Algebra 2 (Schoof) 6^o appello 14 settembre 2021, ore 15:00–17:00.

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. Dimostrare che ogni gruppo di cardinalità 33 è ciclico.
2. Sia R un anello commutativo e siano $I, J \subset R$ due ideali coprimi, vale a dire $I+J=R$. Dimostrare che per ogni $m \geq 1$ anche gli ideali I^m e J^m sono coprimi.
3. Sia $H \subset \mathbf{Z}_{31}^*$ il sottogruppo generato da $\overline{2}$ e $\overline{5}$. Sia $x \in \mathbf{Z}_{31}^*/H$ la classe laterale di H che contiene $\overline{7}$. Determinare l'ordine dell'elemento x di $\mathbf{Z}_{31}^*/H$.
4. Sia p un numero primo. Dimostrare che il polinomio $X^p - Y$ è un elemento irriducibile dell'anello $\mathbf{Z}_p[X, Y]$.
5. Sia $f \in \mathbf{F}_2[X]$ un polinomio di grado 10. Dimostrare che f non è un elemento irriducibile dell'anello $\mathbf{F}_4[X]$.
6. Sia F un campo e sia $a \in F^*$. Sia R l'anello $F[X, Y]/(XY, X+Y+a)$. Dimostrare che R non contiene elementi nilpotenti non nulli (un elemento x si dice nilpotente se $x^m = 0$ per qualche $m \geq 1$).

Soluzioni.

1. Questo è l'esercizio 5 del foglio 3.
2. Questo è l'esercizio 7 del foglio 14.
3. Dal fatto che $2^2 \cdot 5^2 = 100 \equiv 7 \pmod{31}$ segue che $\overline{7}$ sta in H. L'ordine di x è quindi 1.
4. Visto come polinomio in Y con coefficienti nel dominio $\mathbf{Z}_p[X]$, il polinomio $X^p - Y = Y - X^p$ è monico e ha grado 1. Ne segue che è irriducibile.
5. L'affermazione è chiara se f è già riducibile in $\mathbf{F}_2[X]$. Supponiamo quindi che f sia irriducibile in $\mathbf{F}_2[X]$. Allora $\mathbf{F}_2[X]/(f)$ è un campo k di cardinalità 2^{10}. Sia a l'immagine di X in k. Allora il polinomio minimo di a su $\mathbf{F}_2$ è uguale ad f. Il campo k contiene $\mathbf{F}_4$ e il polinomio minimo $g \in \mathbf{F}_4[X]$ di a divide f. Il grado di g è $[k : \mathbf{F}_4] = 5$. Concludiamo che f non è irriducibile nell'anello $\mathbf{F}_4[X]$.
6. Valutare Y in $-X-a$ ci dà un isomorfismo $R \cong F[X]/(X(X+a))$. Poiché a è invertibile, i polinomi X e $X+a$ sono coprimi. Il teorema cinese del resto implica quindi che R è isomorfo a $F[X]/(X) \times F[X]/(X+a) \cong F \times F$. Se un elemento $(a, b) \in F \times F$ soddisfa $(a, b)^m = 0$ per qualche $m \geq 1$, allora $a^m = b^m = 0$ e quindi $a = b = 0$.