Un'introduzione all'algebra moderna

Indice

Introduzione

Il libro è il frutto della collaborazione di due laboratori attivati nell'ambito del Progetto Lauree Scientifiche presso le Università di Torino e Genova. Nelle sue pagine vengono presentati alcuni concetti fondamentali che sono stati e sono tuttora idee portanti dell'algebra, evidenziandone in modo particolare le potenzialità teoriche e applicative come strumenti effettivi di calcolo, più che gli aspetti formali di astrazione e descrizione. In modo particolare, il concetto matematico di gruppo costituisce una sorta di fil rouge che lega le varie tematiche affrontate; lo scopo non è però quello di introdurne una definizione formale per poi illustrarne proprietà ed esempi significativi, ma quello di mostrare come esso scaturisca in modo naturale e fornisca idee nuove e illuminanti nelle più disparate situazioni matematiche e applicative, quali la teoria delle equazioni sui numeri reali e complessi, la cristallografia, la crittografia, la geometria di figure piane, spaziali, pluridimensionali limitate e illimitate e così via.

L'intero percorso è stato suddiviso in moduli, ciascuno dei quali compiutamente strutturato nei vari aspetti teorici e di attività di apprendimento e verifica, in modo che sia possibile svilupparlo per intero, oppure privilegiare l'approfondimento di alcuni dei temi proposti.

Nella scelta degli argomenti presentati, tanto nel complesso della nostra proposta, quanto in ogni singolo modulo in cui è stata suddivisa, abbiamo tenuto ben presenti le istanze, non necessariamente antitetiche, di avvicinare i giovani studenti (o chi è curioso di matematica) ad aspetti della matematica più coinvolgenti e ricchi di fascino, con spiccate valenze culturali ed estetiche, e, nel contempo, di fornire loro strumenti e conoscenze di concreta e immediata utilità nella prosecuzione dei loro studi, in un qualsiasi percorso universitario scientifico o tecnico.

Per facilitare la comprensione dei vari argomenti si suggerisce l'utilizzo di materiali specifici, sia concreti, come costruzioni di vario tipo per la realizzazione di tassellazioni del piano e di poliedri dello spazio [1], sia informatici, come software del tipo Geogebra, Derive, Maple o Mathematica. Nelle varie attività viene dato congruo spazio anche all'utilizzo delle risorse disponibili su Internet, particolarmente ricche ed interessanti in questo settore, sia per quantità sia, soprattutto, per qualità.

Il programma delle attività è suddiviso in 5 temi, uno per ognuno dei moduli, che prevedono due momenti distinti composti da una o più unità didattiche. I cinque temi proposti sono:

- Teoria delle equazioni algebriche
- I numeri complessi
- Strutture algebriche e loro applicazioni
- Simmetrie nel piano e nello spazio
- Le matrici

I laboratori che hanno prodotto il presente materiale sono:

- il laboratorio *Una introduzione all'algebra moderna* presso la Facoltà di Scienze MFN dell'Università di Torino, il cui gruppo di lavoro è costituito dai docenti di scuola media superiore:
  Valeria Andriano, Paola Bracco, Stefano Buccolo, Laura Chiusano, Luciana Ferreri, Anna Maria Iavarone, Michele Maoret, Alessandra Mattiola, Enrica Ornato, Giuseppe Priolo, Emanuele Salvador, Gisella Scagliotti, Stefano Vinti,
  coordinati da Giorgio Ferrarese e Margherita Roggero
- il laboratorio *Strutture numeriche, armonia e bellezza in natura e nell'arte si incontrano* presso la Facoltà di Scienze MFN dell'Università di Genova, il cui gruppo di lavoro è costituito dai docenti di scuola media superiore:
  Sergio Antola, Carla Lesino, Maria Rosaria La Piana,
  coordinati da Grazia Tamone.

Giorgio Ferrarese: giorgio.ferrarese@unito.it

Margherita Roggero: margherita.roggero@unito.it

Dipartimento di Matematica dell'Università di Torino

Via Carlo Alberto 10 - 10123 Torino

1 *http://www.zometool.com*;
http://www.astro-logix.com/
http://mathartfun.com/shopsite_sc/store/html/index.html

Grazia Tamone: tamone@dima.unige.it
Dipartimento di Matematica dell'Università di Genova
Via Dodecaneso 35 - 16146 Genova

Legenda

I simboli che accompagnano i titoli dei vari paragrafi hanno il seguente significato:

★ argomenti particolarmente interessanti, ma impegnativi, non necessari per la comprensione della lezione nel suo complesso;

⊡ attività al computer;

⁕ cenni biografici di qualche matematico a cui si devono risultati importanti presentati nelle lezioni;

♣ elenco di esercizi.

Modulo 1

Teoria delle equazioni algebriche

Lezione 1

Polinomi ed equazioni

Cos'è l'Algebra?

Riportiamo alcuni brani tratti dal libro *LE MATEMATICHE* di A. D. Aleksandrov, A. N. Kolmogorov, M. A. Laurent'ev (Bollati Boringhieri).

L'algebra si caratterizza prima di tutto per il suo metodo, che comporta l'uso di lettere e di espressioni letterali sulle quali si eseguono delle trasformazioni secondo regole ben definite. Nell'algebra elementare, le lettere sottointendono numeri ordinari, pertanto le regole per trasformare le espressioni letterali sono fondate sulle regole generali delle operazioni sui numeri.

Il metodo algebrico, cioè il metodo del calcolo letterale, permea tutta la matematica.

Ciò trova la sua espressione nel fatto che una parte essenziale della soluzione di un qualsiasi problema matematico spesso non è altro che un calcolo algebrico più o meno complesso. Inoltre in matematica si usano vari calcoli letterali, in cui con le lettere non si indicano più numeri, ma altri oggetti. Allora anche le regole per operare con essi possono essere diverse da quelle dell'algebra elementare. Per esempio, in geometria, in meccanica e in fisica si usano i vettori. Come noto, sui vettori si compiono operazioni le cui regole, qualche volta, sono le stesse che valgono per le operazioni sui numeri, mentre altre volte ne differiscono in modo essenziale.

Il valore del metodo algebrico nella matematica e nelle sue applicazioni è cresciuto enormemente negli ultimi decenni.

In primo luogo le crescenti necessità della tecnica richiedono che si giunga alla soluzione numerica di ardui problemi di analisi matematica, e ciò

spesso risulta possibile solo dopo che tali problemi sono stati in qualche modo algebrizzati; questo, a sua volta, pone problemi nuovi, qualche volta difficili, per la stessa algebra.

In secondo luogo, alcune questioni di analisi sono state chiarite soltanto dopo che ad esse sono stati applicati metodi algebrici fondati su profonde generalizzazioni (nel caso in cui le incognite sono infinite) della teoria dei sistemi di equazioni di primo grado.

Infine i rami superiori dell'algebra hanno trovato applicazioni nella fisica moderna; precisamente accade che le nozioni fondamentali della meccanica quantistica si esprimono mediante complicate entità algebriche, di tipo non elementare.

Da questo già si comincia a capire che l'algebra parte da

$$(a+b)(a-b) = a^2 - b^2 \qquad \text{e da} \qquad (a+b)^2 = a^2 + 2ab + b^2$$

ma arriva molto, molto lontano.

Prima di tutto osserviamo che le nostre idee sulla natura dell'algebra e su che cosa sia il problema fondamentale dell'algebra sono cambiate due volte, cosicchè in tempi diversi si sono intese, con il nome di algebra, tre cose assai diverse fra loro.

Nei tempi antichi, qualsiasi regola si trovasse per la soluzione di una certa classe di problemi matematici si trascriveva semplicemente con parole, poiché le indicazioni letterali non erano ancora state escogitate. La stessa parola algebra proviene dalla denominazione dell'importante opera di uno scienziato del nono secolo, **Mohammed al-Kharizmi**, *nella quale erano riportate le regole generali per la soluzione delle equazioni di primo e secondo grado.*

Tuttavia l'introduzione delle indicazioni letterali stesse viene solitamente collegata con il nome di **Viète** *, che cominciò a indicare con lettere non solo le incognite, ma anche le quantità date. Anche* **Cartesio** *fece non poco per sviluppare l'uso della notazione simbolica; egli pure ricorse alle lettere per significare numeri ordinari.*

Questo fu il primo punto di vista sull'algebra. Esso è espresso in modo particolarmente chiaro nel noto libro di **Eulero**, *membro dell'Accademia Russa delle Scienze,* Introduzione all'algebra, *scritto negli anni sessanta del diciottesimo secolo, cioò oltre duecento anni fa:*

per Eulero l'algebra è la teoria del calcolo con quantità diverse.

È da questo momento che ebbe propriamente inizio l'algebra come scienza del calcolo letterale, delle trasformazioni di formule formate da lettere,

delle equazioni algebriche e così via, a differenza dell'aritmetica, in cui si opera sempre su numeri concreti.

Solo ora considerazioni matematiche complesse divennero facilmente descrivibili e accessibili all'indagine: infatti, gettando uno sguardo alla formula letterale, nella maggior parte dei casi se ne poteva subito vedere la **struttura** *o la legge di formazione e la si poteva facilmente trasformare in modo opportuno.*

Alla fine del diciottesimo secolo e all'inizio del diciannovesimo un problema divenne il problema centrale, precisamente come trovare la soluzione delle equazioni algebriche; la difficoltà principale è la soluzione della equazione algebrica di grado n in 1 incognita:

$$x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = 0.$$

Ciò si doveva sia alla sua importanza per tutta la matematica pura e applicata, sia alla difficoltà e alla profondità delle dimostrazioni della maggior parte dei teoremi ad esso connessi.

Verso la metà del diciannovesimo secolo (esattamente cento anni dopo l'algebra di Eulero)

l'algebra era definita come la teoria delle equazioni algebriche.

Questa fu la seconda concezione sulla natura dell'algebra.

Nella seconda metà del secolo diciannovesimo, partendo dalle idee di Galois sulla teoria delle equazioni algebriche, si svilupparono grandemente la teoria dei gruppi e quella dei numeri algebrici.

La teoria dei gruppi è, in particolare, lo strumento algebrico di base nella descrizione delle "simmetrie" come "trasformazioni " che lasciano "invariata" una figura: intuitivamente, come disse Hermann Weyl (1885-19559 "qualcosa che puoi fare alla figura in modo che, quando hai finito di farla, la figura sembra uguale a prima ". Tutte le "simmetrie" di una figura formano un gruppo, che viene chiamato il "gruppo di simmetria" della figura stessa.

Nello stesso periodo, sempre in relazione al problema della risoluzione delle equazioni algebriche, come alla teoria delle varietà algebriche di grado superiore che in quel tempo si studiavano in geometria analitica, l'apparato algebrico si sviluppò nelle più diverse direzioni.

Nella seconda metà del secolo scorso in meccanica, in fisica e nella stessa matematica gli scienziati cominciarono sempre più spesso a studiare grandezze per cui era naturale considerare l'addizione e la sottrazione, e qualche volta anche la moltiplicazione e la divisione, operazioni che tuttavia erano

soggette a leggi e regole diverse da quelle solite che valevano per i numeri razionali.

Citiamo qui i vettori, le matrici, i tensori, gli spinori, i numeri ipercomplessi ecc.

Tutte queste entità si indicano con lettere, ma le regole per operare con esse differiscono l'una dall'altra. Se per un certo insieme di oggetti sono assegnate certe operazioni e certe leggi che quelle operazioni devono soddisfare, si dice allora che è dato un **sistema algebrico**.

La terza concezione sulla natura dell'algebra consiste nel riguardare

l'algebra come studio di diversi sistemi algebrici.

Questa è la cosiddetta **algebra assiomatica, o astratta**.

Essa è astratta perché, a questo punto, non ci interessa più sapere che cosa esattamente stiano a indicare le lettere nel sistema algebrico che stiamo considerando; per noi è importante sapere solo quali leggi (assiomi) debbano soddisfare le operazioni considerate nel sistema. Quest'algebra è detta poi assiomatica perché viene costruita esclusivamente a partire dagli assiomi che sono stati posti a suo fondamento.

Si è così di nuovo ritornati, seppure a un grado superiore, al primo punto di vista sull'algebra, quello del Viète, secondo cui l'algebra è la teoria del calcolo letterale. Cosa si debba intendere con le lettere non ha più importanza. Sono importanti solo le leggi (assiomi) che le operazioni che si eseguono su quelle lettere devono soddisfare.

Naturalmente sono interessanti soltanto quei sistemi algebrici che hanno grande significato per la stessa matematica o per le sue applicazioni.

In questo secolo l'algebra ha avuto applicazioni fondamentali nella geometria (alla topologia e alla teoria dei gruppi di Lie) e, come si è già detto, alla fisica moderna (analisi funzionale e meccanica quantistica).

Negli ultimi tempi sono divenute particolarmente importanti le questioni dell'automazione dei calcoli algebrici.

Le radici dei polinomi

Si dice **equazione algebrica** o **polinomiale** di grado n in 1 incognita un'equazione della forma:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = 0$$

dove $a_0,\ a_1,\ \ldots, a_n \in \mathbb{R}$ ossia i coefficienti $a_1,\ a_2, \ldots, a_n$ sono coefficienti reali assegnati e $a_0 \neq 0$.

Prima di risolvere una equazione è fondamentale chiedersi di quale natura siano le soluzioni cercate. Non sempre si cercano dei numeri; si potrebbe trattare ad esempio di funzioni oppure di vettori oppure di matrici o di altro ancora. Anche nel caso in cui le soluzioni cercate siano numeri, potrebbero essere significativi soltanto i numeri interi oppure soltanto i numeri negativi oppure soltanto i numeri reali compresi tra 0 e 1: queste condizioni particolari si ricavano dal contesto del problema per la cui soluzione l'equazione è stata costruita.

Noi però ci occuperemo solo del caso più semplice in cui **le soluzioni cercate sono numeri e consideremo qualsiasi tipo di numero come soluzione accettabile.**

Precisiamo ora i termini che stiamo usando:

- in tutto questo modulo, con "equazione" intenderemo sempre "equazione polinomiale";
- con $F(x)$ indicheremo in genere un polinomio non–nullo; il polinomio nullo 0, ossia quello che ha tutti i coeffcienti nulli, esiste, ma è spesso una eccezione (l'unica!) per le proprietà di cui ci occuperemo;
- supporremo sempre che l'equazione $F(x) = 0$ sia della forma

  $$x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = 0$$

  ossia che tutti i termini dell'equazione compaiano a primo membro e che poi si siano divisi i due membri per il coefficiente della potenza di x di grado più elevato (ossia del **coefficiente direttivo**) in modo da ottenere a primo membro un **polinomio monico** ossia con coefficiente direttivo 1.
- un numero a è **soluzione di una equazione polinomiale** $F(x) = 0$ se il numero $F(a)$, che si ottiene "sostituendo a al posto della x" in $F(x)$, è 0. In tal caso si dice anche che a è una **radice del polinomio** $F(x)$.

In altri termini, le locuzioni 'soluzione dell'equazione $F(x) = 0$' e 'radice del polinomio $F(x)$' sono dei sinonimi.

Per sapere se un dato numero a è oppure non è soluzione di una certa equazione $F(x) = 0$, non è quindi necessario conoscere una formula risolutiva per quell'equazione, ma è sufficiente eseguire una sostituzione.

Esempio 1.1. *Pur non conoscendo il modo di risolvere le equazioni di quinto grado possiamo dire che il numero* 1 *è soluzione dell'equazione* $x^5 - 3x^2 + 2 = 0$, *poiché* $1^5 - 3 \cdot 1^2 + 2 = 0$, *mentre il numero* -1 *non è una sua soluzione poiché* $(-1)^5 - 3 \cdot (-1)^2 + 2 = -2 \neq 0$.

Equazioni di primo grado. L'equazione di primo grado

$$x + a = 0$$

si risolve immediatamente:

$$x = -a.$$

Equazioni di secondo grado. L'equazione di secondo grado

$$x^2 + px + q = 0$$

era già stata risolta nella remota antichità. La sua soluzione è assai semplice: aggiungendo ai due membri $\frac{p^2}{4} - q$, otteniamo:

$$x^2 + px + \frac{p^2}{4} = \frac{p^2}{4} - q$$

Ma

$$x^2 + px + \frac{p^2}{4} = (x + \frac{p}{2})^2$$

e quindi

$$x + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q}$$

da cui si ricavano le soluzioni dell'equazione quadratica:

$$x_1 = \frac{-p + \sqrt{p^2 - 4q}}{2} \qquad \text{e} \qquad x_2 = \frac{-p - \sqrt{p^2 - 4q}}{2}.$$

La quantità $p^2 - 4q$ si chiama **discriminante** e viene spesso indicata con la lettera greca Δ.

Quando Δ è strettamente positivo, questa formula ci fornisce 2 soluzioni reali distinte x_1 e x_2. Si trovano così **tutte** le soluzioni dell'equazione di secondo grado in quanto 2 è il numero massimo di soluzioni che tale equazione può avere: motiveremo questa affermazione mediante il Teorema di Ruffini.

Quando Δ è nullo, l'equazione ha la soluzione $x_1 = -\frac{p}{4}$, unica ma "da contare come doppia": anche in questo caso il significato sarà chiarito mediante il Teorema di Ruffini.

Quando Δ è negativo, l'equazione non ha soluzioni reali. Ad esempio non esiste alcun numero reale che sia soluzione di $x^2 + 1 = 0$. Introdurremo i **numeri complessi** per ovviare a questo "inconveniente".

Equazioni di grado superiore. Le formule prima ottenute $\frac{-p\pm\sqrt{p^2-4q}}{2}$ sono formule risolutive per radicali per l'equazione di secondo grado $x^2+px+q=0$. Più in generale, una **formula risolutiva per radicali** dell'equazione di grado n:

$$x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = 0$$

permette di trovare una soluzione (o tutte le soluzioni) dell'equazione data mediante un numero finito di operazioni di somma, prodotto, quoziente ed estrazione di radice sui coefficienti $a_1, \cdots, a_n$.

Possiamo pensare una formula risolutiva come una espressione letterale $f(a_1, \cdots, a_n)$ nelle lettere $a_1, \cdots, a_n$ in cui appaiono soltanto somme, prodotti, quozienti ed estrazioni di radici tale che, sostituita nell'equazione precedente, (anch'essa pensata a coefficienti letterali) ed eseguiti i calcoli, porta all'identità $0 = 0$.

Gli algebristi italiani del sedicesimo secolo trovarono formule risolutive per radicali anche per le equazioni di terzo e di quarto grado.

Però:

i successivi studi in questo campo, per equazioni di grado superiore, si scontrarono con difficoltà insormontabili. I più grandi matematici dei secoli sedicesimo, diciassettesimo, diciottesimo e dell'inizio del diciannovesimo (tra i quali ricordiamo Tartaglia, Cardano, Cartesio, Newton, Eulero, D'Alembert, Tschirnhausen, Bézout, Lagrange, Gauss, Abel, Galois, Lobacevskij, Sturm) crearono un grandioso complesso di teoremi e di metodi connessi con questa questione. [1]

Un matematico stranamente non ricordato nell'elenco precedente è l'italiano **Paolo Ruffini**, che diede un contributo fondamentale alla teoria delle equazioni ed ebbe per primo l'idea (e diede la dimostrazione, anche se non del tutto chiara) di uno dei punti essenziali della teoria:

Teorema di Abel–Ruffini
non può esistere una formula risolutiva per radicali delle equazioni di grado ≥ 5.

L'importanza di fattorizzare

Un risultato forse meno riposto, ma altrettanto importante che si deve a Ruffini è il seguente:

[1] LE MATEMATICHE di A. D. Aleksandrov, A. N. Kolmogorov, M. A. Laurent'ev

Teorema 1.2 (Ruffini)**.** *Siano $F(x)$ un polinomio di grado n e c un numero reale. Allora:*

c è una radice di $F(x)$ se e soltanto se $F(x)$ si può **fattorizzare** *nel prodotto di $x - c$ per un polinomio di grado $n - 1$.*

Dim: Per sapere se un numero c è radice del polinomio $F(x)$ possiamo eseguire la **divisione con resto** di $F(x)$ per il polinomio di primo grado $x - c$ ottenendo:

$$F(x) = (x - c) \cdot G(x) + r$$

dove r è un polinomio di grado inferiore al grado di $x - c$, ossia r è un numero reale. Sostituendo poi c al posto di x nei due membri si ottiene $F(c) = r$ e quindi c è radice di $F(x)$ se e soltanto se $r = 0$ ossia se e soltanto se $F(x) = (x - c) \cdot G(x)$. $\diamond$

Come conseguenza di questo importante risultato possiamo definire in modo preciso la **molteplicità** della soluzione c per l'equazione $F(x) = 0$ (o della radice c del polinomio $F(x)$):

Definizione 1.3. *Si dice che c è una soluzione di $F(x) = 0$ di molteplicità k se $F(x)$ è divisibile esattamente per $(x - c)^k$, ma non è divisibile per $(x - c)^{k+1}$.*

Se $F(x) = G_1(x) \cdot G_2(x)$ allora c è radice di $F(x)$ se e soltanto se è radice di almeno uno dei fattori $G_1(x)$ o $G_2(x)$. Vale infatti in $\mathbb{R}$ il cosidetto **principio di annullamento del prodotto** ossia:

$$a \cdot b = 0 \text{ se e solo se } a = 0 \text{ oppure } b = 0.$$

Più precisamente la molteplicità di c come radice di $F(x)$ è la somma delle molteplicità come radice di $G_1(x)$ e di $G_2(x)$.

Come conseguenza del Teorema di Ruffini si può allora provare che:

una equazione polinomiale di grado n ha al massimo n radici, contando ciascuna con la sua molteplicità.

Come già accennato, potremmo considerare anche equazioni polinomiali con coefficienti e soluzioni di tipo diverso, non numerico (ad esempio matrici o funzioni), per i quali il principio di annullamento del prodotto non vale; in tal caso potremmo incontrare anche equazioni con molte più soluzioni del previsto, addirittura infinite!

Un'altra utilissima osservazione suggerita dal Teorema di Ruffini è la seguente:

la difficoltà di risolvere le equazioni polinomiali è esattamente la difficoltà di fattorizzare i polinomi in fattori di grado inferiore.

Dire che non esiste alcuna formula per calcolare le soluzioni delle equazioni di grado ≥ 5 equivale a dire che non esiste alcun metodo per fattorizzare i polinomi di grado ≥ 5.

Per questo motivo un'equazione che si presenti già totalmente o parzialmente fattorizzata costituisce una notevole semplificazione. Eseguire i prodotti e poi accingersi a risolvere l'equazione ottenuta significa vanificare il vantaggio iniziale.

Esempio 1.4. *L'equazione* $(x-2)(x-\frac{4}{3})(x-1)(x+7)(x-\pi)^2 = 0$, *pur avendo grado* 6, *si risolve immediatamente. Le sue soluzioni sono* 2, $\frac{4}{3}$, 1, -7 *e* π *(quest'ultima soluzione ha molteplicità* 2*). Poiché la somma delle molteplicità è* 6 *come il grado dell'equazione, abbiamo sicuramente trovato* ***tutte*** *le soluzioni.*

Esempio 1.5. *L'equazione* $(x^2-2x-6)(x^2+2x-1)(x+\frac{1}{2})x = 0$, *pur avendo grado* 6, *richiede per la sua soluzione soltanto la formula risolutiva delle equazioni di secondo grado. Le sue soluzioni sono infatti, oltre a* $-\frac{1}{2}$ *e* 0, *le soluzioni dell'equazione* $x^2-2x-6=0$ *e le soluzioni dell'equazione* $x^2+2x-1=0$.

Esempio 1.6. *L'equazione* $(x-1)(x-\sqrt{3}) = 0$ *è già fattorizzata nel prodotto di due fattori di primo grado e quindi si risolve immediatamente: le soluzioni sono* $a = 1$ *e* $b = \sqrt{3}$.

Se invece di procedere in questo modo, decidiamo di eseguire il prodotto e poi risolvere mediante la formula risolutiva per le equazioni di secondo grado, otteniamo $x^2-(1+\sqrt{3})x+\sqrt{3} = 0$ *e quindi le due soluzioni:*

$$c = \frac{1+\sqrt{3}+\sqrt{2}\sqrt{2-\sqrt{3}}}{2} \qquad e \qquad d = \frac{1+\sqrt{3}-\sqrt{2}\sqrt{2-\sqrt{3}}}{2}.$$

Poiché una equazione di secondo grado non può avere 4 *soluzioni, i numeri* c *e* d *devono coincidere con* a *e* b. *Quale dei due è* a*?*

Più in generale si può provare che la fattorizzazione di un polinomio nel prodotto di polinomi non ulteriormente fattorizzabili è unica (a meno dell'ordine dei fattori e di costanti moltiplicative). Nel linguaggio dell'algebra si dice allora che i polinomi godono della proprietà di **fattorizzazione unica**.

Soluzioni razionali

Anche se i numeri reali sono veramente "tanti", quelli che si usano in pratica (ad esempio negli esercizi o nelle applicazioni) sono relativamente pochi: i numeri **interi** "piccoli", **numeri razionali** (sia sotto forma di frazioni sia sotto forma di numeri decimali finiti), qualche radicale (come $\sqrt{3}$ o $\sqrt[5]{2}$ e qualche **trascendente** (come π oppure e).

Non è così raro quindi incontrare equazioni in cui tutti i coefficienti sono numeri interi oppure al massimo razionali. Neppure per queste particolari equazioni esistono formule risolutive generali, ossia che permettono di trovare sempre le eventuali soluzioni reali.

Esempio 1.7. *Dalle proprietà che esamineremo nei prossimi paragrafi sarà chiaro che l'equazione* $x^5 - 16x + 2 = 0$ *ha almeno una soluzione reale (anzi ne ha ben* 3*). Però si può dimostrare che tali soluzioni non sono esprimibili mediante una formula per radicali e che quindi questa semplice equazione è una di quelle che non si possono risolvere.*

Tuttavia, è sempre possibile, eseguendo un po' di calcoli, determinare tutte le **soluzioni razionali di una equazione a coefficienti razionali**, ammesso che ce ne siano.

Trasformiamo innanzi tutto l'equazione in una con coefficienti interi, moltiplicando se necessario per un denominatore comune, ottenendo:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = 0$$

dove i coefficienti $a_0, \cdots, a_n$ sono numeri interi. Possiamo supporre $a_n \neq 0$ (in caso contrario 0 è una soluzione e possiamo dividere il polinomio per x).

Ogni sua soluzione razionale $\frac{b}{c}$, si può scrivere in modo che b, c siano numeri interi senza fattori comuni e c sia positivo; allora il numeratore b è un divisore del termine noto a_n e il denominatore c è un divisore del coefficiente direttivo a_0.

Per verificarlo è sufficiente sostituire $\frac{b}{c}$ nell'equazione e poi moltiplicare i due membri per c^n; si ottiene infatti:

$$a_0b^n + a_1b^{n-1}c + \cdots + a_{n-1}bc^{n-1} + a_nc^n = 0.$$

Possiamo raccogliere b dai primi n addendi e portare l'ultimo a secondo membro:

$$b(a_0b^{n-1} + a_1b^{n-2}c + \cdots + a_{n-1}c^{n-1}) = -a_nc^n.$$

Poiché b non ha fattori in comune con c, allora deve dividere a_n; allo stesso modo si prova che c deve dividere a_0.

Per trovare le soluzioni razionali, sarà allora sufficiente scrivere l'elenco di tutte le frazioni che si ottengono mettendo un divisore di a_n al numeratore e un divisore di a_0 al denominatore e sostituirle una ad una nell'equazione, per vedere se qualcuna tra esse è una soluzione.

Con un metodo simile a questo è possibile controllare se un polinomio a coefficienti interi è o meno decomponibile nel prodotto di due polinomi di grado minore, ancora a coefficienti interi (o razionali).

Un consiglio: ogni volta che si è così fortunati da trovare una soluzione $\frac{b}{c}$ dell'equazione, conviene ricorrere al Teorema di Ruffini, dividendo il polinomio a primo membro per $(x - \frac{b}{c})$ o meglio ancora per $(cx - b)$ in modo da abbassare il grado dell'equazione.

Esempio 1.8. *Vogliamo risolvere l'equazione* $F(x) = 0$ *dove* $F(x) = 40x^5 - 58x^4 - 5x^3 + 13x^2 - 17x + 3$.

I divisori b *di* 3 *sono:* $1, -1, 3, -3$.

I divisori c *di* 40 *sono:* 1, 2, 4, 5, 8, 10, 20, 40 *(**NB**: possiamo prendere* $c > 0$*).*

Ci sono 32 *possibili frazioni* $\frac{b}{c}$ *da provare:* $1, \frac{1}{2}, \frac{1}{4}, \ldots\ldots$

Dopo aver verificato che $1, \frac{1}{2}, \frac{1}{4}$ *non sono soluzioni, troviamo che* $\frac{1}{5}$ *lo è.*

Invece di continuare la verifica, dividiamo $F(x)$ *per* $5x - 1$ *ottenendo* $F(x) = (5x - 1)G(x)$ *dove* $G(x) = 8x^4 - 10x^3 - 3x^2 + 2x - 3$.

Procedendo come prima scopriamo che $\frac{3}{2}$ *è una radice di* $G(x)$ *(e quindi anche di* $F(x)$*!)*

Dividendo $G(x)$ *per* $(2x - 3)$ *otteniamo* $H(x) = 4x^3 + x^2 + 1$.

Ripetendo ancora una volta il procedimento per $H(x) = 0$*, scopriamo che non vi sono ulteriori soluzioni razionali; però ora il grado è* 3 *e quindi possiamo determinare le rimanenti soluzioni mediante le formule risolutive.*

♣ Esercizi per la prima lezione

1.1 Trovare, se esiste, un polinomio $G(x)$ tale che:

$$2x^3 - 3x^2 - 6x + 9 = (x^2 - 3) \cdot G(x).$$

1.2 Determinare tutte le soluzioni delle seguenti equazioni:

a. $(3x - \sqrt{2})(4 + 2x) = 0$;

b. $(x - 3)(4 - 5x)(\sqrt{3} - \sqrt{5}x)(\sqrt{3} + \sqrt{5}x) = 0$;

c. $(x - 2\sqrt{5})(x^2 - 5x + 4) = 0$;

d. $(x - \sqrt{2})^4 = 0$;

e. $(x^2 - 5x + 7) = 0$;

f. $(x^2 - 3x - 5)(3x - 2x^2 + 1) = 0$.

1.3 Provare che $\sqrt{3}$ e $-\sqrt{3}$ sono soluzioni di $2x^3 - 3x^2 - 6x + 9 = 0$.
Ci sono anche altre soluzioni?

1.4 Risolvere l'equazione $(x^2+6x+8)(3x^2+12) = 0$ motivando ogni passo del procedimento.

1.5 Trovare tutte le radici reali del polinomio:

$$(x^2 + 6x + 8)^2(3x^2 + 12)(x + 2)$$

precisando per ciascuna la molteplicità.

1.6 Trovare tutte le soluzioni reali dell'equazione:

$$x^4 - 3x^2 = x^3$$

precisando per ciascuna la molteplicità.

1.7 Il numero $\sqrt[5]{2}$ è l'unica soluzione reale delle tre equazioni:

$$x^5 = 2 \quad , \quad x - \sqrt[5]{2} = 0 \quad \text{e} \quad (x - \sqrt[5]{2})^5 = 0.$$

Ciò nonostante le tre equazioni non sono equivalenti dal punto di vista delle soluzioni. Perché?

1.8 Scrivere un polinomio di grado 5 che abbia come radici reali soltanto $a = \sqrt{2}$ con molteplicità 2 e 0 con molteplicità 1. Perché non esiste un polinomio con le caratteristiche precedenti, ma di grado 4?

1.9 Quali delle proprietà dei polinomi presentate nella lezione non vale per il polinomio nullo?

1.10 Si consideri l'equazione $x^2 - (\sqrt{6} + 1 - \sqrt{2})x - (\sqrt{6} + 1)\sqrt{2} = 0$. Provare che per una opportuna scelta del segno si ha:

$$\frac{\sqrt{6} + 1 - \sqrt{2} \pm \sqrt{9 + 2\sqrt{6} + 4\sqrt{3} + 2\sqrt{2}}}{2} = -\sqrt{2}.$$

Qual è la scelta del segno giusta?

1.11 Verificare che $\frac{-p+\sqrt{p^2-4q}}{2}$ è una formula risolutiva per l'equazione $x^2 + px + q = 0$.

1.12 Trovare tutte le radici razionali del polinomio $3x^3 - 6x^2 - x + 2$.

1.13 Trovare tutte le soluzioni razionali delle seguenti equazioni:

a. $2(x + 1)(x - \frac{3}{4})(x^2 - 3) = 0$;

b. $x^3 - 5x^2 + 2x + 8 = 0$;

c. $x^4 - 3x^3 + x^2 - 2x - 3 = 0$;

d. $2x^5 - 13x^4 + 37x^3 - 57x^2 + 48x - 18 = 0$.

Lezione 2

Polinomi e funzioni

Funzioni polinomiali

Ad ogni polinomio $F(x)$ possiamo associare una funzione: quella data dall'espressione $y = F(x)$. Il grafico della funzione $y = F(x)$ ci permette di visualizzare e mettere in evidenza molte proprietà dei polinomi e, viceversa, conoscere le proprietà dei polinomi puo' aiutarci a tracciare un grafico corretto.

Ai polinomi costanti corrispondono funzioni che hanno come grafico una retta orizzontale. Ai polinomi di grado 1, rette oblique. Ai polinomi di grado 2 parabole con l'asse parallelo all'asse y.

Meno familiari sono i grafici di funzioni polinomiali di grado ≥ 3. L'andamento può variare molto a seconda del grado e dei coefficienti, ma tutti i grafici di funzioni polinomiali hanno alcune proprietà in comune.

Intanto possiamo osservare che due polinomi differenti danno sempre luogo a grafici differenti; anzi, i grafici corrispondenti a due polinomi diversi si incontrano soltanto in un numero finito di punti, al più in tanti punti quanto è il maggiore dei loro gradi. Infatti i grafici di $y = F(x)$ e di $y = G(x)$ si incontrano nel punto (a, b) se $b = F(a)$ e $b = G(a)$ e quindi in particolare se a è una soluzione dell'equazione polinomiale $F(x) - G(x) = 0$. Se i due polinomi sono diversi, il polinomio $F(x) - G(x)$ non è il polinomio nullo e quindi ci sono solo un numero finito di soluzioni per l'equazione $F(x) - G(x) = 0$.

Questa proprietà va sotto il nome di **principio di identità dei polinomi.**

In particolare possiamo considerare il caso in cui $G(x)$ sia il polinomio nullo; allora dal principio di identità dei polinomi discende che che il grafico di $y = F(x)$ incontra l'asse x soltanto un numero finito di volte, tante quante sono le radici di $F(x)$.

Più precisamente possiamo dire che ogni radice di $F(x)$ fa attraversare l'asse x al grafico della funzione $y = F(x)$; una radice doppia a fa sì che $F(a) = 0$ e inoltre il grafico attraversi due volte l'asse x nel punto $(a, 0)$ cosicchè il grafico "rimane dalla stessa parte"; se la molteplicità della radice a è k, il grafico attraversa l'asse x k volte nel punto $(a, 0)$ e quindi "passa dalla parte opposta" oppure "rimane dalla stessa parte" a seconda che k sia dispari oppure pari.

Inoltre se fissiamo un qualsiasi numero naturale n, il grafico di una funzione polinomiale (non costante) esce da ogni 'striscia ' orizzontale $-n \leq y \leq n$ per valori della variabile x abbastanza grandi (in simboli $x \gg 0$ oppure $x \to +\infty$) e per valori abbastanza grandi in valore assoluto, ma negativi (in simboli $x \ll 0$ oppure $x \to -\infty$).
più precisamente:

- se il grado di $F(x)$ è pari, il grafico sale al di sopra di ogni striscia sia per x grande sia per x piccolo, se il coefficiente direttivo di $F(x)$ è positivo e scende al di sotto di ogni striscia da entrambe le parti se il coefficiente direttivo di $F(x)$ è negativo;
- se il grado di $F(x)$ è dispari e il coefficiente direttivo di $F(x)$ è positivo il grafico sale al di sopra di ogni striscia per x grande e scende al disotto per x piccolo; l'andamento si rovescia se il coefficiente direttivo di $F(x)$ è negativo.

⊡ Attività col computer

La maggior parte dei calcoli algebrici di cui abbiamo parlato possono oggi essere eseguiti al computer mediante opportuni pacchetti di software come per esempio: Derive, Maple, Mathematica...

Nel seguito useremo il nome Derive per indicare un pacchetto di calcolo algebrico e grafica, ma ogni altro programma con caratteristiche analoghe può andare altrettanto bene.

In mancanza di uno di questi si può usare anche uno dei tanti pacchetti, più semplici, reperibili liberamente in internet, come ad esempio il seguente:

Geogebra: http://www.geogebra.org/cms/it/

che è una delle tante proposte del sito:

Alpha: https://www.wolframalpha.com/

Proponiamo alcune attività al computer che possono aiutare la comprensione e la verifica dell'apprendimento di quanto visto relativamente alla teoria delle equazioni ed in particolare a quanto detto nell'ultimo paragrafo.

Esercizio 2.1. Calcolare con Derive le soluzioni reali delle equazioni $F(x) = 0$ sia nella modalità "soluzioni esatte" sia in quella ''soluzioni approssimate'', commentando le risposte fornite dal computer alla luce della teoria studiata:

$F(x) = x^3 - 3$	$F(x) = x^4 - 3$	$F(x) = x^5 - 3$
$F(x) = x^4 - 3x^2$	$F(x) = x^3 - 3x^2$	$F(x) = x^3 - 6x^2 - 9x = 0$
$F(x) = x^3 - 12x + 2$	$F(x) = x^4 - 12x + 2$	$F(x) = x^5 - 12x + 2$

Esercizio 2.2. Disegnare mediante Derive i grafici delle funzioni $y = F(x)$, dove i polinomi $F(x)$ sono dati nell'Esercizio 2.1. Determinare le radici di $F(x)$ mediante il cursore e confrontare i risultati con quelli ottenuti precedentemente.

Esercizio 2.3. Disegnare mediante Derive i grafici delle funzioni $y = G(x)$ dove:

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

Osservare i grafici ottenuti per riconoscere la molteplicità delle varie radici a seconda dell'andamento vicino ai punti di intersezione con l'asse delle ascisse.

Esercizio 2.4. Disegnare a mano i grafici delle funzioni $y = P(x)$ in base alle loro radici e alle proprietà enunciate nel precedente paragrafo e poi confrontare i risultati con i corrispondenti grafici fatti con Derive:

$P(x) = x^2(x - 2)$	$P(x) = x(x - 3)^2$
$P(x) = -2x(x^2 - 9)$	$P(x) = -x(x^2 + 9)$
$P(x) = -2x^2(x + 3)$	$P(x) = (3 - x)(x - 3)(x + 3)(2x + 1)$

Esercizio 2.5. Valutare il numero di soluzioni reali delle seguenti equazioni $P(x) = 0$ disegnando, mediante Derive, il grafico delle funzioni $y = P(x)$; determinare un intervallo (possibilmente ''piccolo'') che contiene ciascuna di esse e poi trovare le soluzioni mediante Derive:

a. $P(x) = x^3 - 3x^2 - 2x + 1$	**b.** $P(x) = x^3 - 3x^2 - 2x - 1$
c. $P(x) = x^3 + x^2 - 4x + 2$	**d.** $P(x) = x^4 - 3x^2 - 2x + 1$
e. $P(x) = x^5 + 3x^2 - 2x - 1$	**f.** $P(x) = x^4 + 3x^2 - 2x + 1$
g. $P(x) = x^4 - 3x^2 - 2x - 0,1$	**h.** $P(x) = x^5 - 3x^2 - 2x + 1$
i. $P(x) = x^5 + 3x^2 - 2x - 1$	**l.** $P(x) = x^5 + x^4 - 4x + 2,4.$

Esercizio 2.6. Dato il disegno di un grafico di funzione polinomiale, immaginare quale potrebbe essere un possibile polinomio $Q(x)$ il cui grafico sia quello assegnato (o almeno abbia lo stesso andamento generale e le stesse

proprietà principali). I grafici **proposti dall'insegnante** potrebbero essere ottenuti ad esempio dai polinomi seguenti:

$$Q(x) = x(x-2)(4-x)^2 \qquad Q(x) = (x-1)^3(1+2x)$$
$$Q(x) = (x-1)^2(3x+2) \qquad Q(x) = x^2(x-2)(3+x)$$

Esercizio 2.7. Ripetere l'Esercizio 2.6 come gara tra due gruppi di studenti: uno dei due gruppi propone un grafico e l'altro gruppo deve 'indovinare' da quale polinomio è ottenuto. La risposta deve essere ''ragionevolmente corretta'' e i due gruppi possono sostenere le loro ragioni pro o contro la correttezza della risposta. L'insegnate è l'arbitro e decide.

L'anello dei polinomi

Introduciamo ora alcune notazioni e terminologie relative ai polinomi comunemente usate in matematica.

Intanto l'insieme di tutti i polinomi ha un simbolo particolare; più esattamente ci sono molti simboli diversi a seconda del tipo di coefficienti e delle indeterminate considerate.

L'insieme dei polinomi con cui abbiamo in genere fin qui lavorato si denota $\mathbb{R}[x]$ perché i coefficienti sono tutti i possibili numeri reali e vi è una sola indeterminata, indicata con la lettera x.

Nel paragrafo **Soluzioni razionali** abbiamo invece considerato i polinomi dell'insieme $\mathbb{Q}[x]$ (coefficienti razionali e indeterminata x) oppure dell'insieme $\mathbb{Z}[x]$ (coefficienti interi e indeterminata x).

Le equazioni delle curve del piano cartesiano che si studiano in geometria analitica (rette, circonferenze, parabole, ...) sono date da polinomi dell'insieme $\mathbb{R}[x, y]$ (coefficienti in $\mathbb{R}$ e 2 indeterminate x e y).

In generale $A[x_1, \ldots, x_n]$ indica l'insieme di tutti i polinomi a coefficienti in un certo insieme A e indeterminate $x_1, \ldots x_n$.

Consideriamo ora, per fissare le idee, i polinomi di $\mathbb{R}[x]$ (anche se molto di quello che diremo vale più in generale). Abbiamo più volte usato il fatto che tra i polinomi di $\mathbb{R}[x]$ si possono fare delle operazioni: la somma e il prodotto. Rispetto a queste operazioni, i polinomi godono di alcune proprietà che ben conosciamo per le operazioni tra numeri. Tra le altre:

1) la somma e il prodotto sono associative e commutative e vale la proprietà distributiva del prodotto rispetto alla somma;
2) c'è l'elemento neutro rispetto alla somma;
3) c'è l'opposto di ogni elemento;
4) c'è l'elemento neutro rispetto al prodotto.

In altre parole, la somma e il prodotto di due polinomi non dipendono dall'ordine:

$$F(x) + G(x) = G(x) + F(x) \quad \text{e} \quad F(x) \cdot G(x) = G(x) \cdot F(x).$$

Inoltre si ha:

$$F(x) \cdot (G(x) + H(x)) = F(x) \cdot G(x) + F(x) \cdot H(x).$$

L'elemento neutro rispetto alla somma è il polinomio nullo 0 che sommato a ogni altro polinomio lo lascia invariato: $F(x) + 0 = F(x)$; l'elemento neutro rispetto al prodotto è il polinomio costante 1 che moltiplicato a ogni altro polinomio lo lascia invariato: $F(x) \cdot 1 = F(x)$.

L'opposto di un polinomio $F(x)$ è $-F(x)$ ossia $(-1) \cdot F(x)$.

La validità per $\mathbb{R}[x]$ (o per ogni altro insieme dotato di due operazioni) di tutte queste proprietà si sintetizza dicendo che è un **anello commutativo con identità**.

Allo stesso modo $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sono anelli commutativi con identità, mentre $\mathbb{N}$ non lo è.

Possiamo anche dire che $\mathbb{R}$ e $\mathbb{Q}$ sono **campi**, perché per essi vale, oltre alle precedenti, anche la proprietà ulteriore seguente:

5) ogni elemento a diverso da zero ha un inverso ossia un elemento b tale che $ab = 1$.

Invece $\mathbb{Z}$ non è un campo perché ad esempio l'inverso di 2 non è un numero intero.

Gli elementi di un anello dotati di inverso si dicono **unità** oppure **elementi invertibili**. Gli unici elementi invertibili di $\mathbb{Z}$ sono 1 e -1.

Neppure $\mathbb{R}[x]$ è un campo; ad esempio non c'è alcun polinomio che moltiplicato per il polinomio x dia 1 ossia il polinomio x non è una unità di $\mathbb{R}[x]$.

In compenso, $\mathbb{R}[x]$ ha un'altra importante struttura algebrica, quella di **spazio vettoriale reale**. Si riparlerà di spazi vettoriali nelle lezioni sulle simmetrie.

Infine, come già detto, $\mathbb{R}[x]$ è un anello a **fattorizzazione unica**.

★ Equazioni di terzo grado

⋆ **Rivalità e colpi bassi.** *Già l'equazione generale di terzo grado richiese considerazioni piuttosto sofisticate e resistette agli sforzi di tutti i matematici dell'antichità. Essa fu risolta solo nei primi anni del Cinquecento, all'epoca del Rinascimento, dal matematico italiano Scipio Dal Ferro.*

Com'era in uso a quei tempi, Dal Ferro non pubblicò la sua scoperta, ma la comunicò a uno dei suoi allievi. Costui, dopo la morte di Dal Ferro, sfidò in una gara uno dei più forti matematici italiani, Tartaglia, proponendogli di risolvere una serie di equazioni di terzo grado. Tartaglia (1500-57) accettò la sfida e otto giorni prima della fine della gara trovò un metodo per risolvere qualsiasi equazione cubica della forma $x^3+px+q=0$. In due ore egli risolse tutti i problemi dell'avversario.

Cardano (1501-76), professore a Milano di matematica e fisica, avendo saputo della scoperta di Tartaglia, cominciò a pregarlo di comunicargli il suo segreto. Tartaglia alla fine cedette, ma con la promessa che Cardano avrebbe conservato segreto quel metodo. Invece Cardano non mantenne la promessa e pubblicò la scoperta di Tartaglia nella sua opera Ars Magna.

La formula per la soluzione dell'equazione cubica da allora è stata chiamata formula di Cardano, ma sarebbe più giusto chiamarla formula di Tartaglia.[1]

⋆ **La formula.** Osserviamo innanzi tutto che possiamo limitarci a trattare equazioni di terzo grado in cui manchi il termine quadratico. Possiamo infatti ricondurre il generico polinomio di terzo grado

$$y^3 + ay^2 + by + c$$

al tipo voluto mediante il cambio di variabile $x = y - \frac{a}{3}$, come si può facilmente verificare con calcoli diretti.

Consideriamo quindi una equazione del tipo:

$$x^3 + px + q = 0. \tag{1}$$

Poniamo ora $x = u + v$ e sostituiamo, ottenendo:

$$(u+v)^3 + p(u+v) + q = 0,$$

ovvero

$$u^3 + v^3 + q + (3uv + p)(u+v) = 0.$$

Poniamo ora $uv = -\frac{p}{3}$. Una simile sostituzione è lecita in quanto assegnati comunque due numeri A e B, è sempre possibile risolvere il sistema:

$$\begin{cases} u + v = A \\ u \cdot v = B \end{cases}$$

Basterà che u sia una soluzione (reale o complessa!) dell'equazione di secondo grado

$$u(A-u) = B \qquad \text{ossia} \qquad u^2 - Au + B = 0$$

[1] Da LE MATEMATICHE di A. D. Aleksandrov, A. N. Kolmogorov, M. A. Laurent'ev (Bollati Boringhieri).

e che v sia $A - u$.

Con questa scelta di u e v otteniamo:

$$\begin{cases} u^3 + v^3 + q = 0 \\ uv = -\frac{p}{3} \end{cases} \tag{2}$$

Se i numeri u e v soddisfano questo sistema di equazioni, il numero $x = u+v$ sarà una soluzione dell'equazione (1).

Moltiplicando la prima equazione del sistema (2) per u^3 e poi sostituendo $(\frac{-p}{3})^3$ al posto di u^3v^3 otteniamo una equazione quadratica nell'incognita $z = u^3$:

$$z^2 + qz - \frac{p^3}{27} = 0.$$

Risolvendola con la solita formula, otteniamo

$$u^3 = z = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad , \quad v^3 = -q - u^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

da cui

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

che è la formula di Cardano-Tartaglia.

Subito dopo che fu risolta l'equazione cubica, Ferrari (1522-65) risolse anche l'equazione generica di quarto grado.

Se per la soluzione dell'equazione di terzo grado occorreva preliminarmente risolvere una equazione quadratica ausiliaria, analogamente, per risolvere l'equazione di quarto grado bisogna basarsi sulla soluzione preliminare di un'equazione cubica ausiliaria.

★ Le funzioni simmetriche

Consideriamo una equazione di secondo grado $x^2+px+q = 0$ e supponiamo che abbia due soluzioni a e b, ossia $x^2 + px + q = (x - a)(x - b)$. Avremo allora:

$$p = -(a + b) \quad \text{e} \quad q = ab.$$

L'equazione esaminata è perfettamente individuata se si conoscono i due coefficienti p e q e, allo stesso modo, è perfettamente individuata se si conoscono le due soluzioni a e b.

Con una grossa differenza:

se si scambiano tra loro i coefficienti p e q si ottiene in generale un'altra equazione, mentre se si scambiano tra loro le soluzioni a e b l'equazione non cambia.

Ciò è dato dal fatto che $p = -(a+b) = -(b+a)$ e $q = ab = ba$ ossia:

$$x^2 - (a+b)x + ab = x^2 - (b+a)x + ba.$$

Si dice allora che i coefficienti dell'equazione di 2° grado si possono esprimere come

funzioni simmetriche

delle soluzioni.

In questa semplice osservazione c'è in germe l'idea geniale della **Teoria di Galois** che permette di stabilire quali equazioni sono risolubili per radicali e quali no: per approfondire questo argomento si veda la Lezione 6.

La formula risolutiva dell'equazione di secondo grado ci suggerisce anche, come già notato in precedenza, un'altra osservazione:

non tutte le equazioni di secondo grado ammettono soluzioni reali.

Una equazione senza soluzioni è un po' una sconfitta per la matematica. però anche questo ostacolo può essere superato allargando l'insieme numerico in cui cercare le soluzioni, ossia con la costruzione dei **numeri complessi**.

Teorema fondamentale dell'algebra:

Ogni equazione polinomiale $F(x) = 0$ di grado n a coefficienti reali ha sempre esattamente n soluzioni nell'insieme dei **numeri complessi** (pur di contare ciascuna con la sua molteplicità).
Tra queste n soluzioni ve ne sono m che sono numeri reali, dove m è compreso tra 0 e n e inoltre m ha la stessa parità di n ossia è pari se n è pari ed è dispari se n è dispari.

Per approfondire si vedano le Lezioni 3 e 4.

Anche nel caso delle equazioni di terzo grado i coefficienti si possono esprimere mediante le radici; più precisamente siano α, β, γ le soluzioni dell'equazione $x^3 + ax^2 + bx + c = 0$ (supponiamo di essere nel caso più generale in cui sono tutte diverse).

Per il Teorema di Ruffini avremo allora

$$x^3 + ax^2 + bx + c = (x-\alpha)(x-\beta)(x-\gamma)$$

e quindi:

$$\begin{cases} a &= -(\alpha+\beta+\gamma) \\ b &= +(\alpha\beta+\alpha\gamma+\beta\gamma) \\ c &= -(\alpha\beta\gamma) \end{cases}$$

Anche in questo caso a, b, c non cambiano se permutiamo tra loro le tre soluzioni.

Esempio 2.8. *Supponiamo di scrivere nei secondi membri β al posto di α, γ al posto di β e α al posto di γ. Otteniamo :*

$$\begin{cases} -(\beta+\gamma+\alpha) \\ +(\beta\gamma+\beta\alpha+\gamma\alpha) \\ -(\beta\gamma\alpha) \end{cases}$$

che sono ancora a, b, c rispettivamente, esattamente come prima.

I tre coefficienti sono quindi **funzioni simmetriche** delle soluzioni. Non si tratta però di tre qualsiasi funzioni simmetriche, ma dei "mattoncini di base" di tutte le funzioni simmetriche di 3 variabili. Infatti ogni funzione simmetrica di 3 variabili α, β, γ può essere costruita utilizzando somme, prodotti, quozienti ecc. a partire dalle tre funzioni elementari $F_1 = \alpha+\beta+\gamma$, $F_2 = \alpha\beta+\alpha\gamma+\beta\gamma$, $F_3 = \alpha\beta\gamma$.

Allo stesso modo, esprimendo i coefficienti dalle equazioni di quarto, quinto, ... grado per mezzo delle soluzioni delle equazioni stesse, si ottengono le funzioni simmetriche elementari in 4, 5, ... variabili.

⁕ Chi erano....

Niel Henrik Abel. Abel nacque nel 1802 in un paesino della Norvegia che in quel periodo era spaventosamente povera in seguito a guerre e carestie. La sua numerosa famiglia (erano sette fratelli), sebbene rispettabile ed istruita, viveva in gravi ristrettezze economiche.
L'ingegno di Abel si manifestò presto. Il primo ad accorgersene fu un suo insegnante, un matematico, che fece pubblicare una prima raccolta di opere di Abel ancora sedicenne.

Quando Abel aveva diciotto anni suo padre morì e, come secondogenito, gran parte del carico economico della famiglia ricadde su di lui. Così dava lezioni per mantenere la famiglia e trovava anche il tempo per dedicarsi alle sue ricerche matematiche: si stava occupando delle equazioni di quinto grado.

In un primo momento Abel credette di avere trovato una formula risolutiva, ma già nel 1824 pubblicò una memoria in cui dava la dimostrazione

dell' impossibilità di trovare una tale formula generale.
Una precedente dimostrazione, meno soddisfacente, era stata pubblicata da Paolo Ruffini nel 1799; perciò i due nomi compaiono insieme nel ben noto teorema di Abel - Ruffini.
Questo teorema, uno dei più importanti e famosi dell'algebra, venne presentato da Abel quando a Parigi visitò Legendre, Cauchy e altri matematici. Durante questo viaggio egli scrisse a un amico delle difficoltà che incontrava a farsi ascoltare:

"*Ho appena terminato un ampio trattato su una certa classe di funzioni trascendenti, ma il sig. Cauchy non si è neanche degnato di dargli un'occhiata.*"

Abel sperava di trovare un posto come professore universitario; per questo lasciò a Cauchy la sua memoria perché potesse esaminarla e presentarla all' Istituto (l'Accademia delle Scienze), ma Cauchy la smarrì, con il risultato che fu pubblicata solo quando per Abel era ormai troppo tardi.
Durante la sua permanenza a Parigi, infatti, Abel contrasse la tubercolosi; egli continuò comunque ad occuparsi della sua famiglia e degli studi e solo alla fine si concesse qualche giorno con Crelly, la sua fidanzata ormai da cinque anni. Abel morì il 6 aprile 1829 prima di aver compiuto ventotto anni.
Due giorni dopo arrivò una lettera di Crelle, suo amico e sostenitore, che gli annunciava di essere finalmente riuscito a farlo nominare professore di matematica all'università di Berlino.

Dopo la sua morte, sotto la spinta di Jacobi, il console di Norvegia a Parigi fece un'istanza perché si ritrovasse il manoscritto scomparso; Cauchy lo ritrovò nel 1830, anno in cui l'Accademia fece onorevole ammenda nei riguardi di Abel, concedendogli il gran premio di matematica, assieme a Jacobi.

Evariste Galois. Galois nacque nel distretto di Parigi, il 25 ottobre 1811, da una famiglia borghese, colta e politicamente contraria alla monarchia.

I suoi primi 11 anni furono felici; studiava con sua madre che gli trasmise una buona cultura classica e scriveva poesie come suo padre.
Dodicenne, entrò al liceo a Parigi: una vera prigione con regole ferree, porte chiuse a chiave e un preside tirannico.

Grazie alla sua educazione classica si distingueva nelle materie letterarie, finchè non si manifestò in lui un esclusivo interesse per la matematica, che lo portò a trascurare le altre materie tanto che fu bocciato.

Ciò nonostante, le sue qualità non erano apprezzate neppure dagli insegnati di matematica. A 16 anni quando si presentò agli esami della Scuola Politecnica, fu respinto e questa sconfitta lo segnò per tutta la vita.
Nel 1828 incontrò Richard, un professore di matematica che comprese il suo genio sostenendolo negli studi e presentandolo a Cauchy, il quale (anche con lui!) non rispettò la promessa di presentare una sua memoria. Questo episodio non fece altro che aumentare il disprezzo di Galois per le accademie e gli accademici.
A 18 anni si ripresentò al Politecnico ma fu nuovamente respinto; esasperato dall'esaminatore, gli lanciò in faccia un cancellino, causando un grave scandalo.
In quello stesso periodo, ad aggravare il suo stato d'animo, arrivò la notizia della tragica morte di suo padre, suicida a causa di calunnie politiche.

Dopo essersi preparato da solo agli esami finali a 19 anni Galois entrò all' Università e partecipò al Gran Premio di Matematica. Il suo manoscritto giunse al segretario del concorso, che però morì prima di averlo letto e del manoscritto si perse ogni traccia. Questo episodio, sommato a quello di Cauchy, incrementò l'odio di Galois per il sistema e lo portò a gettarsi nella politica.

Cacciato dalla scuola, nel 1831 si unì alla protesta di un gruppo di giovani repubblicani contro il decreto reale di scioglimento del corpo di artiglieria a cui apparteneva; in seguito alla protesta, forse per un malinteso, fu arrestato. Prosciolto da quella prima accusa, dopo pochi mesi fu nuovamente arrestato e condotto in carcere, dove trovò unico rifugio e conforto nella matematica.
Uscito dal carcere in seguito a un'epidemia di colera, per un motivo non del tutto chiaro finì coinvolto in un duello alla pistola. Passò la notte della vigilia a stendere le sue ultime scoperte matematiche. In ciò che scrisse si trova una completa risposta alla questione della risolubilità per radicali delle equazioni. Egli creò così una teoria che ancora oggi porta il suo nome ed è fondamento dell' algebra moderna.

All'alba del 30 maggio 1832 Galois cadde colpito al ventre. Morì il giorno

successivo, ancora ventenne.

♣ Esercizi per la seconda lezione

2.1 Disegnare "a mano" il grafico delle seguenti funzioni $y = F(x)$ e poi controllare la correttezza del disegno fatto confrontandolo con quello eseguito mediante Derive:

a. $F(x) = \frac{1}{3}(x-2)(x+\sqrt{3})(x-1)$ **b.** $F(x) = -3(x-2)^2(x+\frac{1}{2})$
c. $F(x) = x(x-2)^3$ **d.** $F(x) = x(x+\frac{1}{3})^2(x-\frac{1}{3})^2$
e. $F(x) = \frac{x^2(\sqrt{3}-x)^3}{5}$ **f.** $F(x) = x - x^3$.

2.2 Disegnare "a mano" in uno stesso riferimento cartesiano i grafici delle due funzioni $y = (x-1)^3$ e $y = x^3 - x$ individuando i punti in cui i due grafici si incontrano. Confrontare poi coll'analogo disegno fatto mediante Derive.

2.3 Si consideri l'equazione $x^3 + x - 2 = 0$.

a. Determinarne tutte le soluzioni razionali.
b. Determinarne tutte le soluzioni reali.
c. Scrivere mediante la formula di Cardano una soluzione di tale equazione e confrontare il risultato con quanto ottenuto ai punti precedenti.

2.4 Determinare le soluzioni razionali dell'equazione $x^3 - 2x + 1 = 0$.
Trovare una soluzione di $x^3 - 2x + 1 = 0$ mediante la formula di Cardano.
Si possono a questo punto trovare tutte le soluzioni di questa equazione?

2.5 Quali delle proprietà degli anelli non sono soddisfatte da $\mathbb{N}$?

2.6 Provare che il polinomio $x + 1$ non ha inverso nell'anello dei polinomi $\mathbb{R}[x]$.

2.7 Scrivere i coefficienti di una equazione di terzo grado monica per mezzo delle sue radici a, b, c.

2.8 Elencare tutte le sequenze ordinate in cui si possono disporre le tre lettere a, b, c.

2.9 Dire se le seguenti espressioni nelle lettere a, b, c sono oppure non sono funzioni simmetriche:

- $f(a, b, c) = a^2 + b^2 + c^2 - 3abc$;
- $g(a, b, c) = ab^2 + bc^2 + ca^2$;
- $h(a, b, c) = ab - bc + ca$;

Modulo 2

I numeri complessi

Lezione 3

I numeri complessi

Il numero i

Nelle lezioni precedenti abbiamo visto che non tutte le equazioni polinomiali hanno soluzioni in $\mathbb{R}$; il più semplice esempio di equazione senza soluzioni reali è $x^2 + 1 = 0$.

Introduciamo un numero nuovo, che chiameremo i che sia una soluzione di questa equazione, ossia che abbia la proprietà di avere il quadrato uguale a -1:

$$i^2 = -1.$$

Affinché questa costruzione abbia un senso, non possiamo limitarci ad ampliare i numeri reali mediante la sola aggiunta del nuovo numero i, ma dobbiamo far sì che si possano eseguire anche somme e prodotti. Dovremo quindi introdurre anche tutti i numeri del tipo $2i$, $3 + i$, $(i^2 + 5)(\sqrt{2}i - \pi)$ e così via.

Definizione 3.1. *Chiamiamo* **numeri complessi** *tutte le espressioni della forma $a + ib$ dove a e b sono numeri reali.*

Il numero complesso i si dice **unità immaginaria**.

Se $z = a + ib$, il numero reale a si dice **parte reale** di z, denotata $\mathrm{Re}(z)$, e il numero reale b si dice **coefficiente dell'immaginario** di z, denotato $\mathrm{Im}(z)$.

Due numeri complessi sono uguali se e solo se coincidono tra loro le parti reali e coincidono tra loro quelle immaginarie:

$$a + ib = a' + ib' \iff \begin{cases} a = a' \\ b = b' \end{cases}$$

Definiamo le operazioni di somma e prodotto in $\mathbb{C}$ a partire dalle operazioni di $\mathbb{R}$ secondo le regole del calcolo algebrico nel modo seguente:

$$(a+ib)+(c+id)=a+ib+c+id=(a+c)+i(b+d)$$

$$(a+ib)\cdot(c+id)=ac+iad+ibc+i^2bd=ac+iad+ibc-bd= \\ =(ac-bd)+i(ad+bc)$$

Per come sono state definite le operazioni:

(*) possiamo pensare ogni numero reale a come un particolare numero complesso che ha parte immaginaria nulla, ossia a **è** anche il numero complesso $a+i0$.

In $\mathbb{C}$ valgono tante delle proprietà delle operazioni che conosciamo in $\mathbb{R}$. Eccone alcune:

1) la somma e il prodotto sono associative e commutative e vale la proprietà distributiva del prodotto rispetto alla somma;
2) c'è l'elemento neutro rispetto alla somma, infatti:
$$0+(a+ib)=a+ib;$$
3) c'è l'opposto di ogni elemento, infatti:
$$-(a+ib)=(-a)+i(-b);$$
4) c'è l'elemento neutro rispetto al prodotto, infatti:
$$1\cdot(a+ib)=a+ib;$$
5) ogni numero complesso, tranne 0, ha un inverso, infatti:
$$(a+ib)^{-1}=\frac{a}{a^2+b^2}-i\frac{b}{a^2+b^2}.$$

La validità di 1), 2) 3), 4) si esprime nel linguaggio dell'algebra dicendo che $\mathbb{C}$ è un **anello**; la loro validità unita a quella di 5) si esprime dicendo che $\mathbb{C}$ è un **campo**. L'insieme complessivo delle proprietà sopra enunciate (*) 1), ..., 5) si condensa nel liguaggio dell'algebra delle strutture nel modo seguente:

L'insieme $\mathbb{C}$ dei numeri complessi con le operazioni $+$ e $\cdot$ è un campo che estende il campo $\mathbb{R}$.

Ritorniamo ora all'equazione $x^2+1=0$ per osservare che in $\mathbb{C}$ risulta avere, oltre alla soluzione $x=i$, anche la soluzione $x=-i$, come si può verificare immediatamente tramite sostituzione.

Il numero complesso $-i$ ha in realtà le stesse proprietà di i e risulta essere perfettamente intercambiabile con i.

Se $z = a + ib$ è un qualsiasi numero complesso, scambiando in esso i con $-i$ otteniamo il numero complesso $\overline{z} = a - ib$, che si dice **coniugato** di z.

Lasciamo come esercizio la verifica delle seguenti proprietà del coniugato di ogni numero complesso z:

a) la somma di un numero e del suo coniugato $z + \overline{z}$ è un numero reale;

b) i numeri reali sono gli unici numeri complessi che coincidono col loro coniugato: $z = \overline{z} \Longleftrightarrow z \in \mathbb{R}$;

c) il prodotto di un numero diverso da 0 e del suo coniugato $z \cdot \overline{z}$ è sempre un numero reale strettamente positivo.

d) il coniugato di una somma coincide con la somma dei coniugati, ossia

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$$

e) il coniugato di un prodotto coincide col prodotto dei coniugati, ossia

$$\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$$

Si dice **modulo** del numero complesso $z = a + ib$ il numero reale positivo o nullo

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}.$$

Da quanto sopra risulta $|z| = 0$ se e solo se $z = 0$.

Possiamo allora rivedere in altro modo la formula dell'inverso di un numero complesso:

$$z^{-1} = \frac{\overline{z}}{z \cdot \overline{z}} \qquad \text{cioè} \qquad z^{-1} = \frac{\overline{z}}{a^2 + b^2}.$$

Il Teorema Fondamentale dell'Algebra.

Dalla formula risolutiva delle equazioni di 2° grado risulta chiaramente che non solo $x^2 + 1 = 0$, ma **tutte le equazioni di grado** 2 a coefficienti reali $x^2 + px + q = 0$ hanno due soluzioni complesse, eventualmente coincidenti.

Infatti, se il discriminante $\Delta = p^2 - 4q$ è positivo o nullo, ci sono le due radici reali (eventualmente coincidenti) $-\frac{p}{2} + \frac{\sqrt{\Delta}}{2}$ e $-\frac{p}{2} - \frac{\sqrt{\Delta}}{2}$, mentre se Δ è negativo (**e quindi $-\Delta$ è un numero reale positivo!**), ci sono le due radici complesse (non reali) $-\frac{p}{2} + i\frac{\sqrt{-\Delta}}{2}$ e $-\frac{p}{2} - i\frac{\sqrt{-\Delta}}{2}$.

Si noti che queste ultime sono due numeri **complessi coniugati** ossia ottenibili uno dall'altro scambiando i con $-i$, ossia passando ai coniugati!

Introducendo semplicemente il nuovo numero i siamo così riusciti a risolvere tutte le equazioni di secondo grado. Ma le proprietà di $\mathbb{C}$ vanno ben oltre.

Ampliando $\mathbb{R}$ in modo da poter risolvere l'equazione $x^2 + 1 = 0$ succede che **tutte** le equazioni, non solo quelle di secondo grado, diventano risolubili. Vale infatti il seguente importantissimo risultato:

Teorema fondamentale dell'algebra:

Ogni equazione polinomiale di grado positivo n a coefficienti reali

$$x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = 0$$

ha sempre n soluzioni complesse (eventualmente coincidenti) $\alpha_1, \alpha_2, \ldots, \alpha_n$, ossia il polinomio

$$F(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n$$

si decompone nel prodotto di polinomi di grado 1:

$$F(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n).$$

Come nel caso delle equazioni di secondo grado, anche nel caso delle equazioni di grado n può capitare che tutte le soluzioni siano numeri reali, oppure che lo siano solo alcune di esse, oppure nessuna. Può quindi capitare che ci siano soluzioni che sono numeri complessi non reali.

Le proprietà del coniugio che abbiamo elencato nel paragrafo precedente permettono di provare con semplici verifiche la seguente importante proprietà :

se $F(x)$ è un polinomio a coefficienti reali e α è una soluzione dell'equazione $F(x) = 0$, allora anche il suo coniugato $\overline{\alpha}$ è soluzione della stessa equazione.

Se α è reale, allora $\overline{\alpha} = \alpha$; se invece α non è reale, allora α e $\overline{\alpha}$ sono due soluzioni distinte. Quindi tra le n soluzioni di una equazione di grado n, quelle non reali sono sempre in numero pari, perché sono due a due coniugate l'una dell'altra.

Il polinomio $F(x)$ è allora divisibile per $x - \alpha$ e per $x - \overline{\alpha}$ (Teorema di Ruffini) e quindi è divisibile anche per il loro prodotto $(x - \alpha)(x - \overline{\alpha})$ (grazie alla proprietà di fattorizzazione unica). Contrariamente a quanto può

sembrare a prima vista, una volta eseguiti i calcoli il polinomio di secondo grado $(x-\alpha)(x-\overline{\alpha})$ risulta sempre avere **coefficienti reali**!

Possiamo allora dedurre dal teorema fondamentale dell'algebra che

ogni polinomio a coefficienti reali si decompone nel prodotto di polinomi reali di grado 1 (corrispondenti alle sue radici reali) e di polinomi reali di grado 2 con discriminante Δ negativo (corrispondenti alle coppie di radici coniugate non reali).

Nel caso delle equazioni di secondo grado, possiamo interpretare l'informazione fornita dal discriminante nel modo seguente:

il discriminante di un'equazione di secondo grado dice se passando ai coniugati le soluzioni di quell'equazione rimangono invariate oppure si modificano scambiandosi tra loro.

In generale l'azione del coniugio opera una **permutazione** tra le soluzioni di un'equazione, che lascia fisse le soluzioni reali e scambia tra loro due a due quelle non reali.

Vi sono molti modi di dimostrare il Teorema Fondamentale dell'Algebra, nessuno di essi è però del tutto elementare; sono infatti richieste nozioni superiori di analisi, oppure di geometria oppure di algebra.

★ I numeri complessi esistono?

Quello che abbiamo visto è un approccio semplice e intuitivo a $\mathbb{C}$, mentre una **vera** costruzione dei numeri complessi va al di là degli scopi e del tempo di questo corso.

É opportuno comunque sottolineare che l'idea da noi utilizzata, ossia quella di rendere risolubile un'equazione introducendo un nuovo simbolo che indica una sua soluzione, potrebbe riservare delle spiacevoli sorprese.

Potremmo ad esempio provare a rendere risolubile l'equazione $0x = 1$ ampliando $\mathbb{R}$ con un nuovo simbolo α che indica una sua soluzione ossia tale che $0\alpha = 1$. Questo procedimento porterebbe però a una inevitabile contraddizione. Infatti moltiplicando per α i due membri dell'uguaglianza $0 = 0 + 0$ otterremmo $0\alpha = 1$ a primo membro e, grazie alla proprietà distributiva, $(0+0)\alpha = 0\alpha + 0\alpha = 1 + 1 = 2$ a secondo membro, da cui $1 = 2$.

Nel caso dei numeri complessi, possiamo però stare tranquilli: l'unità immaginaria i **esiste veramente** per quel che questa espressione significa in matematica, ossia:

la costruzione di i e dei numeri complessi non causa contraddizioni.

L'unico "problema" causato dall'introduzione del numero i è la perdita dell'**ordinamento** $\leq$ tra i numeri. Non si può infatti parlare di numeri complessi positivi e di numeri complessi negativi.

Potremmo introdurre un qualche ordine tra i complessi in molti modi; ad esempio potremmo usare l'ordine **lessicografico** (analogo a quello delle parole nel vocabolario) chiamando minore tra due numeri complessi quello con parte reale minore e, a parità di parte reale, quello con coefficiente dell'immaginario minore. Però né questo, né alcun altro ordinamento di $\mathbb{C}$ "va d'accordo" con le operazioni.

Un ordinamento va d'accordo con le operazioni se le diseguaglianze si conservano sommando ai due membri uno stesso numero a; inoltre per ogni fissato a ($a \neq 0$), la moltiplicazione per a conserva tutte le diseguaglianze oppure rovescia tutte le diseguaglianze. In particolare, moltiplicare due volte i due membri per uno stesso numero deve in ogni caso conservare le diseguaglianze.

In $\mathbb{C}$ questo non può succedere perché si avrebbe la contraddizione:

$$a < b \iff i{\cdot}i{\cdot}a < i{\cdot}i{\cdot}b \iff -a < -b \iff -a+(a+b) < -b+(a+b) \iff b < a.$$

♣ Esercizi per la terza lezione

3.1 Ridurre le seguenti espressioni alla forma $a + ib$ specificando qual è la parte reale e quale quella immaginaria

$$\begin{array}{lll} (3+4i)+(2+5i) & ; \quad (3+4i)(4+5i) & ; \quad (1+3i)(6-6i) \\ 3i(4+i)^2 & ; \quad (1+\sqrt{3})^3 & ; \quad (2+3i)(2-3i). \end{array}$$

3.2 Calcolare la parte reale e la parte immaginaria dei seguenti numeri complessi:

$$(1+i)(2i-3), \quad (2-i)^2, \quad (1-3i)^3, \quad \frac{6+5i}{3-i}, \quad \frac{3-2i}{1+5i}+\frac{2-3i}{2-i}.$$

3.3 Dire se il numero complesso $-1+i$ è oppure no una soluzione dell'equazione $x^3 - 2x^2 + 5x - 2 = 0$.

3.4 Verificare che i numeri complessi $(1 + i\sqrt{3})$ e $(1 - i\sqrt{3})$ (oltre che naturalmente -2) sono radici del polinomio $x^3 + 8$. Eseguire la verifica sia mediante sostituzione, sia applicando il teorema di Ruffini.

3.5 Verificare che il coniugato di una somma è la somma dei coniugati e che il coniugato di un prodotto è il prodotto dei coniugati.

3.6 Verificare che si ha $z \cdot z' = 0$ se e soltanto se $z = 0$ oppure $z' = 0$.

3.7 Sia z un qualsiasi numero complesso. Verificare che $z + \overline{z}$ e $z \cdot \overline{z}$ sono numeri reali e che $z - \overline{z}$ è "immaginario puro"ossia ha parte reale nulla..

3.8 Si consideri il polinomio $F(x) = 2x^5 - 13x^4 + 37x^3 - 57x^2 + 48x - 18$.

a) Verificare che $1 - i$ è radice di $F(x)$.

b) Trovare tutte le radici razionali di $F(x)$.

c) Determinare la fattorizzazione di $F(x)$ in fattori irriducibili in $\mathbb{R}[x]$.

3.9 Sia $f(x) = -3(x-2)^3(x-3i)(x-i+5)(x^2+x+1)(3i+x)(5+i+x)$

i) Provare senza eseguire i calcoli che, se $a \in \mathbb{R}$, allora $f(a) \in \mathbb{R}$.

ii) Determinare tutte le radici reali di $f(x)$ con la loro molteplicità.

Lezione 4

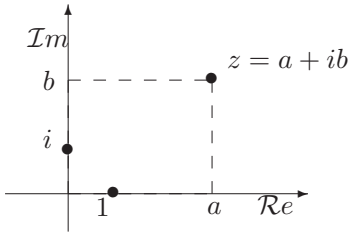
Forma polare dei numeri complessi

Il piano di Gauss

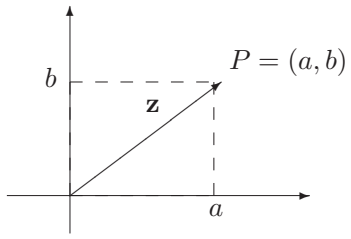
Un numero complesso $a + ib$ è individuato dalla coppia di numeri reali (a, b) e quindi, in modo del tutto naturale, possiamo fargli corrispondere il punto del piano cartesiano $\mathbb{R}^2$ di coordinate (a, b).

Col termine **Piano di Gauss** o Argand-Gauss si intende appunto il piano cartesiano $\mathbb{R}^2$ identificato col campo dei numeri complessi $\mathbb{C}$.

Lo zero di $\mathbb{C}$ corrisponde all'origine delle coordinate, i numeri reali corrispondono ai punti dell'asse X, i numeri immaginari puri, ossia con parte reale nulla, corrispondono ai punti dell'asse Y.



Oppure possiamo far corrispondere ogni numero complesso $z = a + ib$ ad un vettore applicato nell'origine e con secondo estremo nel punto P di coordinate (a, b).



La somma di due numeri complessi corrisponde alla somma in $\mathbb{R}^2$ di vettori applicati nell'origine.

Se, infatti, i numeri complessi $z_1 = a_1 + ib_1$ e $z_2 = a_2 + ib_2$ corrispondono ai punti $P = (a_1, b_1)$ e $Q = (a_2, b_2)$, allora la loro somma $z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2)$ corrisponde al punto $R = (a_1 + a_2, b_1 + b_2)$ individuato dalla somma di vettori $\overrightarrow{OP} + \overrightarrow{OQ} = \overrightarrow{OR}$ (cfr. Lezione 9).

GeoGebra supporta i numeri complessi; ad esempio è possibile simulare le operazioni con i numeri complessi digitando $z = 2 + 3i$ e utilizzando i vettori.

Osserviamo ora gli effetti della moltiplicazione di un numero complesso qualunque $z = a + ib$ per un numero reale qualsiasi k :

$$z \cdot k = (a + ib) \cdot k = ka + ikb$$

Nella rappresentazione geometrica, la moltiplicazione per un numero reale k trasforma il vettore (a, b) nel vettore (ka, kb) il che corrisponde alla moltiplicazione di un vettore per uno scalare, operazione che ha come effetto quello di ottenere un vettore con stessa direzione di quello dato, verso che si mantiene uguale a quello dato se $k > 0$ e che cambia se $k < 0$, e modulo che è k-volte quello di partenza.

Effettuiamo ora la moltiplicazione di $z = a + ib$ per l'unità immaginaria i. Si ha

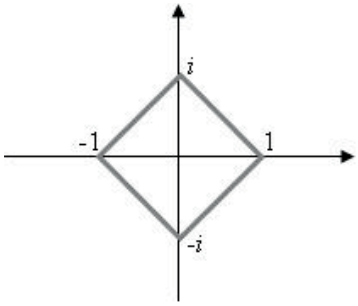
$$(a + ib) \cdot i = ai + i^2 b = -b + ia.$$

Al vettore (a, b) corrisponde perciò il vettore $(-b, a)$; esso ha lo stesso modulo di quello dato ma è ruotato rispetto ad esso di un angolo retto. Quindi *la moltiplicazione per i ha l'effetto di ruotare il vettore di un angolo retto in verso antiorario.*

Le potenze di i assumono ciclicamente i valori $1, i, -1, -i$, infatti

$$i^0 = 1; i^1 = i; i^2 = -1; i^3 = -i; i^4 = 1; i^5 = i; i^6 = -1; ...$$

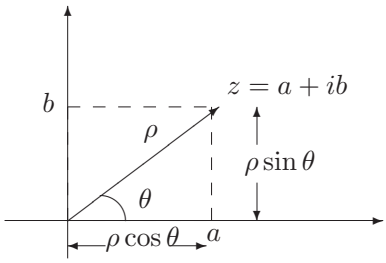
Esse si dispongono sui quattro vertici di un quadrato, come quello rappresentato in figura:



Per poter dare una buona interpretazione geometrica anche del prodotto, introduciamo la **rappresentazione trigonometrica** dei numeri complessi mediante le **coordinate polari**.

Ogni punto del $P = (a, b)$ del piano $\mathbb{R}^2$, $P \neq O$ (e quindi ogni numero complesso $z = a + ib \neq 0$) può essere individuato mediante una coppia di coordinate polari (ρ, θ):

- ρ è il numero reale positivo lunghezza del segmento $\overline{OP}$, ossia $\rho = \sqrt{a^2 + b^2}$
- θ è un qualsiasi angolo (misurato in radianti) tale che $a = \rho \cos\theta$ e $b = \rho \sin\theta$.



I numeri ρ e θ si dicono rispettivamente **modulo** e **argomento** di z. Indicheremo con $z = [\rho, \theta]$ il numero complesso con modulo ρ e argomento θ.

Per $z = 0$ definiamo come modulo $\rho = 0$, poiché corrisponde al segmento di lunghezza nulla $\overline{OO}$; non definiamo invece alcun argomento, che, d'altra parte, risulterebbe superfluo essendo 0 l'unico numero complesso con modulo nullo.

Se d'altra parte $z \neq 0$, allora vi sono infiniti possibili argomenti diversi. L'unico argomento θ_0 di z tale che $0 \leq \theta_0 < 2\pi$ si dice **argomento principale** di z; ogni altro argomento di z differisce da θ_0 per multipli interi

(positivi e negativi) di 2π: $\theta = \theta_0 + 2k\pi$, $k \in \mathbb{Z}$. Se θ_0 è un argomento del numero complesso z, sono argomenti di z anche $\theta_0 - 2\pi$, $\theta_0 + 4\pi$, ...

I passaggi da coordinate cartesiane a coordinate polari e viceversa si ottengono dalle relazioni:

$$\begin{array}{c}\text{da cartesiane}\\ \text{a}\\ \text{polari}\end{array} \quad \begin{cases} \rho = \sqrt{a^2+b^2} \\ \cos\theta = \frac{a}{\rho} \\ \sin\theta = \frac{b}{\rho} \end{cases} \quad ; \quad \begin{array}{c}\text{da polari}\\ \text{a}\\ \text{cartesiane}\end{array} \quad \begin{cases} a = \rho\cos\theta \\ b = \rho\sin\theta \end{cases}$$

Formula del prodotto in coordinate polari.

Siano z_1 e z_2 numeri complessi con coordinate polari $[\rho_1, \theta_1]$ e $[\rho_2, \theta_2]$. Allora il loro prodotto ha come modulo i prodotti dei due moduli e come argomento la somma dei due argomenti, ossia:

$$z_1 \cdot z_2 = [\rho_1 \cdot \rho_2 \quad , \quad \theta_1 + \theta_2].$$

Se infatti calcoliamo il prodotto $z_1 \cdot z_2$ usando le espressioni:

$$z_1 = \rho_1 cos\theta_1 + i\rho_1 sin\theta_1 \quad \text{e} \quad z_2 = \rho_2 cos\theta_2 + i\rho_2 sin\theta_2$$

otteniamo:

$$z_1 \cdot z_2 = (\rho_1\cos\theta_1 + i\rho_1\sin\theta_1)\cdot(\rho_2\cos\theta_2 + i\rho_2\sin\theta_2) =$$
$$= \rho_1\rho_2(\cos\theta_1\ \cos\theta_2 - \sin\theta_1\ \sin\theta_2) + i\rho_1\rho_2(\cos\theta_1\ \sin\theta_2 + \sin\theta_1\cos\theta_2).$$

Applicando a questo punto le formule che danno rispettivamente il coseno e il seno dell'angolo somma troviamo:

$$z_1 \cdot z_2 = \rho_1\rho_2\cos(\theta_1+\theta_2) + i\rho_1\rho_2\sin(\theta_1+\theta_2) = \rho_1\rho_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$$

che fornisce immediatamente modulo e argomento del prodotto dei due numeri complessi.

Un'applicazione particolarmente significativa della formula del prodotto è la seguente:

Potenze n-esime di un numero complesso.

Sia $z = [\rho, \theta]$ un numero complesso espresso mediante coordinate polari e sia n un numero intero.
Allora:

$$z^n = [\rho^n, n\theta].$$

Questa formula si ottiene applicando più volte la formula del prodotto. Inoltre essa vale anche nel caso in cui n sia lo zero o anche un numero intero negativo.

Applicando "a rovescio" la formula delle potenze si ottiene quella che consente di trovare **le radici n-esime** di un numero complesso.

Si noti che abbiamo usato radici n-esime al plurale. Infatti vi è una sola potenza n-esima di un numero z, ma vi sono esattamente n radici n-esime distinte di z (tranne nel caso in cui $z = 0$.)

Radici n-esime di un numero complesso

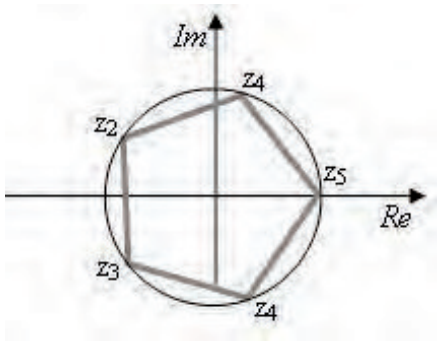
Sia $z = [\rho, \theta]$ un numero complesso non nullo, espresso mediante coordinate polari, e sia n un numero intero positivo.
Allora l'equazione $x^n = z$ ha esattamente n soluzioni distinte le cui espressioni in coordinate polari sono:

$$z_0 = \left[\sqrt[n]{\rho}\ ,\ \frac{\theta}{n}\right]\ ,\ z_1 = \left[\sqrt[n]{\rho}\ ,\ \frac{\theta + 2\pi}{n}\right], \dots$$

$$\dots\ ,\ z_k = \left[\sqrt[n]{\rho}\ ,\ \frac{\theta + 2k\pi}{n}\right], \dots, z_{n-1} = \left[\sqrt[n]{\rho}\ ,\ \frac{\theta + 2(n-1)\pi}{n}\right].$$

L'equazione polinomiale $x^n = z$ ha grado n e quindi non può avere più di n soluzioni distinte. Sarà allora sufficiente provare che quelle scritte sono soluzioni e che sono tutte diverse.

Se eleviamo z_k alla potenza n-esima usando la formula delle potenze in coordinate polari, troviamo un numero complesso che ha modulo ρ e argomento $\theta + 2k\pi$: è proprio z! Per verificare che sono tutte diverse le disegnamo nel piano di Gauss: esse si dispongono ai vertici di un poligono regolare con n lati inscritto nella circonferenza di centro l'origine e raggio $\sqrt[n]{\rho}$.



Esempio 4.1. *Vogliamo calcolare le soluzioni di* $x^4 = 1$ *ossia le radici quarte di* 1. *Sappiamo a priori che dovremo trovare* 4 *numeri complessi diversi.*

Una delle soluzioni è quella ovvia: 1.

Disegnamo allora nel piano di Gauss il quadrato, iscritto nella circonferenza di raggio $\sqrt[4]{1} = 1$*, e avente uno dei vertici in corrispondenza del numero* 1 *ossia nel punto di coordinate* $(1, 0)$*.*

Gli altri vertici del quadrato ci danno le altre soluzioni che risultano essere i*,* -1 *e* $-i$*.*

⊡ Attività al computer

I programmi che già abbiamo usato per calcolare le soluzioni di equazioni polinomiali possiedono anche l'opzione 'soluzioni complesse'. Possiamo riprendere alcuni degli esercizi al computer fatti nelle lezioni precedenti per eseguirli in questa nuova modalità. Possiamo anche chiedere di fattorizzare i polinomi nel prodotto di fattori reali oppure di fattori complessi.

Potremmo anche desiderare di poter vedere in modo grafico le soluzioni complesse di un'equazione come si è fatto per le soluzioni reali, disegnando il grafico della funzione $y = P(x)$. Purtroppo se x e y rappresentano entrambe numeri complessi, il nostro grafico dovrebbe essere disegnato in uno spazio a 4 dimensioni (2 per la x e 2 per la y), un po' troppo anche con il computer.

Possiamo però ridurci a 3 dimensioni (e disegnare in 3D) con il seguente artificio:

poiché a noi interessa soltanto vedere per quali valori di x il polinomio $P(x)$ si annulla, possiamo sostituire la funzione $y = P(x)$ con la funzione $y = |P(x)|$.

Il dominio della funzione sarà l'insieme dei numeri complessi $\mathbb{C}$ visualizzato come piano reale, ossia ogni valore complesso di x_0 corrsiponderà ad un punto del piano di coordinate (a_0, b_0) dove $x_0 = a_0 + ib_0$: nel disegno sarà il piano di quota 0.

Il valore assunto dal polinomio $P(x)$ nel punto $x = x_0$ è in generale un numero complesso, ma il suo modulo $|P(x_0)|$ è un numero reale, che sarà rappresentato dalla quota. Il grafico sarà allora formato dai punti dello spazio di coordinate $(a_0, b_0, |P(a_0 + ib_0)|)$. Poiché il modulo di un numero complesso z è nullo se e soltanto se z stesso è nullo, allora gli zeri della funzione $y = F(x)$ sono esattamente gli zeri della funzione $y = |P(x)|$ e saranno i punti del grafico di quota 0.

★ Cose strane tra i numeri

L'insieme $\mathbb{Z} + i\mathbb{Z}$, costituito dai numeri della forma $n + im$ con n ed m entrambi numeri interi, si chiama **anello degli interi di Gauss** ed è per molti versi simile all'anello dei numeri interi.

Ad esempio in esso è possibile fattorizzare tutti i numeri nel prodotto di numeri non ulteriormente fattorizzabili e questa decomposizione è essenzialmente unica, ossia può variare solo l'ordine dei fattori oppure qualcuno di essi può essere alterato mediante fattori invertibili (che sono soltanto $1,\ -1,\ i,\ -i$).

All'interno di $\mathbb{C}$ vi sono però altri anelli, in apparenza simili a questo, ma con strane proprietà . Vediamo come esempio un anello in cui non vale la proprietà di **fattorizzazione unica** che vale invece in $\mathbb{Z}$ e in $\mathbb{R}[x]$.

L'insieme dei numeri della forma

$$\mathbb{Z} + i\sqrt{5}\mathbb{Z} = \{a + i\sqrt{5}b \mid a, b \in \mathbb{Z}\}$$

è un **anello** come $\mathbb{Z}$.

Gli elementi invertibili di questo anello sono soltanto $1, -1$, ossia gli elementi che hanno modulo 1. Più in generale gli elementi di $\mathbb{Z} + i\sqrt{5}\mathbb{Z}$ hanno modulo il cui quadrato è sempre un numero intero: 0 per 0, 1 per gli invertibili, ≥ 4 per tutti gli altri (e quindi ≥ 16 per i numeri che sono il prodotto di due altri numeri non invertibili).

In questo particolare anello il numero 6 possiede due fattorizzazioni essenzialmente diverse in fattori irriducibili (non ulteriormente fattorizzabili):

$$2 \cdot 3 = (1 + \sqrt{5}i) \cdot (1 - \sqrt{5}i).$$

I fattori 2, 3, $(1+\sqrt{5}i)$ e $(1-\sqrt{5}i)$ hanno quadrato del modulo inferiore a 16 e sono quindi irriducibili; inoltre 2 e 3 non si possono ottenere moltiplicando $(1+\sqrt{5}i)$ o $(1-\sqrt{5}i)$ per un elemento invertibile, perché hanno modulo differente da questi ultimi: le due fattorizzazioni sono quindi essenzialmente diverse.

♣ Esercizi per la quarta lezione

4.1 Rappresentare sul piano di Argand-Gauss i seguenti numeri complessi

$$3 - 2i \quad ; \quad 2 + i \quad ; \quad 2 - i \quad ; \quad -\tfrac{3}{4} - i \quad ; \quad 2i \quad ; \quad 2 + \tfrac{1}{2}i$$

4.2 Determinare graficamente le seguenti somme e differenze $z_1 + z_2$, $z_3 + z_4$, $z_1 - z_3$ e $z_2 - z_4 + z_3$ dove $z_1 = -2 + 3i$, $z_2 = 5 + 4i$, $z_3 = 1 - 6i$, $z_4 = -3 - i$.

4.3 Determinare modulo e argomento dei seguenti numeri complessi:

$z_1 = 2 - i$; $z_2 = 2\sqrt{6} + 5i$; $z_3 = i$; $z_4 = -3 - \sqrt{3}i$

4.4 Trovare modulo e argomento dei seguenti numeri complessi e scriverli in forma trigonometrica:

$-1 + i\sqrt{3}$, -3 , $7i$, $-1 + i$.

4.5 Dato il numero complesso $z = \cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi$ rappresentarlo sul piano e calcolare graficamente z^3.

4.6 Disegnare nel piano di Gauss tutte le radici complesse del polinomio $x^6 - 8$ e determinare per ciascuna parte reale e coefficiente dell'immaginario. Quali tra queste sono reali?

4.7 Disegnare nel piano di Gauss le radici terze di i e le radici terze di $-i$.

4.8 Calcolare la parte reale e la parte immaginaria dei seguenti numeri complessi:

$$(1+i)^5, \quad (2-i)^3 - (1-3i)^2, \quad \frac{6+5i}{3-i}, \quad \frac{(2+i)^3}{5i^{15}}, \quad \frac{3-2i}{1+5i} + \frac{2-3i}{2-i}.$$

4.9 Disegnare nel piano di Gauss i seguenti sottoinsiemi:

(1) $A = \{z \in \mathbb{C} \text{ tali che } \mathrm{Re}(z) > \mathrm{Im}(z)\}$;
(2) $B = \{z \in \mathbb{C} \text{ tali che } z - \overline{z} = i\}$;
(3) $C = \{z \in \mathbb{C} \text{ tali che } |z-2| \geq 2\}$;
(4) $D = \{z = [\rho, \theta] \in \mathbb{C} \text{ tali che } \theta = \frac{\pi}{2}\}$;
(5) $E = \{z = [\rho, \theta] \in \mathbb{C} \text{ tali che } \rho \geq 2\}$;
(6) $F = \{z \in \mathbb{C} \text{ tali che } \mathrm{Re}(z^4) = 0\}$.
(7) $G = \{z = [\rho, \theta] \in \mathbb{C} \text{ tali che } \theta = (2k+1)\pi\,,\ k \in \mathbb{Z}\}$;
(8) $H = \{z = [\rho, \theta] \in \mathbb{C} \text{ tali che } \rho = 1 \text{ e } 0 \leq \theta \leq \pi\}$.

4.10 Trovare la fattorizzazione in fattori irriducibili di $x^4 - 1$ in $\mathbb{R}[x]$.

4.11 Calcolare modulo e argomento del numero complesso $(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})^{53}$ e rappresentarlo nel piano di Gauss. A partire dal disegno, determinare la sua parte reale e la sua parte immaginaria.

4.12 Disegnare nel piano di Gauss le radici quinte di i e le radici terze di $\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.

4.13 Trovare tutte le radici complesse del polinomio $x^6 + 8$. Quali tra queste sono reali?

4.14 Calcolare a mano (se possibile) le soluzioni delle seguenti equazioni e poi risolverle mediante Derive:

a. $x^3 - 1 = 0$ **b.** $x^4 - 1 = 0$ **c.** $x^4 + 1 = 0$ **d.** $x^3 - 3x + 1 = 0$
e. $x^5 - 3x + 1 = 0$.

Modulo 3

Strutture algebriche e loro applicazioni

Lezione 5

Le classi di resto

La divisione con resto in $\mathbb{Z}$

Il **quoziente** (esatto) di due numeri naturali a e b, con $b \neq 0$, è quel numero naturale x (se esiste), tale che $x \cdot b = a$; in tal caso si scrive $x = a : b$. Non sempre però il quoziente esatto esiste; ad esempio non c'è alcun un numero intero x tale che $3 = 2 \cdot x$ e quindi in $\mathbb{Z}$ non c'è il quoziente esatto $3 : 2$ (anche se esiste in $\mathbb{Q}$ il numero non intero $\frac{3}{2}$).

Anche quando il quoziente esatto non esiste, si può comunque eseguire una divisione con resto.

Dati due numeri naturali a e b, con $b \neq 0$, esistono sempre (e sono unici) i due numeri naturali q e r tali che:

$$a = b \cdot q + r \quad \text{con la condizione} \quad r < b$$

I due numeri naturali q e r si dicono rispettivamente **quoziente** e **resto** della **divisione con resto** di a per b.

L'esistenza e l'unicità del quoziente e del resto è meno ovvia di quanto l'abitudine ci porterebbe a pensare e la loro dimostrazione richiede uno strumento matematico non elementare: **l'induzione**. Noi ci limiteremo a considerarle come "ben note".

Nel caso in cui il quoziente "esatto" di a e b esista, allora tale numero coincide col quoziente della "divisione con resto"e il resto è nullo.

Vogliamo ora estendere le due nozioni di divisione al caso dei numeri interi, comprendendo anche la possibilità che i numeri coinvolti siano negativi.

La definizione di "quoziente esatto" può essere copiata dalla precedente, sostituendo ogni volta "naturale" con "intero". C'è qualche novità invece per quel che riguarda la "divisione con resto".

Esempio 5.1. *Supponiamo di voler fissare un appuntamento in un futuro prossimo, e stabilire in quale giorno della settimana cadrà.*

Se oggi è il 7 ottobre ed è giovedì, che giorno sarà il 26 ottobre?

In modo ormai automatico il nostro procedimento mentale è il seguente:

- *da oggi al 26 ottobre ci sono 19 giorni;*
- $19 = 7 \cdot 2 + 5$*;*
- *fra* $14 = 7 \cdot 2$ *giorni sarà nuovamente giovedì;*
- *5 giorni dopo sarà martedì.*

Ma potremmo anche ragionare in modo leggermente diverso:

- $19 = 7 \cdot 3 - 2$*;*
- *fra* $21 = 7 \cdot 3$ *giorni sarà nuovamente giovedì;*
- *2 giorni prima sarà martedì.*

In entrambi i casi abbiamo eseguito una divisione con resto di 19 per 7, ma quoziente e resto ottenuti nei due casi sono diversi.

L'esempio precedente mostra come, prendendo in considerazione anche i numeri interi negativi, quoziente e resto possano non essere unici. Quello che in ogni caso si richiede è che il resto sia "piccolo" ossia che $|r| < b$; si ottengono così due possibili scritture: se $a = bq + r$ e $0 \leq r < b$, aumentando q di una unità si ottiene

$$a = b(q + 1) + (r - b)$$

dove $r' = r - b$ è un numero negativo il cui valore assoluto è minore di b.

Dal punto di vista matematico è di gran lunga preferibile che il quoziente e il resto di una divisione siano sempre univocamente determinati; per questo viene chiamata divisione con resto soltanto quella il cui resto r è un numero positivo o nullo. Così faremo anche noi. Quando, come capiterà tra breve, utilizzeremo anche l'altra possibilità, lo diremo esplicitamente chiamandola "divisione con resto negativo".

Esempio 5.2. *Eseguiamo la divisione di* $a = 23$ *per* $b = 4$ *prima nel modo usuale e poi con resto negativo.*

- $23 = 4 \cdot 5 + 3$
- $23 = 4 \cdot (5 + 1) + 3 - 4$ *ossia* $23 = 4 \cdot 6 - 1$

Possiamo a questo punto precisare cosa intendiamo per divisione tra numeri interi relativi.

Dati due numeri interi a e b, con $b \neq 0$, esistono sempre (e sono unici) i due numeri interi q e r tali che:

$$a = b \cdot q + r \quad \text{con la condizione} \quad 0 \leq r < |b|$$

I due numeri naturali q e r si dicono rispettivamente **quoziente** e **resto** della **divisione con resto** di a per b.

Vediamo ora come si esegue una "divisione con resto" nel caso in cui intervengano anche numeri negativi. **Notiamo che il quoziente ottenuto potrà talvolta anche essere negativo, mentre il resto dovrà in ogni caso essere postivo o nullo**.

- se $a \geq 0$ e $b < 0$ si esegue la divisione di a per $-b$ (che è > 0) e si cambia il segno al quoziente così ottenuto (mentre il resto è proprio lo stesso);
- se $a < 0$ e $b > 0$, si esegue la divisione di $-a$ per b con resto negativo e poi si cambia segno sia al quoziente sia al resto.
- se $a < 0$ e $b < 0$, si esegue la divisione di $-a$ per $-b$ con resto negativo e poi si cambia segno al resto.

Esempio 5.3. *Eseguiamo le seguenti divisioni con resto:*

a) Dividiamo 10 *per* -4*: poiché* $10 = 4 \cdot 2 + 2$ *allora*

$$10 = (-4) \cdot (-2) + 2.$$

b) Dividiamo -19 *per* 5*: da* $19 = 5 \cdot 3 + 4$ *passiamo alla divisione con resto negativo* $19 = 5 \cdot 4 - 1$ *ottenendo poi*

$$-19 = 5 \cdot (-4) + 1.$$

c) Dividiamo -7 *per* -11*: da* $7 = 11 \cdot 0 + 7$ *passiamo alla divisione con resto negativo* $7 = 11 \cdot 1 - 4$ *da cui*

$$-7 = (-11) \cdot 1 + 4.$$

L'algoritmo euclideo

La divisione con resto permette di risolvere in modo particolarmente conveniente il non banale problema del calcolo del massimo comune divisore tra due numeri interi. Ricordiamo intanto di cosa si tratta.

Definizione 5.4. *Siano a e b due numeri interi non entrambi nulli. Si dice* **massimo comune divisore** *tra a e b un intero d tale che:*

1) *d è un divisore di a e b.*
2) *ogni divisore di a e di b è un divisore di d.*

Osserviamo che se d è un massimo comune divisore di a e b, anche $-d$ lo è: per avere un unico massimo comune divisore usualmente si richiede anche che sia positivo ed in tal caso si scrive $MCD(a, b)$.

Il metodo per calcolare il MCD che solitamente si impara alle scuole elementari usa la fattorizzazione in fattori primi.

Ricordiamo che un numero intero è **primo** se non è né 0, né una unità (ossia 1 e -1 nel caso di $\mathbb{Z}$) ed è divisibile soltanto per se stesso, per le unità e per il prodotto tra se stesso e una unità.

NOTA BENE: 0, 1, -1 **non sono numeri primi.**

Teorema fondamentale dell'aritmetica

Ogni numero intero $\neq 0, 1, -1$ si decompone nel prodotto di numeri primi e la decomposizione è unica a meno dell'ordine e del segno dei fattori.

Grazie alla decomposizione in fattori primi possiamo affermare che se a, b sono numeri interi non entrambi nulli, allora esiste il loro massimo comune divisore dato da:

- Se $b = 0$, allora $MCD(a, 0) = a$.
- Se $b = 1$ o $b = -1$, allora $MCD(a, \pm 1) = 1$.
- Se a e b sono non nulli e non invertibili, allora il massimo comune divisore è il numero d che si ottiene come prodotto di tutti i fattori p^r dove p è ogni primo (positivo) che compare nella decomposizione di entrambi i numeri e r è il massimo per cui p^r divide sia a sia b.
- Se non ci sono fattori primi comuni tra a e b, diremo che a e b sono **coprimi** e che $MCD(a, b) = 1$.

Osservazione 5.5. 1 è coprimo con n, $\forall n \in \mathbb{N}$.

Non possiamo definire il $MCD(0, 0)$ perché ogni numero divide 0 e quindi non esiste il numero più grande che divide 0.

Se i numeri a e b sono "piccoli" è piuttosto facile determinare la loro decomposizione in fattori primi e quindi $MCD(a, b)$. Se invece sono "grandi", ad esempio se hanno qualche centinaia di cifre, la loro fattorizzazione può richiedere un tempo lunghissimo anche con l'uso del più potente computer. Quello che può apparire come un inconveniente si è invece trasformato negli ultimi anni in un utilissimo strumento applicativo; ci occuperemo di questo aspetto in uno dei prossimi paragrafi.

Ora invece vediamo come evitare tempi troppo lunghi nel calcolo del MCD facendo ricorso al metodo noto come **algoritmo euclideo**. L'idea di base è molto semplice:

se $a = bq + r$, ogni divisore comune ad a e b (quindi tra gli altri $d = MCD(a, b)$) è anche un divisore comune a b e r.

Supponiamo di voler calcolare $MCD(a, b)$. Procediamo allora nel modo seguente:

1) eseguiamo la divisione con resto $a = bq_1 + r_1$: allora $MCD(a, b) = MCD(b, r_1)$;
2) dividiamo quindi b per r_1 ottenendo $b = r_1q_2 + r_2$: allora $MCD(b, r_1) = MCD(r_1, r_2)$;
3) ripetiamo il procedimento fino ad ottenere un resto nullo. Il resto precedente è $MCD(a, b)$.

Il procedimento ha un numero finito di passi (e termina abbastanza in fretta) poiché ad ogni divisione i numeri coinvolti diventano via via più piccoli.

Esempio 5.6. *Vogliamo calcolare* $MCD(a = 3522, b = 321)$*:*

- $3522 = \mathbf{321} \cdot 10 + \mathbf{312}$
- $321 = \mathbf{312} \cdot 1 + \mathbf{9}$
- $312 = \mathbf{9} \cdot 34 + \mathbf{6}$
- $9 = \mathbf{6} \cdot 1 + \mathbf{3}$
- $6 = \mathbf{3} \cdot 2 + \mathbf{0}$.

Pertanto $MCD(3522, 321) = 3$.

L'algoritmo euclideo permette di ottenere anche una importante relazione che lega due numeri qualsiasi al loro MCD:

Identità di Bézout

se $d = MCD(a, b)$ allora esistono degli interi x, y tali che $d = ax + by$.

Vediamo come si ottengono praticamente i numeri x e y a partire dall'**Esempio** 5.6.

Ricaviamo dalla sequenza di divisioni i vari resti a partire dal MCD:

$\mathbf{3} = \mathbf{9} - \mathbf{6}$, $\mathbf{6} = \mathbf{312} - \mathbf{9} \cdot 34$, $\mathbf{9} = \mathbf{321} - \mathbf{312}$, $\mathbf{312} = \mathbf{3522} - \mathbf{321} \cdot 10$.

Mediante sostituzione otteniamo una relazione tra 3*, il MCD, e i due numeri iniziali:*

$\mathbf{3} = \mathbf{312} \cdot (-1) + \mathbf{9} \cdot 35 = \mathbf{321} \cdot 35 - \mathbf{312} \cdot 36 = \mathbf{3522} \cdot (-36) + \mathbf{321} \cdot 395.$

In conclusione $x = -36$ *e* $y = 395$.

Classi di resto

Se n è un numero intero, indicheremo col simbolo $n\mathbb{Z}$ l'insieme di tutti i suoi multipli (positivi e negativi).

Definizione 5.7. *Diremo che i numeri interi* a *e* b *sono* **congrui modulo** n *e scriveremo*

$$a \equiv b \bmod n.$$

se differiscono per un multiplo di n*, ossia se* $a - b \in n\mathbb{Z}$.

Esempio 5.8. $2\mathbb{Z}$ *è l'insieme di tutti i numeri pari. Si ha poi* $-5 \equiv 37 \bmod 2$ *poiché* $-5-37 = -42$ *che è pari;* $-12 \equiv -48 \bmod 2$ *poiché* $-12-(-48) = 36$ *che è pari; invece* $5 \not\equiv -12 \bmod 2$ *poiché* $5 - (-12) = 17$ *non è pari.*

La relazione di congruenza gode di molte proprietà dell'uguaglianza tra numeri interi. Il simbolo $\equiv$ è stato introdotto dal matematico Gauss proprio per questa sua analogia con la relazione di uguaglianza.

Una comoda caratterizzazione della congruenza modulo n è la seguente:

$a \equiv b \bmod n$ se e solo se i resti della divisione di a e di b per n sono uguali ossia se e solo se $a = nq_1 + r$ e $b = nq_2 + r$.

Se infatti $a - b = nk$ e $b = nq_2 + r$ allora $a = b + nk = n(q_2 + k) + r$; viceversa se $a = nq_1 + r$ e $b = nq_2 + r$ allora $a - b = n(q_1 - q_2)$.

Esempio 5.9. *Ciò che chiamiamo "giovedì" non è in realtà un solo giorno, ma è un insieme di tanti giorni che si ripetono a distanza di* 7 *uno dall'altro. Possiamo immaginare di stabilire una data iniziale per i giorni, una sorta di giorno* 0*, e di numerare poi ciascun giorno successivo con un numero progressivo (e anche ciascun giorno precedente con un numero progressivo negativo). Se il giorno* 0 *è giovedì, sarà giovedì ogni giorno con un numero che differisce da* 0 *per un multiplo di* 7*. Analogamente se il giorno* 39 *è lunedì, è lunedì ogni giorno dato da un numero che differisce da* 39 *per un multiplo di* 7*.*

In altre parole due giorni individuati dai numeri a *e* b *sono lo stesso giorno della settimana se* $a \equiv b \bmod 7$.

Come nell'esempio dei giorni della settimana, possiamo indicare con un "nome collettivo" tutti i numeri che differiscono tra di loro per un multiplo di n: useremo il nome **classe di resto modulo n.**

Ogni classe di resto modulo n è caratterizzata dal comune resto della divisione per n.

Potremo allora ottenere a partire da $\mathbb{Z}$ esattamente n classi di resto modulo n poiché i possibili resti della divisione per n sono gli interi compresi tra 0 e $n-1$. Ogni classe è solitamente indicata usando tale resto (oppure uno qualsiasi dei numeri nella classe) con una soprallineatura per distinguerlo dal numero usuale.

Avremo così:
$\overline{0}$ = interi che divisi per n hanno resto 0
$\overline{1}$ = interi che divisi per n hanno resto 1
$\overline{2}$ = interi che divisi per n hanno resto 2
....
$\overline{n-1}$ = interi che divisi per n hanno resto $n-1$.

Un modo alternativo di indicare le classi che spesso si incontra sui libri è quello di usare parentesi quadre invece della soprallineatura.

Come "la settimana" è un insieme di 7 elementi, ciascuno dei quali è un insieme di tanti giorni, così possiamo costruire un nuovo insieme i cui elementi sono le classi di resto. Il simbolo che useremo per **l'insieme delle classi di resto modulo** n è $\mathbb{Z}_n$. Quindi

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

Attenzione: I numeri 12, 37 e -18 sono differenti ossia $12 \neq 37 \neq -18$; però le loro classi di resto modulo 5 sono uguali poiché la divisione di 12 per 5, la divisione di 37 per 5 e la divisione di -18 per 5 hanno tutte resto 2. Si hanno quindi le uguaglianze apparentemente strane:

$$\overline{12} = \overline{37} = \overline{-18} = \overline{2}.$$

Classi di equivalenza

Nella costruzione delle classi di resto abbiamo fatto uso della nozione intuitiva di "nome collettivo" per analogia a quanto si fa abitualmente ad esempio con i giorni della settimana oppure con le ore sul quadrante di un orologio. Un altro importante esempio di questo genere che già conosciamo sono i numeri razionali. Sappiamo bene infatti che lo stesso numero razionale può essere indicato mediante infinite frazioni, per esempio $\frac{2}{3} = \frac{4}{6} = \frac{10}{15} = \frac{-4}{-6} = \dots$. Le infinite frazioni che corrispondono allo stesso numero razionale formano

quella che si chiama una **classe di equivalenza** (più esattamente due frazioni $\frac{a}{b}$ e $\frac{c}{d}$ sono equivalenti, ossia stanno nella stessa classe di equivalenza, se e solo se $ad = bc$).

Per formalizzare in modo rigoroso situazioni di questo tipo in matematica si usa introdurre il concetto di **relazione di equivalenza**.

Definizione 5.10. *Una relazione ρ in un insieme I individua coppie di elementi di I, in simboli $x\rho y$ se e solo se x è in relazione con y.*

Esempio 5.11. *La relazione R in $\mathbb{N}$ data da $n\ R\ m$ se e solo se $n+m=6$ individua tra le altre le coppie $(2,4)$, $(4,2)$, $(3,3)$, ma non $(2,2)$ oppure $(0,7)$.*

La relazione $\leq$ in $\mathbb{N}$ individua le coppie di numeri naturali (n,m) con $n \leq m$. Quindi 3 è in relazione con 5 poiché $3 \leq 5$, mentre 5 non è in relazione con 3 mediante $\leq$. Si noti che $3 \leq 3$.

La relazione σ in $\mathbb{Z}$ data da $n\ \sigma\ m$ se e solo se $n-m$ è pari, individua tra le altre le coppie $(2,4)$, $(4,2)$, $(3,3)$, ma non $(2,1)$ oppure $(7,0)$.

Definizione 5.12. *Una relazione ρ in I è una relazione di equivalenza se valgono le seguenti tre condizioni:*

(1) *$x\,\rho\,x$ (proprietà riflessiva)*

(2) *se $x\,\rho\,y$ allora $y\,\rho\,x$ (proprietà simmetrica),*

(3) *se $x\,\rho\,y$ e $y\,\rho\,z$ allora $x\,\rho\,z$ (proprietà transitiva).*

Relativamente all'esempio precedente, si può verificare che la relazione R è simmetrica, ma non riflessiva e transitiva, che la relazione $\leq$ è riflessiva e transitiva, ma non simmetrica e infine che σ è proprio una relazione di equivalenza.

Un altro importante esempio di relazione di equivalenza è quello prima introdotto tra le frazioni.

Anche le classi di resto modulo n sono classi di equivalenza rispetto alla relazione di congruenza modulo n: possiamo infatti facilmente verificare che le tre proprietà che caratterizzano una relazione di equivalenza sono soddisfatte.

Ogni elemento dell'insieme I individua una e una sola classe di equivalenza, che per definizione è il sottoinsieme di I formato da tutti gli elementi y equivalenti a x, ossia tali che $y\rho x$. Le classi di equivalenza di I formano una partizione di I, cioè la loro unione dà tutto I e due classi diverse sono sempre disgiunte.

La prova del 9. Alle scuole elementari si impara un metodo per controllare i risultati dei calcoli aritmetici detto appunto ‘‘prova del 9’’. Il primo passo consiste nel determinare a partire da ciascun numero k coinvolto nell'operazione un nuovo numero r compreso tra 0 e 8. Per far questo si esegue la somma delle cifre di k ottenendo un nuovo numero k' più piccolo di k; si sommano poi se necessario le cifre di k' iterando il procedimento fino al risultato voluto. In caso il numero ottenuto sia 9 si pone uguale a 0.

Esempio 5.13. *Se il numero k è* 5792*, si procede nel modo seguente:*
$5+7+9+2=23$
$2+3=5.$

Si ottiene così $r=5$

Il numero r ottenuto a partire da k col metodo prima descritto non è altro che il resto della divisione di k per 9. Per “convincersi ” di questo possiamo ricordare il significato della scrittura posizionale dei numeri.

$5792 = 5\cdot 10^3 + 7\cdot 10^2 + 9\cdot 10 + 2 =$
$= 5\cdot(999+1)+7(99+1)+9(9+1)+2 = (555+77+9)\cdot 9+(5+7+9+2) =$
$= 641\cdot 9 + 23 = 641\cdot 9 + 2(9+1)+3 = 643\cdot 9 + (2+3) = 643\cdot 9 + 5.$

Esempio 5.14. *Per eseguire la prova del 9 relativa all'operazione* $5792 + 3241 = 9033$ *si procede nel modo seguente:*

a) $5+7+9+2=23$, $2+3=5$ *(resto della divisione di 5792 per 9)*
b) $3+2+4+1=10$, $1+0=1$ *(resto della divisione di 3241 per 9)*
c) $5+1=6$
d) $9+0+3+3=15$, $1+5=6$ *(resto della divisione di 9033 per 9)*
e) I due risultati coincidono $6=6$ *e quindi la prova si considera riuscita.*

Attenzione: la prova del 9 non è sempre significativa! Se segnala un errore, vuol dire che un errore c'è effettivamente, ma alcuni errori sfuggono al suo controllo poiché non può per sua stessa natura segnalare errori multipli di 9. Un errore molto comune che causa discrepanze multiple di 9 nei risultati è quello nell'incolonnamento dei numeri in somme e moltiplicazioni.

La comprensione generale della validità di tale procedura richiede uno studio più approfondito di $\mathbb{Z}_n$ (si veda il successivo Esempio 5.15).

L'anello $\mathbb{Z}_n$ delle classi di resto modulo n

In $\mathbb{Z}_n$ si possono definire delle operazioni di somma e prodotto ponendo

$$\overline{a}+\overline{b}=\overline{a+b}$$
$$\overline{a}\cdot\overline{b}=\overline{ab}.$$

Queste operazioni sono *ben definite*, ossia il loro risultato non cambia se sostituiamo ad a un altro numero a' che sia congruo ad a modulo n (oppure a b un numero b' congruo a b modulo n).

Se infatti $a' - a = nk$, dove k è un numero intero, allora:

$$(a' + b) - (a + b) = nk \quad \text{ossia} \quad \overline{a' + b} = \overline{a + b}.$$

Lo stesso accade sostituendo b' a b oppure operando tali sostituzioni nell'operazione di prodotto.

Per prendere dimestichezza con le operazioni in questi nuovi insiemi costruiamo per esteso le tavole additive e moltiplicative di $\mathbb{Z}_n$ con n=4 e n=5.

Per semplicità nelle tabelle omettiamo la soprallineatura per indicare le classi.

Tabella delle operazioni in $\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabella delle operazioni in $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Le operazioni in $\mathbb{Z}_n$ godono di tutte le proprietà che lo rendono un **anello commutativo con identità**, ossia:

1) la somma e il prodotto sono associative e commutative e vale la proprietà distributiva del prodotto rispetto alla somma;
2) c'è l'elemento neutro rispetto alla somma, infatti $\overline{0} + \overline{a} = \overline{0 + a} = \overline{a}$;
3) c'è l'opposto di ogni elemento, infatti $\overline{a} + (\overline{-a}) = \overline{a - a} = \overline{0}$;
4) c'è l'elemento neutro rispetto al prodotto, infatti $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$;

La commutatività delle operazioni di somma e prodotto nel caso di $\mathbb{Z}_4$ e $\mathbb{Z}_5$ risulta chiaramente dalle tabelline precedenti: infatti la loro validità è garantita dalla simmetria rispetto alla diagonale $\searrow$.
Per controllare la proprietà associativa, ad esempio nel caso della somma, potremmo completare una tabella del tipo seguente e verificare che la quinta e la settima colonna coincidono.

a	b	c	b+c	a+(b+c)	a+b	(a+b)+c

In modo alternativo (e più generale) possiamo verificare le proprietà delle operazioni in $\mathbb{Z}_n$ riconducendole alle corrispondenti proprietà per le operazioni tra numeri interi. Verifichiamo a titolo di esempio la proprietà distributiva:

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a\,(b+c)} = \overline{ab + ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$$

Esempio 5.15. ***(Ancora sulla prova del 9)*** *Consideriamo il numero* 5792 *dell' Esempio 5.13. Lo possiamo scrivere come:*

$$5792 = 5 \cdot 10^3 + 7 \cdot 10^2 + 9 \cdot 10 + 2$$

e possiamo calcolare la sua classe di equivalenza modulo 9 *usando quest'ultima scrittura e le proprietà delle operazioni in* $\mathbb{Z}_9$*:*

$$\overline{5792} = \overline{5 \cdot 10^3 + 7 \cdot 10^2 + 9 \cdot 10 + 2} = \overline{5} \cdot \overline{10^3} + \overline{7} \cdot \overline{10^2} + \overline{9} \cdot \overline{10} + \overline{2}.$$

Ora in $\mathbb{Z}_9$ *si ha* $\overline{10} = \overline{1}$ *e quindi* $\overline{10^m} = \overline{10}^m = \overline{1}^m = \overline{1}$ *e quindi*

$$\overline{5792} = \overline{5} + \overline{7} + \overline{9} + \overline{2} = \overline{5 + 7 + 9 + 2} = \overline{23} = \overline{2 \cdot 10 + 3} = \overline{2} + \overline{3} = \overline{5}$$

Il procedimento di sommare le cifre di un certo numero intero k (iterando se necessario il procedimento e considerando la cifra 9 pari a 0) conduce quindi a trovare il numero compreso tra 0 e 8 che è congruo a k modulo 9: si tratta proprio del resto della divisione di k per 9.

Eseguire la prova del 9 su una operazione consiste essenzialmente nel ripetere quella operazione tra le classi di resto modulo 9 **corrispondenti ai numeri.**

Due fatti sorprendenti!

Anche se ben pochi numeri interi hanno un inverso in $\mathbb{Z}$, le loro classi di resto in un anello $\mathbb{Z}_n$ possono averlo. Osservando la tabella della moltiplicazione in $\mathbb{Z}_5$ si vede ad esempio che tutte le classi, tranne $\overline{0}$, hanno un inverso. Si ha infatti: $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{2} \cdot \overline{3} = \overline{1}$, $\overline{4} \cdot \overline{4} = \overline{1}$. $\mathbb{Z}_5$ è dunque un **campo**.

Invece, in $\mathbb{Z}_4$ la classe $\overline{2}$ non ha inverso, come si può dedurre dalla relativa tabella.

La classe $\overline{2}$ in $\mathbb{Z}_4$ ha, d'altra parte, una caratteristica altrettanto strana: pur non essendo la classe nulla, ha come quadrato $\overline{0}$.

Anche nell'anello $\mathbb{Z}_6$ vi sono due classi, $\overline{2}$ e $\overline{3}$, il cui prodotto è la classe $\overline{0}$, pur essendo entrambe diverse dalla classe nulla. Elementi come questi si dicono **divisori dello zero**. Un anello in cui siano presenti divisori dello zero è un anello in cui cui **non vale la legge di annullamento del prodotto**.

Nei prossimi paragrafi vedremo delle applicazioni particolarmente importanti delle operazioni tra classi di resto, in particolare del prodotto e criteri per stabilire velocemente quali elementi hanno e quali non hanno inverso e quali sono divisori dello zero.

★ Crittografia

La **crittografia**, dal greco $\chi\rho\upsilon\pi\tau o\sigma$ = nascosto e $\gamma\rho\alpha\varphi\epsilon\iota\nu$ = scrivere, è lo studio dei metodi per garantire la segretezza del contenuto di un messaggio anche nel caso sia intercettato.

Un metodo crittografico ideale dovrebbe permettere al mittente di crittografare con molta facilità i messaggi e dovrebbe inoltre assicurare che solo il destinatario designato possa decifrarli con facilità.

Nata come raccolta di tecniche e di sistemi per assicurare la riservatezza di messaggi tra regnanti, imperatori, amanti, etc, la crittografia è maturata definitivamente a rango di scienza solo nei primi del 1900 con l'avvento di nuove teorie e tecniche matematiche.

Attualmente è entrata a far parte della nostra vita quotidiana, poiché ne fanno uso tessere Bancomat, telefoni cellulari, trasmissioni televisive, internet e in genere ogni strumento di comunicazione elettronica.

Le sue origini sono antichissime; basti pensare che più di 6000 anni fa si scrivevano geroglifici egizi in modo non standard e ancora oggi si lavora per la loro interpretazione e che nella Bibbia si trova un esempio di crittografia mediante sostituzione di ogni lettera dell'alfabeto con la lettera che occupa la stessa posizione nell' alfabeto scritto al contrario.

⋆ **Il cifrario di Cesare.** Anche Giulio Cesare, era solito **cifrare i messaggi mediante sostituzione**, cioè ad ogni lettera dell'alfabeto ne faceva corrispondere un'altra traslata di un certo numero di posizioni. Se usiamo la chiave 3 tutte le lettere vengono scalate di 3 posizioni, quindi in corrispondenza del vecchio alfabeto troviamo il nuovo

A	B	C	D	E	F	G	H	...	U	V	Z
U	V	Z	A	B	C	D	E	...	R	S	T

Questa tabella è la **chiave** usata per la cifratura ed è la stessa che viene usata per la decifratura; si rende quindi necessaria una precedente comunicazione tra le due parti al fine di scambiarsi questa informazione. Nella necessità di un accordo preliminare sta una delle principali debolezze di questo e di ogni altro metodo crittografico "vecchio stile", perché anche la comunicazione iniziale corre il rischio di essere intercettata.

Possiamo generalizzare il metodo di Cesare ricorrendo alle classi di resto, così da ottenere permutazioni che non solo traslano, ma ''rimescolano'' le lettere e che sono anche facilmente ottenibili dalle due parti.

Associamo ad ogni lettera dell'alfabeto un numero da 1 a 21, o meglio una classe di resto modulo 21.

Fissati poi due numeri interi a e b (**i parametri di cifratura**) otteniamo la lettera che sostituirà la lettera individuata dalla classe $\overline{x}$ come quella individuata da $\overline{y}$ dove

$$\overline{y} = \overline{ax + b}$$

(in pratica basta eseguire il calcolo $ax+b$, dividere per 21 e prendere il resto y.)

Esempio 5.16. *Usiamo la chiave di cifratura* $y = 5x + 1$.

La lettera ***A*** *corrisponde a* $\overline{x} = \overline{1}$ *e quindi sarà sostituita dalla* ***F*** *corrispondente a* $\overline{y} = \overline{5 \cdot 1 + 1} = \overline{6}$.

La lettera ***H*** *corrisponde a* $\overline{x} = \overline{8}$ *e quindi sarà sostituita dalla* ***V*** *corrispondente a* $\overline{y} = \overline{5 \cdot 8 + 1} = \overline{41} = \overline{20}$.

Potremmo costruire in questo modo tutta la tabella della sostituzione ottenendo una ***permutazione delle lettere****. Chi deve decifrare può costruirsi l'intera tabella delle corrispondenze e usarla a rovescio, oppure può usare la formula inversa:* $x = 17y + 4$ *(ottenibile dal fatto che 17 è l'inverso di 5 in* $\mathbb{Z}_{21}$*).*

La lettera ***F*** *che corrisponde a* $\overline{y} = \overline{6}$ *deve essere decifrata come* ***A*** *corrispondente a* $\overline{x} = \overline{17 \cdot 6 + 4} = \overline{106} = \overline{1}$ *e così via.*

Esempio 5.17. *Usiamo ora una differente chiave di cifratura:* $y = 3x + 1$.

La lettera ***A*** *corrisponde a* $\overline{x} = \overline{1}$ *e quindi sarà sostituita dalla* ***D*** *corrispondente a* $\overline{y} = \overline{3 \cdot 1 + 1} = \overline{4}$.

La lettera ***H*** *corrisponde a* $\overline{x} = \overline{8}$ *e quindi sarà sostituita dalla* ***D*** *corrispondente a* $\overline{y} = \overline{3 \cdot 8 + 1} = \overline{25} = \overline{4}$.

*Questa seconda chiave scelta non va bene perché **A** e **H** sono crittografate entrambe come **D**. Chi legge **D** non sa se interpretare come **A** o come **H**.*

Si pone allora naturale una domanda: quali formule del tipo $y = ax + b$ vanno bene?

La risposta sta nella chiave di decifratura $x = cy + d$; se una tale chiave esiste allora lettere diverse devono sicuramente essere state codificate mediante lettere diverse.

Se usiamo la chiave di cifratura $y = ax + b$, quali numeri c e d forniscono la chiave di decifratura $x = cy + d$?

Devono essere scelti in modo che la doppia sostituzione $x \mapsto ax + b \mapsto c(ax + b) + d$ dia sempre come risultato x stesso, almeno come classe di resto modulo 21 ossia $\overline{x} = \overline{c(ax + b) + d}$. Svolgendo i calcoli otteniamo le relazioni:

$$\begin{cases} ca & \equiv & 1 & \mod 21 \\ cb & \equiv & -d & \mod 21 \end{cases}$$

La prima relazione dice che $\overline{c}$ deve essere l'inverso di $\overline{a}$ in $\mathbb{Z}_{21}$; trovato c, le seconda relazione dice che $\overline{d}$ sarà $\overline{-cb}$. Condizione necessaria e sufficiente perché esista la chiave di decifratura è che $\overline{a}$ sia invertibile in $\mathbb{Z}_{21}$.

La risposta alla domanda precedente è quindi:

per avere una buona chiave di cifratura bisogna scegliere a in modo che $\overline{a}$ abbia l'inverso in $\mathbb{Z}_{21}$.

Non sappiamo ancora però quali classi godono di tale proprietà ossia **quali e quante classi di $\mathbb{Z}_n$ ammettono un inverso**.

La funzione di Eulero

Nell'anello $\mathbb{Z}_n$ hanno inverso le classi di quei numeri a tali che $MCD(a, n) = 1$.

Basta infatti ricordare **l'identità di Bézout**:

se $1 = MCD(a, n)$ allora $1 = ax + ny$ per opportuni numeri interi x, y.

Se consideriamo le classi di resto in $\mathbb{Z}_n$ otteniamo:

$$\overline{a} \cdot \overline{x} = \overline{ax} = \overline{ax + ny} = \overline{1}.$$

Il numero x che compare nell'identità di Bézout, e che possiamo calcolare mediante l'algoritmo euclideo, ci dà proprio la classe inversa di $\overline{a}$ in $\mathbb{Z}_n$.

Tutti gli altri elementi $\overline{a}$ di $\mathbb{Z}_n$, quelli tali che $MCD(a, n) \neq 1$, risultano invece essere dei divisori dello zero e non possono avere inverso.

Per sapere quanti sono i valori di a che ci danno un buon cifrario di Cesare, potremmo allora esaminare la tabella della moltiplicazione di $\mathbb{Z}_{21}$ per contare quanti sono gli elementi coprimi con 21. Il metodo è ragionevole perché $\mathbb{Z}_{21}$ ha solo 21 elementi. Non lo sarebbe se lo facessimo nel caso di $\mathbb{Z}_n$ con n molto, molto grande. Nonostante la difficoltà di calcolarlo (anzi proprio per questo!) il numero di elementi invertibili in $\mathbb{Z}_n$ è molto importante. Si denota col simbolo $\phi(n)$ e si chiama **funzione di Eulero** dal nome dell'illustre matematico Leonhard Euler.

Se conosciamo la fattorizzazione di n in fattori primi, c'è un modo diretto e veloce per calcolare il valore della funzione di Eulero $\phi(n)$.

Come abbiamo visto contare le classi invertibili in $\mathbb{Z}_n$ è come contare i numeri tra 1 e $n-1$ che sono coprimi con n.

Se $n = p$ è un primo, allora tutti i numeri tra 1 e $n-1$ (non essendo divisibili per p) sono coprimi con p. Quindi:

$$\phi(p) = p - 1$$

Se n è la potenza di un primo p, ossia $n = p^r$, allora sono coprimi con n tutti i numeri tra 1 e $n-1$ che non sono multipli di p ossia tutti tranne $p \cdot 1$, $p \cdot 2$, $\ldots\ldots p \cdot p^{r-1}$. Quindi:

$$\phi(n) = \phi(p^r) = n - p^{r-1} = p^{r-1}(p-1)$$

Meno facile da capire (ma vera!) è la formula nel caso generale. Se la fattorizzazione di n in prodotti di potenze di primi tutti diversi è $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$, allora

$$\phi(n) = \phi(p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}) = \phi(p_1^{r_1}) \cdot \ldots \cdot \phi(p_k^{r_k}) = p_1^{r_1-1}(p_1-1) \cdot \ldots \cdot p_k^{r_k-1}(p_k-1).$$

Esempio 5.18. *Per* $n = 12$ *abbiamo* $12 = 3 \cdot 2^2$ *e quindi* $\phi(12) = 2 \cdot 2 \cdot 1 = 4$. *I numeri tra* 1 *e* 11 *coprimi con* 12 *sono infatti soltanto i* 4 *seguenti:* 1, 5, 7 *e* 11.

Possiamo a questo punto enunciare un importantissimo risultato.

Teorema di Eulero:

Siano a, n interi positivi primi tra loro. Allora:

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Esempio 5.19. *Consideriamo i due numeri* $a = 2$ *e* $n = 7$ *che sono coprimi. Poiché* 7 *è primo, si ha* $\phi(7) = 7 - 1 = 6$.

Verifichiamo il Teorema di Eulero in questo caso particolare mediante calcoli diretti:

$$2^6 = 64 = 7 \cdot 9 + 1 \text{ quindi } 64 \equiv 1 \bmod 7 \text{ ossia } 2^{\phi(7)} \equiv 1 \bmod 7.$$

Esempio 5.20. *Vogliamo calcolare la cifra x che indica le unità del numero 327^{82} scritto in forma posizionale.*

Anche un computer incontra grosse difficoltà ad eseguire questo calcolo e in ogni caso fornisce soltanto una approssimazione del risultato data dalle prime cifre a sinistra del numero accompagnate da una opportuna potenza di 10, non certo l'ultima cifra a destra.

Eseguiamo in altro modo questo calcolo facendo ricorso al Teorema di Eulero. Osserviamo che calcolare la cifra delle unità equivale a calcolare il resto della divisione per 10 ossia il numero x compreso tra 0 e 9 tale che $\overline{x} = \overline{327^{82}}$ in $\mathbb{Z}_{10}$.

Intanto $327 \equiv 7 \bmod 10$ quindi in $\mathbb{Z}_{10}$ si ha $\overline{x} = \overline{327}^{82} = \overline{7}^{82}$.
Ora, per il teorema di Eulero con $a = 7$, $n = 10$ e $\phi(n) = \phi(10) = 4$ vale la relazione $7^{\phi(10)} = 7^4 \equiv 1 \bmod 10$. Quindi $\overline{x} = \overline{7}^{82} = \overline{7}^{80+2} = (\overline{7}^4)^{20} \cdot \overline{7^2} = \overline{1}^{20} \cdot \overline{49} = \overline{9}$.
La cifra finale di 327^{82} è quindi 9.

Esempio 5.21. *Vogliamo trovare le ultime due cifre decimali (ossia decine e unità) di 3^{925}. Le ultime due cifre decimali corrispondono al resto della divisione per 100. Come nell'esempio precedente usiamo il Teorema di Eulero:*

$$a^{\phi(100)} \equiv 1 \bmod 100.$$

Ora $\phi(100) = \phi(25 \cdot 4) = \phi(5^2 \cdot 2^2) = 5(5-1)2(2-1) = 40$ dunque $3^{40} \equiv 1 \bmod 100$. Inoltre $925 = 40 \cdot 23 + 5$ e quindi

$$\overline{3}^{925} = \overline{3}^{23 \cdot 40 + 5} = (\overline{3}^{40})^{23} \cdot \overline{3}^5 = \overline{1} \cdot (\overline{3}^5) = \overline{243} = \overline{43}.$$

Il Teorema di Eulero è alla base di un metodo crittografico particolarmente ingegnoso che risolve il problema della segretezza nello scambio delle "chiavi" tra il mittente e il destinatario.

⋆ **Il codice RSA.** I metodi crittografici **a chiave pubblica** non richiedono lo scambio di comunicazioni riservate in alcun momento tra mittente e destinatario. Nel seguito tutte le comunicazioni tra i due soggetti si intenderanno come disponibili a chiunque; ad esempio possono avvenire mediante pubblicazione su un giornale oppure su un sito internet completamente accessibile.

La prima metodologia crittografica di questo genere fu sviluppata nel 1978 da tre ricercatori: Ronald Rivest, Adi Shamir e Leonard Adleman; essi

realizzarono una procedura che, dalle loro iniziali, prende il nome di "RSA". L'idea di base del codice RSA è la constatazione , di quanto sia facile moltiplicare tra loro due numeri dati e di quanto sia invece difficile (o meglio calcolativamente lungo) risalire ai fattori dato il prodotto.

In teoria chiunque può decifrare un messaggio crittografato mediante il codice RSA, ma il tempo richiesto per la decifrazione è tanto da rendere il messaggio ormai privo di interesse. Il diretto destinatario possiede invece un metodo di decifratura molto veloce. Vediamo come questa "doppia velocità" possa essere praticamente realizzata.

Ci si accorda (pubblicamente!) su come trasformare i messaggi in sequenze di numeri ciascuno di lunghezza prefissata: sia m uno di questi numeri.

Il **destinatario** del messaggio prepara la chiave di decifrazione nel modo seguente:

- Costruisce un numero n moltiplicando due numeri primi p e q abbastanza grandi in modo che p e q siano maggiori di m: in questo modo m è sicuramente coprimo con $n = pq$. Inoltre sapendo che $n = pq$ egli può facilmente calcolare la funzione di Eulero $\phi(n) = (p-1)(q-1)$.
- Sceglie inoltre un altro numero h coprimo con $\phi(n)$ e calcola l'inverso $\overline{d}$ di $\overline{h}$ in $\mathbb{Z}_{\phi(n)}$ ossia calcola d tale che $hd = 1 + k\phi(n)$.
- Infine rende pubblici i due numeri n e h, mentre mantiene il più assoluto segreto sulla fattorizzazione $n = pq$, sul valore di $\phi(n)$ e su d.

  Il **mittente** adopera queste informazioni, ossia n e h, per crittografare il messaggio m nel modo seguente:
- Calcola la potenza m^h e la divide per n ottenendo un resto c; comunica (pubblicamente) al destinatario il numero c che è il messaggio cifrato. La relazione tra il messaggio originale e la sua cifratura è data da:

$$c \equiv m^h \bmod n \quad \text{ovvero} \quad \overline{c} = \overline{m}^h \quad \text{in} \quad \mathbb{Z}_n.$$

- Il destinatario decodifica il messaggio con l'aiuto del numero d calcolando la potenza c^d. Si ha infatti:

$$\overline{c}^d = \overline{m}^{hd} = \overline{m}^{1+k\phi(n)} = \overline{m} \cdot (\overline{m}^k)^{\phi(n)} = \overline{m} \cdot \overline{1} = \overline{m}.$$

  Qualunque sia il numero m' che ottiene come rappresentante della classe $\overline{c}^d = \overline{m}$, egli può infine ricavare m come resto della divisione di m' per n; infatti m (essendo positivo e minore di n) è proprio il

resto della divisione per n di ogni numero m' congruo a m modulo n.

Come si può vedere nell'ultimo passaggio la validità del Teorema di Eulero sta alla base di questa procedura. Infatti è grazie a tale risultato che possiamo affermare che $(\overline{m}^k)^{\phi(n)} = \overline{1}$.

A titolo di curiosità diciamo che i primi attualmente adoperati per l'RSA hanno un numero di cifre dell'ordine delle centinaia e che il metodo viene considerato del tutto sicuro. In un esperimento del 1994 per "rompere" una chiave RSA di 129 cifre, (ossia per fattorizzare un numero n di 129 cifre), sono stati necessari 8 mesi di lavoro coordinato effettuato da 600 gruppi di ricerca sparsi in 25 paesi, che hanno messo a disposizione 1600 computers, facendoli lavorare in parallelo collegati tra loro attraverso Internet!

Esempio 5.22. *Eseguiamo una simulazione di codifica e decodifica di un messaggio mediante RSA. Il destinatario del messaggio, chiamiamola Francesca, ha scelto i due primi* 5 *e* 11 *e li ha moltiplicati ottenendo* 55*. Perché questa simulazione con numeri così piccoli abbia senso dobbiamo fingere che nessuno (a parte Francesca) sia in grado di calcolare in tempi brevi la fattorizzazione di* 55*.*

Francesca ha calcolato $\phi(55) = (5-1)\cdot(11-1) = 40$*, ha scelto* $h = 3$ *coprimo con* 40 *e ha determinato (mediante l'algoritmo euclideo) un numero* d *tale che* $dh \equiv 1 \mod 40$*, ottenendo* $d = 27$ *(poiché* $3 \cdot 27 = 1 + 2 \cdot 40$*).*

Francesca comunica poi pubblicamente, a tutti coloro che vogliono scriverle in modo riservato, i due numeri $n = 55$ *e* $h = 3$*.*

Paolo vuole mandarle il messaggio $m = 7$*: calcola:* $m^h = 7^3 = 343$*, lo divide per* 55 *e ottiene il resto* $c = 13$ *che spedisce a Francesca. Nessuno è in grado di decodificare il messaggio* $c = 13$ *tranne Francesca che possiede la chiave di decifrazione* $d = 27$*.*

Francesca calcola allora 13^{27} *e quindi divide per* 55 *ottenendo il resto* 7 *che è il messaggio "in chiaro".*

Si noti che Francesca non deve necessariamente calcolare per intero la potenza 13^{27} *prima di eseguire la divisione per* 55*, ma può lavorare nelle classi di resto* $\mathbb{Z}_{55}$ *nel modo seguente:*

$$\overline{13}^{27} = (\overline{13}^3)^9 = \overline{52}^9 = \overline{-3}^9 = \overline{-19683} = \overline{-48} = \overline{7}$$

.

♣ Esercizi per la quinta lezione

5.1 Calcolare MCD di 18779 e 4183 usando l'algoritmo euclideo.

5.2 Scrivere l'identità di Bézout per i numeri 45 e 51.

5.3 Determinare l'unico numero compreso tra 0 e 52 che stia nella classe di resto modulo 52 di $k = 427$ e poi di $h = -444$.

5.4 Come si fa ad ottenere esattamente 3 litri di acqua usando un recipiente da 5 litri e un altro da 7 litri?

5.5 Eseguire in $\mathbb{Z}_{12}$ i calcoli: $\overline{5} \cdot \overline{3} + \overline{21} - \overline{6}$.

5.6 Scrivere la tabellina del $\overline{5}$ in $\mathbb{Z}_{12}$ ossia: $\overline{5 \cdot 0}$, $\overline{5 \cdot 1}$, $\overline{5 \cdot 2}$ .... Quanto fa $\overline{5 \cdot 8734}$?

5.7 Scrivere la lista delle potenze di $\overline{5}$ in $\mathbb{Z}_{12}$ ossia: $\overline{5}^0$, $\overline{5}$, $\overline{5}^2$ .... Quanto fa $\overline{5}^{8734}$?

5.8 Provare che in in $\mathbb{Z}_7$ tutte le classi tranne $\overline{0}$ sono invertibili determinando esplicitamente gli inversi.

5.9 Risolvere le seguenti equazioni in $\mathbb{Z}_7$ mediante sostituzione diretta di ciascun elemento di $\mathbb{Z}_{12}$:

$$\overline{5}x = \overline{1}\ ,\ \overline{2}x = \overline{6}\ ,\ x^2 = \overline{1}\ ,\ x^2 = \overline{0}.$$

5.10 Se $\overline{28} = \overline{2}$ in $\mathbb{Z}_n$, cosa possiamo dire di n?

5.11 Risolvere mediante sostituzione diretta l'equazione in $\mathbb{Z}_8$: $[6]\,[x] = [0]$.

5.12 Calcolare $\phi(100), \phi(528), \phi(121), \phi(297), \phi(700), \phi(215)$

5.13 Trovare la cifra finale di 17^{307} e 18^{75}.

5.14 Calcolare le ultime due cifre di 9^{201} e 302^{46}.

5.15 Fino dalle elementari si imparano alcuni espedienti pratici per riconoscere velocemente se un numero è divisibile per 2, 3, 4, 5 e 11.

Ottenere in modo rigoroso questi criteri operando sulle classi di resto in modo analogo a quanto fatto per la prova del 9.

Perché non si imparano anche criteri per la divisibilità per 7 o per 13?

5.16 Verificare se la relazione tra i punti del piano per cui due punti sono in relazione se e solo se hanno la stessa distanza dall'origine è una relazione di equivalenza.

5.17 Verificare se la relazione tra le rette del piano per cui due rette sono in relazione se e solo se sono parallele è una relazione di equivalenza.

5.18 Verificare se la relazione tra triangoli del piano per cui due triangoli sono in relazione se e solo se sono simili è una relazione di equivalenza.

5.19 Verificare se la relazione tra le rette del piano per cui due rette sono in relazione se e solo se sono perpendicolari è una relazione di equivalenza.

5.20 Verificare se la relazione tra numeri reali per cui due numeri sono in relazione se e solo se uno dei due divide l'altro è una relazione di equivalenza.

5.21 Sia $X = \mathbb{R}[x]/(x^2+1)$ l'insieme delle classi di equivalenza di polinomi ottenuto mediante la relazione di equivalenza per cui due polinomi sono equivalenti se e solo se divisi per $x^2 + 1$ hanno lo stesso resto. Provare che X è in corrispondenza biunivoca con $\mathbb{C}$.

Lezione 6

I gruppi

Le permutazioni

Nel corso di queste lezioni ci siamo più volte imbattuti in situazioni che richiedevano di permutare alcuni oggetti: ricordiamo la permutazione delle radici di un polinomio nella Lezione 2 oppure la permutazione delle lettere in crittografia nella Lezione 5.

Cerchiamo ora un modo più sintetico ed efficace per indicare una permutazione di oggetti, limitandoci per ora a considerare 3 oggetti α, β e γ, come nel caso delle soluzioni di un'equazione di 3° grado.

Vogliamo scrivere per esempio la permutazione che pone β al posto di α, γ al posto di β e α al posto di γ. Possiamo etichettare le tre lettere mediante $1, 2, 3$: stabiliamo che 1 sta per α, 2 sta per β e 3 per γ.

La permutazione precedente può essere individuata mediante la tabella:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

La prima riga contiene gli elementi $1, 2, 3$ (possiamo scriverli sempre in quest'ordine), mentre nella seconda riga scriviamo, sotto a ciascun elemento della prima riga, quello che lo sostituisce: sotto 1 c'è 2 perché 1 rappresenta α, che viene sostituito con β rappresentato dal 2. Denominiamo questa tabellina p_1: 1 passo avanti.

Le due tabelline:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad s_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

rappresentano rispettivamente la permutazione che non muove nulla, detta **permutazione identica o identità**, e la permutazione che lascia fermo 3 e scambia tra loro 1 e 2, detta **scambio 1-2**.

Ecco l'elenco completo delle permutazioni di 3 elementi:

$$e\ ,\quad s_{12}\ ,\quad s_{13}\ ,\quad s_{23}\ ,\quad p_1\ ,\quad p_2$$

dove la terza e la quarta sono gli scambi di 1 con 3 e di 2 con 3 rispettivamente e l'ultima è la permutazione due passi avanti (o un passo indietro):

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Abbiamo affermato che le permutazioni di 3 oggetti sono in tutto 6. Possiamo infatti scegliere tra i 3 elementi quello con cui scambiare 1; per ognuna di tali 3 possibili scelte diverse, abbiamo ancora due possibili scelte per l'elemento con cui scambiare 2 (non possiamo infatti scambiare sia 1 sia 2 con uno stesso elemento). A questo punto dovremo scambiare 3 con l'unico elemento non ancora adoperato.

Più in generale il numero di permutazioni di n oggetti è:

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1$$

che si indica con il simbolo $n!$ e si legge **n fattoriale**.

La composizione di permutazioni

Possiamo eseguire in sequenza due permutazioni una dopo l'altra.

Ad esempio eseguendo prima p_1 e poi s_{12} otteniamo s_{23}; scriveremo:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

La prima trasformazione manda 1 in 2 e la seconda manda 2 in 1; quindi, nella trasformazione "finale", sotto 1 scriviamo di nuovo 1. La prima trasformazione manda 2 in 3 e la seconda manda 3 in 3; quindi, nella trasformazione "finale", sotto 2 scriviamo 3. E così via.

Quella che abbiamo costruito è una operazione nell'insieme di tutte le permutazioni di 3 elementi, che chiameremo **composizione** oppure **prodotto**.

La permutazione identica è l'identità rispetto all'operazione di composizione, perché composta con ogni altra la lascia invariata. Inoltre ogni permutazione ha la permutazione inversa, ossia una permutazione che composta con lei dà la permutazione identica. Se indichiamo con l'apice $^{-1}$ l'inversa si ha:

$$e^{-1} = e\ ,\quad s_{12}^{-1} = s_{12}\ ,\quad s_{13}^{-1} = s_{13}\ ,\quad s_{23}^{-1} = s_{23}\ ,\quad p_1^{-1} = p_2\ ,\quad p_2^{-1} = p_1.$$

L'insieme delle permutazioni di 3 elementi dotato di questa operazione costituisce un **gruppo** che si chiama **gruppo simmetrico su 3 elementi** e si indica con S_3.

Allo stesso modo possiamo costruire i gruppi simmetrici su 4, 5, $\ldots n$ elementi S_4, S_5, $\ldots S_n$.

La permutazione identica su n elementi è l'identità di S_n; per ogni permutazione (che possiamo immaginare individuata da una tabella su due righe come nel caso $n = 3$) la permutazione inversa si ottiene scambiando la riga superiore con la inferiore (e, se si preferisce, riordinando le colonne in modo da riottenere la prima riga scritta in ordine crescente).

In generale si dice **gruppo** un insieme dotato di una operazione che gode delle seguenti proprietà:

a) l'operazione è associativa;

b) esiste un particolare elemento, **l'identità**, che operando con tutti gli altri sia a destra sia a sinistra li lascia invariati.

c) ogni elemento è dotato di un **inverso** ossia di un elemento che operando con esso sia a destra sia a sinistra dà come risultato l'identità.

Attenzione: la proprietà commutativa dell'operazione non è richiesta e in molti dei gruppi più interessanti effettivamente non vale.

L'operazione che abbiamo costruito nell'insieme delle permutazioni di n elementi è associativa, ma **non è commutativa**!

Se consideriamo ad esempio in S_3 le permutazioni che abbiamo chiamato p_1 e s_{12} e le componiamo, vediamo che $p_1 \cdot s_{12} = s_{23}$, ma $s_{12} \cdot p_1 = s_{13}$, infatti

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} .$$

Invece che un intero gruppo (ad esempio di permutazioni) potremmo limitarci a considerarne solo una parte, ma con la condizione che questo insieme più piccolo soddisfi a sua volta le tre condizioni a), b), c) per essere un gruppo: in tal caso si avrà un **sottogruppo**.

Esempio 6.1. *Con le notazioni introdotte prima, l'insieme* $\{e,\ p_1,\ p_2\}$ *è un sottogruppo di* S_3.

Esempio 6.2. *Il sottoinsieme* $\{e,\ s_{12},\ s_{13},\ s_{23}\}$ *non è un sottogruppo di* S_3. *Se infatti componiamo* s_{12} *e* s_{13} *otteniamo* p_1 *che non è uno degli elementi indicati.*

Se invece consideriamo il sottoinsieme $\{e,\ s_{12}\}$ *otteniamo un sottogruppo.*

Il fatto che i quattro elementi considerati nell'esempio precedente non formino un sottogruppo può essere anche dedotto senza fare alcun tipo di verifica dal seguente importante risultato.

Teorema 6.3. *(**Teorema di Lagrange**) Sia G un gruppo con un numero finito n di elementi. Allora il numero di elementi di ogni sottogruppo H di G è un divisore di n.*

In particolare nessun sottogruppo di S_3 può avere quattro elementi perché 4 non è un divisore di 6.

Esempio 6.4. *Vedremo nelle prossime lezioni che certe permutazioni corrispondono a simmetrie di figure geometriche.*

Le simmetrie del triangolo equilatero possono essere rappresentate mediante elementi di S_3: tutti gli elementi di S_3 corrispondono a simmetrie del triangolo equilatero.

Le simmetrie di un quadrato possono essere rappresentate mediante elementi di S_4. Non tutti gli elementi di S_4 corrispondono però a simmetrie del quadrato: le simmetrie del quadrato formano un sottogruppo H di S_4.

Le simmetrie di un rettangolo (non quadrato) formano un altro sottogruppo di S_4, ancora più piccolo, contenuto in H.

Riguardo alle proprietà dei gruppi di permutazioni si possono consultare anche i siti:

http://www.cut-the-knot.org/do_you_know/permutation.shtml

Isometrie del piano

Vediamo ora come il concetto di gruppo sia collegato alla geometria, iniziando con la geometria piana.

Per **isometria** del piano intendiamo un movimento dei punti del piano tale che, a movimento avvenuto, ogni coppia di punti si trovi a distanza uguale a quella che aveva inizialmente, anche se i punti potranno chiaramente occupare posizioni diverse da quelle di partenza.

Sono movimenti di questo tipo:

1. le traslazioni
2. le rotazioni attorno ad un punto
3. le riflessioni (o ribaltamenti) rispetto ad una retta.

Possiamo eseguire uno dopo l'altro due o più movimenti del tipo precedente nell'ordine che preferiamo, magari ripetendoli anche più volte: in linguaggio matematico l'esecuzione in sequenza di due o più movimenti si dice la loro

composizione. Osserviamo che la composizione di due movimenti che non cambiano le distanze tra i punti è ancora un movimento che non cambia le distanze e quindi è una isometria!

Componendo una traslazione ed una riflessione rispetto ad una retta parallela alla direzione di traslazione, scopriamo un nuovo tipo di movimento non compreso nell'elenco precedente:

4. Le riflessioni con scorrimento o **glissoriflessioni**.

Il fatto importante (e un po' sorprendente) è che tutte le isometrie del piano rientrano in uno di questi quattro tipi. Possiamo cioè eseguire una sequenza lunga a piacere di rotazioni, traslazioni e riflessioni, ottenendo alla fine lo stesso risultato che avremmo ottenuto se avessimo applicato UNA SOLA delle quattro isometrie precedenti (anche se non sempre è facile scoprire quale).

Classificazione delle isometrie del piano. *(Chasles, 1831)*
Nel piano i tipi possibili di isometrie si riducono ai seguenti casi: **riflessioni**, **rotazioni**, **traslazioni**, **glissoriflessioni**.

Come fare a riconoscere di che tipo è una isometria? Per il Teorema di Chasles, se lascia fisso almeno un punto è una rotazione oppure una riflessione, mentre se non ne lascia fisso alcuno è una traslazione oppure una glissoriflessione. Nel primo caso è una rotazione se fissa un solo punto ed è una riflessione se ne fissa più di uno.

Anche le simmetrie centrali, ossia le simmetrie rispetto ad un punto, sono isometrie; poiché fissano un solo punto sono rotazioni (più esattamente rotazioni di 180° intorno al centro di simmetria).

Tra le isometrie possiamo considerare anche il movimento che lascia tutti i punti fissi, detto isometria identica o identità; poiché lascia fissi i punti, non modifica neppure le distanze reciproche. Osserviamo inoltre che ad ogni isometria m corrisponde una isometria inversa m', ossia il movimento che eseguito dopo m fa ritornare tutti i punti nella loro posizione di partenza ossia tale che eseguendo prima m e poi m' si ottenga l'isometria identica; notiamo che si ottiene l'isometria identica anche eseguendo m' prima di m.

Attenzione: la composizione di movimenti non è sempre commutativa ossia il risultato può cambiare se eseguiamo in sequenza le stesse isometrie, ma in ordine diverso. Per esempio prima traslare e poi ruotare può dare un risultato diverso dal movimento che si otterrebbe prima ruotando e poi traslando. Per le glissoriflessioni, invece, è indifferente prima traslare e

poi riflettere (rispetto ad una retta parallela alla direzione di traslazione) o viceversa.

Proposizione 6.5. *L'insieme delle isometrie del piano rispetto all'operazione di composizione è un gruppo non commutativo.*

I movimenti eseguiti dalle gru dei cantieri edili sono sempre composizioni di rotazioni e traslazioni. I movimenti del nostro corpo sono composizioni di rotazioni delle nostre articolazioni. Anche per programmare i movimenti di un robot occorre conoscere molto bene le proprietà delle isometrie e delle loro composizioni.

Simmetrie di figure geometriche

A volte, eseguendo una isometria del piano, succede che una certa figura non solo non cambia forma e dimensione (come è naturale conseguenza della conservazione delle distanze), ma si ritrovi ad occupare esattamente gli stessi punti del piano che occupava prima. Per esempio un quadrato, dopo una rotazione di 90° rispetto al suo centro oppure un ribaltamento rispetto ad uno dei suoi assi, torna esattamente su se stesso.

Definizione 6.6. *Una* ***simmetria di una figura*** *è una isometria che "conserva" la figura nella sua posizione iniziale (i punti della figura si possono muovere, ma solo nelle posizioni già occupate da punti della figura stessa).*

Come per le isometrie, tra le varie possibili simmetrie di figure, consideriamo anche la simmetria identica (o identità), che è il movimento del piano che non muove nessun punto.

Se componiamo due simmetrie di una stessa figura piana, l'isometria risultante è ancora una simmetria di quella stessa figura. Inoltre l'isometria inversa della simmetria di una figura è ancora una simmetria per quella figura. In conclusione:

Proposizione 6.7. *L'insieme delle simmetrie di una figura qualsiasi rispetto all'operazione di composizione è un gruppo.*

A questa idea di "simmetria" si è arrivati dopo un lungo percorso storico, a partire dal primo significato "antico" che era parecchio diverso da quello attuale. Ripercorriamo assieme alcune delle tappe più significative di questo percorso .

Il termine "simmetria" deriva dal greco $\sigma\upsilon\nu$ (con) e $\mu\epsilon\tau\rho o\nu$ (misura) e originariamente significava "commensurabilità" ossia possibilità di mettere

in rapporto numerico due o più elementi, attraverso una "misura comune" contenuta in ciascuno un numero intero di volte. Questo è il significato di "simmetria" che si trova negli Elementi di Euclide.

I seguaci della scuola di Pitagora, che consideravano il "numero" base di tutte le conoscenze ("gli elementi dei numeri sono gli elementi delle cose") credevano sempre possibile confrontare due grandezze attraverso rapporti di numeri interi. Questa visione strettamente aritmetica si collegava però con aspetti legati alla geometria e alla musica. Ad esempio, attraverso i numeri 1, 2, 3, si ottiene come somma il 6, considerato "numero perfetto" perché somma dei suoi divisori; inoltre 1, 2, 3 rappresentavano rispettivamente il punto, la linea nel piano e la figura piana, mentre il 4 rappresentava il "solido". Infine 1, 2, 3, 4 erano collegati agli "intervalli musicali" principali (suoni che producono accordi in particolare armonia tra loro, si ottengono considerando corde le cui lunghezze stanno in rapporti come $2:1$, $3:2$, $4:3$).

Come conseguenza di una "commensurabilità" sempre possibile, la scuola pitagorica aveva una visione dell'universo come regno della simmetria (teoria dell' "armonia cosmica"). La dimostrazione dell'esistenza di "numeri non razionali" come ad esempio $\sqrt{2}$, mandò in crisi questa visione del mondo. Era allora "naturale" chiedersi "dove" potesse trovarsi la simmetria, almeno dal punto di vista geometrico.

D'altra parte, il significato originario di simmetria conduceva all'idea di "accordo" tra elementi, fondato su numeri e misure. Infatti due grandezze commensurabili possono sempre essere messe in rapporto tra loro; e in uno dei "dialoghi" di Platone, il Filebo, si dice che l'introduzione di rapporti numerici elimina la discordanza degli opposti, che in tal modo diventano "simmetrici e consonanti". Proprio in Platone la "simmetria" come proprietà legata alla presenza di "proporzioni armoniche" comincia ad essere associata al concetto di "bellezza". Questa idea è ripresa da Aristotele, per il quale la "proporzione" ($\sigma\upsilon\mu\mu\epsilon\tau\rho\iota\alpha$) e la "ordinata disposizione" ($\tau\alpha\xi\iota\varsigma$) sono le principali forme di bellezza; questo è il modello a cui si ispirano ad esempio alcune statue di scultori greci classici.

L'evoluzione dell'idea originaria di simmetria conduce via via a chiamare "simmetrico" anche un "tutto" formato da elementi tra loro "simmetrici nel senso antico" cioè in qualche rapporto di commensurabilità. La diffusione del concetto di simmetria nel mondo latino è dovuta principalmente al trattato dell'architetto romano Vitruvio e viene vista per lo più come proprietà di un "tutto" composto da parti legate da precise corrispondenze numeriche. In Vitruvio emerge ancora più chiaramente il legame tra simmetria, gradevolezza estetica, presenza di armonia nelle proporzioni, anche se

limitatamente al campo dell'architettura. In Vitruvio possiamo ad esempio leggere :

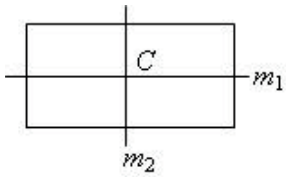
"*Il progetto di un tempio dipende dalla simmetria, i cui principii devono essere diligentemente osservati dall'architetto. Essi sono dovuti alla proporzione. La proporzione è una corrispondenza tra le misure degli elementi di un'intera opera, e dell'intero con una certa parte scelta come modello*".

Nel percorso storico del concetto di simmetria una tappa importante è data dai lavori di Claude Perrault, medico e architetto francese vissuto nella seconda metà del Seicento. Scrive Perrault che l'idea di simmetria va cercata in un "rapporto d'uguaglianza tra parti opposte"; è (in modo ancora intuitivo) quella che noi chiamiamo "simmetria bilaterale", che a sua volta è un caso particolare di simmetria di riflessione. L'idea di "uguaglianza tra le parti" di Perrault è, come dicevamo, ancora molto intuitiva e in parte sbagliata: basta pensare che tra due oggetti che si corrispondono per riflessione c'è un rapporto di uguaglianza di "forma e grandezza" ma anche uno di "disuguaglianza". L'idea è ben esemplificata in "Attraverso lo Specchio " di L. Carroll (l'autore di "Alice nel Paese delle Meraviglie"): Alice, passata al di là dello specchio, trova una stanza che è "la stessa" di prima (sedie, tavolo, caminetto) ma nello stesso tempo "diversa" perché ad esempio l'orologio "al di là " dello specchio segna le ore in senso antiorario per chi è "al di qua". Un altro esempio è dato dalle mani destra e sinistra: esse non sono sovrapponibili, ma sono l'una l'immagine speculare dell'altra; è ragionevole che una configurazione formata da una mano destra (o sinistra) e dalla sua immagine riflessa in uno specchio, si possa definire "simmetrica": ma in che senso?

Un passo avanti verso la soluzione del problema si ha nello studio dei "cristalli" nella seconda metà dell'Ottocento; per una trattazione completa di tale studio rimandiamo alla Lezione 8. Viene fuori l'idea di definire simmetrica una figura nel suo insieme se, come disse il matematico Hermann Weyl (1885-1955) "c'è qualcosa che puoi fare alla figura in modo che, quando hai finito di farla, la cosa sembri uguale a prima "; più precisamente, se la figura è costituita da parti tali che possano "scambiarsi" le posizioni rispetto a determinate "operazioni" in modo che tutto resti invariato. Le "operazioni" nel piano, possono essere, come si è già visto: riflessioni, rotazioni, traslazioni o glissoriflessioni. Si arriva allora, pian piano, alla definizione di "simmetria" data nella Definizione 6.6 e all'idea che ad ogni "simmetria" si possa associare un gruppo.

Le simmetrie del rettangolo. L'insieme delle simmetrie di un rettangolo è costituito dalle riflessioni rispetto alle due rette m_1 e m_2 passanti per i punti medi dei lati e perpendicolari tra loro (indichiamo la simmetria con lo

stesso simbolo della retta), da una rotazione di 180° intorno al loro punto di intersezione C (simbolo r) e dall'operazione identità (simbolo e), che corrisponde alla rotazione nulla o di 360°.



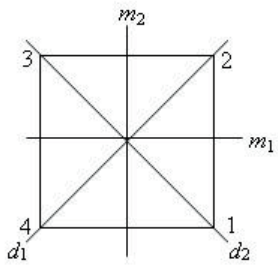
Componendo due qualsiasi di queste simmetrie, ossia applicandole in successione, si ha come risultato una simmetria ancora appartenente all'insieme, come si può osservare dalla seguente tabella:

$*$	e	m_1	m_2	r
e	e	m_1	m_2	r
m_1	m_1	e	r	m_2
m_2	m_2	r	e	m_1
r	r	m_2	m_1	e

La composizione $*$ è quindi un'operazione nell'insieme delle simmetrie del rettangolo, per cui sono valide la proprietà associativa e commutativa; esistono inoltre l'elemento neutro (identità) e l'inverso per ogni elemento dell'insieme.

L'insieme delle simmetrie del rettangolo è dunque un gruppo **commutativo.**

Le simmetrie del quadrato. E' un gruppo anche l'insieme delle simmetrie che mutano in sè un quadrato, costituito dalle tre rotazioni intorno al centro, rispettivamente di 90° , 180° e 270°, dall'identità e dalle riflessioni rispetto alle due rette passanti per i punti medi dei lati e rispetto alle due rette delle diagonali.



Tale gruppo di simmetria non è però commutativo, infatti, cambiando l'ordine di esecuzione di due simmetrie, si possono ottenere due risultati differenti. Ad esempio, una rotazione antioraria di 90° , seguita da una riflessione rispetto alla retta m_1, equivale ad una riflessione rispetto alla retta d_2, mentre la riflessione rispetto a m_1, seguita da una rotazione antioraria di 90°, equivale ad una riflessione rispetto alla retta d_1.

Per vedere in modo più semplice l'azione delle simmetrie, etichettiamo i vertici del quadrato con i numeri da 1 a 4 come in figura; ogni simmetria può allora essere descritta come una permutazione.

Per esempio, una rotazione antioraria di 90°, equivale alla permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

una riflessione rispetto alla retta m_1, equivale alla permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Eseguendo la rotazione antioraria di 90° seguita dalla riflessione rispetto a m_1 otteniamo come risultato una riflessione rispetto alla retta d_2, ciò equivale al prodotto delle permutazioni corrispondenti eseguite nello stesso ordine utilizzato per le simmetrie, il cui risultato è:

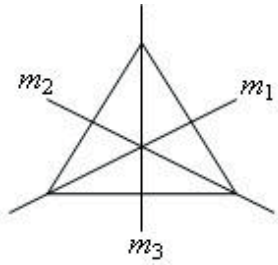
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} .$$

La riflessione rispetto a m_1, seguita dalla rotazione antioraria di 90°, equivale invece ad una riflessione rispetto alla retta d_1 e corrisponde al prodotto delle permutazioni corrispondenti eseguito in ordine inverso rispetto a quello precedente, lo stesso ordine comunque con cui sono state applicate le simmetrie. La permutazione risultato è in questo caso:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} .$$

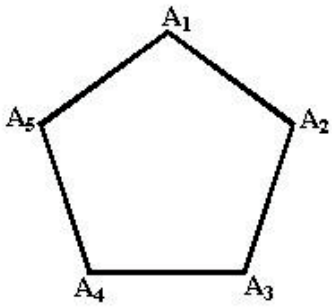
Il gruppo delle simmetrie del quadrato è pertanto un sottogruppo di ordine 8 del gruppo simmetrico S_4. Notiamo che, coerentemente col Teorema di Lagrange, 8 è un divisore di 24.

Le simmetrie di un triangolo equilatero. Anche l'insieme delle simmetrie che mutano in sè un triangolo equilatero è un gruppo non commutativo. Esso è costituito dalle tre riflessioni rispetto ai tre assi di simmetria, dalle due rotazioni intorno al baricentro, rispettivamente di 120° e 240° e dall'identità.



Anche in questo caso, possiamo descrivere le simmetrie del triangolo equilatero attraverso permutazioni di S_3, etichettando i vertici con i numeri 1, 2 e 3. Poiché il triangolo equilatero ammette 6 simmetrie distinte, il suo gruppo delle simmetrie coincide con l'intero gruppo S_3.

Le simmetrie di un poligono regolare. Più in generale, è possibile descrivere il gruppo delle simmetrie di un poligono regolare. Consideriamo un poligono regolare di n lati che possiamo pensare inscritto in una circonferenza il cui centro denotiamo con O. Indichiamo con $A_1, \ldots, A_n$ la sequenza dei vertici (letta, tanto per fissare le idee, in senso orario).



Il gruppo delle simmetrie di tale poligono, che ha esattamente $2n$ elementi come ora mostreremo, è detto **gruppo diedrale** ed è denotato col simbolo D_n.

Ogni elemento di D_n è una trasformazione che, lasciando fisso il poligono, lascia fisso il centro O e trasforma vertici in vertici: quindi è l'identità e oppure è una rotazione di centro O oppure è una riflessione rispetto ad una retta passante per O.

Infatti ogni rotazione di D_n ha centro O e trasforma il vertice A_1 in un vertice A_i: quindi le rotazioni di D_n sono al massimo tante quanti i vertici, ossia n. Anche ogni riflessione di D_n trasforma il vertice A_1 in un vertice A_i ed è quindi la riflessione rispetto alla retta per O e il punto medio del

segmento A_1A_i (se $A_i = A_1$ la retta di riflessione è quella per O e A_1); quindi anche le riflessioni sono al massimo n come i vertici.

D'altra parte, la rotazione di un angolo di $2\pi/n$ in senso antiorario attorno ad O, che chiameremo r_1, sta in D_n; e stanno in D_n anche le rotazioni ottenute componendo r_1 con se stessa $2,\ 3, \ldots, , n-1$ volte, ossia le rotazioni di angoli di ampiezza $4\pi/n,\ 6\pi/n, \ldots,\ 2(n-1)\pi/n$, che chiameremo rispettivamente $r_2,\ r_3, \ldots,\ r_{n-1}$. Quindi in D_n vi sono le n rotazioni date da $r_1,\ r_2,\ r_3, \ldots,\ r_{n-1}$ e dall'identità.

Per quel che riguarda le riflessioni, possiamo notare che, se n è pari, in D_n vi sono le $n/2$ riflessioni con asse la retta congiungente due vertici opposti e le $n/2$ riflessioni con asse la congiungente i punti medi di due lati opposti; se invece n è dispari, gli assi di simmetria congiungono ciascuno degli n vertici col punto medio del lato a lui opposto.

Si può verificare che le n riflessioni si possono ottenere componendo una qualunque riflessione m con ciascuna delle n rotazioni e quindi

$$D_n = \{e,\ r_1,\ \ldots, r_{n-1},\ m,\ mr_1,\ \ldots, mr_{n-1}\}$$

Può essere interessante verificare direttamente come le simmetrie del triangolo equilatero e del quadrato, che sono state sopra descritte in dettaglio, si possono ritrovare come "casi particolari" della trattazione generale per $n = 3$ e $n = 4$ rispettivamente.

A proposito di poligoni regolari

Gli antichi Greci sapevano che una circonferenza può essere divisa con riga e compasso in 3, 5, 15 archi uguali o in n archi uguali dove n è una potenza di 2 moltiplicata per 3, 5, 15 come per esempio, $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2^3$. E negli altri casi?

Dopo "poco più" di 1500 anni **Gauss** (1777-1855) dà la risposta completa a questa questione.

Una circonferenza può essere divisa con riga e compasso in 3, 5, 15, 257 ... 4, 6, 8, 10, 12 ... parti uguali ma non in 7, 11, 13, 14, 19, 22 ... parti uguali.

La regola di Gauss è questa:

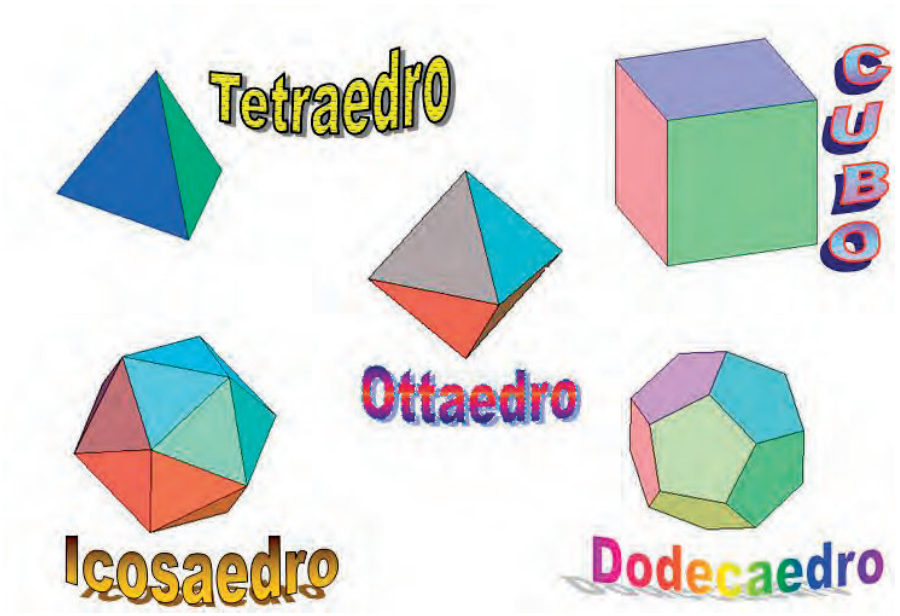
Affinchè un poligono regolare di n lati sia costruibile con riga e compasso occorre che n sia o un numero primo della forma $2^{2^h} + 1$, dove h è un numero naturale (primi di Fermat) o una potenza di 2 eventualmente moltiplicata per numeri del tipo precedente non ripetuti.

Per esempio

- $2^{2^0}+1=3$, $2^{2^1}+1=5$, $2^{2^2}+1=17$, $2^{2^3}+1=257$ sono primi e quindi vanno bene;
- $2^{2^5}+1$ non è primo (è divisibile per 641) e quindi non va bene;
- $4=2^2$, $6=2\cdot 3$, $8=2^3$, $10=2\cdot 5$, $12=2^2\cdot 3$, vanno bene;
- $18=2\cdot 3^2$ non va bene.

Inoltre, non tutti i numeri primi sono del tipo $2^{2^h}+1$: per esempio 11 e 13 non lo sono.

Mentre nel piano vi sono infiniti poligoni regolari, nello spazio i poliedri regolari sono solo 5: **tetraedro**, **cubo**, **ottaedro**, **dodecaedro** e **icosaedro**.



E' possibile definire gli iperpoliedri o politopi regolari in uno spazio di dimensione qualsiasi. Nello spazio di dimensione 4 esistono 6 tipi di iperpoliedri regolari (tra questi il famoso **ipercubo**), ma dalla dimensione 5 in poi ne esistono solo più 3 tipi. Si tratta dei tre iperpoliedri che corrispondono al tetraedro, al cubo ed all'ottaedro. In dimensione 4, come abbiamo già detto, esistono altri tre tipi di iperpoliedri che hanno rispettivamente 24, 120, 600 vertici!

L'ipertetraedro e l'ipercubo in dimensione 4 hanno rispettivamente 5 e 16 vertici, 5 e 8 facce tridimensionali. Nel pensiero greco classico, i solidi

regolari sono entrati anche nella costruzione di una teoria dell'origine e della struttura dell'universo. In uno dei dialoghi di Platone, il Timeo, si descrive la nascita e la struttura di ciò che in natura esiste, sotto forma di mito e in modo strettamente collegato ai solidi regolari. Ai quattro elementi che si riteneva costituissero il mondo corporeo - fuoco, terra, aria, acqua - vengono associati rispettivamente: tetraedro, cubo, ottaedro e icosaedro (in base alla "forma" che, più o meno fantasiosamente, sembrava rapppresentare meglio le caratteristiche degli elementi stessi). Al dodecaedro è associata la "forma dell'universo". Tale solido era infatti considerato da Platone la forma "usata dalla divinità per ricamare le costellazioni sull'insieme dei cieli" (ricordiamo che il dodecaedro è formato da facce pentagonali, e il pentagono rappresentava la figura di riferimento per la scuola pitagorica).

Tale idea ha influenzato anche l'arte: Salvador Dalì nel suo "Sacramento dell'Ultima Cena" disegna un grande dodecaedro fluttuante sul tavolo del banchetto.

I solidi regolari (cioè gli elementi fondamentali) hanno poi una struttura che viene descritta come composizione di "triangoli elementari" particolari, il triangolo rettangolo isoscele e la metà del triangolo equilatero: ogni faccia di un solido è ottenibile attraverso tali triangoli e questa struttura consente di motivare le trasformazioni degli elementi fondamentali attraverso la separazione e la ricombinazione dei triangoli. Questo tentativo di spiegazione di "struttura atomica" è posto tuttora in rapporto con l'attuale fisica delle particelle elementari.

Nello stesso Timeo viene messo già in evidenza il tipo più comune di "simmetria" di cui abbiamo esperienza: quella del corpo umano, che è nel regno animale l'esempio più diffuso di quella che chiamiamo "simmetria bilaterale" (cioè tra destra e sinistra). La simmetria bilaterale è talmente diffusa tra gli animali che riesce difficile pensare si possa attribuire al "caso"; sembra ragionevole pensare che per qualche ragione l'evoluzione "naturale" abbia privilegiato, tra le possibili aggregazioni dei trilioni e trilioni di molecole disponibili, certe configurazioni simmetriche. Alcune motivazioni si possono già notare con relativa facilità: la presenza di simmetria facilita la percezione, e indubbiamente serve a "economizzare". Ma, andando un po' più in profondità, possiamo anche notare ad esempio che la simmetria bilaterale a livello degli occhi permette la "visione binoculare"attraverso cui il cervello valuta la distanza di un oggetto. E ancora: gli studi sul DNA umano hanno messo in evidenza che nel cromosoma Y quasi un ottavo delle lettere G, C, T, A forma delle sequenze "palindromiche", cioè tali che risultano identiche se lette nei due versi sui due filamenti della doppia elica (e per questo il cromosoma Y è stato definito da qualcuno una "galleria degli

specchi"); si pensa che questa simmetria possa servire a fornire "copie di riserva"nel caso di mutazioni nocive.

Gruppi a confronto

Il concetto di gruppo è molto vasto e abbraccia un classe molto ampia di oggetti matematici, spesso di natura e con caratteristiche molto diverse.

Gli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con l'operazione di somma sono dei gruppi. Quando in un gruppo l'operazione è la somma (oppure è una operazione denotata in modo simile alla somma) l'elemento identità si denota con 0 e l'inverso di un elemento si chiama ''opposto".

Per ottenere un gruppo a partire da un insieme numerico e dal prodotto dobbiamo eliminare lo zero (che non ha mai l'inverso moltiplicativo) e, più in generale, considerare soltanto gli elementi dotati di inverso. Se indichiamo con un asterisco il sottoinsieme degli elementi dotati di inverso, otteniamo i gruppi moltiplicativi: $\mathbb{Z}^* = \{1, -1\}$, $\mathbb{Q}^*$,$\mathbb{R}^*$, $\mathbb{C}^*$ (dove gli ultimi tre si ottengono semplicemente cancellando lo zero).

Otteniamo dei gruppi anche a partire dalle classi di resto. Abbiamo infatti i gruppi additivi $(\mathbb{Z}_n\,,\,+)$ con n elementi e i gruppi moltiplicativi $(\mathbb{Z}_n^*\,,\,\cdot)$ con $\phi(n)$ elementi, dove ϕ è la funzione di Eulero (cfr. Lezione 5).

Esempio 6.8. *I gruppi* $(\mathbb{Z}_4\,,\,+)$, $(\mathbb{Z}_5^*\,,\,\cdot)$ *e il gruppo* K *delle simmetrie di un rettangolo (non quadrato) hanno* 4 *elementi ciascuno. Possiamo mettere a confronto le loro strutture mediante le rispettive tabelle delle operazioni.*

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_5^*, \cdot)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(K, *)$	e	m_1	m_2	r
e	e	m_1	m_2	r
m_1	m_1	e	r	m_2
m_2	m_2	r	e	m_1
r	r	m_2	m_1	e

Se prendiamo in esame la prima tabella e in essa sostituiamo gli elementi di $\mathbb{Z}_4$ *con elementi di* $\mathbb{Z}_5^*$ *nel modo seguente:*

$$\begin{array}{rcccc} \mathbb{Z}_4: & 0 & 1 & 2 & 3 \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ \mathbb{Z}_5^*: & 1 & 2 & 4 & 3 \end{array}$$

ci accorgiamo che ritroviamo esattamente (a parte l'ordine con cui sono scritti gli elementi) la seconda tabella scritta sopra ossia la tabella del prodotto in $\mathbb{Z}_5^*$. Non vi è invece nessuna possibile sostituzione negli elementi che potrebbe trasformarla nella tabella della composizione di K.

Due gruppi che, al di là della natura degli oggetti che li costituiscono, hanno sostanzialmente la stessa struttura come $(\mathbb{Z}_4, +)$ e $(\mathbb{Z}_5^*, \cdot)$ si dicono **gruppi isomorfi**. In tal caso è possibile eseguire una sostituzione di elementi dell'uno al posto degli elementi dell'altro in modo che le operazioni risultino tutte corrette. In tal caso, tutte le proprietà valide per l'uno valgono anche per l'altro.

Invece $(\mathbb{Z}_4, +)$ e K non sono gruppi isomorfi, pur avendo lo stesso numero di elementi: si può osservare ad esempio che in K ogni elemento composto con se stesso dà l'identità, mentre in $(\mathbb{Z}_4, +)$ si ha $\overline{3} + \overline{3} = \overline{2} \neq \overline{0}$.

Tra gli esempi di gruppi che abbiamo incontrato (ed in particolare tra i gruppi di simmetrie) possiamo distinguere tipi diversi a seconda di quanti elementi possiedono.

I gruppi delle simmetrie di una figura piana come il quadrato, il rettangolo e il triangolo equilatero si dicono **discreti** in quanto, applicando tutte le trasformazioni di uno di essi ad un qualsiasi punto del piano si ottengono solo un numero finito di posizioni diverse.

In realtà discreto significa letteralmente che non è continuo; ci sono anche gruppi discreti di isometrie che hanno infiniti elementi ma tali che le posizioni in cui spostano un dato punto non si avvicinano mai troppo l'una all'altra (all'intermo di ogni circonferenza possiamo trovarne soltanto un numero finito).

Un esempio di gruppo non discreto è dato, invece, dall'insieme delle rotazioni che trasformano una circonferenza in sè.

I gruppi discreti (se non sono finiti) hanno un insieme numerabile di elementi, ossia possono essere messi in corrispondenza biunivoca con $\mathbb{Z}$. Invece il gruppo delle simmetrie di una circonferenza si può anche chiamare gruppo **continuo** e i suoi elementi si possono mettere in corrispondenza con i numeri reali.

Definizione 6.9. ***Gruppi generati da un numero finito di elementi.*** *Un gruppo additivo (rispettivamente, moltiplicativo) è generato da un numero finito di elementi $a_1, \ldots, a_n$ quando ogni suo elemento può essere scritto come somma (risp. prodotto) degli a_i, o dei loro opposti (inversi), opportunamente scelti.*

Esempio 6.10. *$\mathbb{Z}$ (additivo) è generato dal solo elemento* 1.

$\mathbb{Z}_n$ (additivo) è generato dalla classe $\overline{1}$.

Il gruppo delle simmetrie del rettangolo è generato dagli elementi m_1 *e* m_2 .

★ I gruppi simmetrici

La teoria dei gruppi simmetrici è molto vasta; sono stati già dimostrati moltissimi risultati e si sta ancora studiando la validità o meno di molte congetture. Il motivo di tanto interesse sta nella profondità del loro significato matematico e nelle loro numerose applicazioni in molti campi differenti, matematici e non.

Ricordiamo qui a titolo di esempio (ed anche perché ci saranno utili in seguito) alcuni classici risultati sulle permutazioni.

Teorema 6.11. *Ogni permutazione di* S_n *può essere ottenuta come prodotto di scambi.*

Teorema 6.12. *Ogni permutazione di* S_n *può essere ottenuta come prodotto di scambi del tipo* s_{1k} *(*s_{1k} *scambia l'elemento di posto* 1 *con l'elemento di posto* k*, dove* k *può essere* 2, 3,. . . , n*).*

Le dimostrazioni di questi teoremi vengono lasciate come esercizio al lettore. Per semplicità si consiglia di fissare le idee sul caso $n = 5$ (questo è anche il caso che piò ci sarà utile in seguito). Si consiglia inoltre l'utilizzo di un mazzo di carte come **materiale didattico** (nelle pause della dimostrazione si può anche fare una partita).

Le dimostrazioni possono essere formulate sotto forma di algoritmo e completate da stime del numero massimo di scambi (qualsiasi nel primo caso, di tipo s_{1k} nel secondo caso) necessari per ottenere ogni permutazione.

Come conseguenza dei risultati precedenti possiamo dire:

Corollario 6.13. *Se* H *è un sottogruppo di* S_n *che contiene tutti gli scambi (o anche soltanto gli scambi del tipo* s_{1k}*), allora* H *è tutto* S_n*.*

Un **ciclo** di ordine r (o r-ciclo) di S_n è ogni permutazione c_r di S_n che si ottiene nel modo seguente:

a. si fissano r numeri diversi scelti tra 1 e n e si scrivono in un qualche fissato ordine: siano $a_1,\ a_2,\ \cdots,\ a_r$;

b. si parte da e; si prende (nella seconda riga) l'elemento che sta nel posto a_1 e lo si mette nel posto a_2, si mette poi l'elemento che occupava il posto a_2 nel posto a_3, e così via; si conclude sistemando l'elemento che era nel posto a_r nel posto a_1 che nel frattempo è sempre rimasto vuoto.

Può essere utile tener presente che, per ogni $s \in S_n$, la permutazione $c_r\, s$ si può ottenere col procedimento descritto in **b.** a partire da s invece che da e.

Esempio 6.14. *La permutazione di S_3 che abbiamo indicato con s_{12}, ossia lo scambio degli elementi di posto* 1 *e* 2 *non è altro che il* 2*-ciclo corrispondente ai numeri $a_1 = 1$ e $a_2 = 2$.*

La permutazione di S_3 che abbiamo indicato con p_1, ossia 1 *passo avanti non è altro che il* 3*-ciclo corrispondente ai numeri $a_1 = 1$, $a_2 = 2$ e $a_3 = 3$.*

Esercizio 6.15. Studiare la decomposizione in cicli di una qualsiasi permutazione di S_5.

Esercizio 6.16. Provare che se H è un sottogruppo di S_5 che contiene uno scambio (si fissi s_{12}) e un ciclo d'ordine 5 (si fissi $a_1 = 1,\ a_2 = 2,\ ,\ a_3 = 3,\ a_4 = 4,\ a_5 = 5$), allora H è tutto S_5.

★ Il gruppo di Galois di un'equazione

In questo paragrafo, per semplicità, ci occuperemo soltanto di equazioni con coefficienti interi.

(In realtà tutto quello che diremo vale in generale, solo con qualche complicazione formale.)

Sappiamo che i coefficienti di un'equazione si possono scrivere per mezzo di espressioni simmetriche mediante le soluzioni dell'equazione stessa. In queste espressioni le soluzioni possono essere "permutate tra loro" in tutti i modi possibili senza che le espressioni nel loro complesso vengano alterate.

Piò in generale possiamo considerare tutte le possibili relazioni polinomiali a coefficienti interi nelle soluzioni dell'equazione. Come mostreranno gli esempi seguenti, alcune permutazioni delle soluzioni conservano la correttezza di tali relazioni, mentre altre permutazioni ne rendono false alcune. Vedremo che l'insieme delle permutazioni che rispettano tutte le relazioni polinomiali tra le soluzioni dell'equazione formano un gruppo.

Esempio 6.17. *Consideriamo l'equazione:*

$$(x^2 - 2)(x^2 - 3)(x^2 - 6)(x - 2) = 0$$

le cui soluzioni sono:

$$\alpha_1 = \sqrt{2},\ \alpha_2 = -\sqrt{2},\ \alpha_3 = \sqrt{3},\ \alpha_4 = -\sqrt{3},\ \alpha_5 = \sqrt{6},\ \alpha_6 = -\sqrt{6},\ \alpha_7 = 2.$$

La permutazione che scambia α_1 con α_7 e lascia le altre invariate non è accettabile; infatti l'espressione polinomiale a coefficienti interi $\alpha_7 = 2$ è corretta, mentre sostituendo in essa α_1 ad α_7 otteniamo la relazione errata $\alpha_1 = 2$. Anzi, tutte le permutazioni accettabili dovranno lasciare fermo α_7 in quanto α_7 è un numero intero.

La permutazione che scambia α_1 *con* α_2 *e lascia le altre invariate non è accettabile perché la relazione polinomiale a coefficienti interi* $\alpha_1 \cdot \alpha_3 = \alpha_5$, *che è corretta , verrebbe trasformata nella relazione falsa* $\alpha_2 \cdot \alpha_3 = \alpha_5$.

Risulta invece accettabile, da tutti i punti di vista, la permutazione che scambia α_1 *con* α_2, α_3 *con* α_4 *e lascia invariate* α_5, α_6 *e* α_7. *Possiamo sintetizzare questa permutazione con la tabella:*

$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 \end{pmatrix}.$$

Esempio 6.18. *"**La permutazione coniugio.**" Come abbiamo visto nella Lezione 3, se un'equazione a coefficienti reali ha una soluzione* α *non reale, anche* $\overline{\alpha}$ *è soluzione della stessa equazione. Pertanto possiamo considerare la permutazione che scambia tra loro le soluzioni complesse coniugate e lascia fisse quelle reali. Tale permutazione è sempre accettabile. Infatti il coniugato di una somma è la somma dei coniugati e il coniugato di un prodotto è il prodotto dei coniugati; se* $F(\alpha_1, \ldots, \alpha_n) = G(\alpha_1, \ldots, \alpha_n)$ *è una relazione corretta tra le soluzioni di una equazione, allora* $F(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) = \overline{F(\alpha_1, \ldots, \alpha_n)}$ *e* $G(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) = \overline{G(\alpha_1, \ldots, \alpha_n)}$ *e quindi* $F(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) = G(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$ *è ancora corretta.*

Le permutazioni delle n soluzioni di un'equazione di grado n che rispettano le relazioni polinomiali a coefficienti interi formano un sottogruppo di S_n che si chiama **gruppo di Galois** dell'equazione.

Si noti che almeno una permutazione che va bene c'è sempre: la permutazione e che lascia ferme tutte le soluzioni!

Possiamo poi considerare un insieme più vasto di relazioni polinomiali, ammettendo come coefficienti anche numeri non interi.

Esempio 6.19. *(J. B. Fraleigh, A first course in Abstract Algebra.)*

L'equazione $x^4 - 2 = 0$ *ha le seguenti soluzioni:*

$$\alpha_1 = \sqrt[4]{2},\ \alpha_2 = -\sqrt[4]{2},\ \alpha_3 = i\sqrt[4]{2},\ \alpha_4 = -i\sqrt[4]{2}.$$

Con qualche ragionamento si può vedere che ci sono esattamente 8 *permutazioni accettabili, che sono:*

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad q_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad q_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$q_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad q_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad q_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$q_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad q_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} .$$

Se ora ammettiamo tra i coefficienti delle relazioni oltre ai numeri interi anche $\sqrt{2}$*, allora solo una parte di queste sono accettabili. Ad esempio* q_1 *non è più accettabile perché l'espressione corretta* $\alpha_1^2 = \sqrt{2}$ *si trasformerebbe nell'espressione errata* $\alpha_3^2 = \sqrt{2}$*.*

Con questa ulteriore condizione otteniamo il sottogruppo H *che contiene soltanto le permutazioni:*

$$e \ , \quad q_2 \ , \quad q_4 \ , \quad q_6$$

che costituiscono un sottogruppo ancora più piccolo.

Se a questo punto ammettiamo tra i coefficienti delle relazioni anche $\sqrt[4]{2}$*, otteniamo l'ulteriore sottogruppo* K *costituito da:*

$$e \ , \quad q_4.$$

Se infine ammettiamo tra i coefficienti anche l' unità immaginaria i*, allora otteniamo il sottogruppo banale, costituito solo da*

$$e.$$

Facciamo ora alcune considerazioni su quanto ottenuto.

a. *Il gruppo di Galois dell'equazione* $x^4 - 2 = 0$ *ha dei sottogruppi, ottenibili ampliando l'insieme dei coefficienti delle relazioni soddisfatte dalle soluzioni.*

b. *Il gruppo di Galois iniziale contiene elementi che trasformano una qualsiasi delle soluzioni in ciascuna delle altre soluzioni. Questa caratteristica corrisponde al fatto che* $x^4 - 2$ *non si può spezzare nel prodotto di due polinomi utilizzando soltanto coefficienti interi.*

c. *Considerando relazioni in cui compare anche* $\sqrt{2}$*, invece, gli elementi del sottogruppo* H *scambiano tra loro solo* α_1 *con* α_2 *(le soluzioni di* $x^2 - \sqrt{2} = 0$*) e rispettivamente* α_3 *con* α_4 *(le soluzioni di* $x^2 + \sqrt{2} = 0$*). Questo corrisponde al fatto che il polinomio* $x^4 - 2$ *si può spezzare nel prodotto*

$$(x^2 - \sqrt{2})(x^2 + \sqrt{2})$$

pur di ammettere tra i coefficienti anche $\sqrt{2}$*.*

Utilizzando tra i coefficienti anche $\sqrt[4]{2}$ *non è più possibile scambiare* α_1 *con* α_2 *, poiché utilizzando anche* $\sqrt[4]{2}$, $x^4 - 2$ *si può spezzare nel prodotto:*

$$(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt[2]{2}).$$

Infine utilizzando anche i, *non si possono permutare in alcun modo le radici poiché* $x^4 - 2$ *si spezza completamente come:*

$$(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

d. *Abbiamo inizialmente preso in esame tutte le permutazioni tra le soluzioni che sono compatibili con le relazioni a coefficienti interi, ottenendo il* **gruppo di Galois** *dell'equazione. Abbiamo poi aumentato le relazioni ottenendo via via sottogruppi sempre più piccoli. Si raggiunge il gruppo banale* $\{e\}$ *quando i numeri utilizzati come coefficienti permettono di scrivere tutte le soluzioni!*

e. *Dalle considerazioni precedenti, segue che se le radici di una equazione si possono scrivere mediante radicali allora vi è una catena di sottogruppi uno contenuto nell'altro, che parte dal gruppo di Galois e arriva fino al sottogruppo formato dalla sola permutazione identica* e. *I sottogruppi così ottenuti sono in realtà dei sottogruppi di tipo particolare; non intendiamo entrare in dettagli troppo tecnici, ma notiamo ad esempio che il rapporto tra i numeri di elementi di due gruppi consecutivi è sempre un numero primo.*

Nell'esempio precedente abbiamo calcolato il gruppo di Galois dell'equazione a partire dalle soluzioni dell'equazione. Se conosciamo già le soluzioni, sembra un po' inutile chiederci se c'è o meno una formula per radicali che permette di trovarle: è un cane che si morde la coda.

Vedremo però nell'esempio successivo che non è necessario conoscere già le soluzioni per calcolare il gruppo di Galois di una equazione.

Esempio 6.20. *Il polinomio* $x^5 - 16x + 2$ *non si spezza nel prodotto di due polinomi di grado minore a coefficienti interi. La verifica di questo fatto richiede soltanto semplici considerazioni sui numeri interi e qualche calcolo.*

Allora ogni soluzione di questa equazione deve poter essere scambiata con qualsiasi altra mediante una qualche permutazione del gruppo di Galois. Poiché 5 *è un numero primo, si dimostra che questo può avvenire soltanto se nel gruppo di Galois c'è un* 5 *ciclo.*

Eseguendo lo studio della funzione $y = x^5 - 16x + 2$ *ci si può inoltre convincere che ci sono* 3 *soluzioni reali e due complesse non reali. Nel gruppo di Galois vi è allora anche la permutazione data dal coniugio che è lo scambio delle due soluzioni non reali.*

Come abbiamo già detto nell'Esercizio 6.16, il gruppo di Galois, contenendo uno scambio e un 5*-ciclo, non può essere altro che tutto* S_5.

Arriviamo così alla conclusione del nostro viaggio attraverso la teoria di Galois, che prova la non risolubilità della generica equazione di grado 5.

Se ci fosse la formula risolutiva per le equazioni di grado 5, allora potrebbe servire anche a risolvere per radicali l'equazione dell'**Esempio** 6.20. Potremmo allora partire dal suo gruppo di Galois, che è S_5, aggiungere una alla volta i radicali necessari per scrivere tutte le sue soluzioni, costruendo ad ogni passo sottogruppi via via più piccoli, fino ad arrivare al solo e. Inoltre questa catena di sottogruppi sarebbe del tipo particolare di cui si è detto prima.

Questo però non lo potremo fare, perché Galois ha dimostrato che S_5 non possiede una tale catena di sottogruppi.

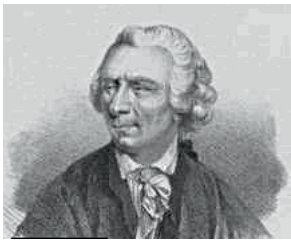
Allora l'equazione $x^5 - 16x + 2 = 0$ non è risolubile per radicali e, a maggior ragione, non lo è l'equazione generica di grado 5.

⁕ Chi erano...

Eulero. Leonhard Euler, meglio conosciuto in italiano come Eulero, è stato senza dubbio uno dei più grandi matematici di tutti i tempi, certamente il più grande del suo secolo, il Settecento, il secolo dei lumi.

La sua opera consta di quasi 90 lavori in ogni settore dello scibile scientifico, molti dei quali prodotti negli ultimi anni della sua vita quando era ormai cieco.

Nacque il 15 aprile 1707 a Basilea, dove la famiglia si era rifugiata per sfuggire alle guerre di religione e dove studiò alla scuola del grande matematico Johann Bernoulli, del quale fu l'allievo preferito, il che già non era cosa facile per l'indole sospettosa ed invidiosa del maestro; pare, però, che Bernoulli gli dedicasse una lezione privata ogni sabato pomeriggio. Anche successivamente, quando Eulero si trasferì all'estero, la corrispondenza fra il vecchio maestro e l'allievo fu sempre intensa e cordiale, fino al riconoscimento della superiorità dell'allievo ed alla sua definizione di Principe dei matematici.



A vent'anni Eulero si trasferì a San Pietroburgo alla corte di Caterina I, grande imperatrice di tutte le Russie, al seguito del figlio di Johann, Daniel Bernoulli, che era stato nominato professore di matematica presso l'Imperiale Accademia delle Scienze; pochi anni dopo assunse la cattedra di Bernoulli e la tenne fino al 1741, quando fu nominato professore di Matematica e Fisica all'Accademia di Berlino. A Berlino rimase fino al 1766, quando ritornò alla sua San Pietroburgo dove rimase fino alla morte nel 1783.

Così vasta fu la sua produzione che l'Accademia delle Scienze continuò a pubblicarne le opere per più di trent'anni dopo la morte. La sua *Introductio in Analisys Infinitorum* in due volumi del 1748 è considerata la base della moderna analisi matematica.

Leggendarie erano la sua memoria e la sua capacità di concentrazione. Si narra che fosse capace di recitare l'intera Eneide parola per parola, che avesse scritto la maggior parte dei suoi lavori in presenza dei figlioletti che giocavano e che fosse in grado di riprendere un discorso interrotto anche a distanza di tempo.

Tra l'altro Eulero ha dato un nome a molte costanti ed operatori matematici, nomi ancora oggi in uso; fu lui per primo a usare il simbolo π (in onore di Pitagora), la lettera i per l' unità immaginaria $\sqrt{-1}$, la notazione f(x) per indicare le funzioni, Σ per le sommatorie, la e per la base dei logaritmi naturali e tante altre ancora oggi in uso.

♣ Esercizi per la sesta lezione

6.1 Calcolare i prodotti tra le permutazioni di S_4:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \qquad t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} .$$

6.2 Calcolare l'inversa in S_4 di ciascuna delle seguenti permutazioni:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \qquad q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} .$$

6.3 Scrivere tutte le permutazioni di S_3 corrispondenti alle simmetrie di un triangolo isoscele e verificare che formano un sottogruppo di S_3.

6.4 Indicato con G il gruppo delle simmetrie del triangolo equilatero:

a) per ogni elemento di G scrivere il corrispondente elemento di S_3;

b) costruire la tabella della composizione di G, confrontarla con quella di S_3 e verificare che G ed S_3 sono gruppi isomorfi.

6.5 Costruire la tabella della composizione del gruppo delle simmetrie di un quadrato. É un gruppo commutativo?

6.6 Costruire la tabella della composizione del gruppo delle simmetrie di un triangolo scaleno. É un gruppo commutativo?

6.7 Scrivere tutte le permutazioni di S_4 corrispondenti alle simmetrie di un rettangolo (non quadrato) e verificare che formano un sottogruppo di S_4.

6.8 Costruire la tabella della composizione del gruppo delle simmetrie di un rombo (non quadrato). Scrivere poi tutte le permutazioni di S_4 corrispondenti alle simmetrie trovate.

6.9 Nella figura sottostante sono rappresentati dei rosoni, figure cioè che hanno le stesse simmetrie di rotazione di un poligono regolare. Trovare qual è il poligono regolare associato a ciascun rosone, evidenziando gli eventuali assi di simmetria e le ampiezze degli angoli delle simmetrie di rotazione.

6.10 Costruire la tabella della somma di $\mathbb{Z}_6$ e la tabella della composizione delle simmetrie del triangolo equilatero. Si tratta di gruppi isomorfi?

6.11 Trovare tutti i sottogruppi additivi di $\mathbb{Z}_6$ e $\mathbb{Z}_7$.

6.12 Trovare tutti i sottogruppi moltiplicativi di $\mathbb{Z}_6^*$ e $\mathbb{Z}_7^*$.

6.13 Individuare da quali numeri è formato il sottogruppo additivo di $\mathbb{Z}$ generato dal numero 3.

6.14 Individuare da quali numeri è formato il sottogruppo additivo di $\mathbb{Z}$ generato dai numeri 6 e 15.

6.15 Verificare che l'insieme $\mathbb{R}[x]$ dei polinomi nella indeterminata x costituisce un gruppo additivo. Costituisce un gruppo moltiplicativo se togliamo il polinomio 0 ?

6.16 $\mathbb{R}[x]$ è un anello? É un campo?

6.17 Provare che $\{z \in \mathbb{C} \mid z = cos(t) + isin(t),\ 0 \leq t < 2\pi\}$ è un sottogruppo moltiplicativo di $\mathbb{C}$.

6.18 Individuare quali isometrie del piano sono rappresentate dalle seguenti equazioni, che associano al punto del piano di coordinate (x, y) il punto dello stesso piano di coordinate (x', y'):

$$\begin{cases} x' = x + 1 \\ y' = y - 1 \end{cases} \qquad \begin{cases} x' = \frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y \\ y' = \frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y \end{cases} \qquad \begin{cases} x' = \frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y \\ y' = \frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y \end{cases}$$

6.19 Determinare il gruppo di Galois dell'equazione $(x-3)(x^2-4x+5) = 0$.

6.20 Determinare il gruppo di Galois dell'equazione $x^4 - 1 = 0$.

6.21 Determinare il gruppo di Galois dell'equazione $x^4 + 1 = 0$.

6.22 Dato l'insieme $\mathbb{Z}$ con l'operazione $*$ definita da $a * b = a + b + 4$ (dove $+$ indica l'ordinaria operazione di somma tra interi):

a) stabilire se è un gruppo;

b) calcolare gli opposti di -6 e 10;

c) calcolare $((-2) * 3) * (-4)$;

d) risolvere l'equazione $2 + (0 * x) = (3 * 0)$.

6.23 Dato l'insieme $\mathbb{R}$ con l'operazione $\circ$ definita da $a \circ b = a + b + a \cdot b$ (dove $+$ e $\cdot$ indicano le ordinarie operazioni di somma e prodotto tra numeri reali):

a) calcolare l'opposto di 7 e quello di $\frac{3}{4}$;

b) calcolare $(-\frac{1}{2} \circ 2) \circ (-3)$;

c) risolvere l'equazione nell'incognita x: $3 - (a \circ x) = (2 \circ a) - a$ dove a è un qualsiasi numero reale.

6.24 Provare mediante un esempio che $\mathbb{Z}_{10}$ non è un campo rispetto alla somma e al prodotto di classi.

6.25 Provare mediante un esempio che $\mathbb{Z}_8$ non è un campo. Qual è il l'inverso della classe $\overline{3}$ rispetto al prodotto? Qual è l'opposto di $\overline{4}$ rispetto alla somma?

Modulo 4

Simmetrie nel piano e nello spazio

Lezione 7

I vettori

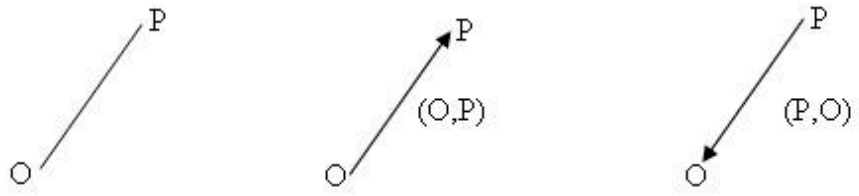
Vettori applicati e loro operazioni

In questo paragrafo supporremo sempre fissato un punto O nel piano (o nello spazio) ordinario detto origine.

Definizione 7.1. *Chiamiamo vettori applicati in O tutte le coppie ordinate del tipo (O, P) dove P è un altro punto del piano (o dello spazio); denotiamo con il simbolo V^O l'insieme di tutti i vettori applicati in O.*

Tra le coppie possibili dobbiamo considerare anche la "coppia identica" (O, O), che chiameremo ***vettore nullo*** *applicato in O.*

Rappresentiamo graficamente questi vettori come frecce o segmenti orientati con la punta nel secondo estremo. La scelta di una freccia si spiega in quanto dobbiamo rappresentare una coppia ordinata di punti e non un semplice insieme costituito da 2 punti.



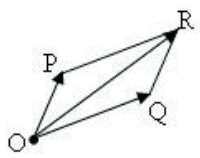
Inoltre osserviamo che nella nostra rappresentazione grafica del vettore applicato (O, P) coinvolgiamo tutti i punti che "stanno tra" O e P; in effetti si tratta di una pura comodità grafica visto che i vettori sono determinati univocamente dagli estremi.

Siano (O, P), (O, Q) due vettori applicati del piano (o dello spazio). Se O, P e Q non sono allineati, possiamo costruire a partire da essi il parallelogramma $OPRQ$, con diagonali PQ e OR; se invece O, P e Q sono allineati, indichiamo con R il punto ottenuto percorrendo prima la freccia (OP) e poi la freccia (OQ) traslata in modo da sovrapporre l'estremo O a P.

Definizione 7.2. ***Somma di vettori applicati.*** *Poniamo:*

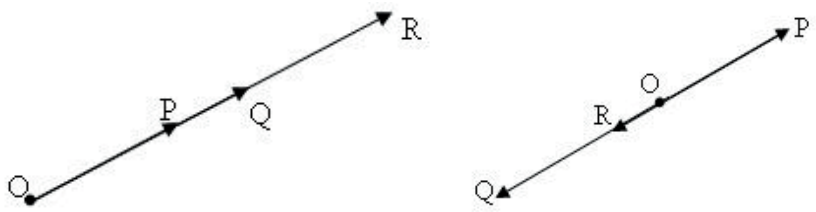
$$(O, P) + (O, Q) = (O, R)$$

dove R è il punto sopra costruito.



Inoltre definiamo:

$$(O, P) + (O, O) = (O, O) + (O, P) = (O, P).$$



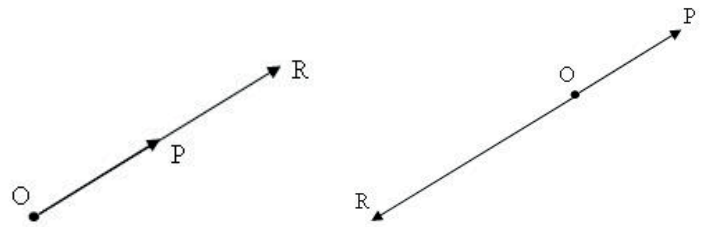
Siano ora λ un numero reale e (O, P) un vettore non nullo. Costruiamo il punto R sulla retta OP in modo che la lunghezza della freccia (O, R) sia $|\lambda|$ volte quella della freccia (O, P) e che il verso di (O, R) sia quello di (O, P) se λ è positivo, quello opposto se è negativo.

Definizione 7.3. ***Prodotto di un vettore applicato per uno scalare*** *Si dice prodotto del vettore (O, P) per lo scalare λ il vettore:*

$$\lambda(O, P) = (O, R)$$

dove R è il punto sopra definito. Nel caso $O = P$ oppure $\lambda = 0$, allora:

$$\lambda(O, P) = (O, O).$$



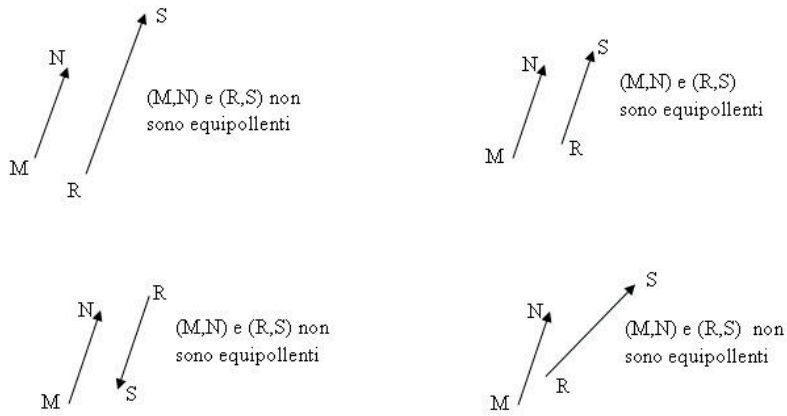
Introduciamo ora il concetto di **vettori applicati equipollenti**. Consideriamo l'insieme $V = \bigcup_P V^P$, dove P varia tra tutti i punti del piano (o dello spazio) e V^P indica l'insieme dei vettori applicati in P: V è quindi l'insieme di **tutti** i vettori applicati.

Definizione 7.4. *Diciamo che (P, Q), (P', Q') sono equipollenti se $P = Q$ e $P' = Q'$ oppure se $P \neq Q$, $P' \neq Q'$ e valgono le tre seguenti condizioni:*

(1) *la retta per P e Q è parallela alla retta per P' e Q'*

(2) *il segmento PQ è congruente al segmento $P'Q'$,cioè i due segmenti hanno la stessa lunghezza*

(3) *i vettori applicati (P, Q) e (P', Q') hanno lo stesso verso.*



Dunque le frecce (P, Q) e (P', Q') sono equipollenti se hanno la stessa lunghezza, la stessa direzione e lo stesso verso.

Osserviamo che la relazione ora introdotta nell'insieme V dei vettori applicati è una relazione d'equivalenza.

Avendo dunque una relazione di equivalenza sull'insieme V possiamo considerare l'insieme delle classi di equivalenza: indichiamo tale insieme con il simbolo $\mathcal{V}$.

Definizione 7.5. *Sia (P, Q) un vettore applicato e consideriamo la classe di equivalenza dei vettori applicati equipollenti ad esso; indicheremo tale*

classe, pensata come elemento dell'insieme $\mathcal{V}$ con il simbolo $\overrightarrow{PQ}$, che d'ora in poi sarà chiamato vettore libero. Il vettore applicato (P, Q) è detto rappresentante di $\overrightarrow{PQ}$.

Denoteremo i vettori liberi anche con lettere in grassetto $\mathbf{v}$, $\mathbf{w}$, $\mathbf{u}$ oppure con la notazione $Q - P = \overrightarrow{PQ}$.

Il vettore $\overrightarrow{OO} = \overrightarrow{PP} = \overrightarrow{QQ} = \ldots$ è detto **vettore nullo** e viene indicato con $\mathbf{0}$ oppure $\vec{0}$.

Osservazione 7.6. Si noti che un vettore libero ammette sempre uno e un unico rappresentante in ogni insieme V^P.

Dato che un vettore libero è un insieme di vettori applicati, per **rappresentare graficamente un vettore libero** basta limitarsi a rappresentare graficamente un solo vettore applicato (cioè a scegliere un rappresentante). Il contesto del discorso e le notazioni chiariranno se ci si sta riferendo a quel particolare vettore applicato o al vettore libero che esso individua.

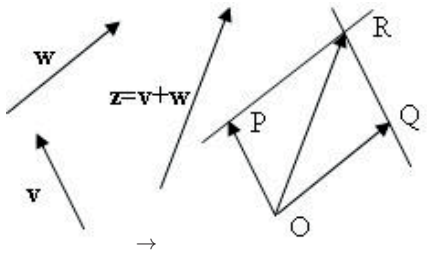
Operazioni tra vettori liberi

Definiamo le operazioni di addizione e moltiplicazione per uno scalare in $\mathcal{V}$.

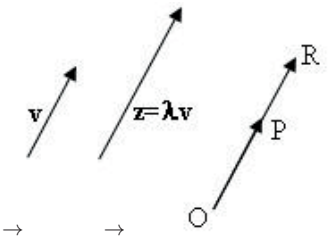
Definizione 7.7. *Fissiamo un punto O del piano (o dello spazio) e siano $\mathbf{v}$ e $\mathbf{w}$ due vettori di $\mathcal{V}$ e λ un numero. Ciascuno dei due vettori liberi ha un unico rappresentante in V^O: siano essi (O, P) e (O, Q) rispettivamente.*

- *La **somma** di $\mathbf{v}$ e $\mathbf{w}$ è il vettore libero $\mathbf{z} = \overrightarrow{OR}$ tale che $(O, R) = (O, P) + (O, Q)$ come vettori applicati in O; in simboli:*

  $$\overrightarrow{OP} + \overrightarrow{OQ} = \overrightarrow{OR} \quad \text{se e solo se} \quad (O, R) = (O, P) + (O, Q)$$



- *L'**opposto** di un vettore $\overrightarrow{OP}$ indicato col simbolo $-\overrightarrow{OP}$ è il vettore $\overrightarrow{PO}$.*
- *Il **prodotto dello scalare** λ per $\overrightarrow{OP}$ è il vettore libero $\overrightarrow{OR}$ tale che $(O, R) = \lambda(O, P)$ come vettori applicati in O.*

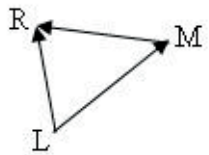


Proposizione 7.8. $(-1)\,\overrightarrow{OP} = -\,\overrightarrow{OP}$.

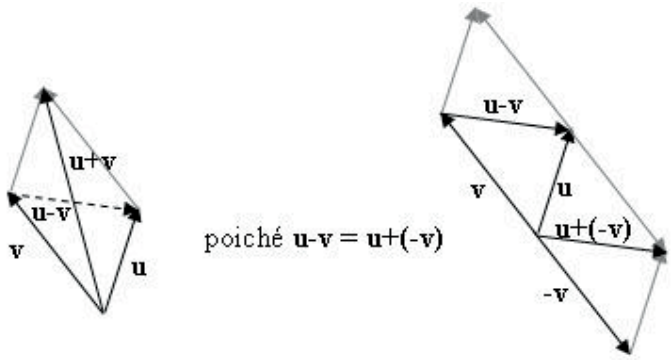
In definitiva abbiamo sfruttato semplicemente le operazioni già definite negli spazi dei vettori applicati; d'altra parte dopo aver operato in tale maniera ci si deve chiedere se quello che abbiamo ottenuto dipende o meno dalla scelta dei rappresentanti, cioè se il vettore $\mathbf{v} + \mathbf{w}$ e il vettore $\lambda\mathbf{v}$ dipendono dalla scelta del punto O. Se accadesse questo chiaramente la precedente definizione sarebbe scorretta; invece tutto funziona bene, come è possibile verificare con l'ausilio di qualche disegno.

Osservazione 7.9. Per ogni terna di punti L, M, R si ha:

$$\overrightarrow{LM} + \overrightarrow{MR} = \overrightarrow{LR}\,.$$



Inoltre, dati due vettori $\mathbf{u}$, $\mathbf{v}$ è utile notare che $\mathbf{u} - \mathbf{v}$ è rappresentato "dall'altra"diagonale del parallelogramma di lati $\mathbf{u}$, $\mathbf{v}$ (tratteggiata nel disegno sottostante).



Proprietà. $\mathcal{V}$ con l'operazione di somma precedentemente introdotta costituisce un gruppo commutativo poiché sono soddisfatte:

- la proprietà associativa e commutativa
- l'esistenza dell'elemento neutro che è $\mathbf{0}$
- ogni vettore libero $\mathbf{v}$ ammette opposto $-\mathbf{v}$.

Oltre a queste valgono anche varie altre proprietà che coinvolgono la somma e il prodotto per uno scalare grazie alle quali $\mathcal{V}$ acquista una nuova struttura.

Definizione 7.10. *$\mathcal{V}$ con le operazioni di somma e prodotto per scalare è detto* ***spazio vettoriale reale****.*

Definizione 7.11. *Due vettori del piano o dello spazio vengono detti* ***linearmente dipendenti*** *(o semplicemente dipendenti) se ammettono rappresentanti paralleli, ossia uno è multiplo dell'altro.*

Tre vettori vengono detti ***(linearmente) dipendenti*** *se ammettono tre rappresentanti complanari.*

Due (analogamente tre) vettori sono detti ***linearmente indipendenti*** *se non sono dipendenti.*

É evidente dalla definizione che tre vettori del piano sono sempre dipendenti.

Nel caso dei vettori del piano si dice poi che $\mathcal{V}$ è uno spazio vettoriale di dimensione 2, poiché fissati due vettori indipendenti $\mathbf{v_1}$ e $\mathbf{v_2}$, ogni altro vettore $\mathbf{u}$ può essere scritto come la somma di un multiplo dell'uno e di un multiplo dell'altro, ossia:

$$\mathbf{u} = \lambda_1 \mathbf{v_1} + \lambda_2 \mathbf{v_2}.$$

In tal caso diciamo che $\mathbf{u}$ è **combinazione lineare** di $\mathbf{v_1}$ e $\mathbf{v_2}$.

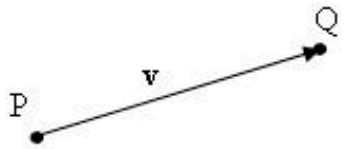
Nel caso dei vettori dello spazio $\mathcal{V}$ si dice di dimensione 3, poiché fissati tre vettori indipendenti $\mathbf{v_1}$, $\mathbf{v_2}$ e $\mathbf{v_3}$, ogni altro vettore $\mathbf{u}$ può essere scritto come somma di loro multipli, ossia:

$$\mathbf{u} = \lambda_1 \mathbf{v_1} + \lambda_2 \mathbf{v_2} + \lambda_3 \mathbf{v_3}.$$

In tal caso diciamo che $\mathbf{u}$ è **combinazione lineare** di $\mathbf{v_1}$, $\mathbf{v_2}$ e $\mathbf{v_3}$.

Traslazioni del piano e dello spazio

Ogni vettore $\mathbf{v}$ individua una e una sola traslazione ossia una funzione che ad un qualsiasi punto P, del piano o dello spazio, associa il punto Q tale che $\mathbf{v} = \overrightarrow{PQ}$.



Proprietà. L'insieme delle traslazioni (del piano o dello spazio) è un gruppo rispetto all'operazione di composizione di isometrie. Si tratta in particolare di un gruppo commutativo.

Osservazione 7.12. La commutatività del gruppo delle traslazioni discende dalla commutatività del gruppo $\mathcal{V}$, anche se le traslazioni formano un sottogruppo del gruppo delle isometrie che, come abbiamo visto, non è commutativo.

Reticoli del piano e dello spazio

Definizione 7.13. *Un* ***reticolo*** *è un insieme di punti del piano (o dello spazio) "indotto" dal gruppo generato (si veda la Definizione 6.9) da due (rispettivamente tre) traslazioni associate a vettori indipendenti.*

I due disegni seguenti illustrano un reticolo piano ed uno spaziale.

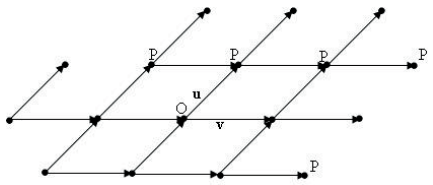


Figura 1. Reticolo nel piano

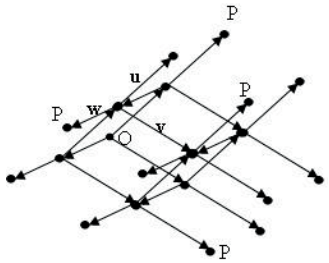


Figura 2. Reticolo nello spazio

Dunque ogni punto P del reticolo piano (spaziale) è ottenibile a partire da un punto O fissato a piacere, dello stesso reticolo, mediante traslazioni successive associate ai vettori $\mathbf{u}$ e $\mathbf{v}$ (rispettivamente $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$ nello spazio).

I punti di un reticolo vengono detti **nodi** del reticolo.

Simmetrie di un reticolo piano

Vogliamo ora studiare le simmetrie di un reticolo ossia le isometrie che portano il reticolo su se stesso. Contrariamente a quanto accade per le figure limitate, come i poligoni o i poliedri, i reticoli possiedono infinite simmetrie.

Iniziamo dal caso dei reticoli piani. Per le simmetrie di traslazione valgono le seguenti (intuitive) proprietà:

- Ogni reticolo ammette infiniti assi di traslazione: ogni retta che passa per due nodi qualsiasi del reticolo è infatti un possibile asse di traslazione.
- Qualunque asse di traslazione è detto filare del reticolo e la minima distanza tra due nodi lungo un filare è detta periodo di identità del filare stesso.
- In un reticolo tutti i filari tra loro paralleli hanno lo stesso periodo di identità .
- Dato un reticolo, due punti del piano sono detti equivalenti rispetto al reticolo se possono essere ottenuti l'uno dall'altro per traslazione parallela ad un filare del reticolo e la loro distanza è un multiplo del periodo di identità del filare.

Un reticolo può possedere anche simmetrie per rotazione. Gli angoli α delle rotazioni che sono simmetrie di un reticolo ammettono sempre multipli interi $n\alpha$ coincidenti con multipli interi dell'angolo giro. Nel seguito per ordine della rotazione intendiamo il minimo positivo di tali interi n.

- Ciascun nodo del reticolo, o punto medio dei lati, o baricentro di qualunque maglia è il centro di una simmetria rotazionale di ordine 2. Ciò deriva dal fatto che ciascun nodo del reticolo è sempre affiancato, in ogni filare che lo contenga, da due nodi equidistanti.
- Se un punto P del piano è centro di una simmetria rotazionale di ordine n compatibile con un reticolo, allora ogni punto equivalente rispetto al reticolo è anch'esso centro di una simmetria rotazionale di ordine n.

Analoghe proprietà valgono per un reticolo spaziale.

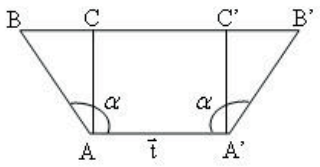
★ La restrizione cristallografica

Sono ben pochi gli angoli di rotazione ammissibili per le simmetrie rotazionali, poiché vale la cosiddetta:

Restrizione cristallografica: in un reticolo bidimensionale, e quindi anche in uno tridimensionale, possono realizzarsi solo simmetrie per rotazione di ordine $n = 1, 2, 3, 4, 6$.

Sia A un centro di una rotazione α di ordine n e sia $\mathbf{t}$ un vettore di traslazione del reticolo, che associa ad A un altro centro di rotazione A' dello stesso ordine.

Ruotando $\mathbf{t}$ rispetto alle due rotazioni di centri A e A' di angoli rispettivamente α e $-\alpha$, individuiamo i punti B e B', dove $\widehat{BAA'} = \widehat{AA'B} = \alpha$ e $\widehat{ABC} = \widehat{A'B'C'} = \pi - \alpha$.



(Ricordiamo che l'insieme delle simmetrie di una figura costituisce un gruppo, quindi se esiste la rotazione α deve anche esistere la rotazione opposta $-\alpha$.)

Poiché B e B' devono essere nodi del reticolo, il segmento BB', parallelo ad AA', deve essere un multiplo intero di $\mathbf{t}$:

$$\overrightarrow{BB'} = m\,\mathbf{t} \text{ con } m \text{ intero} \geq 0.$$

Dalla figura si ricava:

$$\overrightarrow{BB'} = \overrightarrow{BC} + \overrightarrow{AA'} + \overrightarrow{C'B'} \qquad \text{ossia} \qquad m\,\mathbf{t} = \mathbf{t} + 2cos(\pi - \alpha)\mathbf{t}$$

da cui $cos(\alpha) = \frac{1-m}{2}$. Il numero $M = 1 - m$ è intero e $|cos\,\alpha| \leq 1$; quindi i centri di rotazione di ordine 1, 2, 3, 4, 6 sono gli unici compatibili con gli elementi di traslazione del reticolo, come risulta dalla seguente tabella:

M	$cos(\alpha)$	α	n	BB'
2	1	2π	1	$-\mathbf{t}$
1	$\frac{1}{2}$	$\frac{\pi}{3}$	6	0
0	0	$\frac{\pi}{2}$	4	$\mathbf{t}$
-1	$-\frac{1}{2}$	$\frac{2}{3}\pi$	3	$2\mathbf{t}$
-2	-1	π	2	$3\mathbf{t}$

Classificazione dei reticoli piani

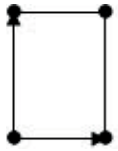
Le simmetrie di un reticolo piano dipendono dalla forma del parallelogramma di base, o **cella elementare**.

Esistono cinque possibili tipi di simmetrie per un reticolo in relazione a cinque forme di celle elementari diverse. Quattro di queste celle vengono dette **primitive**, poiché i parallelogrammi relativi hanno nodi solo ai vertici, mentre la rimanente viene detta **centrata**, poiché, per evidenziare meglio le simmetrie del reticolo, si preferisce scegliere come cella generatrice, invece del parallelogramma individuato dai due vettori generatori, una cella rettangolare, che in questo caso è dotata di un nodo nel suo baricentro.

Se $\mathbf{u}$, $\mathbf{v}$ rappresentano i vettori generatori del reticolo, esse sono:

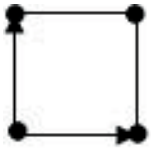
- **Cella Obliqua** (primitiva)
($\mathbf{u}$, $\mathbf{v}$ qualsiasi, ma diversi dai casi seguenti)
Il reticolo presenta solamente simmetrie traslazionali e simmetrie rotazionali di ordine 2.

- **Cella Rettangolare** (primitiva) ($\mathbf{u}$, $\mathbf{v}$ perpendicolari, $|\mathbf{u}| \neq |\mathbf{v}|$)
Il reticolo presenta simmetrie traslazionali, rotazionali di ordine 2 e riflessioni.

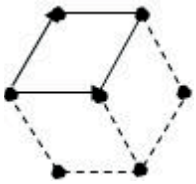


- **Cella Rettangolare centrata** (il triangolo di lati **u**, **v** è isoscele, $|\mathbf{u}| \neq |\mathbf{v}|$)
Il reticolo presenta simmetrie traslazionali, rotazionali di ordine 2, riflessioni e glissoriflessioni.

- **Cella Quadrata** (primitiva) (**u**, **v** perpendicolari, $|\mathbf{u}| = |\mathbf{v}|$)
Il reticolo presenta simmetrie traslazionali, rotazionali di ordine 2 e 4, e riflessioni.



- **Cella Esagonale** (primitiva) (il triangolo di lati **u**, **v** è equilatero)
Il reticolo presenta simmetrie traslazionali, rotazionali di ordine 2, 3 e 6, riflessioni e glissoriflessioni.



Attenzione: la cella esagonale non deve essere considerata come una cella centrata, perché per cella si intende il parallelogramma individuato dai vettori generatori, che non è centrato. Il termine esagonale aiuta semplicemente a ricordare le simmetrie del reticolo.

Sistemi regolari di punti

Definizione 7.14. *Un **sistema regolare di punti** è un insieme di punti ottenuto ripetendo uno stesso insieme di punti, scelto a piacere, lungo i filari di un reticolo ad intervalli uguali al periodo di identità del filare.*

Esempi concreti di sistemi regolari di punti sono le **tassellazioni** o **tappezzerie** del piano e i **cristalli** nello spazio.

Una tassellazione viene ottenuta ripetendo periodicamente una figura senza sovrapposizioni in modo da coprire tutto il piano, mentre un cristallo si ottiene per ripetizione di gruppi di atomi sempre uguali.

Esempi famosi e spettacolari di tassellazioni piane si possono ammirare nelle decorazioni della residenza moresca dell'Alhambra di Granada (XIII e XIV secolo), dove esistono tutti i possibili schemi diversi. Essi furono una ricca e preziosa fonte di ispirazione per l'artista olandese M.C. Escher (1898-1972) che nelle sue opere riuscà ad unire in modo affascinante arte e matematica.

L'interesse di Escher per le tassellazioni inizià infatti nel 1936 quando, durante un soggiorno in Spagna, ebbe l'occasione di visitare il palazzo trecentesco di Granada e di apprezzarne le splendide decorazioni. Però, mentre le figure utilizzate per i mosaici sono forme geometriche, Escher sperimentà le sue particolari tassellazioni applicando rotazioni, traslazioni, riflessioni e glisso-riflessioni ad una grande varietà di figure, quali rettili, uccelli, angeli ed altre forme ancora.

Le tassellazioni sono quindi un ottimo esempio di collaborazione interdisciplinare in cui arte e matematica riescono a rendere visibile l'invisibile!

♣ Esercizi per la settima lezione

7.1 Nel piano, disegnare due vettori linearmente dipendenti e due vettori indipendenti, applicati nell'origine del riferimento cartesiano, specificando le coordinate del secondo estremo dei vari vettori disegnati.

7.2 Disegnare la somma delle due coppie di vettori dell'esercizio precedente, sempre come vettore applicato in O. Scrivere le coordinate del secondo estremo del vettore somma (ci si può aiutare anche con un righello).

7.3 Disegnare 5 vettori non nulli, a due a due linearmente indipendenti, la cui somma sia il vettore nullo.

7.4 Disegnare un vettore $\mathbf{u}$ qualsiasi del piano. Scegliere altri due vettori $\mathbf{v}$ e $\mathbf{w}$ linearmente indipendenti tra loro. Trovare graficamente una combinazione lineare di $\mathbf{v}$ e $\mathbf{w}$ che dia il vettore $\mathbf{u}$.

7.5 Disegnare due vettori $\mathbf{u}$ e $\mathbf{v}$ qualsiasi del piano, che siano linearmente indipendenti. Disegnare quindi i vettori $\mathbf{u} - \mathbf{v}$, $3\mathbf{u} - 2\mathbf{v}$, $\mathbf{v} - \mathbf{u}$ e $3\mathbf{v} - 2\mathbf{u}$.

7.6 Disegnare il traslato del punto $P = (1, -1)$ mediante la traslazione τ di vettore parallelo all'asse x, verso positivo e lunghezza 2.

Disegnare il traslato del punto $P = (1, -1)$ mediante la traslazione σ di vettore parallelo all'asse y, verso positivo e lunghezza 1.

7.7 Con i dati dell'esercizio precedente, disegnare il trasformato del punto P mediante l'isometria ottenuta componendo le traslazioni τ e σ (prima τ e poi σ). Disegnare il trasformato di P rispetto alla composizione $\sigma \circ \tau$ (prima σ e poi τ). Verificare che si ha $\sigma \circ \tau = \tau \circ \sigma$ e che si tratta ancora di una traslazione, determinando anche il vettore di traslazione.

7.8 Verificare in un esempio concreto che la composizione di due riflessioni di assi paralleli (non coincidenti) è una traslazione, scegliendo due rette distinte, parallele ad uno degli assi x o y e scrivendo il trasformato P' di un punto $P = (x_0, y_0)$ mediante la riflessione rispetto alla prima retta e poi il trasformato P'' di P' mediante la riflessione rispetto alla seconda retta.

7.9 Disegnare alcuni punti del reticolo generato dai vettori $\mathbf{x}$ parallelo all'asse x, con verso positivo e lunghezza 3 e $\mathbf{d}$ parallelo alla retta $y = x$, con verso N-E (ossia orientato verso l'alto) e lunghezza 1.

Disegnare una cella elementare associata a tale reticolo.

Evidenziare alcuni elementi di simmetria per ogni tipo di simmetria posseduta.

7.10 Svolgere l'esercizio precedente relativamente al reticolo generato dai vettori $\mathbf{x}$ parallelo all'asse x, con verso positivo e lunghezza 2 e $\mathbf{d}$ parallelo alla retta $y = x$, con verso N-E e lunghezza $\sqrt{2}$.

Svolgere l'esercizio precedente relativamente al reticolo generato dai vettori $\mathbf{x}$ parallelo all'asse x, con verso positivo e lunghezza 2 e $\mathbf{d}$ parallelo alla retta $y = \sqrt{3}x$, con verso N-E (ossia orientato verso l'alto) e lunghezza 1.

7.11 Disegnare un reticolo del piano, individuando in particolare due vettori generatori. Tracciare almeno 5 filari non paralleli.

7.12 Disegnare un sistema regolare di punti associato a ciascuno dei cinque tipi di reticoli.

7.13 Trovare eventuali simmetrie dei vari sistemi regolari di punti disegnati.

7.14 Costruire una o piò tassellazioni del piano. Studiare le eventuali simmetrie di tali tassellazioni.

Lezione 8

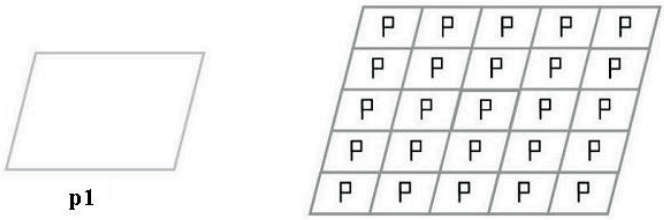
Simmetrie, Decorazioni e Cristalli

Tassellazioni

I gruppi associati agli insiemi delle simmetrie delle tassellazioni del piano sono 17.

I gruppi più semplici sono quelli contenenti solo operazioni di rotazione e di traslazione. Vengono denotati, nella notazione cristallografica, dalla lettera p seguita dal numero n, dove p significa che la cella elementare del reticolo associato alla tassellazione è primitiva e n indica l'ordine massimo delle simmetrie rotazionali.

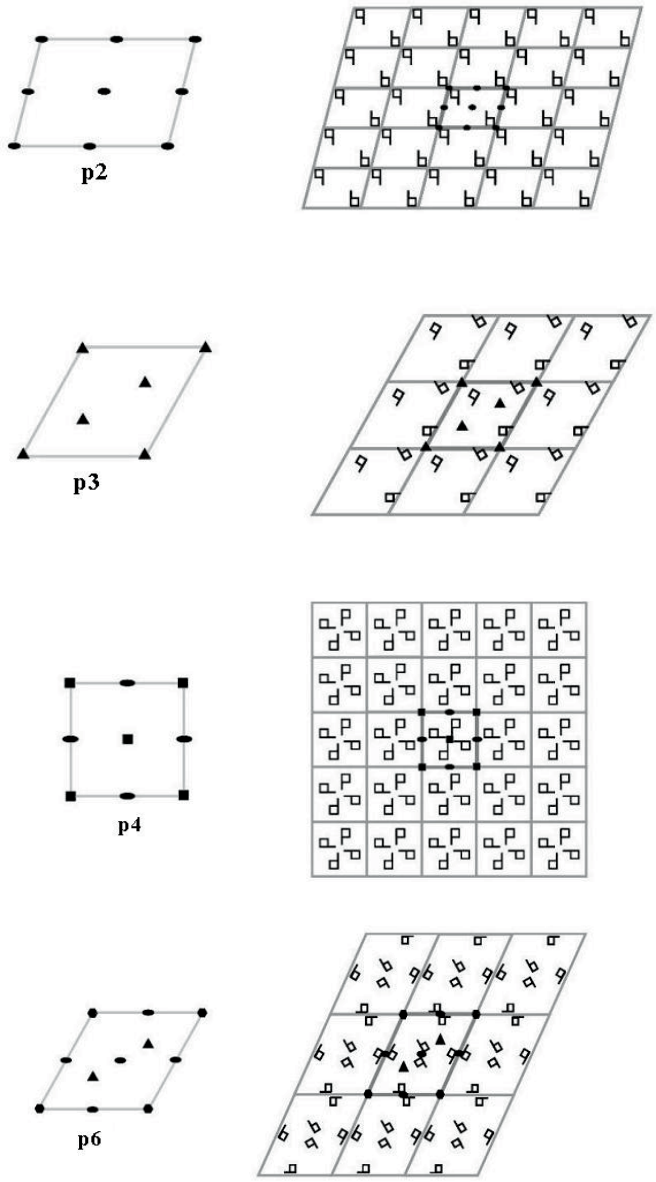
Nel gruppo spaziale **p1** è presente la sola rotazione identica e quindi un punto viene ripetuto soltanto dai vettori traslatori del reticolo. Le uniche simmetrie sono dunque traslazionali.



(I simboli di ovale, triangolo, quadrato ed esagono che compaiono nelle celle elementari associate alle tappezzerie raffigurate di seguito stanno ad

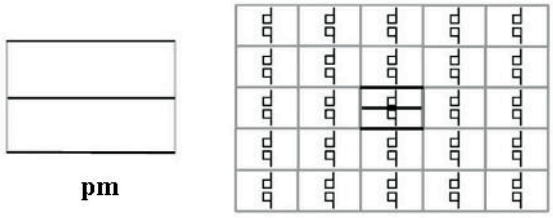
indicare centri di rotazione di ordine 2, 3, 4, 6 rispettivamente, le linee continue indicano assi di riflessione e quelle tratteggiate assi di glissoriflessione.)

Nei gruppi **p2**, **p3**, **p4**, **p6**, oltre ad elementi di simmetria di traslazione vi sono punti di rotazione di ordine 2, 3, 4, 6. Ecco un esempio di tappezzeria per ciascuno di questi tre gruppi:

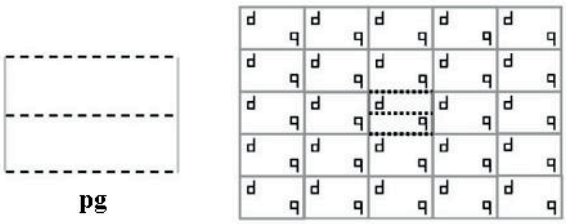


Consideriamo ora i gruppi contenenti operazioni di riflessione rispetto ad una retta.

Tra questi i più semplici sono i due gruppi di simmetrie di una tappezzeria associata ad un reticolo rettangolare dotata di una simmetria di riflessione m oppure di una simmetria di glissoriflessione (detta anche riflessione con scorrimento) g, che vengono rispettivamente indicati con i simboli **pm** e **pg**.

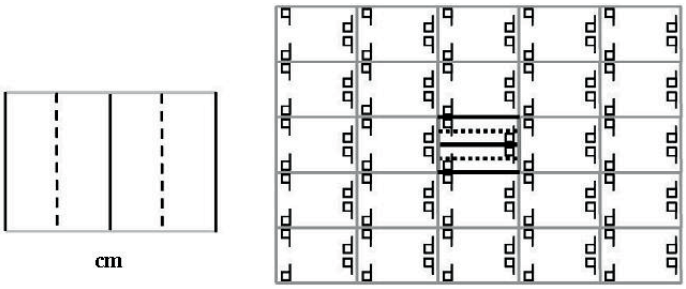


pm



pg

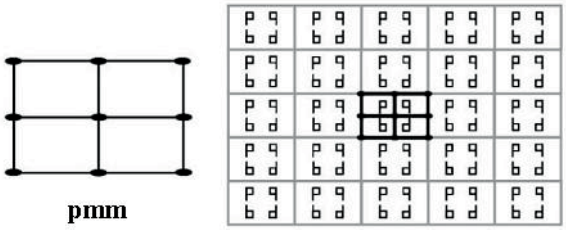
Se invece consideriamo una tappezzeria associata ad una cella rettangolare centrata dotata di una simmetria di riflessione m, si ottiene il gruppo **cm**.



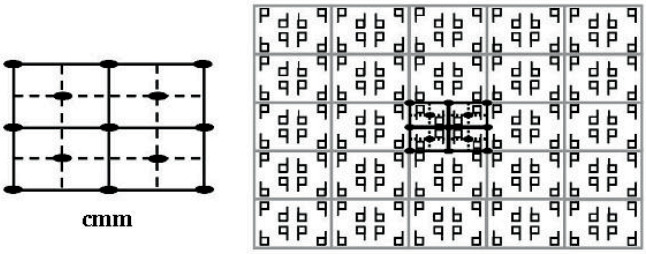
cm

Se la tappezzeria associata al reticolo con cella rettangolare centrata fosse stata dotata di una simmetria di riflessione con scorrimento g, si sarebbe ottenuto lo stesso gruppo di simmetrie. Quindi il gruppo cg coincide con il gruppo cm.

Una tappezzeria associata ad un reticolo rettangolare primitivo o ad uno centrato può possedere oltre alla simmetria di riflessione o di glissoriflessione del punto precedente, una ulteriore simmetria di riflessione m ortogonale alle precedenti, ottenendo così i gruppi **pmm** e **cmm**.

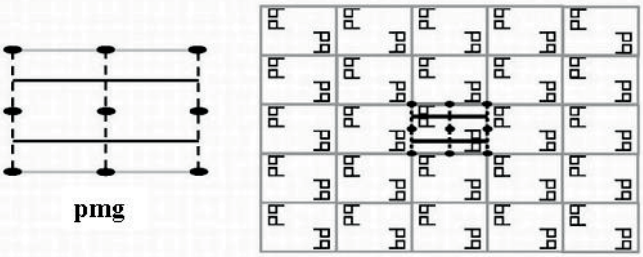


pmm

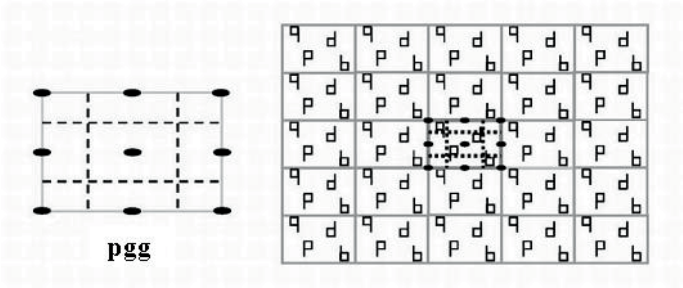


cmm

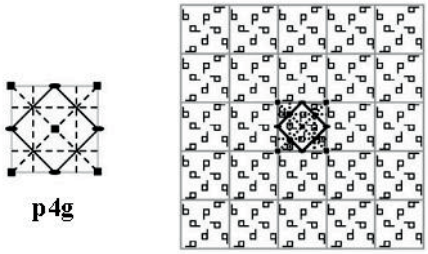
Se si considera poi la possibilità della presenza di simmetrie di riflessione con scorrimento g al posto si quelle di riflessione m si ricavano due ulteriori gruppi spaziali: **pmg** e **pgg**, mentre i gruppi *cmg* e *cgg* sono equivalenti al gruppo *cmm*.

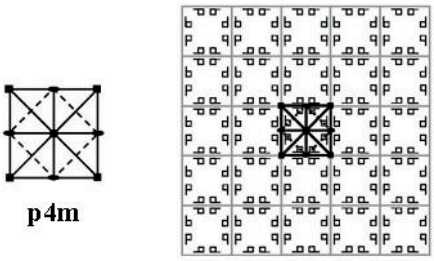


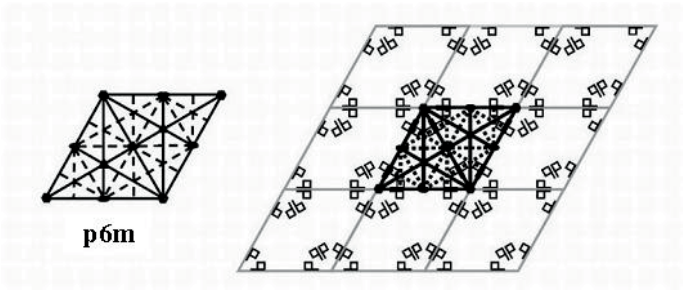
pmg

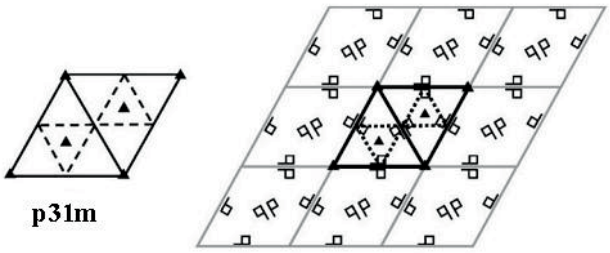


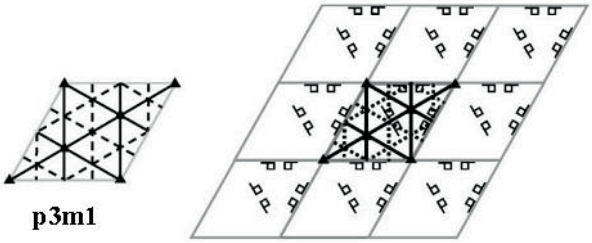
Nei rimanenti gruppi **p4g**, **p4m**, **p6m**, **p31m**, **p3m1** le simmetrie di riflessione m o g vengono associate a rotazione di ordine 3, 4, 6.











Un bell'esempio di simmetria di glissoriflessione è dato dal Pozzo di S. Patrizio.

Pozzo di San Patrizio (Orvieto, 1527) Profondità 62 m,
248 gradini, 72 finestroni.

Classificazione delle isometrie dello spazio

Nello spazio i tipi possibili di isometrie si riducono ai seguenti casi *(Eulero, 1776)*:

- **riflessioni** (rispetto ad un piano);
- **rotazioni**;
- **traslazioni**;
- **glissoriflessioni** (ossia le composizioni di una riflessione con una traslazione in una direzione parallela al piano di simmetria della riflessione);
- **glissorotazioni** (ossia le composizioni di una rotazione con una traslazione parallela all'asse di rotazione);
- **riflessioni rotatorie** (ossia le composizioni di una rotazione con la riflessione rispetto a un piano perpendicolare all'asse di rotazione).

Per prendere confidenza con le isometrie dello spazio consideriamo gli elementi di simmetria di: cubo, tetraedro, ottaedro regolari.

CUBO: 3 assi di rotazione di ordine 4 passanti per i centri di due facce opposte, 4 assi di ordine 3 per due vertici opposti, 6 assi di ordine 2 per i punti medi di due spigoli opposti, 9 piani di riflessione, 1 centro di simmetria.

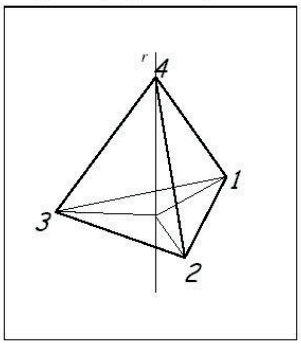
OTTAEDRO: 4 assi di rotazione di ordine 3 per i centri di due facce opposte, 3 assi di ordine 4 per due vertici opposti, 6 assi di ordine 2 per i punti medi di due spigoli opposti, 9 piani di riflessione, 1 centro di simmetria.

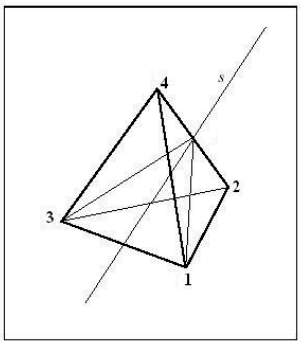
TETRAEDRO: 4 assi di rotazione di ordine 3 per un vertice ed il centro della faccia opposta, 3 assi di ordine 2 per i punti medi di due spigoli opposti, 6 piani di riflessione.

Osservazione: cubo e ottaedro regolare hanno gli stessi elementi di simmetria e quindi gli stessi gruppi di simmetrie.

Esempio 8.1. *Il gruppo delle simmetrie del tetraedro regolare è* S_4. *É sufficiente provare che il gruppo delle simmetrie del tetraedro possiede 24 elementi.*

Considerando i soli elementi di simmetria del tetraedro, otteniamo: 4 rotazioni di 120°*, 4 di* 240°*, 3 rotazioni di* 180°*, 6 riflessioni e l'identità; in totale 18 elementi.*





Ricordiamo ora il Teorema di Lagrange che afferma che l'ordine di ogni sottogruppo di un gruppo finito divide l'ordine del gruppo. Poiché 18 non divide 24 e il più piccolo divisore di 24 maggiore di 18 è 24 stesso, vi devono essere altre 6 *simmetrie oltre a quelle elencate.*

Le 6 simmetrie mancanti sono riflessioni rotatorie, più precisamente le riflessioni rotatorie che si ottengono componendo una rotazione di 90° *(in un verso o nell'altro, quindi due rotazioni possibili) attorno ad uno dei tre assi di rotazione di ordine 2, con una riflessione rispetto al piano passante per il baricentro del tetraedro e perpendicolare all'asse di rotazione. Tre assi per due versi di rotazione ci danno le 6 simmetrie mancanti.*

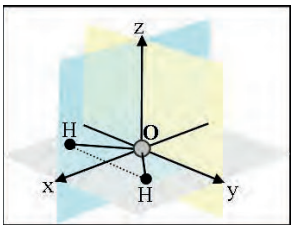
Se consideriamo solamente le simmetrie del tetraedro che otteniamo mediante rotazioni, esse sono esattamente 12 e corrispondono al sottogruppo delle permutazioni pari di S_4*, che si denota con* A_4*.*

Per permutazione pari si intende una permutazione che possa essere ottenuta con un numero pari di scambi successivi. Come già visto, ogni permutazione può essere ottenuta mediante una successione finita di scambi. Sebbene il numero di scambi necessari per ottenere una data permutazione σ non sia univocamente determinato, tuttavia si può provare che, fissata σ, tale numero è sempre pari oppure sempre dispari.

Le simmetrie della molecola dell'acqua. Anche alcune molecole hanno una struttura che presenta simmetrie spaziali facilmente riconoscibili, associate a gruppi di cui non è difficile scrivere la tabella delle operazioni . Consideriamo per esempio la molecola dell'acqua H_2O . Immaginiamo di aver fissato nello spazio un sistema di coordinate , con assi tra loro perpendicolari x, y, z. L'insieme delle simmetrie della molecola dell'acqua è formato dagli elementi seguenti:

- l' identità e;
- la rotazione r di ampiezza π attorno all'asse x;

- la riflessione s_1 rispetto al piano xz;
- la riflessione s_2 rispetto al piano xy.



Rappresentazione della molecola dell'acqua.

La struttura di gruppo (rispetto alla "composizione") è descritta dalla tabella seguente

$\star$	e	r	s_1	s_2
e	e	r	s_1	s_2
r	r	e	s_2	s_1
s_1	s_1	s_2	e	r
s_2	s_2	s_1	r	e

★ I Cristalli

Sembra che le forze che hanno modellato il cristallo siano dotate di una propria volontà di ordine, di simmetria, e questa constatazione è stupefacente in quanto riferita alla materia inanimata; essa eccita la curiosità scientifica, che più o meno è in tutti noi, fa nascere il desiderio di fornire una spiegazione persuasiva.
I cristalli raramente crescono isolati, molto spesso si sviluppano gli uni vicino agli altri con disposizioni casuali, formando dei raggruppamenti. In alcuni casi invece essi crescono seguendo particolari leggi: si hanno allora associazioni che apparentemente sembrano un unico cristallo ma che invece sono un insieme di due o più cristalli uniti in maniera simmetrica.
Questi cristalli, detti geminati, rappresentano l'unione di individui cristallini compenetrati o l'unione di individui con una superficie piana in comune.
I cristalli geminati, in molti casi, con la forma assunta simulano l'appartenenza a una classe di simmetria superiore rispetto alla propria, e quindi una forma più regolare, quasi come se nella materia non vivente esistesse una vanità che sappiamo propria degli esseri viventi.

Da: http://www.comune.pisa.it/gruppogeomineralogico/cristalli.htm

Un cristallo è una porzione di materia solida ed omogenea di forma poliedrica, ossia un solido geometrico avente facce, spigoli e vertici in numero e disposizione dipendenti dalla natura chimica della sostanza che costituisce

il cristallo e dalle condizioni di crescita. Facce e spigoli sono paralleli a piani e direzioni (filari) del reticolo.

La formazione di un cristallo è legata al verificarsi di determinate condizioni che, attraverso una serie di reazioni chimico-fisiche, permettono ad atomi inizialmente disordinati di organizzarsi e distribuirsi in modo regolare ed omogeneo.

I cristalli si possono infatti ottenere da una soluzione per evaporazione del solvente, da un materiale solido sottoposto a particolari condizioni di temperatura e pressione, in seguito ad una reazione chimica, o da un fuso per raffreddamento.

Quest'ultimo è il processo di formazione che produce cristalli durante le fasi di consolidamento del magma. Se il magma si raffredda lentamente (per es. perché racchiuso tra rocce preesistenti) si possono sviluppare cristalli facilmente distinguibili (es. granito); se il raffreddamento è veloce, perché il magma è a contatto dell'atmosfera o l'acqua, si formano solo cristalli difficilmente visibili ad occhio nudo (es. basalto) o addirittura non si ha cristallizzazione, ma si forma un solido amorfo o vetroso (es. ossidiana). La lentezza di raffreddamento e la progressiva liberazione degli elementi volatili permettono la formazione di belle cristallizzazioni sovente tappezzanti cavità dette druse.

I cristalli si formano per crescita graduale da piccolissimi elementi cristallini (germi cristallini), invisibili anche ai più forti ingrandimenti microscopici, attraverso una successiva deposizione di materia che consente loro di raggiungere talvolta dimensioni notevoli, anche diversi metri, come in certi quarzi.

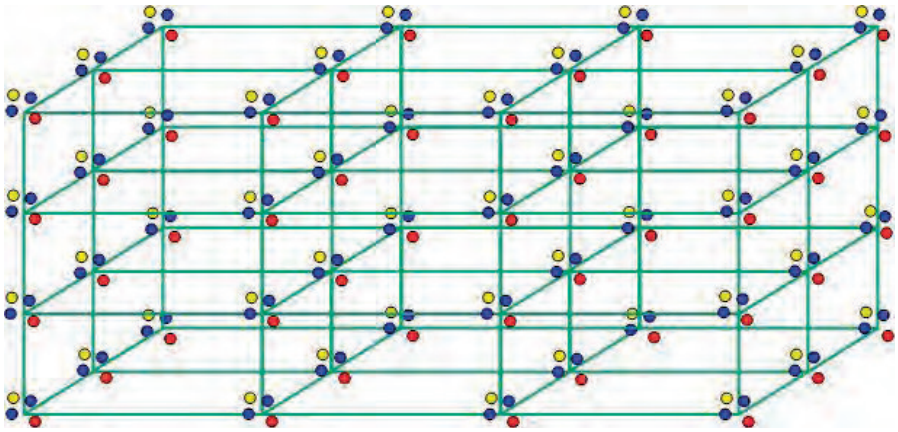
Se un minerale può accrescersi senza resistenze esterne si sviluppa in cristalli singoli, assumendo una determinata forma geometrica, il cosiddetto abito cristallino. Se invece la crescita è ostacolata dallo sviluppo contemporaneo di altri cristalli, ed è il caso più frequente, ne risulta una massa microcristallina e diventa impossibile riconoscere l'abito cristallino senza l'uso di opportuni strumenti (es. microscopia elettronica).

In alcuni casi, più cristalli si accrescono seguendo particolari leggi e si hanno allora associazioni che apparentemente sembrano un unico cristallo, ma che in realtà sono un insieme di due o più cristalli uniti in modo simmetrico. Vengono detti geminati e rappresentano l'unione di individui cristallini compenetrati o aventi una superficie piana in comune.

Inoltre ogni cambiamento delle condizioni ambientali, quali variazioni di temperatura e pressione, può interrompere tale crescita o modificare la struttura dei cristalli.

Comunque, anche se una sostanza di natura cristallina non sempre mostra esteriormente una forma geometrica riconoscibile, possiede ugualmente le caratteristiche del cristallo, in quanto è dotata di una struttura interna, a livello atomico, regolare ed ordinata.

Una **struttura cristallina** è un insieme regolare di atomi che si può ottenere traslando periodicamente lungo tre direzioni non complanari uno stesso insieme di atomi.
Il reticolo associato alla struttura cristallina è detto **reticolo cristallino**.



Nel 1848 **Bravais** scoprì che, a seconda del tipo di simmetrie, esistono 14 tipi diversi di reticoli cristallini, ognuno caratterizzato da una particolare cella elementare. Per rendere più evidente la simmetria del reticolo, invece di utilizzare le 14 celle elementari associate a ciascuno di essi, Bravais, analogamente al caso piano, preferì servirsi di 7 celle elementari, che vengono dette primitive (cioè prive di nodi del reticolo al di fuori dei vertici del parallelepipedo di base), e 7 celle centrate, ottenute dalle 7 primitive aggiungendo opportunamente un nodo nei punti medi degli spigoli o nei baricentri delle facce o della cella stessa).

In base alla forma della cella primitiva associata al reticolo cristallino, i cristalli vengono suddivisi quindi in 7 sistemi cristallini: **triclino**, **monoclino**, **ortorombico**, **tetragonale**, **esagonale**, **trigonale**, **cubico**.

I rapporti tra le dimensioni (parametri) della cella primitiva a, b, c e gli angoli α, β, γ formati da tre spigoli non complanari, sono caratteristici di ogni sostanza cristallina e vengono denominati **costanti cristallografiche**.

La tabella seguente sintetizza i vari tipi di reticoli cristallini. A questo riguardo notiamo che

- Le direzioni degli assi x, y, z rappresentano le direzioni dei vettori generatori del reticolo.

- Il sistema trigonale e quello esagonale vengono spesso considerati come un unico sistema, poiché hanno le stesse costanti cristallografiche. Il numero totale di sistemi in questo caso scende a 6.

- La cella elementare del sistema trigonale viene rappresentata nei due modi raffigurati. La cella a destra, detta romboedrica, si ottiene dalla cella di sinistra considerando come vettori base della cella le congiungenti il nodo sull'asse z (diverso da O) con i due nodi sugli assi x e y (diversi da O) e con il nodo sul piano xy che forma un triangolo equilatero di baricentro O con gli altri due nodi. La cella romboedrica è spesso preferita perché mette chiaramente in evidenza la simmetria rotazionale di ordine 3 del reticolo associato. Per lo stesso motivo la cella elementare del reticolo esagonale viene generalmente rappresentata da un prisma a base esagonale, che mette bene in evidenza la simmetria rotazionale di ordine 6 del reticolo associato.

Una struttura cristallina dunque si ottiene da un reticolo, sostituendo ad ogni punto, o nodo, del reticolo un particolare insieme di atomi che la caratterizza ed è pertanto un sistema regolare di punti (o atomi).

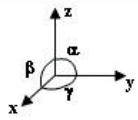
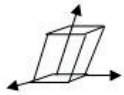
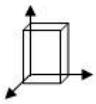
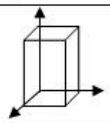
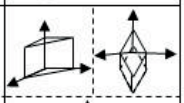
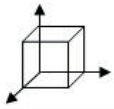
Un cristallo è una parte limitata di una struttura cristallina, le cui facce sono parallele ai piani reticolari, cioè a piani che passano per i nodi del reticolo. Le forme dei cristalli sono classificate in base alle loro simmetrie. La matematica, grazie alla teoria dei gruppi, ha provato che esistono 32 tipi diversi di simmetrie, compatibili con un oggetto finito che sia parte di una struttura cristallina (gruppi puntuali). In particolare osserviamo che tra le simmetrie di una struttura finita non possono esserci traslazioni, per lo stesso motivo per cui non abbiamo trovato traslazioni tra le simmetrie di un triangolo o di un quadrato.

I cristalli vengono quindi suddivisi in 32 classi, una per ogni tipo, o gruppo, di simmetrie. Se invece consideriamo le simmetrie delle strutture cristalline infinite, il numero di possibili simmetrie aumenta di molto, grazie al fatto che le traslazioni sono simmetrie compatibili con tali strutture. I matematici ed i cristallografi hanno provato e verificato sperimentalmente che, per una struttura cristallina, esistono ben 230 tipi o gruppi diversi di simmetrie (gruppi spaziali).

⊡ Attività al computer

Per costruire tassellazioni o sistemi regolari di punti è possibile utilizzare il software Kali reperibile liberamente all'indirizzo:

Figura 1. I sistemi cristallini

Sistema	*Costanti cristallografiche*	*Esempi di cristalli*	
triclino	$\alpha \neq \beta \neq \gamma \neq 90°$ a : b : c	**albite, cianite,...**	
monoclino	$\alpha \neq 90°$ $\beta = \gamma = 90°$ a : b : c	**ortoclasio, gesso, diopside,...**	
ortorombico	$\alpha = \beta = \gamma = 90°$ a : b : c	**topazio, zolfo, aragonite,...**	
tetragonale	$\alpha = \beta = \gamma = 90°$ a : a : c	**zircone, wulfenite,...**	
trigonale	$\alpha = \beta = 90°$ $\gamma = 120°$ a : a : c	**calcite, quarzo,...**	
esagonale		**grafite, zincite,...**	
cubico	$\alpha = \beta = \gamma = 90°$ a : a : a	**pirite, magnetite, salgemma,...**	

http://geometrygames.org/Kali/

Si può utilizzare il fotoricettore per disegnare tapezzerie. Dopo aver stampato un disegno si possono individuare alcuni elementi di simmetria. L'attività può anche essere svolta sotto forma di gioco, eventualmente a squadre.

Ulteriori siti utili sull'argomento sono:

http://specchi.mat.unimi.it/

Sul sito:

http://www.sciences.univ-nantes.fr/sites/genevieve_tulloue/Cristallo/Index_Cristallo.html

si trovano animazioni che illustrano le simmetrie dei vari sistemi cristallini.

Sul sito:

http://www.sciences.univ-nantes.fr/sites/genevieve tulloue/Polyedres/Platon/Index_Platon.html

si trovano animazioni che illustrano i poliedri platonici e quelli archimedei.

Sempre sui poliedri visitare:

http://www.georgehart.com/virtual-polyhedra/vp.html

Alcuni siti web interessanti sui cristalli:

http://www.comune.pisa.it/gruppogeomineralogico/cristalli.htm#inizio

http://jcrystal.com/steffenweber/

http://en.wikipedia.org/wiki/Crystallography

http://en.wikipedia.org/wiki/Crystal

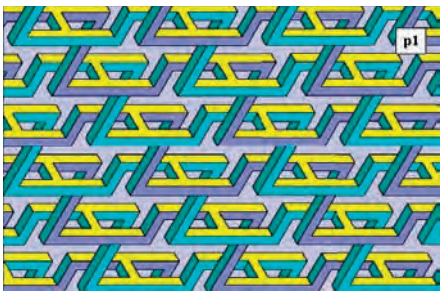
http://academic.brooklyn.cuny.edu/geology/leveson/core/graphics/crystals/crystals_cause.html

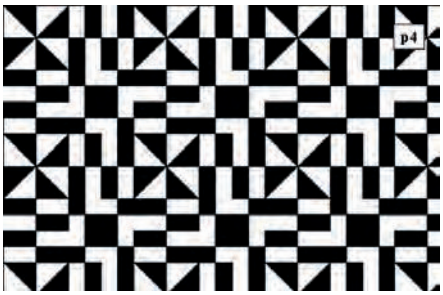
Nel 2014 in tutto il mondo verrà celebrato l'Anno Internazionale della Cristallografia:

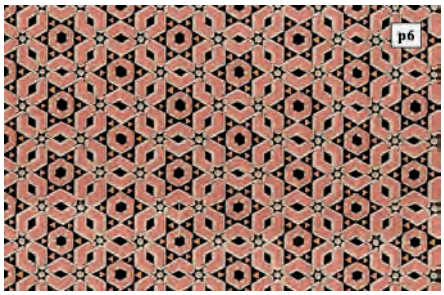
http://www.iycr2014.it/

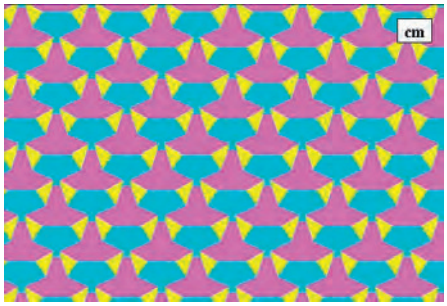
♣ Esercizi per l'ottava lezione

8.1 Verificare che le seguenti tassellazioni appartengono al gruppo delle simmetrie indicato:

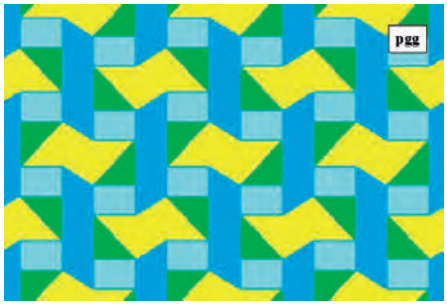


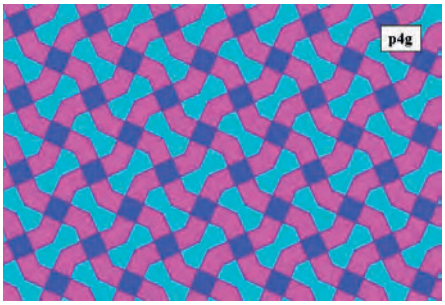




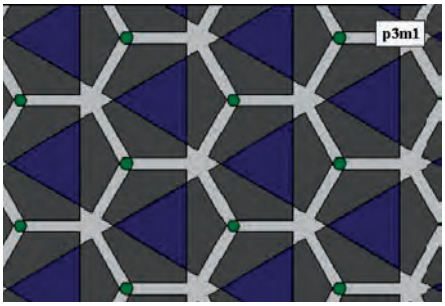

cm

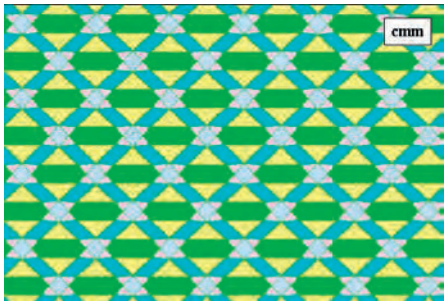

pmg

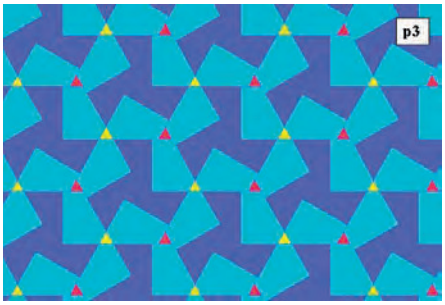

pgg

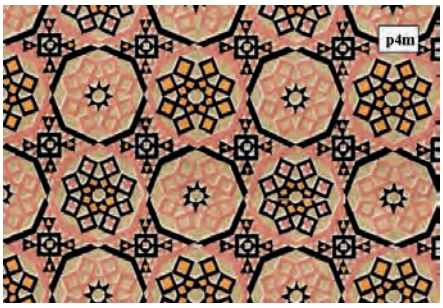

p4g

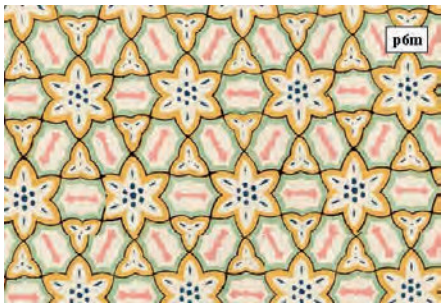

p31m

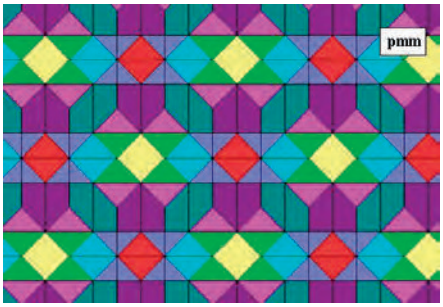

p3m1

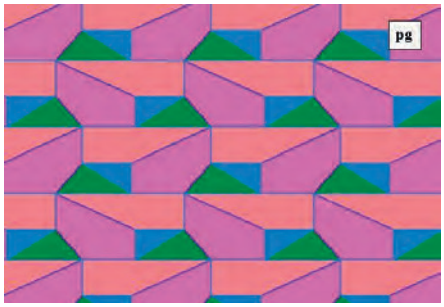

cmm

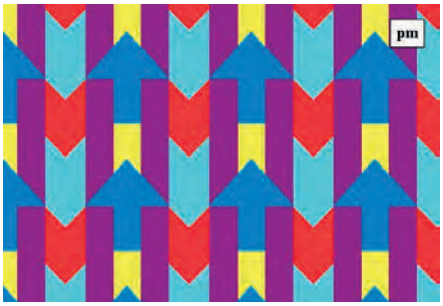

p3


p4m


p6m

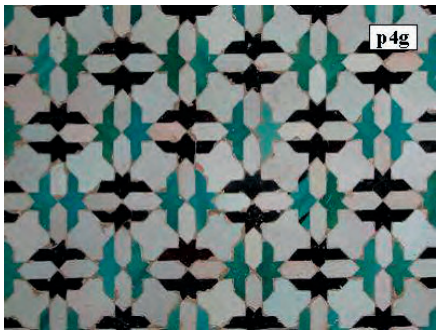

pmm

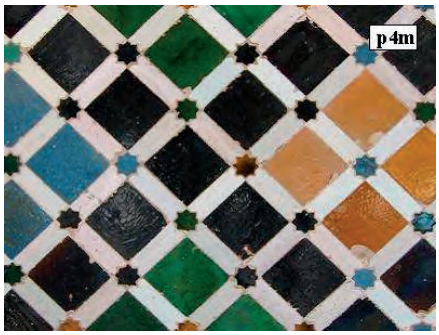

pg

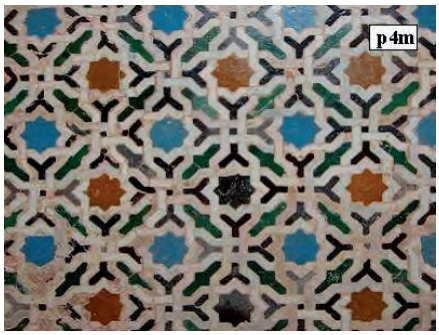

pm

8.2 Trovare il gruppo delle simmetrie dell'ultima tassellazione della figura dell'Esercizio 8.1.

8.3 Verificare che le seguenti tassellazioni che riproducono alcuni dei bellissimi mosaici dell'Alhambra (Granada, Spagna) appartengono al gruppo delle simmetrie indicato:







8.4 Individuare gli elementi di simmetria di una piramide retta a base quadrata.

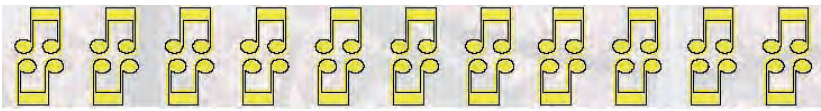
8.5 Verificare che i gruppi delle simmetrie delle seguenti "cornicette infinite" hanno le caratteristiche indicate:

Contiene solo traslazioni

Contiene traslazioni e glissoriflessioni.

Contiene traslazioni e riflessioni di asse verticale.

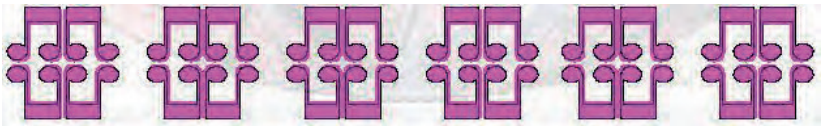
Contiene traslazioni e rotazioni di 180°.



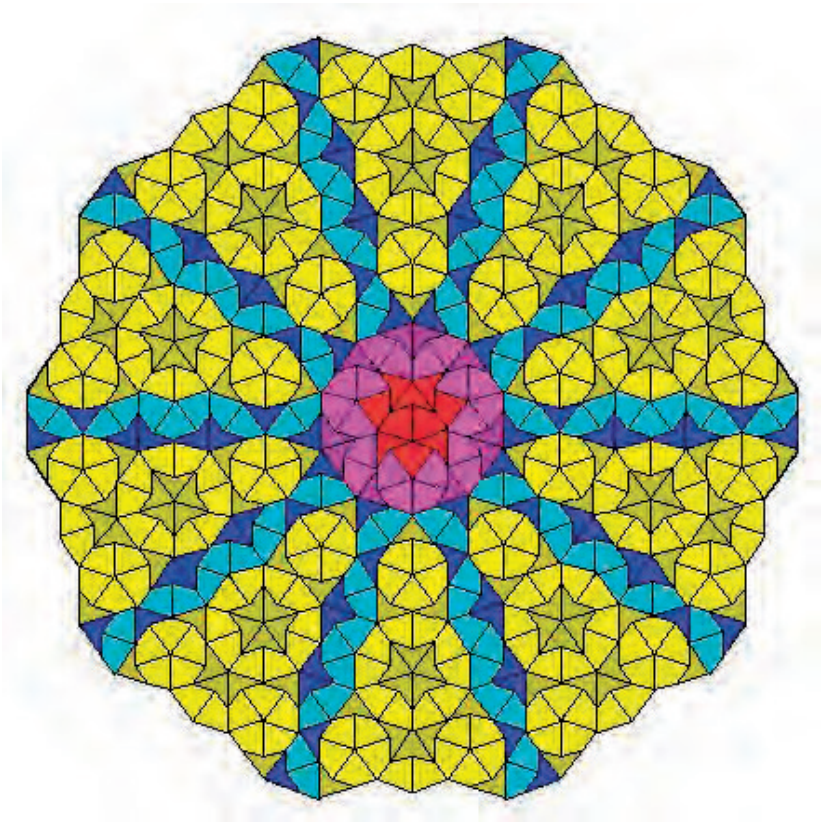
Contiene traslazioni, glissoriflessioni e rotazioni di 180°.

Contiene traslazioni e riflessioni di asse orizzontale.

Contiene traslazioni e riflessioni verticali e orizzontali.



8.6 Quali simmetrie possiede la seguente "tassellazione" di Penrose?
(In proposito si veda anche il sito:
http://www.uwgb.edu/dutchs/symmetry/penrose.htm)



Modulo 5

Le matrici

Lezione 9

Matrici e operazioni

Vettori del piano in componenti.

Considerando il solito riferimento cartesiano ortogonale monometrico del piano, possiamo individuare un vettore mediante una coppia di numeri, esattamente come un punto del piano viene univocamente individuato da una coppia di numeri. Per evitare il rischio di confusione, per indicare un punto P scriveremo la coppia di numeri tra parentesi tonde e separati da una virgola, ossia $P = (x, y)$, mentre per indicare un vettore $\mathbf{v}$, scriveremo la coppia di numeri in verticale, ossia $\binom{a}{b}$ oppure in orizzontale, ma senza la virgola in mezzo: $(a\ b)$.

Definizione 9.1. *$\boldsymbol{v} = \binom{a}{b}$ oppure $\boldsymbol{v} = (a\ b)$ individua il vettore $\boldsymbol{v} = a\boldsymbol{i} + b\boldsymbol{j}$, dove $\boldsymbol{i}$ indica il vettore parallelo all'asse x, di verso positivo e lunghezza 1, e $\boldsymbol{j}$ indica il vettore parallelo all'asse y, di verso positivo e lunghezza 1. I numeri a e b vengono detti **componenti** del vettore $\boldsymbol{v}$.*

In altri termini le componenti di $\mathbf{v} = \binom{a}{b}$ coincidono con le coordinate del punto P tale che $\mathbf{v} = P - O$. Ricordiamo, infatti, che un qualsiasi vettore del piano ammette come rappresentante una freccia del piano applicata in O, quindi le componenti di un vettore $\mathbf{v}$ non sono nient'altro che le coordinate dell'estremo di tale freccia diverso da O. Il vettore nullo $\mathbf{0}$ ha per definizione componenti nulle e viene denotato scrivendo $\binom{0}{0}$ oppure $(0\ 0)$.

Un risultato estremamente importante ma di facile verifica è che il vettore $\overrightarrow{P_1P_2}$, rappresentato dalla freccia che parte da $P_1 = (x_1, y_1)$ ed arriva in $P_2 = (x_2, y_2)$, ha componenti $x_2 - x_1$ e $y_2 - y_1$, pertanto $\overrightarrow{P_1P_2} = (x_2 - x_1\ \ y_2 - y_1)$. Questo giustifica il fatto di aver denotato con $P_2 - P_1$ tale vettore.

Attenzione: il vettore $\overrightarrow{P_2P_1}$ ha componenti $x_1 - x_2$ e $y_1 - y_2$ ed è pertanto uguale al vettore $P_1 - P_2$.

Le componenti di un vettore sono particolarmente comode per calcolare le componenti di un vettore ottenuto sommando altri due vettori, o moltiplicando un vettore per un numero.

Infatti si può verificare che per ogni coppia di vettori $\mathbf{v} = \binom{a}{b}$, $\mathbf{w} = \binom{c}{d}$ e per ogni $\lambda \in \mathbb{R}$ si ha:

$$\mathbf{v} + \mathbf{w} = \begin{pmatrix} a+c \\ b+d \end{pmatrix} \quad \text{e} \quad \lambda\mathbf{v} = \begin{pmatrix} \lambda a \\ \lambda b \end{pmatrix}.$$

In particolare, se $\mathbf{v} = \binom{a}{b}$ allora $-\mathbf{v} = \binom{-a}{-b}$.

Altrettanto utile e semplice è il modo di calcolare la **lunghezza di un vettore** $\mathbf{v}$, detta anche **modulo** di $\mathbf{v}$, che indicheremo con il simbolo $|\mathbf{v}|$, a partire dalle componenti $\binom{a}{b}$; grazie al ben noto **teorema di Pitagora** si ha infatti:

$$|\mathbf{v}| = \sqrt{a^2 + b^2}.$$

Se $\mathbf{v} = \overrightarrow{P_1P_2} = (x_2 - x_1 \;\; y_2 - y_1)$, la distanza tra i punti P_1 e P_2 è data dalla formula:

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Introduciamo ora una nuova operazione tra vettori, detta **prodotto scalare**, la quale associa a due vettori un numero e che risulta estremamente utile per le applicazioni.

Definizione 9.2. *Dati due vettori $\boldsymbol{v} = \binom{a}{b}$, $\boldsymbol{w} = \binom{c}{d}$, il prodotto scalare $\boldsymbol{v} \cdot \boldsymbol{w}$ di $\boldsymbol{v}$ e $\boldsymbol{w}$ è il numero $ac + bd$, che si ottiene moltiplicando "**riga per colonna**" le componenti di $\boldsymbol{v}$ e $\boldsymbol{w}$, scrivendo le prime in riga e le seconde in colonna. In simboli $\boldsymbol{v} \cdot \boldsymbol{w} = (a \;\; b)\binom{c}{d} = ac + bd$.*

Osservazione 9.3. Moltiplicare riga per colonna significa moltiplicare il primo elemento della riga per il primo elemento della colonna e sommare tale prodotto col prodotto del secondo elemento della riga per il secondo elemento della colonna.

Attenzione: noi utilizzeremo sempre il prodotto riga per colonna, ma potrebbe essere utilizzato ugualmente il prodotto colonna per riga. Come vedremo in seguito la differenza è però sostanziale.

Proprietà 9.4. *Se α è l'angolo ($\leq 180^o$) formato da due vettori $\boldsymbol{v}$ e $\boldsymbol{w}$, allora:*

$$\boldsymbol{v} \cdot \boldsymbol{w} = |\boldsymbol{v}||\boldsymbol{w}| cos(\alpha)$$

e quindi:

$$cos(\alpha) = \frac{\boldsymbol{v} \cdot \boldsymbol{w}}{|\boldsymbol{v}||\boldsymbol{w}|}.$$

Dunque conoscendo le componenti di due vettori è possibile calcolare l'angolo da essi formato!

Corollario 9.5. *Due vettori $\boldsymbol{v}$ e $\boldsymbol{w}$, non nulli, sono perpendicolari se e solo se $\boldsymbol{v} \cdot \boldsymbol{w} = 0$.*

Spesso la lunghezza di un vettore viene indicata come $|\mathbf{v}| = \sqrt{\mathbf{v}\cdot\mathbf{v}} = \sqrt{\mathbf{v}^2}$, ciò è giustificato dal fatto che, se $\mathbf{v} = (a, b)$, allora $\mathbf{v}\cdot\mathbf{v} = a^2 + b^2$ e $|\mathbf{v}| = \sqrt{a^2 + b^2}$.

Introduciamo ora uno strumento nuovo, detto matrice, che generalizza il concetto di componenti di un vettore e che ci permetterà di velocizzare e semplificare in seguito i nostri calcoli.

Le matrici

Chiamiamo **matrici** delle tabelle finite di elementi di un insieme $\mathcal{N}$ (in genere, ma non sempre, un insieme di numeri) posti su 'righe e colonne'. Nel seguito, fino a diverso avviso $\mathcal{N} = \mathbb{R}$ sarà sottinteso.

Esempio 9.6. $\begin{pmatrix} 1 & 3 & -2 \\ 0 & \pi & 5 \end{pmatrix}$ *è una matrice 2 righe e 3 colonne, brevemente* 2×3, *ad elementi in* $\mathbb{R}$.

Esempio 9.7. *La scrittura in componenti* $(a\ b)$ *di un vettore* $\boldsymbol{v}$ *costituisce una matrice "riga"* 1×2, *mentre la scrittura dello stesso vettore nella forma* $\binom{a}{b}$ *costituisce una matrice "colonna"* 2×1.

Generalizzando questa situazione chiameremo ***vettore riga*** *ogni matrice con una sola riga di qualsiasi lunghezza e, analogamente, chiameremo* ***vettore colonna*** *ogni matrice con una sola colonna di qualsiasi lunghezza.*

$\mathcal{M}_{m,n}$ è l'insieme di tutte le matrici $m\times n$ ad elementi in $\mathcal{N}$. Ogni matrice $A \in \mathcal{M}_{m,n}$ si può scrivere come $A = (a_{ij})$ con $1 \le i \le m$, $1 \le j \le n$ e a_{ij} è l'elemento che si trova all'incrocio della riga i e della colonna j.

Esempio 9.8. *Per* $m = 3$ *e* $n = 4$ *si ha* $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}$.

Due matrici $A = (a_{ij}) \in \mathcal{M}_{mn}$ e $B = (b_{ij}) \in \mathcal{M}_{m'n'}$ coincidono se hanno le stesse dimensioni $m = m'$ e $n = n'$ e gli elementi di posto corrispondente sono uguali ossia se $a_{ij} = b_{ij}$ per ogni coppia i, j.

Esempio 9.9. $A = \begin{pmatrix} 1 & 2 \end{pmatrix}$ *e* $B = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ *sono diverse.*

$C = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ *e* $D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *sono diverse.*

Le matrici di $\mathcal{M}_{nn}$ si dicono **matrici quadrate**. Se $A = (a_{ij})$ è una matrice quadrata, gli elementi a_{ii} che si trovano su righe e colonne con indice uguale formano la **diagonale principale** di A.

Operazioni tra matrici

Somma di matrici. La somma è definita solo tra matrici aventi le stesse dimensioni e si esegue 'posto per posto'.

In simboli, se $A = (a_{ij})$, $B = (b_{ij}) \in \mathcal{M}_{mn}$, la loro somma è data da:

$$A + B = C \quad \text{dove} \quad c_{ij} = (a_{ij} + b_{ij})$$

La somma di matrici gode delle seguenti proprietà:

(1) **Associativa e commutativa.**

(2) **Esiste l'elemento neutro** rispetto alla somma: è la matrice nulla $\mathbf{0}$ di $\mathcal{M}_{m,n}(\mathbb{R})$ che ha 0 in ogni posto, tale che $A + \mathbf{0} = A$ per ogni matrice A.

(3) **Esiste l'opposto** di ogni matrice $A = (a_{ij})$: è la matrice $-A = (-a_{ij})$, tale che $A + (-A) = \mathbf{0}$.

Nota bene: il simbolo $\mathbf{0}$ può indicare tante matrici di dimensioni diverse, tutte fatte da soli zeri. Non usiamo simboli diversi per distinguerle perché di volta in volta sarà chiaro dal contesto quale stiamo considerando.

Prodotto per uno scalare. Siano A una matrice e λ un numero reale. Col simbolo λA indicheremo la matrice B, con le stesse dimensioni di A, ottenuta moltiplicando per λ ogni elemento di A:

$$\lambda A = \lambda(a_{ij}) = (\lambda a_{ij})$$

Diremo che due matrici non nulle con le stesse dimensioni A e B sono **proporzionali** se $B = \lambda A$ per un qualche $\lambda \in \mathbb{R}$.

Prodotto righe per colonne. Consideriamo un vettore riga e un vettore colonna della stessa lunghezza: $R = (a_1\, a_2\, \dots\, a_n)$ e $C = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$. Definiamo il loro prodotto $R \cdot C$ generalizzando a vettori di lunghezza qualsiasi il prodotto scalare introdotto nel paragrafo precedente:

$$R \cdot C = a_1 b_1 + a_2 b_2 \dots a_n b_n.$$

Il prodotto di due vettori è quindi un numero.

Se $A = (a_{ij}) \in \mathcal{M}_{m,n}$ e $B = (b_{jk}) \in \mathcal{M}_{m',n'}$ sono due matrici di dimensioni tali che $n = m'$, definiamo il loro prodotto $A \cdot B$ come la matrice P di dimensioni $m \times n'$ in cui l'elemento di posto ik è il prodotto della riga i-esima di A e della colonna k-esima di B ossia

$$p_{ik} = a_{i1} b_{1k} + a_{i2} b_{2k} + \dots a_{im} b_{mk}.$$

Esempio 9.10. $\begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} \pi & 0 & 2 \\ -3 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} =$

$$= \begin{pmatrix} 1 \cdot \pi + 2 \cdot (-3) + 3 \cdot 1 & 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 1 & 1 \cdot 2 + 2 \cdot 1 + 3 \cdot 0 \\ -1 \cdot \pi + 0 \cdot (-3) + 5 \cdot 1 & -1 \cdot 0 + 0 \cdot 1 + 5 \cdot 1 & -1 \cdot 2 + 0 \cdot 1 + 5 \cdot 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \pi - 3 & 5 & 4 \\ -\pi + 5 & 5 & -2 \end{pmatrix}$$

Nota bene: La somma è definita solo tra matrici con le stesse dimensioni, mentre il prodotto è definito solo se le righe della prima matrice hanno tanti elementi quanti ne hanno le colonne della seconda.

Il prodotto righe per colonne **non è commutativo**. Infatti:

- può darsi che $A \cdot B$ sia definito, ma $B \cdot A$ no;
- se anche $A \cdot B$ e $B \cdot A$ sono entrambe definite, possono avere dimensioni diverse;
- se anche $A \cdot B$ e $B \cdot A$ sono entrambe definite e hanno le stesse dimensioni (questo accade se A, B sono matrici quadrate con le stesse dimensioni), i due prodotti possono comunque essere matrici diverse.

Esempio 9.11. $A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$, $A \cdot B = \begin{pmatrix} 1 & 4 \\ 1 & 6 \end{pmatrix}$ *mentre* $B \cdot A = \begin{pmatrix} 4 & 2 \\ 5 & 3 \end{pmatrix}$.

Nel seguito ometteremo il simbolo $\cdot$ per il prodotto.

Anche se non è commutativo, il prodotto righe per colonne ammette comunque le seguenti proprietà:

i) **Proprietà associativa:** se A, B, C sono matrici tali che AB e BC sono definite, allora si può fare il prodotto delle tre e vale l'uguaglianza $A(BC) = (AB)C$.

ii) **Proprietà distributive:** se A, B, C sono matrici tali che $A(B+C)$ è definito, allora si ha $A(B+C) = AB + AC$ (e analogamente, $(B+C)A = BA + CA$ ogni volta che le operazioni sono definite).

iii) **Esistenza dell'identità moltiplicativa:** se $\mathcal{I}_n$ è la matrice che ha elementi tutti nulli, tranne quelli sulla diagonale principale che valgono 1, allora ogni volta che il prodotto è possibile si ha $A\mathcal{I}_n = A$ e $\mathcal{I}_n B = B$.

Esempio 9.12. *Le matrici identità* 2×2 *e* 3×3 *sono:*

$$\mathcal{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad \mathcal{I}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nel seguito scriveremo semplicemente $\mathcal{I}$ omettendo l'indice n quando la dimensione sarà chiara dal contesto.

Esempio 9.13. *Consideriamo le matrici* $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ *e* $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. *Se eseguiamo i prodotti nei due modi possibili troviamo* $AB = BA = \mathcal{I}$.

Se A e B sono matrici quadrate $n \times n$ e soddisfano le condizioni $AB = \mathcal{I}$ e $BA = \mathcal{I}$, diciamo che B è **l'inversa** di A (e A è l'inversa di B): in tal caso si scrive $B = A^{-1}$.

Importanti differenze rispetto alle operazioni tra numeri sono mostrate dagli esempi seguenti.

Esempio 9.14. *Consideriamo le due matrici* $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ *e* $B = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, *che sono entrambe diverse dalla matrice nulla* $\mathbf{0}$. *Eseguendo il prodotto si ottiene:* $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathbf{0}$.

Tra le matrici quindi non vale la legge di annullamento del prodotto cioè può capitare che il prodotto di due matrici non nulle sia la matrice nulla.

Esempio 9.15. *Consideriamo le matrici* A *e* B *dell'esempio precedente e la matrice* $C = \begin{pmatrix} 3 & -2 \\ -3 & 2 \end{pmatrix}$, *che sono tutte diverse da* $\mathbf{0}$. *Eseguendo i prodotti si ottiene:* $AB = AC$ *(perché in entrambi i casi si trova* $\mathbf{0}$*), anche se* $B \neq C$.

Tra le matrici quindi non vale la legge di cancellazione, cioè non sempre è possibile "semplificare" una uguaglianza $AB = AC$ ottenendo $B = C$.

Esempio 9.16. *Consideriamo la matrice* $D = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *(che è diversa da* $\mathbf{0}$*) e un'altra matrice qualsiasi* $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Il prodotto delle due è:* $DX = \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$ *che non può in ogni caso essere la matrice identità.*

Quindi non tutte le matrici hanno l'inversa. Si può provare che se una matrice quadrata ammette inversa, allora ne ha una sola.

Esempio 9.17. *La matrice* 2×2 *generica del tipo* $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *ha inversa se e soltanto se il numero* $\Delta = ad - bc$ *non è nullo. Si può infatti verificare con calcoli diretti che se* $\Delta \neq 0$, *allora l'inversa di* X *è la matrice*

$$X^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}.$$

Il numero Δ si chiama **determinante** della matrice X. Più in generale, ad ogni matrice quadrata $A \in \mathcal{M}_{n,n}$ si può associare un numero che si indica $det(A)$, il suo **determinante**, con la proprietà:

la matrice A **ha inversa se e soltanto se** $det(A) \neq 0$**.**

♣ Esercizi per la nona lezione

9.1 Siano dati i vettori $\mathbf{u} = (-1\,2)$ e $\mathbf{v} = (3\ -2)$.

i) Trovare le componenti di $\mathbf{s} = \mathbf{u} + \mathbf{v}$, $\mathbf{d} = \mathbf{u} - \mathbf{v}$, $\mathbf{e} = -2\mathbf{u}$, $\mathbf{f} = -3\mathbf{u} + 2\mathbf{v}$.

ii) Disegnare i vettori ottenuti rispetto al solito riferimento cartesiano ortogonale monometrico.

iii) Calcolare il modulo dei vettori precedenti.

iv) Calcolare i coseni degli angoli formati dai vettori $\mathbf{uv}$, $\mathbf{us}$, $\mathbf{ud}$, $\mathbf{sd}$, $\mathbf{ef}$.

v) Trovare le componenti dei due vettori di modulo 1 ortogonali a $\mathbf{u}$.

vi) Trovare le componenti dei due vettori di modulo 1 che formano un angolo di 30° con $\mathbf{u}$.

9.2 Dati $P = (1, 2)$ e $Q = (3, -1)$, trovare le componenti del punto medio del segmento PQ.

9.3 Il baricentro di un triangolo PQR è il punto G tale che la somma di vettori $GP + GQ + GR = \mathbf{0}$. Trovare le componenti di G quando $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $R = (x_R, y_R)$.

9.4 Verificare se le rette $2x + y - 1 = 0$ e $x - y = 0$ sono parallele. Altrimenti calcolare l'angolo ($\leq 90^o$) da esse formato.

9.5 Verificare se le rette $4x + 2y - 1 = 0$ e $2x + y = 0$ sono parallele. Altrimenti calcolare l'angolo ($\leq 90^o$) da esse formato.

9.6 Verificare se le rette $2x + y - 1 = 0$ e $x - 2y + 3 = 0$ sono perpendicolari. Altrimenti calcolare l'angolo ($\leq 90^o$) da esse formato.

9.7 Verificare se le rette $2x - y - 1 = 0$ e $x - 2y + 3 = 0$ sono perpendicolari. Altrimenti calcolare l'angolo ($\leq 90^o$) da esse formato.

9.8 Siano $A = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$ e $B = \begin{pmatrix} 2 & 1 \\ -2 & 3 \end{pmatrix}$. Calcolare $3A - 2B$, $3(A + B)$, $3A + 3B, -A$.

9.9 Indichiamo con A una matrice con m righe ed n colonne e con B una matrice con h righe e k colonne. Stabilire le dimensioni della matrice prodotto AB nei seguenti casi:

(1) $m = 1$, $n = 2$, $h = 2$ e $k = 2$
(2) $m = 2$, $n = 1$, $h = 1$ e $k = 3$
(3) $m = 1$, $n = 3$, $h = 3$ e $k = 1$
(4) $m = 3$, $n = 1$, $h = 1$ e $k = 3$.

9.10 Siano $A = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ -2 & 3 \end{pmatrix}$ e $C = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

(1) Determinare AB, AC, BC, $(AB)C$, $A(BC)$, $(A + B)C$, $AC + BC$.
(2) Determinare $detA$ e $detB$.
(3) Determinare A^{-1} e B^{-1}.

9.11 Verificare che $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ha $detA = 0$ se e solo se i vettori riga di A sono proporzionali.

9.12 Verificare che $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ha $detA = 0$ se e solo se i vettori colonna di A sono proporzionali.

9.13 Trasformare il sistema lineare $\begin{cases} 2x+3y=1 \\ x+y=2 \end{cases}$ in forma matriciale $A\binom{x}{y}=C$, determinando le matrici A e C.

Verificare che il $detA$ è $\neq 0$ e determinare A^{-1}.

Risolvere il sistema lineare ricavando la matrice $\binom{x}{y}$ dall'equazione matriciale $A\binom{x}{y}=C$.

9.14 In base all'esercizio precedente verificare se le seguenti coppie di rette r e s sono incidenti, parallele o coincidenti. Attenzione: non è necessario trovare gli eventuali punti comuni.

(1) $r:\ x-y+1=0$ e $s:\ x+y=0$;
(2) $r:\ 2x+y=0$ e $s:\ 4x+2y-1=0$;
(3) $r:\ x+2y+1=0$ e $s:\ y=0$;
(4) $r:\ x+y-2=0$ e $s:\ 2x+2y-4=0$.

Lezione 10

Matrici e trasformazioni

Trasformazioni di vettori del piano

Dobbiamo innanzitutto distinguere tra il piano inteso come insieme di punti ed il piano inteso come insieme di vettori. Anche lavorando in componenti la confusione è molto facile, poiché sia i punti, sia i vettori sono individuati da coppie di numeri. Occorre quindi fare molta attenzione alle notazioni che adoperiamo, ricordando che per indicare un punto mediante le sue coordinate scriviamo $P = (a, b)$, mentre per un vettore usiamo la scrittura in riga $\mathbf{v} = (a\ b)$ oppure in colonna $\mathbf{v} = \binom{a}{b}$.

Noi incominceremo ad occuparci delle trasformazioni del piano pensato come insieme di vettori, tenendo a mente che un vettore può sempre essere rappresentato da una freccia applicata nell'origine O, ma che ogni freccia della stessa direzione, verso e lunghezza, applicata in qualsiasi altro punto rappresenta lo stesso vettore.

Tra le trasformazioni più comuni utilizzate tra i vettori abbiamo le rotazioni; utilizzando le matrici diventa abbastanza semplice esprimere il vettore risultato di una rotazione R_α di angolo α applicata al vettore $\mathbf{v} = \binom{a}{b}$. Infatti:

$$R_\alpha(\mathbf{v}) = A\begin{pmatrix} a \\ b \end{pmatrix} \quad \text{dove} \quad A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Attenzione al fatto che l'opposto di $\sin(\alpha)$ compare come secondo elemento della prima riga!

Esempio 10.1. *Sappiamo che ruotando il vettore* $\binom{1}{0}$ *di* 90° *otteniamo il vettore* $\binom{0}{1}$*; verifichiamolo mediante l'uso delle matrici:*

$$\begin{pmatrix} \cos(90^o) & -\sin(90^o) \\ \sin(90^o) & \cos(90^o) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Un'altra trasformazione abbastanza comune tra vettori è la riflessione o ribaltamento S_r rispetto ad una retta r.

Esempio 10.2. *La riflessione S_x rispetto all'asse x e S_y rispetto all'asse y di un vettore $\boldsymbol{v}$ sono date rispettivamente dalle matrici*

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad e \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

nel senso che

$$S_x(\boldsymbol{v}) = B\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix} \quad e \quad S_y(\boldsymbol{v}) = C\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -a \\ b \end{pmatrix}.$$

Anche la **proiezione ortogonale** P_r di un vettore $\mathbf{v}$ su una retta r può essere espressa mediante una matrice.

Esempio 10.3. *Le proiezioni ortogonali P_x sull'asse x e P_y sull'asse y sono date rispettivamente dalle matrici:*

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad e \quad E = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

nel senso che

$$P_x(\boldsymbol{v}) = D\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix} \quad e \quad P_y(\boldsymbol{v}) = E\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ b \end{pmatrix}.$$

Consideriamo infine una **dilatazione** o **omotetia** K_λ di fattore λ, dove λ è un numero reale positivo, ossia la moltiplicazione di ogni vettore $\mathbf{v}$ per il fattore λ; notiamo che se $\lambda > 1$, K_λ ha proprio l'effetto di dilatare la lunghezza dei vettori, mentre se $\lambda < 1$ nel linguaggio abituale diremmo che K_λ è una contrazione. Possiamo ottenere $K_\lambda(\mathbf{v})$ ossia la moltiplicazione di $\mathbf{v}$ per il numero λ mediante la matrice:

$$F = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad \text{poiché} \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \lambda a \\ \lambda b \end{pmatrix}.$$

Trasformazioni inverse

Occupiamoci ora di trovare le matrici delle **trasformazioni inverse** di quelle prima considerate.

La rotazione di angolo α ha come trasformazione inversa la rotazione di angolo $-\alpha$ e quindi la matrice della rotazione inversa di R_α è quella della rotazione

$$R_{-\alpha} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

che si ottiene dalla precedente semplicemente scambiando le righe con le colonne. Attenzione dunque alla posizione dell'opposto di $\sin(\alpha)$!

Il ribaltamento inverso di $S_x(\mathbf{v})$ (rispettivamente di $S_y(\mathbf{v})$) è nuovamente $S_x(\mathbf{v})$ (risp. $S_y(\mathbf{v})$) e quindi non c'è nulla da trovare. Notiamo comunque che scambiando le righe con le colonne le matrici di $S_x(\mathbf{v})$ o $S_y(\mathbf{v})$ non cambiano!

Per quanto riguarda la proiezione ortogonale sull'asse x o y, invece, non è possibile parlare di trasformazione inversa, perché sono infiniti i vettori che ammettono la stessa proiezione e quindi non è più possibile risalire al vettore di partenza conoscendo solamente la sua proiezione.

Per quanto riguarda invece la dilatazione K_λ è facile verificare che la trasformazione inversa è semplicemente la dilatazione $K_{1/\lambda}$, per cui la matrice associata è $F^{-1} = \begin{pmatrix} 1/\lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$.

Osserviamo che in questo caso la matrice inversa non si ottiene semplicemente scambiando le righe con le colonne! Occorre invece utilizzare la formula indicata nell'Esempio 9.17.

Esempio 10.4. *Verifichiamo in due modi diversi che la trasformazione $R_{-\alpha}$ è l'inversa della trasformazione R_α.*

1) $R_{-\alpha}\left[R_\alpha \begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \left[\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}\right]$

$= \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} \cos(\alpha)x - \sin(\alpha)y \\ \sin(\alpha)x + \cos(\alpha)y \end{pmatrix} =$

$= \begin{pmatrix} \cos^2(\alpha)x - \cos(\alpha)\sin(\alpha)y + \sin^2(\alpha)x + \sin(\alpha)\cos(\alpha)y \\ -\sin(\alpha)\cos(\alpha)x + \sin^2(\alpha)y + \cos(\alpha)\sin(\alpha)x + \cos^2(\alpha)y \end{pmatrix} =$

$= \begin{pmatrix} (\cos^2(\alpha) + \sin^2(\alpha))x \\ (\sin^2(\alpha) + \cos^2(\alpha))y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$

2) $[R_{-\alpha}R_\alpha] \begin{pmatrix} x \\ y \end{pmatrix} = \left[\begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}\right] \begin{pmatrix} x \\ y \end{pmatrix} =$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$

Osservazione 10.5. La matrice dell'applicazione inversa di una trasformazione di vettori è data, quando esiste, dalla matrice inversa della matrice della trasformazione di vettori. Tale matrice si calcola mediante la formula dell'Esempio 9.17.

Trasformazioni tra punti del piano

Dopo aver considerato le trasformazioni tra vettori di un piano passiamo ad occuparci delle trasformazioni tra punti.

Iniziamo a considerare quelle che lasciano fisso il punto O, l'origine del nostro riferimento cartesiano.

Tali trasformazioni (o applicazioni o funzioni o ...) sono molto speciali e particolarmente facili da esprimere, perché si ottengono dalle trasformazioni tra vettori appena considerate semplicemente sostituendo le componenti del vettore $\mathbf{v}$ con le coordinate (a, b) del punto P per cui $\mathbf{v} = P - O$. Infatti, se una certa trasformazione tra punti del piano lascia l'origine O invariata e trasforma il punto P nel punto P', potremo pensarla anche come trasformazione tra vettori che trasforma il vettore $\mathbf{v} = P - O$ nel vettore $\mathbf{v}' = P' - O$. Analogamente, ogni trasformazione tra i vettori che trasforma il vettore $\mathbf{v} = P - O$ in $\mathbf{v'} = P' - O$ individua una trasformazione tra punti del piano che lascia fisso O e trasforma P in P'.

Possiamo quindi rappresentare facilmente tutte le trasformazioni precedentemente considerate pensandole come trasformazioni tra punti:

R) La rotazione R_α di angolo α tra vettori diventa la rotazione $R_{0\alpha}$ di centro O ed angolo α tra punti (prima non era necessario specificare che si trattasse di rotazioni di centro O, poiché ragionavamo solamente su frecce applicate in O); così se $P = (a, b)$, le coordinate (a', b') del punto ruotato P' saranno date da:

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

S) La riflessione o ribaltamento rispetto all'asse x e rispetto all'asse y di un punto $P = (a, b)$ saranno date da $S_x(P) = B\binom{a}{b}$ e $S_y(P) = C\binom{a}{b}$, dove B e C sono le matrici considerate nell'Esempio 10.2.

P) La proiezione ortogonale di un punto $P = (a, b)$ sull'asse x o sull'asse y sarà data da $P_x(P) = D\binom{a}{b}$ e $P_y(P) = E\binom{a}{b}$ dove D ed E sono le matrici dell'Esempio 10.3.

D) Infine una dilatazione di centro O di un fattore λ trasformerà il punto $P = (a, b)$ nel punto $P = (a', b') = (\lambda a, \lambda b)$ che possiamo ottenere anche da $\binom{a'}{b'} = F\binom{a}{b}$ dove F è la matrice $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$.

Le trasformazioni inverse sono poi le stesse delle precedenti.

Passiamo ora a considerare trasformazioni tra punti più generali, dove l'origine non sia necessariamente un punto fisso.

Il caso più evidente è sicuramente quello delle traslazioni. Notiamo che le traslazioni non hanno motivo di essere considerate come applicazioni tra vettori, poiché la traslazione di una freccia che rappresenta un certo vettore $\mathbf{v}$, dà un'altra freccia che però rappresenta lo stesso vettore $\mathbf{v}$, avendo conservato la stessa direzione, verso e lunghezza. Dunque ogni traslazione tra vettori coincide con la trasformazione identità, caso decisamente poco interessante!

La situazione è invece molto più interessante tra punti; se infatti trasliamo il punto $P = (x, y)$ lungo un vettore non nullo $\mathbf{v} = \binom{a}{b}$, P si trasforma nel punto P' tale che $P' - P = \mathbf{v}$, per cui $\binom{x'-x}{y'-y} = \binom{a}{b}$ e quindi le coordinate di P' sono $\begin{cases} x' = x + a \\ y' = y + b \end{cases}$ oppure, in forma matriciale:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}.$$

La traslazione inversa della traslazione lungo il vettore $\mathbf{v} = \binom{a}{b}$ è la traslazione opposta, cioè quella lungo il vettore opposto $-\mathbf{v} = \binom{-a}{-b}$ ed ha equazioni $\begin{cases} x' = x - a \\ y' = y - b \end{cases}$ oppure $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} a \\ b \end{pmatrix}$.

Occupiamoci ora di una rotazione del piano di centro un qualsiasi punto $C = (h, k)$ e di angolo α.

Per trovare le equazioni di una tale trasformazione conviene ricondurci al caso già noto delle rotazioni di centro O. Ciò è possibile perché per ruotare il punto $P = (x, y)$ attorno al punto $C = (h, k)$ possiamo procedere nel seguente modo:

a. prima applichiamo una traslazione che porti C in O ossia lungo il vettore $O - C = (-h\ -k)$, che quindi trasformerà il punto $P = (x, y)$ nel punto $P_1 = (x_1, y_1) = (x - h, y - k)$;

b. poi ruotiamo il punto P_1 attorno ad O di un angolo α, ottenendo il punto P_2 di coordinate (x_2, y_2);

c. infine applichiamo la traslazione inversa della precedente che porta O nuovamente in C e quindi P_2 nel punto $P_3 = (x_2 + h, y_2 + k)$. Il punto P_3 ottenuto in questo modo coincide con il punto P' trasformato del punto P mediante la rotazione di centro C ed angolo α.

Possiamo riassumere i passi precedenti con la notazione matriciale nel seguente modo:

a. $P_1 = (x - h, y - k)$;

b. la rotazione di centro O che porta il punto P_1 nel punto $P_2 = (x_2, y_2)$ è data da:

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} cos(\alpha) & -sen(\alpha) \\ sen(\alpha) & cos(\alpha) \end{pmatrix} \begin{pmatrix} x - h \\ y - k \end{pmatrix} = M \begin{pmatrix} x - h \\ y - k \end{pmatrix};$$

c. applicando poi la traslazione inversa otteniamo $P' = P_3 = (x_2 + h, y_2 + k)$ e quindi complessivamente le equazioni cercate sono:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x - h \\ y - k \end{pmatrix} + \begin{pmatrix} h \\ k \end{pmatrix}.$$

Le stesse equazioni possono essere scritte sotto forma esplicita, decisamente meno comoda, come:

$$\begin{cases} x' = cos(\alpha)(x - h) - sen(\alpha)(y - k) + h \\ y' = sen(\alpha)(x - h) + cos(\alpha)(y - k) + k \end{cases}$$

le quali esprimono le coordinate del punto trasformato P' in termini delle coordinate del punto di partenza P, dell'angolo α e del centro di rotazione $C = (h, k)$.

L'inversa di una rotazione di centro qualsiasi si può ottenere per composizione delle applicazioni inverse utilizzate nei punti **a.**, **b.**, **c.**, ma in ordine inverso.

Analogamente, possiamo usare la composizione di applicazioni per trovare le equazioni di un ribaltamento rispetto ad una retta qualsiasi: innanzitutto trasliamo la retta in modo da farla passare per l'origine, quindi la ruotiamo attorno ad O in modo che si sovrapponga all'asse x. Applichiamo ora il ribaltamento rispetto all'asse x e procediamo applicando nell'ordine prima l'inversa della rotazione attorno ad O e poi l'inversa della prima traslazione effettuata.

Applicazioni lineari e applicazioni affini.

Considerando il piano come insieme di vettori, le trasformazioni tra vettori:

$$\mathbf{v}' = f(\mathbf{v}) \text{ del tipo } \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} \text{ dove } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

vengono dette **applicazioni lineari** del piano. Tali applicazioni godono di due proprietà molto importanti:

(1) $f(\mathbf{v} + \mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w})$

(2) $f(k\mathbf{v}) = kf(\mathbf{v})$ e in particolare $f(\mathbf{0}) = \mathbf{0}$.

Si può provare che tutte le applicazioni che godono delle proprietà (1) e (2) possono essere espresse in forma matriciale come sopra.

Le equazioni di una applicazione lineare assumono pertanto la seguente forma esplicita:

$$\begin{cases} x' = ax + by \\ y' = cx + dy \end{cases}$$

in cui x' e y' sono espresse mediante due **polinomi lineari** in x e y ossia di primo grado in x e y, e con termine noto nullo: si tratta cioè di un **sistema di equazioni lineari omogenee** in x, y, x',y', dove omogeneo significa che tutti i monomi hanno lo stesso grado.

Le trasformazioni del piano come insieme di punti da noi considerate sono invece tutte caratterizzate da una forma matriciale generale del tipo:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} h \\ k \end{pmatrix} \text{ dove } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

oppure dalla forma esplicita:

$$\begin{cases} x' = ax + by + h \\ y' = cx + dy + k \end{cases}$$

Tali trasformazioni prendono il nome di **applicazioni affini** e, nel caso in cui mantengono fissa l'origine, godono delle stesse proprietà delle applicazioni lineari.

In generale invece, cioè per le applicazioni affini tali che $(h, k) \neq (0, 0)$, non valgono le due proprietà fondamentali (1) e(2) di cui godono le applicazioni lineari; in particolare si ha $f(0, 0) = (h, k) \neq (0, 0)$.

Notiamo che anche nelle applicazioni affini x' e y' sono date in forma esplicita da equazioni in cui compaiono solo polinomi di grado 1 in x e y; però i termini noti generalmente sono diversi da zero. Spesso viene utilizzato il termine ''lineare" per indicare polinomi di grado 1, anche se non omogenei. Occorre quindi fare molta attenzione quando si usa tale termine per non fare confusione tra i termini "applicazione lineare" e "funzione lineare": la prima è data da polinomi lineari omogenei, mentre la seconda da polinomi lineari il cui termine noto non è necessariamente nullo.

La linearità delle equazioni che definiscono applicazioni affini ha comunque importanti conseguenze. La più importante è il fatto che le applicazioni affini **invertibili**, come traslazioni, rotazioni e dilatazioni, trasformano sempre una retta

in una retta e, più in generale, una curva di grado n in una curva di grado n. Per esempio una circonferenza può essere trasformata da una applicazione affine invertibile in una ellisse, ma non in una retta oppure in una curva di grado superiore al secondo.

Esempio 10.6. *"Stiramento" di una circonferenza lungo l'asse y: l'applicazione affine* $\begin{cases} x' = 1x \\ y' = 4y \end{cases}$ *trasforma l'equazione $x^2 + y^2 = 1$ della circonferenza di centro l'origine e raggio 1, nell'equazione $(\frac{x'}{1})^2 + (\frac{y'}{4})^2 = 1$, che rappresenta l'ellisse di centro l'origine e semiassi 1 e 4.*

Isometrie del piano

Le **isometrie** sono particolari applicazioni lineari (isometrie lineari) o applicazioni affini (isometrie affini) che hanno la proprietà di conservare le misure: le prime conservano la lunghezza dei vettori, le seconde conservano la distanza tra i punti cioè due punti che hanno distanza d continuano ad avere la stessa distanza d dopo la trasformazione (si veda la Lezione 6).

Mediante l'espressione matriciale di una applicazione, sia lineare che affine, è facile capire se si tratta di una isometria o meno. É sufficiente infatti che la matrice 2x2 associata all'applicazione sia di un tipo speciale detto ortogonale.

Definizione 10.7. *Una matrice quadrata è detta **ortogonale** se le sue **colonne** sono vettori di lunghezza 1, a due a due ortogonali tra loro.*

Proprietà 10.8. *In una matrice ortogonale le **righe** sono vettori di lunghezza 1 a due a due ortogonali. Viceversa, una matrice in cui le righe sono vettori di lunghezza 1 a due a due ortogonali è ortogonale.*

Come abbiamo visto le isometrie del piano che lasciano l'origine fissa (isometrie lineari) sono le rotazioni e le riflessioni, mentre le isometrie affini del piano sono le rotazioni, le riflessioni, le traslazioni e le glissoriflessioni.

Proprietà 10.9. *Una matrice quadrata è ortogonale se e solo se la sua trasposta è uguale alla sua inversa, dove per matrice trasposta si intende quella che si ottiene scambiando le righe con le colonne.*

Dunque è molto semplice determinare la matrice inversa di una isometria: basta scambiare le righe con le colonne. Lo avevamo già notato nel caso delle trasformazioni inverse di rotazioni e riflessioni lineari.

Un'ulteriore conseguenza della definizione di matrice ortogonale è che il determinante può essere uguale solamente a 1 o a -1. Una isometria lineare di determinante 1 è una rotazione, mentre se ha determinante -1 è un ribaltamento. Occorre comunque precisare che non vale il viceversa, cioè non tutte le matrici con determinante 1 o -1 sono ortogonali, come ad esempio la matrice $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

★ Applicazioni alla dinamica delle popolazioni

Metodi matematici che coinvolgono anche l'uso di matrici sono spesso usati nelle scienze applicate. Vediamo a titolo di esempio come le matrici permettano di formalizzare in modo sintetico l'evoluzione di una popolazione animale nel tempo.

Consideriamo una certa popolazione animale, per esempio di stambecchi che vivono in un parco naturale. Se il ciclo vitale ottimale degli individui di quella popolazione è di 15 anni, possiamo suddividere gli individui della popolazione (considerando solo le femmine) in tre fasce d'età: da 0 a 5, da 5 a 10 e da 10 a 15. Indichiamo con $x_1(t)$, $x_2(t)$, $x_3(t)$ la consistenza numerica delle tre fasce d'età nell'istante t. Sia $t = 0$ l'istante iniziale di osservazione e $t = 1$ indichi un periodo di 5 anni.

Indichiamo poi con a_i la percentuale di femmine nella fascia di età $i = 1, 2, 3$ che ragiungono la fascia di età sucessiva (ovviamente $a_3 = 0$) e con b_i il numero medio di figlie nate durante un periodo da ogni femmina nella $i - esima$ fascia d'età.

Le consistenze numeriche dei tre gruppi dopo 5 anni, ossia per $t = 1$, sono legate a quelle nel momento iniziale, ossia $t = 0$, dalle relazioni:

$$\begin{cases} x_1(1) &= b_1x_1(0) + b_2x_2(0) + b_3x_3(0) \\ x_2(1) &= a_1x_1(0) \\ x_3(1) &= a_2x_2(0) \end{cases}$$

Se supponiamo che i valori a_i e b_i non cambino nel tempo (ad esempio perché le condizioni dell'ambiente e della popolazione non si sono modificati sostanzialmente), le stesse relazioni legheranno la consistenza numerica delle tre fasce in un qualsiasi istante $t = n$ alle consistenze 5 anni dopo, ossia all'istante $t = n + 1$:

$$\begin{cases} x_1(n+1) &= b_1x_1(n) + b_2x_2(n) + b_3x_3(n) \\ x_2(n+1) &= a_1x_1(n) \\ x_3(n+1) &= a_2x_2(n) \end{cases}$$

Possiamo esprimere sinteticamente questa relazione mediante la notazione matriciale
$\mathbf{X}(n+1) = A\mathbf{X}(n)$ dove $\mathbf{X}(t)$ è il vettore colonna con le tre componenti $x_i(t)$ e

$$A = \begin{pmatrix} b_1 & b_2 & b_3 \\ a_1 & 0 & 0 \\ 0 & a_2 & 0 \end{pmatrix}.$$

Esempio 10.10. *Una matrice A del tipo precedente può essere la seguente:*

$$A = \begin{pmatrix} 0 & 4 & 3 \\ 1/2 & 0 & 0 \\ 0 & 1/4 & 0 \end{pmatrix}.$$

Il numero 4 nella prima riga e seconda colonna significa che mediamente ogni femmina della seconda classe di età genera 4 figlie nell'arco dei 5 anni. Il numero $\frac{1}{2}$ nella seconda riga e prima colonna significa che solo la metà dei cuccioli (femmine) sopravvivono fino ai 5 anni di età.

Poiché moltiplicando a sinistra il vettore $\mathbf{X}(n)$ per la matrice A otteniamo il vettore $\mathbf{X}(n+1)$, moltiplicandolo due volte per A, ossia moltiplicando per A^2, otteniamo la situazione dopo due periodi cioè dopo 10 anni. Analogamente, la matrice A^k permetterà di trovare la situzione dopo k periodi di 5 anni.

Particolarmente interessanti in questa situazione sono i cosidetti **autovettori** della matrice A ossia quei vettori $\mathbf{X}$ tali che $A\mathbf{X} = \mathbf{X}$ o più generalmente tali che $A\mathbf{X} = \lambda\mathbf{X}$, soprattutto se tutti gli elementi che compaiono in esso sono numeri positivi. Se infatti il vettore $\mathbf{X}$ dà la consistenza numerica delle tre fasce d'età della popolazione e vale la relazione $A\mathbf{X} = \mathbf{X}$, allora la popolazione non si modifica nel tempo e si trova quindi in una stato di equilibrio con l'ambiente. Se più generalmente vale la relazione $A\mathbf{X} = \lambda\mathbf{X}$, con $\lambda > 0$, allora il numero di individui della popolazione cambia nel tempo, ma le proporzioni tra le tre fasce d'età si mantengono costanti. Ad esempio se $\lambda = 1,02$, la popolazione dopo 5 anni ha subito un incremento equilibrato del 2% in ogni fascia d'età e lo stesso si potrà riscontrare ogni 5 anni successivi, almeno fino a che la popolazione non sarà cresciuta eccessivamente e i parametri a_i e b_i dovranno essere modificati.

♣ Esercizi per la decima lezione

10.1 Scrivere le matrici associate alle rotazione di centro O di angoli $\pi/3$, $\pi/6$, $\pi/4$, $2\pi/3$ e le loro inverse.

10.2 Scrivere le matrici associate alle riflessioni rispetto alla retta $x = y$ e alla retta $x = -y$.

10.3 Determinare la matrice della rotazione ottenuta applicando prima $R_{\pi/3}$ e poi $R_{\pi/4}$ e verificare che si ottiene la matrice della rotazione $R_{(\pi/3+\pi/4)}$. (Ricordare la formula trigonometrica che esprime il coseno ed il seno della somma di due angoli.)

10.4 Calcolare le matrici delle trasformazioni ottenute applicando prima f e poi g, dove

a. $f = R_{\pi/3}$ e $g = S_x$;
b. $f = S_x$ e $g = K_3$;
c. $f = K_2$ e $g = R_{\pi/6}$.

10.5 Scrivere la matrice della rotazione inversa della trasformazione dell'esercizio precedente, calcolando l'inversa della composizione come composizione delle inverse ... ma attenzione all'ordine!

10.6 Siano $\mathbf{u} = (1\ \ -1)$, $\mathbf{v} = (2\ 1)$. Trovare le componenti dei vettori $R_{\pi/3}(\mathbf{u})$, $R_{\pi/3}(\mathbf{v})$, $R_{\pi/3}(\mathbf{u}+\mathbf{v})$, $R_{\pi/3}(\mathbf{u}) + R_{\pi/3}(\mathbf{v})$, $R_{\pi/3}(4\mathbf{v})$, $4R_{\pi/3}(\mathbf{v})$.

10.7 Scrivere le equazioni matriciali delle rotazioni di centro $H = (1, -1)$ di angoli $\pi/3$, $\pi/6$, $\pi/4$, $2\pi/3$.

10.8 Scrivere le equazioni esplicite delle rotazioni dell'esercizio precedente.

10.9 Siano $H = (1, -1)$, $K = (0, 2)$. Scrivere l'equazione matriciale della trasformazione ottenuta applicando prima $R_{H,\pi/3}$ e poi $R_{K,\pi/4}$, senza svolgere i conti.

10.10 Scrivere l'inversa della trasformazione dell'esercizio precedente, calcolando l'inversa della composizione come composizione delle inverse (in ordine inverso).

10.11 Sia $\binom{x'}{y} = A\binom{x}{y}$, dove $A = \begin{pmatrix} 1 & 2 \\ -3 & 0 \end{pmatrix}$. Verificare esplicitamente che $A(2\binom{x_1}{y_1} + 3\binom{x_2}{y_2}) = 2A\binom{x_1}{y_1} + 3A\binom{x_2}{y_2}$. A è invertibile?

10.12 Sia $\binom{x'}{y'} = A\binom{x}{y} + \binom{1}{-1}$, dove $A = \begin{pmatrix} 1 & 2 \\ -3 & 0 \end{pmatrix}$. Calcolare, se esiste, l'inversa di tale applicazione affine in forma matriciale.

10.13 Nei casi seguenti scrivere le equazioni delle trasformate della curva C mediante l'applicazione f; di cosa si tratta?

a) $C : x + y - 2 = 0$, $f : \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$, dove $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$;

b) $C : 2x^2 + y^2 = 1$, $f : \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$, dove $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$;

c) $C : x^2 + y^2 = 1$, $f : \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$, dove $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$;

d) $C : xy = 1$, $f : \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$, dove $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$;

e) $C : xy = 0$, $f : \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$, dove $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

10.14 Scrivere le equazioni di una applicazione affine che porti la retta r sulla retta r' nei seguenti casi:

a) $r : x + y - 1$, $r' : x - y = 0$;

b) $r : x + y = 0$, $r' : x + y + 1 = 0$.

10.15 Scrivere le equazioni di una applicazione affine che porti la circonferenza $\mathcal{C} : x^2 + y^2 = 1$ sulla circonferenza $\mathcal{C}' : (x - 1)^2 + (y - 2)^2 = 25$.

10.16 Sia A una matrice 2×2, verificare che il determinante della matrice trasposta è uguale al determinante di A.

10.17 Siano A e B due matrici 2×2. Verificare che $det(AB) = detA\, detB$.

10.18 Verificare che una matrice ortogonale 2×2 ha determinante 1 o -1.

10.19 Scrivere l'equazione matriciale di una glissoriflessione rispetto alla retta $x = y$ e di vettore traslatore $(2\ 2)$.

10.20 Si consideri la trasformazione F del piano data dalle equazioni:

$$\begin{cases} x' = \frac{1}{2}y - 1 \\ y' = \frac{1}{2}x + 1 \end{cases}$$

a) Disegnare nel piano cartesiano il triangolo di vertici $A = (3\,,\,2)$, $B = (6\,,\,3)$, $C = (1\,,\,8)$.

b) Trovare i punti A', B', C' trasformati di A, B, C mediante F.

c) Verificare che i due triangoli sono simili, calcolando i rapporti tra le lunghezze dei lati corrispondenti.