Algebra 2 - Seconda prova parziale - 31 gennaio 2013
Tema A

NOME E COGNOME:

MATRICOLA:

Es 1	Es 2	Es 3	Es 4	Es 5	Tot

Risolvere ciascun esercizio su una pagina nuova

1. (a) Verificare che $1+\sqrt{3}$ non è un quadrato in $\mathbb{Q}[\sqrt{3}]$.
   R. Se $1+\sqrt{3} = (a+b\sqrt{3})^2 = a^2+3b^2+2ab\sqrt{3}$ con $a, b \in \mathbb{Q}$ otteniamo rapidamente $a \neq 0$, $b = \frac{1}{2a}$, $4a^4-4a^2+3=0$, a^2 zero del polinomio $4x^2-4x+3$ che non ha zeri razionali (ha discriminante <0), contraddizione.

   (b) Scegliamo $u \in \mathbb{R}$ tale che $u^2 = 1+\sqrt{3}$. Determinare il grado $[\mathbb{Q}(u) : \mathbb{Q}]$.
   R. $\sqrt{3} \in \mathbb{Q}(u)$, $u \notin \mathbb{Q}[\sqrt{3}]$, u zero di $x^2-(1+\sqrt{3}) \in \mathbb{Q}[\sqrt{3}][x]$ dicono $[\mathbb{Q}(u) : Q[\sqrt{3}]] = 2$. Da $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$ segue $[\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(u) : Q[\sqrt{3}]][\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 4$.

   (c) Verificare che u è algebrico su $\mathbb{Q}$ e trovare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
   R. Dalla precedente abbiamo che u è algebrico su $\mathbb{Q}$ con polinomio minimo di grado 4. Da $(u^2-1)^2 = (\sqrt{3})^2$ si ha subito $u^4-2u^2-2=0$ cioè u è zero del polinomio $x^4-2x^2-2 \in \mathbb{Q}[x]$ di grado 4 e monico. Allora si tratta del polinomio minimo (che x^4-2x^2-2 sia irriducibile in $\mathbb{Q}[x]$ segue anche dal criterio di Eisenstein).

   (d) Scrivere $(u^2+1)^{-1}$ come espressione polinomiale in u a coefficienti in $\mathbb{Q}$.
   R. La divisione euclidea fornisce $x^4-2x^2-2 = (x^2+1)(x^2-3)+1$. Calcolando in u si trova $(u^2+1)(u^2-3) = -1$ da cui $(u^2+1)^{-1} = 3-u^2$.

   (e) Controllare se $\mathbb{Q}(u)$ è campo di spezzamento di $f(x)$ su $\mathbb{Q}$.
   R. Si tratta di vedere se $\mathbb{Q}(u)$ contiene tutti gli zeri complessi di $f(x)$. Se $v^2 = 1-\sqrt{3}$ conti analoghi a quelli fatti sopra danno $v^4-2v^2-2=0$, cioè anche v è zero di $f(x)$. Ma $v^2<0$, v non è reale mentre $\mathbb{Q}(u) \subseteq \mathbb{R}$, quindi $\mathbb{Q}(u)$ non è campo di spezzamento di $f(x)$ su $\mathbb{Q}$

2. (a) Se n è un intero positivo, definire il polinomio ciclotomico n-mo $\Phi_n(x)$.

R. È il prodotto $\prod_z (x - z)$ dove z descrive l'insieme delle radici n-esime primitive complesse di 1.

(b) Sia $n = p^2$ con p primo.
Dimostrare che $\Phi_{p^2}(x) = 1 + x^p + \cdots + (x^p)^{p-1}$.
R. Se z è una radice p^2-esima di 1, o z è primitiva oppure $z^p = 1$. Nella scomposizione $x^{p^2} - 1 = (x^p - 1)(1 + x^p + \cdots + (x^p)^{p-1})$, le radici non primitive sono gli zeri di $x^p - 1$, quelle primitive sono gli zeri dell'altro fattore. Quindi $\Phi_{p^2}(x) = (x^{p^2} - 1)/(x^p - 1) = 1 + x^p + \cdots + (x^p)^{p-1}$.

3. Sia $F = \mathbb{Z}/5\mathbb{Z}$ e sia $g(x) = x^2 + x + 1 \in F[x]$.

(a) Verificare che $g(x)$ è irriducibile in $F[x]$.
R. g ha grado 2; basta allora controllare che non abbia zeri in F. E infatti $g(0) = 1$, $g(1) = 3$, $g(2) = 2$, $g(3) = 3$, $g(4) = 1$.

(b) Sia α una radice di $g(x)$ in una opportuna estensione di F e sia $K = F(\alpha)$. Determinare la cardinalità di K.
R. Il polinomio minimo di α è g, di grado 2, quindi gli elementi di $K = F(\alpha)$ si scrivono in modo unico come $a + b\alpha$ con a, $b \in F$. Allora $|K| = 5^2$.

(c) Dire se $h(x) = x^2 - x + 1$ è irriducibile in $K[x]$.
R. h ha grado 2, di nuovo si tratta di vedere se ha zeri, questa volta in K. Tenendo conto che $\alpha^2 + \alpha + 1 = 0$, risulta $h(a + b\alpha) = (a^2 - b^2 - a + 1) + b(2a - b - 1)\alpha$: $h(a + b\alpha) = 0$ se e solo se $(a, b) \in F^2$ è soluzione del sistema

$$\begin{cases} a^2 - b^2 - a + 1 &= 0 \\ b(2a - b - 1) &= 0 \end{cases}$$

Non ci sono soluzioni con $b = 0$. Ma con $b = 2a - 1$ la prima equazione diventa $a(-a + 1) = 0$ e abbiamo le soluzioni $(0, -1)$ e $(1, 1)$, cioè $-\alpha$ e $1 + \alpha$ sono zeri di h, e $h = (x + \alpha)(x - (1 + \alpha))$ in $K[x]$.

4. Dimostrare il teorema:

Dati i campi F, $\bar{F}$ e l'isomorfismo $\eta : F \to \bar{F}$ che estendiamo a $\eta : F[x] \to \bar{F}[x]$ ed estensioni E, $\bar{E}$ rispettivamente di F, $\bar{F}$, sia $u \in E$ algebrico su F con polinomio minimo g. Allora

(a) se esiste un omomorfismo $\varphi : F(u) \to \bar{E}$ che estende η, allora $\varphi(u)$ è zero di $\eta(g)$;
R. Posto $g = b_0 + b_1 x + \ldots + x^r$, risulta $\eta(g)(\varphi(u)) = \eta(b_0) + \eta(b_1)(\varphi(u)) + \ldots + (\varphi(u))^r = \varphi(b_0) + \varphi(b_1)(\varphi(u)) + \ldots + (\varphi(u))^r = \varphi(g(u)) = \varphi(0) = 0$.

(b) se $v \in \bar{E}$ è zero di $\eta(g)$, allora esiste un omomorfismo $\varphi : F(u) \to \bar{E}$ tale che $\varphi_{|F} = \eta$ e $\varphi(u) = v$.

R. Indichiamo con σ l'omomorfismo $F[x] \to F(u)$ di valutazione in u, con $\bar{\sigma}$ l'omomorfismo $\bar{F}[x] \to \bar{F}(v) \leq \bar{E}$ di valutazione in v, e poniamo $\tau = \bar{\sigma} \circ \eta : F[x] \to \bar{F}(v)$. τ è un omomorfismo suriettivo. Osserviamo che $\eta(g)$ è irriducibile in $\bar{F}[x]$ e quindi è il polinomio minimo di v. Ora $f \in F[x]$ appartiene al nucleo di τ se e solo se $\eta(f)(v) = 0$ se e solo se $\eta(g)$ divide $\eta(f)$ se e solo se g divide f: $\ker(\tau) = (g)$. Per il teorema fondamentale di omomorfismo $\tau' : f + (g) \mapsto \tau(f)$ è un isomorfismo di $F[x]/(g)$ su $F(v)$. Anche $\ker(\sigma) = (g)$, e $\sigma' : f + (g) \mapsto f(u)$ è un isomorfismo di $F[x]/(g)$ su $F(u)$. Allora la funzione composta $\varphi = \tau' \circ (\sigma')^{-1}$ è un isomorfismo di $F(u)$ su $\bar{F}(v)$. Se $a \in F$ risulta $\varphi(a) = \tau'((\sigma')^{-1}(a)) = \tau'(a + (g)) = \eta(a)$; inoltre $\varphi(u) = \tau'((\sigma')^{-1}(u) = \tau'(x + (g)) = v$.

5. Siano X, Y insiemi non vuoti.

   (a) Dire che cosa significa $\text{card}(X) \leq \text{card}(Y)$.

   R. Significa: esiste una funzione iniettiva $X \to Y$.

   (b) Dimostrare che $\text{card}(X) \leq \text{card}(Y)$ se e solo se esiste una funzione suriettiva $h : Y \to X$.

   R. Supponiamo dapprima che esista una funzione suriettiva $h : Y \to X$. Per una delle proposizioni equivalenti all'assioma della scelta h ha un'inversa destra $g : X \to Y$, cioè $h \circ g$ è l'identità di X. Questa g è iniettiva.

   Supponiamo ora che esista una funzione iniettiva $f : X \to Y$. Fissiamo un elemento $a \in X$. Restringendo il codominio a $f(X)$ invertiamo f con $f^{-1} : f(X) \to X$. Definendo $h(y) = f^{-1}(y)$ se $y \in f(X)$, $h(y) = a$ se $y \notin f(X)$ otteniamo una funzione suriettiva.