ha p elementi. Concludiamo che il quoziente $\ker f / \mathrm{im}\, f$ ha p^2 elementi.