UNIVERSITÀ DEGLI STUDI DI CAGLIARI
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

Costruzioni con riga e compasso

Relatore:
Prof. Andrea Loi

Candidato:
Angelo Atzeri

Anno Accademico 2010/2011

Indice

Introduzione

Lo scopo di questa tesi è quello di dimostrare che alcune costruzioni geometriche non sono possibili utilizzando solamente una riga non graduata ed un compasso. La tesi è suddivisa in tre capitoli, i primi due dei quali forniscono gli strumenti atti a poter dimostrare l'impossibilità delle costruzioni geometriche considerate.
Nel primo capitolo (Richiami algebrici) vengono richiamati i concetti base e le principali proprietà della teoria dei gruppi, della teoria degli anelli e degli spazi vettoriali.
Nel secondo capitolo (Teoria dei campi) vengono introdotti i concetti di estensione di campo e di grado delle estensioni di campo e vengono dimostrate alcune loro importanti proprietà.
Nel terzo capitolo (Costruzioni con riga e compasso) si introduce un parallelismo tra le costruzioni geometriche possibili e la teoria dei campi, si dimostra il "teorema fondamentale sui punti costruibili", e attraverso quest'ultimo teorema si dimostra infine che la "duplicazione di un cubo", la "trisecazione di un angolo" e la "quadratura del cerchio" sono costruzioni impossibili con il solo ausilio di una riga e di un compasso.

Capitolo 1

Richiami algebrici

1.1 Teoria dei gruppi

Definizione 1.1.1. *Si dice gruppo un insieme non vuoto* $\boldsymbol{G}$ *dotato di un'operazione* $*$ *che soddisfa i seguenti assiomi:*

1. $*$ *è associativa; cioè per ogni* a, b *e* $c \in \boldsymbol{G}$ *si ha:*

$$a * (b * c) = (a * b) * c$$

2. *Esiste un elemento 1 in G tale che* $a * 1 = 1 * a = a$ *per ogni elemento a di G. L'elemento 1 è detto elemento neutro per l'operazione* $*$.

3. *Per ogni elemento a in G, esiste un elemento* a^{-1} *in G tale che* $a * a^{-1} = a^{-1} * a = 1$. *L'elemento* a^{-1} *è detto inverso dell'elemento a.*

Il gruppo G appena definito può essere indicato come $\langle\ G, * \ \rangle$. *Se non vi è pericolo di confusione, indicheremo il gruppo semplicemente con la lettera G.*
Se l'operazione $*$ *gode anche della proprietà commutativa, diremo che G è un gruppo commutativo o, più comunemente, un gruppo abeliano.*

Proposizione 1.1.1. *L'elemento neutro del gruppo G dotato dell'operazione* $*$ *è unico.*

Dimostrazione. Supponiamo per assurdo che esistano due elementi neutri e_1, e_2 in G. Allora

$$e_1 * e_2 = e_2$$
$$e_1 * e_2 = e_1$$

Per cui

$$e_1 = e_2$$

□

Proposizione 1.1.2. *L'inverso* a^{-1} *di un elemento a in G è unico.*

Dimostrazione. Supponiamo per assurdo che esistano due inversi a_1, a_2 dell'elemento a in G. Allora

$$a_1 * (a * a_2) = a_1 * 1 = a_1$$
$$(a_1 * a) * a_2 = 1 * a_2 = a_2$$

Per cui, tenendo conto che $*$ gode della proprietà associativa, si ha

$$a_1 = a_2$$

□

Osservazione 1.1.1. *I simboli comunemente usati per indicare l'operazione definita su un gruppo G sono i simboli* $*$ *e* $+$.
Quando utilizziamo il simbolo $*$, *diremo che utilizziamo la notazione moltiplicativa; solitamente scriveremo ab al posto di* $a * b$, *e chiameremo ab il prodotto di a e b. In notazione moltiplicativa l'elemento neutro è indicato con 1 e l'inverso con* a^{-1}.
Quando utilizziamo il simbolo $+$, *diremo che utilizziamo la notazione additiva, e chiameremo* $a + b$ *la somma di a e b. In notazione additiva l'elemento neutro è indicato con 0 e l'inverso con -a (viene chiamato l'opposto*

di a). La notazione additiva è solitamente utilizzata nel caso di gruppi abeliani.
Qualora non venga specificata la notazione utilizzata, utilizzeremo la notazione moltiplicativa.

Teorema 1 (Legge di cancellazione)**.** *Sia G un gruppo e a, b e c suoi elementi. Allora*

1. *ab = ac implica b = c*
2. *ba = ca implica b = c*

Dimostrazione. Per quanto riguarda la dimostrazione della prima implicazione, si moltiplichino ambo i membri dell'equazione $ab = ac$ a sinistra per a^{-1}; otterremo così che $b = c$. La seconda implicazione si dimostra analogamente. □

Teorema 2. *Sia G un gruppo e a e b due suoi elementi. Allora*

$$ab = 1 \text{ implica } a = b^{-1} \text{ e } b = a^{-1}$$

Dimostrazione. L'equazione $ab = 1$ è equivalente all'equazione $ab = aa^{-1}$; per cui, per la legge di cancellazione, si ha che $b = a^{-1}$. In maniera analoga si dimostra che $a = b^{-1}$. □

Teorema 3. *Sia G un gruppo e a e b due suoi elementi. Allora*

1. $(ab)^{-1} = b^{-1}a^{-1}$
2. $(a^{-1})^{-1} = a$

Dimostrazione. Per quanto riguarda la prima uguaglianza si ha che:

$$(ab)(b^{-1}a^{-1}) = a[(bb^{-1})a^{-1}] = a[1a^{-1}] = aa^{-1} = 1.$$

Per cui $(b^{-1}a^{-1})$ è l'inverso del prodotto ab.
Per quanto riguarda la seconda uguaglianza, si ha che $aa^{-1} = 1$; dunque a è l'inverso di a^{-1}, cioè $a = (a^{-1})^{-1}$. □

Corollario 1.1.1. *Sia G un gruppo e a_1, a_2, ..., a_n suoi elementi. Allora*

$$(a_1a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1}a_1^{-1}$$

Definizione 1.1.2. *Se G è un gruppo finito, il numero di elementi di G è chiamato ordine di G. Si indicherà l'ordine del gruppo G col simbolo*

$$|G|$$

Definizione 1.1.3. *Sia G un gruppo e S un sottoinsieme non vuoto di G. Se il prodotto di due qualunque elementi di S è ancora un elemento di S, diremo che S è chiuso rispetto al prodotto; se l'inverso di ogni elemento di S è ancora un elemento di S, diremo che S è chiuso rispetto al passaggio agli inversi.*

Definizione 1.1.4. *Sia G un gruppo e S un sottoinsieme non vuoto di G. Se*

1. *S è chiuso rispetto al prodotto*
2. *S è chiuso rispetto al passaggio agli inversi*

allora il sottoinsieme S è detto sottogruppo di G

Proposizione 1.1.3. *Sia G un gruppo e S un sottogruppo di G. Allora S è esso stesso un gruppo.*

Dimostrazione. L'operazione definita su S è la restrizione a S dell'operazione definita su G; dunque quest'operazione gode della proprietà associativa. Ogni elemento di S ammette inverso in S in quanto S è chiuso rispetto al passaggio agli inversi. Dal momento che S è non vuoto, esso dovrà contenere almeno un elemento, chiamiamolo a; poiché S è chiuso rispetto agli inversi anche a^{-1} dovrà essere un elemento di S, e dal momento che S è chiuso rispetto ai prodotti sarà un elemento di S anche $aa^{-1} = 1$. Dunque S è un gruppo. □

Osservazione 1.1.2. *Sia G un gruppo. Gli insiemi G e $\{1\}$ sono sottoinsiemi impropri di G, ed è di semplice verifica che siano sottogruppi di G. Questi sottogruppi sono detti sottogruppi banali del gruppo G.*

Definizione 1.1.5. *Sia G un gruppo e H un sottogruppo di G. Per ogni elemento a di G, il simbolo*

$$aH$$

indica l'insieme di tutti i prodotti del tipo ah, dove a rimane fissato e h varia su H.
aH è chiamato laterale sinistro di H in G.
In modo simile

$$Ha$$

è l'insieme di tutti i prodotti ha, dove a rimane fissato e h varia su H. Ha è detto laterale destro di H in G.

Proposizione 1.1.4. *Sia G un gruppo, H un sottogruppo di G e a e b due elementi di G. Se $a \in Hb$, allora $Ha = Hb$.*

Dimostrazione. Poichè $a \in \mathrm{H}b$, si avrà che $a = h_1 b$ per qualche $h_1 \in \mathrm{H}$. Sia $x \in \mathrm{H}a$; ciò significa che $x = h_2 a$ per qualche $h_2 \in \mathrm{H}$. Ma $a = h_1 b$, per cui $x = h_2 a = (h_2 h_1)b$; questo prova che ogni $x \in \mathrm{H}a$ è in $\mathrm{H}b$.
In maniera analoga si dimostra che ogni $y \in \mathrm{H}b$ è in $\mathrm{H}a$. Per cui $\mathrm{H}a = \mathrm{H}b$. □

Definizione 1.1.6. *Siano G e H gruppi. Un omomorfismo da G a H è una funzione f: $G \longrightarrow H$ tale che per ogni coppia di elementi a e b di G, si abbia*

$$f(ab) = f(a)f(b)$$

Nel caso in cui esista un omomorfismo da G su H, diremo che H è un'immagine omomorfa di G.

Definizione 1.1.7. *Siano G e H gruppi. Un isomorfismo da G a H è una funzione bigettiva f: $G \longrightarrow H$ tale che per ogni coppia di elementi a e b di G, si abbia*

$$f(ab) = f(a)f(b)$$

Dunque un isomorfismo è un omomorfismo bigettivo. Nel caso in cui esista un isomorfismo da G a H, diremo che H è un'immagine isomorfa di G.

Definizione 1.1.8. *Se a è un elemento di un gruppo G, si dice coniugato di a un qualsiasi elemento della forma xax^{-1}, con $x \in G$.*

Definizione 1.1.9. *Sia H un sottoinsieme del gruppo G; diremo che H è chiuso rispetto ai coniugati se ogni coniugato di ogni elemento di H è in H.*

Definizione 1.1.10. *Sia H un sottogruppo del gruppo G. H è detto sottogruppo normale di G se è chiuso rispetto ai coniugati; cioè se*

$$\text{per ogni } a \in H \text{ e } x \in G, \text{ si ha } xax^{-1} \in H$$

Definizione 1.1.11. *Sia f: $G \longrightarrow H$ un omomorfismo. Il nucleo di f è l'insieme K di tutti gli elementi di G che sono portati da f nell'elemento neutro di H. Cioè*

$$K = ker(f) = \{\ x \in G \mid f(x) = 1\ \}$$

L'immagine di f è l'insieme I di tutti gli elementi di H che sono immagine di un qualche elemento di G. Cioè

$$I = im(f) = \{\ y \in H \mid \exists\ x \in G \text{ per cui } f(x) = y\ \}$$

Teorema 4. *Sia f: $G \longrightarrow H$ un omomorfismo. Allora*

1. *Il nucleo di f è un sottogruppo normale di G*
2. *L'immagine di f è un sottogruppo di H*

Dimostrazione. Indichiamo con K il nucleo di f. Siano a,$b \in$ K, ciò significa che $f(a) = f(b) = 1$. Consideriamo ora l'elemento $ab \in$ K, si avrà $f(ab) = f(a)f(b) = 1$, cioè $ab \in$ K.
Sia $a \in$ K, allora $f(a) = 1$. Dunque, $f(a^{-1}) = [f(a)]^{-1} = 1^{-1} = 1$.
Essendo K chiuso rispetto ai prodotti e al passaggio agli inversi, K è un sottogruppo di G. Inoltre, sia $a \in$ K e sia $x \in$ G, allora $f(xax^{-1}) = f(x)f(a)f(x^{-1}) = f(x)f(a)[f(x)]^{-1} = 1$, per cui $xax^{-1} \in$ K. Perciò, K è un sottogruppo normale di G.
Siano $f(a)$ e $f(b)$ due elementi dell'immagine di f; allora anche il loro prodotto $f(a)f(b) = f(ab)$ appartiene all'immagine di f. Inoltre, se $f(a)$ è nell'immagine di f, il suo inverso $[f(a)]^{-1} = f(a^{-1})$ è ancora un elemento dell'immagine di f. Dunque l'immagine di f è un sottogruppo di H. □

Definizione 1.1.12. *Sia G un gruppo e H un sottogruppo normale di G. L'insieme i cui elementi sono tutti i laterali di H viene indicato con G/H. Nell'insieme G/H è possibile definire un prodotto, detto prodotto di laterali, nella seguente maniera*

$$Ha \cdot Hb = H(ab)$$

Il prodotto così definito risulta essere una valida operazione sull'insieme G/H.

Teorema 5. *G/H con il prodotto di laterali è un gruppo.*

Dimostrazione. Il prodotto di laterali è associativo, infatti si ha

$$\mathrm{H}a \cdot (\mathrm{H}b \cdot \mathrm{H}c) = \mathrm{H}a \cdot \mathrm{H}(bc) = \mathrm{H}a(bc) = \mathrm{H}(ab)c = \mathrm{H}(ab) \cdot \mathrm{H}(c) = (\mathrm{H}a \cdot \mathrm{H}b) \cdot \mathrm{H}c.$$

L'elemento neutro di G/H è il laterale H1 = H, infatti $\mathrm{H}1 \cdot \mathrm{H}a = \mathrm{H}(1a) = \mathrm{H}(a1) = \mathrm{H}a$, per ogni laterale H$a$ in G/H.
Infine l'inverso di un qualsiasi laterale Ha è il laterale Ha^{-1}, infatti $\mathrm{H}a \cdot \mathrm{H}a^{-1} = \mathrm{H}(aa^{-1}) = \mathrm{H}(a^{-1}a) = \mathrm{H}1 = \mathrm{H}$.
Dunque G/H è un gruppo, che chiameremo gruppo quoziente di G da H. □

Teorema 6. *G/H è un'immagine omomorfa di G.*

Dimostrazione. Consideriamo la funzione f da G in G/H che ad ogni elemento di G associa il suo laterale, cioè la funzione definita come

$$f(x) = \mathrm{H}x.$$

Questa funzione è un omomorfismo, infatti si ha che

$$f(xy) = \mathrm{H}(xy) = \mathrm{H}x \cdot \mathrm{H}y = f(x)f(y)$$

Dunque esiste un omomorfismo da G su G/H, e si ha che G/H è un'immagine omomorfa di G. □

Teorema 7. *Sia G un gruppo e H un sottogruppo di G. Allora*

1. *Ha = Hb se e solo se $ab^{-1} \in H$*
2. *Ha = H se e solo se $a \in H$*

Dimostrazione. Se Ha = Hb, allora $a \in \mathrm{H}b$, per cui $a = hb$ per qualche $h \in \mathrm{H}$. Per cui $ab^{-1} = h$, con $h \in \mathrm{H}$. Dunque $ab^{-1} \in \mathrm{H}$. Viceversa, se $ab^{-1} \in \mathrm{H}$, allora $ab^{-1} = h$, per qualche $h \in \mathrm{H}$, cioè $a = hb$. Dunque Ha = Hb. Questo dimostra il primo punto del teorema.
Per quanto riguarda il secondo punto, deriva dal punto 1. che Ha = H1 se se solo se $a(1)^{-1} = a \in \mathrm{H}$. □

Teorema 8. *Sia f: G ⟶ H un omomorfismo con nucleo K. Allora*

$$f(a) = f(b) \text{ se e solo se } Ka = Kb$$

Dimostrazione. Si ha che

$$f(a) = f(b) \iff f(a)[f(b)]^{-1} = 1 \iff f(ab^{-1}) = 1 \iff ab^{-1} \in \mathrm{K} \iff \mathrm{K}a = \mathrm{K}b$$

□

Teorema 9 (Teorema fondamentale d'omomorfismo)**.** *Sia f: G ⟶ H un omomorfismo di G su H, e sia K il nucleo di f, allora*

$$H \cong G/K$$

Dimostrazione. Per dimostrare che G/K è isomorfo a H, dobbiamo trovare un isomorfismo tra G/K e H. Consideriamo la funzione da G/K in H che a ciascun laterale Kx associa l'elemento $f(x)$; detta ϕ tale funzione avremo

$$\phi(\mathrm{K}x) = f(x)$$

Per verificare che la funzione ϕ sia correttamente definita, consideriamo Ka = Kb, allora per il teorema 8 avremo che $f(a) = f(b)$, cioè $\phi(\mathrm{K}a) = \phi(\mathrm{K}b)$.
ϕ è iniettiva, infatti se $\phi(\mathrm{K}a) = \phi(\mathrm{K}b)$, allora $f(a) = f(b)$, cioè dal teorema 8 Ka = Kb.
ϕ è suriettiva, perché ogni elemento di H è della forma $f(x) = \phi(\mathrm{K}x)$.
Infine, ϕ è un omomorfismo, infatti si ha

$$\phi(\mathrm{K}a \cdot \mathrm{K}b) = \phi(\mathrm{K}ab) = f(ab) = f(a)f(b) = \phi(\mathrm{K}a)\phi(\mathrm{K}b)$$

□

1.2 Teoria degli anelli

Definizione 1.2.1. *Per anello intendiamo un insieme A dotato di un'operazione +, detta somma, e di un'operazione ·, detta prodotto, soddisfacente ai seguenti assiomi:*

1. *A con la sola addizione è un gruppo abeliano.*
2. *La moltiplicazione è associativa.*
3. *La moltiplicazione è distributiva rispetto alla somma. Cioè, per ogni a, b e c di A, si ha che*

$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$

Osservazione 1.2.1. *Dal momento che A con l'operazione di somma è un gruppo abeliano, ci sarà in A un elemento neutro rispetto alla somma: lo indicheremo con il simbolo 0. Inoltre ogni elemento a di A avrà un'inverso additivo, che chiameremo opposto di a e indicheremo con -a.*

Teorema 10. *Siano a e b due elementi di un anello A. Allora*

1. *a0 = 0a = 0*
2. *a(-b) = (-a)b = -(ab)*
3. *(-a)(-b) = ab*

Dimostrazione. Per provare la prima relazione, notiamo che

$$aa + 0 = aa = a(a + 0) = aa + a0$$

Per cui, per le leggi di cancellazione del gruppo additivo A, si ha $a0 = 0$.
Per provare la seconda relazione, notiamo che

$$a(-b) + ab = a[(-b) + b] = a0 = 0$$

da cui otteniamo che $a(-b) = -(ab)$. In maniera analoga si dimostra che $(-a)b = -(ab)$.
Per provare la terza relazione, applicando due volte la relazione precedente, si ottiene

$$(-a)(-b) = -[a(-b)] = -[-(ab)] = ab$$

□

Definizione 1.2.2. *Sia A un anello. Se la moltiplicazione definita su A gode della proprietà commutativa diremo che A è un anello commutativo.*

Definizione 1.2.3. *Sia A un anello. Se vi è in A un elemento neutro rispetto al prodotto, diremo che A è un anello con unità. Denoteremo l'elemento neutro rispetto al prodotto col simbolo 1, e lo chiameremo unità di A.*

Definizione 1.2.4. *Sia A un anello con unità. Se un elemento a di A ammette inverso moltiplicativo, diremo che a è un elemento invertibile di A, ed indicheremo il suo inverso moltiplicativo col simbolo a^{-1}.*

Definizione 1.2.5. *Sia A un anello commutativo con unità in cui ciascun elemento non nullo è invertibile; allora diremo che A è un campo.*

Definizione 1.2.6. *Sia A un anello. Un qualunque elemento non nullo a di A è detto divisore dello zero se esiste un elemento non nullo b in A, tale che il prodotto ab o ba è uguale a zero.*

Definizione 1.2.7. *Sia A un anello. Diremo che A gode della legge di cancellazione per il prodotto se*

$$ab = ac \text{ o } ba = ca \text{ implica } b{=}c$$

per ogni elemento a, b e c appartenenti ad A, con $a \neq 0$.

Teorema 11. *Un anello A gode della legge di cancellazione se e solo se A non possiede divisori dello zero.*

Dimostrazione. Sia A un anello, e supponiamo che su A valga la legge di cancellazione. Consideriamo a e b in A tali che $ab = 0$; se $a = 0$, la dimostrazione è conclusa; altrimenti si ha che $ab = 0 = a0$, per cui per la legge di cancellazione, si ottiene $b = 0$.
Viceversa, consideriamo gli elementi di A ab e ac tali che $ab = ac$, con a non nullo. Allora

$$ab - ac = a(b - c) = 0$$

Dal momento che A non ammette divisori dello zero e che a è non nullo, si ottiene che $(b - c) = 0$, da cui $b = c$. □

Definizione 1.2.8. *Si dice dominio di integrità un anello commutativo con unità per cui è valida la legge di cancellazione. Analogamente, si dice dominio di integrità un anello commutativo con unità che non ammette divisori dello zero.*

Definizione 1.2.9. *Sia A un anello e B un sottoinsieme non vuoto di A. Se la somma di due qualunque elementi di B è ancora un elemento di B, diremo che B è chiuso rispetto alla somma; se l'opposto di ogni elemento di B è ancora un elemento di B, diremo che B è chiuso rispetto agli opposti; se il prodotto di due qualunque elementi di B è ancora un elemento di B, diremo che B è chiuso rispetto ai prodotti.*

Definizione 1.2.10. *Se un sottoinsieme non vuoto $B \subseteq A$ è chiuso rispetto alla somma, agli opposti e ai prodotti, allora B è un sottoanello dell'anello A.*

Definizione 1.2.11. *Sia A un anello e B un sottoinsieme non vuoto di A. Diremo che B assorbe i prodotti in A se, comunque si moltiplichi un elemento di B per un elemento di A, il loro prodotto è un elemento di B. Cioè*

$$\forall\ b \in B\ e\ \forall\ x \in A \Longrightarrow bx,\ xb \in B$$

Definizione 1.2.12. *Un sottoinsieme non vuoto B di un anello A è detto ideale di A se B è chiuso rispetto all'addizione e agli opposti (cioè è un sottogruppo additivo di A), e B assorbe i prodotti in A.*

Osservazione 1.2.2. *Il più semplice esempio di ideale è l'insieme di tutti i multipli di un fissato elemento di un anello, cioè l'insieme di tutti i prodotti ax con a fisso e x che varia su tutti gli elementi di un anello. Esso è un ideale perché*

$$\begin{gathered} xa + ya = (x + y)a \\ -(xa) = (-x)a \\ y(xa) = (yx)a \end{gathered}$$

Questo ideale è chiamato ideale principale generato da a, ed è indicato col simbolo $\langle a \rangle$.

Proposizione 1.2.1. *Sia A un anello e sia J un suo ideale. Se $1 \in J$ allora $J = A$.*

Dimostrazione. Dal momento che J è un ideale di A risulta essere che J è un sottoinsieme di A, cioè $J \subseteq A$. Inoltre, poiché J è un ideale, esso assorbe i prodotti, per cui J conterrà tutti i prodotti del tipo $1a$, dove 1 rimane fisso e a varia in A. Dunque $A \subseteq J$. Dunque risulta che $A = J$. □

Definizione 1.2.13. *Un omomorfismo da un anello A ad un anello B è un applicazione f: $A \longrightarrow B$ che soddisfi le seguenti condizioni*

1. *$f(x + y) = f(x) + f(y)$*
2. *$f(xy) = f(x)f(y)$*

Se esiste un omomorfismo da A su B diremo che B è un'immagine omomorfa di A.

Definizione 1.2.14. *Sia f un omomorfismo dall'anello A all'anello B; il nucleo di f è l'insieme di tutti gli elementi di A che sono portati da f nell'elemento 0 di B. Il nucleo di f è dunque l'insieme*

$$ker(f) = \{\ x \in A \mid f(x) = 0\ \}$$

Osservazione 1.2.3. *Il nucleo di un omomorfismo f: $A \longrightarrow B$ è un ideale di A.*

Definizione 1.2.15. *Se A e B sono due anelli, un isomorfismo da A in B è un omomorfismo che sia iniettivo e suriettivo. Se c'è un isomorfismo da A a B, diremo che A è isomorfo a B e scriveremo*

$$A \cong B$$

Definizione 1.2.16. *Sia A un anello e J un ideale di A. Per ogni elemento $a \in A$, il simbolo $J + a$ indica l'insieme di tutte le somme $j + a$, dove a rimane fissato e j varia su tutto J. Cioè*

$$J + a = \{\ j + a \mid j \in J\ \}$$

$J + a$ è detto laterale di J in A.

Osservazione 1.2.4. *L'insieme di tutti i laterali $J + a$, al variare di a su A, può essere dotato di due operazioni, che chiamiamo somma e prodotto di laterali, definite come*

$$(J + a) + (J + b) = J + (a + b)$$
$$(J + a)(J + b) = J + (ab)$$

La somma e il prodotto così definiti definiti sono determinati senza ambiguità.

Teorema 12. *L'insieme di tutti i laterali di J in A è denotato col simbolo A/J. A/J con le operazioni di somma e prodotto di laterali è un anello.*

Dimostrazione. Dal momento che A è un anello, si ha che la somma e il prodotto di laterali sono associativi, che la somma è commutativa e che il prodotto di laterali è distributivo rispetto alla somma.
L'elemento neutro in A/J rispetto alla somma di laterali è il laterale J = J + 0, infatti, considerato il laterale J + a, si ha

$$(\mathrm{J} + a) + (\mathrm{J} + 0) = \mathrm{J} + (a + 0) = \mathrm{J} + a$$

Infine, l'opposto del laterale J + a è il laterale J + (-a), infatti si ha

$$(\mathrm{J} + a) + (\mathrm{J} + (-a)) = \mathrm{J} + (a + (-a)) = \mathrm{J} + 0$$

L'anello A/J è detto anello quoziente di A su J □

Teorema 13. *Sia A un anello e J un suo ideale. A/J è un'immagine omomorfa di A.*

Dimostrazione. L'omomorfismo naturale che porta A su A/J è la funzione f che ad ogni elemento di A associa il suo laterale, cioè la funzione definita come

$$f(x) = \mathrm{J} + x$$

Questa funzione è un omomorfismo, infatti si ha

$$f(x + y) = \mathrm{J} + (x + y) = (\mathrm{J} + x) + (\mathrm{J} + y) = f(x) + f(y)$$
$$f(xy) = \mathrm{J} + (xy) = (\mathrm{J} + x)(\mathrm{J} + y) = f(x)f(y)$$

Dunque A/J è un'immagine omomorfa di A. □

Teorema 14 (Teorema fondamentale di omomorfismo)**.** *Sia $f : A \longrightarrow B$ un omomorfismo dall'anello A su B, e sia K il nucleo di f. Allora $B \cong A/K$*

Dimostrazione. Per dimostrare che B è isomorfo a A/K dobbiamo trovare un isomorfismo da A/K in B. Consideriamo la funzione ϕ da A/K a B che associa ad ogni laterale K + x l'elemento $f(x)$, cioè

$$\phi(\mathrm{K} + x) = f(x)$$

Ignorando la moltiplicazione, A e B sono gruppi, e per quanto visto nel teorema fondamentale di omomorfismo per gruppi (teorema 9), risulta che ϕ è una funzione bigettiva ben definita da A/K a B. Infine

$$\phi((\mathrm{K} + a) + (\mathrm{K} + b)) = \phi(\mathrm{K} + (a + b)) = f(a + b) = f(a) + f(b) = \phi(\mathrm{K} + a) + \phi(\mathrm{K} + b)$$
$$\phi((\mathrm{K} + a)(\mathrm{K} + b)) = \phi(\mathrm{K} + ab) = f(ab) = f(a)f(b) = \phi(\mathrm{K} + a)\phi(\mathrm{K} + b)$$

Dunque la funzione ϕ è un isomorfismo da A/K in B. □

Definizione 1.2.17. *Un ideale J di un anello commutativo A è detto ideale primo se per ogni coppia di elementi $a, b \in A$ risulta che*

$$se\ ab \in J \Longrightarrow a \in J\ o\ b \in J$$

Definizione 1.2.18. *Un ideale J di un anello A è detto ideale proprio se non è uguale all'intero anello A. Un ideale proprio J di un anello A è detto ideale massimale se non esiste nessun ideale proprio K di A tale che $J \subseteq K$ con $J \neq K$.*

Proposizione 1.2.2. *Sia A un anello commutativo con unità. J è un ideale massimale di A se e solo se A/J è un campo*

Dimostrazione. Sia J un ideale massimale di A. Essendo A un anello commutativo con unità, tale è anche A/J; infatti (J + 1) è l'unità di A/J dal momento che, preso (J + a) in A/J si ha

$$(\mathrm{J} + a)(\mathrm{J} + 1) = (\mathrm{J} + a1) = (\mathrm{J} + a).$$

Il laterale nullo di A/J è (J + 0) = J. Dire che (J + a) è non nullo, equivale, per l'implicazione 2. del teorema 7, a dire che $a \notin$ J. Sia K l'insieme di tutte le somme del tipo

$$xa + j$$

dove x varia su A e j varia su J. K è un ideale; inoltre K contiene a, perché $a = 1a + 0$ e K contiene ogni elemento $j \in$ J poiché j può essere scritto come $0a + j$. Dunque K è un'ideale che contiene J e che è strettamente più grande di J. Ma dal momento che J è un'ideale massimale, risulta che K = A. Segue che $1 \in$ K, così che $1 = xa + j$, per qualche $x \in$ A e $j \in$ J. Dunque 1 - $xa = j \in$ J, per cui, per l'implicazione 1. del teorema 7 risulta che (J + 1) = (J + xa) = (J + x)(J + a), e dunque (J + x) è l'inverso moltiplicativo di (J + a). Dunque A/J è un campo.
Viceversa, sia A un anello commutativo con unità J un suo ideale e A/J un campo. Consideriamo inoltre un ideale K, tale che J $\subset$ K. Preso k in K, essendo k anche un elemento di A, consideriamo il laterale J + k in A/J. Poiché A/J è un campo, esisterà un laterale (J + x) in A/J tale che (J + k)(J + x)=(J + kx)=(J + 1); da ciò, per l'implicazione 1. del teorema 7, deriva che (1 - kx) $\in$ J, cioè esiste $j \in$ J tale che j = 1 - kx. Dal momento che che j, $kx \in$ K, risulta che $j + kx = 1 \in$ K. Dunque K, contenendo l'unità, coincide col campo A e J risulta essere l'ideale massimale di A. □

Definizione 1.2.19. *Sia A un anello commutativo con unità e x un simbolo arbitrario. Ogni espressione della forma*

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

è chiamato polinomio in x a coefficienti in A, o più semplicemente, polinomio in x su A.
Le espressioni a_kx^k, con $k \in \{1, \ldots, n\}$, sono detti termini del polinomio.

Definizione 1.2.20. *I polinomi nell'indeterminata x sono indicati con simboli come a(x), b(x), p(x) e così via. Sia $a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ un polinomio e a_kx^k uno dei suoi termini, allora a_k è detto il coefficiente di x^k.*
Per grado di un polinomio a(x) si intende il più grande n tale che il coefficiente del termine x^n sia diverso da zero. Il grado di a(x) sarà indicato col simbolo

$$deg\ a(x)$$

Il polinomio $0 + 0x + 0x^2 + \ldots$ in cui tutti i coefficienti sono uguali a zero, è detto polinomio nullo ed è indicato col simbolo 0; il polinomio nullo è l'unico polinomio il cui grado non è definito.
Se un polinomio $a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ ha grado n, allora il coefficiente a_n è detto coefficiente direttore del polinomio a(x), mentre il termine a_0 è detto termine noto.
Se un polinomio a(x) ha grado zero, vuol dire che il termine noto a_0 è l'unico termine non nullo: a(x) è detto dunque polinomio costante.

Osservazione 1.2.5. *Per indicare un polinomio a(x) di grado n, possiamo utilizzare la seguente notazione:*

$$a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{k=0}^{n} a_kx^k$$

ricordando che $x^0 = 1$.
Vogliamo ora definire formalmente la somma e il prodotto tra due polinomi

$$a(x) = a_0 + a_1x + \ldots + a_nx^n$$
$$b(x) = b_0 + b_1x + \ldots + b_nx^n$$

E' importante osservare che non stiamo supponendo che i due polinomi abbiamo lo stesso grado; infatti i coefficienti dei polinomi potrebbero essere all'occorrenza nulli. La somma dei polinomi a(x) e b(x) è definita come

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n = \sum_{k=0}^{n} (a_k + b_k)x^k$$

Il grado del polinomio a(x) + b(x) è minore o uguale al più grande grado dei due polinomi a(x) e b(x), cioè $deg(a(x) + b(x)) \leq max\ \{deg\ a(x), deg\ b(x)\}$.
Il prodotto dei polinomi a(x) e b(x) è definito come

$$a(x)b(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots + a_nb_nx^{2n} = \sum_{k=0}^{2n} \Big(\sum_{i+j=k} a_ib_j \Big)x^k$$

Il grado del polinomio a(x)b(x) è minore o uguale della somma dei gradi dei polinomi a(x) e b(x), cioè $deg[a(x)b(x)] \leq deg(a(x)) + deg(b(x))$.
Sia A un anello, col simbolo

$$A[x]$$

indicheremo l'insieme di tutti i polinomi in x con coefficienti in A, con la somma e il prodotto di polinomi appena definiti.

Teorema 15. *Sia A un anello commutativo con unità. Allora A[x] è un anello commutativo con unità.*

Dimostrazione. Siano $a(x)$, $b(x)$ e $c(x)$ polinomi in A[x] definiti come:

$$a(x) = a_0 + a_1x + ... + a_nx^n$$
$$b(x) = b_0 + b_1x + ... + b_nx^n$$
$$c(x) = c_0 + c_1x + ... + c_nx^n$$

Dobbiamo verificare che A[x] con la sola somma è un anello commutativo. Per quanto riguarda l'associatività si ha che

$$a(x) + [b(x) + c(x)] = a(x) + [(b_0 + c_0) + (b_1 + c_1)x + ... + (b_n + c_n)x^n] = [a_0 + (b_0 + c_0)] + [a_1 + (b_1 + c_1)]x + \\ + ... + [a_n + (b_n + c_n)]x^n = [(a_0 + b_0) + c_0] + [(a_1 + b_1) + c_1]x + ... + [(a_n + b_n) + c_n]x^n = [(a_0 + b_0) + \\ + (a_1 + b_1)x + ... + (a_n + b_n)x^n] + c(x) = [a(x) + b(x)] + c(x)$$

Per quanto riguarda la proprietà commutativa si ottiene che

$$a(x) + b(x) = [(a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n] = [(b_0 + a_0) + (b_1 + a_1)x + ... + (b_n + a_n)x^n] = b(x) + a(x)$$

Il polinomio nullo definito in precedenza, cioè lo 0, è l'elemento neutro per quanto riguarda la somma, e l'opposto di ogni polinomio $a(x)$ è il polinomio -$a(x)$ = (-a_0) + (-a_1)x + ... + (-a_n)x^n. Dunque l'insieme A[x] è un anello commutativo.
Per provare l'associatività del prodotto, consideriamo $b(x)c(x) = d(x)$, dove $d(x) = d_0 + d_1x + ... + d_{2n}x^{2n}$; per definizione di prodotto di polinomio, il k-esimo coefficiente di $b(x)c(x)$ sarà dato da

$$d_k = \sum_{i+j=k} b_ic_j$$

Dunque $a(x)[b(x)c(x)] = a(x)d(x) = e(x)$, con $e(x) = e_0 + e_1x + ... + e_{3n}x^{3n}$. Si ha che l-esimo coefficiente di $a(x)d(x)$ sarà dato da

$$e_l = \sum_{h+i+j=l} a_hb_ic_j$$

Per ogni l da 0 a 3n, e_l è il coefficiente del polinomio $a(x)[b(x)c(x)]$. Ripetendo lo stesso processo per trovare l'l-esimo coefficiente di $[a(x)b(x)]c(x)$, si otterrà proprio e_l, e dunque

$$a(x)[b(x)c(x)] = [a(x)b(x)]c(x)$$

Consideriamo $a(x)[b(x) + c(x)] = d(x)$, dove $d(x) = d_0 + d_1x + ... + d_{2n}x^{2n}$; per definizione di addizione e di prodotto tra polinomi, il k-esimo coefficiente di $a(x)[b(x) + c(x)]$ è dato da

$$d_k = \sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} (a_ib_j + a_ic_j) = \sum_{i+j=k} (a_ib_j) + \sum_{i+j=k} (a_ic_j)$$

Ma $\sum_{i+j=k} (a_ib_j)$ è il k-esimo coefficiente di $a(x)b(x)$, e $\sum_{i+j=k} (a_ic_j)$ è il k-esimo coefficiente di $a(x)c(x)$, così il coefficiente d_k è uguale al k-esimo coefficiente di $a(x)b(x) + a(x)c(x)$, cioè

$$a(x)[b(x) + c(x)] = a(x)b(x) + a(x)c(x)$$

Per provare la commutatività del prodotto, consideriamo $a(x)b(x) = d(x)$, dove $d(x) = d_0 + d_1x + ... + d_{2n}x^{2n}$; per definizione di prodotto di polinomi, il k-esimo coefficiente di $a(x)b(x)$ sarà dato da

$$d_k = \sum_{i+j=k} a_ib_j$$

Ma $\sum_{i+j=k} a_ib_j = \sum_{i+j=k} b_ia_j$, che è il k-esimo coefficiente del polinomio $e(x) = b(x)a(x)$. Dunque risulta che $a(x)b(x) = b(x)a(x)$. Il polinomio unità, sarà il polinomio costante 1.
Dunque A[x] è un anello commutativo con unità. □

Teorema 16. *Se A è un dominio di integrità, allora A[x] è un dominio di integrità.*

Dimostrazione. Consideriamo $a(x)$ e $b(x)$ polinomi non nulli in A[x]. Sia a_n il coefficiente direttore di $a(x)$ e b_m il coefficiente direttore di $b(x)$; per definizione di coefficiente direttore, $a_n \neq 0$ e $b_m \neq 0$. Dunque $a_nb_m \neq 0$ perché A è un dominio di integrità. Segue che $a(x)b(x)$ ha un coefficiente non nullo, a_nb_m, per cui non può essere il polinomio nullo. Dunque A[x] è un dominio di integrità. □

Osservazione 1.2.6. *Sia A un dominio di integrità, chiameremo A[x] dominio di polinomi. Se a_n e b_m sono rispettivamente i coefficienti direttori di a(x) e b(x), allora $a_n b_m$ è il coefficiente direttore del polinomio a(x)b(x). Dunque, in un un dominio di polinomi A[x], dove A è un dominio di integrità, si ha che*

$$deg[a(x)b(x)] = deg(a(x)) + deg(b(x))$$

Corollario 1.2.1. *Sia F un campo. Allora F[x] è un dominio di integrità.*

Dimostrazione. Bisogna dimostrare che F è un dominio di integrità, cioè che F non ammette divisori dello zero. Sia a un elemento non nullo in F e sia b un elemento di F tale che $ab = 0$. Dal momento che a è non nullo, essendo F un campo, esiste a^{-1} inverso di a. Moltiplicando ambo i membri di $ab = 0$, per a^{-1} si ottiene $b = 0$. Dunque F è un dominio di integrità e per il teorema 16 tale è anche F[x]. □

Teorema 17 (Algoritmo di divisione per polinomi)**.** *Se a(x) e b(x) sono polinomi su un campo F, e $b(x) \neq 0$, allora esistono q(x) e r(x) su F tali che*

$$a(x) = b(x)q(x) + r(x)$$

con r(x) = 0 o deg(r(x)) < deg(b(x)).
Inoltre la coppia di polinomi q(x) e r(x) è univocamente determinata.

Dimostrazione. Supponiamo che $b(x)$ rimanga fissato, dimostreremo che ogni polinomio $a(x)$ soddisfa alla seguente condizione:

(*) Esistono $q(x)$ e $r(x)$ polinomi su F tali che $a(x) = b(x)q(x) + r(x)$, con $r(x) = 0$ o $\deg(r(x)) < \deg(b(x))$.

Supponiamo per assurdo che esista un polinomio in F[x] che non soddisfi alla suddetta condizione. Sia $a(x)$ il polinomio di grado minore che non soddisfa alla condizione (*); sicuramente $a(x) \neq 0$, perché altrimenti $0 = 0b(x)+0$ e soddisferebbe la condizione (*). Risulta impossibile che $\deg(a(x)) < \deg(b(x))$, perché altrimenti si avrebbe $a(x) = 0b(x) + a(x)$ e $a(x)$ soddisferebbe la condizione (*), per cui si ha che $\deg(a(x)) \geq \deg(b(x))$. Sia $a(x) = a_0 + a_1x + ... + a_nx^n$ e $b(x) = b_0 + b_1x + ... + b_mx^m$ (chiaramente n ≥ m). Possiamo definire un nuovo polinomio, come

$$A(x) = a(x) - \frac{a_n}{b_m}x^{n-m}b(x) = a(x) - (b_0\frac{a_n}{b_m}x^{n-m} + b_1\frac{a_n}{b_m}x^{n-m+1} + ... + b_m\frac{a_n}{b_m}x^{n-m+m}) = a(x) + \\ - (b_0\frac{a_n}{b_m}x^{n-m} + b_1\frac{a_n}{b_m}x^{n-m+1} + ... + a_nx^n)$$

Dunque $A(x)$ è differenza di due polinomi entrambi di grado n aventi lo stesso coefficiente direttore, perciò $A(x)$ ha grado minore di n, e dal momento che $a(x)$ era il polinomio di grado minimo che non soddisfaceva la condizione (*), $A(x)$ soddisfa la condizione (*): per cui esistono polinomi $p(x)$ e $r(x)$ a coefficienti in F tali che

$$A(x) = b(x)p(x) + r(x)$$

con $r(x) = 0$ o $\deg(r(x)) < \deg(b(x))$. Ma allora

$$a(x) = A(x) + \frac{a_n}{b_m}x^{n-m}b(x) = b(x)p(x) + r(x) + \frac{a_n}{b_m}x^{n-m}b(x) = b(x)(p(x) + \frac{a_n}{b_m}x^{n-m}) + r(x).$$

Ponendo $(p(x) + \frac{a_n}{b_m}x^{n-m}) = q(x)$, si ha che $a(x) = b(x)q(x) + r(x)$, e ciò è un assurdo. Dunque il polinomio $a(x)$ soddisfa alla condizione (*).
Per quanto riguarda l'unicità della coppia $q(x)$ e $r(x)$, supponiamo per assurdo che $a(x) = b(x)q_1(x) + r_1(x) = = b(x)q_2(x) + r_2(x)$. Sottraendo membro a membro queste due equazioni, risulta

$$r_2(x) - r_1(x) = b(x)[q_1(x) - q_2(x)]$$

Il polinomio $b(x)[q_1(x) - q_2(x)]$ ha grado uguale alla somma dei gradi dei polinomi $b(x)$ e $(q_1(x) - q_2(x))$ ed è uguale al polinomio $(r_2(x) - r_1(x))$ che se fosse non nullo avrebbe grado minore del grado di $b(x)$, poiché il grado di ciascun $r_i(x)$ è minore del grado di $b(x)$; dunque, per non cadere in assurdo, si dovrà avere che $(r_2(x) - r_1(x)) = 0$, cioè $r_2(x) = r_1(x)$; e di conseguenza da $b(x)[q_1(x) - q_2(x)] = 0$, ricordando che $b(x) \neq 0$ e che F[x] è un dominio di integrità, risulterà che $(q_1(x) - q_2(x)) = 0$, cioè $q_1(x) = q_2(x)$.
Resta così provata l'unicità della coppia $q(x)$ $r(x)$ nel processo di divisione tra polinomi su un campo F. □

Teorema 18. *Sia F un campo, allora ogni ideale di F[x] è un ideale principale.*

Dimostrazione. Sia J un ideale di F[x]. Se J contiene solamente l'elemento 0, allora J è l'ideale principale generato da 0. In caso contrario J conterrà polinomi non nulli; sia $b(x)$ il polinomio non nullo di grado minimo in J e sia $a(x)$ un altro polinomio di J. Per l'algoritmo di divisione dei polinomi (teorema 17), avremo che $a(x) = b(x)q(x) + r(x)$, con $r(x) = 0$ o $\deg(r(x)) < \deg(b(x))$. Segue che $r(x) = a(x)$ - $b(x)q(x)$ e dal momento che $a(x)$, $b(x) \in$ J che è un'ideale, per definizione si ha che $b(x)q(x) \in$ J e $[a(x)$ - $b(x)q(x)] = r(x) \in$ J. Se $r(x)$ è non nullo, allora il suo grado è minore del grado di $b(x)$, ma ciò è un assurdo in quanto $b(x)$ è il polinomio di grado minore in J. Dunque $r(x)$ deve coincidere col polinomio nullo e si ha $a(x) = b(x)q(x)$, cioè J è un ideale principale generato dall'elemento $b(x)$, cioè J $= \langle b(x) \rangle$. □

Definizione 1.2.21. *Sia F un campo e siano a(x) e b(x) in F[x]. Diremo che b(x) è un multiplo di a(x) se*

$$b(x) = a(x)s(x)$$

per un polinomio s(x) in F[x]. Se b(x) è un multiplo di a(x), possiamo anche dire che a(x) è un fattore di b(x), o che a(x) divide b(x), cioè, in simboli

$$a(x) \mid b(x)$$

Osservazione 1.2.7. *Ogni polinomio costante non nullo divide ogni polinomio; infatti consideriamo il polinomio $c \neq 0$ e il polinomio $a(x) = a_0 + a_1x + \ldots + a_nx^n$, si avrà che*

$$a(x) = a_0 + a_1x + \ldots + a_nx^n = c(\tfrac{a_0}{c} + \tfrac{a_1}{c}x + \ldots + \tfrac{a_n}{c}x^n)$$

per cui $c \mid a(x)$.
Un polinomio a(x) è invertibile se e solo se è un divisore del polinomio unità 1. Questo vuol dire che supposto a(x) invertibile, si avrà $a(x)b(x) = 1$, cioè a(x) e b(x) sono entrambi di grado zero, per cui saranno polinomi costanti $a(x) = a$ e $b(x) = b$. Segue dunque che gli elementi invertibili di F[x] sono unicamente i polinomi costanti non nulli.

Definizione 1.2.22. *Una coppia di polinomi non nulli a(x) e b(x) sono detti associati se si dividono l'un l'altro, cioè se $a(x) \mid b(x)$ e $b(x) \mid a(x)$.*

Proposizione 1.2.3. *Gli elementi a(x) e b(x) in F[x] sono associati se e solo se sono ciascuno un multiplo costante dell'altro.*

Dimostrazione. Supponiamo che $a(x)$ e $b(x)$ siano associati; esistono dunque polinomi $c(x)$ e $d(x)$ tali che $a(x) = b(x)c(x)$ e $b(x) = a(x)d(x)$, da cui si ha

$$a(x) = b(x)c(x) = a(x)d(x)c(x)$$

per cui per la legge di cancellazione si ha $d(x)c(x) = 1$, e dunque, per l'osservazione 1.2.7, $d(x)$ e $c(x)$ sono polinomi costanti. □

Definizione 1.2.23. *Se $a(x) = a_0 + a_1x + \ldots + a_nx^n$, gli associati di a(x) sono tutti i suoi multipli costanti non nulli. Tra tutti questi polinomi, il polinomio uguale a $\frac{1}{a_n}a(x)$, avrà come coefficiente direttore 1. Ogni polinomio il cui coefficiente direttore è 1, è detto polinomio monico; dunque ogni polinomio non nullo a(x) ha un unico polinomio monico associato.*

Definizione 1.2.24. *Un polinomio d(x) è detto massimo comune divisore, MCD, di a(x) e b(x) se:*

1. *$d(x) \mid a(x)$ e $d(x) \mid b(x)$*
2. *per ogni altro u(x) in F[x] tale che $u(x) \mid a(x)$ e $u(x) \mid b(x)$, allora $u(x) \mid d(x)$.*

Due diversi MCD di a(x) e b(x) si dividono tra loro, e perciò sono associati. Tra tutti i possibili MCD di a(x) e b(x) sceglieremo quello monico, che chiameremo il massimo comune divisore di a(x) e b(x) e lo indicheremo con MCD[a(x), b(x)].

Teorema 19. *Ogni coppia di polinomi non nulli a(x) e b(x) in F[x] ha un MCD d(x). Inoltre, d(x) può essere espresso come combinazione lineare*

$$d(x) = r(x)a(x) + s(x)b(x)$$

dove r(x) e s(x) sono polinomi in F[x].

Dimostrazione. Sia J l'insieme di tutte le combinazioni lineari del tipo

$$u(x)a(x) + v(x)b(x)$$

dove $u(x)$ e $v(x)$ variano in F[x]; è di facile verifica che J sia un ideale di F[x], e poiché F[x] è un dominio ad ideali principali si avrà che J = $\langle d(x) \rangle$, cioè J è l'ideale principale generato da $d(x)$. Si ha che $a(x) = 1a(x) + 0b(x)$ e che $b(x) = 0a(x) + 1b(x)$, dunque $a(x)$ e $b(x)$ sono elementi di J. Ma ogni elemento di J è un multiplo di $d(x)$, per cui

$$d(x) \mid a(x) \text{ e } d(x) \mid b(x).$$

Sia $k(x)$ un altro divisore comune di $a(x)$ e $b(x)$, per cui esisteranno polinomi $f(x)$ e $g(x)$ tali che $a(x) = k(x)f(x)$ e $b(x) = k(x)g(x)$. Dal momento che $d(x) \in$ J, risulta che $d(x)$ può essere scritto come

$$d(x) = r(x)a(x) + s(x)b(x) = r(x)k(x)f(x) + s(x)k(x)g(x) = k(x)[r(x)f(x) + s(x)g(x)]$$

da cui $k(x) \mid d(x)$ che risulta dunque essere il MCD di $a(x)$ e $b(x)$. □

Definizione 1.2.25. *Due polinomi a(x) e b(x) in F[x] sono detti primi tra loro se il loro MCD è uguale a 1.*

Definizione 1.2.26. *Un polinomio a(x) di grado positivo è riducibile su F se esistono polinomi b(x) e c(x) in F[x], entrambi di grado positivo, tali che a(x) = b(x)c(x).*
Dal momento che b(x) e c(x) hanno entrambi un grado positivo e la somma dei loro gradi è il grado di a(x), allora ciascuno dei gradi di b(x) e c(x) deve essere minore del grado di a(x).

Definizione 1.2.27. *Un polinomio p(x) di grado positivo in F[x] è detto irriducibile su F se esso non può essere espresso come prodotto di due polinomi di grado positivo in F[x]. Dunque p(x) è irriducibile se e solo se è non riducibile.*

Proposizione 1.2.4. *Sia F un campo e sia p(x) un polinomio irriducibile in F[x], allora J = $\langle p(x) \rangle$ è un ideale massimale di F[x]*

Dimostrazione. Supponiamo per assurdo che J = $\langle p(x) \rangle$ non sia massimale, per cui esiste un ideale proprio di F[x], chiamiamolo K, tale che J ⊆ K. Poiché F[x] è un dominio ad ideali principali si ha che K = $\langle b(x) \rangle$, e dal momento che $p(x) \in$ K, si ha che $p(x) = h(x)b(x)$, con $h(x)$ polinomio in F[x]. Ma ciò è un assurdo in quanto avevamo supposto $p(x)$ polinomio irriducibile su F. Dunque J = $\langle p(x) \rangle$ è un ideale massimale di F[x]. □

Lemma 1 (Lemma di Euclide per polinomi)**.** *Sia F un campo e sia p(x) irriducibile su F. Se p(x) | a(x)b(x) allora p(x) | a(x) o p(x) | b(x).*

Dimostrazione. Se $p(x)$ divide $a(x)$ il teorema è dimostrato. Dunque supponiamo che $p(x)$ non divida $a(x)$. Dal momento che $p(x)$ non divide $a(x)$ e che $a(x)$ non divide $p(x)$, segue che MCD[p(x), a(x)] = 1, per cui per il teorema 19 si avrà che

$$1 = k(x)p(x) + f(x)a(x)$$

con $k(x)$ e $f(x)$ polinomi di F[x]. Moltiplicando ambo i membri dell'equazione precedente per $b(x)$, si ottiene

$$k(x)p(x)b(x) + f(x)a(x)b(x) = b(x)$$

ma $p(x)$ divide $a(x)b(x)$, per cui esiste un polinomio $h(x)$ in F[x] tale che $a(x)b(x) = p(x)h(x)$, per cui sostituendo nell'equazione precedente si ha

$$k(x)p(x)b(x) + f(x)p(x)h(x) = p(x)[k(x)b(x) + f(x)h(x)] = b(x)$$

Per cui $p(x)$ divide $b(x)$. □

Corollario 1.2.2. *Sia F un campo e sia p(x) irriducibile su F. Se $p(x)|a_1(x)a_2(x)\cdots a_n(x)$, allora p(x) | a_i(x) per uno dei fattori a_i tra a_1(x), ..., a_n(x).*

Corollario 1.2.3. *Sia F un campo, e siano q_1(x), ..., q_r(x) e p(x) polinomi monici irriducibili su F. Se $p(x)|q_1(x)q_2(x)\cdots q_r(x)$ allora p(x) è uguale a uno dei fattori q_1(x), ..., q_r(x)*

Teorema 20 (Fattorizzazione in polinomi irriducibili)**.** *Sia F un campo. Ogni polinomio a(x) di grado positivo in F[x] può essere scritto come un prodotto*

$$a(x) = k\, p_1(x)p_2(x)\cdots\ p_r(x)$$

dove k è una costante in F e p_1, ..., p_r sono polinomi monici irriducibili di F[x].

Dimostrazione. Supponiamo che esistano polinomi che non soddisfano al teorema, e sia $a(x)$ il polinomio di grado minimo tra quelli che non possono essere fattorizzati come prodotto di polinomi irriducibili. Dunque $a(x)$ è un polinomio riducibile, per cui esistono polinomi $b(x)$ e $c(x)$ in F[x] tali che $a(x) = b(x)c(x)$, dove $b(x)$ e $c(x)$ hanno grado minore del grado di $a(x)$. Dunque $b(x)$ e $c(x)$ posso essere fattorizzati come prodotto di polinomi irriducibili, e perciò anche $a(x)$ può essere fattorizzato come prodotto di polinomi irriducibili. □

Teorema 21. *Se a(x) può essere fattorizzato in due differenti modi come prodotto di polinomi irriducibili, cioè*

$$a(x) = k\, p_1(x)p_2(x) \cdots\ p_r(x) = l\, q_1(x)q_2(x) \cdots\ q_s(x)$$

allora $k = l$, $r = s$ e ciascun p_i è uguale a qualche q_j

Dimostrazione. Nell'equazione $kp_1(x)p_2(x)\cdots p_r(x) = lq_1(x)q_2(x)\cdots q_s(x)$, cancelliamo i fattori comuni a entrambi i membri, uno per uno, finché ci è possibile farlo. Se abbiamo cancellato tutti i fattori, allora il teorema è dimostrato; altrimenti avremo che

$$kp_i(x)\cdots p_k(x) = lq_j(x)\cdots q_t(x)$$

Ora, p_i è un fattore di $kp_i(x)\cdots p_k(x)$, così, per il corollario 1.2.3, si ha che p_i è uguale a uno dei fattori $q_j(x), ..., q_t(x)$, ma ciò è impossibile perché avevamo supposto che non ci fossero più elementi in comune in entrambi i membri dell'equazione iniziale.
Una volta cancellati tutti i polinomi, risulta $k = l$, e il teorema è dimostrato. □

1.3 Spazi vettoriali

Definizione 1.3.1. *Uno spazio vettoriale su un campo K è un insieme V, dotato di due operazione + e · chiamate somma di vettori e prodotto scalare, tali che*

1. *V con la somma di vettori sia un gruppo abeliano.*
2. *Per ogni $k \in K$ e $\boldsymbol{a} \in V$, il prodotto scalare $k\boldsymbol{a}$ è un elemento di V, soddisfacente alle seguenti condizioni: per ogni k, $l \in K$ e $\boldsymbol{a}$, $\boldsymbol{b} \in V$*
   - *$k(\boldsymbol{a} + \boldsymbol{b}) = k\boldsymbol{a} + k\boldsymbol{b}$*
   - *$(k + l)\boldsymbol{a} = k\boldsymbol{a} + l\boldsymbol{a}$*
   - *$k(l\boldsymbol{a}) = (kl)\boldsymbol{a}$*
   - *$1\boldsymbol{a} = \boldsymbol{a}$*

Gli elementi di V sono detti vettori e gli elementi di K sono detti scalari.

Osservazione 1.3.1. *Sia V uno spazio vettoriale. Poiché V con la sola somma di vettori è un gruppo abeliano, esiste un elemento in V chiamato vettore nullo, che indicheremo con $\boldsymbol{0}$; inoltre ogni vettore $\boldsymbol{a}$ in V ha un opposto indicato con $-\boldsymbol{a}$.*

Teorema 22. *Sia V uno spazio vettoriale, allora:*

(a) $0\boldsymbol{a} = \boldsymbol{0}$, per ogni $\boldsymbol{a} \in V$.

(b) $k\boldsymbol{0} = \boldsymbol{0}$, per ogni scalare $k \in K$.

(c) Se $k\boldsymbol{a} = \boldsymbol{0}$, allora $k = 0$ o $\boldsymbol{a} = \boldsymbol{0}$.

(d) $(-1)\boldsymbol{a} = -\boldsymbol{a}$ per ogni $\boldsymbol{a} \in V$.

Dimostrazione. (a) Osserviamo che

$$0\boldsymbol{a} = (0 + 0)\boldsymbol{a} = 0\boldsymbol{a} + 0\boldsymbol{a}$$

dunque $\boldsymbol{0} + 0\boldsymbol{a} = 0\boldsymbol{a} + 0\boldsymbol{a}$, da cui per la legge di cancellazione si ottiene che $\boldsymbol{0} = 0\boldsymbol{a}$.

(b) Si ha

$$\mathrm{k}\boldsymbol{0} = \mathrm{k}(\boldsymbol{0} + \boldsymbol{0}) = \mathrm{k}\boldsymbol{0} + \mathrm{k}\boldsymbol{0}$$

dunque $\mathrm{k}\boldsymbol{0} + \boldsymbol{0} = \mathrm{k}\boldsymbol{0} + \mathrm{k}\boldsymbol{0}$, da cui per la legge di cancellazione si ottiene che $\mathrm{k}\boldsymbol{0} = \boldsymbol{0}$

(c) Se $\mathrm{k} = 0$, il teorema è dimostrato. Se $\mathrm{k} \neq 0$, possiamo moltiplicare $\mathrm{k}\boldsymbol{a} = \boldsymbol{0}$ per $\frac{1}{k}$, ottenendo $\boldsymbol{a} = \boldsymbol{0}$

(d) Abbiamo che:

$$\boldsymbol{a} + (-1)\boldsymbol{a} = 1\boldsymbol{a} + (-1)\boldsymbol{a} = (1 + (-1))\boldsymbol{a} = 0\boldsymbol{a} = \boldsymbol{0}$$

Dunque (-1)$\boldsymbol{a}$ = -$\boldsymbol{a}$

□

Definizione 1.3.2. *Sia V uno spazio vettoriale e sia $U \subseteq V$. Diremo che U è chiuso rispetto al prodotto scalare se $k\boldsymbol{a} \in U$ per ogni scalare k e per ogni $\boldsymbol{a} \in U$.*

Definizione 1.3.3. *Sia V uno spazio vettoriale e sia $U \subseteq V$. Diremo che U è un sottospazio di V se U è chiuso rispetto alla somma e al prodotto scalare.*

Definizione 1.3.4. *Se $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$ sono in V e k_1, k_2, ..., k_n sono scalari, allora il vettore*

$$k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + ... + k_n\boldsymbol{a}_n$$

è detto combinazione lineare dei vettori $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$. L'insieme di tutte le combinazioni lineari di $\boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n$ è un sottospazio di V.

Definizione 1.3.5. *Se U è il sottospazio consistente in tutte le combinazioni lineari di $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$ diremo che U è il sottospazio generato da $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$. In modo equivalente si ha che, U è generato da $\boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n$ se e solo se ogni vettore di U è una combinazione lineare di $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$.*
Se U è generato da $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$ possiamo anche dire che $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_n$ generano U

Definizione 1.3.6. *Sia $S = \{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n \}$ un insieme di vettori distinti nello spazio vettoriale V. Diremo che i vettori in S sono linearmente dipendenti se esistono scalari k_1, k_2, ..., k_n non tutti nulli tali che*

$$k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + ... + k_n\boldsymbol{a}_n = \boldsymbol{0}$$

Ciò è equivalente a dire che almeno uno dei vettori in S è combinazione lineare degli altri vettori di S.
Se $S = \{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n \}$ non sono linearmente dipendenti allora essi si dicono linearmente indipendenti. Cioè i vettori di S sono linearmente indipendenti se e solo se

$$k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + ... + k_n\boldsymbol{a}_n = \boldsymbol{0} \text{ implica } k_1 = k_2 = ... = k_n = 0$$

Cioè non esiste nessun vettore in S che sia uguale a una combinazione lineare degli altri vettori in S.

Osservazione 1.3.2. *Un qualsiasi insieme di vettori contenente il vettore nullo è un insieme di vettori linearmente dipendenti. Inoltre, l'insieme $\{\boldsymbol{a}\}$, contenente un unico vettore non nullo $\boldsymbol{a}$, è un insieme di vettori linearmente indipendenti.*

Lemma 2. *Se $\{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n \}$ è un insieme di vettori linearmente dipendenti allora qualche $\boldsymbol{a}_i$ è una combinazione lineare dei vettori precedenti $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_{i-1}$.*

Dimostrazione. Dal momento che $\{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n \}$ è un insieme di vettori linearmente dipendenti, allora $k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + ... + k_n\boldsymbol{a}_n = \boldsymbol{0}$ per coefficienti k_1, k_2, ..., k_n non tutti nulli. Se k_i è l'ultimo coefficiente non nullo tra loro, allora si ha che $k_1\boldsymbol{a}_1 + k_2\boldsymbol{a}_2 + ... + k_i\boldsymbol{a}_i = 0$, e questa equazione può essere risolta in $\boldsymbol{a}_i$ in termini di $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, ..., $\boldsymbol{a}_{i-1}$. □

Con la notazione $\{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \cancel{\boldsymbol{a}_i}, ..., \boldsymbol{a}_n \}$ intenderemo l'insieme $\{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n \}$ dopo la rimozione del vettore $\boldsymbol{a}_i$.

Lemma 3. *Se $\{\boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n\}$ genera V e $\boldsymbol{a}_i$ è una combinazione lineare dei precedenti vettori, allora $\{\boldsymbol{a}_1, \boldsymbol{a}_2, ..., \cancel{\boldsymbol{a}_i}, ..., \boldsymbol{a}_n\}$ genera ancora V.*

Dimostrazione. Per ipotesi abbiamo che $\boldsymbol{a}_i = k_1\boldsymbol{a}_1 + ... + k_{i-1}\boldsymbol{a}_{i-1}$ per qualche scalare k_1, ..., k_{i-1}. Dal momento che ogni vettore $\boldsymbol{b} \in$ V è una combinazione lineare del tipo

$$\boldsymbol{b} = l_1\boldsymbol{a}_1 + ... + l_i\boldsymbol{a}_i + ... + l_n\boldsymbol{a}_n$$

esso può essere anche scritto come

$$\boldsymbol{b} = l_1\boldsymbol{a}_1 + ... + l_i(k_1\boldsymbol{a}_1 + ... + k_{i-1}\boldsymbol{a}_{i-1}) + ... + l_n\boldsymbol{a}_n$$

in cui non compare $\boldsymbol{a}_i$. Dunque $\{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \cancel{\boldsymbol{a}_i}, ..., \boldsymbol{a}_n \}$ genera ancora V. □

Definizione 1.3.7. *Un insieme di vettori $\{ \boldsymbol{a}_1, \boldsymbol{a}_2, ..., \boldsymbol{a}_n \}$ è detto una base di V se è un insieme di vettori linearmente indipendenti e se tale insieme genera V.*

Teorema 23. *Due qualsiasi basi di uno stesso spazio vettoriale V hanno lo stesso numero di elementi.*

Dimostrazione. Supponiamo per assurdo che V abbia una base A = { $\boldsymbol{a}_1$, ..., $\boldsymbol{a}_n$ } e una base B = {$\boldsymbol{b}_1, ..., \boldsymbol{b}_m$}. Supponiamo n < m. Posto il vettore $\boldsymbol{b}_1$ nell'insieme A, adesso A conterrà { $\boldsymbol{b}_1$, $\boldsymbol{a}_1$, ..., $\boldsymbol{a}_n$ } e tale insieme sarà un insieme di vettori linearmente dipendenti, dal momento che $\boldsymbol{b}_1$ può essere scritto come combinazione lineare dei vettori $\boldsymbol{a}_1$, ..., $\boldsymbol{a}_n$. Per il lemma 2, qualche $\boldsymbol{a}_i$ è combinazione lineare dei precedenti vettori e per il lemma 3 possiamo eliminare il vettore $\boldsymbol{a}_i$ ottenendo l'insieme { $\boldsymbol{b}_1$, $\boldsymbol{a}_1$, ..., $\cancel{\boldsymbol{a}_i}$, ..., $\boldsymbol{a}_n$ } che ancora genera V. Ripetendo questo procedimento una seconda volta ponendo $\boldsymbol{b}_2$ in A = { $\boldsymbol{b}_1$, $\boldsymbol{a}_1$, ..., $\cancel{\boldsymbol{a}_i}$, ..., $\boldsymbol{a}_n$ } si ottiene l'insieme $A = \{\boldsymbol{b}_2, \boldsymbol{b}_1, \boldsymbol{a}_1, ..., \cancel{\boldsymbol{a}_i}, ..., \boldsymbol{a}_n\}$; questo è un insieme di vettori linearmente dipendenti perché $\{\boldsymbol{b}_1, \boldsymbol{a}_1, ..., \cancel{\boldsymbol{a}_i}, ..., \boldsymbol{a}_n\}$ genera V e dunque $\boldsymbol{b}_2$ è combinazione lineare dei vettori $\boldsymbol{b}_1$, $\boldsymbol{a}_1$, ..., $\cancel{\boldsymbol{a}_i}$, ..., $\boldsymbol{a}_n$. Per il lemma 2, qualche $\boldsymbol{a}_j$ è combinazione lineare dei precedenti vettori in A e per il lemma 3 possiamo eliminare il vettore $\boldsymbol{a}_j$ ottenendo l'insieme { $\boldsymbol{b}_2$, $\boldsymbol{b}_1$, $\boldsymbol{a}_1$, ..., $\cancel{\boldsymbol{a}_i}$, ..., $\cancel{\boldsymbol{a}_j}$, ..., $\boldsymbol{a}_n$ } che ancora genera V.
Questo procedimento può essere iterato n volte. Ogni volta un vettore di B è posto in A e un vettore $\boldsymbol{a}_k$ in A può essere eliminato ottenendo ancora un insieme che genera V. Dopo l'n-esima iterazione, A contiene solo i vettori $\boldsymbol{b}_1$, ..., $\boldsymbol{b}_n$ e l'insieme { $\boldsymbol{b}_1$, ..., $\boldsymbol{b}_n$ } ancora genera V. Ma ciò è impossibile perché in tal modo il vettore $\boldsymbol{b}_{n+1}$ è una combinazione lineare di $\boldsymbol{b}_1$, ..., $\boldsymbol{b}_n$, in contrasto con l'ipotesi che B = { $\boldsymbol{b}_1$, ..., $\boldsymbol{b}_n$, ..., $\boldsymbol{b}_m$ } sia un insieme di vettori linearmente indipendenti.
Questa contraddizione mostra che due diverse basi di V devono avere lo stesso numero di elementi. □

Definizione 1.3.8. *Se lo spazio vettoriale V ha base A = { $\boldsymbol{a}_1$, ..., $\boldsymbol{a}_n$ }, diremo che V è uno spazio vettoriale di dimensione finita e diremo che V ha dimensione n. Dunque per il teorema precedente, ogni base di V ha esattamente n elementi.*

Definizione 1.3.9. *Siano U e V due spazi vettoriali su un campo K, una funzione h: U $\longrightarrow$ V è detta omomorfismo se essa soddisfa le seguenti due condizioni:*

a $h(\boldsymbol{a} + \boldsymbol{b}) = h(\boldsymbol{a}) + h(\boldsymbol{b})$

b $h(k\boldsymbol{a}) = kh(\boldsymbol{a})$

dove k è uno scalare. Un omomorfismo di spazi vettoriali è anche detto applicazione lineare.

Capitolo 2

Teoria dei campi

2.1 Estensioni di campi

Definizione 2.1.1. *Sia F un campo, allora un sottocampo di F è un sottoinsieme non vuoto di F che è chiuso rispetto all'addizione e al passaggio all'opposto, rispetto al prodotto e al passaggio all'inverso.*

Definizione 2.1.2. *Se K è un sottocampo di F, possiamo dire che F un un'estensione di campo di K. Qualora sia chiaro dal contesto che sia F che K siano campi, diremo semplicemente che F è un'estensione di K.*

Per quale motivo siamo interessati alla ricerca delle estensioni dei campi?
Se F è un campo arbitrario, esistono polinomi su F che non hanno radici in F. Ma ogni polinomio su un qualunque campo F, ha radici; se queste radici non si trovano in F si troveranno in un'adatta estensione del campo considerato.
In un campo arbitrario F un polinomio di grado n può avere un qualsiasi numero di radici, da 0 a n. Risulterà comunque che F ha un'adatta estensione E tale che ogni polinomio *a(x)* di grado n su F abbia esattamente n soluzioni (radici) in E. Questo è uno dei più importanti motivi per cui ci interessiamo alle estensioni di campo.

Definizione 2.1.3. *Sia E un campo, F un sottocampo di E, e c un qualsiasi elemento di E. Definiamo la funzione di sostituzione σ_c come:*

$$\sigma_c(a(x)) = a(c)$$

La funzione σ_c è una funzione da F[x] in E, ed è facile verificare che si tratta di un omomorfismo.

Il nucleo dell'omomorfismo σ_c è l'insieme di tutti i polinomi *a(x)* tali che $a(c) = \sigma_c(a(x)) = 0$, cioè è l'insieme di tutti i polinomi *a(x)* in F[x] tali che *c* è una radice di *a(x)*.
Indichiamo il nucleo di σ_c con J_c; dal momento che il nucleo di un omomorfismo è un ideale, risulta che J_c è un ideale di F[x].

Definizione 2.1.4. *Un elemento c di E è detto algebrico su F se è radice di un polinomio non nullo a(x) in F[x]; altrimenti tale elemento è detto trascendente su F.*
Chiaramente c è algebrico su F se e solo se J_c contiene polinomi non nulli, mentre c è trascendente su F se e solo se $J_c = \{0\}$.

Sia *c* algebrico su F e sia J_c il nucleo dell'applicazione σ_c. In F[x] ogni ideale è un ideale principale, per cui $J_c = \langle p(x) \rangle$, cioè J_c è l'insieme dei multipli di *p(x)*, con *p(x)* polinomio in F[x]. Dal momento che ogni polinomio di J_c è un multiplo di *p(x)*, risulta che *p(x)* è il *polinomio di grado minimo* tra tutti i polinomi non nulli in J_c.

Proposizione 2.1.1. *Sia p(x) il polinomio di grado minimo in J_c, allora p(x) è irriducibile.*

Dimostrazione. Supponiamo per assurdo che *p(x)* non sia irriducibile, per cui potremmo fattorizzarlo nel prodotto di due polinomi di grado minore, cioè $p(x) = f(x)g(x)$. Ricordando che *c* è una radice del polinomio *p(x)*, si avrebbe che $0 = p(c) = f(c)g(c)$, perciò sia *f(x)* che *g(x)* sono elementi di J_c. Ma ciò è assurdo in quanto *p(x)* è il polinomio di grado minimo in J_c, e dunque *p(x)* è irriducibile. □

Definizione 2.1.5. *Dal momento che ogni multiplo costante di p(x) è un elemento di J_c, possiamo scegliere p(x) in maniera tale che sia monico, cioè che abbia coefficiente direttore 1. Allora p(x) è l'unico polinomio monico di grado minimo in J_c. Questo polinomio p(x) è chiamato il polinomio minimo di c su F.*

Proposizione 2.1.2. *L'immagine di σ_c è un sottocampo di E.*

Dimostrazione. Dal momento che σ_c è un omomorfismo, la sua immagine è chiaramente chiusa rispetto a somma, prodotto e opposti. Per verificare che sia chiusa anche rispetto agli inversi, consideriamo l'elemento non nullo *f(c)* dell'immagine di σ_c; poichè *f(c)* è non nullo, allora *f(x)* non è un elemento di J_c. Dunque *f(x)* non è un multiplo di *p(x)*, e dal momento che che *p(x)* è irriducibile, risulterà che *f(x)* e *p(x)* sono primi tra loro. Perciò, per il teorema 19, esisteranno due polinomi *s(x)* e *t(x)*, tali che $s(x)f(x) + t(x)p(x) = 1$, da cui

$$s(c)f(c) + t(c)p(c) = s(c)f(c) + 0 = s(c)f(c) = 1$$

e perciò *s(c)* è l'inverso moltiplicativo di *f(c)*. Dunque l'immagine di σ_c è un sottocampo di E. □

L'immagine di σ_c è il più piccolo campo contenente F e c; infatti, ogni altro campo contenente F e c dovrà necessariamente contenere ogni elemento della forma:

$$a_0 + a_1c + ... + a_nc^n$$

con a_0, ..., $a_n \in$ F, cioè conterrà ogni elemento dell'immagine di σ_c.
Parlando del più piccolo campo contenente F ec, intendiamo che questo campo contiene F e c e che è contenuto in ogni altro campo contenente F e c. Questo campo è chiamato *campo generato da* F e c, e viene indicato col simbolo

$$\mathrm{F}(c)$$

Corollario 2.1.1. *σ_c è una applicazione con dominio F[x], immagine F(c) e nucleo J_c. Per il teorema fondamentale di omomorfismo (teorema 14) si ha*

$$F(c) \cong F[x]/\langle p(x)\rangle$$

Teorema 24 (Teorema fondamentale delle estensioni di campo)**.** *Sia F un campo e a(x) un polinomio non constante in F[x]. Allora esistono un estensione E di F e un elemento c di E tale che c sia una radice di a(x).*

Dimostrazione. Il polinomio *a(x)*, per il teorema 20, può essere fattorizzato in polinomi irriducibili in F[x]. Se *p(x)* è un fattore irriducibile non costante di *a(x)*, è sufficiente trovare una estensione di F contenente una radice di *p(x)*, dal momento che essa sarà anche una radice di *a(x)*
Se *p(x)* è irriducibile in F[x], allora, per la proposizione 1.2.4, l'ideale $\langle p(x)\rangle$ è un ideale massimale di F[x]. Inoltre, per la proposizione 1.2.2, se $\langle p(x)\rangle$ è un ideale massimale per F[x], allora l'anello quoziente F[x]/$\langle p(x)\rangle$ è un campo. Resta dunque da dimostrare che F[x]/$\langle p(x)\rangle$ è l'estensione di campo cercata.
Posto J = $\langle p(x)\rangle$, ogni elemento di F[x]/J è un laterale di J. Definiamo la funzione h: F $\longmapsto$ F[x]/J, in maniera tale che per ogni elemento di F si abbia $h(a) = \mathrm{J} + a$. Per le proprietà della somma e del prodotto di laterali, la funzione h così definita è un omomorfismo. Dal momento che ogni omomorfismo tra campi è iniettivo (questo è dovuto al fatto che il nucleo di un omomorfismo è un ideale ed un campo non ammette ideali non banali), risulta che h è un isomorfismo tra il suo dominio e la sua immagine. Dunque, F è isomorfo al sottocampo di F[x]/J contenente tutti i laterali di polinomi costanti. Questo sottocampo è perciò una copia isomorfa di F, che può essere identificata con F, per cui F[x]/J è un estensione di F.
Infine mostriamo che il laterale J + x è una radice di $p(x) = a_0 + a_1x + ... + a_nx^n$ in F[x]/J. Nell'insieme F[x]/J, i coefficienti del polinomio non saranno a_0, ..., a_n, ma i loro laterali J + a_0, ..., J + a_n. Posto

$$\mathrm{J} + a_0 = \overline{a}_0, ..., \mathrm{J} + a_n = \overline{a}_n \text{ e } \mathrm{J} + x = \overline{x}$$

avremo che

$$\overline{a}_0 + \overline{a}_1\overline{x} + ... + \overline{a}_n\overline{x}^n = (\mathrm{J} + a_0) + (\mathrm{J} + a_1)(\mathrm{J} + x) + ... + (\mathrm{J} + a_n)(J + x)^n = (\mathrm{J} + a_0) + (\mathrm{J} + a_1x) + ... + (\mathrm{J} + a_nx^n) = \mathrm{J} + p(x) = \mathrm{J}$$

□

Corollario 2.1.2. *Sia a(x) un polinomio di grado n in F[x]. Esiste un estensione di campo E di F che contiene tutte le n radici di a(x).*

2.2 Gradi delle estensioni di campo

Siano F e K campi. Se K è un'estensione di F, possiamo considerare K come uno spazio vettoriale su F. Possiamo trattare gli elementi di K come "vettori" e gli elementi di F come "scalari".

Definizione 2.2.1. *Se K, visto come spazio vettoriale su F, ha dimensione finita, diremo che K è un'estensione finita di F. Se la dimensione dello spazio vettoriale K è n, diremo che K è un'estensione di grado n su F e scriveremo*

$$[K : F] = n$$

Teorema 25. *Sia c un elemento algebrico su F, e sia p(x) il minimo polinomio di c su F, che supponiamo di grado n. Il grado di F(c) su F è uguale al grado di p(x).*

Dimostrazione. Sia $a(c)$ un qualsiasi elemento di F(c); utilizzando l'algoritmo di divisione euclidea per dividere $a(x)$ per $p(x)$ si ottiene

$$a(x) = p(x)q(x) + r(x)$$

con deg $r(x) \leq n - 1$. Da ciò si ottiene che:

$$a(c) = p(c)q(c) + r(c) = 0 + r(c) = r(c)$$

Perciò ogni elemento di F(c) è della forma $r(c)$ dove $r(x)$ ha grado minore o uguale a $n - 1$. Ciò significa che ogni elemento di F(c) può essere scritto nella forma

$$a_0 + a_1 c + ... + a_{n-1}c^{n-1}$$

che è una combinazione lineare di 1, c, c^2, ..., c^{n-1}. Dunque l'insieme {1, c, c^2, ..., c^{n-1} } genera F(c).
Per dimostrare che 1, c, c^2, ..., c^{n-1} sono linearmente indipendenti, supponiamo che $a_0+a_1c+...+a_{n-1}c^{n-1} = 0$. Se i coefficienti a_0, a_1, a_{n-1} fossero non tutti nulli, c sarebbe una radice di un polinomio non nullo di grado minore o uguale a $n - 1$; ma ciò è impossibile perché il polinomio minimo di c su F ha grado n. □

Lemma 4. *Sia E un'estensione finita di K e sia K un'estensione finita di F. Sia { a_1, a_2, ..., a_m } una base dello spazio vettoriale K su F e sia { b_1, b_2, ..., b_n } una base dello spazio vettoriale E su K. Allora l'insieme degli mn prodotti { a_ib_j } è una base dello spazio vettoriale E sul campo F.*

Dimostrazione. Sia c un elemento dello spazio vettoriale E su K, allora può essere scritto come $c = k_1b_1+...+k_nb_n$ con coefficienti k_i in K. Dal momento che ciascun k_i è un elemento dello spazio vettoriale K su F, si potrà scrivere come

$$k_i = l_{i1}a_1 + ... + l_{im}a_m$$

con coefficienti l_{ij} in F. Sostituendo, si ottiene

$$c = (l_{11}a_1 + ... + l_{1m}a_m)b_1 + ... + (l_{n1}a_1 + ... + l_{nm}a_m)b_n = \sum l_{ij}a_ib_j$$

che è una combinazione lineare dei prodotti a_ib_j con coefficienti l_{ij} in F.
Per provare che { a_ib_j } sono linearmente indipendenti supponiamo che $\sum l_{ij}a_ib_j = 0$, cioè

$$(l_{11}a_1 + ... + l_{1m}a_m)b_1 + ... + (l_{n1}a_1 + ... + l_{nm}a_m)b_n = 0$$

Poiché b_1, b_2, ..., b_n sono linearmente indipendenti risulta che $(l_{i1}a_1 + ... + l_{im}a_m) = 0$ per ogni i. Ma $a_1, a_2, ..., a_m$ sono linearmente indipendenti, cosi si avrà che $l_{ij} = 0$. □

Teorema 26. *Supponiamo che $F \subseteq K \subseteq E$, dove E è un'estensione finita di K e K è un'estensione finita di F. Allora E è un'estensione finita di F e si ha*

$$[E : F] = [E : K][K : F]$$

Proposizione 2.2.1. *Sia F un campo e K un'estensione finita di F. Allora [K : F] = 1 se e solo se K = F.*

Dimostrazione. Supponiamo che [K : F] = 1, allora esiste una base $\{\boldsymbol{a}\}$ per lo spazio vettoriale K su F. Per cui per ogni $k_i \in$ K si ha $k_i = f_i\boldsymbol{a}$ con $f_i \in$ F. Consideriamo la funzione h: F $\longrightarrow$ K che a ciascun scalare f_i associa il vettore $f_i\boldsymbol{a} = k_i$. Questa funzione è un omomorfismo; la funzione è suriettiva, infatti per ogni $k_i \in$ K esiste un $f_i \in$ F tale che $k_i = f_i\boldsymbol{a}$ (per definizione di spazio vettoriale). Inoltre tale funzione è anche iniettiva, infatti presi f_i e f_j in F aventi la stessa immagine **k** in K, si avrebbe $\mathbf{k} = f_i\boldsymbol{a} = f_j\boldsymbol{a}$, da cui risulta che f_i e f_j. Dunque la funzione h è un isomorfismo tra F e K.
Se il generatore $\boldsymbol{a}$ appartenesse a K $\setminus$ F, avremmo che preso **1** in K esisterebbe b in F tale che $\mathbf{1} = b\boldsymbol{a}$, per cui $b = \boldsymbol{a}^{-1}$. Per cui risulta che $\boldsymbol{a}$ è un elemento di F, e dunque anche ogni elemento di K è un elemento di F. Valendo dunque la doppia inclusione risulta che K = F.

Viceversa, supponendo che K = F, si consideri l'insieme $\{1\}$. Questo insieme è una base per lo spazio vettoriale K su F, infatti esso è un'insieme di vettori linearmente indipendenti ed inoltre genera K, infatti sia $\mathbf{k} \in$ K si ha che esiste k $\in$ F tale che $\mathbf{k} = \mathbf{k}$ 1. Dunque lo spazio vettoriale K su F ha dimensione 1. □

Se c è algebrico su F, diciamo che F(c) è ottenuto aggiungendo c ad F. Se c e d sono algebrici su F, noi possiamo prima aggiungere c a F, ottenendo in tal modo F(c), e poi aggiungere d a F(c); il campo risultante verrà indicato con F(c, d), ed è il più piccolo campo contenente F, c e d.
Se c_1, ..., c_n sono algebrici su F, indicheremo con F(c_1, ..., c_n) il più piccolo campo contenente F, c_1, ..., c_n; questo campo è ottenuto aggiungendo c_1, ..., c_n a F. Possiamo creare F(c_1, ..., c_n) passo per passo, aggiungendo volta per volta ciascun c_i.
Un'estensione F(c), ottenuta aggiungendo un singolo elemento a F, è chiamata *estensione semplice* di F; un'estensione F(c_1, ..., c_n), ottenuta aggiungendo un numero finito di elementi c_1, ..., c_n è detta *estensione iterata*.

Proposizione 2.2.2. *Ogni estensione finita è un'estensione iterata*

Dimostrazione. Sia K un'estensione finita di F avente grado n. Ciò vuol dire che ogni elemento di K è combinazione lineare di $a_1, ..., a_n$ con coefficienti in F; ma ogni campo contenente F e $a_1, ..., a_n$ contiene tutte le combinazioni lineari di $a_1, ..., a_n$; per cui K è il più piccolo campo contenente F e $a_1, ..., a_n$ e quindi risulta $K = F(a_1, ..., a_n)$. □

Teorema 27. *Se K è un'estensione finita di F, ogni elemento di K è algebrico su F.*

Dimostrazione. Sia K un'estensione di grado n su F, e sia c un qualunque elemento di K. Allora l'insieme $\{1, c, c^2, ..., c^n\}$ è linearmente dipendente, perché contiene $n+1$ vettori di uno spazio vettoriale K di dimensione n. Di conseguenza, esistono scalari a_0, ..., $a_n \in$ F non tutti nulli, tali che $a_0 + a_1c + ... + a_nc^n = 0$. Per cui c è una radice di un polinomio $a(x) = a_0 + a_1x + ... + a_nx^n$ in F[x]. □

Corollario 2.2.1. *Ogni estensione iterata F(c_1, ..., c_n), con c_1, ..., c_n algebrici su F, è un'estensione finita di F. Viceversa, ogni estensione finita di F è un'estensione iterata F(c_1, ..., c_n), dove c_1, ..., c_n sono algebrici su F.*

Capitolo 3

Costruzioni con riga e compasso

Per i geometri dell'antica Grecia la circonferenza e la retta erano le figure geometriche più basilari e le altre figure geometriche non erano altro che varianti e combinazioni di queste ultime. Le costruzioni nella Grecia antica giocavano un ruolo fondamentale: infatti, ogni qualvolta una figura geometrica veniva definita, veniva anche fornito un metodo per costruirla. La circonferenza e la retta sono le figure più semplici da costruire e la loro costruzione necessita dei più basilari strumenti geometrici: una riga non graduata e un compasso.
Per quanto questi strumenti possano sembrare rudimentali possono essere utilizzati per effettuare una sorprendente varietà di costruzioni geometriche. Ad esempio ogni segmento può essere diviso in un qualsiasi numero di segmenti tra loro identici, ogni angolo può essere bisecato; dato un qualsiasi poligono è inoltre possibile costruire un quadrato che abbia la sua stessa area o un multiplo della stessa.
La loro abilità nelle costruzioni geometriche era tale che risulta difficile credere che non fossero in grado di risolvere tre piccoli problemi: duplicare un cubo, trisecare un qualsiasi angolo e quadrare un cerchio. Il primo problema riguarda la costruzione di un cubo che abbia volume doppio di un cubo dato, il secondo problema riguarda la divisione in tre angoli uguali di un angolo qualsiasi e il terzo problema riguarda la costruzione di un quadrato la cui area sia uguale a quella di un dato cerchio.
I matematici, nella Grecia antica così come in tutto il Rinascimento, provarono con grandi sforzi a dare risposta a questi problemi, ma non riuscirono mai a risolverli. Questo fatto non deve sorprendere, dal momento che queste costruzioni sono impossibili.
La risoluzione di questi problemi deriva da alcuni studi sulle estensioni di campi nelle ricerche superiori di algebra moderna.

Sia $\boldsymbol{A}$ un insieme di punti del piano; su questo insieme potremo svolgere le seguenti operazioni:

1. *Operazioni con la riga*: attraverso due qualsiasi punti di $\boldsymbol{A}$, tracciare una retta.
2. *Operazioni con il compasso*: dati tre punti A, B e C in $\boldsymbol{A}$ disegnare un cerchio con centro in C e raggio uguale alla lunghezza del segmento AB.

I punti di intersezione di due qualunque di queste figure (retta-retta, retta-circonferenza, circonferenza-circonferenza) si dicono *costruibili in un passo* da $\boldsymbol{A}$. Un punto P è detto *costruibile* da $\boldsymbol{A}$ se esistono i punti P_1, P_2, ..., $P_n = P$ tali che P_1 sia costruibile in un passo da $\boldsymbol{A}$, P_2 sia costruibile in un passo da $\boldsymbol{A} \cup \{P_1\}$ e così via, in maniera tale che P_i sia costruibile in un passo da $\boldsymbol{A} \cup \{P_1, ..., P_{i-1}\}$.
Chiameremo un punto nel piano *costruibile* se è costruibile da $\mathbb{Q} \times \mathbb{Q}$, cioè dell'insieme dei punti del piano aventi coordinate razionali.
Come è possibile collegare la teoria dei campi allo schema dei punti costruibili? Ovviamente associando a ciascun punto le sue coordinate nel modo sotto descritto.
Supponiamo che il punto P abbia coordinate (a,b) e che sia costruibile da $\mathbb{Q} \times \mathbb{Q}$ in un passo. Associamo al punto P il campo $\mathbb{Q}(a,b)$ ottenuto aggiungendo a $\mathbb{Q}$ le coordinate di P. Generalmente, supponiamo che P sia costruibile da $\mathbb{Q} \times \mathbb{Q}$ in n passi: esisteranno dunque n punti P_1, P_2, ..., $P_n = P$ tali che ciascun P_i sia costruibile in un passo da $\mathbb{Q} \times \mathbb{Q} \cup \{P_1, ..., P_{i-1}\}$. Indichiamo le coordinate di P_1, ..., P_n con (a_1,b_1), ..., (a_n,b_n) rispettivamente. Ai punti P_1, ..., P_n associamo i campi K_1, ..., K_n dove $K_1=\mathbb{Q}(a_1,b_1)$ e per ogni $i > 1$

$$K_i=K_{i-1}(a_i,b_i)$$

Cominciando con $\mathbb{Q}$, noi aggiungiamo prima le coordinate di P_1, poi le coordinate di P_2, e così via, ottenendo in questa maniera la successione di estensioni

$$\mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n = \mathrm{K}$$

Diremo che K è il *campo associato al punto P.*

Lemma 5. *Siano K_1, ..., K_n definiti come in precedenza, allora $[K_i : K_{i-1}] = 1, 2 o 4$.*

Dimostrazione. Ricordiamo che K_{i-1} contiene le coordinate dei punti P_1, ..., P_{i-1} e che K_i si ottiene aggiungendo a K_{i-1} le coordinate x_i, y_i di P_i. Ma P_i è costruibile in un passo da $\mathbb{Q} \times \mathbb{Q} \cup \{P_1, ..., P_{i-1}\}$, così dobbiamo considerare tre casi di intersezione che possono generare P_i, cioè l'intersezione tra due rette, l'intersezione tra una retta e una circonferenza e l'intersezione tra due circonferenze.

Intersezione tra due rette Supponiamo che una delle rette considerate passi per i punti (a_1,a_2) e (b_1,b_2), mentre l'altra passi per i punti (c_1,c_2) e (d_1,d_2). Scriviamo le equazioni di queste rette in termini delle costanti a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 (che sono tutti in K_{i-1}) e poi risolviamo queste equazioni simultaneamente per ottenere le coordinate x e y del punto di intersezione. Chiaramente i valori di x e y sono espressi in termini di a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, per cui sono ancora in K_{i-1}. Così, K_i=K_{i-1}, e dunque per la proposizione 2.2.1 si ha che $[K_i : K_{i-1}] = 1$.

Intersezione tra una retta e una circonferenza Si consideri la retta AB e la circonferenza avente centro C e raggio uguale alla distanza k = $\overline{DE}$. Siano (a_1,a_2), (b_1,b_2) e (c_1,c_2) le coordinate dei punti A, B e C rispettivamente. Per ipotesi K_{i-1} contiene le costanti a_1, a_2, b_1, b_2, c_1, c_2, così come k^2.
La retta AB ha equazione:

$$\frac{y - b_2}{x - b_1} = \frac{b_2 - a_2}{b_1 - a_1}$$

e la circonferenza ha equazione

$$(x - c_1)^2 + (y - c_2)^2 = k^2$$

Risolvendo rispetto a y l'equazione della retta e sostituendo il valore trovato nell'equazione cartesiana della circonferenza (il che equivale a risolvere contemporaneamente le equazioni cartesiane della retta e della circonferenza considerate) si ottiene:

$$(x - c_1)^2 + [\frac{b_2 - a_2}{b_1 - a_1}(x - b_1) + b_2 - c_2]^2 = k^2$$

Le radici di quest'ultima equazione sono le ascisse dei punti di intersezione tra la retta e la circonferenza prese in considerazione. Dunque, le ascisse di entrambi i punti di intersezione sono radici di un'equazione quadratica a coefficienti in K_{i-1}, così come lo sono le ordinate di tali punti di intersezione. Così, se $K_i = K_{i-1}(x_i,y_i)$, con (x_i,y_i) uno dei punti di intersezione, per il teorema 26, si ha:

$$[K_{i-1}(x_i,y_i) : K_{i-1}] = [K_{i-1}(x_i,y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}] = 2 \text{ x } 2 = 4$$

(Questo nel caso in cui x_i, $y_i \notin K_{i-1}$. Mentre se o x_i, o y_i od entrambi sono in K_{i-1}, allora risulta $[K_{i-1}(x_i, y_i) : K_{i-1}] = 1$ o 2.)

intersezione tra due circonferenze Supponiamo che le due circonferenze abbiano equazioni

$$x^2 + y^2 + ax + by + \text{c} = 0$$

e

$$x^2 + y^2 + dx + ey + \text{f} = 0$$

Allora i punti di intersezione tra le due circonferenze devono soddisfare la seguente equazione:

$$(a - d)x + (b - e)y + (c - f) = 0$$

ottenuta sottraendo l'equazione cartesiana della seconda circonferenza dalla prima. Dunque, x e y possono essere trovate risolvendo simultaneamente le due equazioni precedenti, e si giunge alla tesi con un ragionamento analogo a quello utilizzato per dimostrare il caso precedente.

□

Teorema 28 (Teorema fondamentale sui punti costruibili)**.** *Se il punto di coordinate (a,b) è costruibile, allora il grado di $\mathbb{Q}(a)$ su $\mathbb{Q}$ è una potenza di 2; un discorso analogo è valido per il grado di $\mathbb{Q}(b)$ su $\mathbb{Q}$.*

Dimostrazione. Sia P un punto costruibile; per definizione esistono i punti P_1, ..., P_n di coordinate (a_1, b_1), ..., (a_n, b_n), tali che ciascun P_i è costruibile in un passo da $\mathbb{Q} \times \mathbb{Q} \cup \{P_1, ..., P_{i-1}\}$, e P_n = P. Siano K_1, ..., K_n i campi associati a P_1, ..., P_n. Allora

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : \mathbb{Q}]$$

e per il lemma 5 questo è una potenza di 2, diciamo 2^m. Ma

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}]$$

quindi $[\mathbb{Q}(a) : \mathbb{Q}]$ è un fattore di 2^m, cioè una potenza di 2. □

Teorema 29. *E' impossibile "duplicare un cubo" col solo utilizzo di riga e compasso.*

Dimostrazione. Consideriamo un cubo di spigolo 1 (e dunque di volume 1), e poniamolo in un sistema di coordinate cartesiane in maniera tale che uno spigolo del cubo coincida con l'intervallo unitario sull'asse delle ascisse. In questo modo gli estremi dello spigolo giacente sull'asse delle ascisse sarebbero i punti di coordinate $(0;0)$ e $(1;0)$. Se fossimo in grado di duplicare il cubo con l'ausilio di riga e compasso, saremmo in grado di costruire un punto di coordinate $(c;0)$ tale che $c^3 = 2$. Per il teorema 28, $[\mathbb{Q}(c) : \mathbb{Q}]$ dovrebbe essere una potenza di 2, ma per il teorema 25 si ha che $[\mathbb{Q}(c) : \mathbb{Q}] = 3$.
Questa contraddizione mostra che è impossibile duplicare il cubo utilizzando solamente una riga ed un compasso. □

Lemma 6 (Criterio di irriducibilità di Eisenstein)**.** *Sia*

$$a(x) = a_0 + a_1x + ... + a_nx^n$$

un polinomio a coefficienti interi. Se esiste un numero primo p che divide ogni coefficiente di a(x) ad eccezione del coefficiente direttore a_n e tale che p^2 non divide a_0, allora a(x) è un polinomio irriducibile su $\mathbb{Q}$.

Dimostrazione. Supponiamo per assurdo che $a(x)$ possa essere fattorizzato su $\mathbb{Q}$ come $a(x) = b(x)c(x)$, dove $b(x)$ e $c(x)$ sono polinomi a coefficienti interi, che possiamo scrivere come

$$b(x) = b_0 + b_1x + ... + b_kx^k \text{ e } c(x) = c_0 + c_1x + ... + c_mx^m$$

Si avrà che $a_0 = b_0c_0$; poiché p divide a_0 ma p^2 non lo divide, si avrà che solo uno tra b_0 e c_0 è divisibile per p; diciamo che $p \mid c_0$ e $p \nmid b_0$. Si avrà inoltre che $a_n = b_kc_m$ e $p \nmid a_n$; dunque $p \nmid c_m$. Sia s il più piccolo intero tale che $p \nmid c_s$. Si ha

$$a_s = b_0c_s + b_1c_{s-1} + ... + b_sc_0$$

e per la nostra scelta di c_s avremo che ogni termine a secondo membro è divisibile per p ad accezione di b_0c_s. Ma anche a_s è divisibile per p, perciò anche b_0c_s dovrà essere divisibile per p. Ma ciò è impossibile in quanto $p \nmid b_0$ e p $\nmid c_s$. Dunque $a(x)$ non può essere fattorizzato in $\mathbb{Q}$. □

Teorema 30. *E' impossibile "trisecare un angolo" col solo utilizzo di riga e compasso. Ciò significa che esistono angoli che non possono essere trisecati utilizzando solamente riga e compasso.*

Dimostrazione. In particolare mostreremo che un angolo di 60° non può essere trisecato. Se fossimo in grado di trisecare un angolo di 60°, saremmo in grado di costruire un punto $(c;0)$, tale che $c = \cos 20°$; perciò saremmo anche in grado di costruire il punto di coordinate $(b;0)$, con $b = 2\cos 20°$.
Ma dalla trigonometria elementare si ha

$$\cos 3\theta = 4\cos^3 \theta - 3\cos\theta$$

da cui

$$\cos 60° = 4\cos^3 20° - 3\cos 20°$$

Così, $b = 2\cos 20°$ soddisfa l'equazione $b^3 - 3b - 1 = 0$. Il polinomio

$$p(x)=x^3 - 3x - 1$$

è irriducibile su $\mathbb{Q}$ perché $p(x + 1)=x^3 + 3x^2 - 3$ è irriducibile per il criterio di Eisenstein (lemma 6). Per il teorema 25, segue che $\mathbb{Q}(b)$ ha grado 3 su $\mathbb{Q}$, in contraddizione con il teorema 28 che afferma che il suo grado debba essere una potenza di 2. □

Teorema 31. *E' impossibile "quadrare un cerchio" col solo utilizzo di riga e compasso.*

Dimostrazione. Consideriamo una circonferenza di raggio 1. Chiaramente l'area del cerchio avrà valore π. Se fossimo in grado di quadrare il cerchio con riga e compasso, sarebbe possibile costruire il punto di coordinate $(0;\sqrt{\pi})$ e quindi dal teorema 28 si avrebbe che $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ dovrebbe essere una potenza di 2. Ma è ben noto che π è trascendente su $\mathbb{Q}$. Il quadrato di un elemento algebrico è algebrico, quindi $\sqrt{\pi}$ è trascendente. Segue dal corollario 2.2.1 che $\mathbb{Q}(\sqrt{\pi})$ non è un estensione finita di $\mathbb{Q}$, tanto meno una estensione di un qualche grado 2^m come richiesto. □

Bibliografia

[1] Charles C. Pinter; A book of abstract algebra; McGraw-Hill Book Company; 1982