Algebra 1 (Schoof) 2^o appello 19 febbraio 2013, ore 14:00–16:00.

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

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

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

2. 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.

3. Sia R un anello e siano $I, J \subset R$ due ideali di R. Dimostrare che $I \cup J$ è un ideale se e soltanto se $I \subset J$ oppure $J \subset I$.

4. Sia R l'anello $\mathbf{Z}[X,Y]/(X^2-Y, Y-X+1, X+2)$. Determinare il numero di elementi invertibili di R.

5. Sia G un gruppo a sia G^2 il sottogruppo di G generato dagli element g^2 con $g \in G$. Dimostrare che G^2 è un sottogruppo normale di G.

6. Sia R l'anello $\mathbf{Z}[X]/(X^2)$. Quanti omomorfismi *di anelli* $f : R \longrightarrow \mathbf{Z}_9$ ci sono?

Soluzioni.

1. Sia g una radice primitiva modulo p. Allora le altre radici primitive hanno la forma g^i con $\mathrm{mcd}(i, p-1) = 1$. Ce ne sono quindi $\phi(p-1) = \phi(600) = \phi(2^3 3\, 5^2) = 4 \cdot 2 \cdot 20 = 160$.
2. Questo è l'esercizo 3 del foglio 14.
3. Questo è l'esercizo 2 del foglio 11.
4. Si ha che
$$R = \mathbf{Z}[X,Y]/(X^2 - Y, Y - X + 1, X + 2) \cong \mathbf{Z}[Y]/(4 - Y, Y + 3) \cong \mathbf{Z}_7.$$
Poiché 7 è primo, ci sono 6 elementi invertibili in R.
5. Per ogni $g \in G$ e per ogni automorfismo σ di G si ha che $\sigma(g^2) = \sigma(g)^2$. Questo implica che σ preserva G^2. Come consequenza G^2 è un sottogruppo caratteristico ed è quindi normale. Alternativamente: sia $x \in G^2$ e sia $g \in G$. Allora $gxg^{-1} = (gx)^2 x^{-1} g^{-2}$ è prodotto degli elementi $(gx)^2$, x^{-1} e g^{-2} di G^2 ed è quindi contenuto in G^2.
6. Ogni omomorfismo $\phi : \mathbf{Z}[X] \longrightarrow \mathbf{Z}_9$ è determinato da $\phi(X) \in \mathbf{Z}_9$ e, viceversa, per ogni $\overline{a} \in \mathbf{Z}_9$ esiste un omomorfismo $\phi : \mathbf{Z}[X] \longrightarrow \mathbf{Z}_9$ con $\phi(X) = \overline{a}$, vale a dire la mappa che manda un polinomio $g(X) \in \mathbf{Z}[X]$ in $g(\overline{a})$. L'applicazione $\phi \mapsto \phi(X)$ è quindi una corrispondenza biiettiva fra l'insieme degli omomorfismi di anelli $\mathbf{Z}[X] \longrightarrow \mathbf{Z}_9$ e $\mathbf{Z}_9$ stesso.
L'ideale (X^2) è contenuto in $\ker(\phi)$ se e solo se $\phi(X)^2 = \phi(X^2) = \overline{0}$ in $\mathbf{Z}_9$. Per il teorema di isomorfismo l'insieme degli omomorfismi $\mathbf{Z}[X]/(X^2) \longrightarrow \mathbf{Z}_9$ corrisponde quindi via la corrispondenza indicata qua sopra agli elementi $\overline{a} \in \mathbf{Z}_9$ con $\overline{a}^2 = \overline{0}$. In altre parole, $\overline{a}$ appartiene all'insieme $\{\overline{0}, \overline{3}, \overline{6}\}$. Ci sono quindi tre omomorfismi.