Padova, 10 gennaio 2006

Appello di Algebra

Esercizio 1

Sia $\alpha = \sqrt{3} + \frac{i}{\sqrt{2}}$.
a) Trovare il polinomio minimo $f(x)$ di α su $\mathbb{Q}$.
b) Verificare che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$.
c) Verificare se $\mathbb{Q}(\alpha)$ è campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

b) E' intanto chiaro che $\alpha = \sqrt{3} + \frac{i}{\sqrt{2}} \in \mathbb{Q}(\sqrt{3}, i\sqrt{2})$. Quadrando $\alpha - \sqrt{3} = \frac{i}{\sqrt{2}}$ si ricava $\sqrt{3} = \frac{2\alpha^2+7}{4\alpha}$ da cui $\sqrt{3} \in \mathbb{Q}(\alpha)$ e anche $i\sqrt{2} = 2(\alpha - \sqrt{3}) \in \mathbb{Q}(\alpha)$. Si conclude che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$.
a) Da sopra si ricava il grado di $f(x)$ che è $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i\sqrt{2}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$ perchè il polinomio minimo di $i\sqrt{2}$ su $\mathbb{Q}(\sqrt{3})$ è $x^2 + 2$ e il polinomio minimo di $\sqrt{3}$ su $\mathbb{Q}$ è $x^2 - 3$.
Continuando i conti, quadrando di nuovo si ottiene $4\alpha^4 - 20\alpha^2 + 49 = 0$ e quindi α è zero del polinomio $x^4 - 5x^2 + \frac{49}{4}$ che è monico e ha il grado giusto: è il polinomio minimo.
c) E' campo di spezzamento: $f(x)$ è biquadratico a coefficienti reali; le sue radici sono $\alpha, -\alpha, \bar{\alpha}, -\bar{\alpha}$ cioè $\pm\sqrt{3} \pm \frac{i}{\sqrt{2}}$ che sono tutti in $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$.

Esercizio 2

Siano $A, A_1, \dots, A_n, n > 1$, anelli e siano $\phi_i : A \to A_i, 1 \le i \le n$, omomorfismi d' anello. Si consideri l'omomorfismo $\phi : A \to A_1 \times A_2 \times \cdots \times A_n$ definito da $\phi(a) = (\phi_1(a), \phi_2(a), ..., \phi_n(a))$ per ogni $a \in A$.
Si verifichi che:
(a) $\mathrm{Ker}(\phi) = \cap_{i=1}^n \mathrm{Ker}(\phi_i)$;
(b) se ϕ_i è iniettiva per qualche i $(1 \le i \le n)$, allora ϕ è iniettiva;
(c) se ogni ϕ_i è suriettiva, si può concludere che ϕ è suriettiva?

a) $\mathrm{Ker}(\phi) = \{a \in A \mid \phi(a) = 0\}$ dove lo 0 di $A_1 \times A_2 \times \cdots \times A_n$ è $(0, \dots, 0)$ - la coordinata i è lo 0 di A_i. Allora $\phi(a) = (\phi_1(a), \phi_2(a), ..., \phi_n(a)) = (0, \dots, 0)$ se e solo se $\phi_i(a) = 0$ per ogni i cioè se e solo se $a \in \cap_{i=1}^n \mathrm{Ker}(\phi_i)$.
b) Se qualche ϕ_i è iniettiva allora $\mathrm{Ker}(\phi_i) = 0$; segue $\mathrm{Ker}(\phi) = \cap_{i=1}^n \mathrm{Ker}(\phi_i) = 0$ e ϕ è iniettiva.
c) No. Esempio: $A = A_1 = A_2 = \mathbb{Z}$, $\phi_1 = \phi_2 =$identità. Qui $\phi(a) = (a, a)$ e $\mathrm{Im}(\phi) = \{(a, a) \mid a \in \mathbb{Z}\} \subsetneqq \mathbb{Z} \times \mathbb{Z}$.

Esercizio 3

Sia R l'anello $\mathbb{Z}/p^2\mathbb{Z}$, dove p è un primo. Sia G il gruppo

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

(è sottogruppo del gruppo degli invertibili dell'anello delle matrici 2×2 a coefficienti in R).
a) Si scriva esplicitamente l'inverso di $\begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix}$.
b) Qual è l'ordine di G?
c) Si provi che il sottoinsieme

$$H = \left\{ \begin{pmatrix} 1+pb & b \\ 0 & 1 \end{pmatrix} \mid b \in R \right\}$$

è un sottogruppo di G.
d) H è ciclico? è normale in G?

Per ogni $a \in R = \mathbb{Z}/p^2\mathbb{Z}$ è $p^2a = 0$; ne segue $(1+pa)(1-pa) = 1 - p^2a^2 = 1$ cioè $(1+pa)^{-1} = 1 - pa$. Calcoliamo

$$\begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1+pa' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p(a+a') & b+b'+pab' \\ 0 & 1 \end{pmatrix}$$

perchè $p^2aa' = 0$.

a) Dal conto di sopra $\begin{pmatrix} 1+pa' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix}^{-1}$ se e solo se $p(a+a') = 0$ e $b+b'+pab' = 0$, condizioni equivalenti a $pa' = -pa$ e $b' = -b(1+pa)^{-1} = -b(1-pa)$, cioè

$$\begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1-pa & -b(1-pa) \\ 0 & 1 \end{pmatrix}.$$

b) Al posto $(1,1)$ ho gli elementi di $1+pR$. Sono tanti quanti gli elementi di $pR = p\mathbb{Z}/p^2\mathbb{Z}$: sono p. Al posto $(1,2)$ ho un arbitrario elemento di R: sono p^2. Quindi $|G| = p^3$.
c) H è finito e non vuoto. Basta controllare il prodotto:

$$\begin{pmatrix} 1+pb & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1+pb' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p(b+b') & b+b'+pbb' \\ 0 & 1 \end{pmatrix}$$

è della forma $\begin{pmatrix} 1+px & x \\ 0 & 1 \end{pmatrix}$ perchè $p(b+b'+pbb') = p(b+b')$.
d) Poichè $|H| = p^2$, ogni elemento non identico di H ha periodo p o p^2 e H è ciclico se e solo se contiene un elemento di periodo p^2. Calcoliamo $\begin{pmatrix} 1+pb & b \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1+p2b & 2b+pb^2 \\ 0 & 1 \end{pmatrix}$. Se $p = 2$ $2 \cdot 2b = 0$ e $2b + 2b^2 = 2b(b+1) = 0$ perche' o b o $b+1$ è pari. In questo caso allora tutti gli elementi non identici di H hanno ordine 2 e H non è ciclico. Se $p \neq 2$ invece H è ciclico. Si verifica (induzione) che se $n \geq 2$ risulta $\begin{pmatrix} 1+pb & b \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1+npb & nb+\frac{n(n-1)}{2}pb^2 \\ 0 & 1 \end{pmatrix}$. Per $n = p$ $\frac{p(p-1)}{2}$ è multiplo di p, quindi $\begin{pmatrix} 1+pb & b \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix}$, che non è 1 se $b \notin pR$, per esempio se $b = 1$. Ognuno di questi elementi ha allora periodo p^2 ed è un generatore di H.
H è normale in G: se $g = \begin{pmatrix} 1+pa & b \\ 0 & 1 \end{pmatrix}$, $h = \begin{pmatrix} 1+pc & c \\ 0 & 1 \end{pmatrix}$, risulta $ghg^{-1} = \begin{pmatrix} 1+pc & x \\ 0 & 1 \end{pmatrix}$ con $x = b+c+pac-b(1-pa)+(pa+pc)(-b(1-pa))$ e $ghg^{-1} \in H$ perchè $px = pc$.

Esercizio 4

Trovare il campo di spezzamento del polinomio x^4+1 su $\mathbb{R}$, su $\mathbb{Q}$ e sul campo con 16 elementi.

Le radici complesse di x^4+1 sono $\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, $\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$, $-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, $-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}$ (le radici quarte di -1). Il campo di spezzamento su $\mathbb{R}$ è $\mathbb{R}(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}) = \mathbb{R}(i) = \mathbb{C}$.

Il campo di spezzamento su $\mathbb{Q}$ è $\mathbb{Q}(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}) = \mathbb{Q}(\sqrt{2}, i)$.

Se F ha $16 = 2^4$ elementi allora F ha caratteristica 2 e $x^4 + 1 = (x+1)^4$: il campo di spezzamento è F.

Esercizio 5

Si dimostri il seguente enunciato (teorema di isomorfismo):
Siano H, N sottogruppi del gruppo G, e sia $N \trianglelefteq G$.
a) HN è sottogruppo di G contenente N;
b) $H \cap N \trianglelefteq H$;
c) $H/H \cap N \cong HN/N$.

Si veda il testo.

Esercizio 6

Sia A un anello commutativo con unità. Si provi che A è un campo se e solo se i soli ideali di A sono A e 0.

Si veda il testo.