Appunti sui polinomi

Pietro Di Martino e Giovanni Gaiffi

CAPITOLO 1

Alcune osservazioni sulla fattorizzazione dei polinomi

1. Polinomi irriducibili e teorema di fattorizzazione unica

In questo paragrafo, che tratterà della fattorizzazione di polinomi, considereremo (per motivi che diverranno chiari nel corso del paragrafo stesso) anche polinomi a coefficienti in $\mathbb{Z}$, ovvero in un anello che non è un campo. Cercheremo di sottolineare le differenze principali nei due casi, una per esempio è che in $\mathbb{Z}[x]$ non è più vero che tutti i polinomi di grado 0 (ovvero le costanti non nulle) sono invertibili: gli unici polinomi invertibili sono il polinomio 1 e il polinomio -1 (per le altre costanti a non esiste un polinomio di grado 0 b in $\mathbb{Z}[x]$ tale che $a \cdot b = 1$). Useremo la notazione $A[x]$ quando considereremo il caso allargato di polinomi a coefficienti in un anello A commutativo, con unità e privo di divisori di zero.[1] I casi che ci interesseranno saranno essenzialmente quelli dei polinomi a coefficienti in $\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, dunque tutti del tipo descritto e, a parte $\mathbb{Z}$, tutti campi.

Cominciamo introducendo il concetto di polinomio irriducibile in $A[x]$, che avrà lo stesso ruolo del concetto di numero primo in $\mathbb{Z}$.

Definizione 1.1. Dato un polinomio $p(x)$ di $A[x]$ con A anello, se esistono due polinomi $f(x)$ e $g(x)$ in $A[x]$ entrambi non invertibili e tali che

$$p(x) = f(x) \cdot g(x)$$

il prodotto $f(x) \cdot g(x)$ si dice **una fattorizzazione** di $p(x)$ in $A[x]$.

A questo punto possiamo caratterizzare quelli che vogliamo chiamare polinomi irriducibili in $A[x]$:

Definizione 1.2. Sia $f(x)$ un polinomio di $A[x]$ non invertibile. Il polinomio $f(x)$ si dice **riducibile** (o fattorizzabile) in $A[x]$ se in $A[x]$ esiste almeno una fattorizzazione di $f(x)$. Altrimenti il polinomio $f(x)$ si dice **irriducibile**.

Osservazione 1.3. Un modo equivalente di dire che un polinomio $f(x)$ di $A[x]$ è irriducibile (ed è quello che solitamente viene richiamato negli esercizi e nelle dimostrazioni) è affermare che qualsiasi scrittura di $f(x)$ come prodotto di polinomi di $A[x]$:

$$f(x) = g(x)h(x)$$

[1] Si dice in tal caso che A è un dominio. Per esempio l'anello Z è un dominio, mentre l'anello $\mathbb{Z}_{15}$ non lo è.

implica che uno dei due polinomi sia invertibile in $A[x]$. Ovvero nel caso di polinomi a coefficienti in un campo $\mathbb{K}$, essendo gli invertibili tutti e soli i polinomi di grado 0 (le costanti), $f(x)$ è irriducibile in $\mathbb{K}[x]$ se e solo se $f(x)$ ha grado maggiore o uguale a 1 e non può essere scritto come prodotto di due polinomi (non necessariamente distinti) di grado maggiore di 0.

Cominciamo a discutere qualche proprietà sulla irriducibilità che vale nei $\mathbb{K}[x]$ (ma in generale, vedremo, non vale per gli $A[x]$).

Proposizione 1.4. *Negli anelli di polinomi $\mathbb{K}[x]$, con $\mathbb{K}$ campo, tutti i polinomi di grado 1 sono irriducibili.*

Dimostrazione. Supponiamo che il polinomio $f(x) \in \mathbb{K}[x]$ di grado 1 sia il prodotto di due polinomi $g(x)$ e $h(x)$ di $\mathbb{K}[x]$:

$$f(x) = g(x)h(x)$$

Per le proprietà del grado del prodotto di polinomi abbiamo che:

$$1 = deg(f(x)) = deg(g(x)) + deg(h(x))$$

Ovvero uno dei due polinomi deve avere grado 0. E sappiamo che in $\mathbb{K}[x]$ tutti i polinomi di grado 0 sono invertibili. □

Osservazione 1.5. Mostriamo, ad esempio, che in $\mathbb{Z}[x]$ esistono polinomi di primo grado riducibili. Consideriamo $f(x) = 2x - 4$, possiamo scriverlo come $2 \cdot (x - 2)$ ed i polinomi 2 e $x - 2$ non sono invertibili in $\mathbb{Z}[x]$.

Definizione 1.6. Un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ in $\mathbb{Z}[x]$ si dice **primitivo** se il massimo comun divisore tra i suoi coefficienti $a_0, a_1, \ldots, a_n$ è uguale a 1.

La definizione di polinomio primitivo ci permette di individuare i polinomi irriducibili di primo grado in $\mathbb{Z}[x]$ (e dunque di mostrare che, per esempio, il polinomio $x - 2$ è irriducibile in $\mathbb{Z}[x]$).

Proposizione 1.7. *In $\mathbb{Z}[x]$ i polinomi di primo grado sono irriducibili se e solo se sono primitivi.*

Dimostrazione. Se $f(x) = ax + b \in \mathbb{Z}[x]$ di primo grado è il prodotto di due polinomi, allora, per la proprietà del grado[2], deve essere il prodotto di un polinomio di primo grado $h(x) = sx + t$, per un polinomio di grado 0, ovvero una costante $c \in \mathbb{Z}$. Questo, per la definizione di uguaglianza tra polinomi significa che $c \cdot s = a$ e $c \cdot t = b$, dunque che c è un divisore comune dei coefficienti di $f(x)$. Dunque esiste c non invertibile (ovvero diverso da 1 o -1), e quindi una fattorizzazione di $f(x)$ (ovvero $c \cdot h(x)$) se e solo se $f(x)$ non è primitivo. □

[2]Le proprietà del grado continuano a valere in $A[x]$ con A dominio, come potete facilmente verificare.

Abbiamo dunque discusso l'irriducibilità dei polinomi di grado 1 in $\mathbb{K}[x]$ e in $\mathbb{Z}[x]$. Per quanto riguarda i polinomi di grado maggiore di 1, una discussione importante è quella che lega la irriducibilità di un polinomio $f(x)$ in $\mathbb{K}[x]$ di grado $n > 1$ al fatto che esso abbia radici in $\mathbb{K}$. Dal teorema di Ruffini segue che se $f(x)$ ha una radice α in $\mathbb{K}$ allora è riducibile. Infatti si ha che il polinomio $(x - \alpha)$ divide $f(x)$:

$$\underbrace{f(x)}_{grado>1} = g(x) \cdot \underbrace{(x-1)}_{grado=1}$$

Inoltre, per le proprietà del grado, $g(x)$ ha grado maggiore di 0, ovvero non è invertibile.

Viceversa in generale **non è vero** che se un polinomio di grado maggiore di 1 non ha radici allora è irriducibile. Ad esempio il polinomio $x^4 + 2x^2 + 1$ di $\mathbb{R}[x]$ è riducibile in $\mathbb{R}[x]$:

$$x^4 + 2x^2 + 1 = (x^2 + 1)^2$$

ma non ha radici in $\mathbb{R}$ (non esiste nessun numero reale che elevato al quadrato è uguale a -1).

L'unica cosa certa è che un polinomio che non ha radici in $\mathbb{K}$ allora non ha fattori di grado 1 nella sua fattorizzazione in $\mathbb{K}[x]$. Da questo segue che:

Corollario 1.8. *Un polinomio $f(x) \in \mathbb{K}[x]$ di grado 2 e 3 è riducibile se e solo se ha una radice in $\mathbb{K}$.*

Dimostrazione. Abbiamo osservato che, in generale, un polinomio di grado $n > 1$ che ha una radice in $\mathbb{K}$ è riducibile in $\mathbb{K}[x]$. Viceversa se un polinomio di grado 2 o 3 è riducibile allora, sfruttando le proprietà del grado del prodotto di polinomi, necessariamente nel primo caso ($n = 2$) deve essere il prodotto di due fattori di grado 1, mentre nel secondo caso ($n = 3$) può essere il prodotto di un polinomio di grado 1 per un polinomio di grado 2 o il prodotto di tre polinomi di grado 1. Ovvero abbiamo stabilito che i polinomi di grado 2 o 3 riducibili hanno necessariamente un fattore di grado 1 e il teorema di Ruffini ci dice che avere un fattore di grado 1 in $\mathbb{K}[x]$ equivale ad avere una radice in $\mathbb{K}$. □

Gli elementi irriducibili di $\mathbb{K}[x]$ hanno molte analogie con i numeri primi di $\mathbb{Z}$. Un primo risultato importante è quello che ci dice che *se un polinomio irriducibile divide un prodotto di polinomi, allora divide uno dei due fattori*. Enunciamo questo risultato nel seguente teorema, la cui dimostrazione, lasciata come esercizio, coinvolge, analogamente a quello che accade in $\mathbb{Z}$, il lemma di Bezout.

Teorema 1.9 (Primalità di un polinomio irriducibile)**.** *Se $p(x)$ è un polinomio irriducibile in $\mathbb{K}[x]$ dove $\mathbb{K}$ è un campo, e $p(x) \mid f(x) \cdot g(x)$ (dove $f(x), g(x) \in \mathbb{K}[x]$), allora o vale $p(x) \mid f(x)$ o vale $p(x) \mid g(x)$.*

Vale anche l'analogo del teorema di fattorizzazione unica (la dimostrazione è un esercizio caldamente consigliato; è una applicazione del teorema di

primalità: si procede in maniera del tutto simile alla dimostrazione della fattorizzazione unica in $\mathbb{Z}$).

Teorema 1.10 (Teorema di fattorizzazione unica per polinomi)**.** *Ogni polinomio di grado ≥ 1 in $\mathbb{K}[x]$ (dove $\mathbb{K}$ è un campo) è irriducibile o si fattorizza come prodotto di polinomi irriducibili. Inoltre, se*

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_s(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_t(x)$$

sono due fattorizzazioni del polinomio $f(x)$ come prodotto di irriducibili, allora vale che $s = t$ e che i polinomi $p_i(x)$ e i polinomi $q_j(x)$ sono a due a due associati.

Nel teorema di fattorizzazione unica per polinomi i $p_i(x)$ non sono necessariamente distinti. Proprio come nel caso della fattorizzazione tra gli interi, possiamo scrivere la fattorizzazione di un polinomio *accorpando* i fattori uguali e usando le potenze. Si scriverà dunque

$$h(x) = a \cdot q_1^{r_1}(x) \cdot q_2^{r_2}(x) \cdots q_t^{r_t}(x)$$

dove a è il coefficiente direttivo di $h(x)$, i $q_j(x)$ sono i polinomi irriducibili distinti monici[3] della fattorizzazione di $h(x)$, gli r_i sono i numeri naturali positivi che evidenziano quante volte ricorre il polinomio $q_i(x)$ nella fattorizzazione di $h(x)$.[4]

Avendo questa fattorizzazione è molto facile individuare, proprio come avveniva in $\mathbb{Z}$, il *M.C.D.* di due polinomi (se non si conosce già una fattorizzazione, in generale è invece più conveniente. Se infatti consideriamo un polinomio $g(x)$ e la sua fattorizzazione in irriducibili:

$$g(x) = b \cdot p_1^{s_1}(x) p_2^{s_2}(x) \cdot \ldots \cdot p_j^{r_j}(x)$$

allora il *M.C.D.* $(h(x), g(x))$ si otterrà facendo il prodotto degli irriducibili che compaiono sia fra i $p_m(x)$ che fra i $q_n(x)$, ciascuno preso col minimo esponente fra i due esponenti che troviamo nelle due fattorizzazioni.

Esempio 1.11. Consideriamo in $\mathbb{Q}[x]$,

$$h(x) = (x-1)^2(x^2-5)^3(x^4-7x+7)$$

e

$$g(x) = (x-1)^7(x^2-5)(x^5+11x^2+11)^2$$

e supponiamo di sapere che i fattori che compaiono nelle fattorizzazioni sono irriducibili (presto discuteremo un criterio che permette di verificarlo facilmente); allora il *M.C.D.* $(h(x), g(x))$ è

$$(x-1)^2(x^2-5)$$

Gli altri *M.C.D.* $(h(x), g(x))$, come sappiamo, sono tutti i polinomi associati a $(x-1)^2(x^2-5)$.

[3] Un polinomio monico è un polinomio in cui il coefficiente del termine di grado più alto è uguale a 1, tipo $f(x) = x^4 + 6x^3 + x + 6$ in $\mathbb{R}[x]$.

[4] Detto in formule r_i è quel numero naturale tale che $q_i(x)^{r_i}$ divide $h(x)$ e $q_i(x)^{r_i+1}$ non divide $h(x)$.

Osservazione 1.12. L'unicità della fattorizzazione in $\mathbb{K}[x]$ è 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.

Anche in questo caso 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. Dunque 21 lo possiamo fattorizzare anche come $-1\cdot 3\cdot(-1)\cdot 7$ ovvero come $-3\cdot(-7)$.

Osservazione 1.13. Il teorema di fattorizzazione unica vale per ogni $\mathbb{K}[x]$ con $\mathbb{K}$ campo. Per la dimostrazione usiamo il teorema di primalità che a sua volta si dimostra tramite il teorema di Bezout che vale in $\mathbb{K}[x]$ con K campo. Cosa succede se l'insieme dei coefficienti A è un anello ma non un campo? Vale la fattorizzazione unica? La risposta è *"dipende"*... Si può infatti dimostrare che il teorema di fattorizzazione unica vale anche in $\mathbb{Z}[x]$, ma anche mostrare esempi di anelli (che non sono campi) per cui il il teorema di fattorizzazione unica non vale. Consideriamo ad esempio l'insieme $\mathbb{Z}_{30}[x]$ ed il polinomio x^2-1. Facendo i conti si può verificare che:

$$x^2-1=(x-1)(x-29)=(x-19)(x-11)$$

Queste sono due distinte fattorizzazioni in irriducibili.

2. Fattorizzazione in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$

Affrontiamo ora il problema della fattorizzazione nell'anello dei polinomi $\mathbb{K}[x]$, variando $\mathbb{K}$ tra uno dei seguenti campi: $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

2.1. Fattorizzazione in $\mathbb{C}[x]$. Il campo $\mathbb{C}$ dei numeri complessi ha una proprietà molto importante per quanto riguarda le radici di polinomi a coefficienti in $\mathbb{C}$, proprietà che non a caso si chiama **teorema fondamentale dell'algebra** e di cui noi riportiamo solo l'enunciato (la dimostrazione di questo risultato esula dagli obiettivi di questo testo).

Teorema 1.14 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio $f(x)$ a coefficienti in $\mathbb{C}$ di grado maggiore di zero ammette almeno una radice in $\mathbb{C}$.*

Usando il teorema fondamentale dell'algebra e il teorema di Ruffini abbiamo una caratterizzazione completa degli irriducibili in $\mathbb{C}$. Infatti una immediata conseguenza è che:

Corollario 1.15. *Ogni polinomio $f\in\mathbb{C}[x]$ di grado $n>0$ è il prodotto di n fattori di primo grado in $\mathbb{C}[x]$.*

DIMOSTRAZIONE. Procediamo per induzione sul grado n di f. Se f è di primo grado la tesi segue immediatamente. Sia ora $f(x) = \sum_{i=0}^{n} a_i x^i$ 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 1.14 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. □

Dal Corollario 1.15 segue che:

In $\mathbb{C}[x]$ un polinomio è irriducibile se e solo se è di primo grado

In $\mathbb{C}[x]$ quindi 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 $\mathbb{R}[x]$.

Esempio 1.16. 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 (anche se il delta è negativo!):

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

Nel nostro caso:

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

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

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

Per riprova possiamo calcolarci questo prodotto osservando che:

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

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

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

Per la ricerca di radici complesse in polinomi a coefficienti reali (e dunque utile sia per la fattorizzazione in $\mathbb{C}[x]$ che in $\mathbb{R}[x]$) è importante ricordare la funzione coniugio da $\mathbb{C}$ in $\mathbb{C}$:

Definizione 1.17. Chiamiamo funzione **coniugio** la funzione da $\mathbb{C}$ in $\mathbb{C}$ che al numero complesso $a + ib$ associa $\overline{a + ib} = a - ib$.

Esercizio 1.18. Usando la definizione dimostrare le seguenti proprietà della funzione coniugio:

(1) I suoi punti fissi, ovvero gli $z \in \mathbb{C}$ tali che $\overline{z} = z$, sono tutti e soli i numeri reali.
(2) Il coniugio della somma è la somma dei coniugi, ovvero per ogni $z, w \in \mathbb{C}$ $\overline{z + w} = \overline{z} + \overline{w}$.
(3) Il coniugio del prodotto è il prodotto dei coniugi, ovvero per ogni $z, w \in \mathbb{C}$ $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
(4) Il prodotto di un numero complesso per il suo coniugato è un numero reale, ovvero per ogni $z \in \mathbb{C}$ si ha che $z \cdot \overline{z} \in \mathbb{R}$.

Il coniugio permette di dimostrare una interessante proprietà delle radici complesse di un polinomio a coefficienti reali (**ATTENZIONE:** sottolineiamo il fatto che tra le ipotesi che stiamo considerando c'è che i coefficienti del polinomio siano reali), ovvero che se z è una radice di un polinomio $p(x)$ a coefficienti reali, allora $\overline{z}$ è una radice di $p(x)$. Questo è ovvio, ma non è di nessuna utilità, se z è reale in quanto $\overline{z} = z$, ma è invece importante nel caso in cui $z \in \mathbb{C} - \mathbb{R}$:

Proposizione 1.19. *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.*

DIMOSTRAZIONE. sia $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in \mathbb{R}$. Per ipotesi:

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

quindi, dall'enunciato dell'Esercizio 1.18, segue che:

$$\overline{0} = \overline{\sum_{i=0}^{n} a_i \alpha^i} = \sum_{i=0}^{n} \overline{a_i \alpha^i} = \sum_{i=0}^{n} a_i \overline{\alpha^i} = \sum_{i=0}^{n} a_i \overline{\alpha}^i$$

Cioè $f(\overline{\alpha}) = \overline{0} = 0$. □

Nel prossimo esercizio useremo il risultato della Proposizione 1.19 per fattorizzare un polinomio a coefficienti reali in $\mathbb{C}[x]$.

Esercizio 1.20. Sapendo che $f(x) = x^4 - 4x^3 + 3x^2 + 14x + 26$ ha radice $3 + 2i$, fattorizzare il polinomio in $\mathbb{C}[x]$.

Risoluzione. Il polinomio considerato è a coefficienti interi, quindi in particolare reali. Allora possiamo applicare la Proposizione 1.19 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 $f(x)$:

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

Quindi:

$$f(x) = \underbrace{(x-(3+2i))\cdot(x-(3-2i))}_{x^2-6x+13}\cdot(x^2+2x+2)$$

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:

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

Osservazione 1.21. Osserviamo, senza ancora aver parlato di fattorizzazione in $\mathbb{R}[x]$, che la fattorizzazione in $\mathbb{C}[x]$ del polinomio $f(x) = x^4 - 4x^3+3x^2+14x+26$ dell'Esercizio 1.20 fornisce indicazioni importanti sulla fattorizzazione dello stesso polinomio in $\mathbb{R}[x]$.

2.2. Fattorizzazione in $\mathbb{R}[x]$. Anche in $\mathbb{R}[x]$ si possono caratterizzare i polinomi irriducibili attraverso il grado, utilizzando quello che sappiamo della fattorizzazione in $\mathbb{C}[x]$.

Consideriamo un generico polinomio $f(x)\in\mathbb{R}[x]$ di grado n. In particolare $f(x)$ può essere visto come elemento di $\mathbb{C}[x]$ e indichiamo con $z_1,\dots,z_r$ le sue radici complesse e con $m_1,\dots,m_r$ le loro rispettive molteplicità[5]. La fattorizzazione di $f(x)$ in $\mathbb{C}[x]$ è dunque la seguente:

$$\prod_{i=1}^{r}(x-z_i)^{m_i} \tag{2.2}$$

Come si passa dalla fattorizzazione in $\mathbb{C}[x]$ a quella in $\mathbb{R}[x]$? Si osserva che se $z_i\in\mathbb{R}$ allora $(x-z_i)^{m_i}$ è un fattore di $f(x)$ in $\mathbb{R}[x]$, mentre se $z_i\in\mathbb{C}-\mathbb{R}$, allora il fattore $(x-z_i)^{m_i}$ non appartiene a $\mathbb{R}[x]$, ma sappiamo che esiste

[5]Sappiamo, dal Corollario 1.15, che $\sum_{i=1}^{r} m_i = n$, ma in generale $r\le n$. È $r=n$ solo se $f(x)$ ha tutte radici distinte in $\mathbb{C}[x]$.

un'altra radice z_j di $f(x)$ tale che $z_j = \overline{z_i}$ e $m_i = m_j$.
Dunque, nella fattorizzazione 2.2, è presente il fattore

$$((x - z_i) \cdot (x - \overline{z_i}))^{m_i}$$

L'osservazione chiave è che il fattore di secondo grado $(x - z_i) \cdot (x - \overline{z_i})$ è un polinomio reale. Infatti sia $z = a + ib$, $a, b \in \mathbb{R}$ e $b \neq 0$, allora:

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

Come anticipato, i coefficienti del polinomio (1, $-2a$ e $a^2 + b^2$) sono reali.
Riassumendo, date le radici complesse $z_1, \ldots, z_r$ di $f(x)$, se z_i è un numero reale allora $x - z_i$ è un fattore irriducibile di primo grado di $f(x)$ (ripetuto m_i volte) della fattorizzazione in $\mathbb{R}[x]$, se z_i non è un numero reale (ovvero $z_i = a+ib$ con $b \neq 0$) allora $(x-z_i)\cdot(x-\overline{z_i})$ è un fattore di secondo grado della fattorizzazione in $\mathbb{R}[x]$ (ripetuto m_i volte) ed è irriducibile. Quest'ultima proprietà deriva dal fatto che, essendo di secondo grado, o è irriducibile o è il prodotto di due fattori di primo grado. Ma questa seconda opzione possiamo escluderla in quanto, dal teorema di Ruffini sappiamo che i fattori di primo grado sono associati ad una radice nel campo, e sappiamo, per ipotesi, che le radici del polinomio (che sono z e $\overline{z}$) non sono reali ($b \neq 0$).[6].
Dunque la fattorizzazione 2.2 di $f(x)$ in $\mathbb{C}[x]$ fatta di tutti fattori di grado 1, si *trasforma* in una fattorizzazione in $\mathbb{R}[x]$ di $f(x)$ tenendo inalterati i fattori con radici reali e *accorpando* in fattori irriducibili di secondo grado quelli corrispondenti a radici non reali (moltiplicando $x - z$ per $x - \overline{z}$).
Abbiamo scoperto che:

Proposizione 1.22. *Ogni polinomio di grado maggiore di* 2 *in* $\mathbb{R}[x]$ *è riducibile.*

Dimostrazione. Infatti in $\mathbb{C}[x]$ il polinomio $f(x)$ ha $n = deg(f(x))$ radici (non necessariamente distinte)[7] $z_1, \ldots, z_n$. Se una di queste n radici è reale, allora $f(x)$ ha un fattore di grado 1 e dunque è riducibile, altrimenti se sono tutte radici complesse non reali, $f(x)$ è divisibile per il polinomio reale di secondo grado $(x - z_1) \cdot (x - \overline{z_1})$:

$$f(x) = (x - z_1) \cdot (x - \overline{z_1}) \cdot h(x)$$

E per la proprietà del grado del prodotto di polinomi, $h(x)$ ha grado maggiore di 1 e dunque non è invertibile. □

Per concludere la piena caratterizzazione degli irriducibili in $\mathbb{R}[x]$, sapendo che (Proposizione 1.4) in ogni campo i polinomi di grado 1 sono irriducibili, ci resta da approfondire il caso dei polinomi di grado 2. Ma questo è molto semplice, infatti dal Corollario 1.8, sappiamo che $f(x) \in \mathbb{K}[x]$ di grado 2 è riducibile se e solo se ha una radice in $\mathbb{K}$. Nel caso di $\mathbb{K} = \mathbb{R}$ è noto dalla

[6]Si poteva anche esprimere questa osservazione utilizzando il Corollario 1.8: un polinomio di grado 2 è irriducibile se e solo se non ha radici nel campo.

[7]Potrebbe essere anche tutte uguali e dunque una radice di molteplicità n.

scuola superiore che, se $f(x) = ax^2 + bx + c$ è un generico polinomio reale di grado 2, allora $f(x)$ ha radici in $\mathbb{R}$ se e solo se:

$$b^2 - 4ac \geq 0$$

Abbiamo dunque la completa caratterizzazione degli irriducibili in $\mathbb{R}[x]$:
In $\mathbb{R}[x]$ un polinomio è irriducibile se e solo è di primo grado oppure di secondo grado (del tipo $ax^2 + bx + c$ con $a \neq 0$) con $\Delta = b^2 - 4ac$ minore di zero.
Abbiamo dunque un *algoritmo* molto rapido per sapere se un polinomio $f(x)$ è riducibile in $\mathbb{R}[x]$ (basta guardare il grado ed eventualmente calcolare il delta nel caso il grado sia 2). Ma sapere che un polinomio $f(x)$ è riducibile non implica che la sua fattorizzazione in fattori irriducibili sia semplice da trovare.

Esercizio 1.23. Fattorizzare il polinomio $x^4 - 2x^2 - 3 \in \mathbb{R}[x]$.

Questo polinomio è di grado 4 ed è dunque riducibile in $\mathbb{R}[x]$: o è il prodotto di quattro polinomi di grado 1 (4 radici reali non necessariamente distinte), o il prodotto di un polinomio di grado 2 e due di grado 1 (2 radici reali non necessariamente distinte e 2 complesse coniugate) o il prodotto di due polinomi di grado 2 (4 radici complesse a due a due coniugate e non necessariamente distinte). Come si evince da questa prima analisi sarebbe fondamentale riuscire a determinarne le radici complesse. Esiste una formula risolutiva per le equazioni di quarto grado, ma non la conosciamo e dunque cerchiamo di agire diversamente, osservando che il polinomio considerato è, in un certo senso, *particolare*: 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:

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

2.3. Fattorizzazione in $\mathbb{Q}[x]$. In $\mathbb{Q}[x]$, a differenza di quanto visto per $\mathbb{C}[x]$ e $\mathbb{R}[x]$, vedremo che per ogni naturale n esistono polinomi di grado n irriducibili.

Una prima osservazione importante viene offerta dal Lemma di Gauss enunciato (senza dimostrazione) qui sotto: nel caso di un polinomio primitivo a coefficienti interi, la sua irriducibilità in $\mathbb{Q}[x]$ è equivalente alla sua

irriducibilità in $\mathbb{Z}[x]$. Questo è un risultato per niente banale e scontato: infatti, per esempio, se è vero che è ovvio che un polinomio $f(x) \in \mathbb{K}[x]$, riducibile in $\mathbb{K}[x]$, è riducibile in qualsiasi campo $\mathbb{L}$ che contenga strettamente $\mathbb{K}$ (basta considerare la stessa fattorizzazione, infatti i polinomi di $\mathbb{K}[x]$ sono in particolare polinomi di $\mathbb{L}[x]$), il viceversa non è in generale vero. Ad esempio qualsiasi polinomio di secondo grado irriducibile in $\mathbb{R}[x]$ (ad esempio x^2+1) è riducibile in $\mathbb{C}[x]$ (nel caso di x^2+1 è uguale a $(x-i)\cdot(x+i)$).

Lemma 1.24 (Lemma di Gauss)**.** *Sia $f(x) \in \mathbb{Z}[x]$. Se $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$ allora possiamo trovare due polinomi $a_1(x) \in \mathbb{Z}[x]$, associato a $a(x)$, e $b_1 \in \mathbb{Z}[x]$, associato a $b(x)$, tali che*

$$f(x) = a_1(x)b_1(x)$$

Riassumendo, $g(x) \in \mathbb{Q}[x]$ è riducibile se e solo se il polinomio primitivo a coefficienti interi $f(x)$ ad esso associato è riducibile in $\mathbb{Z}[x]$. Abbiamo in definitiva ridotto la fattorizzazione in $\mathbb{Q}[x]$ a quella in $\mathbb{Z}[x]$ con notevoli vantaggi come vedremo da qui in avanti.

Cominciamo mostrando un primo criterio molto utile per riconoscere (e costruire) polinomi irriducibili in $\mathbb{Q}[x]$.

Teorema 1.25 (Criterio di Eisenstein)**.** *Sia*

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

un polinomio primitivo di grado maggiore di 1 a coefficienti interi. Se esiste un numero primo p tale che:

(1) *p NON divide il coefficiente direttivo a_n,*
(2) *p divide tutti gli a_i con $i < n$,*
(3) *p^2 non divide il termine noto a_0,*

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$, e dunque - per il lemma di Gauss - in $\mathbb{Q}[x]$.

Dimostrazione. Supponiamo che $f(x)$ sia uguale al prodotto dei due polinomi $g(x) = \sum_{i=0}^{r} b_i x^i$ e $h(x) = \sum_{i=0}^{s} c_i x^i$ di $\mathbb{Z}[x]$, entrambi di grado maggiore o uguale a 1. Da $f(x) = g(x)h(x)$ e dalla definizione di uguaglianza tra polinomi, segue che tutti i coefficienti del polinomio a destra sono uguali a tutti i coefficienti del polinomio a sinistra. Facendo i conti, otteniamo un sistema dove gli $n+1$ coefficienti a_i di $f(x)$ sono espressi tramite i coefficienti di $g(x)$ e $h(x)$ come segue[8]:

$$a_i = \sum_{j=0}^{i} b_j \cdot c_{i-j} \tag{2.3}$$

Partiamo *dal basso* del sistema 2.3: $a_0 = b_0 c_0$. Per ipotesi p divide a_0, ma p^2 non divide a_0: questo significa che p divide uno tra b_0 e c_0, ma non

[8]Esclusivamente per semplicità di notazione consideriamo anche i coefficienti nulli di $g(x)$ e $h(x)$ dei termini di grado maggiore rispettivamente di r e s. Ovvero $b_j = 0$ se $j > r$ e $c_t = 0$ se $t > s$.

entrambi. Il ruolo dei b_i e dei c_i è simmetrico quindi possiamo, senza perdere di generalità, supporre che p divida b_0 e non c_0.

A questo punto la seconda equazione del sistema 2.3 è $a_1 = b_1c_0 + b_0c_1$, che diventa:

$$b_1c_0 = a_1 - b_0c_1$$

Ora sappiamo che p divide a_1 (ipotesi), p divide b_0 (appena stabilito) e dunque p divide b_1c_0. Sappiamo anche che p non divide c_0 e di conseguenza divide b_1.

Iterando questo procedimento si ottiene che p divide ogni b_i e di conseguenza divide $a_n = b_rc_s$: ma questo è contro l'ipotesi. L'assurdo nasce dal fatto di aver supposto che $f(x)$, che verifica le tre condizioni del criterio di Eisenstein, possa essere scritto come prodotto di due polinomi di grado maggiore o uguale a 1. □

Come detto il criterio di Eisenstein permette di costruire polinomi irriducibili in $\mathbb{Q}[x]$ e addirittura permette di trovarne *infiniti* per ogni grado $n > 0$:

Corollario 1.26. *In $\mathbb{Q}[x]$ esistono polinomi irriducibili di grado $n > 0$ qualsiasi.*

Dimostrazione. Basta considerare il polinomio $x^n - 2$ ed applicare Eisenstein con primo $p = 2$. Infatti 2 divide il termine noto (2), ma il quadrato di p (4) non divide il termine noto. E infine 2 non divide il coefficiente direttivo (1). Lo stesso ragionamento permette di dimostrare che $x^n - p$, per un qualsiasi primo p, è irriducibile. □

Un altro punto importante per fattorizzare in $\mathbb{Q}[x]$ un polinomio $f(x)$ a coefficienti interi è il fatto che la conoscenza del coefficiente direttivo e del termine noto di $f(x)$ permette di limitare la ricerca delle *possibili* radici razionali di $f(x)$ (e dunque, in termini di fattorizzabilità, dei possibili fattori di grado 1 di $f(x)$) ad un insieme finito di numeri razionali. Per la precisione:

Proposizione 1.27. *Se $f(x) \in \mathbb{Z}[x]$ e r/s (ridotto ai minimi termini, ovvero con $(r, s) = 1$) è una radice in $\mathbb{Q}$, allora r divide il termine noto e s divide il coefficiente direttivo di $f(x)$.*

Dimostrazione. Sia $f(x) = \sum_{j=0}^{m} b_j x^j$ a coefficienti interi, l'ipotesi che r/s sia radice equivale a:

$$\sum_{i=0}^{n} b_i \left(\frac{r}{s}\right)^i = 0$$

Moltiplicando tutto per s^n si ottiene:

$$b_n r^n + \underbrace{b_{n-1}r^{n-1}s + ... + b_0 s^n}_{\text{è un multiplo di } s} = 0 \tag{2.4}$$

Per cui $s|b_n r^n$, ma essendo $(s, r) = 1$ questo implica $s|b_n$. Analogamente se raccogliamo in 2.4 r, otteniamo che r deve dividere $b_0 s^n$, ma essendo $(r, s) = 1$ questo implica che $r|b_0$. □

Esempio 1.28. Consideriamo il polinomio $f(x) = x^4 + 3x^3 + x^2 - 6x - 6$. Dalla Proposizione 1.27 segue che se r/s è una radice razionale, allora r divide -6 e s divide 1. Ovvero sappiamo che le uniche radici razionali possibili di $f(x)$ sono da ricercare nell'insieme finito:

$$A = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

Sostituendo in $f(x)$ non si trova 0 in nessuno di questi casi, dunque $f(x)$ non ha radici razionali.
ATTENZIONE: questo non significa che $f(x)$ sia irriducibile! Sappiamo solo che $f(x)$ non ha fattori di grado 1, ma potrebbe essere il prodotto di due fattori irriducibili di grado 2.

Esercizio 1.29. Il polinomio dell'esempio precedente è irriducibile in $\mathbb{Q}[x]$?
Suggerimento: se non vi riesce leggete più avanti...

La Proposizione 1.27 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 di polinomi di grado 2 e 3 in $\mathbb{Q}[x]$, infatti un polinomio di questo tipo o è irriducibile o ha una radice razionale.

Esercizio 1.30. Dire se $f(x) = x^3 - x^2 - 8x + 12$ è irriducibile in $\mathbb{Q}[x]$.

Risoluzione. I divisori del termine noto sono $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$, i divisori del coefficiente del termine di grado massimo sono $\{\pm 1\}$ quindi le possibili radici razionali sono: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. Proviamo a calcolare la funzione polinomiale $f(x)$ per questi valori fino a che non troviamo una radice; 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:

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

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:

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

A questo punto cominciamo ad avere diversi strumenti per la fattorizzazione in $\mathbb{Q}[x]$: innanzitutto sappiamo che ci possiamo ridurre ad un polinomio, associato a quello di partenza, primitivo e a coefficienti interi. Sui polinomi primitivi a coefficienti interi conosciamo un criterio *diretto* di irriducibilità (Eisenstein). Inoltre, la fattorizzazione è molto più semplice in $\mathbb{Z}[x]$. Cerchiamo di capire perché riprendendo in mano il polinomio $f(x)$ dell'Esempio 1.28. Abbiamo già visto che non ha radici, dunque se è fattorizzabile è il prodotto di due polinomi di grado 2 (che per il lemma di Gauss possiamo supporre a coefficienti interi).

Consideriamo due generici polinomi di grado 2 in $\mathbb{Z}[x]$:

$$g(x) = ax^2+bx+c$$
$$h(x) = dx^2+ex+f$$

Per quanto osservato sopra, $f(x) = x^4+3x^3+x^2-6x-6$ è fattorizzabile se e solo se è il prodotto di due polinomi di grado 2, ovvero se e solo se esiste una soluzione del seguente sistema di 5 equazioni a coefficienti interi:

$$\begin{cases} 1 = a\cdot d \\ 3 = a\cdot e + b\cdot d \\ 1 = a\cdot f + b\cdot e + c\cdot d \\ -6 = b\cdot f + c\cdot e \\ -6 = c\cdot f \end{cases}$$

Sapere che, pur cercando la fattorizzazione in $\mathbb{Q}[x]$, possiamo risolvere in $\mathbb{Z}$ è di grande aiuto. Infatti risolvere *algoritmicamente* questo sistema in $\mathbb{Z}$ è possibile: ogni singola equazione infatti può avere solo un numero finito (anche uguale a 0) di soluzioni intere; studiando tutti i casi possibili e *risalendo* il sistema o si determina una soluzione intera o altrimenti si deduce che il sistema è irrisolvibile e dunque $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e di conseguenza in $\mathbb{Q}[x]$. Questo procedimento di fattorizzazione in $\mathbb{Z}[x]$ risolvendo il sistema per casi è noto come **metodo della forza *bruta***. Applichiamo questo metodo al nostro sistema: vedremo così concretamente i vantaggi di sapere di potersi limitare a cercare soluzioni intere del sistema. Da $1 = a\cdot d$ ad esempio, segue che o $a=d=1$ oppure $a=d=-1$ (ma se $f(x)=g(x)\cdot h(x)$,

allora $f(x) = -g(x) \cdot (-h(x))$ e dunque possiamo considerare $a = d = 1$). Andiamo dunque a riscriverci il nostro sistema:

$$\begin{cases} 1 = a \cdot d \\ 3 = a \cdot e + b \cdot d \\ 1 = a \cdot f + b \cdot e + c \cdot d \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases} \leftrightarrow \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = f + b \cdot e + c \\ -6 = b \cdot f + c \cdot e \\ -6 = c \cdot f \end{cases}$$

Da $-6 = c \cdot f$ si ottiene che o $c = 1$ e $f = -6$, o $c = -1$ e $f = 6$, o $c = 2$ e $f = -3$ o infine $c = -2$ e $f = 3$ (essendo $g(x)$ e $h(x)$ dello stesso grado generici, il loro ruolo è completamente simmetrico e dunque non è necessario considerare anche i casi speculari tipo $c = 6$ e $f = -1$). Otteniamo dunque 4 sistemi con meno variabili. Bisogna studiarli tutti:

$$\begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = -6 + b \cdot e + 1 \\ -6 = -6b + e \\ c = 1 \\ f = -6 \end{cases} \quad \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = 6 + b \cdot e - 1 \\ -6 = 6b - e \\ c = -1 \\ f = 6 \end{cases}$$

$$\begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = -3 + b \cdot e + 2 \\ -6 = -3b + 2e \\ c = 2 \\ f = -3 \end{cases} \quad \begin{cases} a = d = 1 \\ 3 = e + b \\ 1 = 3 + b \cdot e - 2 \\ -6 = 3b - 2e \\ c = -2 \\ f = 3 \end{cases}$$

È facile verificare che i primi tre sistemi non hanno soluzioni intere (portano rispettivamente alle seguenti equazioni irrisolvibili in $\mathbb{Z}$: $5e = 12$, $7b = -3$, $5e = 3$), mentre l'ultimo ha soluzione (con $b = 0$ ed $e = 3$). Dunque esiste una fattorizzazione di $f(x)$ in $\mathbb{Q}[x]$ (nonostante $f(x)$ non abbia radici razionali):

$$\underbrace{x^4 + 3x^3 + x^2 - 6x - 6}_{f(x)} = (\underbrace{x^2 - 2}_{g(x)})(\underbrace{x^2 + 3x + 3}_{h(x)})$$

3. Esercizi

Esercizio 1.31. 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 $x - 1$.

Risoluzione. 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 terzo grado, quindi con i nostri strumenti possiamo trovare questa radice solo se è razionale (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:

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

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 calcolando 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 $\mathbb{R}$:

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

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

Risoluzione. 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. Nel caso della riducibilità in $\mathbb{Q}[x]$ se il polinomio è a coefficienti interi (come $g(x)$) la Proposizione 1.27 permette di limitare le possibili radici razionali ad un insieme finito (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: $\{\pm\frac{1}{2}, \pm\frac{1}{4}, \pm 1\}$. Proviamoli, 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:

$$\begin{aligned} g(-\tfrac{1}{4}) &= -\tfrac{1}{16} + \tfrac{5}{16} - \tfrac{3}{4} + 1 = \tfrac{1}{2} \\ g(-1) &= -4 + 5 - 3 + 1 = -1 \\ g(-\tfrac{1}{2}) &= -\tfrac{1}{2} + \tfrac{5}{4} - \tfrac{3}{2} + 1 = \tfrac{1}{4} \end{aligned}$$

$g(x)$ 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 troviamo $g(1) = 13 = 0$, quindi $g(x)$ è riducibile in $\mathbb{Z}_{13}[x]$ perché ha una radice e dunque per Ruffini è divisibile per $x - 1$:

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

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 usa la seguente osservazione:

Osservazione 1.33. La formula per la risoluzione delle equazioni di secondo grado vale in ogni campo $\mathbb{K}$ (e quindi in particolare per campi finiti).

DIMOSTRAZIONE. Supponiamo di dover risolvere:

$$ax^2 + bx + c = 0 \tag{3.1}$$

con a, b, c appartenenti ad un qualsiasi campo $\mathbb{K}$ e $a \neq 0$ (questo per garantire che effettivamente stiamo risolvendo un'equazione di secondo grado). Ripercorriamo i passi che portano alla formula risolutiva delle equazioni reali di secondo grado per far vedere che le uniche cose che usiamo sono le proprietà di campo di $\mathbb{R}$:

(1) Sommiamo ad entrambi i membri di 3.1 l'opposto di c:

$$ax^2 + bx = -c \tag{3.2}$$

(2) Moltiplichiamo entrambi i membri per l'inverso di a che indichiamo con a^{-1} (sappiamo che esiste in $\mathbb{K}$ l'inverso di $a \neq 0$):

$$x^2 + a^{-1} \cdot bx = a^{-1} \cdot (-c) \tag{3.3}$$

(3) Aggiungiamo ad entrambi i membri di 3.3 $[(2a)^2]^{-1} \cdot b^2$:

$$x^2 + a^{-1} \cdot bx + [(2a)^2]^{-1} \cdot b^2 = a^{-1} \cdot (-c) + [(2a)^2]^{-1} \cdot b^2 \tag{3.4}$$

(4) È facile vedere (sfruttando la commutatività in $\mathbb{K}$) che il primo membro di 3.4 non è nient'altro che $(x + (2a)^{-1} \cdot b)^2$, si ha dunque:

$$(x + (2a)^{-1} \cdot b)^2 = a^{-1} \cdot (-c) + [(2a)^2]^{-1} \cdot b^2$$

che ha soluzione in $\mathbb{K}$ se e solo se:

$$a^{-1} \cdot (-c) + [(2a)^2]^{-1} \cdot b^2 = [(2a)^2]^{-1} \cdot (b^2 - 4a \cdot c)$$

è un quadrato in $\mathbb{K}$.

Per concludere, basta osservare che $a \neq 0$ è un quadrato in $\mathbb{K}$ se e solo se a^{-1} è un quadrato in $\mathbb{K}$ e quindi $[(2a)^2]^{-1}$ è sempre un quadrato. Perciò l'equazione 3.1 ha soluzione in $\mathbb{K}$ se e solo se $b^2 - 4a \cdot c$ (che solitamente indichiamo con Δ) è un quadrato in $\mathbb{K}$. Se in $\mathbb{K}$ esiste radice di Δ e Δ è diverso da zero, allora ne esistono esattamente 2 distinte[9]. Le soluzioni dell'equazione 3.1 in questo caso sono allora due distinte e si ottengono sommando $-(2a)^{-1} \cdot b$ alle radici di Δ. □

[9]Supponiamo $\Delta \neq 0$ abbia radice in $\mathbb{K}$ allora l'equazione $x^2 = \Delta$ è equivalente a

$$(x - \sqrt{\Delta}) \cdot (x + \sqrt{\Delta}) = 0$$

che in un campo, dove non ci sono divisori di zero, ha esattamente due soluzioni distinte $\sqrt{\Delta}$ e $-\sqrt{\Delta}$.

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 $\mathbb{Z}_{13}[x]$.

Esercizio 1.34. Fattorizzare il polinomio $f(x) = x^5 + x^2 + 1$ in $\mathbb{Q}[x]$.

Risoluzione. Il polinomio $f(x)$ non ha radici in $\mathbb{Q}[x]$. Infatti dalla Proposizione 1.27 sappiamo che le uniche possibili radici razionali di $f(x)$ sono 1 e -1, ma valutando il polinomio in questi due valori si ottiene:

$$f(1) = 3 \quad f(-1) = 1$$

Il teorema di Ruffini ci dice dunque che $f(x)$ non ha fattori lineari in $\mathbb{Q}[x]$. A questo punto o $f(x)$ è irriducibile o è il prodotto di due polinomi irriducibili rispettivamente di secondo e terzo grado. Procediamo con il metodo della forza bruta (osserviamo che possiamo prendere i due eventuali polinomi fattore monici):

$$x^5 + x^2 + 1 = (x^3 + ax^2 + bx + c)(x^2 + dx + e) =$$
$$= x^5 + (a + d)x^4 + (e + ad + b)x^3 + (ae + bd + c)x^2 + (be + cd)x + ce$$

Abbiamo dunque il seguente sistema a coefficienti interi:

$$\begin{cases} a + d = 0 \\ e + ad + b = 0 \\ ae + bd + c = 1 \\ be + cd = 0 \\ ce = 1 \end{cases}$$

Da $ce = 1$ seguono due possibilità $c = e = 1$ oppure $c = e = -1$, in entrambi i casi si ha $b = a = -d$. Sostituendo in $e + ad + b = 0$ si ottiene, nel caso $e = 1$:

$$a^2 - a - 1 = 0$$

e nel caso $e = -1$:

$$a^2 - a + 1 = 0$$

In entrambi i casi non esistono soluzioni intere. Dunque il metodo della forza bruta ci dice che il polinomio $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 1.35. Fattorizzare il polinomio $f(x) = x^4 - 1$ in $\mathbb{Z}_5[x]$.

Risoluzione. Il polinomio $f(x)$ ha 1 come radice, dunque per il teorema di Ruffini è divisibile per $x-1$. Osserviamo prima di proseguire che il risultato della divisione restituirà $f(x)$ come prodotto di $x-1$ per un polinomio $g(x)$ di terzo grado. Per completare la fattorizzazione di $f(x)$ dovremo dunque studiare la riducibilità di $g(x)$ che, essendo di terzo grado, è equivalente alla

ricerca di radici in $\mathbb{Z}_5[x]$ del polinomio suddetto. Procediamo ora con la divisione di $f(x)$ per $x-1$:

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

Dunque:

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

Valutiamo se $g(x)$ ha radici in $\mathbb{Z}_5$:

$$g(0)=1 \quad g(1)=4 \quad g(2)=15=0 \quad g(3)=40=0 \quad g(4)=85=0$$

Perciò da Ruffini segue che $g(x)$ è fattorizzabile come:

$$g(x)=(x-2)(x-3)(x-4)$$

Concludendo:

$$f(x)=(x-1)(x-2)(x-3)(x-4)$$

Osserviamo che potevamo arrivare alla conclusione in maniera molto più rapida sfruttando le proprietà degli $\mathbb{Z}_p$ ed in particolare il piccolo teorema di Fermat. Infatti sappiamo che il polinomio x^5-x si annulla per ogni valore di $\mathbb{Z}_5$ e basta osservare che:

$$x^5-x=x(x^4-1)$$

Ovvero x^4-1 si annulla in tutti gli elementi di $\mathbb{Z}_5$ tranne che in 0 e dunque è fattorizzabile proprio come:

$$f(x)=(x-1)(x-2)(x-3)(x-4)$$

Esercizio 1.36. Sia $p(x)=x^4-4x^3+6x^2-4x+5$. Sapendo che $2+i$ è una radice complessa del polinomio $p(x)$ fattorizzarlo in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$.

Risoluzione. Se $\alpha=2+i$ è radice, allora (Proposizione 1.19) anche il suo complesso coniugato $\overline{\alpha}=2-i$ è radice di $p(x)$. Dunque il polinomio è divisibile per:

$$(x-(2+i))(x-(2-i))=(x-2)^2-i^2=x^2-4x+4+1=x^2-4x+5$$

Eseguiamo la divisione:

$$\begin{array}{cccccc|l} x^4 & -4x^3 & +6x^2 & -4x & +5 & | & x^2-4x+5 \\ x^4 & -4x^3 & +5x^2 & & & | & x^2+1 \\ & & x^2 & -4x & +5 & | & \\ & & x^2 & -4x & +5 & | & \\ & & & & 0 & | & \end{array}$$

Abbiamo dunque trovato che:

$$p(x) = (x^2 - 4x + 5)(x^2 + 1)$$

che è la fattorizzazione in irriducibili in $\mathbb{R}[x]$, infatti entrambi i polinomi di secondo grado non hanno soluzioni reali. Visto che $x^2 + 1$ ha come radici complesse i e $-i$ la fattorizzazione in irriducibili di $p(x)$ in $\mathbb{C}[x]$ è:

$$p(x) = (x - (2 + i))(x - (2 - i))(x - i)(x + i)$$

Esercizio 1.37. Fattorizzare il polinomio $x^4 + 4x^3 - 19x^2 + 8x - 42$ come prodotto di irriducibili in $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_3[x]$, $\mathbb{Z}_{13}[x]$.

Esercizio 1.38. Fattorizzare il polinomio $x^4 - 4x^3 + x^2 + 8x - 6$ come prodotto di irriducibili in $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_{11}[x]$.

Esercizio 1.39. Consideriamo il polinomio

$$p(x) = x^4 - x^3 - x^2 - x - 2$$

Fattorizzare $p(x)$ come prodotto di irriducibili in$\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_3[x]$.

Esercizio 1.40. Fattorizzare il polinomio $f(x) = x^6 - x^5 - 2x^4 - 2x^2 + 2x + 4$ come prodotto di irriducibili in $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$, $\mathbb{Z}_2[x], \mathbb{Z}_3[x]$.

Esercizio 1.41. Dimostrare che per ogni $p \in \mathbb{N}$ primo, il polinomio:

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

è irriducibile in $\mathbb{Q}[x]$.