I polinomi di un campo: $\mathbb{K}[x]$

§1.1 Elementi preliminari

Prima di procedere ad enunciare le proprietà più rilevanti dell'anello dei polinomi $\mathbb{K}[x]$, si ricorda che esso è un **anello euclideo** in cui la funzione grado coincide con il grado del polinomio, ossia $g = \deg$. Si enuncia ora invece la definizione di radice.

Definizione 1.1.1. Si dice che $\alpha \in \mathbb{K}$ è una **radice** del polinomio $f(x) \in \mathbb{K}[x]$ se $f(\alpha) = 0$.

Proposizione 1.1.2

Se $\alpha \in \mathbb{K}$ è una radice di $f(x) \in \mathbb{K}[x]$, allora $(x - \alpha)$ divide $f(x)$.

Dimostrazione. Dal momento che $\mathbb{K}[x]$ è un anello euclideo, si può eseguire la divisione euclidea tra $f(x)$ e $(x-\alpha)$, ossia esistono $q(x), r(x) \in \mathbb{K}[x]$ tali che $f(x) = q(x)(x-\alpha)+r(x)$ con $\deg r(x) < \deg(x - \alpha)$ o con $r(x) = 0$.

Se $r(x) \neq 0$, poiché $\deg r(x) < \deg(x - \alpha)$, si deduce che $\deg r(x) = 0$, ossia che $r(x)$ è un invertibile. In entrambi i casi, $r(x)$ è comunque una costante. Pertanto, valutando il polinomio in α, si ricava:

$$0 = f(\alpha) = \underbrace{q(\alpha)(\alpha - \alpha)}_{=0} + r(\alpha),$$

da cui $r(\alpha) = 0$. Quindi $f(x) = q(x)(x - \alpha)$, e si verifica la tesi. □

Teorema 1.1.3

Sia $f(x) \in \mathbb{K}[x]$ di grado n. Allora $f(x)$ ha al più n radici.

Dimostrazione. Se n è nullo, allora $f(x)$ è una costante non nulla, e quindi non ammette radici, in accordo alla tesi.

Sia allora $n \geq 1$. Se $f(x)$ non ha radici in $\mathbb{K}$, allora la tesi è ancora soddisfatta. Altrimenti sia ζ_1 una radice di $f(x)$. Si divida $f(x)$ per $(x - \zeta_1)$ e se ne prende il quoziente $q_1(x)$, mentre si ignori il resto, che, per la *Proposizione 1.1.2*, è nullo.

Si reiteri il procedimento utilizzando $q_1(x)$ al posto di $f(x)$ fino a quando il grado del quoziente non è nullo o il quoziente non ammette radici in $\mathbb{K}$, e si chiami quest'ultimo quoziente $\lambda(x)$. Infatti, poiché i gradi dei quozienti diminuiscono di 1 ad ogni iterazione, è garantito che l'algoritmo termini al più dopo n iterazioni.

In questo modo, numerando le radici, si può scrivere $f(x)$ come:

$$f(x) = \alpha(x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_k)\lambda(x). \tag{1.1}$$

Si osserva che $x-\zeta_i$ è irriducibile $\forall\, 1 \leq i \leq k$. Se $f(x)$ ammettesse un'altra fattorizzazione in cui compaia un fattore $x-\alpha$ con $\alpha \neq \zeta_i\ \forall\, 1 \leq i \leq k$, allora $f(x)$ ammetterebbe due fattorizzazioni in irriducibili, dacché $x-\alpha$ non sarebbe un associato di nessuno dei $x-\zeta_i$, né tantomeno di un irriducibile $\lambda(x)$.

Se infatti $x-\alpha$ fosse un associato di un irriducibile $\lambda(x)$, $x-\alpha$ dividerebbe $\lambda(x)$, e quindi $\lambda(x)$ ammetterebbe α come radice. Se $\lambda(x)$ è una costante, questo è a priori assurdo, $\lightning$. Se invece $\lambda(x)$ non è una costante, il fatto che ammetta una radice contraddirebbe il funzionamento dell'algoritmo di fattorizzazione espresso in precedenza, $\lightning$. Quindi $x-\alpha$ non è associato di nessun irriducibile di $\lambda(x)$.

Allora il fatto che $f(x)$ ammetta due fattorizzazioni in irriducibili è assurdo, dacché $\mathbb{K}[x]$ è un anello euclideo, e quindi un UFD, $\lightning$. Quindi le radici sono esattamente $k \leq n$, da cui la tesi. □

§1.2 Sottogruppi moltiplicativi finiti di $\mathbb{K}$

Si illustra adesso un teorema che riguarda i sottogruppi moltiplicativi finiti di $\mathbb{K}$, da cui conseguirà, per esempio, che $\mathbb{Z}_p^*$ è sempre ciclico, per qualsiasi p primo.

Lemma 1.2.1

Per ogni $n \in \mathbb{N}$ vale la seguente identità:

$$n = \sum_{d|n} \varphi(d).$$

Dimostrazione. Si consideri il gruppo ciclico $\mathbb{Z}_n$ per $n \in \mathbb{N}$. Si osserva che $|\mathbb{Z}_n| = n$.

Si definisca X_d come l'insieme degli elementi di G di ordine d. Dal momento che ogni elemento appartiene a uno e uno solo di questi X_d, per ogni divisore d di n, allora si può partizionare G nel seguente modo:

$$G = \bigcup_{d|n} X_d.$$

Dal momento che $\mathbb{Z}_n$ è ciclico, ogni X_d ha esattamente $\varphi(d)$ elementi, e dunque si deduce che:

$$n = |G| = \sum_{d|n} |X_d| = \sum_{d|n} \varphi(d),$$

ossia la tesi. □

Teorema 1.2.2

Un sottogruppo moltiplicativo finito di un campo $\mathbb{K}$ è sempre ciclico.

Dimostrazione. Sia G un sottogruppo finito di un campo $\mathbb{K}$ definito sulla sua operazione di moltiplicazione, e sia $|G| = n$.

Si definisca X_d come l'insieme degli elementi di G di ordine d. Dal momento che ogni elemento appartiene a uno e uno solo di questi X_d, per ogni divisore d di n, allora si può partizionare G nel seguente modo:

$$G = \bigcup_{d|n} X_d,$$

da cui:

$$n = |G| = \sum_{d|n} |X_d| \,. \tag{1.2}$$

Dal *Lemma 1.2.1* e da (1.2), si ricava infine la seguente equazione:

$$\sum_{d|n} |X_d| = n = \sum_{d|n} \varphi(d). \tag{1.3}$$

Adesso vi sono due casi: o $|X_n| > 0$ o $|X_n| = 0$.

Nel primo caso si concluderebbe che esiste almeno un elemento in G di ordine n, e quindi che esiste un generatore con cui G è ciclico, ossia la tesi.

Nel secondo caso si dimostra un assurdo. Dal momento che $|X_n| = 0$, esiste sicuramente un divisore proprio d di n tale che $|X_d| > \varphi(d)$. Altrimenti, se $|X_d| \leq \varphi(d)$ per ogni divisore d, si ricaverebbe la seguente disuguaglianza:

$$\sum_{\substack{d|n\\ d\neq n}} |X_d| \leq \sum_{\substack{d|n\\ d\neq n}} \varphi(d) \implies \sum_{d|n} |X_d| \overbrace{=}^{|X_n|=0} \sum_{\substack{d|n\\ d\neq n}} |X_d| \leq \sum_{\substack{d|n\\ d\neq n}} \varphi(d) \overbrace{<}^{\varphi(n)\geq 1} \sum_{d|n} \varphi(d).$$

Tuttavia questo è un assurdo, dal momento che per (1.3) deve valere l'uguaglianza, ↯.

Sia $g \in X_d$ e si consideri (g), il sottogruppo generato da g. Vale in particolare che $|(g)| = d$.

Si consideri adesso il polinomio $f(x) = x^d - 1 \in \mathbb{K}[x]$. Tutti e d gli elementi di (g) sono già soluzione di $f(x)$. Tuttavia, poiché $|X_d| > \varphi(d)$, esiste sicuramente un elemento h in X_d che non appartiene a (g). Infatti se tutti gli elementi di X_d appartenessero a (g) vi sarebbero più di $\varphi(d)$ generatori, ↯.

Infine, poiché $h \in X_d$, anch'esso è soluzione di $f(x)$. Questo è però un assurdo, poiché, per il *Teorema 1.1.3*, $f(x)$ ammette al più d radici, mentre così ne avrebbe almeno $d+1$, ↯.

Quindi $|X_d| > 0$, e G è ciclico. □

§1.3 Il quoziente $\mathbb{K}[x]/(f(x))$

Nell'ambito dello studio delle radici di un polinomio, il quoziente $\mathbb{K}[x]/(f(x))$ gioca un ruolo fondamentale. Infatti, come vedremo in seguito, se $f(x)$ è irriducibile, questo diventa un campo, e, soprattutto, ammette sempre una radice per $f(x)$.

In realtà, il quoziente $\mathbb{K}[x]/(f(x))$ si comporta pressocché allo stesso modo dei più familiari $\mathbb{Z}/n\mathbb{Z}$. Infatti le principali regole dell'aritmetica modulare potrebbero essere estese anche a tale quoziente, senza particolari sacrifici.

Si enuncia adesso un teorema importante, che è equivalente – anche nella dimostrazione – all'analogo per i campi $\mathbb{Z}/p\mathbb{Z}$.

Teorema 1.3.1
$\mathbb{K}[x]/(f(x))$ è un campo se e solo se $f(x)$ è irriducibile.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

$(\implies)$ Sia $f(x) \in \mathbb{K}[x]$ irriducibile. Affinché l'anello commutativo $\mathbb{K}[x]/(f(x))$ sia un campo è sufficiente dimostrare che ogni suo elemento non nullo ammette un inverso

moltiplicativo.

Sia $\alpha(x)+(f(x)) \in \mathbb{K}[x]/(f(x))$ non nullo. Allora $\alpha(x)$ non è divisibile da $f(x)$, e pertanto $\text{MCD}(\alpha(x), f(x)) = 1$[1].

Allora, per l'*Identità di Bézout*, esistono $\beta(x)$, $\lambda(x) \in \mathbb{K}[x]$ tali che:

$$\alpha(x)\beta(x) + \lambda(x)f(x) = 1.$$

Dacché $\alpha(x)\beta(x) - 1 \in (f(x))$, si deduce che $\alpha(x)\beta(x) + (f(x)) = 1 + (f(x))$, e quindi $\beta(x) + (f(x))$ è l'inverso moltiplicativo di $\alpha(x) + (f(x))$, da cui la dimostrazione dell'implicazione.

$(\Longleftarrow)$ Si dimostra l'implicazione contronominalmente. Sia $f(x) \in \mathbb{K}[x]$ riducibile. Allora esistono $\alpha(x)$ e $\beta(x)$ non invertibili tali che $f(x) = \alpha(x)\beta(x)$, da cui si ricava che:

$$[\alpha(x) + (f(x))][\beta(x) + (f(x))] = f(x) + (f(x)) = 0 + (f(x)),$$

ossia l'identità di $\mathbb{K}[x]/(f(x))$.

Tuttavia, se $\mathbb{K}[x]/(f(x))$ fosse un campo, e quindi un dominio, ciò non sarebbe ammissibile, dacché non potrebbero esservi divisori di zero. Quindi $\mathbb{K}[x]/(f(x))$ non è un campo. □

Osservazione. Una notazione per indicare un elemento di $\mathbb{K}[x]/(f(x))$ alternativa e più sintetica di $a + (f(x))$ è $\overline{a}$, qualora sia noto nel contesto a quale $f(x)$ si fa riferimento.

Proposizione 1.3.2

Nell'anello $\mathbb{K}[x]/(f(x))$ esiste sempre una radice di $f(x)$, convertendo opportunamente i coefficienti da $\mathbb{K}$ a $\mathbb{K}[x]/(f(x))$.

Dimostrazione. Sia $\overline{x} = x + (f(x)) \in \mathbb{K}[x]/(f(x))$ e si descriva $f(x)$ come:

$$f(x) = a_n x^n + \ldots + a_0.$$

Allora, computando $f(x)$ in $\overline{x}$ e convertendone i coefficienti, si ricava che:

$$f(\overline{x}) = \overline{a_n}\,\overline{x}^n + \ldots + \overline{a_0} = \overline{a_n x^n} + \ldots + \overline{a_0} = \overline{f(x)} = \overline{0}.$$

[1] Si ricorda che in un PID la nozione di *massimo comun divisore* (MCD) è più ambigua di quella di $\mathbb{Z}$. Infatti $\text{MCD}(a, b)$ comprende tutti i generatori dell'ideale (a, b), e quindi tutti i suoi associati. Pertanto si dirà $\text{MCD}(a, b)$ uno qualsiasi di questi associati, e nel nostro caso 1 è un buon valore, dacché l'MCD deve essere un associato di un'unità.

Quindi $\overline{x}$ è una radice di $f(x)$, da cui la tesi.

□