# Richiami e approfondimenti di Algebra per il Corso ALGEBRA COMPUTAZIONALE

Università degli Studi di Verona

– Corso di Laurea in Matematica Applicata –

* * *

Prof. Lidia Angeleri

Anno accademico 2008-2009

# Indice

# 1 Gruppi e sottogruppi

## 1.1 Gruppo

Un *gruppo* $(G,+)$ è costituito da un insieme non vuoto $G$ e un'operazione $+ : G \times G \to G$, $(a,b) \mapsto ab$ su $G$ che gode delle seguenti proprietà:
**(G1)** associatività: $a+(b+c)=(a+b)+c$ per $a,b,c \in G$;
**(G2)** elemento neutro: $a+0_G = 0_G + a = a$ per ogni $a \in G$;
**(G3)** elemento inverso: per ogni $a \in G$ esiste $b \in G$ tale che $a+b=b+a=0_G$;
Il gruppo $(G,+)$ si dice *abeliano* se vale anche la proprietá:
**(G4)** commutativa: $a+b=b+a$ per $a,b \in G$.

## 1.2 Sottogruppo

Sia $(G,+)$ un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice *sottogruppo* di $G$ se $H$ è un gruppo rispetto all'operazione $+$ di $G$. In tal caso si scrive $H \leq G$.

*OSSERVAZIONE*
Un sottoinsieme $H \subset G$ è un sottogruppo se e solo se $H \neq \emptyset$ e per tutti gli $a,b \in H$ si ha $a-b \in H$.

## 1.3 Laterale di $G$ modulo $H$.

Ogni sottogruppo $H$ di gruppo $(G,+)$ definisce una *relazione di equivalenza* su $G$

$$a \sim b \quad \text{se} \quad a-b \in H$$

La classe di equivalenza di un elemento $a$ rispetto a $\sim$ è

$$[a] = \{x \in G \mid x \sim a\} = \{h+a \mid h \in H\} = H+a$$

$[a]$ si chiama *laterale destro* di $G$ modulo $H$ con rappresentante $a$.

## 1.4 Esempi.

$(\mathbb{Z},+)$ è un gruppo abeliano. I suoi sottogruppi sono i sottoinsiemi di forma $n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$ con $n \in \mathbb{N}_0$. I laterali (destri e sinistri) di $\mathbb{Z}$ modulo $n\mathbb{Z}$ sono esattamente le classi di resto $[0],[1],[2],...,[n-1]$ di $\mathbb{Z}$ modulo $n$ e formano il gruppo $(\mathbb{Z}/n\mathbb{Z},+)$ rispetto all'addizione

$$[a]+[b]=[a+b]$$

## 1.5 Teorema di Lagrange

Sia $(G,+)$ un gruppo finito e sia $H \leq G$. Allora l'ordine $\mid H \mid$ divide l'ordine $\mid G \mid$.
Più precisamente si ha

$$\mid G \mid = \mid H \mid \cdot [G:H]$$

dove $[G:H]$ è *l'indice* di $H$ in $G$, ovvero il numero dei laterali destri di $G$ modulo $H$.

# 2 Gruppi ciclici

## 2.1 Il sottogruppo generato da un elemento

Sia $(G, \cdot)$ un gruppo con elemento neutro $e$.
Per $a \in G$ e un intero $n \in \mathbb{Z}$ si pone

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot ... \cdot a}_{n} & \text{se } n > 0 \\ e & \text{se } n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}}_{n} & \text{se } n < 0 \end{cases}$$

Definiamo $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. L'insieme $\langle a \rangle$ è un sottogruppo di $G$. Il suo ordine si indica con $ord(a) =\mid \langle a \rangle \mid$ e si chiama *ordine dell'elemento* $a$.

## 2.2 L'ordine di un elemento

Sia $(G, \cdot)$ un gruppo e sia $a \in G$.
**(1)** Se $a^l \neq a^k$ per $l \neq k$ allora $ord(a) = \infty$.
**(2)** Se esistono $l \neq k$ tali che $a^l = a^k$ allora $ord(a) = m < \infty$, dove $m$ è il minimo intero positivo tale che $a^m = e$.

*COROLLARIO*
Se $\mid G \mid = n$, allora $ord(a)$ divide $n$ e quindi $a^n = e$.

**Esempio.** L'ordine di un elemento $[a] \in (\mathbb{Z}/n\mathbb{Z}, +)$ si calcola come $\frac{n}{\text{MCD}(a,n)}$. Dunque se $[a]$ é un elemento con $\text{MCD}(a, n) = 1$, si ha $< [a] >= \mathbb{Z}/n\mathbb{Z}$.

## 2.3 Gruppo ciclico

Un gruppo $(G, \cdot)$ è detto *ciclico* se esiste un elemento $a \in G$ tale che $G = \langle a \rangle$.

## 2.4 Omomorfismo, isomorfismo

Siano $(G, \cdot)$ e $(G', *)$ due gruppi. Un'applicazione $f : G \to G'$ si dice:
- *omomorfismo* se $f(a \cdot b) = f(a) * f(b)$ per $a, b \in G$;
- *isomorfismo* se $f$ è un omomorfismo biiettivo.
Se esiste un isomorfismo $f : G \to G'$ si dice che $G$ e $G'$ sono *isomorfi* e si scrive $G \cong G'$.

## 2.5 Classificazione dei gruppi ciclici

Sia $(G, \cdot)$ un gruppo ciclico.
**(1)** Se $\mid G \mid = \infty$, allora $(G, \cdot) \cong (\mathbb{Z}, +)$.
**(2)** Se $\mid G \mid = m$ allora $(G, \cdot) \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

# 3 L'anello dei polinomi

## 3.1 Il concetto di anello

Un anello $(R, +, \cdot)$ è costituito da un insieme non vuoto $R$ e due operazioni $+, \cdot : R \times R \to R$ su $R$ che godono delle proprietà:
**(R1)** $(R, +)$ è un gruppo abeliano con elemento neutro $0_R$;
**(R2)** $(R, \cdot)$ gode della proprietà associativa e possiede un elemento neutro $1_R$;
**(R3)** Leggi distributive:
$a(b + c) = ab + ac$,
$(a + b)c = ac + bc$.
Un anello si dice *commutativo* se $(R, \cdot)$ gode della proprietà commutativa.

## 3.2 Elemento invertibile. Campo

Sia $(R, +, \cdot)$ un anello.
**(1)** Un elemento $a \in R$ è *invertibile* se esiste un elemento $b \in R$ tale che $ab = ba = 1_R$
In tal caso $b$ è univocamente determinato e si indica con $a^{-1}$.
**(2)** $(R, +, \cdot)$ si dice *campo* se $R$ è commutativo e ogni elemento $0 \neq a \in R$ è invertibile, in altre parole, se (R\{0}, $\cdot$) è un gruppo abeliano.

## 3.3 Esempio: $\mathbb{Z}/n\mathbb{Z}$.

Sia $n \in \mathbb{N}$. Come sopra, denotiamo con

$$n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$$

l'insieme di tutti gli interi che sono divisibili per $n$, ovvero i multipli di $n$. Consideriamo la relazione di equivalenza

$$a \sim b \quad \text{se} \quad a - b \in n\mathbb{Z}$$

Le classi di resto modulo $n$, ovvero le classi di equivalenza rispetto a $\sim$,

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \mathrm{mod} n\} = \{x \in \mathbb{Z} \mid x - a \in n\mathbb{Z}\}$$

con l'addizione

$$[a] + [b] = [a + b]$$

e la moltiplicazione

$$[a] \cdot [b] = [ab]$$

formano l'anello commutativo $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.
Una classe di resto $[a]$ è un elemento invertibile di $\mathbb{Z}/n\mathbb{Z}$ se e solo se $1 \leq a \leq n$ e $\mathrm{MCD}(a, n) = 1$.
Quindi $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se $n$ è un numero primo.

## 3.4 L'anello dei polinomi.

Dato un campo $K$, l'insieme $K[x]$ di tutti i polinomi nell'indeterminata $x$ con coefficienti in $K$ forma un anello rispetto alla somma e moltiplicazione di polinomi, detto *anello dei polinomi*. Dato un polinomio

$$f = \sum_{i=0}^{n} a_i x^i$$

con $n \in \mathbb{N}_0$ e coefficienti $a_0, a_1, \dots a_n \in K$, $a_n \neq 0$, diremo che $a_n$ è il *coefficiente direttivo* e $n = \deg f$ il *grado* di $f$. Il polinomio 0 per convenzione ha grado -1.

OSSERVAZIONI

1. $\deg(fg) = \deg f + \deg g$ per $f, g \in K[x] \setminus \{0\}$.
2. $f \in K[x]$ è invertibile se e solo se $\deg f = 0$.

## 3.5 Divisione col resto

**Proposizione** Sia $K$ un campo e siano $f, g \in K[x]$ due polinomi non nulli. Allora esistono $q, r \in K[x]$ tali che

$$f = qg + r \quad \text{e} \quad \deg(r) < \deg(g)$$

Diremo che il polinomio $g$ *divide* il polinomio $f$ se $r = 0$, ovvero se $f = gq$ per un $q \in K[x]$. Denotiamo con

$$(g) = \{gq \mid q \in K[x]\}$$

l'insieme di tutti i polinomi $f$ che sono divisibili per $g$, ovvero i multipli di $g$.

## 3.6 Polinomi irriducibili.

**Teorema:** Sia $K$ un campo e sia $f \in K[x]$ un polinomio. Sono equivalenti i seguenti enunciati:

1. $f$ non è invertibile e possiede soltanto divisori banali (ovvero: se $g, h \in K[x]$ sono polinomi tali che $gh = f$, allora $g$ oppure $h$ è invertibile).
2. $\deg f = n > 0$ e $f$ non può essere scritto come prodotto di due polinomi di grado $< n$.

In tal caso diremo che $f$ è un polinomio *irriducibile* di $K[x]$.

## 3.7 Fattorizzazione di polinomi.

**Teorema:** Sia $K$ un campo. Ogni polinomio $f \in K[x]$ di grado $n > 0$ può essere scritto come prodotto di polinomi irriducibili e questa scomposizione è unica a meno dell'ordine e di associazione. Più precisamente:

(i) Esistono polinomi irriducibili $p_1, \dots, p_n \in R$ tali che $f = p_1 \cdot \ldots \cdot p_n$.

(ii) Se anche $q_1, \dots, q_m \in R$ sono polinomi irriducibili tali che $f = q_1 \cdot \ldots \cdot q_m$, allora $m = n$ ed esistono una permutazione $\sigma \in S_n$ e polinomi invertibili $c_1, \dots, c_n$ tali che $p_i = c_i\, q_{\sigma(i)}$ per ogni $1 \leq i \leq n$.

## 3.8 Identità di Bézout.

Sia $K$ un campo e siano $f_1, \ldots, f_r \in K[x]$. Un elemento $d \in R$ è detto *massimo comun divisore* di $f_1, \ldots, f_r$ se soddisfa

1. $d \mid f_i$ per ogni $1 \leq i \leq r$,
2. se $t \mid f_i$ per ogni $1 \leq i \leq r$, allora $t \mid d$;

Scriveremo $d = MCD(f_1, \ldots, f_r)$. Se $d$ è un polinomio invertibile, diremo che $f_1, \ldots, f_r$ sono *coprimi*.

OSSERVAZIONI:

1. **L'Algoritmo Euclideo.** Possiamo calcolare il massimo comun divisore di $f, g \in K[x] \setminus \{0\}$ tramite divisioni successive come segue:

   Se $g \mid f$, allora $g = MCD(f, g)$. Altrimenti poniamo $r_0 = g$ e eseguiamo divisioni col resto:

   $$\begin{array}{llll} f = q_1\, r_0 + r_1 & \text{con} & q_1, r_1 \in R & \text{e} \quad \deg(r_1) < \deg(r_0) \\ r_0 = q_2\, r_1 + r_2 & \text{con} & q_2, r_2 \in R & \text{e} \quad \deg(r_2) < \deg(r_1) \\ \vdots & & \vdots & \vdots \\ r_{n-1} = q_{n+1}\, r_n + r_{n+1} & \text{con} & q_{n+1}, r_{n+1} \in R & \text{e} \quad r_{n+1} = 0. \end{array}$$

   Allora

   $$r_n = MCD(f, g).$$

2. **Identità di Bézout:** $f, g \in K[x] \setminus \{0\}$ sono coprimi se e solo se esistono polinomi $r, s \in K[x]$ tali che

   $$1 = rg + sf$$

## 3.9 Zeri di polinomi

Sia $K$ un campo, e sia $f \in K[x]$, $f = \sum_{i=0}^{n} a_i x^i$. Per $\alpha \in K$ poniamo

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i.$$

L'elemento $\alpha \in K$ è detto *zero* (oppure *radice*) di $f$ se $f(\alpha) = 0$.

**Teorema di Ruffini.** Sia $K$ un campo. Un elemento $\alpha \in K$ è uno zero di un polinomio $f \in K[x]$ se e solo se il polinomio $x - \alpha$ divide $f$.

**Corollario.** Un polinomio $f \in K[x]$ di grado $n$ su un campo $K$ possiede al più $n$ zeri distinti.

## 3.10 Polinomi irriducibili di grado $\leq 3$.

Sia $K$ un campo.
**(1)** Ogni polinomio $f = a_0 + a_1 x$ di grado 1 è irriducibile e ammette l'unico zero $\alpha = -a_1^{-1} a_0 \in K$.
**(2)** Se $f \in K[x]$ è un polinomio irriducibile di grado $\deg f > 1$ allora $f$ non ammette zeri.
**(3)** Un polinomio $f \in K[x]$ di grado $\deg f \in \{2, 3\}$ è irriducibile se e solo se non ammette zeri.

**Esempio.** $f = x^4 + x^2 + 1 \in \mathbb{F}_2[x]$ non ammette zeri, ma è riducibile poiché $f = (x^2 + x + 1)^2$.

# 4 Estensioni di campi

## 4.1 Sottocampi, estensioni.

Sia $(F, +, \cdot)$ un campo. Un sottoinsieme non vuoto $K \subset F$ si dice *sottocampo* se $K$ è un campo rispetto alle operazioni $+$ e $\cdot$ definite in $F$. In tal caso si dice anche che $F$ è un'*estensione* di $K$.

OSSERVAZIONE: Un sottoinsieme $K \subset F$ è un sottocampo se e solo se:

(i) $(K, +)$ è un sottogruppo del gruppo abeliano $(F, +)$,

(ii) $(K \setminus \{0\})$ è un sottogruppo del gruppo abeliano (F\{0}, $\cdot$).

In tal caso $F$ è anche uno spazio vettoriale su $K$. La dimensione di $F$ come spazio vettoriale su $K$ è detta *grado* dell'estensione e si indica con $[F : K] = \dim_K F$. Un'estensione si dice *finita* se $[F : K] < \infty$.

## 4.2 L'anello quoziente $K[x]/(f)$.

Sia $K$ un campo, e sia $f \in K[x]$ un polinomio di grado $n$. Consideriamo la seguente relazione di equivalenza su $K[x]$:

$$g \sim h \quad \text{se} \quad g - h \in (f).$$

Denotiamo con $\overline{g} = \{h \in K[x] \mid g \sim h\}$ la classe di equivalenza del polinomio $g \in K[x]$ rispetto a $\sim$, e con $K[x]/(f)$ l'insieme di tutte le classi di equivalenza.
Definiamo l'addizione

$$\overline{g} + \overline{h} = \overline{g + h}$$

e la moltiplicazione

$$\overline{g} \cdot \overline{h} = \overline{gh}$$

Rispetto a queste operazioni $K[x]/(f)$ è un anello.
Inoltre $F = K[x]/(f)$ è un campo se e solo se il polinomio $f$ è *irriducibile*. In tal caso, identificando gli elementi di $K$ con i polinomi di grado zero, possiamo interpretare $K \subset F$ come un'estensione di campi di grado $[F : K] = n$. Gli elementi

$$\overline{1}, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}$$

formano una base di $F$ su $K$. Se $K$ è un campo finito di $q$ elementi, allora $F$ è un campo finito di $q^n$ elementi.

## 4.3 Esempio: $\mathbb{F}_4$

Per $K = \mathbb{Z}/2\mathbb{Z}$, $f = x^2 + x + 1$, otteniamo un campo di quattro elementi $F = \{0, 1, \alpha, \alpha^2\}$ dove $\alpha = \overline{x}$. Si osservi: l'elemento $\alpha \in F$ è uno zero del polinomio $f \in F[x]$, e $F$ consiste degli zeri del polinomio $g = x^4 - x = (x - 1) \cdot f$.

## 4.4 Teorema di Kronecker

Sia $K$ un campo e sia $f \in K[x]$ di grado $n > 0$. Allora esiste un'estensione $K \subset F$ di grado $[F : K] \leq n$ nella quale $f$ possiede uno zero $\alpha \in F$.

### 4.5 Campi di riducibilità completa.

Sia $K$ un campo e sia $f \in K[x]$ un polinomio di grado $n > 0$. Allora esiste un'estensione $K \subset F$ di grado $[F : K] \leq n!$ tale che

1. $f = a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$ con $a \in K$, $\alpha_1, \alpha_2, ..., \alpha_n \in F$.
2. Se $K \subset F' \subset F$ è un campo intermedio contenente $\alpha_1, \ldots, \alpha_n$, allora $F' = F$.

$F$ è detto *campo di riducibilità completa* (o *di spezzamento*) di $f$ su $K$ ed è unico a meno di isomorfismo.

**Esempio.** Il campo $F$ in 4.3 è il campo di riducibilità completa del polinomio $f = x^4 - x$ su $K = \mathbb{Z}/2\mathbb{Z}$.

### 4.6 Definizione.

Siano $K$ e $K'$ due campi. Un'applicazione $\varphi : K \to K'$ si dice:
- *omomorfismo* se per tutti gli elementi $a, b \in K$ si ha:

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

$$\varphi(1_K) = 1_{K'}$$

- *isomorfismo* se $\varphi$ è un omomorfismo biiettivo; in tal caso $K$ e $K'$ sono campi *isomorfi* e si scrive $K \cong K'$.

## 5 Campi finiti

### 5.1 La caratteristica.

Per ogni campo finito $K$ esiste un numero primo $p$ tale che $K$ è un'estensione finita di $\mathbb{Z}/p\mathbb{Z}$. Diremo che $p$ è la *caratteristica* di $K$.

OSSERVAZIONE: Su un campo $K$ di caratteristica $p \neq 0$ si ha:
**(1)** Se $0 \neq x \in K$ e $m \in \mathbb{Z}$, allora $mx = 0_K$ se e solo se $m \in p\mathbb{Z}$.
**(2)** $(x + y)^p = x^p + y^p$ per tutti gli $x, y \in K$.

### 5.2 Cardinalità di un campo finito.

Sia $K$ è un campo finito.
**(1)** Esistono un numero primo $p$ e un numero $n \in \mathbb{N}$ tali che $K$ possiede $p^n$ elementi.
**(2)** $x^{p^n} = x$ per ogni $x \in K$.
**(3)** Se $K \subset F$ è un'estensione di campi, $f \in K[x]$ e $\alpha \in F$, allora $f(\alpha^{p^n}) = (f(\alpha))^{p^n}$.

### 5.3 Teorema di classificazione dei campi finiti

1. Per ogni numero primo $p$ e ogni $n \in \mathbb{N}$ esiste un campo $F$ di $p^n$ elementi.

   $F = \mathbb{F}_{p^n} = GF(p^n)$ è detto *campo di Galois* di ordine $p^n$ e si ottiene come campo di riducibilità completa del polinomio $g = x^{p^n} - x$ su $\mathbb{Z}/p\mathbb{Z}$. Più precisamente, $F$ consiste degli zeri di $g$.

2. Ogni campo finito è isomorfo a un campo di Galois $\mathbb{F}_{p^n}$.

## 5.4 Sottocampi di campi finiti.

Dati un numero primo $p$ e un numero naturale $n \in \mathbb{N}$, si hanno i seguenti enunciati.

1. Se $L$ è sottocampo di $\mathbb{F}_{p^n}$, allora $L$ possiede $p^m$ elementi, dove $m$ è un divisore di $n$.
2. Per ogni divisore positivo $m$ di $n$ esiste uno e un solo sottocampo $L$ di $\mathbb{F}_{p^n}$ di $p^m$ elementi. Si ha
$$L = \{x \in \mathbb{F}_{p^n} \mid x^{p^m} = x\}.$$

## 5.5 Teorema dell'elemento primitivo.

Per ogni campo finito $F = \mathbb{F}_{p^n}$ esiste $\alpha \in F$ tale che
$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}.$$

La dimostrazione si basa sul seguente

## 5.6 Lemma.

Ogni sottogruppo finito del gruppo moltiplicativo $(F \setminus \{0\}, \cdot)$ di un campo $F$ è ciclico.

## 5.7 Il polinomio minimo

Sia $K \subset F$ un'estensione di campi, e sia $\alpha \in F$. Si dice che $\alpha$ è un elemento *algebrico* su $K$ se $\alpha$ è uno zero di un polinomio $f \in K[x]$. In tal caso si hanno i seguenti enunciati:

1. Esiste uno e un solo polinomio $h \in K[x]$ monico e irriducibile tale che $h(\alpha) = 0$, detto *polinomio minimo* di $\alpha$ su $K$.
2. Per ogni $g \in K[x]$ si ha $g(\alpha) = 0$ se e solo se $h$ divide $g$.
3. Il campo $K[x]/(h)$ è isomorfo a un sottocampo $K(\alpha)$ di $F$. In particolare, $K \subset K(\alpha)$ è un'estensione di grado $d = \deg h$ con $K$-base 1, $\alpha$, $\alpha^2, ..., \alpha^{d-1}$.

## 5.8 Corollario

Sia $F$ un campo finito di caratteristica $p$ e sia $K = \mathbb{Z}/p\mathbb{Z}$.

1. Se $f$ è il polinomio minimo su $K$ di un elemento $\alpha \in F$, allora $d = degf$ è il minimo intero positivo tale che $\alpha^{p^d} = \alpha$.
2. Se $f \in K[x]$ è un polinomio irriducibile di grado $d$, allora il campo di riducibilità completa di $f$ su $K$ contiene esattamente $p^d$ elementi e $f$ divide il polinomio $x^{p^d} - x$.

*DIMOSTRAZIONE*
**(1)** Sappiamo che $K(\alpha)$ è un estensione di $K$ con base $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, quindi possiede $p^d$ elementi. Per 5.2 si ha che $\alpha^{p^d} = \alpha$. Sia adesso $n \in \mathbb{N}$ tale che $\alpha^{p^n} = \alpha$. Allora qualsiasi elemento $\beta \in K(\alpha)$ soddisfa $\beta^{p^n} = \beta$, poichè $\beta = a_0 1 + a_1\alpha + ... + a_{d-1}\alpha^{d-1}$ con $a_0, a_1, ..., a_{d-1} \in K$ e $\beta^{p^n} = (a_0 1 + a_1\alpha + ... + a_{d-1}\alpha^{d-1})^{p^n} = a_0^{p^n} + a_1^{p^n}\alpha^{p^n} + ... + a_{d-1}{}^{p^n}(\alpha^{d-1})^{p^n} = a_0 1 + a_1\alpha + ... + a_{d-1}\alpha^{d-1} = \beta$. Deduciamo che i $p^d$ elementi di $K(\alpha)$ sono zeri del polinomio $g = x^{p^n} - x$, pertanto $p^d \leq p^n$ e $d \leq n$.
**(2)** Sia $L$ il campo di riducibilità completa di $f$ e sia $\alpha \in L$ uno zero di $f$. Mostriamo che gli zeri di $f$ sono esattamente i $d$ elementi $\alpha$, $\alpha^p$,...,$\alpha^{p^{d-1}}$.

Poiché $f(\alpha) = 0$, segue da 5.2 che $f(\alpha^{p^i}) = 0$ per ogni $i$. Dunque basta verificare che $\alpha$, $\alpha^p$,...,$\alpha^{p^{d-1}}$ sono elementi distinti. Supponiamo per assurdo che esistano $1 \leq i \leq j \leq d$ tali che $\alpha^{p^i} = \alpha^{p^j}$ e $i \neq j$. Sappiamo che $f$ è irriducibile con $f(\alpha) = 0$, quindi $f = c\,h$ dove $c \in K$ e $h \in K[x]$ è il polinomio minimo di $\alpha$ su $K$. In particolare $d = \deg f = \deg h$ e segue da (1) che $d$ è il minimo intero positivo con $\alpha^{p^d} = \alpha$. D'altra parte $\alpha = \alpha^{p^d} = (\alpha^{p^j})^{p^{d-j}} = (\alpha^{p^i})^{p^{d-j}} = \alpha^{p^{d-(j-i)}}$ con $d - (j - i) < d$, una contraddizione.
Concludiamo che gli zeri $\alpha$, $\alpha^p$,..., $\alpha^{p^{d-1}}$ di $f$ sono tutti contenuti in $K(\alpha)$, dunque $L = K(\alpha)$ possiede $p^d$ elementi. L'ultimo enunciato segue da 5.3. □

# 6 Polinomi ciclotomici

## 6.1 Radici $m$-esime dell'unità

Sia $m \in \mathbb{N}$ e sia $K$ un campo finito la cui caratteristica $p$ non divide $m$. Sia $K_m$ il campo di riducibilità completa di $f = x^m - 1$ su $K$. Gli zeri di $f$ si chiamano *radici m-esime dell'unità* e formano un sottoinsieme di $K_m \setminus \{0\}$ che indichiamo con $E_m(K)$.
Segue da 5.6 che $E_m(K)$ è un sottogruppo ciclico di $K_m \setminus \{0\}$, e si verifica che possiede $m$ elementi. Quindi

$$E_m(K) \cong (\mathbb{Z}/m\mathbb{Z}, +).$$

Le radici $m$-esime dell'unità che generano il gruppo $E_m(K)$ sono dette *radici primitive*. Esse formano un sottoinsieme $P_m(K) \subset E_m(K)$ di ordine

$$|P_m(K)| = |\{a \in \mathbb{Z} \,|\, 1 \leq a < m, MCD(a, m) = 1\}| = \varphi(m)$$

dove $\varphi$ denota la *funzione di Eulero*, vedi 2.2.

## 6.2 Polinomi ciclotomici.

Sia dunque $P_m(K) = \{a_1, a_2, ..., a_{\varphi(m)}\}$.
Il polinomio

$$\phi_m = (x - a_1)(x - a_2) \cdot ... \cdot (x - a_{\varphi(m)}) \in K_m[x]$$

si chiama *polinomio ciclotomico*.
Si ha *deg* $\phi_m = \varphi(m)$ e si dimostra $\phi_m \in K[x]$.

## 6.3 Esempi

| | $\varphi(m)$ | $E_m$(K) | $P_m$(K) | $\phi_m$ |
|---|---|---|---|---|
| m = 1 | 1 | 1 | 1 | $x - 1$ |
| m = 2 | 1 | 1, -1 | -1 | $x + 1$ |
| m = 3 | 2 | 1, $\alpha, \alpha^2$ | $\alpha, \alpha^2$ | $(x - \alpha)(x - \alpha^2) = x^2 + x + 1$ |

Si noti che $\phi_1 \cdot \phi_2 = x^2 - 1$ e $\phi_1 \cdot \phi_3 = x^3 - 1$.

## 6.4 Teorema sulla scomposizione in polinomi ciclotomici

Se $d_1, ..., d_r$ sono i divisori positivi di $m$, allora in $K[x]$ abbiamo

$$x^m - 1 = \phi_{d_1} \cdot \phi_{d_2} \cdot ... \cdot \phi_{d_r}$$

*DIMOSTRAZIONE*
Sia $d$ un divisore di $m$, $m = dq$. Allora $(x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + ... + x^d + 1) = x^m - 1$.
Possiamo quindi considerare $E_d(K) = \{$ zeri di $x^d - 1\}$ come sottoinsieme di $E_m(K)$. Allora gli elementi di $P_d(K)$ appartengono a $E_m(K)$ e generano il sottogruppo $E_d(K)$ di ordine $d$, ovvero sono quegli elementi di $E_m(K)$ che hanno ordine $d$. D'altra parte ogni elemento di $E_m(K)$ ha come ordine un divisore di $m$ poichè $|E_m(K)| = m$ (vedi capitolo 2). Otteniamo quindi

$$E_m(K) = P_{d_1}(K) \cup P_{d_2}(K) \cup ... \cup P_{d_r}(K)$$

Scomponendo $(x^m - 1)$ nei suoi fattori linerari e raggruppando tutti gli elementi di ordine $d_1$, tutti gli elementi di ordine $d_2$, ecc... vediamo che $x^m - 1 = \phi_{d_1}\phi_{d_2}...\phi_{d_r}$. □

## 6.5 Corollario: calcolo ricorsivo dei polinomi ciclotomici

**(1)** $x^4 - 1 = \phi_1\phi_2\phi_4$ implica $\phi_4 = \dfrac{x^4 - 1}{\phi_1\phi_2} = \dfrac{x^4 - 1}{x^2 - 1} = x^2 + 1$.
**(2)** Se $p$ è primo, $x^p - 1 = \phi_1\phi_p = (x-1)(x^{p-1} + x^{p-2} + ... + x + 1)$ implica $\phi_p = x^{p-1} + x^{p-2} + ... + x + 1$.

## 6.6 Esempio

Siano $p$ primo e $n \in \mathbb{N}$. Se $K = \mathbb{Z}/p\mathbb{Z}$ e $m = p^n - 1$, allora $E_m(K) = \mathbb{F}_{p^n} \setminus \{0\}$.

Siano ad esempio $p = 2, n = 4$, quindi $m = 15$. Abbiamo $x^{15} - 1 = \phi_1\phi_3\phi_5\phi_{15} \in K[x]$.
Quanti fattori irriducibili possiede $x^{15} - 1$ ?

$\phi_1 = x - 1$ e $\phi_3 = x^2 + x + 1$ sono entrambi irriducibili su $K$.

Esaminiamo $\phi_5$. Il suo grado è $\deg(\phi_5) = \varphi(5) = 4$. Ogni suo fattore irriducibile $f$ è (a meno di una costante) polinomio minimo di un elemento $\alpha \in P_5(K)$, ovvero di un elemento $\alpha \in E_{15}(K) = \mathbb{F}_{16} \setminus \{0\}$ che ha ordine 5. Per 5.8 (1) sappiamo che $\deg f = d$ è il minimo intero positivo tale che $\alpha^{2^d} = \alpha$, ovvero $\alpha^{2^d - 1} = 1$. Dunque $d \leq \deg \phi_5 = 4$ ed è il minimo intero positivo tale che 5, l'ordine di $\alpha$, divida $2^d - 1$. Abbiamo $\{2^d - 1 | d \leq 4\} = \{1, 3, 7, 15\}$ e concludiamo $d = 4$. Dunque $\phi_5$ è irriducibile.

Esaminiamo adesso $\Phi_{15}$. Il suo grado é $\varphi(15) = 8$. I suoi fattori irriducibili sono (a meno di una costante) polinomi minimi di radici primitive quindicesime dell'unità, vale a dire di elementi di $\mathbb{F}_{16} \setminus \{0\}$ di ordine 15, e quindi hanno tutti grado $d$ dove $d \leq 8$ è il minimo intero positivo tale che 15 divida $2^d - 1$. Come sopra segue $2^d - 1 = 15$ e $d = 4$. Ciò dimostra che $\Phi_{15}$ è prodotto di due polinomi irriducibili di grado 4.

In tutto abbiamo quindi $1 + 1 + 1 + 2 = 5$ fattori irriducibili.

## 6.7 Bibliografia

S. Bosch, *Algebra*, Springer, Unitext 2003.
I.N.Herstein, *Algebra*, Editori Riuniti 2003.