Corso di Algebra 1 - a.a. 2013-2014

Prova scritta del 13.2.2014

1. Sia G il gruppo moltiplicativo $\mathbb{Z}/21\mathbb{Z}^*$.
   (a) Dimostrare che G è isomorfo a $\mathbb{Z}/6Z \times \mathbb{Z}/2\mathbb{Z}$.
   (b) Per quali interi positivi n esiste un omomorfismo iniettivo di gruppi da $\mathbb{Z}/n\mathbb{Z}$ a G?
   (c) Dimostrare che per ogni intero positivo n non esiste un omomorfismo suriettivo di gruppi da $\mathbb{Z}/n\mathbb{Z}$ a G.

2. Sia G un gruppo finito e sia $l(G)$ il minimo degli interi positivi k tali che $g^k = 1$ per ogni elemento g di G.
   (a) Dimostrare che $l(G)$ divide $\#G$.
   (b) Determinare $l(A_4)$ e $l(S_4)$.
   (c) Fornire un esempio in cui G non è ciclico e $l(G) = \#G$.

3. Siano A un anello commutativo e I e J due ideali di A.
   (a) Dimostrare che $(I + J)(I \cap J) \subseteq IJ$.
   (b) Dimostrare che $(I + J)(I \cap J) = IJ$ se $A = \mathbb{Z}$.
   (c) Stabilire se vale $(I + J)(I \cap J) = IJ$ nel caso in cui $A = \mathbb{Z}[X]$, $I = (2)$ e $J = (X)$.

4. Trovare il più piccolo numero primo p tale che il polinomio $f(X) = X^3 - X + 1$ sia riducibile in $\mathbb{F}_p[X]$. Determinare inoltre il grado del campo di spezzamento di f su $\mathbb{F}_p$.

Soluzioni

1. (a) Essendo $21 = 7 \cdot 3$ con $\mathrm{mcd}(7,3) = 1$, per il teorema cinese del resto c'è un isomorfismo di anelli $\mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, dunque anche un isomorfismo di gruppi $\mathbb{Z}/21\mathbb{Z}^* \cong (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})^* = \mathbb{Z}/7\mathbb{Z}^* \times \mathbb{Z}/3\mathbb{Z}^*$. Inoltre, se p è un numero primo, $\mathbb{Z}/p\mathbb{Z}^*$ ha ordine $p-1$, dunque per concludere basta dimostrare che $\mathbb{Z}/p\mathbb{Z}^*$ è ciclico per $p = 7$ e $p = 3$. In effetti si verifica facilmente che $\mathbb{Z}/7\mathbb{Z}^*$ è generato per esempio da $\overline{3}$ e $\mathbb{Z}/3\mathbb{Z}^*$ da $\overline{2}$.

   (b) Gli omomorfismi iniettivi da $\mathbb{Z}/n\mathbb{Z}$ a G sono in corrispondenza biunivoca con gli elementi di G di ordine n. Per il punto precedente, gli n cercati sono dunque quelli per cui esiste in $\mathbb{Z}/6Z \times \mathbb{Z}/2\mathbb{Z}$ un elemento di ordine n. Ora, dato $(a,b) \in \mathbb{Z}/6Z \times \mathbb{Z}/2\mathbb{Z}$ si ha $\mathrm{ord}((a,b)) = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. Poiché i possibili valori di $\mathrm{ord}(a)$ sono i divisori di 6 (cioè $1,2,3,6$) e i possibili valori di $\mathrm{ord}(b)$ sono i divisori di 2 (cioè $1,2$), concludiamo che gli n richiesti sono $1,2,3,6$.

   (c) Se per assurdo esistesse un omomorfismo suriettivo $f\colon \mathbb{Z}/n\mathbb{Z} \to G$, il gruppo G sarebbe ciclico, generato da $f(\overline{1})$. Allora G (e quindi $\mathbb{Z}/6Z \times \mathbb{Z}/2\mathbb{Z}$) conterrebbe un elemento di ordine $\#G = 12$, cosa falsa per quanto dimostrato nel punto precedente.

2. (a) Dati $g \in G$ e un intero k, si ha $g^k = 1$ se e solo se k è un multiplo di $\mathrm{ord}(g)$. Dunque vale $g^k = 1$ per ogni $g \in G$ se e solo se k è un multiplo comune degli ordini di tutti gli elementi di G. Ne segue che $l(G)$ è il minimo comune multiplo degli ordini di tutti gli elementi di G e che se $g^k = 1$ per ogni $g \in G$ allora $l(G)$ divide k. Per concludere basta notare che, per il teorema di Lagrange, $g^{\#G} = 1$ per ogni $g \in G$.

   (b) A parte l'elemento neutro (che ha ordine 1), A_4 contiene solo i 3-cicli (che hanno ordine 3) e le coppie di trasposizioni disgiunte (che hanno ordine 2); gli altri elementi di S_4 sono le trasposizioni (che hanno ordine 2) e i 4-cicli (che hanno ordine 4). Per quanto detto nel punto precedente, si deduce che $l(A_4) = \mathrm{mcm}(3,2) = 6$ e $l(S_4) = \mathrm{mcm}(3,2,4) = 12$.

   (c) Un esempio è dato da S_3 (che non è ciclico, non essendo nemmeno abeliano). Infatti gli ordini degli elementi di S_3 sono 1 (per l'elemento neutro), 2 (per le trasposizioni) e 3 (per i 3-cicli). Come prima si trova allora $l(S_3) = \mathrm{mcm}(2,3) = 6 = \#S_3$.

3. (a) Per definizione di somma e prodotto di ideali, un elemento $a \in (I+J)(I \cap J)$ si può scrivere nella forma $a = \sum_{i=1}^{n}(b_i + c_i)d_i$ con $n \in \mathbb{N}$, $b_i \in I$, $c_i \in J$ e $d_i \in I \cap J$. Per ogni $i = 1, \ldots, n$ si ha $b_i d_i \in IJ$ (perché $b_i \in I$ e $d_i \in J$) e $c_i d_i = d_i c_i \in IJ$ (perché $d_i \in I$ e $c_i \in J$), dunque anche $(b_i + c_i)d_i = b_i d_i + c_i d_i \in IJ$, e quindi $a \in IJ$.

   (b) Esistono $m, n \in \mathbb{N}$ tali che $I = m\mathbb{Z}$ e $J = n\mathbb{Z}$, e vale $I + J = \mathrm{mcd}(m,n)\mathbb{Z}$, $I \cap J = \mathrm{mcm}(m,n)\mathbb{Z}$ e $IJ = mn\mathbb{Z}$. L'uguaglianza richiesta segue allora dal fatto che $\mathrm{mcd}(m,n)\mathrm{mcm}(m,n) = mn$.

   (c) Dato $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, si ha $f \in I$ se e solo se ogni a_i è pari, mentre $f \in J$ se e solo se $a_0 = 0$. Ne segue che $f \in I \cap J$ se e solo se ogni a_i è pari e $a_0 = 0$; da ciò si deduce facilmente che $I \cap J = (2X) = IJ$. D'altra parte $f \in I + J = (2, X)$ se e solo se a_0 è pari, quindi se $f \in (I+J)(I \cap J)$ allora $a_0 = 0$ e a_1 è multiplo di 4. Concludiamo che $(I + J)(I \cap J) \neq IJ$, perché per esempio $2X \in IJ$ ma $2X \notin (I + J)(I \cap J)$.

4. Avendo grado 3, f è riducibile se e solo se ha una radice. Ora, f non ha radici in $\mathbb{F}_2$ (perché $f(0) = f(1) = 1$) e nemmeno in $\mathbb{F}_3$ (perché $f(0) = f(1) = f(2) = 1$). Invece $f(3) = 0$ in $\mathbb{F}_5$, quindi il primo p cercato è 5. Inoltre in $\mathbb{F}_5[X]$ si ha $f = (X + 2)g$ con $g = X^2 - 2x - 2$ irriducibile (perché $g(0) = g(2) = 3$, $g(1) = 2$, $g(3) = g(4) = 1$). Dunque un'estensione $\mathbb{F}_5 \subset K$ è campo di spezzamento per f se e solo se lo è per g, e si ha $K = \mathbb{F}_5(\alpha)$ con α radice di g in K (l'altra radice di g essendo $2 - \alpha = -2\alpha^{-1}$). Poiché g è proprio il polinomio minimo di α su $\mathbb{F}_5$ (dato che è irriducibile e monico e $g(\alpha) = 0$), concludiamo che $[K : \mathbb{F}_5] = \deg(g) = 2$.