Corso di Algebra - a.a. 2005-2006

Prova scritta del 26.9.2006 – soluzioni

1. Un elemento g di G genera un sottogruppo il cui ordine è pari all'ordine di g. Per il teorema di Lagrange l'ordine di un sottogruppo di G deve dividere l'ordine di G, e quindi deve essere una potenza di p. Se $n > 0$, G contiene elementi diversi dall'elemento neutro. Sia g uno di questi elementi. L'ordine di g è p^h, dove $h > 0$ perchè $g \neq 1$. Dunque, se poniamo $\gamma = g^{p^{h-1}}$, da un lato $\gamma^p = g^{p^h} = 1$, dall'altra $\gamma \neq 1$. Quindi l'ordine di γ è p.

2. Ogni elemento di $\mathbb{Z}\times\mathbb{Z}$ è della forma (h,k), dove h e k sono interi. Mostriamo che il sottogruppo G di $\mathbb{Z}\times\mathbb{Z}$ generato da (h,k) è diverso da $\mathbb{Z}\times\mathbb{Z}$. Se $k = 0$ ogni elemento di G ha seconda componente nulla, e quindi $G \neq \mathbb{Z}\times\mathbb{Z}$; analoga conclusione si raggiunge se $h = 0$. Possiamo quindi supporre che h e k non siano nulli. Ogni elemento di G è della forma $(a,b) = (mh, mk)$, dove m è un intero, e quindi $ka = hb$. Ne segue che qualsiasi coppia (c,d) con $kc \neq hd$ non può appartenere a G. Un esempio di coppia con questa proprietà è $(h+1, k)$. Infatti $k(h+1) = kh + k \neq hk$, dato che $k \neq 0$.

3. (a) Se $a \in r(I)$, allora $a^n \in I$ per qualche n. Se $b \in A$, $(ba)^n = b^n a^n \in I$, dato che $a^n \in I$ e I è un ideale, cioè $ba \in r(I)$. Supponiamo che anche b appartenga a $r(I)$, e quindi $b^m \in I$ per qualche m. Vogliamo mostrare che $a + b \in r(I)$. Se h è un intero positivo, sappiamo che

$$(a+b)^h = \sum_{i=0}^{h} \binom{h}{i} a^i b^{h-i}$$

Scegliamo $h \geq n + m$. Allora, per ogni i compreso tra 0 e h, o $i \geq n$, o $h - i \geq m$. Nel primo caso $a^i \in I$, nel secondo $b^{h-i} \in I$. In ogni caso si conclude che ogni addendo appartiene a I, e quindi che $(a+b)^h \in I$. In definitiva $a + b \in r(I)$. È chiaro che $I \subset r(I)$. In particolare, se $I = A$, allora $r(I) = A$. Viceversa, se questo accade, $1 \in r(I)$. Visto che $1^n = 1$ per ogni n, ne segue che $1 \in I$, e quindi che $I = A$.

(b) Se $A = \mathbb{Z}$ e $I = 4\mathbb{Z}$, allora $2 \in r(I)$, dato che $2^2 = 4$. Ne segue che $r(I) = 2\mathbb{Z}$, che è diverso da I.

4. (a) Se I è proprio, deve essere $1_B \notin I$, dunque (essendo $\alpha(1_A) = 1_B$ per definizione di omomorfismo) $1_A \notin \alpha^{-1}(I)$, per cui $\alpha^{-1}(I)$ è proprio.
Se I è primo e $a, a' \in A$ sono tali che $aa' \in \alpha^{-1}(I)$, allora $\alpha(a)\alpha(a') = \alpha(aa') \in I$, da cui segue che $\alpha(a) \in I$ (cioè $a \in \alpha^{-1}(I)$) o $\alpha(a') \in I$ (cioè $a' \in \alpha^{-1}(I)$); tenendo conto che $\alpha^{-1}(I)$ è proprio per quanto visto sopra, questo dimostra che $\alpha^{-1}(I)$ è primo.

(b) Si ricordi che, se K è un campo, gli ideali primi di $K[X]$, a parte (0), sono massimali e sono tutti e soli quelli della forma (P) con P polinomio monico irriducibile di $K[X]$. Inoltre, essendo $\mathbb{C}$ algebricamente chiuso, i polinomi irriducibili di $B = \mathbb{C}[X]$ sono quelli di primo grado, mentre i polinomi irriducibili di $A = \mathbb{R}[X]$ sono quelli di primo grado e quelli di secondo grado con discriminante negativo (cioè aventi radici complesse coniugate non reali).
Sia ora J un ideale primo di B. Se $J = (0)$, chiaramente $\alpha^{-1}(J) = (0)$. È facile vedere che se $J = (X - a)$ con $a \in \mathbb{R}$, allora $\alpha^{-1}(J) = (X - a) \subset A$, mentre se $J = (X - a)$ con $a \in \mathbb{C} \setminus \mathbb{R}$, allora $\alpha^{-1}(J) = ((X - a)(X - \bar{a})) \subset A$ (si osservi che $(X - a)(X - \bar{a}) = X^2 - (a + \bar{a})X + a\bar{a}$ e $a + \bar{a}, a\bar{a} \in \mathbb{R}$): infatti, in entrambi i casi è chiaro che $\alpha^{-1}(J)$ (che è un ideale proprio) contiene l'ideale indicato, il quale è massimale per quanto detto prima, per cui deve valere l'uguaglianza.
Dunque la risposta richiesta è la seguente: se $I = (0)$ c'è un solo J, cioè (0); se $I = (X - a)$ (con $a \in \mathbb{R}$) c'è un solo J, cioè $(X - a)$; se $I = (X^2 + bX + c)$ (con $b, c \in \mathbb{R}$ e $b^2 - 4c < 0$) ci sono due J, cioè $(X - r)$ e $(X - \bar{r})$, dove r e $\bar{r}$ sono le radici (non reali) di $X^2 + bX + c$.

5. È facile dimostrare che P non ha radici in K: a tal fine si può verificare direttamente che per ogni $a \in K$ si ha $a^3 \neq 2$; in alternativa basta osservare che, se r è una radice di P, allora $r^6 = (r^3)^2 =$

$2^2 = 4$, mentre $0^6 = 0$ e $a^6 = 1$ se $0 \neq a \in K$ per il piccolo teorema di Fermat. Essendo $\deg(P) = 3$ ne segue che P è irriducibile in $K[X]$. Pertanto I è massimale e F è un campo.

Si ha $\dim_K F = \deg(P)$, e quindi $|F| = |K|^3 = 7^3 = 343$.