Algebra 2 (Schoof) 2^o esonero 31 gennaio 2012, ore 15:00–17:00.

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

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

1. Scrivere i gruppi $\mathbf{Z}_{120}^*$ e $\mathbf{Z}_{10!}^*$ come prodotto di gruppi ciclici.

2. Sia R un anello commutativo. Dimostrare che $\mathfrak{p}$ è un punto chiuso di $\mathrm{Spec}(R)$ se e solo se $\mathfrak{p}$ è un ideale massimale.

3. Sia R un anello commutativo. Un elemento $e \in R$ si dice *idempotente* se $e^2 = e$.
   (a) Supponiamo che R sia un campo. Determinare gli elementi idempotenti di R.
   (b) Sia p un numero primo e sia $n \geq 1$. Determinare gli elementi idempotenti di $\mathbf{Z}_{p^n}$.

4. Fattorizzare il polinomio $X^4 + X^3 + X^2 + X + 1$ in fattori irriducibili negli anelli $\mathbf{C}[X]$, $\mathbf{R}[X]$, $\mathbf{Q}[X]$, $\mathbf{Z}_5[X]$ e $\mathbf{Z}_2[X]$.

5. Sia A l'insieme dei generatori del gruppo moltiplicativo $\mathbf{F}_{81}^*$. Sia B l'insieme degli elementi $x \in \mathbf{F}_{81}^*$ per cui $\mathbf{F}_{81} = \mathbf{F}_3(x)$.
   (a) Determinare $\#A$ e $\#B$;
   (b) Dimostrare che $A \subset B$;
   (c) Esibire il polinomio minimo su $\mathbf{F}_3$ di un elemento $x \in B - A$.

Soluzioni.

1. Questo è il primo esercizio del foglio 12.

2. Questo è l'esercizio 7 del foglio 11.

3. Se R è un campo ed $e \in R$ soddisfa $e^2 = e$, allora si ha che $e(1-e) = 0$. Poiché un campo è privo di divisori di zero, abbiamo che $e = 0$ oppure $e = 1$. Supponiamo adesso che $R = \mathbf{Z}_{p^n}$ e che $e(1-e) = 0$ per un elemento $e \in R$. Se e è invertibile, allora si ha che $1 - e = 0$. Se e non è invertibile, allora e è divisibile per p. In questo caso $1 - e$ *non* è divisibile per p ed è invertibile. Si ha quindi che $e = 0$. Gli elementi idempotenti sono quindi $\{0, 1\}$.

4. In $\mathbf{C}[X]$ il polinomio $f = X^4 + X^3 + X^2 + X + 1$ si fattorizza in fattori lineari. Gli zeri sono $e^{\frac{2\pi i k}{5}}$ per $1 \leq k \leq 4$. Moltiplicando i fattori con zeri complessi coniugati, in $\mathbf{R}[X]$ troviamo la fattorizzazione $(X^2 - 2\cos(\frac{2\pi}{5})X + 1)(X^2 - 2\cos(\frac{4\pi}{5}) + 1)$. I fattori sono irriducibili, perché i loro zeri non sono reali. I tre polinomi irriducibili di grado ≤ 2 in $\mathbf{Z}_2[X]$ non dividono f. Il polinomio f è quindi irriducibile in $\mathbf{Z}_2[X]$ e anche in $\mathbf{Z}[X]$. Per il Lemma di Gauss f è quindi irriducibile in $\mathbf{Q}[X]$. In $\mathbf{Z}_5[X]$ abbiamo che $f = (X-1)^4$.

5. La cardinalità di A è $\varphi(81-1) = 32$. La cardinalità di B è $3^4 - 3^2 = 72$. Questo segue dal fatto che x soddisfa $\mathbf{F}_{81} = \mathbf{F}_3(x)$ se e solo se x *non* è contenuto in qualche sottocampo proprio di $\mathbf{F}_{81}$. Per ogni x, le potenze x^i appartengono al campo $\mathbf{F}_3(x)$. Quindi, se x genera il gruppo $\mathbf{F}_{81}^*$, allora $\mathbf{F}_3(x)$ contiene per forza ogni elemento di $\mathbf{F}_{81}$. Questo dimostra che $A \subset B$.

   Per la parte (c) va esibito un polinomio irriducibile f di grado 4 con la proprietà che gli zeri a di f non hanno ordine 80 nel gruppo moltiplicativo $\mathbf{F}_{81}^*$. Ci sono diversi modi. Per esempio, poiché 5 divide $\#\mathbf{F}_{81}^*$, esiste $a \in \mathbf{F}_{81}^*$ di ordine 5. Il fatto che 5 *non* divide $\#\mathbf{F}_9^*$, dimostra che $\mathbf{F}(a) = \mathbf{F}_{81}$. L'elemento a è zero del polinomio $f = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$, il quale è quindi irriducibile.

   Alternativamente, se a è uno zero di f, gli altri zeri sono a, a^3, a^9 e a^{27}. Il termine noto di f è quindi uguale a $a^{1+3+9+27} = a^{40}$. Basta quindi trovare un polinomio monico irriducibile f di grado 4 e con termine noto $+1$. Per esempio $f = X^4 + X^2 + X + 1$. Per dimostrare che questo polinomio f è irriducibile, basta dimostrare che non ha zeri in $\mathbf{F}_9$. Poiché ogni $b \in \mathbf{F}_9$ è zero di $X^9 - X = X(X^4 - 1)(X^4 + 1)$, questo segue dal fatto che $\mathrm{mcd}(f, X^4 \pm 1) = 1$ in $\mathbf{F}_3[X]$. Ci sono otto polinomi $f \in \mathbf{F}_3[X]$ con questa proprietà.