Geometria

16 giugno 2015

Capitolo 1

Gruppi e anelli

1.1 Gruppi

Definizione 1.1.1. *Si definisce* gruppo *un insieme G non vuoto munito di un'operazione binaria interna $*\colon G \times G \to G$, ossia tale per cui sono rispettati gli assiomi seguenti:*

1. *vale la proprietà associativa, cioè $\forall g_1, g_2, g_3 \in G$ vale $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$;*
2. *esiste l'elemento neutro, cioè $\exists e \in G\colon \forall g \in G$, $g * e = e * g = g$;*
3. *esiste l'inverso, ossia $\forall g \in G\ \exists g' \in G\colon g * g' = g' * g = e$.*

Dove non ci saranno ambiguità, d'ora in poi indicheremo l'operazione interna del gruppo come una moltiplicazione, omettendo il simbolo $*$: scriveremo dunque $x * y = xy$. L'inverso di un elemento x sarà indicato, coerentemente, con x^{-1}.

La struttura di gruppo si compone sempre di un insieme e di un'operazione, perciò si identifica convenzionalmente con la coppia $(G, *)$; uno insieme può formare gruppi differenti in base all'operazione associata. Il gruppo è detto *commutativo* (o *abeliano*) se vale anche la proprietà commutativa, cioè $\forall x, y \in G$, $xy = yx$.

L'elemento neutro di un gruppo è sempre unico: se e ed e' rispettano la seconda proprietà, allora $e' = ee' = e$ quindi coincidono. Lo stesso vale per l'inverso, dato $x \in G$: se a e b sono due inversi di x, allora

$$b = eb = (ax)b = a(xb) = ae = a. \tag{1.1.1}$$

Elenchiamo di seguito alcuni esempi, più o meno immediati, di gruppi.

- Gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con l'usuale operazione di addizione. Più in generale, gli elementi di un campo qualsiasi formano un gruppo rispetto all'addizione.
- Gli insiemi $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$, privati dello zero, con l'usuale moltiplicazione. Lo stesso accade per gli elementi non nulli di un campo qualsiasi: dato un campo K, saremo soliti indicare il gruppo moltiplicativo $(K \setminus \{0\}, \cdot)$ con il simbolo $K^{\times}$.
- Le rotazioni in un piano, con l'operazione di composizione, che è anche abeliano.
- Le rotazioni in $\mathbb{R}^3$, sempre con la composizione, sono ancora un gruppo. Esso però non è abeliano, perché due rotazioni effettuate rispetto ad assi differenti in generale non commutano.
- L'insieme $\{-1, 1\}$ forma un gruppo rispetto alla moltiplicazione.

Definizione 1.1.2. *Un sottoinsieme H di un gruppo G è detto* sottogruppo *di G se è a sua volta un gruppo con l'operazione di G.*

In altre parole, H è un gruppo contenuto in un gruppo più grande. Questa definizione equivale alle richieste:

1. H deve essere chiuso rispetto all'operazione del gruppo G, ossia se $a, b \in H$ allora $ab, ba \in H$;

2. ogni elemento di H deve avere il suo inverso in H.

Di conseguenza, H deve anche contenere l'elemento neutro (lo stesso!) di G, poiché se $x \in H$, allora anche x^{-1} vi appartiene, dunque anche $xx^{-1} = e$.

Ogni gruppo ammette sempre due sottogruppi: il gruppo stesso e il *sottogruppo banale* $\{e\}$ del suo elemento neutro. Gli altri sottogruppi, se esistono, sono detti *propri*. Se un gruppo è abeliano, allora anche tutti i suoi sottogruppi lo sono. Alcuni esempi di sottogruppi sono i seguenti.

- L'insieme $\mathbb{T} = \{z \in \mathbb{C} \colon |z| = 1\}$, detto *gruppo circolare*, è un sottogruppo di $\mathbb{C}^\times$. Poiché $\mathbb{C}^\times$ è abeliano, lo è anche $\mathbb{T}$.

- In $\mathbb{R}^2$, sia $R(\theta)$ la rotazione antioraria di un angolo θ. L'insieme $\{R(0), R(\pi/2), R(\pi), R(3\pi/2)\}$ è un sottogruppo del gruppo delle rotazioni nel piano.

1.2 Relazioni di equivalenza

Una relazione binaria su un insieme X lega due elementi dell'insieme. Essa si definisce come un sottoinsieme di $X \times X$, intendendo che due elementi a, b sono messi in relazione da R se $(a, b) \in R$. Solitamente una relazione di questo tipo si indica con il simbolo $\sim$, cioè $a \sim b$.

Definizione 1.2.1. *La relazione $\sim$ è una relazione di equivalenza su X se è binaria e valgono le seguenti proprietà:*

1. *è riflessiva: $a \sim a$;*

2. *è simmetrica: se $a \sim b$, allora $b \sim a$;*

3. *è transitiva: se $a \sim b$ e $b \sim c$, allora anche $a \sim c$.*

Con questa relazione di equivalenza possiamo "raggruppare" gli elementi di X in vari insiemi di elementi tutti in relazione tra loro. Vediamo se questa suddivisione è buona, cioè se un elemento è categorizzato in uno solo di questi insiemi o meno.

Definizione 1.2.2. *Si chiama* classe di equivalenza *di un elemento $a \in X$, rispetto alla relazione $\sim$, l'insieme*

$$[a] = \{b \in X : b \sim a\}.$$

L'elemento a è detto rappresentante *della classe $[a]$.*

Teorema 1.2.3. Due classi di equivalenza, rispetto alla relazione $\sim$, $[a]$ e $[a']$ coincidono se e solo se $a \sim a'$.

Dimostrazione. Siano le due classi $[a] = \{x \in X : x \sim a\}$ e $[a'] = \{y \in X : y \sim a'\}$. Sia $[a] \subseteq [a']$: preso un elemento $x \in [a]$, si ha ovviamente che $x \sim a$. Poiché $a \sim a'$, per la proprietà transitiva $x \sim a'$ quindi $x \in [a']$, e viceversa per simmetria: allora $[a] \equiv [a']$. Poniamo ora le due classi coincidenti, siccome $a \in [a]$ e $a' \in [a']$, poichè le due classi coincidono si ha che a appartiene anche ad $[a']$ e a' appartiene anche ad $[a]$, quindi $a \sim a'$. □

Teorema 1.2.4. Due classi di equivalenza sono distinte se e solo se sono disgiunte: se $[a] \neq [b]$ allora $[a] \cap [b] = \varnothing$.

Dimostrazione. Sia per assurdo che esista un elemento $c \in [a] \cap [b]$. Allora esso è in relazione sia con a che con b, ma allora per la proprietà transitiva $a \sim b$, quindi le due classi coincidono, il che è una contraddizione. Le due classi devono quindi essere disgiunte. □

Le classi distinte individuate da una relazione di equivalenza in X costituiscono una partizione di X.

Definizione 1.2.5. *Sia $\{S_i\}_{i\in I}$ una famiglia di sottoinsiemi di un insieme X. Tale famiglia si dice* partizione *di X se:*

- $S_i \neq \varnothing \ \forall i \in I$;
- $S_i \cap S_j = \varnothing$ *per ogni* $i \neq j$;
- $\bigcup_{i\in I} S_i \equiv X$.

Sia $\{S_i\}_{i\in I}$ una partizione di un insieme X: si può sempre definire una relazione di equivalenza $\sim$ su X, ponendo che $\forall a, b \in X$, $a \sim b$ se e solo se $\exists i \in I \colon a, b \in S_i$. Una tale relazione soddisfa la definizione di relazione di equivalenza:

1. Qualsiasi $a \in X$ sta in almeno uno dei sottoinsiemi S_i, per il terzo punto della 1.2.5, quindi $a \sim a$.
2. Se esiste un $i \in I$ per cui $a, b \in S_i$, certamente scambiando l'ordine di b e a entrambi appartengono comunque a S_i, quindi se $a \sim b$ anche $b \sim a$.
3. Se $a \sim b$ e $b \sim c$, allora esiste $i \in I$ per il quale $a, b \in S_i$ ed esiste un altro indice $j \in I$ per cui $b, c \in S_j$. Se $i \neq j$, però, b non potrebbe appartenere ad entrambi perché la loro intersezione sarebbe vuota. Allora $i = j$, e per tale indice $a, b, c \in S_i$ (o S_j), quindi $a \sim c$.

1.3 Anelli

Definizione 1.3.1. *Un insieme non vuoto A, dotato di due operazioni binarie interne $*$ e $\diamond$, si dice anello se valgono le seguenti proprietà:*

1. $(A, *)$ *è un gruppo abeliano;*
2. $(A, \diamond)$ *è un semigruppo, cioè è solo associativo;*
3. $\forall a, b, c \in A$ *valgono* $(a * b) \diamond c = (a \diamond c) * (b \diamond c)$ *e* $a \diamond (b * c) = (a \diamond b) * (a \diamond c)$.

Intenderemo sempre che la seconda operazione avrà sempre la precedenza sulla prima, se non diversamente specificato: vale a dire, $x * y \diamond z$ significherà $x * (y \diamond z)$; in caso contrario si usano le parentesi dove necessario. D'ora in poi, per mantenere una notazione più familiare e semplice, ci riferiremo all'operazione $*$ come ad un'*addizione* (e la indicheremo con $+$), e all'operazione $\diamond$ come ad una *moltiplicazione*. Infatti l'addizione e la moltiplicazione che tutti conosciamo soddisfano questi assiomi, che comunque possono essere generalizzati ad operazioni differenti, come il prodotto tra polinomi o matrici.

L'anello si dice *commutativo* se anche $(A, \cdot)$ è commutativo, cioè $ab = ba \ \forall a, b \in A$; la commutatività dell'addizione è sempre garantita dal fatto che $(A, +)$ è abeliano. L'elemento neutro dell'addizione in un anello esiste sempre, dato che $(A, +)$ è un gruppo: indicheremo tale elemento con 0, o con 0_A se ci sarà bisogno di specificare l'anello al quale appartiene. L'esistenza dell'elemento neutro della moltiplicazione, invece, non è data per certa: se esiste, l'anello si dice *dotato di unità*, e la indicheremo con 1 o 1_A.

Ecco alcuni esempi di anelli.

- $\mathbb{Z}$ è un anello con le usuali operazioni di addizione e moltiplicazione, come del resto $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e ogni altro campo.
- L'insieme $K[x]$ dei polinomi (di grado qualunque) con termini presi da un campo K forma un anello con le note operazioni di somma e prodotto tra polinomi.

Definiamo per $n \in \mathbb{Z}$ l'addizione di a con se stesso $n - 1$ volte come

$$na = \underbrace{a + a + \cdots + a}_{n \text{ volte}}, \tag{1.3.1}$$

per $n \in \mathbb{N}$, e con $0a = 0_A$; per $n < 0$, basta porre $na = -(-n)a$ per ricondursi ai casi precedenti. Definiamo poi a moltiplicato con se stesso $n-1$ volte come

$$a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ volte}} \tag{1.3.2}$$

con $n > 0$, e (se esiste l'unità) $a^0 = 1_A$. Per $n < 0$ questa operazione non è definita.

Ricaviamo alcune semplici proprietà delle due operazioni.

- $0_A a = a 0_A = 0_A$. Possiamo infatti scrivere sempre $0_A a = (0_A + 0_A)a$, e per la proprietà distributiva abbiamo $0_A a = 0_A a + 0_A a$, per cui aggiungendo l'opposto $-0_A a$ ai due membri (esiste sempre, essendo $(A, +)$ un gruppo) troviamo $0_a a = 0$. La dimostrazione è analoga per $a0_A$.
- $(na)b = a(nb) = n(ab)$, che di dimostra facilmente sfruttando la proprietà distributiva partendo da $(a + a + \cdots + a)b$.
- $a(-b) = (-a)b = -(ab)$, ponendo $n = -1$ nella precedente.

Definizione 1.3.2. *Un elemento $a \neq 0_A$ di un anello A si dice* divisore dello zero *se esiste un elemento $b \in A$ tale che $ab = 0_A$ oppure $ba = 0_A$.*

Ovviamente i due casi coincidono se l'anello è commutativo, ma in generale non lo si può affermare.

Esempi

- L'insieme $\mathscr{C}(-1, 1)$ delle funzioni $f\colon (-1, 1) \to \mathbb{R}$ continue è un anello con addizione e moltiplicazione. In esso, definiamo le funzioni

$$f(x) = \begin{cases} 0 & -1 < x < 0 \\ x^2 & 0 \leq x < 1 \end{cases} \qquad \text{e} \qquad g(x) = \begin{cases} x^2 & -1 < x < 0 \\ 0 & 0 \leq x < 1 \end{cases}$$

  La f è un divisore dello zero, in quanto g non è la funzione identicamente nulla di $\mathscr{C}(-1, 1)$, ma $fg = 0$ per ogni $x \in (-1, 1)$. Per lo stesso motivo, ovviamente, anche g è divisore dello zero.

Teorema 1.3.3. Un anello A è privo di divisori dello zero se e solo se valgono le leggi di cancellazione per il prodotto.[1]

Dimostrazione. Supponiamo che A sia un anello privo di divisori dello zero, e prendiamo l'ipotesi $ax = ay$: dalla proprietà distributiva si ha $a(x - y) = 0$. Dato che non esistono divisori dello zero in A, se $a \neq 0$ deve necessariamente essere $x - y = 0$, ossia $x = y$. La dimostrazione per $xa = ya \Rightarrow x = y$ è del tutto analoga.

Partiamo ora dalle relazioni $ax = ay \Rightarrow x = y$ e $xa = ya \Rightarrow x = y$. Se esistessero $x, y \neq 0$ tali che $xy = 0$ (ossia x e y divisori dello zero), allora risulterebbe anche $xy = 0 = x0$ da cui $y = 0$, poiché valgono le leggi di cancellazione del prodotto. Ma ciò contraddice l'ipotesi che $x, y \neq 0$ quindi tali x e y non possono esistere: allora A è privo di divisori dello zero. □

Definizione 1.3.4. *Sia A un anello con unità. Un elemento $a \in A$ si dice* invertibile *se esiste $b \in A$ tale per cui $ab = ba = 1$. Tale b si indica con a^{-1}.*

Teorema 1.3.5. Se A è un anello dotato di unità, i suoi elementi invertibili non sono divisori dello zero.

[1] Ossia se per ogni $a, x, y \in A$ con $a \neq 0$ le relazioni $ax = ay$ e $xa = ya$ implicano $x = y$.

Dimostrazione. Se esistesse un elemento $a \in A$ invertibile e divisore dello zero, allora esisterebbe un elemento $b \in A \setminus \{0\}$ tale che $ab = 0$. Si ottiene però che

$$b = 1b = a^{-1}ab = a^{-1}0 = 0 \tag{1.3.3}$$

ossia $b = 0$, che contraddice l'ipotesi $b \neq 0$ legata all'esistenza di b. Dunque non può esistere un tale b: vale a dire, a non è un divisore dello zero. $\square$

Definizione 1.3.6. *Un anello si dice* dominio d'integrità *se è commutativo ed è privo di divisori dello zero.*

Sono domini d'integrità gli anelli di $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con le usuali operazioni di somma e prodotto.

Definizione 1.3.7. *Si chiama* corpo *un anello dotato di unità in cui ogni elemento non nullo è invertibile.*

Definizione 1.3.8. *Si dice* campo *un corpo commutativo con almeno due elementi.*

Il piccolo teorema di Wedderburn afferma, inoltre, che ogni corpo finito è un campo. Possiamo dare una definizione alternativa di campo, equivalente alla precedente, basata su degli assiomi.

Definizione 1.3.9. *Si definisce* campo *la terna $(K, +, \cdot)$ in cui K è un insieme non vuoto e $+$ e $\cdot$ sono operazioni interne $K \times K \to K$, per le quali:*

- *$(K, +)$ è un gruppo abeliano, con elemento neutro 0_K;*
- *$(K \setminus \{0_K\}, \cdot)$ è un gruppo abeliano, con elemento neutro 1_K;*
- *vale la proprietà distributiva, per cui $\forall a, b, c \in K$ vale $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Questa definizione è in sostanza una generalizzazione della struttura di $(\mathbb{R}, +, \cdot)$. È quindi, ovviamente, un campo $(\mathbb{R}, +, \cdot)$, e lo sono anche $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.

1.4 Ideali

Definizione 1.4.1. *Sia A un anello e I un suo sottoinsieme. Se $(I, +)$ è un sottogruppo di $(A, +)$ e per ogni $x \in I$ e $a \in A$:*

- *$ax \in I$, allora I è detto* ideale sinistro*;*
- *$xa \in I$, allora I è detto* ideale destro*;*
- *$ax, xa \in I$, allora I è detto* ideale bilatero*.*

In altre parole, preso un elemento di un ideale sinistro (destro) possiamo moltiplicarlo a sinistra (destra) per qualsiasi elemento dell'anello e ottenere ancora un elemento dell'ideale. Nel caso di un anello commutativo, le tre definizioni naturalmente coincidono, e parleremo semplicemente di *ideale*.

Dalla chiusura di I rispetto alla somma otteniamo inoltre che qualsiasi ideale deve sempre contenere lo zero dell'anello. Ogni anello ammette sempre due ideali detti *banali*: $\{0\}$ e l'anello A stesso. Gli ideali non banali sono detti *propri*. Se l'anello è dotato di unità, allora un ideale è proprio se e solo se non la contiene: se infatti $I \ni 1$, allora poiché il prodotto $1a$ per qualsiasi a nell'intero anello deve essere incluso in I, tale ideale contiene tutti gli elementi di A, ma allora $I = A$.

Degli esempi importanti di ideali, che incontreremo in seguito, sono i seguenti.

- Dato $p \in \mathbb{Z}$, chiamiamo $p\mathbb{Z}$ l'insieme $\{x \in \mathbb{Z} \colon x = np, n \in \mathbb{Z}\}$ ossia l'insieme dei multipli interi di un certo intero p. Se $x, y \in p\mathbb{Z}$, siano essi $x = np$ e $y = mp$, allora $x + y = (n + m)p$ e poiché $n + m \in \mathbb{Z}$ allora $x + y \in p\mathbb{Z}$. Per un qualunque $z \in \mathbb{Z}$, inoltre, $xz = npz = (nz)p$ e $nz \in \mathbb{Z}$ quindi $xz \in p\mathbb{Z}$. L'insieme $p\mathbb{Z}$ è dunque un ideale di $\mathbb{Z}$, per qualunque p.

- I numeri pari formano l'insieme $2\mathbb{Z}$, che è un ideale per il punto precedente. I numeri dispari, invece, non formano un ideale, in quanto non comprendono lo zero.
- Nell'anello delle funzioni continue $\mathscr{C}(\mathbb{R})$, è un ideale l'insieme delle funzioni che si annullano in un dato punto, ad esempio per cui $f(1) = 0$.

Definiamo ora alcuni tipi particolari di ideali (per semplicità, le daremo per anelli commutativi).

Definizione 1.4.2. *Un ideale I di un anello A è detto* primo *se:*

- *è un sottoinsieme proprio di A;*
- *se $a, b \in A$ sono tali che $ab \in I$, allora almeno uno dei due appartiene a I.*

Questo concetto ricalca la definizione di *numeri primi*: se un numero $p \in \mathbb{Z}$ è primo, ogni volta che divide un prodotto xy con $x, y \in \mathbb{Z}$ allora p divide a oppure b. Le due definizioni sono in effetti collegate: un numero intero (positivo) n è primo se e solo se $n\mathbb{Z}$ è un ideale primo.

Definizione 1.4.3. *Un ideale A si dice* massimale *se $I \neq A$, per ogni ideale $J \supseteq I$ si ha o che $J = I$ oppure $J = A$.*

Gli ideali massimali sono dunque degli elementi massimali rispetto all'operazione di inclusione insiemistica tra gli *ideali propri* di un anello (escludendo quindi dalle opzioni l'anello stesso). Essi non sono contenuti propriamente in nessun altro ideale proprio dell'anello.

Se ogni elemento x di un ideale I, di un anello A, può essere scritto come

$$x = \sum_{i=1}^{n} a_k i_k$$

con $a_k \in A$ e $i_k \in I$, ossia come combinazione lineare di un numero finito di suoi elementi $\{i_k\}_{k=1}^{n}$, diciamo che l'ideale è *generato* da tali elementi, e si indica solitamente come $I = (i_1, \dots, i_n)$. Il caso in cui l'ideale è generato da un solo elemento è di particolare importanza, e merita una sua definizione.

Definizione 1.4.4. *Un ideale I di un anello A si dice* principale *se è generato da un solo elemento.*

In linea con la notazione precedente, l'ideale principale generato da a si indica con (a). Si può dimostrare che l'ideale principale (a) è il più piccolo ideale che comprende a.

1.5 Anelli quoziente

Riprendiamo ora le relazioni di equivalenza, introdotte nel capitolo 1.2. Dati un ideale (bilatero) I di un anello A e due elementi $a, b \in A$, stabiliamo la relazione

$$a \sim b \Leftrightarrow a - b \in I.$$

È facile vedere, con le proprietà degli ideali, che tale relazione è anche di congruenza. Se $a \sim b$ si dice anche che a e b sono *congruenti modulo I*. Da essa possiamo costruire le classi di equivalenza nell'anello: la classe $[a]_I$ (indichiamo con il pedice $[\cdot]_I$ il fatto che la relazione è basata sull'ideale I, per maggiore chiarezza) consiste in tutti quegli elementi x di A che "distano a dall'ideale I", ossia tali per cui $x - a \in I$. Alternativamente, gli elementi $x \in [a]_I$ sono la somma di a e di un elemento dell'ideale I, e per questo motivo si indica la classe di equivalenza come $I + a$. Formalmente, dunque,

$$[a]_I = I + a = \{x \in A : x = a + i, i \in I\}.$$

Possiamo definire delle operazioni su queste classi come di seguito:

- l'addizione di $[a]_I = I + a$ e $[b]_I = I + b$ come la classe di rappresentante $a + b$, ossia $I + (a + b)$;

- analogamente, la moltiplicazione di due classi $[a]_I[b]_I = (I+a)(I+b)$ come la classe che ha come rappresentante il prodotto dei due rappresentanti, ossia $I+ab$.

Si può verificare che queste operazioni sono ben definite, ossia che non dipendono dalla scelta dei rappresentanti. Con queste due operazioni, l'insieme delle classi di equivalenza forma un anello, detto *anello quoziente* (rispetto alla relazione stabilita).

Definizione 1.5.1. *Dato un ideale bilatero I di un anello A, si chiama* anello quoziente *l'insieme, indicato con $A\,/\,I$, delle classi di equivalenza $[a]_I = \{x \in A\colon x = a+i, i \in I\}$, con le operazioni*

$$\begin{gathered}(I+a)+(I+b) = I+(a+b)\\ (I+a)(I+b) = I+ab.\end{gathered} \tag{1.5.1}$$

Lo zero dell'anello quoziente è indicato come $I+0$, ed è chiaramente l'ideale I stesso. Notiamo che se $a \in I$, allora $I+a$ è ancora lo zero di $A\,/\,I$: infatti, essendo I chiuso rispetto alla somma, l'addizione di un elemento dell'ideale (cioè I) con a (che è in I) produce ancora un elemento nell'ideale, vale a dire un elemento di $I = I+0$. L'identità moltiplicativa, se esiste, sarà indicata con $I+1$.

Proviamo a prendere il quoziente di A con gli ideali banali.

- Per $I = \{0\}$, scelto un $a \in A$ abbiamo che $b \in [a] = I+a$ se $b-a \in I$, cioè $b-a=0$: ma ciò è possibile solo se $b=a$, dunque $I+a = \{a\}$ per qualsiasi $a \in A$.
- Per $I = A$, se $b \in I+a$ dovrà essere $b-a \in A$: questo è sempre vero qualsiasi sia b, quindi $I+a = A$ per qualsiasi a! Ciò significa che $A\,/\,A$ è composto da un solo elemento.

L'ideale $I = 2\mathbb{Z}$ di $\mathbb{Z}$ è massimale: infatti se un ideale J contiene I, allora $J = k\mathbb{Z}$ per un $k \in N$ che sia divisore di 2. Ma allora $k \in \{1,2\}$, cioè $k\mathbb{Z}$ è ancora $2\mathbb{Z}$ oppure è tutto $\mathbb{Z}$. Perciò $2\mathbb{Z}$ è un ideale massimale; lo stesso di dimostra per qualsiasi $p\mathbb{Z}$ con p primo. Questo risultato si generalizza nel seguente teorema.

Teorema 1.5.2. Sia A un anello commutativo con unità e sia $I \subset A$ un ideale proprio: allora I è primo se e solo se A/I è un dominio d'integrità.

Dimostrazione. Supponiamo che $A\,/\,I$ sia un dominio di integrità, per cui prese due classi $I+a$ e $I+b$, se $I+ab = I+0$ deve necessariamente risultare $I+a = I+0$ oppure $I+b = I+0$. Passando dalle classi di $A\,/\,I$ agli elementi di A, il fatto che $I+ab$ sia $I+0$ significa che ab è nell'ideale I. Analogamente se $I+a = I+0$ significa che $a \in I$. Ma ciò vuol dire che se $ab \in I$ allora uno dei due tra a e b è necessariamente nell'ideale: questa è proprio la definizione di ideale primo, quindi I è primo.

Sia ora I un ideale primo: se $ab \in I$, almeno uno tra a e b deve appartenere a I. Nel linguaggio delle classi di equivalenza ciò significa che se $(I+a)(I+b) = I+ab = I+0$, allora $I+a = I+0$ oppure $I+b = 0$. Queste affermazioni sono equivalenti a dire che non esistono $a, b \notin I$ tali che $ab \in I$, cioè

$$\nexists I+a, I+b \in A\,/\,I\colon (I+a)(I+b) = I+0$$

quindi $A\,/\,I$ è un dominio di integrità. □

Teorema 1.5.3. Sia A un anello commutativo con unità e sia $I \subset A$ un ideale proprio: I è massimale se e solo se A/I è un campo.

Dimostrazione. Sia I un ideale massimale: allora non può esistere un ideale J tale che $I \subset J \subset A$. Dimostriamo che $A\,/\,I$ è un campo mostrando che ogni suo elemento non nullo è invertibile. Sia $I+a$ un elemento non nullo di $A\,/\,I$, ossia deve essere $a \notin I$. Fissato questo elemento, costruiamo l'insieme $J_a = \{j \in A\colon j = i+ax, i \in I, x \in A\}$. Sicuramente, poiché A è commutativo, lo è anche J_a. Inoltre è anche un ideale: infatti, dati $j_1 = i_1 + ax_1$, $j_2 = i_2 + ax_2$ e $b \in A$ abbiamo

$$\begin{gathered} j_i + j_2 = \underbrace{i_1 + i_2}_{\in I} + a(\underbrace{x_1 + x_2}_{\in A}) \in J_a;\\ j_1 b = (i_1 + ax_1)b = \underbrace{i_1 b}_{\in I} + a(\underbrace{x_1 b}_{\in A}) \in J_a.\end{gathered} \tag{1.5.2}$$

Tutti gli elementi $i \in I$ sono della forma $i + a0$, dunque $I \subseteq J$. Esistono anche elementi di J che non appartengono a I? Dato che I è proprio, non può contenere l'unità, come avevamo già visto. Allora l'elemento $i + a1 = i + a$ appartiene a J, ma non a I.[2] Di conseguenza $I \subset J$: per la massimalità di I, però, ciò implica $J \equiv A$. Perciò J deve contenere l'unità, che potremo dunque scrivere come $i^* + ax^*$ per qualche $i^* \in I$ e $x^* \in A$. Preso questo x^*, vediamo che la classe $I + x^* \in A \,/\, I$ è l'inverso di $I + a$:

$$(I + x^*)(I + a) = I + ax^* = I + (1 - i^*) = I + 1 \tag{1.5.3}$$

poiché se $i^* + ax^* = 1$ allora $ax^* = 1 - i^*$, e $I - i^* = I$. Ma $I + 1$ è l'unità di $A \,/\, I$, dunque ogni elemento non nullo (ossia con $a \notin I$) di $A \,/\, I$ ammette un inverso: ciò prova che $A \,/\, I$ è un campo.

Sia ora $A \,/\, I$ un campo: allora, poiché deve possedere almeno due elementi, I non può essere uguale ad A, perché come abbiamo già visto $A \,/\, A$ contiene un solo elemento. Dunque I è un ideale proprio. Prendiamo ora un ideale J tale che $I \subseteq J \subseteq A$ con $I \neq J$. Esiste dunque un x che appartiene a J ma non a I, di conseguenza $I + x \neq I + 0$. Non essendo l'elemento nullo di $A \,/\, I$, che per ipotesi è un campo, $I + x$ è invertibile: esiste una classe $I + y \in A \,/\, I$ tale per cui

$$I + 1 = (I + y)(I + x) = I + xy,$$

quindi $xy = 1 + i^*$ per qualche $i^* \in I$. Ora, $I \subseteq J$, perciò $i^* \in J$, e analogamente $x \in J$ quindi anche $xy \in J$: ma allora anche $1 = xy - i^*$ appartiene a J. Dato che J contiene l'unità, segue necessariamente che $J = A$, perciò I è massimale. □

Corollario 1.5.4. In un anello commutativo con unità, ogni ideale massimale è primo.

Dimostrazione. Se I è massimale, per il teorema 1.5.3 $A \,/\, I$ è un campo, quindi in particolare è anche un dominio di integrità: ma allora dal teorema 1.5.2 I è primo. □

L'implicazione inversa, ossia che ogni ideale primo è massimale, in generale è falsa (il problema sta nell'affermazione "un campo è un dominio d'integrità", che non si può invertire). Vedremo in che ambito essa è vera quando introdurremo i domini *a ideali principali.*

1.6 Omomorfismi di anelli

Definizione 1.6.1. *Siano* $(A, +, \cdot)$ *e* $(B, *, \diamond)$ *due anelli: un* omomorfismo *di anelli è un'applicazione* $\varphi\colon A \to B$ *che preserva le operazioni, cioè tale che per ogni* $a, b \in A$ *si ha*

$$\varphi(a + b) = \varphi(a) * \varphi(b) \;\text{ e }\; \varphi(ab) = \varphi(a) \diamond \varphi(b). \tag{1.6.1}$$

Se gli anelli sono dotati di unità, si richiede che l'omomorfismo, oltre alle operazioni, preservi anche l'unità, ossia $\varphi(1_A) = 1_B$.

Ad esempio la funzione da $\mathbb{Z}$ in sé definita come $\varphi(a) = 0$ per qualsiasi $a \in \mathbb{Z}$, cioè che porta qualsiasi elemento nello zero, chiaramente preserva le operazioni, ma non è un omomorfismo d'anelli in quanto $\varphi(1) = 0$ che ovviamente non è l'unità di $\mathbb{Z}$.

Definizione 1.6.2. *Sia* $\psi\colon A \to B$ *un omomorfismo di anelli. Si definisce* nucleo *di* ψ *e si denota con* $\operatorname{Ker}\psi$ *l'insieme*

$$\operatorname{Ker}\psi = \{a \in A \colon \psi(a) = 0_B\},$$

ossia l'insieme degli elementi di A *che hanno lo zero di* B *come immagine.*

Teorema 1.6.3. Se $\psi\colon A \to B$ è un omomorfismo di anelli, allora il suo nucleo è un ideale di A.

[2] Se $i + a \in I$, ossia $i + a = i'$ per qualche $i' \in I$, allora seguirebbe che $a = i' - i$, cioè $a \in I$.

Dimostrazione. Verifichiamo le proprietà di ideale: per $x, y \in \operatorname{Ker}\psi$ e $a \in A$, si ha

$$\psi(x+y) = \psi(x) + \psi(y) = 0_B + 0_B = 0_B \tag{1.6.2}$$

quindi $x + y \in \operatorname{Ker}\psi$, e

$$\psi(ax) = \psi(a)\psi(x) = \psi(a)0_B = 0_B \tag{1.6.3}$$

quindi anche $ax \in \operatorname{Ker}\psi$, e analogamente per xa. Allora $\operatorname{Ker}\psi$ è proprio un ideale di A. □

Come già visto negli omomorfismi tra gruppi, anche un omomorfismo tra gli anelli A e B è iniettivo se e solo se il suo nucleo è $\{0_A\}$. Se l'anello è commutativo, i suoi ideali sono tutti anche nuclei di omomorfismi di anelli.

1.7 Anelli dei polinomi

Passiamo ora a trattare un tipo di anelli molto importante: gli anelli composti da polinomi.

Definizione 1.7.1. *Si dice* polinomio *a coefficienti in un anello A una successione di elementi di A definitivamente nulla:*

$$p = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots).$$

I polinomi si rappresentano anche, più comunemente, indicando il posto di ogni elemento della successione con delle potenze di un'incognita, come ad esempio

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n. \tag{1.7.1}$$

Generalmente, indicheremo i polinomi semplicemente con delle lettere, senza usare la notazione "funzionale" $p(x)$ ma solo p. Useremo $p(x)$ invece quando esprimeremo il polinomio tramite le potenze di x, per evitare di confonderlo con i termini noti.

L'ultimo coefficiente non nullo del polinomio, a_n, che nella scrittura predecente è il coefficiente assegnato alla potenza di grado massimo, si dice *coefficiente direttivo.* Il termine a_0 è invece il *termine noto.*

Tra polinomi definiamo la somma come

$$\begin{aligned}(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) + (b_0, b_1, b_2, \dots, b_m, 0, 0, \dots) = \\ (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_m + b_m, a_{m+1} + 0, a_{m+2} + 0, \dots, a_n, 0, 0, \dots),\end{aligned} \tag{1.7.2}$$

dove in questo caso $n > m$, e il prodotto come il polinomio che ha come componente di posto k il coefficiente

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}. \tag{1.7.3}$$

Con queste due operazione è facile vedere che $A[x]$, l'insieme dei polinomi a coefficienti in A, è a sua volta un anello. Il polinomio unità di $A[x]$ è il polinomio avente come primo coefficiente l'unità di A, 1_A, e tutti i successivi nulli; il polinomio nullo è il polinomio con tutti i coefficienti nulli.

Possiamo definire un'applicazione lineare $j \colon A \to A[x]$ che porta un elemento di A nel polinomio avente come termine noto tale elemento, ossia la mappa

$$j(a) = (a, 0, 0, \dots).$$

Tale applicazione è un omomorfismo di anelli, in quanto preserva le operazioni e l'unità: infatti dati $a, b \in A$ risulta

$$\begin{aligned} j(a+b) = (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = j(a) + j(b) \\ j(ab) = (ab, 0, 0, \dots) = (a, 0, 0, \dots)(b, 0, 0, \dots) = j(a)j(b), \end{aligned}$$

mentre porta l'unità 1_A nel polinomio $(1_A, 0, 0, \dots)$ che è l'unità di $A[x]$. Si nota facilmente anche che tale omomorfismo j è iniettivo, dato che $\operatorname{Ker} j = \{0_A\}$.

Ordinando gli elementi del polinomio in ordine di indici crescenti, la posizione del coefficiente direttivo indica il *grado* del polinomio, che quando scritto come combinazione lineare di potenze è anche il grado della potenza massima che appare.

Un polinomio non nullo $p(x) = a_n x^n + \cdots + a_0 \in A[x]$, con $a_n \neq 0$, si dice di grado n, e si indica con $\deg p = \deg p(x) = n$. Convenzionalmente si assegna al polinomio (identicamente) nullo il grado -1. Se $a_n = 1$, il polinomio si dice *monico*.

Proprietà 1.7.2. Si hanno le seguenti proprietà tra i gradi dei polinomi e le operazioni:

- $\deg(a + b) \leq \max\{\deg a, \deg b\}$;
- $\deg(ab) \leq \deg a + \deg b$.[3]

Ad esempio, nell'anello $\mathbb{Z} / 12\mathbb{Z}$, si considerino i due polinomi $a(x) = [6]x^2$ e $b(x) = [2]x$: si ha che $\deg a = 2$ e $\deg b = 1$. La loro somma è un polinomio di grado 2, ma per il prodotto si vede che sebbene nell'anello [6] e [2] non siano nulli, lo è il loro prodotto perché 12 appartiene alla stessa classe di equivalenza di 0, quindi $a(x)b(x) = [6][2]x^3 = [12]x^3 = [0]x^3 = [0]$; di conseguenza $\deg\big(ab\big) = -1 \neq \deg a + \deg b = 3$. Le due proprietà precedenti sono in ogni caso rispettate.

Il caso dell'uguaglianza accade quindi soltanto se non esistono divisori dello zero nell'anello, vale a dire che esso è un dominio d'integrità: in questo caso il prodotto di due elementi non nulli non è mai nullo.

Siano A e B due anelli con unità, e $f \colon A \to B$ un omomorfismo d'anelli con unità. Anche $\tilde{f} \colon A[x] \to B[x]$ definito come $\tilde{f}\big(p(x)\big) = f(a_n)x^n + \cdots + f(a_0)$, con $f(a_i) \in B$, allora, è un omomorfismo di anelli con unità. Non è detto però che sia $\deg \tilde{f}(p) = \deg p$: potrebbe accadere infatti che il coefficiente direttivo di p appartenga al nucleo di f. Infine, come richiesto dalla definizione, $\tilde{f}(1_{A[x]}) = \big(f(1_A), 0, 0, \dots\big) = (1_B, 0, 0, \dots) = 1_{B[x]}$.

1.8 Divisione tra polinomi

Sia $K[x]$ l'anello dei polinomi su un campo K: non avendo divisori dello zero, $ab \neq 0_K$ se a e b (elementi di K) non sono nulli. Vale sempre, allora, l'uguaglianza $\deg(fg) = \deg f + \deg g$.

Teorema 1.8.1 (Algoritmo euclideo delle divisioni successive)**.** Sia K un campo, e $a, b \in K[x]$, con b diverso dal polinomio nullo. Esistono sempre, e sono unici, due polinomi r e q tali che

$$a = qb + r, \text{ con } \deg r < \deg b. \tag{1.8.1}$$

Dimostrazione. Dimostriamo l'esistenza dei due polinomi, per induzione, su $n = \deg a$. Se $n = -1$, allora $q = r = 0$, cioè $qb + r = 0$, e poiché per ipotesi $\deg b \neq -1$ perché non è nullo, si ha automaticamente che $\deg b > -1 = \deg r$. I due polinomi cercati quindi sono entrambi dei polinomi identicamente nulli. Sia ora $n > -1$, e siano $a(x) = a_n x^n + \cdots + a_0$, $b(x) = b_m x^m + \cdots + b_0$.

- se $m > n$, allora poniamo $a = 0 \cdot b + a$ (scegliamo cioè $q = 0$ nella (1.8.1)), e ciò significa che il resto è proprio a. Dunque $\deg r = n < m = \deg b$.
- se $m \leq n$, definiamo $\tilde{a} = \tilde{a}(x) = a(x) - b_m^{-1} a_n x^{n-m} b(x)$. Il coefficiente di grado massimo dell'ultimo termine è $-b_m^{-1} a_n x^{n-m} b_m x^m = -b_m^{-1} b_m a_n x^{n-m+m} = -a_n x^n$, quindi $\deg \tilde{a} \leq n - 1$ poiché il coefficiente di grado n, che è il grado massimo di a, è cancellato. Per l'ipotesi di induzione, quindi, esistono due polinomi $\tilde{q}$ e $\tilde{r}$ tali che $\tilde{a} = \tilde{q}b + \tilde{r}$, per cui $\deg \tilde{r} < \deg b$. Risulta quindi

$$\begin{aligned} a(x) &= \tilde{q}(x)b(x) + b_m^{-1} a_n x^{n-m} b(x) + \tilde{r}(x) = \\ &= \big(\tilde{q}(x) + b_m^{-1} a_n x^{n-m}\big) b(x) + \tilde{r}(x). \end{aligned}$$

[3] Contrariamente a ciò che ci si aspetterebbe, non è un'uguaglianza perché pur essendo i coefficienti direttivi dei due polinomi non nulli, potrebbero esistere divisori dello zero in A, dunque non è detto che se $a, b \in A$ non sono nulli si abbia necessariamente $ab \neq 0$.

Scelti $q(x) = \tilde{q}(x) + b_m^{-1} a_n x^{n-m}$ e $r(x) = \tilde{r}(x)$, si ha dunque l'uguaglianza $a = qb + r$ con $\deg r = \deg \tilde{r} < \deg b$.

Abbiamo trovato dunque che q e r secondo la (1.8.1) esistono sempre, qualunque sia il grado di a.

Siano q, r e $\overline{q}, \overline{r} \in A[x]$ tali da soddisfare entrambe (le coppie) la (1.8.1), ossia che $a = \overline{q}b + \overline{r}$ e $a = qb + r$, con $\deg \overline{r} < \deg b$ e $\deg r < \deg b$. Allora risulta

$$0 = a - a = (q - \overline{q})b + r - \overline{r} \tag{1.8.2}$$

Per la prima delle 1.7.2 risulta $\deg\big(r - \overline{r}\big) < \max\{\deg r, \deg \overline{r}\} < \deg b$. Se $\overline{q} \neq q$, poiché la loro differenza non sarebbe un polinomio nullo, si avrebbe $\deg(q - \overline{q}) \geq 0$, e il prodotto $(\overline{q} - q)b$ darebbe un polinomio di grado sicuramente maggiore di quello di b, poiché K non ha divisori dello zero: dunque $\deg\big((q - \overline{q})b\big) > \deg b$. Ma se dalla (1.8.2) risulta $(\overline{q} - q)b = r - \overline{r}$, quindi i loro gradi devono essere uguali. Troviamo allora

$$\deg(r - \overline{r}) = \deg\big((\overline{q} - q)b\big) > \deg b > \deg(r - \overline{r}) \tag{1.8.3}$$

che è chiaramente un assurdo. Di conseguenza deve essere $\overline{q} = q$ e $\overline{r} = r$, cioè i polinomi quoziente e resto sono unici. □

La dimostrazione di questo teorema è molto rigorosa, ma non è che una trascrizione "più tecnica" di quello che dovrebbe già essere noto dalla divisione tra polinomi (ma anche tra numeri naturali!):

- Se a è nullo, allora quoziente e resto sono entrambi nulli.
- Se a ha un grado minore di b, il quoziente è nullo e il resto è a stesso.
- Se a ha un grado maggiore di b, allora abbiamo una divisione "non banale" e ci aspettiamo un quoziente che ha come grado la differenza tra quelli di a e b.

Quando il resto della divisione è nullo, ossia $a = qb$, diremo che b *divide* a, e lo indicheremo con la notazione $a|b$. Poiché gli elementi dell'ideale principale (a) sono della forma ax per $x \in A$, vediamo subito che $a|b$ implica $b \in (a)$, e viceversa.

Definizione 1.8.2. *Dato un campo K, siano $a, b \in K[x]$ due polinomi non nulli. Si dice* massimo comune divisore *tra a e b ogni polinomio $d \in K[x]$ tale che:*

- *d divide sia a che b;*
- *se un altro polinomio c divide a e b, allora divide anche d.*

Questa definizione ricalca quella del massimo comune divisore tra numeri interi. Per i numeri in $\mathbb{Z}$, però, è noto che se z è il massimo comune divisore tra m e n, allora lo è anche $-z$. Anche per i polinomi vale un risultato simile: dato un massimo comune divisore in $K[x]$, tutti i suoi multipli per una costante in K lo sono ancora.

Teorema 1.8.3. Siano $a, b \in K[x]$ non nulli, e d un massimo comun divisore tra i due. Se d' è un altro massimo comune divisore, allora vale la relazione $d' = kd$ per qualche $k \in K \setminus \{0\}$.

Dimostrazione. Per la definizione di massimo comune divisore, d e d' dividono entrambi a e b, e si dividono a vicenda, ossia $d|d'$ e $d'|d$. Dunque esistono $\alpha, \beta \in K[x]$ tali che $d = \alpha d'$ e $d' = \beta d$. Otteniamo da queste due uguaglianze che $d = \alpha\beta d$. Poiché $d \neq 0$ — altrimenti dovrebbe essere $a = 0$, contro le ipotesi fatte — per le leggi di cancellazione si ha $\alpha\beta = 1$. La somma dei gradi di α e β deve quindi essere nulla, cioè il grado del polinomio unità: l'unico modo possibile affinché accada è che $\deg \alpha = \deg \beta = 0$, ossia che entrambi siano, oltre che polinomi, anche elementi (scalari) del campo K, cioè $\alpha = k \in K$ e $\beta = h \in K$. Ma allora $hk = 1$, cioè h e k sono invertibili, perciò non possono essere nulli. Dunque $d' = kd$ con $k \in K \setminus \{0\}$. □

A causa di questa arbitrarietà nella costante moltiplicativa, è conveniente stabilire la seguente definizione.

Definizione 1.8.4. *Dati $a, b \in K[x]$ non nulli, il massimo comune divisore di a e b con coefficiente direttivo unitario è detto* massimo comune divisore monico.

D'ora in poi, quando ci riferiremo al massimo comune divisore, sottintenderemo che prendiamo quello monico.

Teorema 1.8.5 (Algoritmo di Euclide)**.** Dato un campo K, e $a, b \in K[x]$ non nulli, esiste sempre un massimo comune divisore tra di loro.

Dimostrazione. Dato che $b \neq 0$, esistono $q_1, r_1 \in K[x]$ tali da poter scrivere $a = q_1 b + r_1$ e per cui $\deg r_1 < \deg b$. Se $r_1 = 0$, allora $a = qb$, quindi $b|a$ e ovviamente anche $b|b$; se esiste un $c \in K[x]$ tale che $c|a$, esso è b che è quindi il massimo comune divisore.

Se $r_1 \neq 0$, dividiamo b per esso: esistono $q_2, r_2 \in K[x]$ per cui $\deg r_2 < \deg r_1$ e

$$b = q_2 r_1 + r_2. \tag{1.8.4}$$

Se adesso $r_2 = 0$, troviamo che r_1 è il massimo comune divisore. Infatti, $r_1|b$ dal fatto che $b = r_1 q_2$, inoltre $a = q_1 b + r_1 = q_1(q_2 r_1) + r_1 = (q_1 q_2 + 1) r_1$ dunque $r_1|a$. Prendiamo dunque un $c \in K[x]$ che divida sia a che b: ciò significa che esistono $\alpha, \beta \in K[x]$ tali che $a = c\alpha$ e $b = c\beta$.

$$c\alpha = a = q_1 b + r_1 = q_1 c\beta + r_1 \Rightarrow r_1 = (\alpha - q_1\beta)c \tag{1.8.5}$$

ossia $c|r_1$. Il polinomio r_1 soddisfa dunque la definizione 1.8.2 di massimo comune divisore.

Se invece $r_2 \neq 0$, ancora possiamo dividere r_1 per r_2, dato che esistono $q_3, r_3 \in K[x]$ tali che $\deg r_3 < \deg r_2$ e

$$r_1 = q_3 r_2 + r_3. \tag{1.8.6}$$

Se $r_3 = 0$, allora esattamente come prima si dimostra che r_2 è il massimo comune divisore tra a e b.

Se $r_3 \neq 0$, iteriamo ancora una volta dividendo r_2 per r_3 e distinguendo i casi se il resto di questa divisione è nullo o no. Ad ogni passo, se il resto r_k è nullo l'algoritmo ha fine e r_{k-1} è il massimo comune divisore cercato. Il procedimento deve necessariamente avere un termine, in quanto ad ogni passo il grado del resto è decrementato (almeno) di 1 a partire da $\deg b$, cioè

$$\deg b > \deg r_1 > \deg r_2 > \dots \tag{1.8.7}$$

e si giunge dopo un numero finito di passi con un resto non nullo. Tale resto, come nei casi precedenti, è il massimo comune divisore di a e b. □

Teorema 1.8.6 (Identità di Bézout)**.** Dato un campo K e $a, b \in K[x]$, se d è il loro massimo comune divisore, allora esistono $\xi, \eta \in K[x]$ tali per cui si ha

$$d = \xi a + \eta b. \tag{1.8.8}$$

Dimostrazione. La determinazione di tali ξ e η si può fare tramite l'algoritmo di Euclide delle divisioni successive. Effettuiamo la prima divisione ottenendo $a = q_1 b + r_1$, da cui $r_1 = a - q_1 b$. Se r_1 è il massimo comune divisore, ci basta porre $\xi = 1$ e $\eta = -q_1$. Altrimenti, seguendo il teorema precedente dividiamo b come $b = q_2 r_1 + r_2$. Se r_2 è il massimo comune divisore,

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 - q_1 q_2) b \tag{1.8.9}$$

perciò poniamo $\xi = -q_2$ e $\eta = 1 - q_2 q_2$ per trovare la (1.8.8). Altrimenti dividiamo ancora r_1 per r_2 e procediamo, una volta trovato il massimo comune divisore, ad esprimerlo tramite i resti delle divisioni precedenti fino a risalire ad a e b. Anche in questo caso, come nell'algoritmo di Euclide, il numero di iterazioni è finito quindi in un numero finito di passi siamo sicuri di trovare due termini ξ e η che soddisfino la (1.8.8). □

Vediamo un esempio pratico: siano $a(x) = x^3 - 5$ e $b(x) = x^2 + 4$, due polinomi in $\mathbb{Q}[x]$. Dividiamo a per b con l'algoritmo di Euclide, ottenendo

$$\begin{aligned} x^3 - 5 &= x \cdot (x^2 + 4) + (4x - 5) \\ x^2 + 4 &= \left(\frac{1}{4}x + \frac{5}{16}\right)(4x - 5) + \frac{41}{16} \\ 4x - 5 &= \left(\frac{64}{41}x - \frac{80}{41}\right) \cdot \frac{41}{16} \end{aligned}$$

perciò $4x - 5$, ossia $x - \frac{5}{4}$, (data la convenzione stabilita precedentemente), è un massimo comune divisore di a e b.

1.9 Polinomi primi e irriducibili

Definizione 1.9.1. *Dato $a \in K[x]$ con $\deg a > 0$, esso si dice* primo *se ogniqualvolta $a|bc$ allora $a|b$ o $a|c$.*

Il seguente lemma mostra un legame tra i polinomi primi e i corrispettivi ideali principali generati da essi.

Lemma 1.9.2. Dato $a \in K[x]$ con $\deg a > 0$, l'ideale (a) è primo se e solo se a è primo.

Dimostrazione. Siano $b, c \in K[x]$. Se (a) è primo e $a|bc$, allora $bc \in (a)$. Per la definizione di ideale primo, però, ciò implica che $b \in (a)$ o $c \in (a)$, ossia $a|b$ o $a|c$. Dunque a è primo.

Sia ora a un polinomio primo: se $a|bc$ allora $a|b$ oppure $a|c$. Ma $a|bc$ implica $bc \in (a)$, e analogamente $a|x$ implica $x \in (a)$. Allora (a) è un ideale primo. □

Definizione 1.9.3. *Sia $a \in K[x]$ con $\deg a = n > 0$. Esso si dice* irriducibile *se è divisibile solo per i polinomi $c \in K[x]$ con $\deg c = 0$ e per quelli della forma λa, con $\lambda \in K \setminus \{0\}$.*

Notiamo subito che tutti i polinomi di grado 1, ossia della forma $p(x) = x - \alpha$, sono sempre irriducibili.

Teorema 1.9.4. Dato un campo K, un polinomio in $K[x]$ di grado positivo è irriducibile se e solo se è primo.

Dimostrazione. Sia $a \in K[x]$ irriducibile: prendiamo $b, c \in K[x]$ e supponiamo che $a|bc$. Mostriamo che se a non divide b, allora $a|c$. Escludiamo il caso $b = 0$, per il quale si avrebbe che $a|b$: abbiamo quindi $a, b \neq 0$. Sia dunque d il massimo comune divisore tra a e b. Essendo a irriducibile, abbiamo che o $d = \lambda$ o $d = \mu a$, per $\lambda, \mu \in K \setminus \{0\}$. Il secondo caso non è possibile, perché a quel punto $a = \mu^{-1}d$ quindi dividerebbe b. Dunque $d = \lambda$, con $\lambda = 1$ prendendo il polinomio monico. Per l'identità di Bézout 1.8.6, abbiamo allora

$$d = 1 = \xi a + \eta b$$

per qualche $\xi, \eta \in K[x]$. Moltiplicando per c, otteniamo $c = c\xi a + c\eta b$: poiché per ipotesi però $a|bc$, esiste $g \in K[x]$ tale per cui $ga = bc$. Allora

$$c = c\xi a + \eta ga = (c\xi + \eta g)a$$

ossia $a|c$.

Sia ora $a \in K[x]$ primo: se fosse riducibile, allora $\exists f, g \in K[x]$ (diversi da multipli scalari di a) con $\deg f, \deg g > 0$ tali che $a = fg$: allora $a|fg$. Essendo primo, però, divide sicuramente uno dei due, sia esso f: esiste quindi $\xi \in K[x]$, non nullo, per il quale $f = a\xi$. Ma allora

$$a = fg = a\xi g \Rightarrow (1 - \xi g)a = 0$$

ossia $\xi g = 1$: di conseguenza $\deg \xi + \deg g = 0$. Dato che $\deg g > 0$ e $\deg \xi \geq 0$, questo è assurdo: ciò prova che non esistono f, g diversi da multipli scalari di a e di grado positivo che dividono a, che quindi non è riducibile. □

Teorema 1.9.5 (della fattorizzazione unica)**.** Ogni polinomio $a \in K[x]$, con $\deg a > 0$, può essere scritto come prodotto di polinomi irriducibili (almeno uno), non necessariamente distinti. Tale fattorizzazone, a meno di permutazioni, è unica.

Dimostrazione. Dimostriamolo per induzione su $\deg a = n$ Per prima cosa sia $n = 1$: per quanto già detto, essendo di primo grado è già irriducibile, quindi è la fattorizzazione cercata. Supponiamo che la tesi sia vera da 1 a n. Se a è irriducibile, la dimostrazione è conclusa; altrimenti, scriviamo $a = gh$ per qualche $g, h \in K[x]$. Se g e h sono entrambi irriducibili abbiamo trovato la fattorizzazione; se non è questo il caso, almeno uno tra g e h ha comunque un grado minore di quello di a, e per l'ipotesi di induzione è dunque riducibile. Procediamo scomponendo g o h, fino a trovare $a = q_1 q_2 \dots q_n$, dove q_n deve per forza essere irriducibile per le ipotesi fatte.

Potendo scrivere $a = p_1 \dots p_s = q_1 \dots q_t$, con p_i, q_j ($i \in \{1, \dots, n\}$ e $j \in \{1, \dots, t\}$) irriducibili, si possono riordinare i fattori in modo da avere $s = t$ riscrivendo i vari $p_i = k_i q_i$, con $k_i \in K \setminus \{0\}$. □

A questo punto, possiamo dividere tutti i fattori irriducibili per delle costanti opportune in K per renderli monici, come nel seguente corollario.

Corollario 1.9.6. Dato $a \in K[x]$, con $\deg a = s > 0$, esso si può sempre scrivere univocamente come $a = ka_1 \dots a_s$, in cui

- $k \in K \setminus \{0\}$ è il coefficiente direttivo di a;
- a_i, $\forall i \in \{1, \dots, s\}$ è monico e irriducibile.

Dimostrazione. Preso $a \in K[x]$, possiamo esprimerlo come $a = k_1 a_1$ con a_1 monico. Se si esegue lo stesso ragionamento su $a = p_1 \dots p_t$, nel teorema precedente, si ottiene $a = k_1 k_2 \dots k_s a_1 \dots a_s$ con i vari a_i monici e irriducibili $\forall i \in \{1, \dots, n\}$, si ha che $k_1 k_2 \dots k_s \in K$, perciò deve essere il coefficiente direttivo del polinomio corrispondente. □

1.10 Domini a ideali principali

Definizione 1.10.1. *Un dominio d'integrità A è detto* a ideali principali *se è tutti i suoi ideali propri sono principali, ossia se per ogni ideale $I \subset A$ esiste $a \in A$ per cui $I = (a)$.*

Dimostriamo subito l'inverso del corollario 1.5.4 che avevamo anticipato.

Teorema 1.10.2. In un dominio a ideali principali, un ideale è primo se e solo se è massimale.

Dimostrazione. Abbiamo già dimostrato nel corollario 1.5.4 che se un ideale è primo, allora è anche massimale. Sia A un dominio a ideali principali, I un suo ideale primo e J un altro ideale tali che $I \subseteq J \subseteq A$. Sappiamo che esistono $a, b \in A$ tali che $I = (a)$ e $J = (b)$. Poiché $(a) \subseteq (b)$, si ha $a \in (b)$ quindi esiste $x \in A$ tale che $a = xb$: allora $a|xb$. L'ideale I è primo, quindi anche a è un polinomio primo, perciò abbiamo che $a|b$ oppure $a|x$. Nel primo caso, si ha $b \in (a)$ perciò $(a) = (b)$, ossia $I = J$. Nel secondo caso, esiste $y \in A$ tale che $ya = x$, ma allora $x = y(xb) = x(yb)$. Poiché A è un dominio di integrità, e $x \neq 0$, ciò implica che $yb = 1$, e di conseguenza $1 \in (b)$. Ma un ideale che contiene l'unità coincide con l'anello intero, perciò $(b) = A$. Ciò prova che I è massimale. □

Mostriamo ora che possiamo sfruttare molte utili proprietà, come la completa equivalenza tra "primo" e "irriducibile", nello studio degli anelli di polinomi in una incognita, in virtù del seguente teorema.

Teorema 1.10.3. Dato un campo K, l'anello $K[x]$ è un dominio a ideali principali.

Dimostrazione. Sia I un ideale di $K[x]$. Se $I = \{0\}$, ovviamente $I = (0)$ quindi è un ideale principale. Se $I \neq \{0\}$ allora in esso ci sono dei polinomi di grado maggiore di zero. Poniamo

$$m := \min\{\deg p \colon p \in I\}$$

che esiste per il principio del buon ordinamento.[4] Sia $g \in I \setminus \{0\}$ tale che $\deg g = m$: vogliamo mostrare che $(g) = I$. Chiaramente $(d) \subseteq I$ dalla definizione di ideale. Prendiamo inolte $y \in I$: certamente esistono $q, r \in K[x]$ tali per cui $\deg r < \deg y$ e $y = qg + r$. Di conseguenza, $r = y - qg \in I$: se però $r \neq 0$, avremmo $\deg r < \deg g$ che viola l'ipotesi fatta (g ha il grado minore tra tutti i polinomi di I). Deve necessariamente essere allora $r = 0$, da cui $y = qg$. Ma allora $g|y$, e poiché questo vale per ogni $y \in I$ risulta $I \subseteq (d)$. Ciò prova che $I = (d)$, perciò ogni ideale di $K[x]$ è un ideale principale. □

Corollario 1.10.4. Ogni ideale principale $I \in K[x]$, con $I \neq (0)$, ha un unico generatore monico.

Dimostrazione. Poniamo $I = (g)$ con $g(x) = a_n x^n + \cdots + a_0$ con $a_n \neq 0$. Possiamo allora moltiplicare g per a_n^{-1}, ottenendo che I è anche generato da $\tilde{g} = a_n^{-1} g$ che è monico, cioè $(\tilde{g}) = (g)$: ciò prova l'esistenza di un generatore monico di I. Dimostriamone l'unicità: sia $I = (h)$, con h monico. Poiché $(h) = (\tilde{g})$, risulta che $\tilde{g}|h$ e $h|\tilde{g}$ ossia esistono $\alpha, \beta \in K[x]$ per cui $h = \alpha\tilde{g}$ e $\tilde{g} = \beta h(x)$. Quindi $h = \alpha\beta h$, e poiché $I \neq \{0\}$ e $K[x]$ è un dominio d'integrità risulta $\alpha\beta = 1$. Dunque $\alpha, \beta \in K \setminus \{0\}$: $h = \alpha\tilde{g}$ per ipotesi è monico, e dato che lo è anche $\tilde{g}$ si ottiene $\alpha = 1$. Di conseguenza $h = \tilde{g}$, cioè il generatore monico è unico. □

Teorema 1.10.5. Sia (g) un ideale non nullo di $K[x]$. Ogni classe laterale di $(g) \in K[x] \,/\, g$ si può rappresentare univocamente nella forma $(g) + r$, con $\deg r < \deg g$.

Dimostrazione. Una classe laterale dell'ideale (g) è del tipo $(g) + f$, per $f \in K[x]$. Per il teorema 1.8.5 esistono sempre $q, r \in K[x]$, con $\deg r < \deg g$ tali che $f = qg + r$. Si ha allora

$$(g) + f = (g) + qg + r = (g) + r,$$

dato che $qg \in (g)$, quindi un tale r esiste. Mostriamo che è unico. Supponiamo che esista anche un $r' \in K[x]$ tale che la classe laterale si possa rappresentare come $(g) + r'$, con $\deg r' < \deg g$. Dalle proprietà 1.7.2 risulta

$$\deg(r' - r) \leq \max\{\deg r', \deg r\} < \deg g.$$

Ora, nel caso $\deg(r' - r) \geq 0$, se fosse $r' - r \in (g)$ allora si avrebbe $r' - r = hg$ per qualche $h \in K[x]$, ma allora $\deg(r' - r) = \deg(hg)$ e contemporaneamente

$$\deg(r' - r) < \deg g \geq \deg(hg)$$

che porta ad una contraddizione. Dunque $\deg(r' - r) = 0$, ossia $r' - r = 0 = 0 \cdot g$ perciò $r' - r \in (g)$. Avendo i due rappresentanti in relazione, le due classi laterali sono equivalenti. □

Corollario 1.10.6. Sia K un campo finito e $g \in K[x]$ di grado $n > 0$. Allora $|K[x] \,/\, (g)| = |K|^n$.

Dimostrazione. Sapendo che le classi laterali sono scritte come $(g) + r(x)$, ora ipotizziamo due casi, cioè $\deg r(x) = 0$, oppure $\deg r(x) = -1$, ricaviamo:

$$\begin{aligned} &\deg r(x) = 0 \text{ si ha } (g) + r(x) = (g) + a_0, \\ &\deg r(x) = 1 \text{ si ha } (g) + r(x) = (g) + a_1 x + a_0. \end{aligned}$$

Nel primo caso si ritrovano tutte le possibili combinazioni degli $a_0 \in K$, che sono m, nel secondo caso le possibili combinazioni sono m^2. Si può arrivare dunque a dimostrare la tesi. □

Teorema 1.10.7. Sia $g \in K[x]$ con $\deg g > 0$. L'ideale (g) è massimale se e solo se g è irriducibile.

Dimostrazione. Non bisogna far altro che applicare dei teoremi già visti in precedenza:

$$(g) \text{ è massimale } \Leftrightarrow (g) \text{ è primo } \Leftrightarrow g \text{ è primo } \Leftrightarrow g \text{ è irriducibile}$$

per i teoremi, in ordine, 1.10.2, 1.9.2 e 1.9.4. □

[4] Il principio del buon ordinamento afferma che *ogni insieme di numeri naturali non vuoto contiene un numero che è più piccolo di tutti gli altri.*

Corollario 1.10.8. Dato $g \in K[x]$ con $\deg g > 0$, $K[x] / (g)$ è un campo se e solo se g è irriducibile.

Dimostrazione. Dal teorema precedente abbiamo che g è irriducibile se e solo se (g) è massimale. Collegando anche il teorema 1.5.3 troviamo la tesi. □

Vediamo un esempio concreto delle conseguenze di questi teoremi. Partiamo dall'anello $\mathbb{R}[x]$ dei polinomi a coefficienti reali, e un polinomio irriducibile di grado maggiore di 1, come $x^2 + 1$. Essendo irriducibile, l'ideale $(x^2 + 1)$ è primo e massimale, e $\mathbb{R}[x] / (x^2 + 1)$ un campo. I suoi elementi, dal teorema 1.10.5, si scrivono tutti come un elemento di $(x^2 + 1)$ più un polinomio di primo grado, ossia se $p \in \mathbb{R}[x] / (x^2 + 1)$ allora

$$p = (x^2 + 1) + ax + b. \tag{1.10.1}$$

Prendiamo un'altro elemento $q = (x^2 + 1) + cx + d$. La somma di due elementi è definita in modo naturale come

$$p + q = (x^2 + 1) + ax + b + (x^2 + 1) + cx + d = (x^2 + 1) + (a + c)x + b + d \tag{1.10.2}$$

e il prodotto come

$$pq = [(x^2 + 1) + ax + b] \cdot [(x^2 + 1) + cx + d] = (x^2 + 1) + acx^2 + (ad + bc)x + bd. \tag{1.10.3}$$

Il termine acx^2 però ha lo stesso grado di $x^2 + 1$, quindi non deve comparire. Possiamo in effetti trovare un modo per eliminarlo: aggiungendo e sottraendo ac al risultato, otteniamo

$$\begin{aligned} pq &= (x^2 + 1) + acx^2 + ac + (ad + bc)x + bd - ac = \\ &= (x^2 + 1) + ac(x^2 + 1) + (ad + bc)x + bd - ac = \\ &= (x^2 + 1) + (ad + bc)x + bd - ac \end{aligned} \tag{1.10.4}$$

dato che $ac(x^2 + 1) \in (x^2 + 1)$ quindi viene "assorbito" dall'ideale.

Prendiamo ora l'insieme $\mathbb{R}^2$ delle coppie di numeri reali, e dotiamolo delle operazioni

$$\begin{gathered} (b, a) + (\beta, \alpha) = (b + \beta, a + \alpha) \\ (b, a)(\beta, \alpha) = (a\beta + b\alpha, b\beta - a\alpha). \end{gathered} \tag{1.10.5}$$

Questa struttura individua un ulteriore campo, di cui non è difficile notare il legame con il precedente $\mathbb{R}[x] / (x^2 + 1)$. Troviamo infatti un isomorfismo $\gamma \colon \mathbb{R}[x] / (x^2 + 1) \to \mathbb{R}^2$, definito come

$$\gamma \colon (x^2 + 1) + ax + b \mapsto (b, a) \tag{1.10.6}$$

che li lega. Ovviamente quest'ultimo campo $\mathbb{R}^2$, con le operazioni definite, non è altro che il campo complesso come costruito da Hamilton, ma con la coppia (a, b) in ordine contrario. Per passare alla notazione comune $a + ib$ non dobbiamo far altro che definire un nuovo insieme $\hat{\mathbb{C}} = \{a + ib \colon a, b \in \mathbb{R}\}$ con le note operazioni, e tale che $i^2 = -1$. L'isomorfismo che mette in relazione i due campi è evidentemente un $\varphi \colon \mathbb{C} \to \hat{\mathbb{C}}$ per il quale

$$\varphi(b, a) = a + ib. \tag{1.10.7}$$

1.11 Radici di un polinomio

Definizione 1.11.1. *Dato un anello A commutativo e con unità e un polinomio $p \in A[x]$, si dice* radice *di p un elemento $\alpha \in A$ per cui $p(\alpha) = 0$.*

Teorema 1.11.2 (di Ruffini)**.** Dato un campo K e un polinomio $p \in K[x]$, α è una radice di p se e solo se $(x - \alpha)|p$.

Dimostrazione. Sia α una radice di p. Possiamo dividere p per $x-\alpha$, il cui grado non è nullo, ottenendo che

$$p(x) = q(x)(x-\alpha) + r(x)$$

con $\deg r < \deg\big((x-\alpha)\big) = 1$. Dato che $\deg r \in \{0,1\}$, quindi, $r(x) = k$ per qualche $k \in K$, eventualmente $k = 0$ se $\deg r = -1$. Ma essendo α una radice di p, valutando $p(\alpha)$ otteniamo

$$0 = p(\alpha) = q(\alpha)(\alpha-\alpha) + k = k$$

perciò $k = r(x) = 0$: di conseguenza $p(x) = q(x)(x-\alpha)$, ossia $(x-\alpha)|p$.

Sia ora $(x-\alpha)|p$: possiamo dunque scrivere $p(x) = g(x)(x-\alpha)$ per qualche $g \in K[x]$. Ma allora, valutandolo in α, risulta

$$p(\alpha) = g(\alpha)(\alpha-\alpha) = 0$$

quindi α è una radice di p. $\square$

Per esempio, sia $f(x) = a_1x + a_0 \in K[x]$ con $a_1 \neq 0$. Si ha che $\alpha = -\frac{a_0}{a_1}$ è sempre una radice.

Si può, visti i teoremi precedenti, porre una relazione tra la presenza di una radice e la possibilità di ridurre un polinomio. Sia $f(x) \in K[x]$ e $\deg f(x) > 1$, se $f(x)$ ammette una radice α, allora $f(x)$ deve essere riducibile come $f(x) = (x-\alpha)g(x)$.

Non è detto, in generale, che ogni polinomio riducibile abbia necessariamente una radice: basta prendere in $\mathbb{R}[x]$ il polinomio x^4+2x^2+1. Esso si può scomporre in $(x^2+1)(x^2+1)$, che chiaramente non hanno radici reali. Se invece il polinomio *è riducibile* e ha grado 2 o 3, allora certamente ha una radice: in fatti almeno uno dei fattori in cui è scomposto deve avere grado 1, cioè sarà della forma $x-\lambda$, perciò tale λ è una radice.

Un caso importante è quello dei numeri complessi: in tale campo, si può sempre scomporre un polinomio (non costante) in un prodotto di opportuni polinomi di primo grado, per via del seguente teorema (che non dimostriamo).

Teorema 1.11.3 (Teorema fondamentale dell'algebra)**.** Ogni polinomio in $\mathbb{C}[x]$ di grado positivo ammette sempre una radice in $\mathbb{C}$.

Definizione 1.11.4. *Siano K un campo, $f \in K[x]$ e $\alpha \in K$. Si dice che α è una radice di f con* molteplicità algebrica *$r \in \mathbb{N}$ se $(x-\alpha)^r|f$ ma $(x-\alpha)^{r+1}$ non divide f.*

In particolare, una radice di molteplicità algebrica 1 è detta *semplice*.

Teorema 1.11.5. Sia $f \in K[x]$ con $\deg f \geq 0$. Date le radici distinte $\alpha_1, \dots, \alpha_k$ di f con molteplicità algebrica rispettivamente $r_1, \dots, r_k$, si ha che $\sum_{i=1}^n r_i \leq \deg f$.

Dimostrazione. Poniamo f, secondo il teorema 1.9.5, come prodotto di opportuni polinomi p_i:

$$f = p_1 \dots p_k, \tag{1.11.1}$$

Data una radice α_1, si ha che $(x-\alpha_1)|f$ e dunque possiamo dividere f ottenendo

$$f(x) = (x-\alpha_1)\tilde{p}(x)p_2(x)\dots p_k(x). \tag{1.11.2}$$

Iteriamo il procedimento r_1 volte, dove r_1 è la molteplicità algebrica di α_1: infatti dalla definizione 1.11.4 $(x-\alpha_1)^{r_1}|f$. Dunque risulta

$$f(x) = (x-\alpha_1)^{r_1} \dots (x-\alpha_k)^{r_1} g(x) \tag{1.11.3}$$

per un certo $g \in K[x]$ non nullo. Passiamo alla radice α_2: poiché $\alpha_2 \neq \alpha_1$, certamente $x-\alpha_2$ non divide $(x-\alpha_1)^{r_1}$, quindi dovrà dividere g. Scomponendo g in fattori, sempre per il teorema 1.9.5, $x-\alpha_2$ dividerà uno di essi, e si procede a dividere r_2 volte, tante quante la molteplicità algebrica di α_2, ottenendo

$$f(x) = (x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2} h(x) \tag{1.11.4}$$

per qualche $h \in K[x]$ non nullo. Procedendo in questo modo fino ad esaurire i fattori di f. Presa una radice α_i, possiamo sempre dividere uno dei fattori del polinomio r_i volte, per la definizione della molteplicità algebrica r_i, ottenendo infine

$$f(x) = (x - \alpha_1)^{r_1}(x - \alpha_2)^{r_2} \dots (x - \alpha_k)^{r_k} z(x) \tag{1.11.5}$$

con z irriducibile. Allora dalle proprietà 1.7.2 otteniamo

$$\deg f = \sum_{i=1}^{k} r_i + \deg z \geq \sum_{i=1}^{k} r_i \tag{1.11.6}$$

che prova la tesi. □

Corollario 1.11.6 (Principio d'identità dei polinomi)**.** Siano $\alpha_1, \dots, \alpha_{n+1}$ elementi distinti di K. Se $f, g \in K[x]$, al più di grado n, sono tali che $f(\alpha_i) = g(\alpha_i)$ $\forall i \in \{1, \dots, n+1\}$, allora $f = g$.

Dimostrazione. Supponiamo per assurdo che sia $f \neq g$. Allora si ha che $f - g \neq 0$, perciò $n \geq \deg(f - g) \geq 0$. Se $f(\alpha_i) = g(\alpha_i)$ $\forall i \in \{1, \dots, n+1\}$, allora ogni α_i è radice di $f - g$, che ha quindi $n + 1$ radici. Per il teorema precedente, però, risulterebbe $\deg(f - g) \geq \sum_{k=1}^{n+1} r_i \geq n + 1$ (nel migliore dei casi, $\deg(f - g) = n + 1$ se ogni radice è semplice), che è assurdo perché come visto si ha $\deg(f - g) \leq n$. Dunque deve essere $f - g = 0$, ossia $f = g$. □