1. Esercizitazione 16 febbraio 2006

In questa prima esercitazione abbiamo fatto pratica con la divisione tra polinomi, finalizzata in particolare a calcolare un M.C.D. tra due polinomi $f(x)$ e $g(x)$ attraverso l'algoritmo di Euclide. Abbiamo ribadito le analogie, già discusse a lezione, tra l'anello $\mathbb{Z}$ e l'anello dei polinomi $\mathbb{K}[x]$ (introdotto nella prima lezione) dove $\mathbb{K}$ è un campo (per ora scelto tra il campo dei numeri razionali $\mathbb{Q}$, o quello dei numeri reali $\mathbb{R}$ o uno $\mathbb{Z}_p$).
In particolare abbiamo usato i seguenti risultati dell'anello $\mathbb{K}[x]$ le cui dimostrazioni sono del tutto simili a quelle fatte per i numeri interi (e che avete visto nel corso di LMM):

Teorema 1.1 (Teorema di divisione)**.** *Dati due polinomi $f(x)$,$g(x)$ in $\mathbb{K}[x]$ non entrambi nulli, esistono* **unici** *due polinomi in $\mathbb{K}[x]$ che indichiamo con $q(x)$ e $r(x)$ e chiamiamo rispettivamente quoziente e resto della divisione tra $f(x)$ e $g(x)$ tali che:*

1. $f(x) = g(x) \cdot q(x) + r(x)$
2. *Il polinomio resto $r(x)$ è uguale a zero (e in questo caso si dice che il polinomio $g(x)$* **divide** *il polinomio $f(x)$) oppure il grado di $r(x)$ è strettamente minore del polinomio $g(x)$.*

Teorema 1.2 (Teorema M.C.D. tra polinomi)**.** *Dati due polinomi $f(x)$,$g(x)$ in $\mathbb{K}[x]$ non entrambi nulli, esiste un polinomio $d(x)$ (che chiameremo* **un M.C.D.** *tra $f(x)$ e $g(x)$) tale che:*

1. *$d(x)$ divide sia $f(x)$ che $g(x)$*
2. *Ogni altro divisore comune $h(x)$ di (f) e $g(x)$ ha grado minore o uguale di $d(x)$. (Questa proprietà è equivalente alla seguente: ogni altro divisore comune $h(x)$ di $f(x)$ e $g(x)$ divide $d(x)$)*

Osservazione 1.3. Se $d(x)$ è un M.C.D. tra due polinomi $f(x)$ e $g(x)$ di $\mathbb{K}[x]$, allora qualsiasi polinomio ottenuto moltiplicando $d(x)$ per un elemento k di $\mathbb{K}$ diverso da zero continua ad essere un *M.C.D* tra $f(x)$ e $g(x)$ perché $k \cdot d(x)$ ha lo stesso grado di $d(x)$ (k è diverso da zero) inoltre è un divisore comune di $f(x)$ e $g(x)$. Infatti sappiamo che:

$$\underbrace{f(x) = d(x) \cdot h(x)}_{ipotesi\ d(x)\ divide\ f(x)} \qquad \underbrace{g(x) = d(x) \cdot t(x)}_{ipotesi\ d(x)\ divide\ g(x)}$$

e di conseguenza:

$$\underbrace{f(x) = (k \cdot d(x)) \cdot k^{-1} \cdot h(x)}_{quindi\ anche\ k \cdot d(x)\ divide\ f(x)} \qquad \underbrace{g(x) = (k \cdot d(x)) \cdot k^{-1} \cdot t(x)}_{quindi\ anche\ k \cdot d(x)\ divide\ g(x)}$$

Quindi il M.C.D. tra due polinomi non è unico, a meno di non stabilire una convenzione: per esempio quella di chiamare M.C.D. quello con coefficiente direttivo (cioè coefficiente del termine di grado massimo) uguale a 1. Per esempio se troviamo che $5x - 2$ è un M.C.D. tra due polinomi in $\mathbb{Q}[x]$, il M.C.D. con coefficiente direttivo uguale a 1 tra i due polinomi sarà:

$$\frac{1}{5} \cdot (5x - 2) = x - \frac{2}{5}$$

Teorema 1.4 (Algoritmo di Euclide)**.** *Per calcolare un M.C.D. $d(x)$ tra due polinomi $f(x)$ e $g(x)$ di $\mathbb{K}[x]$ si può usare l'algoritmo di Euclide (ovvero una successione*

di divisioni che dato che la successione dei gradi dei polinomi coinvolti è una successione decrescente di numeri naturali termina in un numero finito di passi). La dimostrazione del fatto che alla fine l'algoritmo di Euclide restituisce un M.C.D. tra $f(x)$ e $g(x)$ è del tutto analoga a quella fatta per gli interi.

Teorema 1.5 (Lemma di Bezout)**.** *Se $d(x)$ è un M.C.D. tra due polinomi $f(x)$ e $g(x)$ di $\mathbb{K}[x]$, allora esistono due polinomi $t(x)$ e $h(x)$ in $\mathbb{K}[x]$ tali che:*

$$f(x) \cdot h(x) + g(x) \cdot t(x) = d(x)$$

Tali polinomi si possono calcolare risalendo l'algoritmo di Euclide.

Esercizio 1.6. Calcolare quoziente e resto della divisione tra i due polinomi $x^6 - 1$ e $x^4 + x^3 + x^2 - 4x + 1$ in $\mathbb{Q}[x]$.

Anche l'algoritmo di divisione tra polinomi è simile all'algoritmo di divisione tra numeri interi: il punto di partenza è confrontare i termini di grado maggiore dei due polinomi. Per esempio tra $f(x) = x^6 - 1$ e $g(x) = x^4 + x^3 + x^2 - 4x + 1$ i termini di grado maggiore sono rispettivamente x^6 e x^4. Ci chiediamo per cosa dobbiamo moltiplicare x^4 per arrivare ad x^6, la risposta è ovviamente x^2. Allora moltiplichiamo $g(x)$ per x^2 è il risultato lo sottraiamo da $f(x)$. Quello che otterremo sarà un polinomio di grado minore di 6 perchè nella sottrazione $f(x) - x^2 \cdot g(x)$ si cancella il termine x^6. Continueremo fino a che non otteniamo 0 o un polinomio di grado minore a $g(x)$ (cioè fino a che non otteniamo il resto della divisione tra $f(x)$ e $g(x)$).

$$\begin{array}{lllllll|l} x^6 & & & & & & -1 & | & x^4+x^3+x^2-4x+1 \\ x^6 & +x^5 & +x^4 & -4x^3 & +x^2 & & & | & x^2 \\ & -x^5 & -x^4 & +4x^3 & -x^2 & -1 & & & \end{array}$$

A questo punto dobbiamo *confrontare* x^4 (il termine principale di $g(x)$) con $-x^5$ (il termine principale del polinomio ottenuto). Il secondo passaggio sarà quindi quello di moltiplicare $g(x)$ per $-x$:

$$\begin{array}{lllllll|l} x^6 & & & & & & -1 & | & x^4+x^3+x^2-4x+1 \\ x^6 & +x^5 & +x^4 & -4x^3 & +x^2 & & & | & x^2-x \\ & -x^5 & -x^4 & +4x^3 & -x^2 & -1 & & & \\ & -x^5 & -x^4 & -x^3 & +4x^2 & -x & & & \\ & & & 5x^3 & -5x^2 & +x & -1 & & \end{array}$$

Il polinomio ottenuto è di grado minore di $g(x)$ quindi abbiamo terminato l'algoritmo di divisione tra $f(x)$ e $g(x)$ e in particolare, se dovessimo calcolare un M.C.D. tra $f(x)$ e $g(x)$, avremmo terminato il primo passo dell'algoritmo di Euclide:

$$f(x) = g(x) \cdot \underbrace{(x^2 - x)}_{q_1(x)} + \underbrace{(5x^3 - 5x^2 + x - 1)}_{r_1(x)}$$

Algoritmo che continuerebbe dividendo $g(x)$ per $r_1(x)$ e poi r_n per r_{n+1} fino a trovare un resto nullo.

Esercizio 1.7. Calcolare il M.C.D. in $\mathbb{Z}_3[x]$ tra $f(x) = x^2 - x + 4$ e $g(x) = x^3 + 2x^2 + 3x + 2$

Osserviamo che essendo il campo dei coefficienti $\mathbb{Z}_3$, i coefficienti stessi sono classi di equivalenza modulo 3. In particolare abbiamo (usando come rappresentanti delle classi i numeri compresi tra 0 e 2):

$$x^2 - x + 4 = x^2 + 2x + 1 \quad \text{e} \quad x^3 + 2x^2 + 3x + 2 = x^3 + 2x^2 + 2$$

Iniziamo con l'algoritmo di divisione, confrontando i due termini principali osserviamo che bisogna moltiplicare x^2 per x per ottenere x^3:

$$\begin{array}{cccc|l} x^3 & +2x^2 & +3x & +2 & x^2 + 2x + 1 \\ x^3 & +2x^2 & +x & & x \\ & & 2x & +2 & \end{array}$$

Abbiamo quindi terminato il primo passo dell'algoritmo di Euclide:

$$g(x) = f(x) \cdot \underbrace{x}_{q_1(x)} + \underbrace{(2x+2)}_{r_1 x}$$

Il secondo passo prevede di dividere $f(x)$ per $r_1(x)$. I coefficienti direttivi dei due polinomi sono rispettivamente x^2 e $2x$, ma **attenzione** non si può moltiplicare per $\frac{1}{2} \cdot x$ perchè questa scrittura in $\mathbb{Z}_3$ non ha alcun senso. Il ragionamento però è analogo a quello che si farebbe in $\mathbb{Q}[x]$ (dove appunto moltiplicheremmo per $\frac{1}{2}x$): si tratta di moltiplicare per x moltiplicato per l'inverso di 2 in $\mathbb{Z}_3$ (che sappiamo esistere, essendo $\mathbb{Z}_3$ un campo!). Trovare questo inverso non è difficile visto che in $\mathbb{Z}_3$ ci sono tre elementi di cui uno è l'elemento nullo. Basta osservare che $2 \cdot 2 = 4$ ovvero 1 in $\mathbb{Z}_3$. Perciò l'inverso di 2 in $\mathbb{Z}_3$ è 2 e quindi nella divisione tra $f(x)$ e $r_1(x)$ dobbiamo moltiplicare per $2x$ il polinomio $r_1(x)$ e togliere il risultato da $f(x)$:

$$\begin{array}{ccc|l} x^2 & +2x & +1 & 2x + 2 \\ 4x^2 & +4x & & 2x \\ -3x^2 & -2x & +1 & \end{array}$$

Osserviamo che in $\mathbb{Z}_3$ il polinomio trovato è uguale al polinomio $x + 1$, possiamo perciò continuare nell'algoritmo di divisione perché questo polinomio ha lo stesso grado di $2x + 2$, che dovremo moltiplicare per 2:

$$\begin{array}{ccc|l} x^2 & +2x & +1 & 2x + 2 \\ 4x^2 & +4x & & 2x + 2 \\ & x & +1 & \\ & x & +1 & \\ & & 0 & \end{array}$$

Perciò il secondo passo dell'algoritmo di Euclide è anche quello conclusivo:

$$f(x) = r_1(x) \cdot \underbrace{(2x+2)}_{q_2(x)} + \underbrace{0}_{r_2(x)}$$

E un M.C.D. tra $f(x)$ e $g(x)$ è l'ultimo resto non zero dell'algoritmo di Euclide ovvero $r_1(x)$.

Vista la semplicità dei conti non è difficile trovare i due polinomi $t(x)$ e $h(x)$ dell'identità di Bezout, ovvero tali che:

$$f(x) \cdot t(x) + g(x) \cdot h(x) = r_1(x)$$

Infatti dal primo passo dell'algoritmo di Euclide segue che:

$$g(x) - f(x) \cdot x = r_1(x)$$

E perciò i due polinomi cercati sono: $t(x) = -x$ (o se si vuole mantenere la convenzione di usare come rappresentanti delle classi in $\mathbb{Z}_3$ i numeri 0, 1 e 2 $t(x) = 2x$) e $h(x) = 1$).

Esercizio 1.8. Trovare il M.C.D. in $\mathbb{Q}[x]$ tra le seguenti coppie di polinomi:

(1) $x^5 - x^4 + 3x^2 - 2x^2 + 2x - 1$ e $x^6 + x^5 - 2x^4 + 6x^3 + 5x + 3$
(2) $x^9 - 1$ e $x^{11} - 1$
(3) $x^5 - 2x^3 + x^2 - 3x - 3$ e $x^3 + x^2 - 3x - 3$
(4) $x^5 + x^4 - 3x^3 + 2x^2 - 1$ e $x^3 - 2x^2 - x + 2$
(5) $x^3 + 3x^2 - 4$ e $x^3 - x^2 - 3x + 6$

Come detto per calcolare un M.C.D. tra due polinomi si può procedere con l'algoritmo di Euclide, ovvero una serie di divisioni tra polinomi fino ad arrivare ad una divisione con resto nullo.
Calcoliamo per esempio il M.C.D. tra $f(x) = x^9 - 1$ e $g(x) = x^{11} - 1$ (ricordiamoci che il campo dei coefficienti è $\mathbb{Q}$):

$$\begin{array}{rrr|l} x^{11} & & -1 & x^9 - 1 \\ x^{11} & -x^2 & & x^2 \\ & x^2 & -1 & \end{array}$$

Primo passo algoritmo di Euclide:

$$g(x) = f(x) \cdot \underbrace{x^2}_{q_1(x)} + \underbrace{(x^2 - 1)}_{r_1(x)}$$

Continuiamo dividendo $f(x)$ per $r_1(x)$:

$$\begin{array}{rrrrr|l} x^9 & & & -1 & x^2 - 1 \\ x^9 & -x^7 & & & x^7 + x^5 + x^3 + x \\ & x^7 & & -1 & \\ & x^7 & -x^5 & & \\ & & x^5 & -1 & \\ & & x^5 & -x^3 & \\ & & & x^3 & -1 \\ & & & x^3 & -x \\ & & & x & -1 \end{array}$$

Secondo passo algoritmo di Euclide:

$$f(x) = r_1(x) \cdot \underbrace{(x^7 + x^5 + x^3 + x)}_{q_2(x)} + \underbrace{x - 1}_{r_2(x)}$$

L'algorimo continua dividendo $r_1(x)$ per $r_2(x)$, è evidente (prodotto notevole) senza fare la divisione che il terzo passo dell'algoritmo di Euclide sarà:

$$\underbrace{(x^2 - 1)}_{r_1(x)} = \underbrace{(x - 1)}_{r_2(x)} \cdot \underbrace{(x + 1)}_{q_2(x)} + \underbrace{0}_{r_3(x)}$$

Perciò l'algoritmo è terminato e un M.C.D. tra $f(x)$ e $g(x)$ è l'ultimo resto non zero, ovvero $r_2(x) = x - 1$.
Trovato un M.C.D. tra $f(x)$ $g(x)$ facciamo due esercizi supplementari:

(1) Trovare i due polinomi dell'algoritmo di Bezout, ovvero $t(x)$ e $h(x)$ tali che:

$$f(x) \cdot t(x) + g(x) \cdot h(x) = x - 1$$

(2) Trovare un[1] m.c.m. tra $f(x)$ e $g(x)$ ovvero un polinomio $m(x)$ che è multiplo sia di $f(x)$ che di $g(x)$ e tale che ogni polinomio che è multiplo comune di $f(x)$ e $g(x)$ ha grado maggiore o uguale di $m(x)$.

Per trovare $t(x)$ e $h(x)$ scriviamoci brevemente i tre passi dell'algoritmo di Euclide e *risaliamoli*:

(1) $g(x) = f(x) \cdot \underbrace{x^2}_{q_1(x)} + \underbrace{(x^2 - 1)}_{r_1(x)}$

(2) $f(x) = r_1(x) \cdot \underbrace{(x^7 + x^5 + x^3 + x)}_{q_2(x)} + \underbrace{x - 1}_{r_2(x)}$

(3) $\underbrace{(x^2 - 1)}_{r_1(x)} = \underbrace{(x - 1)}_{r_2(x)} \cdot \underbrace{(x + 1)}_{q_2(x)} + \underbrace{0}_{r_3(x)}$

Dal primo passo si trova che:

$$g(x) - f(x) \cdot q_1(x) = r_1(x)$$

E dal secondo passo si trova che:

$$r_2(x) = f(x) - r_1(x) \cdot q_2(x)$$

Sostituendo $r_1(x)$ in questa seconda uguaglianza si trova che:

$$r_2(x) = f(x) - (g(x) - f(x) \cdot q_1(x)) \cdot q_2(x)$$

ovvero:

$$r_2(x) = f(x) \cdot \underbrace{(1 + q_1(x) \cdot q_2(x))}_{t(x)} + g(x) \cdot \underbrace{(-q_2(x))}_{h(x)}$$

Per trovare un m.c.m. tra $f(x)$ e $g(x)$, una volta trovato il M.C.D. si procede come eravate abituati a fare per i numeri interi, ovvero si fattorizzano $f(x)$ e $g(x)$ a partire dalla divisione per il M.C.D.. Otteniamo:

$$f(x) = (x - 1) \cdot (x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

[1]L'uso dell'articolo indeterminato ha la stessa spiegazione che nel caso del M.C.D., infatti se $m(x)$ è un m.c.m. tra $f(x)$ e $g(x)$, allora anche ogni altro polinomio ottenuto dalla moltiplicazione di $m(x)$ per una costante diversa da zero è m.c.m. tra $f(x)$ e $g(x)$.

e

$$g(x) = (x-1) \cdot (x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

Sappiamo inoltre che in $\mathbb{Q}[x]$ i due fattori $(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ e $(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ sono primi[2] tra loro (altrimenti $(x-1)$ non sarebbe un M.C.D. tra $f(x)$ e $g(x)$ perché esisterebbe un fattore comune di grado maggiore). Perciò un m.c.m. tra $f(x)$ e $g(x)$ è:

$$(x-1)\cdot(x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)\cdot(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$$

[2]Ovvero i loro M.C.D. sono le costanti diverse da zero.

2. Esercizitazione 23 febbraio 2006

Affrontiamo il problema della fattorizzazione nell'anello dei polinomi $\mathbb{K}[x]$ a coefficienti in $\mathbb{K}$, dove $\mathbb{K}$ è uno dei seguenti campi: $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$ (con p primo). Sappiamo che in $\mathbb{K}[x]$ ogni polinomio di grado maggiore o uguale a 1 è irriducibile oppure è fattorizzabile (in maniera unica[3]) come prodotto di fattori irriducibili.
Ricordiamo che la definizione di polinomio irriducibile si riferisce a polinomi a coefficienti in un anello A (quindi in particolare vale anche per polinomi di $\mathbb{Z}[x]$ e questo ci permetterà di lavorare anche in $\mathbb{Z}[x]$).
Il problema della fattorizzazione consiste quindi di due parti: riconoscere se il polinomio considerato è irriducibile in $\mathbb{K}[x]$ e in caso di risposta negativa riuscire a trovarne una fattorizzazione. Vedremo che la difficoltà di queste due parti dipende dal campo $\mathbb{K}$ su cui stiamo lavorando, quindi distinguiamo i vari casi.

(1) **Irriducibilità e fattorizzazione in** $\mathbb{C}[x]$
In questo caso possiamo caratterizzare i polinomi irriducibili in base al grado, infatti sappiamo che vale il seguente teorema:

Teorema 2.1 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio $f(x)$ a coefficienti in $\mathbb{C}$ di grado maggiore di zero ammette almeno una radice in $\mathbb{C}$.*

Da cui possiamo ricavare il seguente importante corollario:

Corollario 2.2. *Ogni polinomio $f \in \mathbb{C}[x]$ di grado $n > 0$ è il prodotto di n fattori di primo grado in $\mathbb{C}[x]$.*

Dim. Procediamo per induzione sul grado n di f. Se f è di primo grado non c'è niente da dimostrare. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in \mathbb{C}$ e $a_n \neq 0$, $n > 1$. Possiamo scrivere $f(x) = a_n g(x)$ con $g(x)$ monico. Sia α radice di $g(x)$, la cui esistenza è assicurata dal teorema 2.1 allora:

$$f(x) = a_n(x - \alpha)g_1(x) \quad \text{con} \quad deg(g_1) = n - 1$$

quindi g_1 e di conseguenza f si scrivono come prodotto di fattori di grado 1. □

Ovvero in $\mathbb{C}[x]$ un polinomio è irriducibile se e solo è di primo grado.
In $\mathbb{C}[x]$ il problema quindi non è quello di riconoscere se un polinomio è irriducibile ma quello di riuscire a fattorizzare polinomi di grado maggiore a 1. E fattorizzare un polinomio equivale a trovarne le radici perchè tutti i suoi fattori irriducibili sono di grado 1. Dobbiamo cioè essere in grado di risolvere equazioni polinomiali a coefficienti complessi, cosa che può essere anche molto complicata. Prima di vedere un esempio, sottolineiamo il fatto che la ricerca di radici complesse è importante, come vedremo, anche per la fattorizzazione in $\mathbb{R}[x]$.

[3] A meno dell'ordine dei fattori e di moltiplicazione per invertibili, cioè le costanti. Ovvero la fattorizzazione $(x-1)\cdot(x-2)$ del polinomio x^2-3x+2 potrebbe essere scritta anche $(x-2)\cdot(x-1)$, ma questa fattorizzazione la consideriamo identica alla precedente, abbiamo cambiato solo l'ordine dei fattori. Così come consideriamo identica la fattorizzazione $\frac{1}{2} \cdot (x-1) \cdot 2 \cdot (x-2)$, in quanto abbiamo solo moltiplicato per invertibili (il cui prodotto è 1) i due fattori irriducibili. Osserviamo l'analogia con l'unicità della fattorizzazione in primi dei numeri in $\mathbb{Z}$. Il numero 21 è uguale a $7 \cdot 3$, noi consideriamo identica (perchè cambiamo solo l'ordine) la fattorizzazione $3 \cdot 7$, ma anche la fattorizzazione che si può ottenere moltiplicando per invertibili il cui prodotto totale sia 1. Gli invertibili in $\mathbb{Z}$ sono 1 e -1. 21 lo possiamo scrivere anche come $-1 \cdot 3 \cdot (-1) \cdot 7$ ovvero come $-3 \cdot (-7)$.

Esempio 2.3. Fattorizzare il polinomio $x^2 + 4x + 5 \in \mathbb{C}[x]$ come prodotto di irriducibili.

Dobbiamo trovare le radici complesse del polinomio $x^2 + 4x + 5$, ovvero le soluzioni complesse dell'equazione

$$x^2 + 4x + 5 = 0 \tag{2.1}$$

La formula risolutiva dell'equazione di secondo grado ci permette di trovare le soluzioni complesse (non abbiamo più paura di delta negativi nei complessi!):

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Nel nostro caso:

$$x_{1,2} = \frac{-4 \pm \sqrt{-4}}{2} = \frac{-4 \pm 2i}{2} = -2 \pm i$$

Quindi il polinomio $x^2 + 4x + 5 \in \mathbb{C}[x]$ si fattorizza in irriducibili come:

$$(x - (-2 + i)) \cdot (x - (-2 - 1))$$

Per riprova possiamo calcolarci questo prodotto osservando che:

$$(x - (-2 + i)) \cdot (x - (-2 - 1)) = ((x + 2) + i) \cdot ((x + 2) - i)$$

E questo sappiamo essere un prodotto notevole (ovvero la differenza di quadrati):

$$((x + 2) + i) \cdot ((x + 2) - i) = (x + 2)^2 - i^2 = x^2 + 4x + 5$$

Una proprietà importante sulle radici complesse la troviamo introducendo la seguente definizione:

Definizione 2.4. Dato il complesso $z = a + ib$ si chiama **complesso coniugato** di z, il numero complesso $a - ib$ che indichiamo con $\overline{z}$. (Cioè il numero complesso che ha parte reale uguale a z e parte immaginaria opposta a quella di z.)

Proposizione 2.5. *Sia $f(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$ e sia $\alpha \in \mathbb{C}$ una radice di f. Allora anche $\overline{\alpha}$ è una radice di f.*

ATTENZIONE questa proposizione è vera se i coefficienti del polinomio che stiamo considerando sono reali!

Esercizio 2.6. Sapendo che $f(x) = x^4 - 4x^3 + 3x^2 + 14x + 26$ ha radice $3 + 2i$, fattorizzare il polinomio in $\mathbb{C}[x]$

Il polinomio considerato è a coefficienti interi, quindi in particolare reali. Allora possiamo applicare la proposizione 2.5 e concludere che anche $3 - 2i$ è radice del polinomio, da questo segue che $(x - (3 + 2i)) \cdot (x - (3 - 2i)) =$

$x^2 - 6x + 13$ divide $f(x)$:

$$\begin{array}{cccccc|c} x^4 & -4x^3 & +3x^2 & +14x & +26 & | & x^2 - 6x + 13 \\ x^4 & -6x^3 & +13x^2 & & & | & x^2 + 2x + 2 \\ & 2x^3 & -10x^2 & +14x & +26 & & \\ & 2x^3 & -12x^2 & +26x & & & \\ & & 2x^2 & -12x & +26 & & \\ & & 2x^2 & -12x & +26 & & \\ & & & & 0 & & \end{array}$$

Quindi:

$$f(x) = (x - (3 + 2i)) \cdot (x - (3 - 2i)) \cdot (x^2 + 2x + 2)$$

E per completare la fattorizzazione in $\mathbb{C}[x]$ resta da fattorizzare il polinomio $x^2 + 2x + 2$. Calcoliamo le radici del polinomio attraverso la formula risolutiva delle equazioni di secondo grado:

$$x_{1,2} = \frac{-2 \pm \sqrt{-4}}{2} = \frac{-2 \pm 2i}{2} = \frac{2 \cdot (-1 \pm i)}{2} = -1 \pm i$$

Per cui la fattorizzazione di $f(x)$ è data da:

$$(x - (3 - 2i)) \cdot (x^2 + 2x + 2) \cdot (x - (1 + i)) \cdot (x - (1 - i))$$

(2) **Irriducibilità e fattorizzazione in $\mathbb{R}[x]$**
Anche in $\mathbb{R}[x]$ si possono caratterizzare i polinomi irriducibili attraverso il grado. Infatti consideriamo un generico polinomio $f(x) \in \mathbb{R}[x]$: dalla proposizione 2.5 segue che se $f(x)$ ha una radice complessa $\alpha = a + ib$ con parte immaginaria diversa da zero ($b \neq 0$), allora una radice complessa distinta di $f(x)$ è $\overline{\alpha}$, quindi $f(x)$ è divisibile per:

$$(x - \alpha) \cdot (x - \overline{\alpha}) = (x - (a + ib)) \cdot (x - (a - ib)) = x^2 - 2ax + a^2 + b^2$$

L'osservazione fondamentale è che $x^2 - 2ax + a^2 + b^2$ è un polinomio a coefficienti reali (irriducibile in $\mathbb{R}[x]$) perchè abbiamo ipotizzato che le sue radici non fossero reali ($b \neq 0$). Quindi i fattori irriducibili in $\mathbb{R}[x]$ hanno grado 1 o 2. Sicuramente tutti i polinomi di grado 1 sono irriducibili, per quelli di grado 2, del tipo $ax^2 + bx + c$, basta vedere se hanno radici reali o no, cioè basta determinare il delta. Se $\Delta \geq 0$ allora il polinomio $ax^2 + bx + c$ ha due radici reali (una di molteplicità due se $\Delta = 0$) e quindi è riducibile, se $\Delta < 0$ il polinomio non ha radici reali, quindi non è prodotto di termini di grado uno e dunque è irriducibile.
Riassumendo abbiamo caratterizzato gli elementi irriducibili di $\mathbb{R}[x]$:

Proposizione 2.7. *$f(x) \in \mathbb{R}[x]$ è irriducibile se e solo se è di grado 1 oppure è di grado 2 (del tipo $ax^2 + bx + c$) e $b^2 - 4ac$ è minore di zero.*

Anche in questo caso però sapere che un polinomio $f(x)$ sia riducibile non implica che la sua fattorizzazione in fattori irriducibili sia semplice. Solitamente, se siamo in grado, si cercano le radici complesse di $f(x)$: quelle che appartengono a $\mathbb{R}$ determinano i fattori di grado 1 della fattorizzazione, le altre (quelle eventuali con parte immaginaria non nulla) determinano (insieme al loro complesso coniugato) gli eventuali fattori irriducibili di grado 2 del polinomio.

Esempio 2.8. Fattorizzare il polinomio $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$.

Questo polinomio è di grado 4 ma non ha termini di grado dispari. Possiamo quindi, con la semplice sostituzione $x^2 = t$, ottenere un polinomio di grado 2 associato a quello di partenza: t^2-2t-3. Cerchiamo di fattorizzare questo polinomio in $\mathbb{R}[t]$. Dalla formula risolutiva delle equazioni di secondo grado otteniamo:

$$t_{1,2} = \frac{2 \pm \sqrt{16}}{2}$$

Ovvero $t^2 - 2t - 3 = (t-3) \cdot (t+1)$. Quindi:

$$x^4 - 2x^2 - 3 \underbrace{=}_{x^2=t} t^2 - 2t - 3 = (t-3) \cdot (t+1) \underbrace{=}_{t=x^2} (x^2-3) \cdot (x^2+1)$$

In questo caso è facile vedere che $x^2 + 1$ è irriducibile in $\mathbb{R}[x]$ (ha radici complesse i e $-i$), mentre $x^2 - 3 = (x - \sqrt{3}) \cdot (x + \sqrt{3})$. Concludendo si ha che la fattorizzazione in irriducibili di $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$ è data da:

$$(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x^2 + 1)$$

(3) **Irriducibilità e fattorizzazione in $\mathbb{Q}[x]$**

In $\mathbb{Q}[x]$, a differenza di quanto visto finora, non riusciamo a caratterizzare i polinomi irriducibili in base al grado, infatti si può dimostrare che per ogni naturale n si trovano polinomi di grado n irriducibili in $\mathbb{Q}[x]$. Possiamo osservare però che se $f(x) \in \mathbb{Q}[x]$, allora moltiplicando per il minimo comun denominatore dei coefficienti razionali otteniamo un polinomio $g(x)$ a coefficienti interi che è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è $f(x)$. Quindi il problema dell'irriducibilità e della fattorizzazione in $\mathbb{Q}[x]$ può essere ridotto allo studio di polinomi a coefficienti interi. Questo facilita molto le cose infatti consideriamo un polinomio $f(x) = \sum_{j=0}^{m} b_j x^j$ a coefficienti interi. Abbiamo visto che trovare le eventuali radici nel campo in cui si vuole fattorizzare è molto importante per la fattorizzazione perchè permette di individuare gli eventuali fattori di grado 1. Supponiamo dunque che $\alpha = \frac{r}{s}$ sia una radice razionale[4] ridotta ai minimi termini, cioè $(r, s) = 1$, allora:

$$b_n \frac{r^n}{s^n} + ... + b_1 \frac{r}{s} + b_0 = 0$$

e moltiplicando tutto per s^n si ottiene:

$$b_n r^n + \underbrace{b_{n-1} r^{n-1} s + ... + b_0 s^n}_{\text{è un multiplo di } s} = 0 \tag{2.2}$$

Per cui $s | b_n r^n$, ma essendo $(s, r) = 1$ questo implica $s | b_n$. Analogamente se raccogliamo in 2.2 r, otteniamo che r deve dividere $b_0 s^n$, ma essendo $(r, s) = 1$ questo implica che $r | b_0$.

Conclusione: Se $f(x) \in \mathbb{Z}[x]$ e r/s è una radice in $\mathbb{Q}$, allora r divide il termine noto e s divide il coefficiente del termine di grado massimo.

Questa osservazione è di fondamentale importanza in quanto limita ad un insieme finito e ristretto la ricerca di possibili radici razionali (e quindi fattori irriducibili di grado 1) di un polinomio a coefficienti interi. Questo permette per esempio di avere un algoritmo per discutere l'irriducibilità

[4] Ricordiamo che pur essendo $f(x)$ a coefficienti interi stiamo discutendo la fattorizzazione in $\mathbb{Q}[x]$.

di polinomi di grado 3 in $\mathbb{Q}[x]$, infatti un polinomio di questo tipo o è irriducibile o ha una radice razionale: perchè se è riducibile o è il prodotto di tre fattori di grado 1, oppure è il prodotto di un fattore di grado 1 per uno di grado 2, in ogni caso se è riducibile deve avere un fattore di grado 1 (e quindi una radice razionale).

Esercizio 2.9. Dire se $f(x) = x^3 - x^2 - 8x + 12$ è irriducibile in $\mathbb{Q}[x]$, e eventualmente trovarne una fattorizzazione in fattori irriducibili.

I divisori del termine noto sono $\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ i divisori del coefficiente del termine di grado massimo sono $\{\pm1\}$ quindi le possibili radici razionali sono: $\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$. Proviamo a calcolare i valori della funzione polinomiale $f(x)$ per questi valori fino a che non troviamo una radice e se non la troviamo vuol dire che $f(x)$ è irriducibile in $\mathbb{Q}[x]$:

$$f(1) = 4 \neq 0 \qquad f(-1) == 18 \neq 0 \qquad f(2) = 0$$

Dunque $f(x)$ è riducibile e ha $(x-2)$ come fattore di grado 1. A questo punto si potrebbe continuare a cercare altre radici razionali per vedere se ci sono altri fattori di $f(x)$ di grado 1 diversi da $(x-2)$, ma forse nel caso di un polinomio di grado 3 conviene procedere dividendo $f(x)$ per $(x-2)$ in modo da trovare un fattore di grado 2 che sappiamo dire se è riducibile o meno in $\mathbb{Q}[x]$ attraverso la formula risolutiva delle equazioni di secondo grado:

$$\begin{array}{rrrrl}
x^3 & -x^2 & -8x & +12 & \mid\ x-2 \\
x^3 & -2x^2 & & & \mid\ x^2+x-6 \\
 & x^2 & -8x & +12 & \mid \\
 & x^2 & -2x & & \mid \\
 & & -6x & +12 & \mid \\
 & & -6x & +12 & \mid \\
 & & & 0 & \mid
\end{array}$$

Quindi $f(x) = (x-2)\cdot(x^2+x-6)$. Si tratta di vedere se $x^2+x-6=0$ ha o meno due soluzioni razionali. Dalla formula risolutiva si ottiene:

$$x_{1,2} = \frac{-1 \pm \sqrt{25}}{2} = \frac{-1 \pm 5}{2}$$

E quindi x^2+x-6 è riducibile in $\mathbb{Q}[x]$ e si fattorizza come $(x+3)\cdot(x-2)$. La fattorizzazione in irriducibili di $x^3-x^2-8x+12$ in $\mathbb{Q}[x]$ è dunque data da:

$$x^3 - x^2 - 8x + 12 = (x-2)^2 \cdot (x+3)$$

(4) **Irriducibilità e fattorizzazione in $\mathbb{Z}_p[x]$**
Accenniamo solamente alla fattorizzazione in questo particolare anello di polinomi. Anche in questo caso, come per $\mathbb{Q}[x]$ non caratterizziamo i polinomi irriducibili in base al grado come avevamo fatto per $\mathbb{R}[x]$ o $\mathbb{C}[x]$, ma in questo caso abbiamo un algoritmo finito elementare (anche se può essere molto dispendioso come tempo) per mostrare che un polinomio è irriducibile o viceversa trovarne una fattorizzazione in irriducibili. Sia infatti $f(x) \in \mathbb{Z}_p[x]$ di grado n allora se è riducibile ha un fattore irriducibile che ha grado minore o uguale a $n/2$ se n è pari e a $n-1/2$ se n è dispari. Essendo $\mathbb{Z}_p$ finito i polinomi di grado minore di un fissato k sono finiti (sono p^k) e quindi un modo per trovare una fattorizzazione di $f(x)$ è provare a

dividere per tutti i polinomi di grado minore o uguale di $n/2$ (o $n-1/2$ nel caso n dispari). Se nessuno di questi divide $f(x)$ allora $f(x)$ è irriducibile, altrimenti continuiamo con lo stesso procedimento fino a che non si scrive $f(x)$ come prodotto di irriducibili. Proviamo con questo metodo a risolvere il seguente esercizio:

Esercizio 2.10. Dimostrare che $f(x) = x^5 + x^2 + 1$ è irriducibile in $\mathbb{Z}_2[x]$

Per prima cosa vediamo di escludere che ci siano fattori di grado 1 che fattorizzano $f(x)$. Per questo basta mostrare che $f(x)$ non ha radici in $\mathbb{Z}_2$, in effetti $f(0) = 1$ e $f(1) = 3 \equiv 1$. Mostrato che non ci possono essere fattori di grado 1 l'unica possibile fattorizzazione di $f(x)$ può essere come un polinomio di grado 3 per un polinomio di grado 2. I polinomi di grado uguale a 2 in $\mathbb{Z}_2[x]$ sono x^2+x+1, x^2+x e x^2+1 e x^2...allora con pazienza facciamo la divisione di $f(x)$ per questi quattro polinomi. $f(x)$ risulterà irriducibile se da queste divisioni non verrà mai resto uguale a zero, cioè se nessun polinomio di grado 2 in $\mathbb{Z}_2[x]$ divide $f(x)$:

$$\begin{array}{cccccc|l}
x^5 & & & +x^2 & +1 & & x^2+x+1 \\
x^5 & +x^4 & +x^3 & & & & x^3+x^2 \\
 & x^4 & +x^3 & +x^2 & +1 & & \\
 & x^4 & +x^3 & +x^2 & & & \\
 & & & & +1 & &
\end{array}$$

Quindi $f(x) = (x^2+x+1)\cdot(x^3+x^2) + \underbrace{1}_{resto\ diverso\ da\ 0}$

$$\begin{array}{cccccc|l}
x^5 & & & +x^2 & +1 & & x^2+x \\
x^5 & +x^4 & & & & & x^3+x^2+x \\
 & x^4 & & +x^2 & +1 & & \\
 & x^4 & +x^3 & & & & \\
 & & x^3 & +x^2 & +1 & & \\
 & & x^3 & +x^2 & & & \\
 & & & & +1 & &
\end{array}$$

Quindi $f(x) = (x^2+x)\cdot(x^3+x^2+x) + \underbrace{1}_{resto\ diverso\ da\ 0}$

$$\begin{array}{cccccc|l}
x^5 & & +x^2 & & +1 & & x^2+1 \\
x^5 & +x^3 & & & & & x^3+x+1 \\
 & x^3 & +x^2 & & +1 & & \\
 & x^3 & & +x & & & \\
 & & x^2 & +x & +1 & & \\
 & & x^2 & & +1 & & \\
 & & & x & & &
\end{array}$$

Quindi $f(x) = (x^2+1)\cdot(x^3+x+1) + \underbrace{x}_{resto\ diverso\ da\ 0}$

$$\begin{array}{llll} x^5 & +x^2 & +1 & \mid\ x^2 \\ x^5 & & & \mid\ x^3+1 \\ & x^2 & +1 & \mid \\ & x^2 & & \mid \\ & & +1 & \mid \end{array}$$

Quindi $f(x) = (x^2) \cdot (x^3+1) + \underbrace{1}_{resto\ diverso\ da\ 0}$

3. Esercizitazione 2 marzo 2006

Abbiamo già osservato che $g(x) \in \mathbb{Q}[x]$ è riducibile se e solo se il polinomio $f(x)$ ad esso associato a coefficienti interi è riducibile in $\mathbb{Q}[x]$, ma dal lemma di Gauss possiamo concludere che scoprire se $g(x)$ è irriducibile in $\mathbb{Q}[x]$ o no è un problema equivalente a scoprire se $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e non in $\mathbb{Q}[x]$!!!) o no.
Ecco perché spesso studieremo dei polinomi a coefficienti interi: si tratta di una limitazione solo apparente del nostro campo d'azione, in realtà studiando la riducibilità dei polinomi a coefficienti interi abbiamo tutte le informazioni che ci servono per conoscere la riducibilità dei polinomi in $\mathbb{Q}[x]$. A questo riguardo, un'arma importante a nostro favore è il seguente criterio di irriducibilità (di cui tralasciamo la dimostrazione):

Teorema 3.1 (Criterio di Eisenstein)**.** *. Sia*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ \in \mathbb{Z}[x]$$

Se esiste un numero primo p tale che p NON divide a_n, ma $p \mid a_{n-1}$,$p \mid a_{n-2}$, $\ldots$,$p \mid a_1$, $p \mid a_0$ e inoltre p^2 NON divide a_0, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e dunque in $\mathbb{Q}[x]$).

Grazie a questo criterio, possiamo facilmente costruire polinomi irriducibili in $\mathbb{Q}[x]$ di qualsiasi grado. Per esempio, se vogliamo un polinomio irriducibile di grado 1117, basterà considerare

$$x^{1117} - 2$$

Infatti il criterio di Eisenstein, applicato facendo riferimento al numero primo 2, ci garantisce che tutti i polinomi della forma $x^n - 2$ sono irriducibili in $\mathbb{Q}[x]$. Oppure avremmo potuto prendere

$$8x^{1117} - 12x^{501} - 9x^4 - 27x^3 - 15x - 33$$

e ancora il criterio di Eisenstein (applicato con il numero primo 3) ci garantisce che questo polinomio è irriducibile in $\mathbb{Q}[x]$.

Esempio 3.2. Dimostrare che per ogni $p \in \mathbb{N}$ primo il polinomio:

$$\sum_{i=0}^{p-1} x^i$$

è irriducibile in $\mathbb{Q}[x]$

Dimostreremo questo risultato utilizzando il criterio di Eisenstein. Ma prima di questa abbiamo bisogno del seguente risultato intermedio:

Lemma 3.3. *Dati $f(x) \in \mathbb{K}[x]$ e $a, b \in \mathbb{K}$ con $a \neq 0$ si ha che $f(x)$ è riducibile se e solo se $f(ax+b)$ (cioè il polinomio ottenuto dal cambio di variabile tra x e $ax+b$) è riducibile.*

Basta infatti notare che $f(x) = g(x) \cdot h(x)$ se e solo se $f(ax+b) = g(ax+b) \cdot h(ax+b)$ e inoltre $deg(g(x)) = (g(ax+b))$ e $deg(h(x)) = deg(h(ax+b))$.
Con questo risultato procediamo a mostrare che qualsiasi sia p primo $\sum_{i=0}^{p-1} x^i$ è irriducibile in $\mathbb{Q}[x]$. Per prima cosa osserviamo che vale la seguente uguaglianza:

$$x^p - 1 = (x-1) \cdot (\sum_{i=0}^{p-1} x^i)$$

Facendo il cambio di variabile tra x e $x+1$ otteniamo:

$$(x+1)^p - 1 = x \cdot (\sum_{i=0}^{p-1} (x+1)^i) \tag{3.1}$$

Osserviamo che per il lemma 3.3 il polinomio $\sum_{i=0}^{p-1} x^i$ è riducibile se e solo se lo è il polinomio $\sum_{i=0}^{p-1}(x+1)^i$. E noi utilizzeremo Eisenstein per mostrare che quest'ultimo è irriducibile.
Utilizzando il teorema del binomio di Newton si può scrivere $(x+1)^p$ come segue:

$$(x+1)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^i$$

Sostituendo nell'equazione 3.1 e portando fuori il termine con $i = 0$ si ha:

$$\sum_{i=1}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^i + 1 - 1 = x \cdot (\sum_{i=0}^{p-1} (x+1)^i)$$

Ovvero:

$$x \cdot \sum_{i=1}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^{i-1} = x \cdot (\sum_{i=0}^{p-1} (x+1)^i)$$

Quindi:

$$\sum_{i=1}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^{i-1} = \sum_{i=0}^{p-1} (x+1)^i \tag{3.2}$$

Osserviamo che il primo membro dell'equazione ha termine di grado massimo $p-1$ e di coefficiente 1, mentre gli altri coefficienti sono tutti multipli di p (è in questo passaggio che si usa l'ipotesi che p sia un numero primo: prova a spiegare perché!) e il termine noto (ovvero il coefficiente del termine di grado zero) è proprio p e quindi non è divisibile per p^2. Di conseguenza per il criterio di Eisenstein

$$\sum_{i=1}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^{i-1}$$

è irriducibile, ma l'equazione 3.2 ci dice che questo polinomio è uguale al polinomio

$$\sum_{i=0}^{p-1} (x+1)^i$$

che dunque è anch'esso irriducibile. □

Esercizio 3.4 (Compito d'esame 2005)**.** Sia $g(x) \in \mathbb{R}[x]$ il polinomio

$$g(x) = x^3 - 2x^2 + 2x - 1$$

(1) Fattorizzare $g(x)$ in prodotto di polinomi irriducibili.
(2) Considerato il polinomio

$$f_a(x) = x^4 - 2ax^2 + 2ax - 1$$

dimostrare che, per ogni $a \in \mathbb{R}$, un M.C.D. tra $g(x)$ e $f_a(x)$ è il polinomio $x - 1$.

Sappiamo che il polinomio $g(x)$ è riducibile in $\mathbb{R}[x]$, in quanto ha grado 3. Questo in particolare significa che $g(x)$ ha una radice reale. Osserviamo che non abbiamo studiato formule risolutive delle equazioni di secondo grado, quindi con i nostri strumenti possiamo trovare questa radice solo se è razionale (infatti il polinomio che stiamo considerando in $\mathbb{R}[x]$ è a coefficienti interi): possiamo cioè provare tutte le possibili radici razionali che otteniamo dai divisori del coefficiente direttivo e del termine noto.
Però leggendo il testo dell'esercizio non abbiamo bisogno nemmeno di questo passaggio, infatti se dobbiamo mostrare che $x-1$ è un M.C.D. di $g(x)$ con un altro polinomio, allora $x-1$ dovrà essere un divisore di $g(x)$ (e quindi 1 una radice di $g(x)$). Andiamo a verificare che $x-1$ è un fattore irriducibile di $g(x)$: che sia irriducibile è certo, visto che è di grado 1, dobbiamo mostrare che effettivamente è un divisore di $g(x)$ (se così non fosse potremmo intanto concludere che l'affermazione della seconda parte dell'esercizio è falsa). In realtà si vede subito che $x-1$ è un divisore perchè $g(1) = 1-2+2-1 = 0$, ma a noi per la fattorizzazione interessa comunque dividere i due polinomi:

$$\begin{array}{cccc|l} x^3 & -2x^2 & +2x & -1 & x-1 \\ x^3 & -x^2 & & & x^2-x+1 \\ \cline{1-3} & -x^2 & +2x & -1 & \\ & -x^2 & +x & & \\ \cline{2-3} & & x & -1 & \\ \cline{3-4} & & & 0 & \end{array}$$

Abbiamo trovato che $g(x) = (x-1)\cdot(x^2-x+1)$, a questo punto verifichiamo se x^2-x+1 è riducibile o meno in $\mathbb{R}[x]$ attraverso il calcolo del delta: essendo negativo ($\Delta = 1-4 = -3$) il polinomio è irriducibile in $\mathbb{R}[x]$ e quindi la fattorizzazione cercata è proprio:

$$g(x) = (x-1)\cdot(x^2-x+1)$$

A questo punto per dimostrare che $x-1$ è un $M.C.D.(g(x), f_a(x))$ cominciamo mostrando che $x-1$ divide $f_a(x)$ per ogni $a \in \mathbb{R}$ (e quindi è un fattore comune). Basta osservare che $f_a(1) = 1-2a+2a-1 = 0$. Ora se mostriamo che x^2-x+1 non è un divisore di $f_a(x)$ per qualsiasi scelta di a in $\mathbb{R}$, abbiamo la tesi. Procediamo dunque calcolandoci il resto della divisione di $f_a(x)$ per x^2-x+1, che sarà un polinomio $r_a(x)$ che dipenderà dal coefficiente a. Dovremo osservare che $r_a(x)$ non è uguale al polinomio nullo qualsiasi sia la scelta di a in $\mathbb{R}$:

$$\begin{array}{ccccc|l} x^4 & & -2ax^2 & +2ax & -1 & x^2-x+1 \\ x^4 & -x^3 & +x^2 & & & x^2-x-2a \\ \cline{2-3} & -x^3 & +x^2\cdot(1-2a) & +2ax & -1 & \\ & -x^3 & +x^2 & -x & & \\ \cline{3-4} & & -2a\cdot x^2 & +x\cdot(2a+1) & -1 & \\ & & -2a\cdot x^2 & +2a\cdot x & -2a & \\ \cline{4-5} & & & x & -1+2a & \end{array}$$

Osserviamo che il polinomio resto $r_a(x)$ è sempre di grado 1 qualsiasi sia la scelta di a in $\mathbb{R}$: in particolare non sarà mai uguale al polinomio nullo.

Esercizio 3.5. Dato il polinomio $g(x) = 4x^3+5x^2+3x+1$ fattorizzarlo in prodotto di irriducibili in $\mathbb{Q}[x]$ e in $\mathbb{Z}_{13}[x]$.

Sappiamo che un polinomio di grado 3 è sicuramente riducibile in $\mathbb{R}[x]$ o in $\mathbb{C}[x]$, ma non conosciamo un algoritmo per trovare questa fattorizzazione. In $\mathbb{Q}[x]$ e in $\mathbb{Z}_p[x]$ un polinomio di grado 3 non sappiamo se è riducibile o no, ma abbiamo un algoritmo finito per rispondere a questa domanda e per trovare un'eventuale fattorizzazione in irriducibili del polinomio stesso. Questo perchè, come già osservato, la riducibilità di un polinomio di grado 3 è equivalente all'esistenza di una radice nel campo e, nel caso della riducibilità in $\mathbb{Q}[x]$, se il polinomio è a coefficienti interi (come $g(x)$) abbiamo osservato che le possibili radici razionali sono un insieme finito (determinato tramite il calcolo dei divisori del termine noto e del coefficiente direttivo), mentre nel caso della riducibilità in $\mathbb{Z}_p[x]$ il numero delle possibili radici è ovviamente finito in quanto è finito il campo dei coefficienti.
I divisori del coefficiente direttivo sono $\{\pm 1, \pm 2 \pm 4\}$ mentre quelli del termine noto sono $\{\pm 1\}$, quindi le possibili radici razionali di $g(x)$ sono i numeri: $\{\pm\frac{1}{2}, \pm\frac{1}{4}, \pm 1\}$, andiamoli a provare, ma prima osserviamo che il polinomio $g(x)$ ha tutti coefficienti positivi e quindi non potrà avere radici positive: ci possiamo dunque limitare a provare, tra le possibili radici razionali, quelle negative:

$$\begin{array}{l} g(-\frac{1}{4}) = -\frac{1}{16} + \frac{5}{16} - \frac{3}{4} + 1 = \frac{1}{2} \\ g(-1) = -4 + 5 - 3 + 1 = -1 \\ g(-\frac{1}{2}) = -\frac{1}{2} + \frac{5}{4} - \frac{3}{2} + 1 = -\frac{1}{4} \end{array}$$

$g(x)$ non ha dunque radici razionali e quindi è irriducibile in $\mathbb{Q}[x]$.
Per quanto riguarda $\mathbb{Z}_{13}[x]$ valutando $g(x)$ per tutti gli elementi del campo si può verificare se esistono una o più radici. In questo caso è facile vedere che $g(1) = 13 = 0$, quindi $g(x)$ è riducibile in $\mathbb{Z}_{13}[x]$:

$$\begin{array}{llll|l} 4x^3 & +5x^2 & +3x & +1 & x-1 \\ 4x^3 & -4x^2 & & & 4x^2+9x+12 \\ \cline{1-3} & 9x^2 & +3x & +1 & \\ & 9x^2 & -9x & & \\ \cline{2-3} & & 12x & +1 & \\ & & 12x & -12 & \\ \cline{3-4} & & & +13 & \\ & & & 0 & \end{array}$$

Dunque $g(x) = (x-1)\cdot(4x^2+9x+12)$ in $\mathbb{Z}_{13}[x]$, si tratta di vedere se $4x^2+9x+12$ è irriducibile o meno in $\mathbb{Z}_13[x]$. Per questo si può procedere in due modi: o si provano tutti gli elementi di $\mathbb{Z}_{13}[x]$ alla ricerca di un'eventuale radice, oppure si osserva la formula risolutiva delle equazioni di secondo grado:

$$x_{1,2} = (2a)^{-1} \cdot (-b \pm \sqrt{\Delta})$$

Come si può notare l'inverso di $2a$ esiste perchè $\mathbb{Z}_{13}$ è un campo, quindi l'esistenza delle soluzioni in $\mathbb{Z}_{13}$ dipende dal fatto che il Δ sia un quadrato in $\mathbb{Z}_{13}$. Scegliamo questa seconda strada, il Δ in questo caso è uguale a $81 - 192 = -111$ che in $\mathbb{Z}_{13}$ è equivalente a 6. Dobbiamo controllare se 6 è un quadrato in $\mathbb{Z}_{13}$:

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 3, 5^2 = 25 = 12, 6^2 = 10$$

E qui ci possiamo fermare perchè in $\mathbb{Z}_{13}$ $7 = -6$, $8 = -5$, $9 = -4$, $10 = -3$, $11 = -2$, $12 = -1$ e quindi i loro quadrati sono identici. Si può dunque concludere che 6 non è un quadrato in $\mathbb{Z}_{13}$ e quindi $4x^2 + 9x + 12$ è irriducibile in $\mathbb{Z}_{13}[x]$.

Come ultimo esercizio di oggi vediamo la costruzione di un campo finito con p^n elementi dove p è un numero primo e n un naturale maggiore di 1 (se n è uguale a 1, sappiamo che $\mathbb{Z}_p$ è un campo con p elementi).
Avete visto a lezione che per costruire un tale campo bisogna trovare un polinomio irriducibile di grado n in $\mathbb{Z}_p[x]$.

Esercizio 3.6. Costruire un campo con 25 elementi.

Dal teorema visto a lezione sappiamo che esiste un campo con $5^2 = 25$ elementi, inoltre sappiamo che otteniamo un campo fatto in questa maniera dal quoziente di $\mathbb{Z}_5[x]$ con un polinomio irriducibile di grado 2. Approfittiamo di questo esercizio per fare una considerazione generale per la costruzione di campi finiti con p^2 elementi: osserviamo che la funzione quadrato che associa ad un elemento il suo quadrato non è iniettiva in $\mathbb{Z}_p$ (qualunque sia p primo) e quindi non è neanche surgettiva, perciò esiste almeno un elemento a di $\mathbb{Z}_p$ che non è un quadrato. Trovato questo elemento il polinomio $x^2 - a$ è irriducibile in $\mathbb{Z}_p$ perchè non ha radici.
Tornando al caso $\mathbb{Z}_5$ osserviamo che $1^2 = 1$, $2^2 = 4$, $3^2 = 9 = 4$ e $4^4 = 16 = 1$, quindi né 2 né 3 sono quadrati in $\mathbb{Z}_5$, perciò $x^2 - 2$ e $x^2 - 3$ sono sicuramente irriducibili in $\mathbb{Z}_5[x]$.
Un campo con 25 elementi sarà quindi il quoziente: $\mathbb{Z}_5[x]/(x^2 - 2)$, gli elementi di questo campo sono tutti i possibili resti di polinomi in $\mathbb{Z}_5[x]$ divisi per $x^2 - 2$, ovvero i polinomi di grado minore o uguale a 2. Gli elementi di $\mathbb{Z}_5[x]/(x^2 - 2)$ sono dunque del tipo $ax + b$ con $a, b \in \mathbb{Z}_5$. Osserviamo che per l'appunto esistono 25 diversi elementi:

0	x	$2x$	$3x$	$4x$
1	$x+1$	$2x+1$	$3x+1$	$4x+1$
2	$x+2$	$2x+2$	$3x+2$	$4x+2$
3	$x+3$	$2x+3$	$3x+3$	$4x+3$
4	$x+4$	$2x+4$	$3x+4$	$4x+4$

Ricordiamo che gli elementi di $\mathbb{Z}_5[x]/(x^2 - 2)$ sono classi di equivalenza modulo $x^2 - 2$, ovvero nella classe di x (che scegliamo come rappresentante perchè è quello di grado minore) ci stanno tutti i polinomi di $\mathbb{Z}_5[x]$ che differiscono da x per un multiplo di $x^2 - 2$ (per esempio $x^2 + x - 2$).
Sappiamo che $\mathbb{Z}_5[x]/(x^2-2)$ è un campo, ma se alcune proprietà sono ovvie (esistenza di elementi neutri, 0 per la somma e 1 per il prodotto, proprietà delle operazioni che continuano a valere come valevano su $\mathbb{Z}_5[x]$) non è immediato capire dato un elemento quale sia il suo opposto e il suo inverso (che in un campo sappiamo esistere per ogni elemento diverso da 0). Proviamo per esempio con l'elemento x:

- Opposto di x: Dobbiamo trovare un elemento di $\mathbb{Z}_5[x]/(x^2-2)$ che sommato a x sia uguale all'elemento 0. Prendiamo un generico elemento $ax + b$ di $\mathbb{Z}_5[x]/(x^2 - 2)$ sommiamolo a x e imponiamo che questo sia uguale a 0 per trovare a e b:

$$x + (ax + b) = x \cdot (1 + a) + b = 0 \Leftrightarrow \begin{cases} 1 + a = 0 \\ b = 0 \end{cases} \Leftrightarrow \begin{cases} a = -1 = 4 \\ b = 0 \end{cases}$$

  Quindi l'opposto di x in $\mathbb{Z}_5[x]/(x^2 - 2)$ è $4x$ $(x + 4x = 5x = 0)$.
- Inverso di x: Dobbiamo trovare un elemento $ax + b$ di $\mathbb{Z}_5[x]/(x^2 - 2)$ che moltiplicato a x sia uguale all'elemento 1, ovvero $x \cdot (ax + b) = ax^2 + bx$ diviso per $x^2 - 2$ deve dare resto 1. Impostiamo la divisione e imponiamo

che il resto sia 1 per trovare a e b e quindi il polinomio inverso di x:

$$\begin{array}{llll} ax^2 & +bx & & | \quad x^2-2 \\ ax^2 & & -2a & | \quad a \\ & bx & +2a & \end{array}$$

Da questa divisione segue che la classe di ax^2+bx in $\mathbb{Z}_5[x]/(x^2-2)$ è $bx+2a$. Imporre che questa sia uguale a 1 significa, per il principio di identità dei polinomi, imporre $b=0$ e $2a=1$ ovvero $3\cdot 2a = 6a = a = 3\cdot 1 = 3$. Quindi l'inverso di x in $\mathbb{Z}_5[x]/(x^2-2)$ è $3x$. La riprova è che $x\cdot 3x = 3x^2$ che diviso per x^2-2 dà resto 6 che in $\mathbb{Z}_5$ è nella stessa classe di 1.

Per esercizio provare a calcolare qualche altro opposto e inverso di elementi di $\mathbb{Z}_5[x]/(x^2-2)$. Osserviamo che l'essere l'opposto (o l'inverso) di un elemento è una relazione simmetrica essendo in campi commutativi: cioè se a è l'inverso di b allora b è l'inverso di a.

4. Esercizitazione 9 marzo 2006

Esercizio 4.1. Dimostrare che l'anello dei polinomi $\mathbb{K}[x]$ è uno spazio vettoriale su $\mathbb{K}$ con la somma tra polinomi e il prodotto tra polinomi e costanti di $\mathbb{K}$ definite nel modo usuale.

Esercizio 4.2. Dimostrare che l'insieme dei polinomi a coefficienti in $\mathbb{K}$ di grado minore o uguale di n (che indicheremo con $\mathbb{K}_n[x]$) è un sottospazio vettoriale di $\mathbb{K}[x]$ qualsiasi sia $n \in \mathbb{N}$[5].
Qualsiasi sia n, abbiamo per definizione di $\mathbb{K}_n[x]$ (vedi nota) che il polinomio nullo appartiene a $\mathbb{K}_n[x]$, ci rimane quindi da verificare che $\mathbb{K}_n[x]$ sia chiuso per somma e per prodotto per scalare, ma questo segue banalmente dalle proprietà del grado, infatti:

- $deg(p(x) + q(x)) \leq max(deg(p(x)), deg(q(x)))$ quindi se $p(x)$ e $q(x)$ appartengono a $\mathbb{K}_n[x]$, allora $p(x) + q(x)$ ha grado minore o uguale a n e quindi anch'esso appartiene a $\mathbb{K}_n[x]$.
- Sia $p(x) \in \mathbb{K}_n[x]$, se $\lambda = 0$ allora sappiamo che $\lambda \cdot p(x) = 0 \in \mathbb{K}_n[x]$. Altrimenti se $\lambda \in \mathbb{K}$ è diverso da zero si ha che:

  $$deg(\lambda \cdot p(x)) = deg(\lambda) + deg(p(x)) = 0 + deg(p(x)) = deg(p(x)) \leq n$$

  e quindi per ogni $\lambda \in \mathbb{K}$ si ha che $\lambda \cdot p(x) \in \mathbb{K}_n[x]$.

Esercizio 4.3. Dire quali dei seguenti sottoinsiemi di $\mathbb{R}_n[x]$ sono sottospazi vettoriali di $\mathbb{R}_n[x]$:

(1) $V_1 = \{p(x) \in \mathbb{R}_n[x] | p(2) = 0\}$
(2) $V_2 = \{p(x) \in \mathbb{R}_n[x] | p(1) = 1\}$
(3) $V_3 = \{p(x) \in \mathbb{R}_n[x] | \sum_{i=0}^{n} a_i x^i, \quad a_i \in \mathbb{Z}\}$
(4) $V_4 = \{p(x) \in \mathbb{R}_n[x] | p(1) = -p(2)\}$
(5) $V_5 = \{p(x) \in \mathbb{R}_n[x] | \sum_{i=0}^{[n/2]} a_{2i} x^{2i}\}$ Dove con $[n/2]$ indichiamo la parte intera di $n/2$.

(1) La dimostrazione che V_1 sia un sottospazio vettoriale di $\mathbb{R}_n[x]$ ricalca quella vista nell'esempio trattato a lezione con radice uguale a 1 (vedi note integrative). È ovvio che le proprietà dimostrate non dipendono dalla radice scelta. In generale l'insieme dei polinomi di $\mathbb{K}[x]$ che hanno una radice k in $\mathbb{K}$ è dunque uno spazio vettoriale, osserviamo che questo insieme equivale all'insieme dei polinomi di $\mathbb{K}[x]$ che sono divisibili per $x - k$.
(2) V_2 è un insieme che non verifica nessuna delle tre proprietà che definiscono un sottospazio vettoriale, ma per dimostrare che non è un sottospazio vettoriale basta osservarne una (per esercizio mostrare anche che non verifica le altre) e in particolare quella più semplice da verificare, ovvero che il polinomio 0 non appartiene a V_2. Infatti tale polinomio valutato in qualsiasi elemento vale sempre 0 e non potrà mai essere uguale a 1.
(3) V_3 è l'insieme dei polinomi di grado minore o uguale a n a coefficienti in $\mathbb{Z}$. Il polinomio 0 appartiene a V_3 e la somma di due polinomi a coefficienti interi è un polinomio a coefficienti interi: quindi V_3 è chiuso per la somma. *Sfortunatamente* però V_3 non è chiuso per prodotto scalare infatti sia $p(x) \in$

[5] In realtà qui insorge un problema non avendo definito il grado per il polinomio nullo. Spesso si trova definito il grado del polinomio nullo uguale a $-\infty$, possiamo adottare questa convenzione, oppure anche considerare $\mathbb{K}_n[x]$ come l'insieme di tutti i polinomi di grado minore o uguale a n, a cui aggiungiamo il polinomio nullo.

V_3, se scegliamo un qualsiasi numero reale a che non sia intero e nemmeno razionale (per essere sicuri che non ci siano semplificazioni), per esempio $\sqrt{2}$, allora $a \cdot p(x)$ è un polinomio non a coefficienti interi. Quindi V_3 non è sottospazio vettoriale di $\mathbb{R}_n[x]$.

(4) 0 appartiene a V_4 infatti: $p(1) = 0 = -p(2) = 0$. Siano $p(x)$ e $g(x)$ polinomi di V_4 allora valutiamo la loro somma e la moltiplicazione di uno dei due per uno scalare $r \in \mathbb{R}$ e verifichiamo se continua a valere la proprietà che definisce V_4:

$$(p+g)(1) = p(1) + g(1) \underbrace{=}_{p(x)\in V_4,\ g(x)\in V_4} -p(2) - g(2) = -(p+g)(2)$$

$$(r \cdot p)(1) = r \cdot p(1) \underbrace{=}_{p(x)\in V_4} r \cdot (-p(2)) = -(r \cdot p)(2)$$

Quindi V_4 è un sottospazio vettoriale di $\mathbb{R}_n[x]$.

(5) V_5 è il sottoinsieme di $\mathbb{R}_n[x]$ dei polinomi che hanno solo monomi di grado pari o equivalentemente tutti i coefficienti dei termini di grado dispari sono uguali a zero. Questa seconda *versione* mostra che il polinomio 0 appartiene a V_5. Ora osserviamo che la somma tra due polinomi è definita facendo le somme tra monomi dello stesso grado, quindi se sommiamo due polinomi con solo monomi di grado pari otteniamo un polinomio formato solo da monomi di grado pari. È banale osservare che V_5 è chiuso anche per prodotto scalare e quindi è un sottospazio vettoriale di $\mathbb{R}_n[x]$.

Lemma 4.4. *Sia V uno spazio vettoriale su un campo $\mathbb{K}$, U e W due sottospazi di V, allora $U \cap W$ è un sottospazio vettoriale di V.*

Dim. Dobbiamo mostrare che $U \cap W$ verifica le proprietà della definizione di sottospazio:

(1) $O \in U \cap W$, infatti essendo U e W due sottospazi, certamente $O \in U$ e $O \in W$.

(2) Siano $v_1, v_2 \in U \cap W$ allora:

$$\begin{cases} \underbrace{v_1 + v_2 \in U}_{U \text{ è sottospazio}} \\ \underbrace{v_1 + v_2 \in W}_{W \text{ è sottospazio}} \end{cases} \Rightarrow \quad v_1 + v_2 \in U \cap W$$

(3) Sia $v \in U \cap W$ allora per ogni $\lambda \in \mathbb{K}$ si ha:

$$\begin{cases} \underbrace{\lambda \cdot v \in U}_{U \text{ è sottospazio}} \\ \underbrace{\lambda \cdot v \in W}_{W \text{ è sottospazio}} \end{cases} \Rightarrow \quad \lambda \cdot v \in U \cap W \qquad \square$$

Definizione 4.5. Dati $\{v_1, v_2, \ldots, v_k\}$ vettori di V si definisce $Span(v_1, v_2, \ldots, v_k)$ l'insieme di tutte le possibili combinazioni lineari dei $\{v_1, v_2, \ldots, v_k\}$.

Esempio 4.6. Dimostrare che per ogni n e ogni scelta di vettori $\{v_1, v_2, \ldots, v_k\}$ di V si ha che $Span(v_1, v_2, \ldots, v_k)$ è un sottospazio vettoriale[6] di V.

[6]Non è detto che sia un sottospazio proprio.

Osservazione 4.7. Osserviamo che se $v_1, \ldots, v_n$ è un insieme di vettori linearmente indipendenti allora anche $\lambda \cdot v_1, \ldots, v_n$ è un insieme di vettori linearmente indipendenti, qualsiasi sia $\lambda \in \mathbb{K}\backslash\{0\}$ (perchè?). Dalla dimostrazione del teorema mostrato a lezione sulla possibilità di estrarre una base da un insieme di generatori segue che ogni sottoinsieme massimale di $\mathcal{M}$ è una base di V, quindi la base di uno spazio vettoriale non è unica. Se infatti $v_1, \ldots, v_n$ è una base di V allora anche $\lambda \cdot v_1, \ldots, v_n$ è una base di V, qualsiasi sia $\lambda \in \mathbb{K}\backslash\{0\}$.

Esercizio 4.8. Dimostrare che $\mathbb{K}_n[x]$ (che sappiamo dall'esercizio 4.2 essere un sottospazio vettoriale di $\mathbb{K}[x]$) è di dimensione finita $n+1$. (Suggerimento: mostrare che $\{1, x, x^2, \ldots, x^n\}$ è una base).

Esercizio 4.9. Consideriamo il seguente sottoinsieme di $\mathbb{Q}[x]$:

$$W = \{p(x) \in \mathbb{Q}[x] | deg(p(x)) \leq 3 \text{ e } p(x) \text{ è divisibile per } (x-4)\}$$

(1) Dimostrare che W è sottospazio vettoriale di $\mathbb{Q}[x]$.
(2) Trovare una base di W.

(1) Per dimostrare che W è un sottospazio di $\mathbb{Q}[x]$ basta osservare che W è l'intersezione di due sottospazi di $\mathbb{Q}[x]$, ovvero U l'insieme dei polinomi di grado minore o uguale a 3 e V l'insieme dei polinomi divisibili per $x-4$ (o equivalentemente che si annullano in 4).
(2) Un polinomio $p(x)$ di W è per definizione del tipo:

$$\underbrace{(x-4)}_{divisibile\ per\ x-4} \cdot \underbrace{(ax^2+bx+c)}_{di\ grado\ \leq 3} \qquad a, b, c \in \mathbb{Q}$$

Ovvero:

$$p(x) = ax^2(x-4) + bx(x-4) + c(x-4)$$

Quindi $\{(x-4),\ x(x-4),\ x^2(x-4)\}$ è un insieme di generatori di W, è facile dimostrare che questi tre vettori sono anche linearmente indipendenti (come del resto tutti gli insiemi di polinomi composti da polinomi che confrontati a due a due hanno tutti grado diverso). Quindi $\{(x-4),\ x(x-4),\ x^2(x-4)\}$ è una base di W, che abbiamo scoperto avere dimensione 3.[7]

Esercizio 4.10. Sia W il sottospazio di $\mathbb{R}^3$ generato dai vettori: $(1, -1, 0)$ e $(b-1, b+1, -b)$ (con $b \in \mathbb{R}$) e U il sottoinsieme di $\mathbb{R}^3$ definito da:

$$U = \{(x, y, z \in \mathbb{R}^3 | x + y + 2z = 0\}$$

(1) Dimostrare che U è sottospazio di $\mathbb{R}^3$.
(2) Calcolare la dimensione di U e al variare di $b \in \mathbb{R}$ la dimensione di W.
(3) Calcolare, al variare di $b \in \mathbb{R}$, la dimensione di $U \cap W$.

(1) È ovvio che il vettore $(0, 0, 0)$ appartiene ad U infatti: $0 + 0 + 2 \cdot 0 = 0$. Siano (x_1, y_1, z_1) e (x_2, y_2, z_2) due vettori di U e consideriamo:

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$$

e

$$\lambda \cdot (x_1, y_1, z_1) = (\lambda x_1, \lambda y_1, \lambda z_1)$$

[7] In generale è facile osservare che la dimensione di uno spazio intersezione $U \cap V$ è minore o uguale della minima dimensione tra U e V.

al variare di λ in $\mathbb{R}$. Dobbiamo mostrare che questi due elementi appartengono ancora ad U, ma la verifica è del tutto banale infatti:

$$(x_1 + x_2) + (y_1 + y_2) + 2(z_1 + z_2) = \underbrace{x_1 + y_1 + 2z_1}_{=0} + \underbrace{x_2 + y_2 + 2z_2}_{=0} = 0$$

e

$$\lambda x_1 + \lambda y_1 + 2\lambda z_1 = \lambda \underbrace{(x_1 + y_1 + 2z_1)}_{=0} = 0$$

(2) Faremo di più di determinare la dimensione di U: ne cercheremo una base. Il sottospazio U è determinato dalla condizione $x + y + 2z$ che ha due gradi di libertà, ovvero se fissiamo un valore s alla variabile z e un valore t alla variabile y abbiamo che il valore di x è univocamente determinato ed è uguale a $-t - 2s$, si ha cioè:

$$\begin{cases} y = s \\ z = t \\ x = -t - 2s \end{cases}$$

e quindi ogni vettore (x, y, z) di U è del tipo:

$$(-t - 2s, t, s) = (-1, 0, 1) \cdot t + (-2, 1, 0) \cdot s$$

cioè $\{(-1, 0, 1), (-2, 1, 0)\}$ è un insieme di generatori di U (quindi la dimensione di U è minore o uguale a 2). È facile mostrare che i due vettori sono anche linearmente indipendenti e quindi $\{(-1, 0, 1), (-2, 1, 0)\}$ è una base di U e $\dim(U) = 2$.
Per quanto riguarda W bisogna capire al variare di $b \in \mathbb{R}$ se i due vettori $(1, -1, 0)$ e $(b - 1, b + 1, -b)$ siano linearmente indipendenti (e quindi una base di W) oppure linearmente dipendenti (e quindi $\dim(W) = 1$ e una sua base è composta da uno dei due vettori):

$$h \cdot (1, -1, 0) + l \cdot (b - 1, b + 1, -b) = (0, 0, 0)$$

Otteniamo il sistema:

$$\begin{cases} h + l \cdot (b - 1) = 0 \\ -h + l \cdot (b + 1) = 0 \\ -bl = 0 \end{cases}$$

Se $b \neq 0$ allora l deve essere uguale a zero e di conseguenza anche $h = 0$. Quindi se $b \neq 0$ i due vettori $(1, -1, 0)$ e $(b - 1, b + 1, -b)$ sono linearmente indipendenti e formano una base di W che risulta essere uno spazio vettoriale di dimensione 2. Se $b = 0$ allora il sistema diventa:

$$\begin{cases} h - l = 0 \\ -h + l = 0 \\ 0 = 0 \end{cases}$$

Che è risolto per ogni scelta di $h = l$ e quindi $(1, -1, 0)$ e $(b - 1, b + 1, -b)$ sono linearmente dipendenti e W ha dimensione uno.

(3) Osserviamo che i generatori di W stanno in U infatti:

$$1 - 1 + 2 \cdot 0 = 0 \quad (b - 1) + (b + 1) + 2 \cdot (-b) = 2b - 2b = 0$$

Quindi $W \subseteq Q$ e $W \cap Q = W$. Perciò abbiamo già trovato la dimensione di $W \cap U$ nel punto precedente.

5. Esercizitazione 16 marzo 2006

In questa lezione abbiamo affrontato esercizi sulle applicazioni lineari tra due spazi vettoriali, in particolare abbiamo usato l'osservazione fatta a lezione per associare ad una applicazione lineare L dal $\mathbb{K}$-spazio vettoriale V al $\mathbb{K}$-spazio vettoriale W (a partire da due basi $ß_1$ e $ß_2$ di V e W rispettivamente degli spazi vettoriali) una matrice detta matrice associata a L rispetto alle basi $ß_1$ e $ß_2$ di V e W.

Esercizio 5.1. Si consideri la trasformazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^2$ definita sulle coordinate rispetto alle basi canoniche di $\mathbb{R}^3$ e $\mathbb{R}^2$ da:

$$L\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x - 2y - z \\ x + y + z \end{pmatrix}$$

(1) Scrivere la matrice associata ad L rispetto alle basi canoniche di $\mathbb{R}^3$ e $\mathbb{R}^2$.
(2) Determinare una base di $Ker(L)$ e $Imm(L)$.

Innanzitutto l'esercizio dichiara che L è un'applicazione lineare (in effetti è facile provare che lo sono tutte le applicazioni da $\mathbb{R}^n$ a $\mathbb{R}^m$ che *agiscono* sulle coordinate in maniera che il risultato sia una combinazione lineare delle stesse), ma per questa prima volta, proviamo che effettivamente L ha le caratteristiche per essere definita un'applicazione *lineare*, ovvero:

- $\forall\ v, w \in \mathbb{R}^3$ si ha che $L(v + w) = L(v) + L(w)$. Controlliamo che sussista questa uguaglianza, siano (x_1, y_1, z_1) e (x_2, y_2, z_2) le coordinate di v e w rispettivamente allora: $(v + w) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$ quindi:

$$L(v+w) = L\begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{pmatrix} = \begin{pmatrix} (x_1 + x_2) - 2(y_1 + y_2) - (z_1 + z_2) \\ (x_1 + x_2) + (y_1 + y_2) + (z_1 + z_2) \end{pmatrix}$$

  Mentre:

$$L(v)+L(w) = \begin{pmatrix} x_1 - 2y_1 - z_1 \\ x_1 + y_1 + z_1 \end{pmatrix} + \begin{pmatrix} x_2 - 2y_2 - z_2 \\ x_2 + y_2 + z_2 \end{pmatrix} = \begin{pmatrix} (x_1 + x_2) - 2(y_1 + y_2) - (z_1 + z_2) \\ (x_1 + x_2) + (y_1 + y_2) + (z_1 + z_2) \end{pmatrix}$$

- $\forall\ v \in V$ e $\forall\ k \in \mathbb{K}$ si ha che $L(k \cdot v) = k \cdot L(v)$. Anche in questo caso andiamo a provare questa uguaglianza:

$$L(k \cdot v) = L\begin{pmatrix} k \cdot x \\ k \cdot y \\ k \cdot z \end{pmatrix} = \begin{pmatrix} k \cdot x - 2k \cdot y - k \cdot x \\ k \cdot x + k \cdot y + k \cdot z \end{pmatrix}$$

  Mentre:

$$k \cdot L(v) = k \cdot \begin{pmatrix} x - 2y - z \\ x + y + z \end{pmatrix} = \begin{pmatrix} k \cdot x - 2k \cdot y - k \cdot x \\ k \cdot x + k \cdot y + k \cdot z \end{pmatrix}$$

E ora passiamo alle richieste vere e proprie dell'esercizio:

(1) Per scrivere una matrice associata a L bisogna fissare una base ordinata[8] per ognuno dei due spazi. In questo caso le basi sono state fissate, prendiamo come basi ordinate di $\mathbb{R}^2$ e di $\mathbb{R}^3$ rispettivamente:

$$ß_{\mathbb{R}^2} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

[8]Ordinata, perchè per la costruzione della matrice è importante anche l'ordine in cui si considerano gli elementi delle due basi.

$$ß_{\mathbb{R}^3} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Per scrivere la matrice associata a L rispetto a queste basi bisogna calcolare l'immagine degli elementi di $ß_{\mathbb{R}^3}$ tramite L (Sappiamo anche che questi elementi costituiscono un insieme di generatori per $Imm(L)$, questo ci servirà al punto successivo). Le coordinate di questi elementi (che sono di $\mathbb{R}^2$) rispetto alla base $ß_{\mathbb{R}^2}$ ci forniscono le colonne della matrice associata a L:

$$L\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \quad L\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}; \quad L\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Perciò la matrice $A_{ß_{\mathbb{R}^3}, ß_{\mathbb{R}^2}}$ associata a L nelle basi suddette è la seguente:

$$A_{ß_{\mathbb{R}^3}, ß_{\mathbb{R}^2}} = \begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

(2) Sappiamo che $Imm(L)$ è generata dai vettori $\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} -2 \\ 1 \end{pmatrix}; \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, ma sappiamo anche che questi non saranno una base (infatti $\mathbb{R}^2$ ha dimensione 2 e quindi $Imm(L)$ avrà al massimo dimensione 2), per trovare una base di $Imm(L)$ possiamo portare in forma a scala per colonna la matrice $A_{ß_{\mathbb{R}^3}, ß_{\mathbb{R}^2}}$. Sappiamo infatti che sommando una colonna per una combinazione lineare delle altre non cambiamo $Imm(L)$. La forma a scala però, rispetto a quella che abbiamo, permette di individuare immediatamente, tra l'insieme dei generatori di $Imm(L)$ (le colonne della matrice), un sottoinsieme massimo di vettori linearmente indipendenti, cioè una base[9]. Procediamo quindi con sostituzioni delle colonne come segue:

$$\begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix} \overbrace{\longrightarrow}^{2a=2a+2\cdot 1a} \begin{pmatrix} 1 & 0 & -1 \\ 1 & 3 & 1 \end{pmatrix} \overbrace{\longrightarrow}^{3a=3a+1a-\frac{2}{3}\cdot 2a} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \end{pmatrix}$$

Quindi una base di $Imm(L)$ è data dai due vettori $\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} 0 \\ 3 \end{pmatrix}$. Possiamo osservare che avendo $Imm(L)$ dimensione 2, si ha che $Imm(L) = \mathbb{R}^2$ e quindi L è un'applicazione surgettiva.
Per trovare una base di $Ker(L)$, cerchiamo di capire come sono fatti i suoi elementi. Per definizione un vettore v sta in $Ker(L)$ se $L(v) = 0$. Questo si traduce nel seguente sistema nelle coordinate x, y, z di v:

$$\begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Ovvero abbiamo il sistema:

$$\begin{cases} x - 2y - z = 0 \\ x + y + z = 0 \end{cases} \tag{5.1}$$

[9]Facciamo notare che in un caso come questo è molto semplice individuare un insieme massimo di vettori linearmente indipendenti a prescindere dalla riduzione a scala della matrice. Il procedimento che presentiamo quindi non è finalizzato per risolvere questo esercizio in particolare, ma per dare un **metodo generale** per risolvere problemi di questo genere.

Osserviamo che, in generale, risolvere un sistema di questo tipo (lineare nelle variabili) si riduce a *lavorare* sui coefficienti delle variabili coinvolte, possiamo quindi associare ad un sistema siffatto una matrice di dimensione $n \times m$ (dove n è il numero di equazioni del sistema e m il numero di variabili) che ha nella i-esima colonna i coefficienti della i-esima variabile e nell'ultima colonna i termini noti. Otteniamo quindi una matrice 2×4 ottenuta da $A_{\mathcal{B}_{\mathbb{R}^3},\mathcal{B}_{\mathbb{R}^2}}$ a cui abbiamo aggiunto all'ultima colonna i termini noti (in questo caso due zeri):

$$\begin{pmatrix} 1 & -2 & -1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Questa matrice viene chiamata matrice completa associata al sistema lineare 5.1, mentre la matrice senza la colonna dei termini noti (nel nostro caso $A_{\mathcal{B}_{\mathbb{R}^3},\mathcal{B}_{\mathbb{R}^2}}$) è detta matrice incompleta associata al sistema 5.1. Osserviamo che nel caso di un sistema omogeneo (ovvero con termini noti tutti uguali a zero) qualsiasi manipolazione del sistema attraverso sostituzione di una riga con la somma della stessa per una combinazione lineare delle altre lascia inalterata l'ultima colonna della matrice. Possiamo dunque, nel caso di sistemi omogenei (che sono quelli che vengono fuori nello studio di Ker di applicazioni lineari), lavorare sulla matrice incompleta (che nel caso di applicazioni lineari non è altro che la matrice associata alla applicazione lineare stessa).
Probabilmente sapete già risolvere sistemi di questo tipo, ma cerchiamo di dare un *algoritmo*. L'idea è quella solita, ricavarsi una variabile, sostituire nelle altre equazioni, etc., etc. Quello che si fa è di lavorare su un sistema equivalente (cioè con lo stesso insieme di soluzioni di quello di partenza). Vogliamo stabilire un sistema equivalente particolarmente adatto per le nostre esigenze è quindi cercare di arrivare a quello: il sistema in questione è quello corrispondente alla matrice ottenuta dalla matrice incompleta del sistema 5.1 ridotta a scala per righe. Andiamo quindi a ridurre $A_{\mathcal{B}_{\mathbb{R}^3},\mathcal{B}_{\mathbb{R}^2}}$ per riga, ovvero operando sulle righe della matrice:

$$\begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix} \overset{2a=2a-1a}{\longrightarrow} \begin{pmatrix} 1 & -1 & -1 \\ 0 & 3 & 2 \end{pmatrix}$$

Chiamiamo le entrate non zero delle righe (1 nella prima riga e 3 nella seconda) pivot della matrice ridotta a scala. Il sistema corrispondente a questa matrice è:

$$\begin{cases} x - 2y - z = 0 \\ 3y + 2z = 0 \end{cases} \tag{5.2}$$

Risolviamo il sistema trovando le variabili corrispondenti a dove sono i pivot nella matrice a scala (nel nostro caso i pivot sono nella prima e seconda colonna, quindi le variabili corrispondenti sono la prima e la seconda: nella nostra notazione x e y) rispetto alle altre (nel nostro caso z) e troviamo:

$$\begin{cases} x = 2 \cdot (-\frac{2}{3}z) + z = -\frac{1}{3}z \\ y = -\frac{2}{3}z \end{cases}$$

Abbiamo risolto il sistema[10] e dunque sappiamo che i vettori che stanno in $Ker(L)$ sono della forma:

$$\begin{pmatrix} -\frac{1}{3}z \\ -\frac{2}{3}z \\ z \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ 1 \end{pmatrix} \cdot z$$

Quindi il vettore:

$$\begin{pmatrix} -\frac{1}{3} \\ -\frac{2}{3} \\ 1 \end{pmatrix}$$

genera $Ker(L)$ e ne è dunque anche una base. In particolare L non è iniettiva perché $Ker(L)$ non è composto dal solo vettore nullo.

Osservazione 5.2. Dallo svolgimento dell'esercizio precedente segue che determinare il nucleo di un'applicazione lineare $L : V \to W$ (tra due spazi di dimensione finita) consiste nel risolvere un sistema lineare omogeneo con n variabili (dove n è la dimensione di V). Abbiamo anche trovato che la dimensione del nucleo è uguale al numero di *variabili libere* del sistema lineare omogeneo: ovvero al numero n delle variabili meno il numero dei pivot trovati sulla forma a scala della matrice associata al sistema lineare omogeneo. Avendo dimostrato che la dimensione di uno spazio vettoriale è invariante, ed essendo il numero di variabili del sistema anch'esso fissato, da questo si può indurre che il numero dei pivot di una matrice è invariante: cioè non dipende dalle particolari scelte fatte per portare la matrice nella forma a scala.

Esercizio 5.3. Si consideri l'applicazione lineare $A_t : \mathbb{R}^4 \to R^3$, al variare di $t \in \mathbb{R}$, che associa a $v \in \mathbb{R}^4$ il vettore $A_t \cdot v$ ottenuto moltiplicando v a destra della matrice seguente:

$$A_t = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & 0 \\ t & t^3 & 1+t & 1 \end{pmatrix}$$

Trovare, se esistono, valori del parametro t per i quali si ha che: $dim(Ker(A_t)) = 2$.

Dall'osservazione 5.2 segue che il nucleo di A_t ha dimensione 2 se e solo se portando in forma a scala A_t troviamo due pivot.
Facciamo una rapida analisi della matrice in questione: le due prime righe sono sicuramente linearmente indipendenti, perciò il numero di pivot è almeno 2 e al massimo sarà 3 (ci sono solo tre righe).
Portiamo A_t a scala:

$$\begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & 0 \\ t & t^3 & 1+t & 1 \end{pmatrix} \overbrace{\longrightarrow}^{2a=2a-1a} \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ t & t^3 & 1+t & 1 \end{pmatrix} \overbrace{\longrightarrow}^{3a=3a-t\cdot 1a} \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & t^3-t & 1-t & 1-t \end{pmatrix}$$

Osservazione 5.4. Prima di procedere osserviamo che nel secondo passaggio abbiamo scambiato la terza riga con la terza riga meno t volte la prima riga. E se t fosse zero? Il problema non sussiste, in quanto vorrebbe dire non avere fatto nulla: ovvero aver sostituito alla terza riga la terza riga! Diverso sarebbe stato se avessimo sostituito alla prima riga la stessa combinazione, in questo caso infatti dobbiamo stare attenti a non *cancellare* informazioni. Se t fosse 0 sostituiremmo alla prima

[10] Trovando che ci sono infinite soluzioni, una per ogni scelta di z. Solitamente in questo caso si dice che cè una variabile libera, appunto z.

riga la terza riga, ovvero perderemmo *per sempre* le informazioni sulla prima riga. Si deve perciò stare attenti a non sostituire al posto di una riga un suo multiplo senza controllare che questo multiplo sia diverso da zero.

A questo punto affinché la matrice abbia due pivot è necessario che l'ultima riga non abbia entrate non nulle prima della quarta colonna, ovvero che:

$$t^3 - t = 1 - t = 0$$

Che è risolto solo da $t = 1$. Si ha quindi che A_1 è l'unica applicazione del tipo considerato che ha il nucleo di dimensione 2. Proviamo a trovare una base di $Ker(A_1)$, sappiamo già che il sistema omogeneo:

$$A_1 \cdot \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

ha matrice a scala della forma:

$$\begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Quindi dobbiamo risolvere il sistema trovando le variabili x e w in funzione delle variabili libere y e z:

$$\begin{cases} x + y + 2z + w = 0 \\ -w = 0 \\ 0 = 0 \end{cases}$$

Troviamo $w = 0$ e $x = -y-2z$ quindi un generico vettore di $Ker(A_1)$ è della forma:

$$\begin{pmatrix} -y - 2z \\ y \\ z \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \cdot y + \begin{pmatrix} -2 \\ 0 \\ 1 \\ 0 \end{pmatrix} \cdot z$$

E i due vettori:

$$\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}; \begin{pmatrix} -2 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

sono un insieme di generatori linearmente indipendenti (quindi una base) di $Ker(A_1)$.

Esercizio 5.5. Sia $g : \mathbb{Q}^3 \to \mathbb{Q}^2$ definita da:

$$g(x, y, z) = (2x + y + 2z, x + y + 3z)$$

Trovare una base di $Imm(g)$ e di $Ker(g)$.

La matrice associata a g nelle basi canoniche di $\mathbb{Q}^3$ e $\mathbb{Q}^2$ è:

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

Portiamola in forma a scala:

$$G \overbrace{\longrightarrow}^{2a=2\cdot 2a-1a} \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 4 \end{pmatrix}$$

Da questo segue che una base di $Imm(G)$ è data da:

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix}; \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Gli elementi di $Ker(g)$ sono le soluzioni del sistema:

$$\begin{cases} 2x + y + 2z = 0 \\ y + 4z = 0 \end{cases}$$

Da risolvere in funzione della variabile libera z, quindi: $y = -4z$ e $x = z$. Perciò un generico elemento di $Ker(g)$ è della forma:

$$\begin{pmatrix} z \\ -4z \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ -4 \\ 1 \end{pmatrix} \cdot z$$

Dunque $Ker(g)$ ha dimensione uno e una sua base è data dal vettore:

$$\begin{pmatrix} 1 \\ -4 \\ 1 \end{pmatrix}$$

6. Esercizitazione 23 marzo 2006

Esercizio 6.1. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema in $\mathbb{Z}_5$:

$$\begin{cases} x_1 - x_2 + x_3 + x_4 = 1 \\ x_2 - x_4 = 0 \\ x_3 + x_4 = 1 \end{cases} \tag{6.1}$$

La matrice completa associata al sistema 6.1 è:

$$A = \begin{pmatrix} 1 & -1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

che è già in forma a scala. I pivots sono 3, nessuno dei quali nell'ultima colonna, quindi il sistema è risolubile. L'unica variabile libera è x_4, quindi troveremo le soluzioni del sistema in funzione di x_4 e avremo 5 soluzioni distinte, una per ogni scelta possibile di x_4 in $\mathbb{Z}_5$:

$$\begin{cases} x_1 = x_4 - (1 - x_4) - x_4 + 1 \\ x_2 = x_4 \\ x_3 = 1 - x_4 \end{cases} \longrightarrow \begin{cases} x_1 = x_4 \\ x_2 = x_4 \\ x_3 = 1 - x_4 \end{cases}$$

Le soluzioni del sistema sono dunque del tipo $(x_4, x_4, 1 - x_4, x_4)$ per ogni scelta di x_4 in $\mathbb{Z}_5$.

Esercizio 6.2. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema in $\mathbb{Z}_7$:

$$\begin{cases} x_1 + x_2 - x_3 = 1 \\ x_1 + x_3 = 0 \\ x_1 + x_2 + x_3 = 0 \end{cases} \tag{6.2}$$

La matrice completa associata al sistema 6.2 è:

$$A = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & 0 \end{pmatrix}$$

Portiamola in forma a scala con sostituzioni lineari (ribadiamo che la scelta delle sostituzioni lineari da effettuare per portare la matrice a scala non è univoca):

$$A \overset{(2a)=(2a)-(1a)}{\overbrace{\longrightarrow}} A_1 = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & -1 & 2 & -1 \\ 1 & 1 & -1 & 0 \end{pmatrix} \overset{(3a)=(3a)-(1a)}{\overbrace{\longrightarrow}} A_2 = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

La matrice A_2 è in forma a scala ed ha un pivot nell'ultima colonna quindi il sistema 6.2 è impossibile perchè equivalente a:

$$\begin{cases} x_1 & +x_2 & -x_3 & = 1 \\ & -x_2 & +2x_3 & = -1 \\ & & 0 & = -1 \end{cases}$$

Esercizio 6.3. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema in $\mathbb{Q}$:

$$\begin{cases} x_1 - 3x_2 + x_3 + 2x_4 = 0 \\ 2x_1 - 6x_2 + x_3 + 5x_4 = 1 \\ 3x_1 - 9x_2 + 2x_3 + 10x_4 = 4 \end{cases} \tag{6.3}$$

La matrice completa associata al sistema 6.3 è:

$$A = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 2 & -6 & 1 & 5 & 1 \\ 3 & -9 & 2 & 10 & 4 \end{pmatrix}$$

Portiamola in forma a scala con sostituzioni lineari:

$$A \overset{(2a)=(2a)-2\cdot(1a)}{\overbrace{\longrightarrow}} A_1 = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 3 & -9 & 2 & 10 & 4 \end{pmatrix}$$

$$A_1 \overset{(3a)=(3a)-3\cdot(1a)}{\overbrace{\longrightarrow}} A_2 = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & -1 & 4 & 4 \end{pmatrix}$$

$$A_2 \overset{(3a)=(3a)-(2a)}{\overbrace{\longrightarrow}} A_3 = \begin{pmatrix} 1 & -3 & 1 & 2 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 3 & 3 \end{pmatrix}$$

A_3 è in forma a scala, non ha pivots nell'ultima colonna e quindi è risolubile, inoltre ha come unica variabile libera x_2, quindi avrà infinite soluzioni, una per ogni scelta di x_2. Troviamo l'espressione di queste soluzioni in funzione di x_2, scriviamo il sistema corrispondente alla matrice A_3, che sappiamo essere equivalente a 6.3:

$$\begin{cases} x_1 & -3x_2 & +x_3 & +2x_4 & = 0 \\ & & -x_3 & +x_4 & = 1 \\ & & & +3x_4 & = 3 \end{cases} \longrightarrow \begin{cases} x_1 = 3x_2 - 2 \\ x_3 = 0 \\ x_4 = 1 \end{cases}$$

Perciò le soluzioni del sistema 6.3 sono del tipo $(3x_2 - 2, x_2, 0, 1)$.

Esercizio 6.4. Trovare tutte le soluzioni del seguente sistema lineare omogeneo $\mathbb{Z}_{11}$:

$$\begin{cases} 6x + y + 4z = 0 \\ 7x + 8y + 8z = 0 \\ 10x + y + z = 0 \\ 2x + y + 7z = 0 \end{cases} \tag{6.4}$$

Innanzitutto osserviamo che il sistema 6.4 ha 4 equazioni e 3 incognite, vedremo che una volta ridotto a scala una delle equazioni sarà un'identità del tipo $0 = 0$ e quindi del tutto ininfluente. Possiamo procedere con la matrice incompleta corrispondente a 6.4 in quanto l'ultima colonna rimarrà immutata da ogni sostituzione lineare:

$$B = \begin{pmatrix} 6 & 1 & 4 \\ 7 & 8 & 8 \\ 10 & 1 & 1 \\ 2 & 1 & 7 \end{pmatrix}$$

Per portare la matrice a scala in questo caso risolviamo alcune congruenze. Vogliamo trovare l'inverso di 7 in $\mathbb{Z}_{11}$, osserviamo che $7 \cdot 8 = 56 \equiv 1\ (11)$ perciò la prima sostituzione lineare che facciamo è: $(2a) = 8 \cdot 6 \cdot (2a) - (1a)$ Osserviamo che $8 \cdot 6 = 48 \equiv 4\ (11)$ dunque:

$$B \overset{2a)=4\cdot(2a)-(1a)}{\xrightarrow{\hspace{2em}}} B_1 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 10 & 1 & 1 \\ 2 & 1 & 7 \end{pmatrix}$$

L'inverso di 10 in $\mathbb{Z}_{11}$ è ovviamente 10 stesso (o -1 che dir si voglia) quindi operiamo le due seguenti sostituzioni lineari: $(3a) = -6 \cdot (3a) - (1a)$ e $(4a) = 3 \cdot (4a) - (1a)$:

$$B_1 \overset{3a)=-6\cdot(3a)-(1a)}{\xrightarrow{\hspace{2em}}} B_2 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 0 & 4 & 1 \\ 2 & 1 & 7 \end{pmatrix} \overset{(4a)=3\cdot(4a)-(1a)}{\xrightarrow{\hspace{2em}}} B_3 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 0 & 4 & 1 \\ 0 & 2 & 6 \end{pmatrix}$$

A questo punto sostituiamo alla quarta riga $2 \cdot (4a) - (3a)$ e poi osserviamo che l'inverso di 4 in $\mathbb{Z}_{11}$ è 3 e perciò operiamo anche la sostituzione lineare $(3a) = 9 \cdot 3 \cdot (3a) - (2a)$ (27 è congruo a 5 modulo 11):

$$B_3 \overset{4a)=2\cdot(4a)-(3a)}{\xrightarrow{\hspace{2em}}} B_4 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 0 & 4 & 1 \\ 0 & 0 & 0 \end{pmatrix} \overset{(3a)=5\cdot(3a)-(2a)}{\xrightarrow{\hspace{2em}}} B_5 = \begin{pmatrix} 6 & 1 & 4 \\ 0 & 9 & 6 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

La matrice B_5 è a scala ed ha tre pivots, quindi ha un'unica soluzione che sappiamo già essere la soluzione identicamente nulla: $x = y = z = 0$.

Esercizio 6.5. Discutere la risolubilità, ed eventualmente trovare tutte le soluzioni, del seguente sistema in $\mathbb{Z}_{11}$ in dipendenza del parametro λ:

$$\begin{cases} 3x + 2y - 5z = 6 \\ 5x + (2 + \lambda)y - 2z = 4 \\ 9x + 5y - 3z = 3\lambda \end{cases} \tag{6.5}$$

La matrice completa associata al sistema 6.5 è:

$$A = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 5 & 2+\lambda & -2 & 4 \\ 9 & 5 & -3 & 3\lambda \end{pmatrix}$$

Portiamola in forma a scala, l'inverso di 5 in $\mathbb{Z}_11$ è 9, e quindi operiamo le due seguenti sostituzioni lineari: $(2a) = 9 \cdot 3 \cdot (2a) - (1a)$ e $(3a) = (3a) - 3 \cdot (1a)$ (osserviamo che $27 \equiv 5$ (11)).

$$A \overset{(2a)=5\cdot(2a)-(1a)}{\overbrace{\rightarrow}} A_1 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & 8+5\lambda & -5 & 3 \\ 9 & 5 & -3 & 3\lambda \end{pmatrix}$$

$$A_1 \overset{(3a)=(3a)-3\cdot(1a)}{\overbrace{\rightarrow}} A_2 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & 8+5\lambda & -5 & 3 \\ 0 & -1 & 1 & 3\lambda-7 \end{pmatrix}$$

A questo punto si potrebbe attuare la sostituzione lineare: $(8+5\lambda) \cdot (3a) + (2a)$ il problema è che a seconda del valore di λ il coefficiente che moltiplica la terza riga da sostituire potrebbe essere nullo (se $\lambda = 5$ si ha $8+5\lambda = 33 \equiv 0$ (11)). Abbiamo due modi per aggirare il problema: studiare a parte il caso $\lambda = 5$ oppure in maniera più semplice effettuare prima la sostituzione tra la seconda riga e la terza e poi effettuare la sostituzione lineare:

$$A_2 \overset{(3a)\leftrightarrow(2a)}{\overbrace{\rightarrow}} A_3 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & -1 & 1 & 3\lambda-7 \\ 0 & 8+5\lambda & -5 & 3 \end{pmatrix}$$

$$A_3 \overset{(3a)=(8+5\lambda)(2a)+(3a)}{\overbrace{\rightarrow}} A_4 = \begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & -1 & 1 & 3\lambda-7 \\ 0 & 0 & 3+5\lambda & (3\lambda-7)\cdot(8+5\lambda)+3 \end{pmatrix}$$

La matrice trovata è a scala, ma non sappiamo dove sta il pivot nell'ultima riga. Se $3+5\lambda \neq 0$, allora la matrice ha tre pivots nessuno dei quali sull'ultima colonna, e quindi il sistema ha una e una sola soluzione. Risolviamo $3+5\lambda = 0$, si trova che λ deve essere uguale a 6. Dobbiamo quindi studiare a parte il caso $\lambda = 6$:

$$\begin{pmatrix} 3 & 2 & -5 & 6 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Quindi se $\lambda = 6$ il sistema 6.5 non ha soluzioni.

Esercizio 6.6. Consideriamo il seguente sistema a coefficienti in $\mathbb{Z}_p$:

$$\begin{cases} x + 5y - 6z = 0 \\ 2x - 8y - 14z = 12 \\ -x + 7y + 10z = 0\lambda \end{cases} \tag{6.6}$$

Discutere al variare di p tra i numeri primi la risolubilità del sistema 6.6

La matrice completa associata al sistema 6.6 è la seguente:

$$A = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 2 & -8 & -14 & 12 \\ -1 & 7 & 10 & 0 \end{pmatrix}$$

Cerchiamo di portarla a scala stando attenti di fare tutte mosse consentite: ovvero di non moltiplicare per zero le righe che andiamo a sostituire.

$$A \overset{(2a)=(2a)-2\cdot(1a)}{\longrightarrow} A_1 = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & -18 & -2 & 12 \\ -1 & 7 & 10 & 0 \end{pmatrix}$$

$$A_1 \overset{(3a)=(3a)+(1a)}{\longrightarrow} A_2 = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & -18 & -2 & 12 \\ 0 & 12 & 4 & 0 \end{pmatrix}$$

A questo punto per ridurre la matrice a scala, osserviamo che il minimo comun multiplo tra 18 e 12 è 36 e quindi operiamo la seguente sostituzione lineare: $(3a) = 3 \cdot (3a) + 2 \cdot (2a)$. Questa sostituzione lineare non è però permessa in $\mathbb{Z}_3$ dove moltiplicare per 3 equivale a moltiplicare per zero, quindi tratteremo a parte il caso $\mathbb{Z}_3$. Per tutti i $p \neq 3$ possiamo tranquillamente operare la sostituzione lineare e si ottiene:

$$A_2 \overset{(3a)=3\cdot(3a)+2\cdot(2a)}{\longrightarrow} A_3 = \begin{pmatrix} 1 & 5 & -6 & 0 \\ 0 & -18 & -2 & 12 \\ 0 & 0 & 8 & 24 \end{pmatrix}$$

Per capire se la matrice è in forma a scala, bisogna capire per quali valori di p gli *apparenti* pivots si potrebbero annullare, e quindi trattare a parte i divisori primi di 1, -18 e 8 che sono 2 e 3. Si può quindi dire che se $p \neq 2$ e $p \neq 3$ allora la matrice ha tre pivots nessuno dei quali nell'ultima colonna e quindi il sistema 6.6 ha una e una sola soluzione. Se $p = 2$ la matrice A_3 ridotta modulo 2 diventa:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

E quindi il sistema 6.6 ha due gradi di libertà e dunque 4 soluzioni in $\mathbb{Z}_2$ una per ogni scelta possibile della coppia di variabili libere (y, z). Ci rimane di trattare il caso $p = 3$, torniamo alla matrice A_2, ovvero prima della sostituzione lineare che in $\mathbb{Z}_3$ non potevamo effettuare e riduciamo tale matrice modulo 3, si ha:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \overset{(3a)=(3a)-(2a)}{\longrightarrow} A_3 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Quindi il sistema 6.6 in $\mathbb{Z}_3$ ha un grado di libertà e dunque 3 soluzioni, una per ogni possibile scelta della variabile libera z.

7. Esercizitazione 2 maggio 2006

In questa lezione abbiamo parlato di applicazioni lineari invertibili: in particolare di come riconoscere se una applicazione lineare è invertibile e come trovarne l'inversa quando esiste.

In generale un'applicazione f dall'insieme A all'insieme B si dice invertibile se esiste un'applicazione f^{-1} da B ad A tale che: $f^{-1} \circ f = Id_A$ e $f \circ f^{-1} = Id_B$. Sappiamo che un'applicazione f da A a B è invertibile se e solo se è bigettiva. Cosa succede nel caso di applicazioni lineari tra spazi vettoriali? Innanzitutto ci piacerebbe che un'applicazione lineare invertibile avesse inversa che rispettasse ancora lineare. Questo è vero come afferma la seguente proposizione:

Proposizione 7.1. *L'inversa L^{-1} di un'applicazione lineare invertibile $L : V \to W$ è anch'essa lineare.*

Dim. Dobbiamo mostrare, sfruttando l'ipotesi L lineare e invertibile, due cose:

(1) per ogni coppia w_1, w_2 di elementi di W si ha: $L^{-1}(w_1 + w_2) = L^{-1}(w_1) + L^{-1}(w_2)$.
(2) Per ogni w di W e per ogni scalare k si ha: $L^{-1}(k \cdot w) = k \cdot L^{-1}(w)$

Siano dunque $w_1, w_2 \in W$ e consideriamo $L^{-1}(w_1 + w_2)$ che è un elemento di V, applicandoci L otteniamo $L(L^{-1}(w_1 + w_2))$, che per definizione di inversa è uguale a $w_1 + w_2$. Analogamente applichiamo L all'elemento $L^{-1}(w_1) + L^{-1}(w_2)$ di V otteniamo $L(L^{-1}(w_1) + L^{-1}(w_2))$ che per la linearità di L è uguale a $L(L^{-1}(w_1)) + L(L^{-1}(w_2))$ e per definizione di inversa otteniamo $w_1 + w_2$. Abbiamo ottenuto la stessa immagine tramite L, ed essendo L iniettiva questo implica che $L^{-1}(w_1) + L^{-1}(w_2)$ è uguale a $L^{-1}(w_1 + w_2)$ come volevamo. Analogamente preso uno scalare k e un elemento w di W se applichiamo L a $L^{-1}(k \cdot w)$ otteniamo $k \cdot w$ e se applichiamo L a $k \cdot L^{-1}(w)$ per la linearità di L otteniamo sempre $k \cdot w$. Dall'iniettività di L si conclude che $L^{-1}(k \cdot w)$ è uguale a $k \cdot L^{-1}(w)$. □

Osservazione 7.2. Sia $L : V \to W$ un'applicazione lineare. Sappiamo che

$$dim(ImmL) + dim(KerL) = dimV \tag{7.1}$$

in particolare se L è invertibile la dimensione del nucleo è nulla (L deve essere iniettiva) e la dimensione dell'immagine è uguale alla dimensione di W (L deve essere surgettiva) quindi si ottiene come condizione necessaria affinché L sia invertibile che $dim(V) = dim(W)$. Ovviamente il viceversa non è vero: non tutte le applicazioni lineari tra spazi della stessa dimensione sono invertibili.
Supponiamo che $L : V \to W$ sia lineare tra due spazi della stessa dimensione, per poter dire che L è invertibile dobbiamo mostrare che L è iniettiva e surgettiva (ovvero bigettiva), in realtà sempre dalla uguaglianza 7.1 segue che: L tra due spazi della stessa dimensione è bigettiva se e solo se è iniettiva se e solo se è surgettiva.

L'osservazione 7.2 ci permette di poter rispondere senza difficoltà alla domanda se un'applicazione lineare sia o meno invertibile, passando attraverso la matrice associata all'applicazione lineare stessa. Sia $L : V \to W$ un'applicazione lineare se V e W hanno dimensioni diverse, L non è invertibile, altrimenti se $dim(V) = dim(W) = n$ fissiamo una base B_V di V e una base B_W di W e scriviamo la matrice associata a L rispetto a queste basi: otteniamo una matrice A_L quadrata $n \times n$. Sappiamo che L è surgettiva (e di conseguenza bigettiva come osservato in 7.2) se e solo se A_L ha rango massimo, ovvero se e solo se A_L ridotta a scala ha n pivots diversi da zero o equivalentemente se e solo se $det(A_L) \neq 0$[11]. Abbiamo quindi un algoritmo per dire, data un'applicazione lineare, se è invertibile.
D'ora innanzi tratteremo applicazioni lineari tra spazi $\mathbb{R}^n$ e sceglieremo come base per scrivere le matrici associate quella canonica di $\mathbb{R}^n$ (questa scelta è dovuta solo a comodità, i risultati sarebbero ugualmente validi con un altra scelta).

Esercizio 7.3. Sia $T : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione lineare definita come segue:

$$T(x, y, z) = (y + z, x + 2y + z, y + 2z)$$

[11]Ovvero se A_L come matrice è invertibile, cioè se esiste una matrice $n \times n$ B tale che $A_L \cdot B = B \cdot A_L = I_n$, dove I_n è la matrice identità $n \times n$ con 1 sulla diagonale principale e 0 fuori dalla diagonale principale e $\cdot$ è il prodotto righe per colonne tra le matrici.

Considerando la base canonica di $\mathbb{R}^3$ la matrice associata a T è:

$$A_T = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Calcoliamo il determinante di A_T sviluppando lungo la prima colonna, si ottiene:

$$det(A_T) = (-1) \cdot (2 - 1) = -1 \neq 0$$

Quindi A_T è invertibile come matrice ovvero l'applicazione T è invertibile. Saremmo potuti arrivare alla stessa conclusione portando a scala A_T e osservando che ha tre pivots diversi da zero.

Abbiamo visto che esiste un algoritmo per dire se una applicazione lineare è invertibile, cerchiamo ora di rispondere ad un'altra domanda: è possibile trovare, in maniera algoritmica, l'applicazione inversa di un'applicazione invertibile? La risposta è sì, vediamo come.
Supponiamo che $L : \mathbb{R}^n \to \mathbb{R}^n$ sia una applicazione invertibile e indichiamo con L^{-1} la sua inversa. Siano A_L e $A_{L^{-1}}$ le matrici quadrate associate rispettivamente a L e L^{-1} rispetto alla base canonica di $\mathbb{R}^n$. Allora deve essere $A_L \cdot A_L^{-1} = A_{L^{-1}} \cdot A_L = I_n$.
Prima di andare avanti provate questo esercizio:

Esempio 7.4. Date A e B matrici quadrate si ha $A \cdot B = I$ se e solo se $B \cdot A = I$.

Invece di cercare direttamente L^{-1} cerchiamo una matrice $A_{L^{-1}}$ tale che $A_L \cdot A_{L^{-1}}$ sia uguale a I_n. Trovata la matrice $A_{L^{-1}}$ sappiamo scrivere la corrispondente applicazione lineare L^{-1}.
Per risolvere

$$A_L \cdot A_{L^{-1}} = I_n \tag{7.2}$$

indichiamo con v_i l'i-esimo vettore colonna di $A_{L^{-1}}$, allora otteniamo n sistemi lineari del tipo $A_L \cdot v_i = e_i$ (dove e_i è l'i-esimo vettore colonna di I_n, ovvero il vettore tutto di 0 tranne che al posto i dove ha 1). Risolvendo questi n sistemi lineari, nelle incognite le coordinate dei vettori v_i, otteniamo la matrice $A_{L^{-1}}$. Dobbiamo quindi scrivere la matrice completa di ogni sistema che è uguale ad A_L a cui aggiungiamo come colonna dei termini noti v_i, portare A_L a scala e quindi risolvere i sistemi. Osserviamo che la matrice incompleta è, per tutti gli n sistemi, sempre A_L e quindi le operazioni per portarla a scala sono sempre le stesse, possiamo dunque fare tutto in un'unica volta, considerando la matrice $n \times 2n$ ottenuta aggiungendo le colonne della matrice I_n dopo quelle di A_L. Vediamo come procedere per trovare l'inversa dell'applicazione lineare T dell'esempio 7.3. La matrice A_T associata a T l'abbiamo già scritta, consideriamo quindi la seguente matrice:

$$(A_T|I) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{pmatrix}$$

E portiamola a scala:

$$(A_T|I) \underbrace{\longrightarrow}_{\text{scambio tra (1) e (2)}} A_1 = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{pmatrix}$$

$$A_1 \underbrace{\rightarrow}_{(3)=(3)-(2)} A_2 = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix}$$

A questo punto potremmo risolvere i tre sistemi a scala:

$$\begin{cases} v_{11} + 2v_{12} + v_{13} = 0 \\ v_{12} + v_{13} = 1 \\ v_{13} = -1 \end{cases}$$

$$\begin{cases} v_{21} + 2v_{22} + v_{23} = 1 \\ v_{22} + v_{23} = 0 \\ v_{23} = 0 \end{cases}$$

$$\begin{cases} v_{31} + 2v_{32} + v_{33} = 0 \\ v_{32} + v_{33} = 0 \\ v_{33} = 1 \end{cases}$$

E trovare tutti gli elementi v_{ij} della matrice $A_{T^{-1}}$, ma vogliamo trovarla senza dover risolvere all'indietro sistemi, per far questo basta non accontentarsi di portare la matrice $(A_T|I)$ a scala, ma ridurre A_T all'identità, in questo modo (prova a dire perchè) otterremo $(I|A_{T^{-1}})$:

$$A_2 \underbrace{\rightarrow}_{(2)=(2)-(3),(1)=(1)-(3)} A_3 = \begin{pmatrix} 1 & 2 & 0 & 1 & 1 & -1 \\ 0 & 1 & 0 & 2 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix}$$

$$A_3 \underbrace{\rightarrow}_{(1)=(1)-2(2)} A_4 = \begin{pmatrix} 1 & 0 & 0 & -3 & 1 & 1 \\ 0 & 1 & 0 & 2 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix}$$

A_4[12] è dunque la nostra matrice $(I|A_{T^{-1}})$ per cui:

$$A_{T^{-1}} = \begin{pmatrix} -3 & 1 & 1 \\ 2 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix}$$

Possiamo verificarlo facendo il prodotto tra A_T e $A_{T^{-1}}$ e vedendo che sia uguale a I_3 (provare).
A questo punto ricaviamo T^{-1}:

$$T^{-1}(x, y, z) = (-3x + y + z, 2x - z, -x + z)$$

Facciamo un'ulteriore controprova componendo T e T^{-1}:

$$T^{-1}(T \begin{pmatrix} x \\ y \\ z \end{pmatrix}) = T^{-1} \begin{pmatrix} y + z \\ x + 2y + z \\ y + 2z \end{pmatrix} = \begin{pmatrix} -3(y + z) + x + 2y + z + y + 2z \\ 2(y + z) - y - 2z \\ -y - z + y + 2z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Esempio 7.5. Consideriamo la matrice:

$$A = \begin{pmatrix} 0 & 1 & -1 & 1 \\ 1 & 2 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

[12] In questo caso siamo stati *fortunati* perchè tutti i pivots sono venuti uguali ad 1, se così non fosse stato, supponiamo avessimo ottenuto che il pivot della seconda riga era uguale a 5, bastava fare un ulteriore passaggio sostituendo alla seconda riga la seconda riga divisa per 5.

Dimostrare che A è invertibile e trovarne l'inversa.

Equazioni cartesiane di un sottospazio V di $\mathbb{R}^n$

Vogliamo mostrare ora che è sempre possibile descrivere un sottospazio V di $\mathbb{R}^n$ come l'insieme degli elementi di $\mathbb{R}^n$ che sono soluzioni di un sistema lineare omogeneo (le equazioni del suddetto sistema si chiameremo equazioni cartesiane di V). Queste equazioni sono particolarmente utili quando dobbiamo trovare l'intersezione tra due spazi vettoriali V e W, infatti se sappiamo che gli elementi di V sono le soluzioni di un sistema 1 e quelli di W sono le soluzioni di un sistema 2, gli elementi di $V \cap W$ saranno quelli che sono soluzioni sia di 1 che di 2, cioè sono le soluzioni del sistema ottenuto mettendo insieme le equazioni di 1 e 2.
Supponiamo di conoscere i generatori di V: $V = Span(v_1, \dots, v_h)$ se scriviamo la matrice A (di dimensione $n \times h$) che ha come colonne i v_i e consideriamo l'applicazione lineare L_A che ad ogni vettore t di $\mathbb{R}^h$ associa il vettore $A \cdot v$ di $\mathbb{R}^n$ ottenuto dal prodotto di A con t. Sappiamo che $Imm(L_A)$ è generata dalle colonne di A, quindi $Imm(L_A) = V$. Quali vettori s di $\mathbb{R}^n$ appartengono a V? Quelli per cui esiste $t \in \mathbb{R}^h$ tale che $A \cdot t = s$. Ovvero dobbiamo discutere le condizioni di risolubilità del seguente sistema:

$$A \cdot \begin{pmatrix} t_1 \\ \vdots \\ t_h \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \tag{7.3}$$

Dove le incognite sono i t_i. Osserviamo che se la matrice A avesse rango n vorrebbe dire che $dim(Imm(L_A)) = V = n$ e quindi che V è tutto $\mathbb{R}^n$ e quindi potremmo per esempio descrivere V come l'insieme degli elementi di $\mathbb{R}^n$ che verificano l'identità $0 = 0$. Supponiamo quindi di essere in un caso più interessante con rango di A uguale a $p < n$. Allora riducendo a scala la matrice completa $(A|s)$ del sistema 7.3 otteniamo che le ultime $n - p$ righe di A sono nulle e quindi otteniamo delle condizioni (lineari omogenee) sulle coordinate di s affinchè il sistema sia risolubile, ovvero affinchè s appartenga a V. Tali condizioni sono le equazioni cartesiane di V.
Vediamo un esempio:

Esercizio 7.6. Sia U il sottospazio di $\mathbb{R}^4$ generato dai vettori $(1, 2, 0, 1)$ e $(0, 1, 1, 1)$ (possiamo anche scrivere $U = Span\{(1, 2, 0, 1), (0, 1, 1, 1)\}$) e W il sottospazio di $\mathbb{R}^4$ definito come segue:

$$W = \{(x, y, z, t) \in \mathbb{R}^4 | x - y + z - 2t = 0\}$$

Determinare:

(1) una base di W.
(2) Una base di $U + W$.
(3) Un supplementare di U (cioè un sottospazio vettoriale V di $\mathbb{R}^4$ tale che $V \cap U = \{O\}$ e $V + U = \mathbb{R}^4$).
(4) Una base di $U \cap W$.

Procediamo un passo per volta:

(1) Trovare una base di W significa trovare gli elementi di $\mathbb{R}^4$ che risolvono l'equazione $x - y + z - 2t = 0$, abbiamo una sola equazione in quattro incognite e quindi abbiamo tre variabili libere, scriviamo dunque $x = y -$

$z + 2t$, ovvero un generico elemento di W è del tipo:

$$\begin{pmatrix} y - z + 2t \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \cdot y + \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \cdot z + \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot t$$

Quindi una base di W è data dall'insieme:

$$\{\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \end{pmatrix}\}$$

(2) Avendo una base di U e una base di W trovare una base di $U + W$ è molto semplice, infatti mettendo insieme gli elementi delle due basi troviamo un insieme di generatori di $U + W$ da cui dobbiamo estrarre una base. Quindi:

$$\{\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}\}$$

genera $U + W$ (sappiamo già che questa non sarà una base, perchè $U + W$ è contenuto in $\mathbb{R}^4$ e quindi al più avrà dimensione 4), mettiamo questi vettori in una matrice e riducendo a scala la matrice estraiamo una base (provate a farlo da soli).

(3) Per determinare un supplementare di U basta completare la base di U ad una base di $\mathbb{R}^4$, ovvero scrivere una matrice con prime due colonne i vettori della base di U e poi aggiungerci quattro colonne con i vettori della base canonica di $\mathbb{R}^4$. Siamo sicuri che questa matrice ha rango 4 (perchè cè un insieme di 4 vettori colonna linearmente indipendenti), riducendola a scala troviamo una base di $\mathbb{R}^4$ che comprende anche i due vettori di U, allora lo spazio V uguale allo Span dei due vettori di tale base che non sono in U è tale che $U + V = \mathbb{R}^4$ e $U \cap V = \{O\}$.

(4) Per trovare una base dell'intersezione conviene scrivere le coordinate cartesiane di U. Dobbiamo trovare le condizioni di risolubilità del seguente sistema nelle incognite t_1, t_2:

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}$$

La matrice completa associata al sistema è:

$$A = \left\{ \begin{array}{ccc} 1 & 0 & x \\ 2 & 1 & y \\ 0 & 1 & z \\ 1 & 1 & t \end{array} \right\}$$

Riduciamo A a scala:

$$A \underbrace{\rightarrow}_{(2)=(2)-2(1),(4)=(4)-(1)} A_1 = \begin{Bmatrix} 1 & 0 & x \\ 0 & 1 & y-2x \\ 0 & 1 & z \\ 0 & 1 & t-x \end{Bmatrix}$$

$$A_1 \underbrace{\rightarrow}_{(3)=(3)-(2),(4)=(4)-(2)} A_2 = \begin{Bmatrix} 1 & 0 & x \\ 0 & 1 & y-2x \\ 0 & 0 & z-y+2x \\ 0 & 0 & t-y+x \end{Bmatrix}$$

Per essere risolubile il sistema devono essere $z-y+2x=0$ e $t-y+x=0$, cioè abbiamo trovato che:

$$U = Span\{(1,2,0,1),(0,1,1,1)\} = \{(x,y,z,t) \in \mathbb{R}^4 | z-y+2x=0 \text{ e } t-y+x=0\}$$

A questo punto gli elementi di $U \cap W$ sono le soluzioni del sistema omogeneo:

$$\begin{cases} z-y+2x=0 \\ t-y+x=0 \\ x-y+z-2t=0 \end{cases}$$