(b) (*Schema di dimostrazione*) Per dimostrare che K non è un campo di funzioni razionali, ricorriamo alle proprietà geometriche della sua superficie di Riemann. Abbiamo visto (§ 7) che questa superficie è un toro privato di un punto. D'altra parte, la superficie di Riemann del campo delle funzioni razionali $\mathsf{C}(t)$ è il piano complesso stesso. Ora, esiste un teorema di topologia, il quale afferma che il toro e il piano non sono omeomorfi e che non possono essere resi tali eliminando insiemi finiti di punti. Se ammettiamo questo teorema, la proposizione seguente completerà la dimostrazione.

(8.8) PROPOSIZIONE *Siano* $K = \mathsf{C}(x)[y]/(f)$ *e* $L = \mathsf{C}(t)[u]/(g)$ *campi di funzioni con superfici di Riemann* S *e* T *rispettivamente. Un omomorfismo* $\varphi : L \to K$, *che sia l'identità sul sottocampo* C, *induce tra le loro superfici di Riemann un'applicazione* $\varphi^* : S' \to T$ *definita e continua tranne che su un insieme finito di punti di* S. *Se* φ *è un isomorfismo,* φ^* *diventa un omeomorfismo eliminando da* S *e* T *insiemi finiti opportuni.*

Si noti che l'applicazione φ^* va dalla superficie di Riemann di K a quella di L, nella direzione opposta a φ.

Dimostrazione. La superficie di Riemann T è il luogo $g(t,u) = 0$ in C^2. In base alla proposizione (7.11), ogni elemento $\alpha \in K$ definisce una funzione continua su S', sicché la coppia di funzioni $(\varphi(t), \varphi(u))$ definisce un'applicazione continua $S' \to \mathsf{C}^2$. Poiché $g(t,u) = 0$ in L e poiché φ è un omomorfismo che lascia fissi i coefficienti di g, si ha anche $g(\varphi(t), \varphi(u)) = 0$. Dunque S' viene mandata in T, e questa è l'applicazione φ^* richiesta. Se φ è un isomorfismo, il suo inverso φ^{-1} definisce un'applicazione $T' \to S$, che è una funzione inversa di φ^* sul complementare di un insieme finito. ∎

9 Campi algebricamente chiusi

Un campo F si dice *algebricamente chiuso* se ogni polinomio $f(x) \in F[x]$ di grado positivo ha una radice in F. Il fatto che il campo C dei numeri complessi è algebricamente chiuso è noto come teorema fondamentale dell'algebra.

(9.1) TEOREMA FONDAMENTALE DELL'ALGEBRA *Ogni polinomio non costante a coefficienti complessi ha una radice complessa.*

Abbiamo già usato spesso questo teorema. Una dimostrazione si trova alla fine del paragrafo (p. 621).

Se un campo F è algebricamente chiuso, ogni polinomio non costante $f(x) \in F[x]$ ha un fattore lineare $x - \alpha$, sicché gli unici polinomi irriducibili sono i polinomi di grado 1. Ne segue che ogni polinomio è un prodotto di fattori

lineari. Inoltre, non esistono estensioni algebriche di F diverse da F stesso (da cui l'espressione "algebricamente chiuso"). Infatti ogni elemento algebrico su F è una radice di un polinomio irriducibile monico $f(x) \in F[x]$. Tale polinomio deve essere della forma $x - \alpha$, sicché $\alpha \in F$.

Può essere conveniente considerare il campo F che si sta studiando come un sottocampo di un campo algebricamente chiuso. Per esempio, conviene considerare i campi di numeri come sottocampi di C. Si dice che un'estensione K di F è una *chiusura algebrica di* F se soddisfa alle seguenti condizioni:

(9.2) (a) *K è algebrico su F,*

(b) *K è un campo algebricamente chiuso.*

(9.3) COROLLARIO *Sia F un sottocampo di* C. *Allora il sottoinsieme $\overline{F}$ di* C *costituito da tutti i numeri che sono algebrici su F è una chiusura algebrica di F.*

Dimostrazione. È già stato dimostrato (3.10) che $\overline{F}$ è un campo. Facciamo vedere che $\overline{F}$ è algebricamente chiuso. Sia $f(x) \in \overline{F}[x]$ un polinomio non costante. Allora $f(x)$ ha una radice α in C, e $\overline{F}(\alpha)$ è algebrico su $\overline{F}$. Poiché $\overline{F}$ è algebrico su F, α è algebrico su F, in base a (3.11). Pertanto $\alpha \in \overline{F}$. ∎

Non è difficile costruire una chiusura algebrica di un campo finito F_p come un'unione dei campi F_q, dove $q = p^r$ è una potenza di p. Per fare ciò, scegliamo una successione di interi $r_1, r_2, \ldots$ con le seguenti proprietà: (i) r_i divide r_{i+1}, e (ii) ogni intero n divide qualche r_i. Possiamo prendere $r_i = i!$, per esempio. Poniamo $q_i = p^{r_i}$ e $F_i = \mathsf{F}_{q_i}$. Ora, da (i) segue che F_{i+1} contiene un sottocampo isomorfo a F_i (6.4), sicché possiamo costruire una catena di campi $F_1 \subset F_2 \subset \cdots$. Sia $\overline{F}$ l'unione insiemistica di questa catena di campi. Allora, (ii) ci dice che ogni campo finito F_q, con $q = p^r$, è isomorfo a un sottocampo di qualche campo F_i, e quindi ad un sottocampo $\overline{F}$, che è una chiusura algebrica di F_p.

Il teorema seguente può essere dimostrato usando il lemma di Zorn.

(9.4) TEOREMA *Ogni campo F ha una chiusura algebrica, e se K_1, K_2 sono due chiusure algebriche di F, esiste un isomorfismo $\varphi : K_1 \to K_2$, che è l'identità sul sottocampo F.* ∎

Dunque la chiusura algebrica di un campo è essenzialmente unica.

(9.5) COROLLARIO *Sia $\overline{F}$ una chiusura algebrica di F e sia K un'estensione algebrica arbitraria di F. Allora esiste una sottoestensione $K' \subset \overline{F}$ isomorfa a K.* ∎

Dimostrazione del teorema fondamentale dell'algebra. Per dimostrare che $f(x_0) = 0$, basta dimostrare che il valore assoluto $|f(x_0)|$ è zero. L'esistenza di un tale $x_0 \in \mathbf{C}$ è dimostrata dai due lemmi seguenti:

(9.6) LEMMA *Sia $f(x)$ un polinomio non costante e sia $x_0 \in \mathbf{C}$ un punto in cui $f(x_0) \neq 0$. Allora $|f(x_0)|$ non è il minimo di $|f(x)|$.*

(9.7) LEMMA. *Sia $f(x)$ un polinomio a coefficienti complessi. Allora $|f(x)|$ ha un minimo in qualche punto $x_0 \in \mathbf{C}$.*

Dimostrazione del lemma (9.6). Osserviamo innanzitutto che il polinomio $x^k - c$ ha una radice, per ogni $c \in \mathbf{C}$. Un numero reale non negativo r ha una radice k-esima reale, poiché la funzione continua x^k, la quale vale zero per $x = 0$ e tende a $+\infty$ per x che tende a $+\infty$, assume tutti i valori reali ≥ 0, in virtù del teorema del valor medio. Scriviamo il numero complesso c nella forma $c = re^{i\theta}$, dove $r = |c|$ e $\theta = \arg c$. Sia s una radice k-esima reale di r. Allora la radice k-esima richiesta di c è

$$\alpha = se^{i\theta/k}. \tag{9.8}$$

Sia ora $f(x)$ un polinomio non costante e sia $x_0 \in \mathbf{C}$ un punto in cui $f(x_0) \neq 0$. È conveniente normalizzare f. Effettuiamo un cambiamento di variabile, sostituendo x con $x + x_0$, per spostare il punto in questione nell'origine, sicché $x_0 = 0$. Inoltre moltiplichiamo $f(x)$ per $f(0)^{-1}$. Allora $f(0) = 1$, e dobbiamo dimostrare che 1 non è il valore minimo di $|f(x)|$.

Denotiamo con k il minimo esponente non nullo di x che compare in f, sicché

$$f(x) = 1 + ax^k + (\text{termini di grado} > k).$$

Sia α una radice k-esima di $-a^{-1}$. Effettuiamo un ulteriore cambiamento di variabile, sostituendo x con αx. Allora f assume la forma seguente:

$$f(x) = 1 - x^k + (\text{termini di grado più alto}) = 1 - x^k + x^{k+1}g(x),$$

per qualche polinomio $g(x)$. Se x è un numero reale positivo piccolo, per la disuguaglianza triangolare si ha:

$$|f(x)| \leq |1 - x^k| + |x^{k+1}g(x)| = 1 - x^k + x^{k+1}|g(x)| = 1 - x^k(1 - x|g(x)|).$$

Poiché $x|g(x)|$ è piccolo per piccoli valori di x, il termine $x^k(1 - x|g(x)|)$ è positivo se x è un numero reale positivo sufficientemente piccolo. Per un tale x si ha: $|f(x)| < |f(0)|$. ∎

Dimostrazione del lemma (9.7). Possiamo supporre che il polinomio f non sia una costante. Per valori grandi di x, anche $f(x)$ assume valori grandi; si ha cioè

$$|f(x)| \to \infty \text{ per } |x| \to \infty. \tag{9.9}$$

Per dimostrare ciò, il termine noto di f è irrilevante, sicché possiamo supporre che esso sia nullo. Allora $f(x)$ è divisibile per x, ossia: $f(x) = xg(x)$. Procedendo per induzione sul grado, l'asserzione è vera per $g(x)$, oppure $g(x)$ è costante, e di conseguenza essa risulta vera anche per $f(x)$.

Ora, poiché $f(x)$ assume valori grandi per valori grandi di x, l'estremo inferiore m di $|f(x)|$ nell'intero piano complesso è anche l'estremo inferiore in un disco sufficientemente grande $|x| \leq r$. Poiché il disco è compatto e $|f(x)|$ è una funzione continua, essa ha un minimo nel disco. ∎

Oltre a quella appena sviluppata, vi sono varie altre dimostrazioni del teorema fondamentale dell'algebra. Una è particolarmente interessante, sebbene non sia così facile renderla precisa come quella appena vista. A grandi linee, la dimostrazione è la seguente. Come prima, dobbiamo dimostrare che un polinomio non costante

$$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 \tag{9.10}$$

ha una radice. Se $a_0 = 0$, allora 0 è una radice, sicché possiamo supporre che $a_0 \neq 0$. Consideriamo la funzione $f : \mathbf{C} \to \mathbf{C}$ definita dal polinomio (9.10).

Denotiamo con C_r una circonferenza di raggio r col centro nell'origine. Studiamo le immagini $f(C_r)$ delle circonferenze C_r. In coordinate polari, scriviamo $z = re^{i\theta}$. Allora $z^n = r^n e^{in\theta}$. Mentre θ varia da 0 a 2π, il punto z percorre un giro lungo la circonferenza di raggio r. Nello stesso tempo, $n\theta$ varia da 0 a $2\pi n$, sicché il punto z^n percorre n giri lungo la circonferenza di raggio r^n.

Per valori sufficientemente grandi di r, il termine z^n è dominante nell'espressione (9.10), e otterremo

$$|f(z) - z^n| \leq \frac{1}{2} r^n.$$

La dimostrazione di questo fatto è simile alla dimostrazione del lemma (9.6). Per i nostri scopi, il fattore $\frac{1}{2}$ potrebbe essere sostituito da un qualunque numero reale positivo minore di 1. La precedente disuguaglianza mostra che, mentre z^n percorre n volte la circonferenza di raggio r^n, anche $f(z)$ percorre n giri intorno all'origine. Un buon modo per visualizzare questo fatto è dato dal modello del "cane al guinzaglio". Se si porta a spasso un cane girando n volte intorno a un isolato, anche il cane gira n volte, sia pure seguendo un percorso diverso. Ciò sarà vero purché il guinzaglio sia più corto del raggio dell'isolato. Qui z^n rappresenta la posizione della persona al tempo θ, e $f(z)$ rappresenta la posizione del cane. La lunghezza del guinzaglio è $\frac{1}{2} r^n$.

Facciamo variare ora il raggio r. Poiché f è una funzione continua, l'immagine $f(C_r)$ varierà con r in modo continuo. Quando r è molto piccolo, $f(C_r)$ descrive un piccolo cappio intorno al termine noto a_0 di f. Questo piccolo cappio non si