Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2006/2007
AL2 - Algebra 2, gruppi, anelli e campi
Tutorato 6 (21 dicembre 2006)
Stefano Urbinati

1. Provare che i seguenti numeri complessi α sono algebrici su $\mathbb{Q}$ trovando un polinomio non nullo $f(X) \in \mathbb{Q}[X]$ tale che $f(\alpha) = 0$:

$$1+\sqrt{2}; \quad \sqrt{2}+\sqrt{3}; \quad 1+i; \quad \sqrt{1+\sqrt[3]{2}}.$$

SOLUZIONE:

(a) $(1+\sqrt{2})^2 = 3+\sqrt{2}$ da cui $(1+\sqrt{2})^2 - 2(1+\sqrt{2}) - 1 = 0$; pertanto $X^2 - 2X - 1 \in \mathbb{Q}[X]$ ha $1+\sqrt{2}$ come radice.

(b) $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$ e $(\sqrt{2}+\sqrt{3})^4 = 49+20\sqrt{6}$; pertanto $(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$; allora $X^4 - 10X + 1 \in \mathbb{Q}[X]$ ha $\sqrt{2}+\sqrt{3}$ come radice.

(c) $(1+i)^2 = 2i$; allora $(1+i)^2 - 2(1+i) + 2 = 0$; pertanto $X^2 - 2X + 2 \in \mathbb{Q}[X]$ ha $1+i$ come radice.

(d) Poniamo $\alpha = \sqrt{1+\sqrt[3]{2}}$; allora $\alpha^2 = 1+\sqrt[3]{2}$ da cui $\alpha^2 - 1 = \sqrt[3]{2}$. Elevando al cubo si ottiene $(\alpha^2-1)^3 = 2$ da cui $\alpha^6 - 3\alpha^4 + 3\alpha^2 - 3 = 0$. Pertanto il polinomio $X^6 - 3X^4 + 3X^2 - 3 \in \mathbb{Q}[X]$ ha $\sqrt{1+\sqrt[3]{2}}$ come radice.

2. Stabilire se i seguenti numeri complessi α sono algebrici o trascendenti sopra l'assegnato campo F; per gli elementi algebrici trovati determinare il polinomio minimo su F:

(a) $\alpha = 1+i, \quad F = \mathbb{Q}$; $\qquad \alpha = \sqrt{2}+i, \quad F = \mathbb{Q}$;

(b) $\alpha = \sqrt{\pi}, \quad F = \mathbb{Q}$; $\qquad \alpha = \sqrt{\pi}, \quad F = \mathbb{Q}(\pi)$;

(c) $\alpha = \pi^2, \quad F = \mathbb{Q}(\pi)$; $\qquad \alpha = \pi^2, \quad F = \mathbb{Q}(\pi^3)$.

SOLUZIONE:

(a) $1+i$ è per l'esercizio precedente algebrico di grado 2 con $X^2 - 2X + 2$ come polinomio minimo su $\mathbb{Q}$.

Sia $\alpha = \sqrt{2}+i$; allora da $\alpha - i = \sqrt{2}$, elevando al quadrato, si ottiene $\alpha^2 - 3 = 2\alpha i$ da cui, elevando di nuovo al quadrato, si ha $\alpha^4 - 2\alpha^2 + 9 = 0$; pertanto $\sqrt{2}+i$ è radice di $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$; quindi $\sqrt{2}+i$ è algebrico su $\mathbb{Q}$.

Inoltre $X^4 - 2X^2 + 9$, essendo irriducibile su $\mathbb{Q}$ (perché?; decomporre $X^4 - 2X^2 + 9$ in fattori irriducibili in $\mathbb{R}[X]$), è il polinomio minimo di α su $\mathbb{Q}$.

Oppure, poiché $\mathbb{Q}(\sqrt{2}+i) = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$ (verificare!) e $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$, si ha che il polinomio $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ è irriducibile in $\mathbb{Q}[X]$ ed è pertanto il polinomio minimo di $\sqrt{2}+i$ su $\mathbb{Q}$.

(b) $\sqrt{\pi}$ è trascendente su $\mathbb{Q}$ perché se $\sqrt{\pi}$ fosse algebrico su $\mathbb{Q}$, allora anche $\pi = \sqrt{\pi}\sqrt{\pi}$ sarebbe algebrico su $\mathbb{Q}$.
Poiché π è trascendente su $\mathbb{Q}$, $\sqrt{\pi} \notin \mathbb{Q}(\pi)$ (verificare!!); inoltre $X^2 - \pi \in \mathbb{Q}(\pi)[X]$ ha $\sqrt{\pi}$ come radice; pertanto $\sqrt{\pi}$ è algebrico su $\mathbb{Q}(\pi)$ di grado 2.

(c) $\pi^2 \in \mathbb{Q}(\pi)$; quindi π^2 è algebrico su $\mathbb{Q}(\pi)$ di grado 1.
$\pi^2 \notin \mathbb{Q}(\pi^3)$; se $\pi^2 \in \mathbb{Q}(\pi^3)$, allora $\pi^2 = \frac{a_0+a_1\pi^3+\cdots+a_n\pi^{3n}}{b_0+b_1\pi^3+\cdots+b_m\pi^{3m}}$ con $a_0, a_1, \cdots, a_n \in \mathbb{Q}$, $b_0, b_1, \cdots, b_m \in \mathbb{Q}$, $a_n \neq 0$ e $b_m \neq 0$ da cui $(b_0 + b_1\pi^3 + \cdots + b_m\pi^{3m})\pi^2 = a_0 + a_1\pi^3 + \cdots + a_n\pi^{3n}$; poiché π è trascendente su $\mathbb{Q}$, seguirebbe che se $m \geqslant n$, allora $b_m = 0$ e se $n > m$, allora $a_n = 0$.
$X^3 - \pi^6 = X^3 - (\pi^3)^2 \in \mathbb{Q}(\pi^3)[X]$ ed ha π^2 come radice; pertanto π^2 è algebrico su $\mathbb{Q}(\pi^3)$ ed il suo grado è $\leqslant 3$; se il suo grado fosse 2, esisterebbe un polinomio monico di grado 2 in $\mathbb{Q}(\pi^3)[X]$, $f(X)$, tale che $f(\pi^2) = 0$; allora $f(X)$ dovrebbe dividere $X^3 - \pi^6$in $\in \mathbb{Q}(\pi^3)[X]$, e ciò è assurdo, poiché $X^3 - \pi^6$ si decompone in $\mathbb{R}[X]$ in $(X - \pi^2)(X^2 + \pi^2 X + \pi^4)$.

3. Sia il campo K una estensione del campo F. Provare che se $a \in K$ è algebrico di grado dispari su F, allora anche a^2 è algebrico di grado dispari e $F(a) = F(a^2)$.

SOLUZIONE:

Poiché a è algebrico di grado dispari, $[F(a) : F] = 2n + 1$ con $n \geqslant 0$. Se $n = 0$, $a \in F$ da cui $a^2 \in F$; pertanto a^2 è algebrico di grado 1 e $F(a) = F(a^2) = F$. Possiamo allora supporre che $n \geqslant 1$; poiché $a^2 \in F(a)$, si ha che $F \subseteq F(a^2) \subseteq F(a)$; quindi $[F(a^2) : F] \leqslant [F(a) : F]$ da cui a^2 è anche esso algebrico su F; inoltre si ha:

$$[F(a) : F] = [F(a^2) : F][F(a) : F(a^2)];$$

poiché $[F(a) : F]$ è dispari, anche $[F(a^2) : F]$ e $[F(a) : F(a^2)]$ sono dispari, cioè a^2 è algebrico di grado dispari su F;

inoltre $X^2 - a^2 \in F(a^2)[X]$ ed ha a come radice; quindi $[F(a) : F(a^2)] = 1$ da cui $a \in F(a^2)$; pertanto $F(a) = F(a^2)$.

4. Provare che $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{2})$ sono isomorfi come $\mathbb{Q}$-spazi vettoriali ma non come campi.

SOLUZIONE:

Sia $\varphi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(i)$ l'applicazione definita da $\varphi(a + b\sqrt{2}) = a + ib$. Si verifica facilmente che φ è un isomorfismo di $\mathbb{Q}$-spazi vettoriali.

Supponiamo che esista un isomorfismo $\psi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(i)$ di campi; poiché $\psi(1) = 1$, ψ ristretto a $\mathbb{Q}$ dovrebbe essere l'identità; sia $\psi(\sqrt{2}) = a + ib$ con $a, b \in \mathbb{Q}$; poiché $2 = \sqrt{2} \cdot \sqrt{2}$ si dovrebbe avere $2 = \psi(\sqrt{2}) \cdot \psi(\sqrt{2}) = (a + ib)^2 = a^2 - b^2 + 2iab$ da cui seguirebbe che $a = \pm\sqrt{2} \in \mathbb{Q}$ oppure $b^2 = -2$, che è assurdo in entrambi i casi. Ne consegue che i campi $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{2})$ non sono isomorfi.

5. Sia il campo K una estensione del campo F e sia $c \in F$. Provare che se $X^n - c \in F[X]$ è irriducibile in $F[X]$ ed $a \in K$ è una radice di $X^n - c$,

allora per ogni intero positivo m che divide n il grado di a^m su F è $\frac{n}{m}$. Qual è il polinomio minimo di a^m su F?

SOLUZIONE:

Poiché a è radice di un polinomio irriducibile di grado n di $F[X]$, $X^n - c$, si ha che $[F(a) : F] = n$. Sia m un intero positivo che divide n: a^m è radice del polinomio $X^{\frac{n}{m}} - c \in F[X]$ e quindi algebrico su F di grado $\leqslant \frac{n}{m}$; da $F \subseteq F(a^m) \subseteq F(a)$ segue che

$$n = [F(a) : F] = [F(a^m) : F][F(a) : F(a^m)] \leqslant \frac{n}{m}[F(a) : F(a^m)];$$

poiché $X^m - a^m \in F(a^m)[X]$ ha a come radice, $[F(a) : F(a^m)] \leqslant m$; pertanto da $n = [F(a) : F] \leqslant \frac{n}{m} \cdot m$ segue che $[F(a^m) : F] = \frac{n}{m}$ e $[F(a) : F(a^m)] = m$; poiché il grado di a^m è $\frac{n}{m}$, il suo polinomio minimo su F è $X^{\frac{n}{m}} - c$.

6. Siano $F = \mathbb{Q}$, $E_1 = \mathbb{Q}(\sqrt{2})$ e $E_2 = E_1(\sqrt{1+\sqrt{2}})$. Trovare il polinomio minimo di $\sqrt{1+\sqrt{2}}$ su F. E' E_2 il suo campo di spezzamento?

   SOLUZIONE:

   Poniamo $\alpha = \sqrt{1+\sqrt{2}}$; allora $\alpha^2 = 1 + \sqrt{2}$ da cui $\alpha^2 - 1 = \sqrt{2}$; elevando al quadrato, si ottiene $\alpha^4 - 2\alpha^2 - 1 = 0$; quindi $X^4 - 2X^2 - 1 \in \mathbb{Q}[X]$ ha α come radice; inoltre $X^4 - 2X^2 - 1$ è irriducibile in $\mathbb{Q}[X]$ (applicare il criterio di Eisenstein a $(X-1)^4 - 2(X-1)^2 - 1$); quindi $X^4 - 2X^2 - 1$ è il piolinimio minimo di α su $\mathbb{Q}$.

   Il polinomio $X^4 - 2X^2 - 1$ ha in $\mathbb{C}$, oltre alle due radici reali, $\pm\sqrt{1+\sqrt{2}}$, due radici non reali $\pm\sqrt{1-\sqrt{2}}$; poiché $E_2 = E_1(\sqrt{1+\sqrt{2}}) \subseteq \mathbb{R}$, E_2 non è il campo di spezzamento di $X^4 - 2X^2 - 1$.

7. Sia il campo K una estensione algebrica del campo F; provare che se D è un dominio d'integrità tale che $F \subseteq D \subseteq K$, allora D è un campo.

   SOLUZIONE:

   Sia d un qualunque elemento *non nullo* di D; sia $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a - 0 \in F[X]$ il suo polinomio minimo; quindi $d^n + a_{n-1}d^{n-1} + \cdots + a_1d + a - 0 = 0$.

   Se $n = 1$, allora $d \in F^\star$ e quindi d è invertibile; sia $n \geqslant 1$; allora $a_0 \neq 0$ (se $a_0 = 0$, si avrebbe $0 = d^n + a_{n-1}d^{n-1} + \cdots + a_1d = d(d^{n-1} + a_{n-1}d^{n-2} + \cdots + a_1)$ da cui, essendo $d \neq 0$, $d^{n-1} + a_{n-1}d^{n-2} + \cdots + a_1 = 0$ e ciò è assurdo poiché $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a - 0$ è il polinomio minimo di d). Pertanto $d(d^{n-1} + a_{n-1}d^{n-2} + \cdots + a_1)(-a_0)^{-1} = 1$ con $(d^{n-1} + a_{n-1}d^{n-2} + \cdots + a_1)(-a_0)^{-1} \in D$; quindi d è invertibile in D:

8. Si consideri il polinomio $f(X) = X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$.

   (a) Provare che $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

   (b) Sia u una radice reale di $f(X)$ (dire perché esiste); si consideri l'estensione $\mathbb{Q}(u)$ di $\mathbb{Q}$; esprimere ciascuno dei seguenti elementi attraverso la base $\{1, u, u^2\}$:

   $$u^4;\ u^5;\ 3u^5 - u^4 + 2;\ (u+1)^{-1};\ (u^2 - 6u + 8)^{-1}.$$

SOLUZIONE:

(a) Basta applicare il criterio di Eisenstein con $p = 3$.

(b) Un polinomio di $\mathbb{R}[X]$ di grado 3 ha sempre una radice reale; più in generale, un polinomio di $\mathbb{R}[X]$ di grado dispari ha sempre una radice reale; poiché $u^3 = 6u^2 - 9u - 3$ si ha.

i. $u^4 = u(6u^2 - 9u - 3) = 6u^3 - 9u^2 - 3u = 27u^2 - 57u - 18$;

ii. $u^5 = u(27u^2 - 57u - 18) = 27(6u^2 - 9u - 3) - 57u^2 - 18u = 105u^2 - 261u - 81$;

iii. 1 Metodo : basta trovare una identità di Bézout per i due polinomi, sicuramente primi tra loro, X^3-6X^2+9X+3 e $X+1$: dividendo X^3-6X^2+9X+3 per $X+1$ si ottiene $X^3-6X^2+9X+3 = (X+1)(X^2-7X+16)-13$ da cui $1 = -\frac{1}{13}(X^3-6X^2+9X+3)+\frac{1}{13}(X+1)(X^2-7X+16)$;valutando i polinomi in u si ha: $1 = \frac{1}{13}(u+1)(u^2-7u+16)$ da cui $(u+1)^{-1} = \frac{1}{13}(u^2-7u+16)$. 2 Metodo: $(u+1)^{-1}$ è della forma au^2+bu+c e si ha $(u+1)(au^2+bu+c) = 1$; si ottiene il sistema;

$$\begin{cases} 7a+b=0 \\ -9a+b+c=0 \\ -3a+c-1=0 \end{cases}$$

che ha come soluzione $a = \frac{1}{13}$, $b = \frac{-7}{13}$, $c = \frac{16}{13}$; quindi $(u+1)^{-1} = \frac{1}{13}(u^2-7u+16)$.

iv. Con l'algoritmo delle divisioni successive si ottiene

$$1 = -\frac{1}{35}(X-9)f(X) + \frac{1}{35}(X^2-6X+8)(X^2-9X+1);$$

pertanto $(u^2-6u+8)^{-1} = \frac{1}{35}(u^2-9u+1)$.

9. Provare che nessuno campo finito F è algebricamente chiuso.

(Sugg.: Se $F = \{a_0, \cdots, a_n\}$ si consideri il polinomio $a_1 + (X-a_0)(X-a_1)\cdots(X-a_n) \in F[X]$, dove $a_1 \neq 0$.)

SOLUZIONE:

Il polinomio $a_1 + (X-a_0)(X-a_1)\cdots(X-a_n) \in F[X]$ non ha in F alcuna radice: per ogni elemento elemento a_j di F si ha $a_1+(a_j-a_0)(a_j-a_1)\cdots(a_j-a_j)\cdots(a_j-a_n) = a_1 \neq 0$.