Università degli studi di Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2004/2005
AL2 - Algebra 2, gruppi anelli e campi
Soluzioni
10 dicembre 2004

1 Polinomio minimo e ampliamenti

1. Determinare il polinomio minimo di z sul campo K

   (a) $z = 2 + i$, $K = \mathbb{Q}$.
   (b) $z = \sqrt{2} + 2i$, $K = \mathbb{Q}$.
   (c) $z = 2i$, $K = \mathbb{Q}$.
   (d) $z = \pi + i$, $K = \mathbb{R}$.
   (e) $z = \sqrt{3}$, $K = \mathbb{Q}$.
   (f) $z = \sqrt[3]{6}$, $K = \mathbb{Q}$.

Soluzione 1.1. *(a) Per prima cosa verifichiamo che z è algebrico su K, cioè determiniamo un polinomio non nullo di cui z è radice.*

$$\begin{aligned} z &= 2+i \\ z-2 &= i \\ (z-2)^2 &= i^2 \\ z^2-4z+4 &= -1 \\ z^2-4z+5 &= 0 \end{aligned}$$

Quindi $f(X) = X^2 - 4X + 5 \in \mathbb{Q}[X]$ ha per radice $z = 2 + i$, quindi z è algebrico. Verifichiamo che $f(X)$ è anche il polinomio minimo. Per fare questo dobbiamo vedere che è irriducibile. Essendo $f(X)$ di grado 2 *è sufficiente far vedere che*$f(X) = 0$ *non ha radici in $\mathbb{Q}$. Usando la formula per le soluzioni di un'equazione di grado 2 otteniamo che le radici di $f(X) = 0$ sono:*

i. $z = 2 + i$
ii. $z = 2 - i$

Notiamo che possiamo trovare le radici di $f(X)$ più rapidamente osservando che $f(X)$ ha coefficienti in $\mathbb{Q}$ quindi reali e una soluzione complessa $z = 2 + i$ quindi anche $\overline{z} = 2 - i$ deve essere una radice di $f(X) = 0$.
Quindi il polinomio minimo di $z = 2 + i$ su $\mathbb{Q}$ è $f(X) = X^2 - 4X + 5$.

(b) Il polinomio minimo di $z = \sqrt{2} + 2i$ su$\mathbb{Q}$ è $X^4 + 4X^2 + 36$.

(c) *Il polinomio minimo di* $z = 2i$ *su* $\mathbb{Q}$ *è* $X^2 + 4$.

(d) *Il polinomio minimo di* $z = \pi + i$ *su* $\mathbb{R}$ *è* $X^2 - 2\pi X + \pi + 1$.

(e) *Il polinomio minimo di* $z = \sqrt{3}$ *su* $\mathbb{Q}$ *è* $X^2 - 3$.

(f) *Il polinomio minimo di* $z = \sqrt[3]{6}$ *su* $\mathbb{Q}$ *è* $X^3 - 6$.

2. Costruire esplicitamente i seguenti ampliamenti di $\mathbb{Q}$

   - $\mathbb{Q}(\sqrt{2})$.
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   - $\mathbb{Q}(\sqrt{2}, \sqrt{6})$.
   - $\mathbb{Q}(\sqrt{2}, \sqrt{8})$.
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$.
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7})$.

   Soluzione 1.2. *(a)*

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$$

(b)

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$$

(c)

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{6}) &= \left\{a + b\sqrt{2} + c\sqrt{6} + d\sqrt{12} : a, b, c, d \in \mathbb{Q}\right\} \\ &= \left\{a + b\sqrt{2} + c\sqrt{6} + 2d\sqrt{3} : a, b, c, d \in \mathbb{Q}\right\} \\ &= \left\{a + b\sqrt{2} + c\sqrt{6} + d'\sqrt{3} : a, b, c, d' \in \mathbb{Q}\right\} \\ &= \mathbb{Q}(\sqrt{2}, \sqrt{3}) \end{aligned}$$

(d)

$$\mathbb{Q}(\sqrt{2}, \sqrt{8}) = \mathbb{Q}(\sqrt{2})$$

(e)

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

(f)

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7}) &= \Big\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} + a'\sqrt{7} + b'\sqrt{14} \\ &\quad + c'\sqrt{21} + d'\sqrt{42} : a, b, c, d, a', b', c', d' \in \mathbb{Q}\Big\} \end{aligned}$$

3. Dimostrare che per ogni $d \in Q$ i seguenti ampliamenti di $\mathbb{Q}$ sono isomorfi:

(a) $\mathbb{Q}(\sqrt{d})$.

(b) $\mathbb{Q}(a + b\sqrt{d})$.

(c) $\mathbb{Q}(c\sqrt{d})$.

Per ogni a, b e $c \in \mathbb{Q}$.

Soluzione 1.3. *Ricordiamo che*

$$\mathbb{Q}(\sqrt{d}) = \left\{a + b\sqrt{d} : a, b \in \mathbb{Q}\right\}$$

Dimostriamo che $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}(c\sqrt{d})$. *Sia,* $\phi : \mathbb{Q}(c\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ *definita da*

$$\phi(x + yc\sqrt{d}) = x + y\sqrt{d}$$

Verificare che ϕ *è un omomorfismo di campi iniettivo e un semplice esercizio. Notiamo che* $\dim_{\mathbb{Q}} \mathbb{Q}(c\sqrt{d}) = 2 = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d})$, *quindi sono isomorfi. Analogamente si ottiene che* $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}(a + b\sqrt{d})$.

2 Campi di spezzamento

1. Sia $f(X)$ un polinomio di grado n su $\mathbb{Z}_p$ e sia α una sua radice (in un opportuno ampliamento di $\mathbb{Z}_p$). Mostrare che le radici di $f(X)$ sono:

$$\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}.$$

Dedurne che se $m(X)$ è irriducibile su $\mathbb{Z}_p$, allora $m(X)$ ha tutte le sue radici in $\dfrac{\mathbb{Z}_p[X]}{(m(X))}$.

Soluzione 2.1. *Osserviamo che* $\forall\ a \in \mathbb{Z}_p$ *si ha*

$$(X - a)^p = X^p - a^p$$

Più in generale si ha

$$(a_n X^n + \ldots + a_1 X + a_0)^p = a_n^p X^p n + \ldots + a_1^p X + a_0^p$$

Sia $f(X) = a_n X^n + \ldots + a_1 X + a_0$ *allora*

$$\begin{aligned} f(X)^p &= a_n^p X^p n + \ldots + a_1^p X + a_0^p && (1)\\ &= a_n (X^p)^n + \ldots + a_1 (X^p) + a_0 && (2)\\ &= f(X^p) && (3) \end{aligned}$$

Dove abbiamo usato il piccolo teorema di Fermat per dire che $a_i^p = a_i$. *Quindi procediamo per induzione. Sappiamo per ipotesi che* α *è radice. Allora*

$$f(\alpha^p) = f(\alpha)^p = 0$$

Quindi α^p è radice. Supponiamo che $\beta = \alpha^{p^i}$ sia radice, allora $\beta^p = \alpha^{p^{i+1}}$ è radice.

$$f(\alpha^{p^{i+1}}) = f(\beta^p) = f(\beta)^p = f(\alpha^{p^i})^p = 0$$

Quindi α^{p^i} $\forall i$ sono radici di $f(X)$. Sia $m(X)$ irriducibile su $\mathbb{Z}_p$ allora su $K = \dfrac{\mathbb{Z}_p[X]}{(m(X))}$ ha una radice data da $\overline{X}$. Quindi tutte le sue radici sono date da $\overline{X}^{p^i}$,e appartengono a K.

2. Determinare un campo contenente $\mathbb{Z}_3$ in cui il polinomio $X^4 + 2X^3 + 2X + 2$ ha tutte le sue radici.

   Soluzione 2.2. *Poniamo $f(X) = X^4 + 2X^3 + 2X + 2$, osserviamo che $f(X)$ non ha radici in $\mathbb{Z}_3$. Ma*

   $$f(X) = (X^2 + 1)(X^2 + 2X + 2)$$

   Poniamo $g(X) = X^2 + 1$, allora $g(X)$ è irriducibile perché ha grado 2 e non ha radici in $\mathbb{Z}_3$. Poniamo

   $$K = \mathbb{Z}_3[X]/(g(X)) = \left\{a + b\overline{X} : a, b \in \mathbb{Z}_3\right\}$$

   Poniamo, per semplicità, $i = \overline{X}$, allora su K

   $$g(t) = (t^2 + 1) = (t + 2i)(t + i)$$

   Poniamo $h(t) = t^2 + 2t + 2$, vediamo se $h(t)$ ha radici in K. Si ha che $2 + i$ e $2 + 2i$ sono radici di $h(t)$. Quindi

   $$h(t) = (t - (2 + i))(t - (2 + 2i))$$

   Dunque K è il campo di spezzamento di f, infatti su K

   $$f(t) = (t + 2i)(t + i)(t - (2 + i))(t - (2 + 2i)).$$

3. Determinare il campo di spezzamento dei seguenti polinomi sul campo K.

   (a) $x^2 - 2$, $K = \mathbb{Q}$
   (b) $x^4 + 5x^2 - 6$, $K = \mathbb{Q}$
   (c) $2x^2 - 6$, $K = \mathbb{Q}$
   (d) $x^4 + 2$, $K = \mathbb{Q}$
   (e) $x^2 - 2\sqrt{3}x + 1$, $K = \mathbb{Q}[\sqrt{3}]$
   (f) $x^5 - 4x^4 + 12x^2 - 4x - 8$, $\mathbb{K} = \mathbb{Q}$

Soluzione 2.3. *(a) Osserviamo che su $\mathbb{Q}$ x^2-2 è irriducibile. Quindi $K = \mathbb{Q}[x]/(x^2-2) = \mathbb{Q}[\sqrt{2}]$ è un campo. Notiamo che su K, si ha*

$$t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$$

Quindi K è il campo di spezzamento di $x^2 - 2$.

(b) Il campo di spezzamento di $x^4 + 5x^2 - 6$ è $\mathbb{Q}[i\sqrt{6}]$

(c) Il campo di spezzamento di $2x^2 - 6$ è $\mathbb{Q}[\sqrt{3}]$

(d) Il campo di spezzamento di $x^4 + 2$ è $\mathbb{Q}[i\sqrt{4}2$

(e) Il campo di spezzamento di $x^2 - 2\sqrt{3}x + 1$ è $\mathbb{Q}[\sqrt{3}, \sqrt{2}]$

(f) Il campo di spezzamento di $x^5 - 4x^4 + 12x^2 - 4x - 8$ è $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$

3 Numeri algebrici

1. Dimostrare che $\cos(1°) + i\sin(1°)$ è algebrico su $\mathbb{Q}$, dove $1° = \frac{2\pi}{360}$

   Soluzione 3.1. *Poniamo $z = \cos(1°)+i\sin(1°)$, per dimostrare che z è algebrico su $\mathbb{Q}$ basta trovare un polinomio* non nullo *$f(X)$ a coefficienti in $\mathbb{Q}$ tale che z è radice di $f(X) = 0$. Notiamo che, in notazione complessa*

   $$z = e^{\frac{2\pi i}{360}}$$

   Quindi

   $$\begin{aligned} z &= e^{\frac{2\pi i}{360}} \\ z^{360} &= \left(e^{\frac{2\pi i}{360}}\right)^{360} \\ z^{360} &= e^{2\pi i} = 1 \\ z^{360} - 1 &= 0. \end{aligned}$$

   Quindi z è radice di $f(X) = X^{360} - 1 = 0$, dunque è algebrico su $\mathbb{Q}$. Notiamo che $f(X)$ non è il polinomio minimo di z, infatti $f(X)$ è riducibile, essendo 1 radice di $f(X) = 0$.

2. In generale dimostrare che $\cos(m°) + i\sin(m°)$ è algebrico su $\mathbb{Q}$ per ogni intero m

   Soluzione 3.2. *Analogamente all'esercizio 1, si ha che, posto $z = \cos(m°) + i\sin(m°)$, z è radice di $X^{360} - 1 = 0$*

4 Campi Finiti

1. Sia F un campo con un numero finito q di elementi

(a) Dimostrare che esiste un numero primo p tale che

$$pa = \underbrace{a + \cdots + a}_{p-volte} = 0$$

per ogni $a \in F$.

(b) Dimostrare che $q = p^n$ per un certo intero n.

(c) Se $a \in F$, dimostrare che $a^q = a$.

(d) Se $b \in K$ è algebrico su F, dimostrare che $b^{q^m} = b$ per qualche intero $m > 0$.

Soluzione 4.1. *(a) Basta vedere che esiste un numero primo p tale che:*

$$\underbrace{1 + \cdots + 1}_{p-volte} = 0$$

Poiché F ha un numero finito di elementi, esiste sicuramente un intero positivo m tale che

$$\underbrace{1 + \cdots + 1}_{m-volte} = 0$$

Sia, p il più piccolo intero positivo che ha la proprietà precedente, poniamo

$$C = \{i \cdot 1 : i \in \mathbb{Z}\}$$

Allora $C \cong \mathbb{Z}_p$, ma C è un campo quindi p è un numero primo.Ricordiamo che p si chiama la caratteristica di F e che C è il sottocampo fondamentale di F.

(b) Osserviamo che F è uno spazio vettoriale di dimensione finita su $C = \mathbb{Z}_p$. Sia $n = \dim_C F = \deg F$. Consideriamo $v_1 \dots v_n$ una base di F su C. Quindi ogni elemento di F si scrive in modo unico *come $a_1v_1 + \cdots + a_nv_n$, con $a_i \in C \cong \mathbb{Z}_p$. Allora*

$$q = \#(F) = p^n$$

(c) Osserviamo che il gruppo delle unità di F ha ordine $q-1$, quindi per ogni $a \in F^*$ si ha

$$a^{q-1} = 1$$

Quindi per ogni $a \in F$ si ha, essendo $0^q = 0$

$$a^q = a$$

(d) *Se $b \in K$ è algebrico su F, allora esiste un polinomio $f(X)$ a coefficienti in F non nullo irriducibile di grado m tale che $f(b) = 0$. consideriamo l'estensione $\widetilde{K}$ di F grado m data $f(X)$ allora, a meno di isomorfismo, $b \in \widetilde{K} \subset K$ e $\widetilde{K}$ è un campo finito con q^m elementi. Quindi per quanto detto in precedenza si ha*

$$b^{q^m} = b.$$

2. Sia F un campo con p^n elementi, provare che esiste un polinomio q in $\mathbb{Z}_p[x]$ tale che $F \cong \mathbb{Z}_p[x] / (q)$.

Soluzione 4.2. *Ricordiamo che il sottocampo fondamentale di F è $\mathbb{Z}_p$. Osserviamo che il gruppo delle unità di F ha ordine $p^n - 1$. Quindi per ogni $\alpha \in F^*$ si ha*

$$\alpha^{p^n-1} = 1$$

Quindi ogni elemento di F verifica l'equazione

$$q(X) = X^{p^n} - X = 0$$

$q(X) \in \mathbb{Z}_p[X]$. Osserviamo che $q(X)$ ha p^n radici in F, quindi F è il campo di spezzamento di $q(X)$. Poiché il campo di spezzamento di $q(X)$,a meno di isomorfismo, è $\mathbb{Z}_p[X]/(q(X))$, si ha che $F \cong \mathbb{Z}_p[X]/(q(X))$.

3. Costruire un campo, se possibile, con le seguenti cardinalità: 3, 6, 16, 27, 32, 144, 256, 3125.

Soluzione 4.3. *Sappiamo che i campi finiti possono aver cardinalità solo potenze di un numero primo, per cui le cardinalità possibili sono* 3, $27 = 3^3$,$32 = 2^5$, $32 = 2^8$ *e* $3125 = 5^5$

5 Irriducibilità

1. Trovare le componenti irriducibili di $f(x)$ in $K[x]$, con $K = \mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$

   (a) $f(x) = x^4 - 4x^3 + 2x^2 + 8x - 8$

   (b) $f(x) = x^4 + 2x^3 - x^2 + 2x + 1$

   (c) $f(x) = 2x^3 + 6x^2 + 6x + 2$

   (d) $f(x) = x^9 + 3x^6 + 3x^3 + 1$

Soluzione 5.1. *Sia $K = \mathbb{Z}$ allora*

(a) $f(x) = x^4 - 4x^3 + 2x^2 + 8x - 8 = (x - 2)^2(x^2 - 2)$

(b) $f(x) = x^4 + 2x^3 - x^2 + 2x + 1 = (1 - x + x^2)(1 + 3x + x^2)$

(c) $f(x) = 2x^3 + 6x^2 + 6x + 2 = 2(1 + x)^3$

(d) $f(x) = x^9 + 3x^6 + 3x^3 + 1 = (1 + x)^3(1 - x + x^2)^3$

Sia $K = \mathbb{Q}$ *allora*

(a) $f(x) = x^4 - 4x^3 + 2x^2 + 8x - 8 = (x - 2)^2(x^2 - 2)$

(b) $f(x) = x^4 + 2x^3 - x^2 + 2x + 1 = (1 - x + x^2)(1 + 3x + x^2)$

(c) $f(x) = 2x^3 + 6x^2 + 6x + 2 = 2(1 + x)^3$

(d) $f(x) = x^9 + 3x^6 + 3x^3 + 1 = (1 + x)^3(1 - x + x^2)^3$

Sia $K = \mathbb{R}$ *allora*

(a) $f(x) = x^4 - 4x^3 + 2x^2 + 8x - 8 == (x - 2)^2(x - \sqrt{2})(x + \sqrt{2})$

(b) $f(x) = x^4 + 2x^3 - x^2 + 2x + 1 = (1 - x + x^2)(x - \frac{-3-\sqrt{5}}{2})(x - \frac{-3+\sqrt{5}}{2})$

(c) $f(x) = 2x^3 + 6x^2 + 6x + 2 = 2(1 + x)^3$

(d) $f(x) = x^9 + 3x^6 + 3x^3 + 1 = (1 + x)^3(1 - x + x^2)^3$