Padova, 5 luglio 2006

Appello di Algebra

Esercizio 1

Provare che $u = \sqrt{1+\sqrt{2}}$ è algebrico su $\mathbb{Q}$.
a) Si determini il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
b) Si trovi il polinomio minimo di u su $\mathbb{Q}(\sqrt{2})$.
c) Si trovi una base di $\mathbb{Q}(u)$ sul campo $\mathbb{Q}(\sqrt{2})$.

a) Quadrando si trova $\sqrt{2} = u^2 - 1$ (e quindi $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(u)$). Quadrando ancora si trova che $(u^2-1)^2 = 2$, cioè u è zero del polinomio $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$, e u è algebrico su $\mathbb{Q}$. È un polinomio biquadratico, i cui zeri complessi sono u, $-u$, v, $-v$ dove $v = i\sqrt{\sqrt{2}-1}$. Si vede subito che è irriducibile in $\mathbb{Q}[x]$, ed è quindi il polinomio minimo $f(x)$ cercato.
b) Da a) segue che $[\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$ e quindi il grado del polinomio minimo di u su $\mathbb{Q}(\sqrt{2})$ è $[\mathbb{Q}(u) : \mathbb{Q}(\sqrt{2})] = 2$. Allora il polinomio minimo di u su $\mathbb{Q}(\sqrt{2})$ è $x^2 - 1 - \sqrt{2}$.
c) Poichè $[\mathbb{Q}(u) : \mathbb{Q}(\sqrt{2})] = 2$ una base di $\mathbb{Q}(u)$ sul campo $\mathbb{Q}(\sqrt{2})$ è $\{1, u\}$.

Esercizio 2

a) Si dia la definizione di sottogruppo normale di un gruppo.
b) Sia $\mathbb{R}$ il campo dei reali. Sia G il gruppo

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

(sottogruppo del gruppo degli invertibili dell'anello delle matrici 3×3 a coefficienti in $\mathbb{R}$). Si considerino i seguenti sottoinsiemi di G:

$$H = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}; K = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, c \in \mathbb{R} \right\}; L = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Si dica, giustificando la risposta, quali di questi sono sottogruppi di G, e quali sono sottogruppi normali di G.

a) vedi libro.
b) Se g, $g' \in G$

$$g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}; \quad g' = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}$$

calcoliamo

$$gg' = \begin{pmatrix} 1 & a'+a & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix}, \quad g^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Notiamo che H, K, L sono non vuoti. Poi: se g, $g' \in H$ è $b = c = b' = c' = 0$ e quindi $gg' \in H$, $g^{-1} \in H$: H è sottogruppo. Invece K non è chiuso per il prodotto: se $a = 1$, $b = c = 0$, $a' = b' = 0$, $c' = 1$ è g, $g' \in K$ ma $gg' \notin K$. Le formule di sopra del prodotto e dell'inverso permettono analogamente di vedere che anche L è un sottogruppo.

Con g, g' come sopra, calcoliamo

$$gg'g^{-1} = \begin{pmatrix} 1 & a' & -ca' + ac' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}.$$

Se $g' \in H$ cioè $b' = c' = 0$ può essere $-ca' \neq 0$: H non è normale in G. Invece se $g' \in L$ cioè $c' = 0$, risulta $gg'g^{-1} \in L$ per ogni $g \in G$: L è normale in G.

Esercizio 3

Determinare il campo di spezzamento E del polinomio $x^6 - 6x^3 + 8$ su $\mathbb{Q}$, il grado di E su $\mathbb{Q}$ e una $\mathbb{Q}$-base di E.

$x^6 - 6x^3 + 8 = (x^3 - 2)(x^3 - 4)$. Le sue radici sono le radici terze di 2 e le radici terze di 4:

$$\sqrt[3]{2},\ \sqrt[3]{2}\epsilon,\ \sqrt[3]{2}\epsilon^2,\ \sqrt[3]{4},\ \sqrt[3]{4}\epsilon,\ \sqrt[3]{4}\epsilon^2$$

dove ϵ è uno zero di $x^2 + x + 1$. Poichè $\sqrt[3]{4} = (\sqrt[3]{2})^2$ risulta $E = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$ e si calcola subito $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 6$ perchè $\epsilon \notin \mathbb{Q}(\sqrt[3]{2})$.

Esercizio 4

Si dimostri il primo teorema di Sylow:
"Sia G un gruppo finito di ordine $p^\alpha m$, dove p è un numero primo e m non è divisibile per p. Allora G contiene un sottogruppo di ordine p^α."

vedi libro

Esercizio 5

Sia $A = \mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$ con norma $N \colon \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}$ definita da $N(a + b\sqrt{-6}) = a^2 + 6b^2$.
a) Provare che non esistono elementi di A di norma 2 o 5.
b) Provare che gli elementi 2, 5, $2 - \sqrt{-6}$ sono irriducibili ma non primi.
c) Trovare due fattorizzazioni di 10 nel prodotto di due elementi irriducibili non associati.
d) Provare che l'ideale generato da 2 e $\sqrt{-6}$ non contiene l'elemento 1.

Si verifica subito che la scrittura degli elementi di A nella forma $a + b\sqrt{-6}$ con $a, b \in \mathbb{Z}$ è unica, che $(a + b\sqrt{-6})(a - b\sqrt{-6}) = N(a + b\sqrt{-6})$ e che $N(uv) = N(u)N(v)$.
a) Se a, $b \in \mathbb{Z}$ e $b \neq 0$ risulta $a^2 + 6b^2 \geq 6$; se invece $b = 0$ allora $a^2 + 6b^2 = a^2$, ma 2 e 5 non sono quadrati in $\mathbb{Z}$.
b),c) Da $N(uv) = N(u)N(v)$, $N(u) \geq 0$, $N(1) = 1$ segue che gli invertibili di A sono 1, -1 (i soli elementi di norma 1) e che u è associato di v se e solo se $u = \pm v$.
Se $2 = uv$ allora $4 = N(u)N(v)$: $N(u)$, $N(v)$ non sono 2, quindi uno tra $N(u)$, $N(v)$ è 1 e la fattorizzazione è banale: 2 è irriducibile. Analogamente si vede che 5 è irriducibile.
Se $2 - \sqrt{-6} = uv$ allora $10 = N(2 - \sqrt{-6}) = N(u)N(v)$: $N(u)$, $N(v)$ non sono 2 nè 5, quindi uno tra $N(u)$, $N(v)$ è 1 e la fattorizzazione è banale: $2 - \sqrt{-6}$ è irriducibile. Lo stesso per $2 + \sqrt{-6}$.
Infine $10 = 2 \cdot 5 = (2 - \sqrt{-6})(2 + \sqrt{-6})$ ma 2, 5, $2 - \sqrt{-6}$, $2 + \sqrt{-6}$ non sono associati. Questo prova che non sono primi: dividono un prodotto ma non dividono alcuno dei fattori.
d) Gli elementi dell'ideale generato da 2 e $\sqrt{-6}$ sono combinazioni lineari $2(a + b\sqrt{-6}) + \sqrt{-6}(c + d\sqrt{-6}) = (2a - 6b) + (2b + c)\sqrt{-6}$ con a, b, c, $d \in \mathbb{Z}$: il primo coefficiente è sempre pari.

Esercizio 6

Sia A un anello commutativo con unità e siano I e J due ideali di A.
a) Si provi che $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$ è un ideale di A contenuto in $I \cap J$.
b) Verificare che se I e J sono ideali primi di A, allora IJ è ideale primo se e solo se IJ coincide con I o con J.

a) vedi libro
b) Se I e J sono primi e $IJ = I$ o $IJ = J$, certo IJ è primo. Viceversa, supponiamo $IJ \neq I$ e $IJ \neq J$. Allora $IJ \subset I$ e $IJ \subset J$ per a), e le inclusioni sono strette: esistono $a \in I$ e $b \in J$ tali che $a \notin IJ$ e $b \notin IJ$. Però il prodotto $ab \in IJ$, e IJ non è primo.