Note di Algebra 2

a.a. 2016/17

docente: Michela Brundu

Capitolo 0 - Background

Nozioni di base sui gruppi

Definizione. Sia G un insieme non vuoto e sia $* : G \times G \to G$ un'operazione definita da $(a, b) \mapsto a * b$.
Se valgono le seguenti proprietà:

1. l'operazione "$*$" è associativa, i.e. $(a * b) * c = a * (b * c)$, $\forall\, a, b, c \in G$;
2. esiste un elemento neutro per "$*$", i.e. $\exists\, e \in G : a * e = e * a = a$, $\forall\, a \in G$;
3. ogni elemento di G ha inverso in G, i.e. $\forall\, x \in G\ \ \exists\, y \in G$ tale che $x * y = y * x = e$;

allora la coppia $(G, *)$ si dice *gruppo*.
Se inoltre vale

4. $\forall x, y \in G,\ x * y = y * x$,

il gruppo G viene detto *commutativo* o *abeliano*.

Osservazione 0.1. In un gruppo $(G, *)$ l'inverso di ogni elemento $x \in G$ è unico e si indica con x^{-1}.
L'elemento neutro è unico e si indica con e_G (o 1_G, secondo la notazione moltiplicativa per i gruppi, o 0_G, secondo quella additiva).
Per evidenziare il suo elemento neutro, un gruppo si denota anche con $(G, *, e_G)$ (o, a seconda dell'operazione, con $(G, \cdot, 1_G)$ e $(G, +, 0_G)$, rispettivamente).

Esempio 0.1.1. I più noti esempi di gruppi numerici sono $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$. Inoltre anche $(\mathbb{Q}^*, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{C}^*, \cdot, 1)$ sono, come i precedenti, gruppi commutativi. Un gruppo numerico è anche quello costituito dall'insieme $\{1, -1\}$ rispetto all'operazione di prodotto.

Esempio 0.1.2. Un altro esempi di gruppo, ma non numerico, è l'insieme $\mathcal{S}_n$ delle biiezioni di un insieme finito di n elementi in sé rispetto alla composizione di applicazioni. Ad esempio,

$$\mathcal{S}_3 := \{f : \{a, b, c\} \to \{a, b, c\}, \text{ dove } f \text{ è biiettiva}\}.$$

In generale, $(\mathcal{S}_n, \circ)$, è un gruppo (non commutativo).

Esempio 0.1.3. Ricordiamo anche i *gruppi classici*:

$$(SO(n, \mathbb{R}), *) \subset (SL(n, \mathbb{R}), *) \subset (GL(n, \mathbb{R}), *)$$

detti, rispettivamente, *Special Orthogonal Linear Group*, *Special Linear Group* e *General Linear Group*.
Quest'ultimo è costituito da tutte le matrici $n \times n$ non degeneri (cioè a determinante non nullo); $SL(n, \mathbb{R})$ è costituito da tutte le matrici $n \times n$ a determinante 1, mentre $SO(n, \mathbb{R})$ è costituito da tutte le matrici ortogonali a determinante 1.
Qui l'operazione " $*$ " indica il prodotto righe per colonne tra matrici.

Definizione. Sia H un sottoinsieme non vuoto di un gruppo $(G, *)$. Se $(H, *)$ è un gruppo, allora viene detto *sottogruppo di* G, e si scrive $H \leq G$.

Richiamiamo una nota caratterizzazione di sottogruppo:

Proposizione 0.2. *(Criterio di sottogruppo). Sia $(G, *)$ un gruppo e sia H un suo sottinsieme non vuoto. Allora*

$$H \leq G \iff \begin{cases} (i) & \forall a, b \in H, \quad a * b \in H \\ (ii) & \forall a \in H, \quad\ \ a^{-1} \in H. \end{cases}$$

□

D'ora in poi useremo la notazione moltiplicativa, salvo negli esempi con una diversa operazione.

Corollario 0.3. *Se $(G, \cdot, 1_G)$ è finito, allora $H \leq G$ se e solo se vale (i).*

Dimostrazione. " $\Rightarrow$ " Ovvia.
" $\Leftarrow$ " Per il Criterio precedente, basta provare che (i) implica (ii). Dunque sia $a \in H$. Poiché H è chiuso

rispetto al prodotto per ipotesi, allora $a \cdot a \in H$, $a \cdot a \cdot a \in H$ e, ricorsivamente, si ottiene che $a^n \in H$, per ogni $n \in \mathbb{N}$. Dato che il gruppo G è finito, devono esistere $m_0, n_0 \in \mathbb{N}$ distinti e tali che $a^{n_0} = a^{m_0}$. Non è restrittivo supporre $m_0 > n_0$. Dunque, ponendo $k = m_0 - n_0 \geq 1$, dall'uguaglianza precedente (in G) moltiplicando ambo i membri per a^{-n_0} si ha $1_G = a^k = a \cdot a^{k-1}$, da cui si ottiene che a^{k-1} è l'inverso di a e tale elemento appartiene ad H in quanto è una potenza di a. □

Definizione. Dati un gruppo G e un suo sottogruppo H, se $a \in G$, si definisce *classe laterale destra di a rispetto ad H* l'insieme

$$Ha := \{ha \,|\, h \in H\}.$$

Analogamente, si definisce *classe laterale sinistra di a rispetto ad H* l'insieme

$$aH := \{ah \,|\, h \in H\}.$$

Osservazione 0.4. Per ogni $a, b \in G$, c'è una naturale corrispondenza biunivoca $Ha \longleftrightarrow Hb$. In particolare, se H è finito, tutte le classi laterali hanno lo stesso numero di elementi.
Inoltre c'è una naturale corrispondenza biunivoca tra l'insieme delle classi laterali destre e l'insieme delle classi laterali sinistre:

$$\{aH \,|\, a \in G\} \quad \longleftrightarrow \quad \{Ha \,|\, a \in G\}$$

data da $aH \mapsto Ha$.

Osservazione 0.5. Sia $H \leq G$; si verifica facilmente che

$$G = \bigsqcup_{a \in G} Ha \quad \text{e anche} \quad G = \bigsqcup_{a \in G} aH$$

i.e. G è l'unione disgiunta delle classi laterali destre e anche l'unione disgiunta delle classi laterali sinistre.

C'è un profondo legame tra la struttura delle classi laterali e il sottogruppo corrispondente. Infatti si può intendere ogni classe laterale destra come la classe di un elemento rispetto ad una opportuna relazione d'equivalenza associata al sottogruppo.

Definizione. Dati un gruppo G e un suo sottogruppo H, si definisce *relazione indotta da H* la relazione $\equiv_H$ definita da

$$a \equiv_H b \iff ab^{-1} \in H,$$

con $a, b \in G$.

Proposizione 0.6. *La relazione $\equiv_H$ è una relazione di equivalenza.*

Dimostrazione. È necessario dimostrare le tre proprietà di cui gode una relazione di equivalenza:
- $\forall a \in G$ si ha che $a \cdot a^{-1} = 1_G \in H \Rightarrow a \equiv a$, quindi $\equiv_H$ gode della proprietà riflessiva;
- $\forall a, b \in G$, se $a \equiv_H b \implies ab^{-1} \in H$, quindi, per la chiusura di H rispetto all'inverso, si ha che $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} \in H$, da cui $b \equiv_H a$, quindi $\equiv_H$ gode della proprietà simmetrica;
- se $a \equiv_H b$ e $b \equiv_H c \implies ab^{-1}, bc^{-1} \in H \implies (ab^{-1}) \cdot (bc^{-1}) = a \cdot (b^{-1}b) \cdot c^{-1} = a \cdot 1_G \cdot c^{-1} = ac^{-1} \iff a \equiv_H c$, quindi $\equiv_H$ gode della proprietà transitiva.

In conclusione, $\equiv_H$ è una relazione di equivalenza. □

Denotando la classe di ogni elemento $a \in G$ rispetto alla relazione di equivalenza $\equiv_H$ con $[a]$, si prova il seguente risultato

Proposizione 0.7. *Sia $H \leq G$; per ogni $a \in G$ vale $[a] = Ha$.*

Dimostrazione. Per definizione, $[a] = \{x \in G \,|\, x \equiv_H a\} = \{x \in G \,|\, xa^{-1} \in H\}$.
Pertanto $[a] = \{x \in G \,|\, \exists\, h \in H : xa^{-1} = h\} = \{ha \,|\, h \in H\} = Ha$. □

Definizione. Sia G un gruppo finito; si definisce *ordine di* G il numero dei suoi elementi e si indica con $o(G)$ o con $|G|$.

Da 0.4 e 0.5 segue facilmente il noto

Teorema 0.8. *(Lagrange). Siano G un gruppo finito e $H \leq G$. Allora $o(H) \,|\, o(G)$.* □

Definizione. Si definisce *indice di G in H* il numero delle classi laterali destre, e si indica con $in_G(H)$.

Osservazione 0.9. Dal teorema di Lagrange, dalle definizioni di classi laterali e di indice di sottogruppo, si ottiene immediatamente che

$$in_G(H) = \frac{o(G)}{o(H)}.$$

Ricordiamo una particolare tipologia di gruppi. Sia a un simbolo e si consideri l'insieme

$$\langle a \rangle := \{a^i : i \in \mathbb{Z}\}$$

dove a^i denota una "potenza formale" di a. Si definisca per ogni $i, j \in \mathbb{Z}$:

$$a^i \cdot a^j := a^{i+j}, \quad a^1 := a, \quad a^0 := 1.$$

Si prova facilmente il seguente fatto:

Proposizione 0.10. - Definizione. La terna $(\langle a \rangle, \cdot, 1)$ è un gruppo commutativo detto *gruppo ciclico generato da a.* □

La precedente nozione astratta trova una sua espressione in casi specifici. Infatti, Se $(G, \cdot, 1_G)$ è un gruppo e $a \in G$, con a^n si intende il prodotto $a \cdot a \cdot \cdots \cdot a$ fatto n volte, se $n \in \mathbb{N}^*$ e si estende in modo canonico agli interi negativi: se $n \in \mathbb{Z}$ e $n < 0$, con a^n si intende il prodotto $a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}$ fatto $-n$ volte. Ponendo infine $a^0 := 1_G$, si ottiene che l'insieme $\{a^i : i \in \mathbb{Z}\}$ è un sottogruppo di G e ovviamente un gruppo ciclico rispetto al prodotto di G. Per questo si formula la seguente

Definizione. Sia G un gruppo e $a \in G$; si dice *sottogruppo ciclico generato da a* l'insieme $\{a^i : i \in \mathbb{Z}\}$ e si denota con $\langle a \rangle$. Si definisce *ordine* di a (e si indica con $o(a)$) l'ordine del sottogruppo $\langle a \rangle$.

Osservazione 0.11. È immediato verificare che

$$o(a) = \min\{n \in \mathbb{N} : a^n = 1_G\}.$$

Dal teorema di Lagrange seguono facilmente i seguenti fatti:

Corollario 0.12. *Siano G un gruppo finito e $a \in G$. Allora $o(a) \mid o(G)$.*

Dimostrazione. Per definizione, $o(a) = o(H)$, con $H = \langle a \rangle$. Per il teorema di Lagrange, $o(H) \,|\, o(G)$ qualsiasi sia $H \leq G$, da cui $o(a) \,|\, o(G)$. □

Corollario 0.13. *Per ogni $a \in G$, si ha che $a^{o(G)} = 1_G$.*

Dimostrazione. Per il corollario 0.12, esiste $k \in \mathbb{N}$ tale che $o(G) = k\, o(a)$; si ha quindi,

$$a^{o(G)} = a^{k\, o(a)} = (a^{o(a)})^k = 1_G^k = 1_G$$

dove la penultima uguaglianza segue dalla definizione di $o(a)$. □

Sottogruppi normali e quozienti

Definizione. Un sottogruppo H di un gruppo G si dice *normale* (e si scrive con $H \triangleleft G$) se vale:

$$\forall g \in G\,, \forall\, h \in H\,, \quad ghg^{-1} \in H.$$

Viene lasciata al lettore la dimostrazione della nota caratterizzazione di sottogruppo normale:

Proposizione 0.14. *Sia H un sottogruppo di un gruppo G. Sono fatti equivalenti:*
i) $H \triangleleft G$*;*
ii) $gHg^{-1} = H$ *per ogni* $g \in G$*;*
iii) $\forall\, g \in G$, $\forall\, h \in H$, $\exists\, k \in H$ *tale che* $gh = kg$*;*
iv) per ogni $g \in G$ *vale:* $Hg = gH$*, cioè la classe laterale destra e la classe laterale sinistra di ogni elemento coincidono.* □

Osservazione 0.15. Si osservi che non è vero che se $gH = Hg$, allora $gh = hg$, per ogni $h \in H$.
Si ha invece la formulazione in 0.14 *iii*), dove si noti che, in generale, $h \neq k$.

Ricordiamo ora che si può dotare l'insieme delle classi laterali destre rispetto a un sottogruppo H (cioè delle classi di equivalenza di $\equiv_H$, come visto in 0.7) della struttura di gruppo solo se H è normale. Tale fatto si fonda sul seguente risultato preliminare, che mostra come si può definire un prodotto nell'insieme delle classi laterali destre.

Lemma 0.16. *Sia $H \leq G$. Allora*

$$H \triangleleft G \iff \forall a, b \in G, \exists\, c \in G \text{ tale che } (Ha)(Hb) = Hc.$$

Dimostrazione.

" $\Rightarrow$ " Si osservi che $(Ha)(Hb) = H(aH)b = H(Ha)b$, dove la prima uguaglianza segue dalla proprietà associativa del prodotto in G e la seconda dal fatto che $aH = Ha$, essendo $H \triangleleft G$ per ipotesi.
Infine $H(Ha)b = (HH)(ab) = H(ab)$ ove la prima uguaglianza segue, come prima, dall'associatività e la seconda dal fatto che $HH = H$ (uguaglianza vera in quanto $e \in H \Rightarrow H \subseteq HH$ e H è chiuso rispetto al prodotto, quindi, ovviamente, $HH \subseteq H$).

" $\Leftarrow$ " Vogliamo provare che, per ogni $a \in G$, vale $aHa^{-1} \subseteq H$.
Per ipotesi, scelto a, per ogni $b \in G$ esiste $c \in G$ tale che $(Ha)(Hb) = Hc$. Dato che tale relazione vale per qualsiasi b, si consideri $b = a^{-1}$: in questo caso si ottiene $(Ha)(Ha^{-1}) = Hc$.
Si osservi che H è sottogruppo di G, quindi $1_G \in H$, da cui

$$aHa^{-1} = (1_G \cdot a)(Ha^{-1}) \subseteq Hc.$$

Per provare la tesi è sufficiente dunque mostrare che $Hc \subseteq H$. Ma quest'ultimo fatto si prova ricordando nuovamente che $1_G \in H$: quindi dalla precedente inclusione si ottiene che

$$1_G = aa^{-1} = a \cdot 1_G \cdot a^{-1} \in Hc$$

da cui segue immediatamente che $c^{-1} \in H$, quindi, per la chiusura rispetto all'inverso, $(c^{-1})^{-1} = c \in H$; pertanto $Hc \subseteq H$. □

Proposizione - Definizione 0.17. *Sia $(G, \cdot_G, 1_G)$ un gruppo. Se $H \triangleleft G$, allora l'insieme:*

$$G/H := \{[a] \mid a \in G\} \quad \textit{dove} \quad [a] := \{x \in G \mid x \equiv_H a\}$$

è un gruppo rispetto al prodotto definito da:

$$[a] \cdot_{G/H} [b] := [a \cdot_G b]$$

e viene detto gruppo quoziente di G modulo H.

Dimostrazione. Occorre anzitutto provare che l'operazione è ben definita, cioè che per $a, a', b, b' \in G$:

$$[a] = [a'],\ [b] = [b'] \quad \Rightarrow \quad [a \cdot_G b] = [a' \cdot_G b'],$$

ovvero che il risultato dell'operazione non dipende dalla scelta dei rappresentanti dei due fattori.
Possiamo riscrivere l'implicazione da provare nel seguente modo, grazie a 0.7 e alla definizione di classe d'equivalenza $[x] = xH$:

$$a' = ah,\ b' = bk \text{ (dove } h, k \in H) \quad \Rightarrow \quad a'b' = ab\lambda \text{ per un opportuno } \lambda \in H.$$

Ma si ha

$$(ab)^{-1}a'b' = (b^{-1}a^{-1})(ah)(bk) = b^{-1}hbk = (b^{-1}hb)k \in H$$

in quanto $b^{-1}hb \in H$ poiché H è normale.
Restano da provare gli assiomi di gruppo. È facile vedere che $1_{G/H} = [1_G]$ e che $[x]^{-1} = [x^{-1}]$, per ogni $x \in G$. L'associatività del prodotto segue immediatamente dalla corrispondente proprietà in G. □

Corollario 0.18. Se G è un gruppo finito e H un suo sottogruppo normale, allora

$$o(G/H) = \frac{o(G)}{o(H)} = in_G(H).$$

Dimostrazione. Discende immediatamente dal Teorema di Lagrange o meglio dall'osservazione seguente (vedi 0.9). Basta osservare che $in_G(H)$, cioè il numero delle classi laterali destre rispetto ad H, è esattamente l'ordine del gruppo G/H per la definizione 0.17. □

Osservazione 0.19. Poiché in un gruppo commutativo ogni sottogruppo è normale, se G è commutativo è sempre possibile quozientarlo rispetto ad ogni suo sottogruppo.

Richiami sugli omomorfismi di gruppi

Definizione. Siano $(A, *_A, e_A)$ e $(B, *_B, e_B)$ due gruppi. Un'applicazione $f : A \longrightarrow B$ si dice *omomorfismo di gruppi* se $\forall a, a' \in A$ allora $f(a *_A a') = f(a) *_B f(a')$.
Si chiama *immagine di* f, e si denota con $\mathrm{Im}(f)$, il sottoinsieme di B

$$\mathrm{Im}(f) := \{b \in B \mid \exists\, a \in A : f(a) = b\}$$

Si chiama *nucleo di f*, e si denota con $\ker(f)$, il sottoinsieme di A

$$\ker(f) = \{a \in A \mid f(a) = e_B\}.$$

Osservazione 0.20. È noto che $\mathrm{Im}(f)$ è un sottogruppo del gruppo B, mentre $\ker(f)$ è sottogruppo normale del gruppo A.

Esempio 0.20.1. L'applicazione $f_0 : A \longrightarrow B$ definita da $a \mapsto e_B$ è un omomorfismo di gruppi, detto *omomorfismo nullo*. Altro semplice esempio di omomorfismo è l'applicazione identica $id_A : A \to A$ di un gruppo A in sé.

Esempio 0.20.2. L'applicazione

$$\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \cdot) \quad \text{definita da} \quad x \mapsto 2^x$$

è un omomorfismo di gruppi.

Esempio 0.20.3. Sia $(G, \cdot)$ un gruppo e $H \triangleleft G$. L'applicazione

$$\pi : G \longrightarrow G/H \quad \text{definita da} \quad x \mapsto [x] = Hx$$

è un omomorfismo di gruppi suriettivo (*epimorfismo di gruppi*), detto *proiezione canonica di G sul quoziente* G/H.

Ricordiamo i più noti risultati sull'argomento, rimandando la dimostrazione ad altri corsi.

Teorema 0.21. *(Primo Teorema di Omomorfismo di Gruppi). Se $f : A \longrightarrow B$ un omomorfismo di gruppi, allora esiste un unico omomorfismo iniettivo di gruppi $h : A/\ker(f) \to B$ tale che il diagramma*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\pi}\searrow & & \nearrow{\scriptstyle h} \\ & A/\ker(f) & \end{array}$$

sia commutativo, cioè tale che $f = h \circ \pi$, dove $\pi : A \to A/\ker(f)$ è la proiezione canonica. □

Teorema 0.22. *(Secondo Teorema di Omomorfismo di Gruppi). Sia $f : A \longrightarrow B$ un omomorfismo di gruppi, allora esiste una biezione tra i sottogruppi di A che contengono $\ker(f)$ e i sottogruppi di B che sono contenuti in $\mathrm{Im}(f)$.*
In particolare se $H \triangleleft K \triangleleft A$ sono sottogruppi normali e $H \triangleleft A$, allora è (ben) definito un epimorfismo di gruppi $A/H \to A/K$ che induce un isomorfismo canonico

$$\frac{A/H}{K/H} \cong A/K.$$ □

Ricordiamo infine che si può dotare il prodotto cartesiano di due gruppi della struttura di gruppo in modo naturale.

Proposizione - Definizione 0.23. *Siano $(G, \cdot, 1_G)$ e $(G', \cdot, 1_{G'})$ due gruppi. Il prodotto cartesiano $G \times G'$ è un gruppo rispetto all'operazione di prodotto così definita: comunque scelti $(g_1, g_1'), (g_2, g_2') \in G \times G'$ si pone*

$$(g_1, g_1') \cdot_{G\times G'} (g_2, g_2') = (g_1 \cdot_G g_1', g_2 \cdot_{G'} g_2').$$

Dimostrazione. Per definizione di $\cdot_{G\times G'}$, si ha immediatamente che $G\times G'$ è chiuso rispetto a tale operazione.
Ponendo $1_{G\times G'} := (1_G, 1_G')$ tale elemento è ovviamente neutro.
Inoltre, per ogni $(x, y) \in G \times G'$, l'elemento $(x^{-1}, y^{-1}) \in G \times G'$ è effettivamente il suo inverso. Infatti $(x, y) \cdot_{G\times G'} (x^{-1}, y^{-1}) = (x \cdot_G x^{-1}, y \cdot_{G'} y^{-1}) = (1_G, 1_{G'}) = 1_{G\times G'}$.
In ultimo si verifica l'associatività in quanto immediata conseguenza dell'associatività in G e in G'. □

Nozioni di base su anelli e ideali

Definizione. Si dice *anello* un insieme non vuoto A dotato di due operazioni binarie, dette *somma* e *prodotto*, e di un elemento *zero di* A, denotati rispettivamente con $+_A$, $\cdot_A$ (o, brevemente, con $+$ e $\cdot$) e 0_A , che soddisfano le seguenti proprietà:
(1) la terna $(A, +_A, 0_A)$ è un gruppo commutativo;
(2) il prodotto è associativo;
(3) il prodotto è distributivo rispetto alla somma (cioè per ogni $a, b, c \in A$ vale: $a(b + c) = ab + ac$ e $(b + c)a = ba + ca$).
Inoltre
(4) se esiste un elemento neutro per il prodotto, che si denota con 1_A, allora si dice che A è un *anello unitario*;
(5) se il prodotto è commutativo allora si dice che A è un *anello commutativo*.

L'esempio–tipo di anello (infinito) è l'insieme $\mathbb{Z}$ dei numeri interi con le usuali operazioni di somma e prodotto. Altri esempi di anelli (sempre rispetto alle operazioni consuete) sono $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Si osservi che sono tutti anelli commutativi unitari.

Si rimanda a corsi precedenti la dimostrazione della seguente

Proposizione 0.24. *Per ogni $n \in \mathbb{N}^*$, il gruppo additivo commutativo $\mathbb{Z}_n$ è un anello rispetto al prodotto definito da $[a][b] = [ab]$, per ogni $[a], [b] \in \mathbb{Z}_n$.* □

Osservazione 0.25. Se A è un anello allora per ogni $x \in A$ vale $x0_A = 0_A = 0_A x$. Infatti...

Tuttavia il prodotto di due elementi può essere nullo anche se non lo è nessuno dei due.

Definizione. In un anello A un elemento non nullo x tale che esista $y \neq 0_A$ per cui $xy = 0_A$ si dice *zero divisore sinistro*. Analogamente, se esiste $y \neq 0_A$ per cui $yx = 0_A$, allora x si dice *zero divisore destro*. Uno zero divisore sia sinistro che destro si dice *zero divisore bilatero* o semplicemente *zero divisore*. L'insieme di tutti gli zero divisori di un anello A si denota con $ZD(A)$.

Si prova facilmente la seguente utile proprietà, valida in un qualunque anello.

Proposizione 0.26. *(Legge di cancellazione). Se $x \in A$ è un non zero divisore allora, per ogni $y, z \in A$ vale*

$$xy = xz \quad \Rightarrow \quad y = z.$$

□

Definizione. Un anello privo di zero divisori si dice *integro*. Se inoltre è commutativo e unitario si dice *dominio di integrità* o semplicemente *dominio*.

Gli anelli citati prima, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sono tutti domini. Invece $\mathbb{Z}_n$ è un dominio se e solo se n è un numero primo.

Richiamiamo una importante nozione e alcune proprietà relative, lasciate al lettore.

Definizione. In un anello unitario A un elemento non nullo x si dice *invertibile* o *unità di A* se esiste un elemento $y \in A$ tale che $xy = 1_A = yx$. L'insieme di tutti gli elementi invertibili di A si denota con $\mathcal{U}(A)$.

Proposizione - Definizione 0.27. *Sia A un anello unitario e $x \in A$ un elemento invertibile. Allora esiste un unico elemento $y \in A$ tale che $xy = 1_A = yx$. Tale elemento si dice inverso di x e si denota con x^{-1}.*

Proposizione 0.28. *$\mathcal{U}(A)$ è un gruppo rispetto al prodotto di A. Inoltre $\mathcal{U}(A) \cap ZD(A) = \emptyset$.* □

Esempio 0.28.1. È chiaro che $\mathcal{U}(\mathbb{Z}) = \{+1, -1\}$ e che, in generale, $\mathcal{U}(A) \supseteq \{1_A, -1_A\}$, in quanto tali elementi sono sempre invertibili. La situazione opposta è quella di $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: infatti $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^*$, $\mathcal{U}(\mathbb{R}) = \mathbb{R}^*$, $\mathcal{U}(\mathbb{C}) = \mathbb{C}^*$. In questi casi dunque il gruppo degli elementi invertibili è il più grande possibile. In generale vale solo $\mathcal{U}(A) \subseteq A^*$.

Definizione. Sia A un anello unitario tale che $\mathcal{U}(A) = A^*$: in tal caso si dice che A è un *corpo*. Se inoltre A è commutativo, diremo che è un *campo*.

Con questa terminologia, alla luce dell'esempio precedente, è chiaro che $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono campi, mentre $\mathbb{Z}$ non lo è. Proveremo che $\mathbb{Z}_n$ è un campo se e solo se n è un numero primo, attraverso una rapida dimostrazione che usa la funzione di Eulero.

Si osservi infine che ogni corpo è un dominio (segue immediatamente da 0.28).

Definizione. Se A è un anello, un suo *sottoanello* è un suo sottoinsieme non vuoto che è un anello rispetto alle stesse operazioni di A. Inoltre, se A è unitario, un suo sottoanello che contenga 1_A si dice *sottoanello unitario*.

È chiaro che se B è un sottoanello di A, in particolare $(B, +_A)$ è un sottogruppo (normale) del gruppo $(A, +_A)$ e inoltre B è chiuso rispetto al prodotto di A. È interessante osservare che tali proprietà sono anche sufficienti a rendere B un sottoanello di A, come mostra il seguente risultato.

Proposizione 0.29. *(Caratterizzazione di sottoanello). Se A è un anello e $\emptyset \neq B \subseteq A$ allora*

$$B \text{ è un sottoanello di } A \quad \Longleftrightarrow \quad \forall x, y \in B: \quad x - y \in B,\ xy \in B.$$

Dimostrazione. Lasciata al lettore. □

Osservazione 0.30. Se B è un sottoanello di A, si può considerare il gruppo quoziente A/B (si ricordi che $(A,+)$ è un gruppo commutativo, dunque ogni suo sottogruppo è normale). Tuttavia tale gruppo non è un anello rispetto al prodotto "naturale" definito da $[x][y] = [xy]$. Questo induce a definire un'altra "sottostruttura buona" per quozientare un anello in modo da ottenere un anello.

Definizione. Se A è un anello e $\emptyset \neq I \subseteq A$, diciamo che I è un *ideale di* A se
i) $(I,+_A)$ è un sottogruppo di $(A,+_A)$;
ii) per ogni $x \in I$, $a \in A$ si ha $ax \in I$ e $xa \in I$.
La *(ii)* viene detta anche *proprietà di assorbimento.*

Osservazione - Definizione 0.31. Sia A un anello. Allora:
i) un ideale di A è un sottoanello non unitario di A (anche se A è unitario);
ii) il sottoinsieme $\{0_A\}$ è un ideale di A, detto *ideale nullo*, e denotato con (0_A);
iii) il sottoinsieme $A \subseteq A$ è un ideale di A.
Gli ideali (0_A) e A sono detti *ideali banali* di A. Un ideale I si dice *proprio*, quando $I \neq A$ e $I \neq (0_A)$.

Vedremo che gli ideali di $\mathbb{Z}$ sono tutti e soli i suoi sottogruppi additivi, cioè i sottoinsiemi del tipo

$$(n) := \{nx \mid x \in \mathbb{Z}\} = n\mathbb{Z}.$$

Gli ideali di $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono solo quelli banali. Ciò accade in qualunque campo:

Proposizione 0.32. *Se A è un anello commutativo unitario e I è un suo ideale, allora:*
i) $I = A \Leftrightarrow I$ contiene un elemento invertibile;
ii) A è un campo $\Leftrightarrow$ gli unici ideali di A sono gli ideali banali: (0_A) e $(1_A) = A$.

Dimostrazione. *i)* "$\Rightarrow$" Ovvio, in quanto A è un anello unitario quindi $1_A \in A = I$.
"$\Leftarrow$" Supponiamo che $x \in I$ e x invertibile; allora esiste $x^{-1} \in A$ cioè $1_A = x \cdot x^{-1} \in I$ per la proprietà di assorbimento. Quindi $1_A \in I$ e dunque, ancora per la proprietà di assorbimento, per ogni $a \in A$ si ha che $1_A \cdot a = a \in I$, quindi $I = A$.
ii) Ricordiamo che, per definizione, A è un campo $\Leftrightarrow \mathcal{U}(A) = A^*$.
"$\Rightarrow$" Supponiamo che I sia un ideale non nullo di A. Allora esiste $x \in I$ con $x \neq 0_A$, quindi x è invertibile. Per (i) vale quindi che $I = A = (1_A)$.
"$\Leftarrow$" Dobbiamo provare che $\mathcal{U}(A) = A^*$. Ricordiamo che l'inclusione "$\subseteq$" è sempre vera. Per provare l'altra, sia $x \in A$ con $x \neq 0_A$ e mostriamo che x è invertibile.
Si consideri l'ideale principale generato da x: poiché $x \neq 0_A$ allora $(x) \neq (0_A)$, quindi $(x) = A$ per ipotesi. Dunque $A = \{ax \mid a \in A\}$; in particolare $1_A = ax$ per qualche $a \in A$ quindi a è l'inverso di x. □

Il problema di determinare una sottostruttura adatta al passaggio della struttura di anello al quoziente viene risolto dalla struttura di ideale. Infatti, se I è un ideale di A, allora $I \triangleleft (A,+)$ dunque $(A/I,+)$ è un gruppo commutativo. Inoltre il seguente noto risultato (la cui dimostrazione è stata vista in altri corsi) conclude la questione.

Proposizione 0.33. *Se I è un ideale di un anello A, allora il gruppo commutativo $(A/I,+)$ è un anello rispetto al prodotto definito da $[x][y] = [xy]$, per ogni $[x],[y] \in A/I$.* □

Osservazione 0.34. Se I è un ideale di un anello A allora:
1. A unitario $\Rightarrow A/I$ unitario;
2. A commutativo $\Rightarrow A/I$ commutativo.

Proposizione-Definizione 0.35. *Sia A un anello e $S \subseteq A$ un suo sottinsieme non vuoto. Allora*

$$(S) := \left\{ \sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}, a_i \in A, x_i \in S \right\}$$

è un ideale di A, detto ideale generato da S, e il sottoinsieme S si dice sistema di generatori di (S).

Dimostrazione. Occorre provare che:
1) $x, y \in (S) \Rightarrow x - y \in (S)$;
2) $x \in (S), a \in A \Rightarrow xa \in (S)$.

Osserviamo preliminarmente che sia x che y sono combinazioni lineari finite di elementi di S a coefficienti in A. Quindi se si denotano con $x_1, \ldots, x_n$ tutti gli elementi di S che compaiono in almeno una delle due combinazioni lineari, si possono scrivere x e y come

$$x = \sum_{i=1}^{n} a_i x_i \ , \quad y = \sum_{i=1}^{n} b_i x_i$$

per opportuni $a_i, b_i \in A$ (dove, eventualmente, alcuni tra gli a_i e b_i sono nulli).
Pertanto

$$x - y = \sum_{i=1}^{n} (a_i x_i - b_i x_i) = \sum_{i=1}^{n} (a_i - b_i) x_i$$

e questo è chiaramente un elemento di (S), dunque (1) è provata.
2) Si consideri ora il prodotto ax:

$$ax = a \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (a a_i) x_i \in (S)$$

e anche tale elemento appartiene a (S). □

La seguente caratterizzazione motiva la definizione precedente:

Proposizione 0.36. *(S) è il più piccolo ideale di A contenente S.*

Dimostrazione. Proviamo anzitutto che $(S) \supseteq S$. Tale fatto segue immediatamente da fatto che, se $x \in S$ allora $x = 1_A x \in (S)$. Resta da provare che, se I è un ideale contenente S allora $I \supseteq (S)$.
Si consideri dunque un generico elemento di (S):

$$\sum_{i=1}^{n} a_i x_i$$

con $a_i \in A$ e $x_i \in S$, per ogni $i = 1, \ldots, n$. Poiché $I \supseteq S$ allora $x_i \in I$, per ogni $i = 1, \ldots, n$. Ma I è un ideale, quindi anche $a_i x_i \in I$ per ogni $a_i \in A$. Infine si ricordi che I è un sottogruppo additivo, in quanto ideale, quindi $\sum_{i=0}^{n} a_i x_i \in I$. □

Notazione. Se $S = \{x_1 \ldots, x_n\}$ è un insieme finito, si denota con $(x_1 \ldots, x_n)$ l'ideale generato da S.

Definizione. Un ideale I si dice *finitamente generato (f.g.)* se esiste un sistema di generatori finito di I, cioè esistono $x_1, \ldots, x_n \in A$ tali che $I = (x_1, \ldots, x_n)$.

Osservazione 0.37. Se $I = (x_1, \ldots, x_n)$, tutti i suoi elementi sono del tipo $\sum_{i=1}^{n} a_i x_i$ con $a_i \in A$.

Definizione. Se $I = (x) = \{ax \mid a \in A\}$ allora I è detto *ideale principale*. Se un anello ha solo ideali principali si dice *Principal Ideal Ring* (PIR), se inoltre è integro si dirà *Principal Ideal Domain* (PID).

Concludiamo con un risultato che permette di costruire un terzo anello partendo da due anelli dati.

Proposizione 0.38. *Siano A e B due anelli, allora l'insieme $A \times B$ dotato delle operazioni*

$$(a, b) +_{A\times B} (a', b') := (a +_A a', b +_B b'), \quad \forall (a, b), (a', b') \in A \times B$$
$$(a, b) \cdot_{A\times B} (a', b') := (a \cdot_A a', b \cdot_B b'), \quad \forall (a, b), (a', b') \in A \times B$$

è un anello.
Inoltre, se A e B sono anelli unitari, allora anche $A \times B$ è un anello unitario con identità $1_{A\times B} = (1_A, 1_B)$.

Dimostrazione. Lasciata al lettore. □

Generalizzando la situazione precedente, dati gli anelli $A_1, \ldots, A_s$, anche $A_1 \times \cdots \times A_s$ può essere dotato della struttura anello con le operazioni "componente per componente" analoghe a quelle definite in 0.38.

D'ora in poi considereremo sempre, tranne dove diversamente specificato, anelli commutativi.

Definizione. Siano A e B due anelli e sia $f : A \to B$ un'applicazione tale che:
1) $f(x +_A y) = f(x) +_B f(y)$, $\forall x, y \in A$ (ossia f preserva la somma);
2) $f(x \cdot_A y) = f(x) \cdot_B f(y)$, $\forall x, y \in A$ (ossia f preserva il prodotto).
Allora f viene detta *omomorfismo di anelli*. Se inoltre A e B sono anelli unitari e vale
3) $f(1_A) = 1_B$,
allora diciamo che f è un *omomorfismo unitario di anelli*.

Proposizione 0.39. *Sia $f : A \to B$ un omomorfismo di anelli. Allora*
1) $f(0_A) = 0_B$;
2) $f(-a) = -f(a)$, *per ogni* $a \in A$.
Se inoltre A e B sono anelli unitari e f è un omomorfismo unitario di anelli allora
3) $f(a^{-1}) = f(a)^{-1}$, *per ogni* $a \in \mathcal{U}(A)$.
In tal caso la restrizione di f agli elementi invertibili di A è un omomorfismo di gruppi moltiplicativi $f : \mathcal{U}(A) \to \mathcal{U}(B)$.

Dimostrazione. Le proprietà (1) e (2) seguono dal fatto che un omomorfismo di anelli è un omomorfismo dei gruppi additivi soggiacenti (definizione, parte (1)).
(3) Essendo f omomorfismo unitario, vale $1_B = f(1_A) = f(aa^{-1}) = f(a)f(a^{-1})$, dunque $f(a^{-1})$ è l'inverso di $f(a)$ in B. L'ultima affermazione è un semplice esercizio lasciato al lettore. □

Richiamiamo un noto risultato (dimostrato in altri corsi), dove le nozioni di immagine e di nucleo di un omomorfismo di anelli sono le stesse di quelle introdotte per gli omomorfismi di gruppi. Di seguito ricordiamo i teoremi fondamentali sugli omomorfismi di anelli.

Proposizione 0.40. *Sia $f : A \to B$ un omomorfismo di anelli. Allora* $\mathrm{Im}(f)$ *è un sottoanello di B e* $\ker(f)$ *è un ideale di A.* □

Teorema 0.41. *(Primo Teorema di omomorfismo di anelli). Se $f : A \longrightarrow B$ un omomorfismo di anelli, allora esiste un unico monomorfismo di anelli $h : A/\ker(f) \to B$ tale che il diagramma*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi}\searrow & & \nearrow_{h} \\ & A/\ker(f) & \end{array}$$

sia commutativo, cioè tale che $f = h \circ \pi$, dove $\pi : A \to A/\ker(f)$ è la proiezione canonica. □

Teorema 0.42. *(Secondo Teorema di omomorfismo di anelli).*
Sia $f : A \longrightarrow B$ un omomorfismo di anelli, allora esiste una biezione tra gli ideali di A che contengono $\ker(f)$ *e gli ideali di B che sono contenuti in* $\mathrm{Im}(f)$. *In particolare se $H \subseteq K \subseteq A$ sono ideali, allora è (ben) definito un epimorfismo di anelli $A/H \to A/K$ che induce un isomorfismo canonico di anelli*

$$\frac{A/H}{K/H} \cong A/K.$$ □

Da tale teorema discende un utile corollario:

Corollario 0.43. *(Caratterizzazione degli ideali dei quozienti). Gli ideali di un anello quoziente A/J sono tutti e soli del tipo J/I, dove J è un ideale di A contenente I.* □

Interessante può essere considerare un'omomorfismo di anelli che abbia per dominio un particolare esempio di anello, ossia un campo. In tal caso vale il seguente fatto:

Proposizione 0.44. *Sia K un campo e B un anello qualsiasi. Se $f : K \to B$ è un omomorfismo di anelli non identicamente nullo, allora f è iniettivo.*

Dimostrazione. Per ipotesi K è un campo e quindi ha solo ideali banali. Per la proposizione 0.40, $\ker(f)$ è un ideale di K. Per questo motivo o $\ker(f) = K$ o $\ker(f) = \{0\}$. Nel primo caso f sarebbe l'applicazione identicamente nulla, che è contro l'ipotesi. Dunque $\ker(f) = \{0\}$ e quindi f risulta essere iniettivo. □

Divisione euclidea e ideali di $\mathbb{Z}$

Teorema 0.45. *(Divisione euclidea). Dati due interi a e b con $b \neq 0$ esiste un'unica coppia di interi q ed r, detti quoziente e resto, tali che:*

$$a = b \cdot q + r \quad con \quad 0 \leq r < |b|$$

dove $|b|$ indica il valore assoluto del divisore.

Dimostrazione.
Esistenza. Consideriamo l'insieme:

$$S = \{a - nb \,|\, n \in Z\,,\, a - nb \geq 0\}.$$

Tale insieme è non vuoto infatti: se $n = a$ si ha

$$a - nb = a - ab = a(1 - b)$$

mentre se $n = -a$ si ha

$$a - nb = a + ab = a(1 + b)$$

e poiché $b \neq 0$ almeno uno dei due prodotti deve essere positivo.
Per il principio del buon ordinamento esiste un intero positivo r che è il minimo di S, dunque per tale r esisterà un numero intero q tale che $r = a - qb$. Inoltre essendo r il minimo di S si deve avere $r < |b|$. Infatti se, per assurdo, così non fosse, avremmo che $r' := r - |b| \geq 0$ e che

$$r' = r - |b| = (a - qb) - |b| = a - \left(q + \frac{|b|}{b}\right) b$$

dunque r' sarebbe in S, ma poiché è più piccolo di r, che è il minimo, siamo giunti ad un assurdo.
Unicità. Supponiamo che ci siano due coppie (q, r) e (q', r') tali che:

$$a = bq + r, \qquad 0 \leq r < |b|, \qquad \text{e} \qquad a = bq' + r', \qquad 0 \leq r' < |b|.$$

Allora si ha

$$r - r' = -(q - q')b. \tag{$*$}$$

Inoltre poiché r e r' sono positivi e minori di $|b|$:

$$r - r' \leq r < |b| \quad \text{e} \quad r' - r \leq r' < |b|$$

quindi da (*) si ricava $|q - q'| \cdot |b| \leq |r - r'| < |b|$ ovvero $|q - q'| < 1$ e poiché si tratta di un numero intero e positivo: $|q - q'| = 0$.
Quindi, da $(*)$ si deduce anche $r - r' = 0$ cioè le coppie sono uguali. □

Tale risultato consente di determinare tutti i sottogruppi del gruppo additivo $\mathbb{Z}$. Chiaramente tra questi ci sono i sottogruppi ciclici del tipo $\langle n \rangle = n\mathbb{Z} = \{an \,|\, a \in \mathbb{Z}\}$, per ogni $n \in \mathbb{Z}$. Il teorema 0.45 permette di provare che non ce ne sono altri. Come ulteriore conseguenza si determinano tutti gli ideali dell'anello $\mathbb{Z}$.

Corollario 0.46. *I sottogruppi di $(\mathbb{Z}, +, 0)$ sono tutti e soli i sottogruppi ciclici $\langle n \rangle$, con $n \in \mathbb{Z}$.*

Dimostrazione. Sia H un sottogruppo di $\mathbb{Z}$. Se H è nullo, allora è ciclico. Altrimenti sia $n \in H$ il minimo elemento positivo (che esiste per il Principio del Buon Ordinamento, essendo $H \cap \mathbb{N} \neq \emptyset$).
Per definizione di sottogruppo si ha $\langle n \rangle \subseteq H$. Per dimostrare che sono uguali, consideriamo un qualunque $h \in H$ e la divisione di h per n, essendo $n \neq 0$. Per 0.45, esistono $q, r \in \mathbb{Z}$ tali che $h = nq + r$ con $0 \leq r < n$. Essendo $nq \in \langle n \rangle \subseteq H$ e $h \in H$, allora anche $r = h - nq \in H$. Ma $r < n$ come osservato prima ed n è il minimo positivo di H per ipotesi; quindi necessariamente $r = 0$, da cui $h = nq$ e quindi $H \subseteq \langle n \rangle$.

Corollario 0.47. *Gli ideali di $\mathbb{Z}$ sono tutti e soli del tipo (n), con $n \in \mathbb{N}$. In particolare, $\mathbb{Z}$ è un PID.*

Dimostrazione. Immediato dal fatto che ogni ideale è un sottogruppo di $(\mathbb{Z}, +, 0)$ e dunque del tipo $\langle n \rangle$ per 0.46. Chiaramente $\langle n \rangle = (n)$. □

Campo dei quozienti di un dominio

La costruzione del campo dei quozienti di un dominio generalizza in modo naturale la costruzione del campo $\mathbb{Q}$ dei numeri razionali partendo dal dominio $\mathbb{Z}$, vista in altri corsi.

Anche se tale argomento riguarda la teoria degli anelli in generale, in letteratura viene spesso svolto nella parte riguardante i polinomi. Infatti una delle applicazioni più interessanti concerne proprio l'anello dei polinomi a coefficienti in un campo, come vedremo nel prossimo paragrafo.

Definizione. Sia A un dominio di integrità. In $A \times A^*$ consideriamo la seguente relazione:

$$(x, y) \sim (x', y') \iff xy' = x'y.$$

Si verifica facilmente che $\sim$ è una relazione d'equivalenza. L'insieme quoziente $A \times A^*/\sim$ si denota con $Q(A)$ e il suo generico elemento $[(x, y)]$ si denota con x/y.

In $Q(A)$ sono definite in modo naturale due operazioni indotte da quelle di A:

$$\frac{x}{y} + \frac{x'}{y'} := \frac{xy' + x'y}{yy'}$$

$$\frac{x}{y} \cdot \frac{x'}{y'} := \frac{xx'}{yy'}$$

Proposizione - Definizione 0.48. *Le operazioni precedenti sono ben definite e con esse $Q(A)$ è un campo, detto campo dei quozienti di A.*

Dimostrazione. Lasciamo al lettore la verifica che le operazioni di somma e prodotto sono ben definite e che, rispetto ad esse, $Q(A)$ è un anello commutativo unitario.
Resta da verificare che, comunque preso un elemento diverso da zero di $Q(A)$, esiste in $Q(A)$ il suo inverso. Sia dunque $a/b \neq 0_{Q(A)}$ cioè

$$\frac{a}{b} \neq \frac{0_A}{1_A} \iff (a, b) \not\sim (0, 1) \iff a \neq 0.$$

Pertanto in $Q(A)$ esiste b/a. Si verifica immediatamente che

$$\frac{a}{b} \cdot \frac{b}{a} = 1_{Q(A)}.$$

□

Esempio 0.48.1. È chiaro che $Q(\mathbb{Z}) = \mathbb{Q}$.

Per calcolare rapidamente il campo dei quozienti dei noti campi numerici, utilizzeremo il seguente risultato.

Teorema 0.49. *Se A è un dominio allora:*
i) l'applicazione $i : A \longrightarrow Q(A)$ t.c. $i(x) = x/1$ è un monomorfismo di anelli;
ii) A è un campo $\iff$ l'omomorfismo i è un isomorfismo.

Dimostrazione. *i)* Si verifica immediatamente che i è un omomorfismo di anelli, infatti:

$$i(x + y) = \frac{x + y}{1} = \frac{x}{1} + \frac{y}{1} = i(x) + i(y)$$

e inoltre

$$i(xy) = \frac{xy}{1} = \frac{x}{1} \cdot \frac{y}{1} = i(x)i(y)$$

Per quanto riguarda l'iniettività, si osservi che

$$\ker(i) = \{x \in A : i(x) = 0\} = \left\{x \in A : \frac{x}{1} = 0_{Q(a)} = \frac{0}{1}\right\}$$

ma $x/1 = 0/1 \iff x = 0$ dunque $\ker(i) = \{0\}$.
ii) Basta provare che A è un campo $\iff$ i è suriettiva.
"$\Rightarrow$" Sia $a/b \in Q(A)$. Poiché $a/b = ab^{-1}$, basta provare che $b^{-1} \in \mathrm{Im}(i)$, essendo $\mathrm{Im}(i)$ un sottoanello di $Q(A)$. Consideriamo $b \in A$; poiché A è un campo per ipotesi, esiste $b^{-1} \in A$. Allora $\frac{b^{-1}}{1} \in \mathrm{Im}(i)$ e quindi i è suriettiva.
"$\Leftarrow$" Dobbiamo provare che per ogni $a \in A$ esiste $b \in A$ tale che $ab = 1$. Per ipotesi i è suriettiva dunque $i(a)^{-1} \in Q(A)$ appartiene all'immagine di i. Pertanto esiste $b \in A$ tale che $i(b) = i(a)^{-1}$. Quindi $i(a)i(b) = 1_{Q(A)}$. Essendo i un monomorfismo di anelli:

$$i(ab) = 1_{Q(A)} \quad \Rightarrow \quad ab = 1_A. \qquad \square$$

Esempio 0.49.1. Dal risultato precedente segue che $Q(\mathbb{Q}) = \mathbb{Q}$, $Q(\mathbb{R}) = \mathbb{R}$ e $Q(\mathbb{C}) = \mathbb{C}$.

Teorema 0.50. *(Proprietà universale del campo dei quozienti). Siano A un dominio, K un campo e $j : A \longrightarrow K$ un omomorfismo di anelli. Allora esiste un unico omomorfismo di anelli $\psi : Q(A) \longrightarrow K$ tale che $j = \psi \circ i$.*

Dimostrazione. Proviamo dapprima l'esistenza. Sia $\psi : Q(A) \longrightarrow K$ definito da

$$\psi\left(\frac{x}{y}\right) = j(x)j(y)^{-1}.$$

Verifichiamo che ψ è ben definito: sia $x'/y' = x/y$. Allora $x'y = xy'$, quindi essendo j un omomorfismo di anelli:

$$j(x'y) = j(xy') \quad \Rightarrow \quad j(x')j(y) = j(x)j(y') \quad \Rightarrow \quad j(x')j(y')^{-1} = j(x)j(y)^{-1}.$$

Pertanto l'immagine di un elemento di $Q(A)$ non dipende dalla scelta del rappresentante.
Verifichiamo ora che ψ è un omomorfismo. Utilizzando la definizione di somma in $Q(A)$, le proprietà della somma in K e il fatto che j sia un omomorfismo d'anelli si ha:

$$\begin{aligned}\psi\left(\frac{x}{y} + \frac{x'}{y'}\right) &= \psi\left(\frac{xy' + yx'}{yy'}\right) = j(xy' + yx')j(yy')^{-1} = [j(xy') + j(yx')]j(yy')^{-1} = \\ &= j(xy')j(yy')^{-1} + j(yx')j(yy')^{-1} = j(x)j(y')j(y)^{-1}j(y')^{-1} + j(y)j(x')j(y)^{-1}j(y')^{-1} = \\ &= j(x)j(y)^{-1} + j(x')j(y')^{-1} = \psi\left(\frac{x}{y}\right) + \psi\left(\frac{x'}{y'}\right).\end{aligned}$$

In modo analogo

$$\begin{aligned}\psi\left(\frac{x}{y} \cdot \frac{x'}{y'}\right) = \psi\left(\frac{xx'}{yy'}\right) &= j(xx')j(yy')^{-1} = j(x)j(x')[j(y)j(y')]^{-1} = \\ &= j(x)j(x')j(y)^{-1}j(y)^{-1} = \psi\left(\frac{x}{y}\right) \cdot \psi\left(\frac{x'}{y'}\right).\end{aligned}$$

Questo prova l'esistenza dell'omomorfismo richiesto. Si lascia al lettore la dimostrazione dell'unicità. $\square$

Corollario 0.51. *Siano A e A' due domini e sia $\alpha : A \longrightarrow A'$ un omomorfismo di anelli. Allora esiste un unico omomorfismo di anelli $\overline{\alpha} : Q(A) \longrightarrow Q(A')$ che estende α. In particolare, $\overline{\alpha}$ è definito da*

$$\overline{\alpha}\left(\frac{x}{y}\right) = \frac{\alpha(x)}{\alpha(y)}$$

per ogni $x/y \in Q(A)$.

Dimostrazione. Si consideri il diagramma seguente, dove la freccia diagonale denota la composizione $i' \circ \alpha$

$$\begin{array}{ccc} A & \stackrel{\alpha}{\longrightarrow} & A' \\ {\scriptstyle i}\downarrow & \searrow & \downarrow{\scriptstyle i'} \\ Q(A) & & Q(A') \end{array} .$$

Ovviamente $i' \circ \alpha : A \to Q(A')$ è un omomorfismo di anelli, in quanto i' e α lo sono. Quindi, per 0.50, esiste un unico omomorfismo di anelli $\overline{\alpha} : Q(A) \longrightarrow Q(A')$ tale che $i' \circ \alpha = \overline{\alpha} \circ i$. Questo significa che il diagramma

$$\begin{array}{ccc} A & \stackrel{\alpha}{\longrightarrow} & A' \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle i'} \\ Q(A) & \stackrel{\overline{\alpha}}{\longrightarrow} & Q(A') \end{array}$$

è commutativo o, equivalentemente, che $\overline{\alpha}$ estende α.
L'ultima affermazione dell'enunciato è una facile verifica. □

Capitolo 1 - Teoria dei gruppi *

Cenni di aritmetica modulare

In questo paragrafo vedremo alcuni risultati "storici" della teoria dei gruppi finiti, ma avremo bisogno della struttura di anello di $\mathbb{Z}$ e degli $\mathbb{Z}_n := \mathbb{Z}/(n)$ (vedi 0.33 e 0.47). In realtà avremo bisogno soltanto dell'operazione di prodotto. Ricordiamo infine che $o(\mathbb{Z}_n) = n$.

Diremo che due interi non nulli $a, b \in \mathbb{Z}$ sono *coprimi* se non hanno divisori comuni, a parte 1 e -1, e scriveremo $(a, b) = 1$.

Proposizione 1.1. *Sia $\Phi_n := \{a \in \mathbb{N}^* \mid a < n, (a, n) = 1\}$. Allora le classi in $\mathbb{Z}_n$ degli elementi di Φ_n formano un gruppo rispetto al prodotto usuale di $\mathbb{Z}_n$.*

Dimostrazione.
Vogliamo dunque provare che $U_n := \{[a] \in \mathbb{Z}_n \mid a \in \Phi_n\}$ è un gruppo rispetto al prodotto.

(*i*) Osserviamo dapprima che $[0] \notin U_n$ in quanto Φ_n non contiene 0 e nessun multiplo di n. Inoltre vale la legge di cancellazione, cioè comunque scelti $a, b, c \in \Phi_n$ allora $[a][b] = [a][c] \Rightarrow [b] = [c]$. Dall'ipotesi: $ab - ac \in (n) \Rightarrow a(b - c) \in (n) \Rightarrow b - c \in (n) \Rightarrow [b] = [c]$, dove la penultima implicazione segue dal fatto che a ed n non hanno divisori comuni.

(*ii*) Mostriamo che U_n è chiuso rispetto al prodotto. Siano $[a], [b] \in U_n$ tali che a, b siano i rispettivi rappresentanti canonici; pertanto $(a, n) = 1$ e $(b, n) = 1$ dunque $(ab, n) = 1$. Se $ab < n$ allora $ab \in \Phi_n$ e quindi $[ab] \in U_n$, come richiesto. Altrimenti, si scelga il rappresentante canonico c di $[ab]$, cioè tale che $c = ab - qn > 0$ e $ab - (q + 1)n < 0$. Ne segue che $c < n$ e $(c, n) = 1$, dunque $c \in \Phi_n$ e quindi $[ab] = [c] \in U_n$.

(*iii*) È immediato vedere che $[1]_{\mathbb{Z}_n} \in U_n$. Infatti $1 \leq n$ e $(1, n) = 1$ qualunque sia $n \in \mathbb{N}^*$.

(*iv*) Associatività del prodotto: verificata in quanto vale nell'anello $\mathbb{Z}_n$.

(*v*) Esistenza dell'inverso. Sia $[a] \in U_n$ e si consideri l'insieme $\{[a]^k \mid k \in \mathbb{N}\} \subseteq U_n$, dove l'inclusione vale per (*ii*). Essendo U_n finito, anche $\{[a]^k \mid k \in \mathbb{N}\}$ è finito, perciò esistono p, q con $p \neq q$ tali che $[a]^p = [a]^q$. Si assuma ad esempio che $p = q + s,\ s \neq 0$. Vale dunque: $[a]^{q+s} = [a]^p = [a]^q$ e ciò implica, per la legge di cancellazione provata in (*i*), che $[a]^s = [1]$ e quindi $[a]^{s-1} = [a]^{-1}$. Si noti che $s - 1 \geq 0$, dunque $[a]^{s-1} \in U_n$. Pertanto esiste l'inverso di $[a]$ in U_n. □

Possiamo riformulare la proposizione precedente nel seguente modo:

Teorema 1.2. *Sia $\pi' : \Phi_n \to \mathbb{Z}_n$ la restrizione della proiezione canonica $\pi : \mathbb{Z} \to \mathbb{Z}_n$. Allora $U_n := \mathrm{Im}(\pi')$ è un gruppo rispetto all'operazione di prodotto di $\mathbb{Z}_n$.* □

Il precedente risultato permette di associare il gruppo (moltiplicativo) U_n ad ogni n non nullo. Il suo ordine è il numero di elementi di Φ_n in quanto π' è iniettivo. Si introduce dunque la seguente nozione.

Definizione. La funzione $\phi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ definita (a tratti) da:

$$\begin{cases} \phi(1) & := & 1 \\ \phi(n) & := & \#\Phi_n = o(U_n), \quad \forall n > 1 \end{cases}$$

si dice *funzione di Eulero*.

Ad esempio $\Phi(2) = \{1\}$, $\Phi(3) = \{1, 2\}$, $\Phi(4) = \{1, 3\}$, $\Phi(5) = \{1, 2, 3, 4\}$, $\Phi(6) = \{1, 5\}$, ...
Quindi $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, ... È chiaro che, se n è primo, allora $\phi(n) = n - 1$.

Teorema 1.3. *(Eulero). Siano $n \in \mathbb{N}^*$ e $a \in \mathbb{N}$ tali che $(a, n) = 1$. Allora*

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

Dimostrazione. Per ipotesi $[a] \neq [0]$ in $\mathbb{Z}_n$. Sia $b \in \mathbb{N}$ il rappresentante canonico di $[a]$, cioè $b \equiv_n a$ e $0 < b < n$. Poiché $(a, n) = 1$ e b differisce da a per un multiplo di n, anche $(b, n) = 1$ e dunque $b \in \Phi_n$.
Ne segue che la sua classe in $\mathbb{Z}_n$ appartiene al gruppo U_n introdotto in 1.1: $[b] \in U_n$. Dunque per 0.13, si ha che $[b]^{o(U_n)} = [1]$.
Ma $[b] = [a]$ e $o(U_n) = \phi(n)$ per definizione di funzione di Eulero, quindi $[a]^{\phi(n)} = [1]$ in $\mathbb{Z}_n$. □

* Versione 20.3.2017

Esercizio 1.3.1. Determinare i gruppi U_8 e U_9. Uno dei due è ciclico e l'altro no.

Immediata conseguenza del teorema di Eulero, nel caso in cui n sia primo (e quindi $\phi(n) = n - 1$), è il seguente famoso risultato

Teorema 1.4. *(Piccolo Teorema di Fermat). Sia p un numero primo e $a \in \mathbb{N}$ non sia multiplo di p. Allora*

$$a^{p-1} \equiv 1 \pmod{p}. \qquad \square$$

La restante parte di questo paragrafo è dedicata alla dimostrazione del cosiddetto *Teorema Cinese dei Resti*. Qui verrà provato nell'ambito dell'algebra modulare, quindi riguarda i numeri interi. Ritroveremo ulteriori formulazioni in altri contesti.

A tale scopo, ricordiamo dapprima alcuni risultati riguardanti i gruppi ciclici e fissiamo le notazioni.
Si prova facilmente il seguente risultato, la cui dimostrazione è lasciata al lettore:

Lemma 1.5. *Siano A e B due gruppi ciclici e $f : A \to B$ un omomorfismo di gruppi. Se a è un generatore di A allora* $\mathrm{Im}(f)$ *è un sottogruppo ciclico di B e $f(a)$ è un suo generatore.* $\square$

Segue immediatamente l'importante risultato sui gruppi ciclici:

Teorema 1.6. *Due gruppi ciclici dello stesso ordine sono isomorfi e, in particolare, si ha che ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_n$.* $\square$

Ricordiamo che due numeri interi n e m si dicono *coprimi* se non hanno fattori comuni, cioè se $(n, m) = 1$. Inoltre si denota con $m.c.m.(a, b)$ il *minimo comune multiplo* (positivo) di due interi a e b.

Il seguente risultato (importante per suo conto) sarà utile per provare il teorema conclusivo di questa parte.

Teorema 1.7. *Siano A e B gruppi ciclici finiti, di ordini n e m rispettivamente. Allora*

$$n \text{ ed } m \text{ sono coprimi } \iff A \times B \text{ è un gruppo ciclico di ordine } nm.$$

Dimostrazione. Ovviamente il gruppo $A \times B$ ha ordine nm. Osserviamo preliminarmente che, posto $t := m.c.m.(n, m)$, si ha $(x, y)^t = (x^t, y^t) = (1_A, 1_B)$, per ogni $(x, y) \in A \times B$ (per definizione di minimo comune multiplo e per 0.13 applicato ad A e B).
Siano a un generatore di A e b un generatore di B. In particolare, $o(a) = n$ e $o(b) = m$.
Si consideri il sottogruppo ciclico di $A \times B$ generato dall'elemento (a, b):

$$T := \langle (a, b) \rangle \leq A \times B.$$

Proviamo che tale sottogruppo ha ordine t. Come osservato all'inizio, $(a, b)^t = (a^t, b^t) = (1_A, 1_B)$. Supponendo che esista $\tau < t$ tale che $(a, b)^\tau = (1_A, 1_B)$, si vede immediatamente che $n|\tau$ e che $m|\tau$. Dunque τ è un multiplo comune di n e m, il che è assurdo. Pertanto $t = o((a, b)) = o(T)$. Proviamo ora l'equivalenza richiesta.

"$\Rightarrow$" Supponiamo che n ed m siano coprimi. In tal caso $t = nm$, quindi $o(T) = nm = o(A \times B)$ e dunque $T = A \times B$, che risulta pertanto ciclico.

"$\Leftarrow$" Supponiamo ora che $A \times B$ sia ciclico; dunque ammette un elemento di ordine nm. Sia esso (x, y). Come osservato preliminarmente anche per esso vale $(x, y)^t = (x^t, y^t) = (1_A, 1_B)$. Quindi nm divide t: impossibile a meno che $t = nm$. Questo implica che n ed m sono coprimi. $\square$

Esempio 1.7.1. Poiché $(2, 3) = 1$ si ha l'isomorfismo $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Teorema 1.8. *Siano m e n due naturali coprimi tra loro e u e v due interi. Allora esiste $x \in \mathbb{Z}$ tale che*

$$x \equiv_m u \quad e \quad x \equiv_n v.$$

Dimostrazione. Consideriamo i gruppi ciclici additivi $\mathbb{Z}_m$ e $\mathbb{Z}_n$; per il teorema 1.7. $\mathbb{Z}_m \times \mathbb{Z}_n$ è un gruppo (additivo) ciclico di ordine mn ed è generato da $([1]_m, [1]_n)$.
Consideriamo le classi di u e v nei due gruppi considerati: $[u]_m \in \mathbb{Z}_m$ e $[v]_n \in \mathbb{Z}_n$, e il corrispondente elemento nel gruppo prodotto: $([u]_m, [v]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$.
Essendo tale gruppo ciclico, ogni suo elemento è multiplo di un suo generatore; quindi esiste $x \in \mathbb{Z}$ tale che

$$([u]_m, [v]_n) = x([1]_m, [1]_n) = ([x]_m, [x]_n)$$

cioè $x \equiv_m u$ e $x \equiv_n v$, come richiesto. □

Si può generalizzare il precedente risultato, considerando una s-upla $(m_1, \dots m_s)$, dove gli $m_i \in \mathbb{N}$ sono a due a due coprimi, cioè $(m_i, m_j) = 1$ se $i \neq j$.

Vale infatti il seguente teorema la cui dimostrazione, qui omessa, è una facile generalizzazione del caso precedente con due elementi.

Teorema 1.9. *(Teorema Cinese dei Resti in $\mathbb{Z}$). Siano $m_1, \dots, m_s$ numeri naturali a due a due coprimi. Allora:*

$$\forall\, u_1, \dots, u_s \in \mathbb{Z} \quad \exists\, x \in \mathbb{Z} \qquad \textit{tale che} \qquad x \equiv_{m_1} u_1, \dots,\ x \equiv_{m_s} u_s$$

cioè il sistema di equazioni modulari

$$\begin{cases} X \equiv_{m_1} u_1 \\ X \equiv_{m_2} u_2 \\ \quad \vdots \\ X \equiv_{m_s} u_s \end{cases}$$

ha soluzione in $\mathbb{Z}$. □

Tale risultato si può riformulare nel linguaggio dei gruppi come segue:

Teorema 1.10. *Siano $m_1, \dots, m_s \in \mathbb{N}$ a due a due coprimi. Allora il monomorfismo naturale di gruppi*

$$\mathbb{Z}_{m_1 \dots m_s} \quad \longrightarrow \quad \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_s}$$

definito da

$$[x]_{m_1 \dots m_s} \quad \mapsto \quad ([x]_{m_1}, [x]_{m_2}, \dots, [x]_{m_s})$$

è suriettivo e dunque è un isomorfismo di gruppi.

Dimostrazione. La verifica che tale applicazione sia omomorfismo di gruppi e iniettiva è lasciata per esercizio. La suriettività segue da 1.9. □

Esempio 1.10.1. Risolviamo il sistema di equazioni modulari

$$\begin{cases} X \equiv_{60} 38 \\ \\ X \equiv_{11} 7 \end{cases}$$

che sappiamo ammettere soluzione intera per il Teorema Cinese dei Resti, in quanto 60 e 11 sono coprimi. Se $x \in \mathbb{Z}$ è una soluzione, allora $x = 38 + 60a = 7 + 11b$ per opportuni interi a e b. Cerchiamo dunque le soluzioni intere dell'equazione

$$38 + 60a = 7 + 11b \qquad (*)$$

in modo elementare (ovviamente è sufficiente determinare una sola tra a e b...). Si può ad esempio ridurla "modulo 11", ottenendo $38 + 60a \equiv_{11} 7 \quad \Rightarrow \quad 5 + 5a \equiv_{11} 7 \quad \Rightarrow \quad 5a \equiv_{11} 2$. Quest'ultima equazione è facilmente risolubile in $\mathbb{Z}_{11}$: basta determinare l'inverso di $[5] \in \mathbb{Z}_{11}$ e moltiplicare ambo i membri per tale elemento. Un facile calcolo (e l'uso accorto di 0.12) mostra che $[5]^{-1} = [9] \in \mathbb{Z}_{11}$. Pertanto si ha $a \equiv_{11} 18 \equiv_{11} 7$. Scegliendo proprio $a = 7 \in \mathbb{Z}$, da $(*)$ si ottiene $b = 41$ e dunque $x = 38 + 60 \cdot 7 = 7 + 11 \cdot 41 = 458$, che è una delle soluzioni richieste.
La procedura effettuata e il Teorema 1.10 mostrano che *tutte* le soluzioni intere sono gli elementi della classe

$$[458]_{660} \in \mathbb{Z}_{660} \cong \mathbb{Z}_{60} \times \mathbb{Z}_{11}.$$

Denotiamo con $M_{n,m}(\mathbb{R})$ l'insieme delle matrici $n \times m$ ad elementi reali (dove n ed m sono interi positivi). È noto che $M_{n,m}(\mathbb{R})$ è un gruppo commutativo rispetto all'usuale somma di matrici.

In questo paragrafo ci occuperemo però di gruppi *moltiplicativi* di matrici, dove il prodotto è inteso essere quello usuale "righe per colonne". È chiaro che in tale ambito ha senso parlare solo di insiemi di matrici quadrate (cioè di sottoinsiemi di $M_{n,n}(\mathbb{R})$) affinché siano chiusi rispetto al prodotto.

Inoltre, richiedendo anche la proprietà di contenere l'inverso di ogni suo elemento, tali sottoinsiemi dovranno essere costituiti da matrici invertibili. Tale minima richiesta è sufficiente per costituire il primo (e più grande) dei *gruppi classici*.

Proposizione - Definizione 1.11. *Per ogni intero positivo n, l'insieme*

$$GL_n(\mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) \mid A \text{ è invertibile } \}$$

è un gruppo rispetto al prodotto, detto Gruppo Lineare Generale e denotato anche con GL_n.

Dimostrazione. Esercizio. □

Ricordiamo un fatto importante, trattato in altri corsi, riguardante il determinante di una matrice:

Teorema 1.12. *(Binet) Siano $A, B \in M_{n,n}(\mathbb{R})$. Allora* $\det(AB) = \det(A)\det(B)$. □

Osservazione 1.13. Tenendo presente che una matrice A è invertibile se e solo se $\det(A) \neq 0$, il risultato precedente implica che

$$\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$$

è un omomorfismo di gruppi *moltiplicativi*.

Esercizio 1.13.1. Provare che tale omomorfismo è suriettivo ma non iniettivo.

Nel cercare eventuali sottogruppi di GL_n, viene in aiuto il fatto che il nucleo di un omomorfismo è sempre un sottogruppo (normale). In particolare, il nucleo dell'omomorfismo "det" è un particolare e importante sottogruppo del gruppo lineare:

Definizione. Per ogni intero positivo n, il sottogruppo normale di $GL_n(\mathbb{R})$

$$SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1 \} = \ker(\det)$$

è detto *Gruppo Lineare Speciale* e denotato anche con SL_n.

Esercizio 1.13.2. Utilizzando l'esercizio precedente e il Primo Teorema di omomorfismo per gruppi, come si può descrivere (in prima approssimazione!) il quoziente GL_n/SL_n ? Come sono fatti i suoi elementi?

Un altro sottogruppo notevole di GL_n ha un'origine geometrica. È stato osservato in altri corsi che, posto $Aut(\mathbb{R}^n)$ il gruppo degli automorfismi dello spazio vettoriale $\mathbb{R}^n$ (cioè delle applicazioni lineari biunivoche di $\mathbb{R}^n$ in sé), si ha l'isomorfismo di gruppi $GL_n \cong Aut(\mathbb{R}^n)$ (una volta fissate due basi di $\mathbb{R}^n$).

Non è difficile mostrare che le matrici che corrispondono ad automorfismi che preservano il prodotto scalare di $\mathbb{R}^n$ sono tutte e sole quelle per cui l'inversa coincide con la trasposta. Si introduce dunque la seguente nozione:

Proposizione - Definizione 1.14. *Per ogni intero positivo n, l'insieme*

$$O_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) \mid A^{-1} = {}^tA \}$$

è un sottogruppo di $GL_n(\mathbb{R})$, detto Gruppo Lineare Ortogonale e denotato anche con O_n.

Dimostrazione. Lasciata al lettore (traccia: osservare che tale insieme è chiuso rispetto al prodotto e rispetto all'inverso). □

Osservazione 1.15. Se A è una matrice ortogonale, allora $\det(A^{-1}) = \det({}^tA)$. Dunque, per tale uguaglianza e per il teorema di Binet:

$$1 = \det(I_n) = \det(A\,A^{-1}) = \det(A)\,\det(A^{-1}) = \det(A)\,\det({}^tA) = \det(A)^2.$$

Pertanto $\det(A) = \pm 1$. Quindi le matrici ortogonali sono di due tipi: o "speciali" o con determinante -1.

Ricordiamo che l'intersezione di due sottogruppi è un sottogruppo. Pertanto l'insieme delle matrici ortogonali che sono speciali

$$SO_n(\mathbb{R}) := \{A \in O_n(\mathbb{R}) \mid \det(A) = 1\ \} = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$$

è un sottogruppo di $GL_n(\mathbb{R})$.

Definizione. Il sottogruppo $SO_n(\mathbb{R})$ di $GL_n(\mathbb{R})$ si dice *Gruppo Lineare Ortogonale Speciale.*

Il quadro dei gruppi classici introdotto finora è dunque

$$\begin{array}{ccc} SO_n & \subset & O_n \\ \cap & & \cap \\ SL_n & \subset & GL_n \end{array}$$

Esercizio 1.15.1.
- Provare che le precedenti inclusioni sono strette (almeno nel caso $n = 2$).
- Quali tra i sottogruppi precedenti sono normali nei gruppi che li contengono?

(Nel seguito, riferendoci a divisori e multipli di un numero naturale, intenderemo sempre interi positivi.)

Gli esempi di gruppi finiti visti finora (anche nei corsi precedenti) sono essenzialmente di due tipi: abeliani (i prototipi sono gli $\mathbb{Z}_n$ e loro prodotti) e non abeliani (l'esempio-base è il gruppo simmetrico $\mathcal{S}_n$). Per iniziare uno studio più approfondito, uno strumento efficace si rivela essere un'indagine sulle "sottostrutture": in questo caso sui sottogruppi di un gruppo dato.

Trattando di gruppi finiti, il primo e fondamentale invariante è l'ordine. Il risultato più significativo è infatti il teorema di Lagrange (0.8) che - ricordiamo - afferma che in un qualunque gruppo finito G vale:

$$\textit{comunque scelto un sottogruppo } H \textit{ di } G \quad \textit{allora} \quad o(H)|o(G).$$

È naturale chiedersi se vale il viceversa, cioè:

$$\textit{comunque scelto un intero } h \textit{ che divide } o(G) \quad \textit{allora} \quad \textit{esiste un sottogruppo } H \textit{ di ordine } h?$$

Vedremo che, per quanto la domanda sia semplice, la risposta non lo è: si presenta articolata, essendo in generale negativa. Tuttavia è affermativa in alcune categorie che dipendono o dal "tipo" di gruppo G o dal "tipo" di intero h che si sceglie tra i fattori di $o(G)$.

Una prima semplice classe in cui si ha la totale inversione del teorema di Lagrange è costituita dai gruppi ciclici. Vedremo subito dopo che si inserisce nel quadro più vasto dei gruppi abeliani.

Proposizione 1.16. *Sia G un gruppo ciclico di ordine n e sia m un divisore di n. Allora G possiede un sottogruppo di ordine m.*

Dimostrazione. Se x è un generatore di G allora n è il più piccolo intero positivo tale che $x^n = 1$. Essendo m un divisore di n, esiste t tale che $n = tm$. Consideriamo il sottogruppo $H := \langle x^t \rangle$ di G. Si verifica facilmente che $o(x^t) = m$ e quindi $o(H) = m$. □

Tale situazione si estende alla grande famiglia di gruppi in cui *vale l'inverso del teorema di Lagrange*: quella dei gruppi commutativi.

Teorema 1.17. *Sia G un gruppo finito abeliano di ordine n. Se m è un divisore di n, allora G ha un sottogruppo di ordine m.*

Per dimostrare questo risultato, utilizzeremo un teorema di Cauchy che è simile ma (apparentemente!) più debole e che si rivelerà utile anche nel caso non commutativo. Premettiamo una semplice nota.

Osservazione 1.18. Se $x \in G$ è un elemento di ordine t, allora il sottogruppo ciclico $\langle x \rangle$ ha ordine t.

Teorema 1.19. *(Teorema di Cauchy per gruppi abeliani) Sia G un gruppo finito abeliano di ordine n. Se p è un divisore primo di n, allora G ha un elemento, e quindi un sottogruppo, di ordine p.*

Dimostrazione. Procediamo per induzione su n. Se $n = 2$ il teorema è ovviamente vero.
Se $n > 2$ e n è primo, allora ogni elemento di G ha ordine n. Supponiamo dunque che n non sia primo e che il teorema sia vero per tutti i gruppi di ordine strettamente minore di n. Assumiamo per assurdo che nessun elemento di G abbia ordine p. Di conseguenza, nessun elemento ha per ordine un multiplo di p (segue facilmente da Proposizione 1.16). Pertanto, scelto un qualunque elemento $h \in G$, $h \neq 1_G$, il sottogruppo ciclico $H := \langle h \rangle$ ha ordine $o(H) = o(h)$ che non è multiplo di p. Ne consegue che $H \neq G$ e inoltre (dal teorema di Lagrange):

$$p \mid o(G), \;\; p \not| \, o(H) \quad \Rightarrow \quad p \mid o(G/H).$$

Quindi G/H è un gruppo non banale il cui ordine è diviso da p ed è strettamente minore di n. Per l'ipotesi induttiva, ammette un elemento di ordine p, che indichiamo con $[x]$. Questo significa che

$$[x]^p = 1_{G/H} \quad \Rightarrow \quad x^p \in H = \langle h \rangle \quad \Rightarrow \quad \exists\, r \in \mathbb{N} : \; x^p = h^r.$$

Poniamo $m := o(h)$ e $d := MCD(m, r)$. Determiniamo l'ordine dell'elemento $x^{m/d}$. Osserviamo anzitutto che tale elemento non è l'identità. Infatti se lo fosse, anche $[x^{m/d}] = 1_{G/H}$ e quindi $[x]^{m/d} = 1_{G/H}$. Ma $[x]$

ha ordine p, quindi necessariamente p dovrebbe dividere m/d e quindi $p|m$, contro l'ipotesi iniziale.
Calcoliamo ora la potenza p-esima di tale elemento:

$$\left(x^{m/d}\right)^p = (x^p)^{m/d} = (h^r)^{m/d} = (h^m)^{r/d} = 1_G$$

dove l'ultima uguaglianza segue da $h^m = 1_G$. Pertanto l'ordine di $x^{m/d}$ divide p, ma poiché p è primo coincide con p. □

Possiamo ora provare il teorema centrale sui gruppi abeliani finiti.

Dimostrazione di 1.17. Anche in questo caso si procede per induzione su n, osservando che il teorema è banalmente vero per $n = 2$ e per m primo, per il teorema di Cauchy.
Si assuma quindi $n \geq 2$ e si supponga il teorema vero per tutti i gruppi di ordine $< n$.
Sia p un divisore primo di m (che non è primo!). Dunque p divide n e quindi, per il teorema di Cauchy, G ha un sottogruppo H di ordine p.
Il gruppo quoziente G/H è ancora abeliano e ha ordine $n/p < n$. Inoltre m/p divide n/p, pertanto, per l'ipotesi induttiva, G/H ha un sottogruppo di ordine m/p. Denotiamo tale sottogruppo con K/H, dove $K \leq G$. Per il teorema di Lagrange

$$o(K/H) = o(K)/o(H) \quad \Rightarrow \quad m/p = o(K)/p \quad \Rightarrow \quad o(K) = m$$

e ciò conclude la dimostrazione. □

Il secondo ambito in cui *vale l'inverso del teorema di Lagrange* è relativo ai divisori *primi* (o in generale potenze di primi) dell'ordine del gruppo.

La dimostrazione del seguente fondamentale risultato è di tipo combinatorico; in letteratura sono disponibili altre dimostrazioni che utilizzano l'azione di un gruppo su un insieme o nozioni come centralizzante e normalizzante. Quella qui proposta non necessita di particolari prerequisiti: anche se piuttosto articolata è tuttavia elementare.

Ricordiamo solo che, dal calcolo combinatorio, per definizione di coefficiente binomiale, si ha che il numero dei sottoinsiemi di k elementi di un insieme di n elementi è

$$\binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!}.$$

Teorema 1.20. *(Primo Teorema di Sylow, 1872) Sia G un gruppo finito di ordine n. Se p^α è un divisore di n (dove p è primo e $\alpha \in \mathbb{N}$), allora G ha un sottogruppo di ordine p^α.*

Dimostrazione. Fissiamo anzitutto alcune notazioni.
Per ipotesi $n = p^\alpha r$, per un opportuno intero positivo r. Sia R la massima potenza di p che divide r, cioè

$$p^R \,|\, r \quad \text{ma} \quad p^{R+1} \nmid r.$$

Step 1. Consideriamo ora tutti i sottoinsiemi di G aventi p^α elementi e sia $\mathcal{A}$ l'insieme di tali sottoinsiemi. Come ricordato, la cardinalità di $\mathcal{A}$ è:

$$N := |\mathcal{A}| = \binom{n}{p^\alpha}.$$

Definiamo in $\mathcal{A}$ la seguente relazione

$$X \sim Y \iff \text{esiste } g \in G \text{ tale che } X = Yg$$

che risulta facilmente essere d'equivalenza. Consideriamo la partizione di $\mathcal{A}$ associata a tale relazione:

$$\mathcal{A} = A_1 \sqcup A_2 \sqcup \cdots \sqcup A_t \tag{$*$}$$

che è unione disgiunta delle t classi di equivalenza. Posto $a_i := |A_i|$, ovviamente

$$N = a_1 + a_2 + \cdots + a_t.$$

Step 2. Se p^{R+1} dividesse tutti gli a_i, allora per l'uguaglianza precedente dividerebbe N, contro il Lemma 1.21 (che proveremo in seguito). Dunque esiste un i_0 tale che $p^{R+1} \nmid a_{i_0}$. Per brevità omettiamo l'indice, ponendo $A := A_{i_0}$ e $a := a_{i_0}$. Poiché A è una delle classi di equivalenza della partizione $(*)$ secondo la precedente relazione d'equivalenza, esiste qualche $X \in \mathcal{A}$ per cui

$$A = [X] = \{Xg \ , \ g \in G\}.$$

Chiaramente gli elementi di tipo Xg non sono necessariamente distinti al variare di g in G. Consideriamo ad esempio quelli che coincidono con X e definiamo il seguente sottoinsieme di G:

$$H := \{g \in G \ , \ Xg = X\}.$$

Step 3. Proviamo ora che H è un sottogruppo di G e calcoliamo il suo ordine.
Ovviamente H è non vuoto in quanto $1_G \in H$. Inoltre, se $g, f \in H$ allora $Xg = X = Xf$, dunque $Xgf^{-1} = X$ e quindi $gf^{-1} \in H$. Pertanto $H \leq G$ e quindi, denotando con h l'ordine di H, per il teorema di Lagrange si ha $h|n$.
Si osservi che H serve anche a descrivere gli elementi di A; infatti, come osservato, $Xg = Xf$ se e solo se $gf^{-1} \in H$. Ne segue che

$$|A| = \frac{|G|}{|H|} \quad \Rightarrow \quad ah = n.$$

Mostriamo dapprima che p^α divide h. Si osservi anzitutto che p^R divide r per ipotesi, quindi essendo $n = p^\alpha r$ si ha che $p^{R+\alpha}$ divide n. Ma $n = ah$ e $p^{R+1} \nmid a$ come visto in Step 2. Questo implica che p^α divide h.
D'altra parte, fissato un elemento $x \in X$, l'applicazione

$$H \longrightarrow X \quad \text{definita da} \quad h \mapsto xh$$

è ben definita in quanto $xH \subseteq X$ (per definizione di H) ed è iniettiva perché il prodotto xh è quello di G, dove vale la Legge di cancellazione (dunque $xh_1 = xh_2 \Rightarrow h_1 = h_2$). Di conseguenza $|H| \leq |X|$, cioè $h \leq p^\alpha$. Pertanto

$$p^\alpha \,|\, h, \ \ h \leq p^\alpha \quad \Longrightarrow \quad h = p^\alpha.$$

In tal modo si è provato che H è un sottogruppo di G di ordine p^α, come richiesto. □

Resta da provare una proprietà combinatorica usata nella dimostrazione precedente. Utilizziamo le stesse notazioni: p denota un numero primo, $r, \alpha \in \mathbb{N}^*$ e si pone $N := \binom{p^\alpha r}{p^\alpha}$.

Lemma 1.21. *Sia R tale che $p^R \,|\, r$ e $p^{R+1} \nmid r$. Allora $p^{R+1} \nmid N$.*

Dimostrazione. È sufficiente mostrare che N ed r sono divisibili per la stessa potenza di p. Infatti $p^{R+1} \nmid r$ per ipotesi e quindi si avrebbe che $p^{R+1} \nmid N$.
Scriviamo esplicitamente N:

$$N = \binom{p^\alpha r}{p^\alpha} = \frac{p^\alpha r \cdot (p^\alpha r - 1) \cdots (p^\alpha r - p^\alpha + 1)}{p^\alpha!} = r \cdot \frac{(p^\alpha r - 1) \cdots (p^\alpha r - p^\alpha + 1)}{(p^\alpha - 1)!}.$$

A questo punto basta provare che il numeratore e il denominatore della precedente frazione sono divisibili per la stessa potenza di p. Si osservi che sia al numeratore che al denominatore ci sono $(p^\alpha - 1)$ fattori, ed esattamente

$$\text{numeratore} = \prod_{t=1}^{p^\alpha - 1} (p^\alpha r - t), \quad \text{denominatore} = \prod_{t=1}^{p^\alpha - 1} t.$$

Basta dunque provare che, per ogni $t = 1, \ldots, (p^\alpha - 1)$,

$$p^s \,|\, t \iff p^s \,|\, (p^\alpha r - t).$$

Osserviamo preliminarmente che tale equivalenza ha senso solo per $s < \alpha$, in quanto $t \leq p^\alpha - 1$.
"$\Rightarrow$" Sia s tale che $p^s \mid t$. Dunque $t = p^s M$ e quindi $p^\alpha r - t = p^\alpha r - p^s M = p^s(p^{\alpha-s} r - M)$. Essendo $\alpha - s > 0$ come osservato, si ottiene che $p^\alpha r - t = p^s K$, con $K \in \mathbb{N}$, come volevamo.
"$\Leftarrow$" Sia s tale che $p^s \mid (p^\alpha r - t)$. Dunque $p^\alpha r - t = p^s M'$ per un certo M' e quindi $t = p^\alpha r - p^s M' = p^s(p^{\alpha-s} r - M')$. Essendo $\alpha - s > 0$ come osservato, si ottiene che $t = p^s K'$, con $K' \in \mathbb{N}$, come volevamo. □

Dal I Teorema di Sylow discende immediatamente la seguente generalizzazione di 1.19.

Corollario 1.22. *(Teorema di Cauchy per gruppi finiti) Sia G un gruppo finito di ordine n. Se p è un divisore primo di n, allora G ha un sottogruppo, e quindi un elemento, di ordine p.* □

A questo punto è naturale introdurre le seguenti nozioni.

Definizione. Se p è un numero primo, un gruppo di ordine p^k (per qualche $k \in \mathbb{N}^*$) si dice *p–gruppo.*

Definizione. Se p è un numero primo e G è un gruppo finito, ogni suo sottogruppo $H \leq G$ che è un p-gruppo si dice *p–sottogruppo* di G.

Pertanto il I Teorema di Sylow afferma che, se G è un gruppo finito e $o(G) = p^\alpha r$, allora G ha un p-sottogruppo. Più precisamente, se $p \nmid r$, allora G ha p-sottogruppi di ordine

$$p, p^2, \ldots, p^\alpha$$

e nessuno di ordine maggiore. Quelli di ordine massimo p^α sono detti *p-sottogruppi di Sylow* o brevemente *p-Sylow.*

Enunciamo, senza dimostrare, gli altri due teoremi di Sylow.

Teorema 1.23. *(Secondo Teorema di Sylow) Sia G un gruppo finito e p un primo che divide $o(G)$. Allora*
i) ogni p-sottogruppo di G è contenuto in un p-Sylow;
ii) tutti i p-Sylow sono tra loro coniugati, cioè se H_1 e H_2 sono p-Sylow, allora esiste $g \in G$ tale che $gH_1g^{-1} = H_2$.

Teorema 1.24. *(Terzo Teorema di Sylow) Sia G un gruppo finito e p un primo tale che $o(G) = p^\alpha s$ con $\alpha \geq 1$ e $p \nmid s$. Posto N il numero dei p-Sylow di G, si ha:*
i) N divide s;
ii) $N \equiv 1 (\mathrm{mod}\, p)$.

Esempio 1.24.1. Sia G il gruppo simmetrico $\mathcal{S}_4$. Tenuto conto che $o(G) = 24 = 2^3 \cdot 3$, per quali p e quanti sono i p-sottogruppi di G?

Osservazione 1.25. Sia G un gruppo finito abeliano e p un primo che divide $o(G)$. Allora G ha un unico p-Sylow.

Capitolo 2 - Teoria degli anelli *

Facendo riferimento alle nozioni e ai risultati richiamati nel Capitolo 0, proseguiamo lo studio degli anelli con alcuni esempi significativi.

Esempio 2.1.1. In analogia con l'insieme $M^{n,n}(\mathbb{R})$ delle matrici $n \times n$ a entrate reali, dato un anello commutativo unitario A, si definisce l'insieme $M^{n,n}(A)$ delle matrici $n \times n$ a entrate in A.
Anch'esso può essere dotato di due operazioni di somma e prodotto (righe per colonne) come segue: per ogni $M = (m_{ij}), N = (n_{ij}) \in M^{n,n}(A)$ si definiscono

$$(M+N)_{ij} := m_{ij} + n_{ij}, \quad (MN)_{ij} := \sum_{k=1}^{n} m_{ik}\, n_{kj}.$$

Rispetto a tali operazioni, $M^{n,n}(A)$ è un anello unitario. Infatti è chiuso rispetto alle operazioni di somma e prodotto e sono verificate le seguenti proprietà:

i) $(M^{n,n}(A), +)$ è un gruppo abeliano;
ii) il prodotto è associativo;
iii) vale la proprietà distributiva del prodotto rispetto alla somma;
iv) la matrice identica I_n è l'elemento neutro del prodotto.

Vediamo ad esempio la dimostrazione di (*iii*).
Siano $M, N, P \in M^{n,n}(A)$, con $M = (m_{ij})$, $N = (n_{ij})$ e $P = (p_{ij})$. Con le operazioni definite prima si ottiene che

$$(MN)_{ij} := \sum_{k=1}^{n} m_{ik}\, n_{kj} \quad \text{e} \quad (MP)_{ij} := \sum_{k=1}^{n} m_{ik}\, p_{kj}.$$

da cui

$$(MN+MP)_{ij} = (MN)_{ij} + (MP)_{ij} = \sum_{k=1}^{n} m_{ik}\, n_{kj} + \sum_{k=1}^{n} m_{ik}\, p_{kj} = \sum_{k=1}^{n} (m_{ik}n_{kj} + m_{ik}p_{kj}).$$

D'altra parte

$$(M(N+P))_{ij} = \sum_{k=1}^{n} m_{ik}\, (N+P)_{kj} = \sum_{k=1}^{n} m_{ik}\, (n_{kj} + p_{kj}).$$

Pertanto, per la (corrispondente) proprietà distributiva del prodotto rispetto alla somma in A, si ottiene che $(MN+MP)_{ij} = (M(N+P))_{ij}$, per ogni $i, j = 1, \ldots, n$. Quindi le matrici $MN+MP$ e $M(N+P)$ coincidono.
Diamo un cenno della dimostrazione di (*iv*). La matrice identica

$$I_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

dove $1 = 1_A$ e $0 = 0_A$, si rappresenta sinteticamente con $I_n = (\delta_{ij})$, dove δ_{ij} è il *simbolo di Kronecker*.
Se $M = (m_{ij})$ è una qualunque matrice di $M^{n,n}(A)$ allora

$$(MI_n)_{ij} := \sum_{k=1}^{n} m_{ik}\, \delta_{kj} = m_{ij}.$$

Pertanto $MI_n = M$ e analogamente si prova che $I_n M = M$.
Quindi se A è un anello unitario anche $M^{n,n}(A)$ è unitario, con elemento neutro I_n. Invece $M^{n,n}(A)$ non è un anello commutativo nemmeno se lo è A.

* Versione 5.5.2017

Esempio 2.1.2. Un anello A che non sia commutativo ma per cui valga comunque $\mathcal{U}(\mathcal{A}) = \mathcal{A}^*$, si dice corpo. I *quaternioni di Hamilton* sono un esempio di corpo che non è un campo.

Definizione. *(Dedekind, 1871).* Si dice *campo numerico* un qualsiasi sottocampo di $\mathbb{C}$.

Esempio 2.1.3. L'insieme

$$\mathbb{Q}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$$

è un anello commutativo rispetto alle medesime operazioni di $\mathbb{C}$ (dunque sottoanello di $\mathbb{C}$) ed è anche un campo. È dunque un campo numerico.

Esempio 2.1.4. L'insieme degli *interi di Gauss*

$$\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$$

è un anello commutativo rispetto alle medesime operazioni di somma e prodotto di $\mathbb{C}$ (dunque sottoanello di $\mathbb{C}$), ma non è un campo.

Operazioni tra ideali - Generatori

Vediamo come determinare altri ideali di un anello a partire da due ideali, attraverso le "operazioni" di intersezione, somma, prodotto. Come accade per i sottogruppi o per i sottospazi vettoriali, l'intersezione di due sottostrutture è ancora una sottostruttura della categoria che si sta considerando, ma l'unione no. Anche per gli ideali succede questo: si introduce dunque una nozione "sostitutiva" all'unione, quella di "somma".

Proposizione-Definizione 2.2. *Dati I, J ideali di un anello commutativo A allora:*
(i) $I \cap J$ *è un ideale di* A*;*
(ii) $I + J := \{x + y \mid x \in I, y \in J\}$ *è un ideale di* A*, detto ideale somma di* I *e* J*;*
(iii) $IJ := \{\sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{N}, x_i \in I, y_i \in J\}$ *è un ideale di* A*, detto ideale prodotto di* I *e* J*.*

Dimostrazione.
(i) Per definizione di ideale, devo verificare che $\forall x, y \in I \cap J$ e $\forall z \in A$ si ha che: $x - y \in I \cap J$ e $xz \in I \cap J$. Poiché $x, y \in I$, essendo I un ideale per ipotesi, allora $x - y \in I$; analogamente $x - y \in J$. Quindi $x - y \in I \cap J$. Inoltre, se $z \in A$ e $x \in I$ ed essendo I un ideale allora $xz \in I$; analogamente $xz \in J$. Quindi $xz \in I \cap J$; pertanto $I \cap J$ è un ideale di A.
(ii) Per definizione di ideale, devo verificare che $\forall a, b \in I + J$ e $\forall c \in$A valgono: $a - b \in I + J$ e $ac \in I + J$. Per ipotesi: $a = x + y$ e $b = x' + y'$, per opportuni $x, x' \in I$ e $y, y' \in J$. Quindi, applicando le proprietà commutativa e associativa della somma in A e la definizione di opposto, si ottiene

$$a - b = (x + y) - (x' + y') = x + y - x' - y' = (x - x') + (y - y') \in I + J$$

in quanto, essendo I un ideale, $x - x' \in I$ e analogamente $y - y' \in J$.
Per verificare la proprietà di assorbimento, si utilizzano la proprietà distributiva del prodotto rispetto alla somma e le proprietà di assorbimento relative agli ideali I e J ottenendo

$$(x + y)c = xc + yc \in I + J.$$

Pertanto $I + J$ è un ideale di A.
(iii) Ancora per la definizione di ideale, basta verificare che: $\forall a, b \in IJ$, $\forall c \in A$ valgono: $a - b \in IJ$ e $ac \in IJ$. Poiché

$$a = \sum_{i=1}^{n} x_i y_i \ , \quad b = \sum_{j=1}^{m} x'_j y'_j$$

per opportuni $n, m \in \mathbb{N}, x_i, x'_i \in I, y_i, y'_i \in J$, si ottiene immediatamente che $a - b \in IJ$.
Per verificare la proprietà di assorbimento si utilizzano le proprietà distributiva e associativa del prodotto nell'anello A:

$$ac = \left(\sum_{i=1}^{n} x_i y_i\right) \cdot c = \sum_{i=1}^{n} x_i (y_i c).$$

Ma per la proprietà di assorbimento relativa a J si ha che $y_i c \in J$ per ogni i e dunque $ac \in IJ$. □

Osservazione 2.3. Se I e J sono due ideali di A, allora $IJ \subseteq I \cap J$. Infatti ogni espressione del tipo $\sum_{i=1}^{n} x_i y_i$, con $x_i \in I$ e $y_i \in J$, per ogni i, appartiene a I per la proprietà di assorbimento relativa ad I e in quanto I è chiuso rispetto alla somma. Analogamente appartiene a J.

Ricordando il simbolo (S) introdotto per denotare l'ideale generato da un insieme S (vedi 0.35, Cap. 0), si provano facilmente le seguenti proprietà.

Proposizione 2.4. *Se I e J sono ideali di un anello A, allora:*
i) $I + J = (I \cup J)$;
ii) *se* $I = (S)$ *e* $J = (T)$ *allora* $I + J = (S \cup T)$ *e* $IJ = (st \mid s \in S, t \in T)$;
iii) *se I e J sono finitamente generati allora gli ideali $I + J$ e IJ sono anche'essi finitamente generati;*
iv) *se* $I = (x)$ *e* $J = (y)$ *sono ideali principali allora* $IJ = (xy)$ *è principale.*

Dimostrazione.
i) Si osservi che, per definizione, $(I \cup J) = \{\sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}, a_i \in A, x_i \in I \cup J\}$.
"$\subseteq$" Se $x \in I + J$, allora esistono $i \in I$ e $j \in J$ tali che $x = i + j$ dunque $x \in (I \cup J)$.
"$\supseteq$" Se $x \in (I \cup J)$, come osservato x è del tipo $\sum_{i=1}^{n} a_i x_i$, con $x_i \in I \cup J$. Non è restrittivo supporre che (a meno di un cambio di nomi degli indici) siano $x_1, \ldots, x_r \in I$ e $x_{r+1}, \ldots, x_n \in J$ (eventualmente alcuni possono appartenere a entrambi gli ideali). Dunque

$$x = \sum_{i=1}^{n} a_i x_i = \left(\sum_{i=1}^{r} a_i x_i \right) + \left(\sum_{i=r+1}^{n} a_i x_i \right)$$

e chiaramente il primo addendo appartiene a I e il secondo a J, quindi $x \in I + J$.
ii) Per il punto precedente, vale $I + J = (I \cup J) = ((S) \cup (T))$. Inoltre, per 0.36, $S \subseteq (S)$ e $T \subseteq (T)$. Dunque si ha immediatamente che $(S \cup T) \subseteq ((S) \cup (T))$. Resta da provare l'altra inclusione.
Se $x \in ((S) \cup (T))$ allora tale elemento è del tipo $x = \sum_{i=1}^{n} a_i x_i$, con $a_i \in A, x_i \in (S) \cup (T)$ .....
iii) Segue immediatamente da (ii).
iv) Segue immediatamente da (ii). □

Divisibilità e Massimo Comun Divisore in $\mathbb{Z}$

Richiamiamo alcune nozioni note e fissiamo le notazioni. Se $a, b, c \in \mathbb{Z}$ e $a = bc$ diremo, equivalentemente, che a è un *multiplo* di b (e anche di c) o che b *divide* a (e anche che c *divide* a) e scriveremo $b|a$ (e $c|a$).

Definizione. Siano $a, b \in \mathbb{Z}$; diciamo che un intero $d \in \mathbb{Z}$ è un *massimo comun divisore* di a e b se verifica le seguenti proprietà:
1. $d|a$ e $d|b$;
2. per ogni $e \in \mathbb{Z}$ tale che $e|a$ ed $e|b$, allora $e|d$.

Ricordiamo che, per 0.47, Cap. 0, $\mathbb{Z}$ è un dominio a ideali principali. Quindi, comunque scelti $a, b \in \mathbb{Z}$, l'ideale (a, b) è principale, cioè del tipo (d), per un opportuno $d \in \mathbb{Z}$.

Proposizione 2.5. *Siano $a, b, d \in \mathbb{Z}$. Sono fatti equivalenti:*
i) $(a, b) = (d)$;
ii) *d è un massimo comun divisore di a e b.*

Dimostrazione.
i) $\Rightarrow$ *ii)* Se $(a, b) = (d)$ allora d è un massimo comun divisore di a e b. Infatti a e b appartengono a (d) dunque sono entrambi multipli di d. Inoltre, se e divide a e b, allora $a = eh$ e $b = ek$ per opportuni $h, k \in \mathbb{Z}$. Poiché $d \in (a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$ allora esistono necessariamente $s, t \in \mathbb{Z}$ tali che $d = as + bt$. Quindi $d = ehs + ekt = e(hs + kt)$ e dunque e divide d.
ii) $\Rightarrow$ *i)* Per ipotesi $d|a$ e $d|b$; dunque a e b appartengono a (d), quindi $(a, b) \subseteq (d)$. D'altro canto, per l'implicazione precedente (a, b) è un ideale principale generato da un massimo comun divisore di a e b. Sia esso e; si avrebbe dunque $(a, b) = (e) \subseteq (d)$, cioè $d|e$. Ma e divide d per definizione di massimo comun divisore; pertanto $e = \pm d$ e, chiaramente, $(e) = (d)$, come volevamo. □

Nella proposizione precedente si è visto che, se d è un massimo comun divisore di a e b, esistono $s, t \in \mathbb{Z}$ tali che $d = as + bt$. Ma il ragionamento fatto prova soltanto che tali interi esistono. Vediamo ora un procedimento costruttivo per determinarli.

Teorema 2.6. *(Lemma di Bézout). Se $a, b \in \mathbb{Z}$ allora esiste un massimo comun divisore d di a e b. Inoltre esistono $s, t \in \mathbb{Z}$, detti coefficienti di Bézout, tali che*

$$as + bt = d.$$

Tale uguaglianza è detta Identità di Bézout.

Dimostrazione. Se $a = 0$ allora b è un massimo comun divisore di a e b. Sia allora $a \neq 0$ e si consideri l'insieme

$$X = \{ax + by > 0 \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{N}.$$

Si osservi anzitutto che X è non vuoto, infatti se $a > 0$ ponendo $x = 1, y = 0$ si ottiene un'espressione positiva; se invece $a < 0$ ponendo $x = -1, y = 0$ si ottiene un'espressione positiva.
Pertanto X ammette minimo, che denotiamo con d, e siano $s, t \in \mathbb{Z}$ tali che

$$as + bt = d. \qquad (*)$$

Utilizzando il Teorema della divisione euclidea (0.45), si può dividere a per d, in quanto $d \neq 0$, ottenendo $a = dq + r$ per opportuni q, r, con $0 \leq r < d$. Sostituendo in tale uguaglianza l'espressione di d in $(*)$, si ottiene

$$r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq)$$

e quindi r ha la forma di un elemento di X. Chiaramente, se $r > 0$, necessariamente $r \in X$, contraddicendo il fatto che $r < d$ e che d è il minimo di X.
Dunque deve essere $r = 0$ e quindi $a = dq$ ossia d divide a. Analogamente, scambiando i ruoli di a e b si prova che d divide b.
Per concludere la dimostrazione, resta da provare che per ogni $e \in \mathbb{Z}$ tale che $e|a, e|b$ allora $e|d$.
Per ipotesi $a = ke$ e $b = he$ per opportuni k, h; dunque, sostituendo tali espressioni in $(*)$ si ottiene $ske + the = d$ ossia $(sk + th)e = d$, cioè la tesi. □

Osservazione 2.7. Siano $a, b \in \mathbb{Z}^*$; se d è un massimo comun divisore di a e b, anche $-d$ lo è. È chiaro che non ce ne sono altri. Pertanto due numeri interi hanno esattamente due massimi comuni divisori, uno l'opposto dell'altro. In particolare uno solo positivo.

Definizione. Siano $a, b \in \mathbb{Z}^*$. Il loro unico massimo comun divisore positivo si dice *il Massimo Comune Divisore* di a e b e si denota con $MCD(a, b)$ o anche con (a, b).

Il risultato che segue risponde alla naturale domanda "esiste un metodo per determinare il MCD di due interi che non sia lo scomporre entrambi in fattori primi?". La risposta è affermativa.

Proposizione 2.8. *(Algoritmo delle divisioni successive). Siano $a, b \in \mathbb{Z}^*$. Considerando la divisione euclidea di a per b e, successivamente, di b per il resto e poi di ogni resto per il successivo si ottiene la sequenza di uguaglianze:*

1. $a = bq + r_1$, *con* $0 \leq r_1 < |b|$
2. $b = r_1 q_1 + r_2$, *con* $0 \leq r_2 < r_1$
3. $r_1 = r_2 q_2 + r_3$, *con* $0 \leq r_3 < r_2$

   ...

i. $r_{i-2} = r_{i-1} q_{i-1} + r_i$, *con* $0 \leq r_i < r_{i-1}$.

Allora tale sequenza è finita e, posto n il numero di tali divisioni successive, si ha che $r_n = 0$ e $r_{n-1} = (a, b)$.

Dimostrazione. Per costruzione si determina la successione strettamente decrescente dei resti:

$$0 \leq \ldots < r_i < r_{i-1} < \ldots < r_1 < |b|$$

Per il principio del minimo in $\mathbb{N}$, l'insieme dei resti ammette minimo e quindi esiste $n \in \mathbb{N}$ tale che $r_n = 0$. Dunque l'uguaglianza n-esima è $r_{n-2} = r_{n-1} q_{n-1}$. In particolare r_{n-1} divide r_{n-2}.
Considerando l'uguaglianza $(n-1)$-esima $r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$ è chiaro che r_{n-1} divide anche r_{n-3}. Iterando il ragionamento, si prova che r_{n-1} divide a e b. In modo simile si prova che r_{n-1} è il massimo comun divisore di a e b. □

Si osservi che la procedura descritta in 2.8 consente di determinare, in modo costruttivo, i coefficienti e quindi l'identità di Bézout relativi al MCD determinato.

Esempio 2.8.1. Calcoliamo $MCD(24, 110)$. Con l'algoritmo delle divisioni successive si ha:

1. $a = bq + r_1$ $\quad 110 = 24 \cdot 4 + 14$
2. $b = r_1q_1 + r_2$ $\quad 24 = 14 \cdot 1 + 10$
3. $r_1 = r_2q_2 + r_3$ $\quad 14 = 10 \cdot 1 + 4$
4. $r_2 = r_3q_3 + r_4$ $\quad 10 = 4 \cdot 2 + 2$
5. $r_3 = r_4q_4 + r_5$ $\quad 4 = 2 \cdot 2$

Dunque $r_5 = 0$ e $r_4 = 2$ è il $MCD(24, 110)$. Inoltre dalla quarta uguaglianza e, risalendo, dalle precedenti si ottiene:

$$2 = 10 - 4 \cdot 2 = 10 - (14 - 10 \cdot 1) \cdot 2 = 3 \cdot 10 - 2 \cdot 14 = 3 \cdot (24 - 14 \cdot 1) - 2 \cdot 14 = 3 \cdot 24 - 5 \cdot 14$$

e infine $2 = 3 \cdot 24 - 5(110 - 24 \cdot 4)$. Quindi l'identità di Bézout corrispondente è

$$2 = 23 \cdot 24 - 5 \cdot 110.$$

Esercizio 2.8.2. Calcolare $MCD(833, 2431)$ e $MCD(833, 997)$.

Lemma 2.9. *Sia $[a]$ un elemento non nullo di $\mathbb{Z}_n$. Allora*

$$[a] \text{ è invertibile} \quad \Leftrightarrow \quad (a, n) = 1.$$

Dimostrazione. " $\Leftarrow$ " Si può supporre $a < n$; dunque per il Teorema di Eulero (1.3), si ha $a^{\phi(n)} \equiv_n 1$, cioè $[a]^{\phi(n)} = [1]$ in $\mathbb{Z}^n$. Da cui segue che $[a]^{\phi(n)-1}[a] = [1]$ e quindi $[a]^{\phi(n)-1} = [a]^{-1}$.
"$\Rightarrow$ " Supponiamo che $(a, n) = d \neq 1$, dunque $d|a$ e $d|n$ e quindi $a = da'$ e $n = dn'$.
Poiché $d \neq 1$ allora $[n'] \neq [0]$ ma si hanno le uguaglianze in $\mathbb{Z}^n$:

$$[a][n'] = [an'] = [a'dn'] = [a'][n] = [0]$$

quindi $[a]$ risulta essere uno zero divisore e quindi non invertibile per 0.28. □

Si ricordi che, nel Capitolo 1, si è definita l'applicazione $\pi' : \Phi_n \to \mathbb{Z}_n$ come la restrizione della proiezione canonica da $\mathbb{Z}$ a $\mathbb{Z}_n$ e che $\mathrm{Im}(\pi')$ è un gruppo rispetto all'operazione di prodotto di $\mathbb{Z}_n$ (vedi 1.2). È immediato osservare che π' è iniettiva e dunque biiettiva sull'immagine. Avendo definito $\phi(n) = \#\Phi_n$, dal Lemma precedente si ha immediatamente il seguente

Corollario 2.10. *Per ogni $n \in \mathbb{N}^*$, si ha $\phi(n) = \#(\mathcal{U}(\mathbb{Z}_n))$.* □

Proposizione 2.11. *Per ogni $n \in \mathbb{N}^*$ sono equivalenti:*

i) l'anello $\mathbb{Z}_n$ è un campo
ii) n è un numero primo,
iii) l'anello $\mathbb{Z}_n$ è un dominio di integrità.

Dimostrazione. $(i) \Leftrightarrow (ii)$ Per definizione $\mathbb{Z}_n$ è un campo se e solo se $\#(\mathcal{U}(\mathbb{Z}_n)) = n - 1$. Per il precedente Corollario 2.10, ciò equivale a $\phi(n) = n - 1$ e questo vale se e solo se n è un numero primo.
$(i) \Rightarrow (iii)$ Immediato da 0.28.
$(iii) \Rightarrow (ii)$ Supponiamo che n non sia primo; dunque esistono $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}^*$ tali che $n = ab$. Quindi $[0] = [n] = [ab] = [a][b]$. D'altra parte $[a] \neq [0] \neq [b]$. Ne segue che sia $[a]$ che $[b]$ sono zero divisori: assurdo poiché $\mathcal{ZD}(\mathbb{Z}_n) = \emptyset$ per ipotesi. □

D'ora in poi, salvo altre specificazioni, A denoterà un anello commutativo unitario.

In analogia con quanto visto in $\mathbb{Z}$, introduciamo le seguenti nozioni.

Definizione. Dati $a, b \in A$, si dice che b *divide* a (oppure che b è *divisore* di a oppure che b è un *fattore* di a oppure che a è *multiplo* di b) se esiste $q \in A$ tale che $a = bq$. Si scrive $b|a$.

In $\mathbb{Z}$, ad esempio, 3 divide 6, ma 5 non divide 6. Mentre in $\mathbb{Q}$ anche 5 divide 6, infatti $\frac{6}{5} \in \mathbb{Q}$ e $6 = 5 \cdot \frac{6}{5}$.

Osservazione 2.12. Se A è un anello unitario allora i divisori di 1_A sono tutti e soli gli elementi di $\mathcal{U}(A)$. Inoltre lo zero divide solo se stesso, ma è diviso da tutti.

Vediamo, nei seguenti esempi, la divisibilità in $\mathbb{Z}$.

Esempio 2.12.1. In $\mathbb{Z}$ vale il teorema della divisione Euclidea (0.45), dunque presi $a, b \in \mathbb{Z}^*$ esistono e sono unici due interi q ed r tali che $a = bq + r$ e $0 \leq r < |b|$. In tale contesto, $b \mid a \iff r = 0$. Infatti:
"$\Leftarrow$" se $r = 0$ si ha ovviamente che $a = bq$ e quindi $b \mid a$.
"$\Rightarrow$" Viceversa, se esiste $n \in \mathbb{Z}$ tale che $a = nb$, allora usando l'unicità di q ed r, deve essere $q = n$ e $r = 0$.

Esempio 2.12.2. In $\mathbb{Z}$ dividiamo 16 e -16 per 5 e -5 in tutti i modi possibili, ricordando che $r <| b |$.
- -) $16 = 5 \cdot 3 + 1$, quindi $q = 3$ e $r = 1$;
- -) $16 = (-5)(-3) + 1$, quindi $q = -3$ e $r = 1$;
- -) $-16 = 5(-4) + 4$, quindi $q = -4$ e $r = 4$;
- -) $-16 = (-5)4 + 4$, quindi $q = 4$ e $r = 4$.

Osserviamo che in tutti e quattro i casi si ha che $0 < r <| b |$.

Definizione. Siano $a, b \in A^*$ tali che $b|a$ e $a|b$; allora a e b si dicono *associati*.

Ad esempio in $\mathbb{Z}$ i numeri 3 e -3 sono associati, in quanto $(-3)|3$ e $3|(-3)$. Infatti $3 = (-3)(-1)$ e $-3 = 3(-1)$. Si osservi che -1 è un elemento invertibile di $\mathbb{Z}$. La prossima proposizione mostra che questo è un fatto che vale in generale.

Lemma 2.13. *Comunque scelti $a \in A^*$ e $u \in \mathcal{U}(A)$, gli elementi a e ua sono associati.*

Dimostrazione. Sia $b = ua$; chiaramente a divide b. Inoltre u è invertibile, dunque esiste $u^{-1} \in A$. Moltiplicando entrambi i membri dell'uguaglianza per u^{-1}, si ottiene $u^{-1}b = a$. Dunque anche b divide a. □

Lemma 2.14. *Sia A un dominio. Se $a, b \in A$ sono associati allora esiste $u \in \mathcal{U}(A)$ tale che $b = au$.*

Dimostrazione. Per ipotesi esistono $q, q' \in A$ tali che $a = qb$ e $b = q'a$. Componendo le due uguaglianze, si ottiene che $a = (q'a)q = aq'q$ in quanto A è commutativo. Da cui si ha

$$0_A = a - aq'q = a(1_A - qq')$$

Essendo A un dominio, si ha $1_A - qq' = 0_A$ quindi $qq' = 1_A$. Pertanto q è invertibile in A con inverso q'. □

Da 2.13 e 2.14 segue immediatamente la seguente caratterizzazione di elementi associati in un dominio d'integrità.

Proposizione 2.15. *Sia A un dominio d'integrità e siano $a, b \in A$. Allora*

$$a, b \text{ sono associati} \Leftrightarrow \text{esiste } u \in \mathcal{U}(A) \text{ tale che } b = au.$$

□

Osservazione 2.16. Sono lasciate al lettore le verifiche dei seguenti fatti.
1) La proprietà di essere associati è simmetrica, cioè y è associato a $x \Leftrightarrow x$ è associato a y.
2) Un elemento x è associato ad $y \Leftrightarrow (x) = (y)$.
3) Ogni elemento x di A è diviso da tutti gli elementi invertibili di A ($x = 1_A x = uu^{-1}x$) e dagli associati di x ($y = ux \Leftrightarrow x = u^{-1}y$)
4) Se A è un campo e $x \in A^*$ allora i suoi divisori sono tutti gli elementi non nulli, infatti $\mathcal{U}(A) = A^*$.

Definizione. Un divisore di x non invertibile e non associato si dice *divisore proprio*.

Ad esempio: $5 \in \mathbb{Z}$ ha per divisori 1, -1 (invertibili), 5, -5 (associati). Quindi non ha divisori propri. Mentre $6 \in \mathbb{Z}$ ha per divisori 1, -1, 6, -6, 2, -2, 3, -3. Quindi 2, -2, 3, -3 sono divisori propri.

In un campo ogni elemento non nullo non ha divisori propri.

Caratteristica di un anello

Se A è un anello unitario e $m \in \mathbb{N}^*$, allora $m1_A$ denota l'elemento $1_A + \cdots + 1_A$, somma di m addendi.

Definizione. Sia A un anello unitario; se l'insieme $\{m \in \mathbb{N}^* |\ m1_A = 0_A\}$ è non vuoto, il suo minimo n si dice *caratteristica di* A e si scrive $ch(A) = n$. Se invece tale insieme è vuoto, si pone $ch(A) = 0$.

Esempi di anelli di caratteristica 0 sono $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, mentre $ch(\mathbb{Z}_n) = n$, $ch(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$, $ch(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$.

Proposizione 2.17. *Se A è un anello unitario finito, allora $ch(A) > 0$.*

Dimostrazione. Si consideri l'insieme $X = \{m1_A | m \in \mathbb{N}^*\}$. Poiché $X \subseteq A$ e A è un anello finito, anche X è finito; allora esistono $p, q \in \mathbb{N}^*$ tali che $p1_A = q1_A$ e si può supporre $p > q$. Dato che A è un anello, esiste l'opposto di $q1_A$, pertanto l'uguaglianza precedente implica $(p-q)1_A = 0_A$, con $p - q \in \mathbb{N}^*$ e quindi $ch(A) > 0$. □

È naturale chiedersi se vale il viceversa. La risposta è negativa e vedremo in seguito esempi di anelli infiniti ma con caratteristica positiva. Diamo ora un'importante caratterizzazione della nozione ora introdotta.

Proposizione 2.18. *Sia A un anello unitario; allora l'applicazione*

$$f : \mathbb{Z} \longrightarrow A \quad \text{definita da} \quad n \mapsto n1_A$$

è un omomorfismo di anelli unitari, il cui nucleo è $\ker(f) = (n)$*, dove $n = ch(A)$.*
In particolare f è iniettiva se e solo se $ch(A) = 0$.

Dimostrazione. Proviamo anzitutto che f è un omomorfismo di anelli, cioè che f rispetta la somma e il prodotto. Infatti per ogni $n, m \in \mathbb{Z}$ si ha:

$$f(n +_{\mathbb{Z}} m) = 1_A(n +_{\mathbb{Z}} m) = 1_A n +_A 1_A m = f(n) +_A f(m)$$

e anche

$$f(n \cdot_{\mathbb{Z}} m) = 1_A(n \cdot_{\mathbb{Z}} m) = 1_A n \cdot_A 1_A m = f(n) \cdot_A f(m)$$

Inoltre $f(1_{\mathbb{Z}}) = 1_A$ per definizione, quindi f è un omomorfismo di anelli unitari.
Ricordiamo che $\ker(f)$ è un ideale di $\mathbb{Z}$, che è un PID; pertanto esiste $n \in \mathbb{N}$ (possiamo sempre scegliere il generatore non negativo) tale che $\ker(f) = (n)$. Questo implica che $f(n) = 0_A$. Bisogna distinguere due casi: se $n > 0$, si ha che $n1_A = 0_A$ e quindi A ha caratteristica positiva m, con $m \leq n$. In particolare $m1_A = 0_A$ e quindi $m \in \ker(f)$. Dunque $m \in (n)$, cioè n divide m. Ma questo implica $m = n$.
Se invece $\ker(f) = (0_{\mathbb{Z}})$, allora f è iniettiva e quindi per ogni $n \neq 0_{\mathbb{Z}}$ si ha: $n1_A = f(n) \neq f(0_{\mathbb{Z}}) = 0_A$. Pertanto $ch(A) = 0$.
L'ultima affermazione segue facilmente e viene lasciata al lettore. □

Definizione. Con le notazioni precedenti, l'immagine di f è un sottoanello di A, detto *sottoanello fondamentale* di A e denotato con $F_a(A)$.

Con tale nozione si può riformulare quanto visto sopra.

Proposizione 2.19. *Sia A un anello unitario; allora*
a) $ch(A) = 0$ se e solo se $F_a(A) \cong \mathbb{Z}$;
b) $ch(A) = n$ se e solo se $F_a(A) \cong \mathbb{Z}_n$.

Dimostrazione. Si osservi dapprima che, per il Primo Teorema di omomorfismi di anelli, f si può scrivere come $f_1 o\ \pi$, dove $\pi : \mathbb{Z} \to \mathbb{Z}/\ker(f)$ è la proiezione canonica sul quoziente ed $f_1 : \mathbb{Z}/\ker(f) \to A$ è un monomorfismo di anelli. Pertanto la sua restrizione all'immagine

$$f_1 : \mathbb{Z}/\ker(f) \to \mathrm{Im}(f_1) = \mathrm{Im}(f) = F_a(A)$$

è un isomorfismo. La tesi segue immediatamente da 2.18. □

Proposizione 2.20. *Sia A un dominio; allora o $ch(A) = 0$ o $ch(A) = p$, dove p è un numero primo.*

Dimostrazione. Con le notazioni di 2.18 e 2.19, se $ch(A) \neq 0$, allora il sottoanello fondamentale di A è $F_a(A) \cong \mathbb{Z}_n$. Poiché A è integro, lo è anche $F_a(A)$; pertanto $\mathbb{Z}_n$ è integro, quindi n è primo. □

Osservazione 2.21. Se A è un dominio allora $Q(A)$ ha la stessa caratteristica di A. Infatti è immediato provare che l'immersione canonica $i : A \to Q(A)$ induce l'isomorfismo $i : F_a(A) \to F_a(Q(A))$.

In quanto segue sia A un anello commutativo e unitario.

Definizione. Un ideale M di A ($M \neq A$) si dice *massimale* se non esiste un ideale I di A tale che $M \subsetneq I \subsetneq A$.

Definizione. Un ideale P di A si dice *primo* se per ogni $x, y \in A$, se $xy \in P$ allora $x \in P$ oppure $y \in P$.

Osservazione 2.22. È immediato osservare che l'ideale (0_A) è primo se e solo se A è un dominio.

Esempio 2.22.1. Nell'anello $\mathbb{Z}$ l'ideale nullo è primo. In ogni campo l'ideale nullo è primo.

Non è sempre facile provare che un ideale sia primo o massimale. Ma innanzitutto vogliamo provare l'esistenza di ideali massimali in ogni anello. A tale scopo ricordiamo un importante risultato della Logica matematica.

Teorema 2.23. *(Lemma di Zorn). Sia S un insieme non vuoto e parzialmente ordinato. Se ogni sottoinsieme totalmente ordinato di S ha un maggiorante, allora S ha un elemento massimale.* □

Teorema 2.24. *(Lemma di Krull). Sia I un ideale di A, con $I \neq A$. Allora esiste un ideale massimale M che contiene I.*

Dimostrazione. Sia $S = \{H \text{ ideale proprio di } A \mid I \subseteq H\}$. Si osservi che S è un insieme parzialmente ordinato rispetto all'inclusione tra insiemi ed è non vuoto, poiché $I \in S$.
Sia $\{J_\lambda\}_{\lambda\in\Lambda} \subseteq S$ un insieme totalmente ordinato, con J_λ ideale di A, per ogni $\lambda \in \Lambda$. Si consideri

$$J := \bigcup_{\lambda\in\Lambda} J_\lambda.$$

Non è difficile provare che J è un ideale di A. Inoltre J è maggiorante, in S, per l'insieme $\{J_\lambda\}_{\lambda\in\Lambda}$.
Infatti, $I \subseteq J$ e $J \neq A$ (dunque $J \in S$); inoltre $J_\lambda \subseteq J$, per ogni $\lambda \in \Lambda$ (dunque J è maggiorante).
Allora, per il Lemma di Zorn, S ha un elemento massimale che indichiamo con M. Pertanto tale M è un ideale proprio di A e contiene I.
Resta da provare che M è un ideale massimale. Se ci fosse un ideale K di A tale che $M \subset K \subset A$ allora $K \in S$, il che è un assurdo poiché M è elemento massimale di S. □

Il seguente risultato individua un legame importante tra le nozioni di ideale primo e di ideale massimale.

Teorema 2.25. *Ogni ideale massimale è primo.*

Dimostrazione. Sia M un ideale massimale di un anello A e siano $x, y \in A$ tali che $xy \in M$. Si supponga $x \notin M$ e si consideri l'ideale $M + (x)$. Si osservi che $M + (x) \supsetneq M$, perché se fossero uguali, si avrebbe $(x) \subseteq M$, ma ciò è impossibile dato che $x \notin M$. Ma M è un ideale massimale, dunque necessariamente $M + (x) = A$.
Osserviamo che $1_A \in A = M + (x)$, dunque esistono $m \in M$, $\alpha \in A$ tali che $1_A = m + \alpha x$. Moltiplicando ambo i membri per y, si ottiene $y = my + \alpha xy$.
Si noti che $my \in M$, perché M è un ideale e $m \in M$. D'altra parte $xy \in M$ per ipotesi, dunque per la proprietà di assorbimento, anche $\alpha xy \in M$.
Poiché M è un ideale, e dunque chiuso rispetto alla somma, ne segue che $y = my + \alpha xy \in M$. Quindi M è un ideale primo. □

Proposizione 2.26. *Sia A un anello unitario e sia I un ideale proprio di A. Allora:*
i) I è un ideale massimale di $A \iff A/I$ è un campo
ii) I è un ideale primo di $A \iff A/I$ è un dominio

Dimostrazione.
i) Per 0.32, A/I è un campo se e solo se ha come ideali $\{[0]\}$ oppure A/I, cioè per ogni ideale J/I di A/I, con $I \subseteq J$, si ha $J/I = \{[0]\}$ o $J/I = A/I$. Per 0.43, ciò è equivalente a dire che per ogni ideale J di A, con $I \subseteq J$, allora $J = I$ oppure $J = A$. Questo significa che I è massimale.
ii) La tesi segue immediatamente, osservando che

$$xy \in I \iff [xy] = 0_{A/I} \iff [x] \cdot [y] = 0_{A/I}$$

per ogni $x, y \in A$. □

Esempio 2.26.1. Osserviamo che nella Proposizione 2.26 l'ipotesi che A sia unitario è essenziale. Infatti se così non è, può accadere che I sia un ideale massimale ma che A/I non sia un campo, e addirittura che non sia integro. Si considerino ad esempio $A = 2\mathbb{Z} = (2\mathbb{Z}, +, \cdot, 0)$ e $I = 4\mathbb{Z} = \big(4\big)$ suo ideale massimale. Allora

$$A/I = 2\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{2}\}$$

e $\overline{2} \cdot \overline{2} = \overline{0}$. Di conseguenza A/I non è integro e quindi non è un campo.

Esempio 2.26.2. Nell'anello $\mathbb{Z}$ sono equivalenti:
i) (n) è un ideale massimale;
ii) n è un numero primo;
iii) (n) è un ideale primo.
Infatti (n) è massimale $\iff$ non esiste $m \in \mathbb{Z}$ tale che $(n) \subsetneqq (m) \subsetneqq \mathbb{Z}$ $\iff$ non esiste $m \in \mathbb{Z}$ tale che $m \neq n$, $m \neq 1$ e $m|n$ $\iff$ n è primo.
D'altra parte, (n) è primo $\iff$ $[\ xy \in (n) \Longrightarrow x \in (n)$ oppure $y \in (n)]$ $\iff$ $[\ n|xy \Longrightarrow n|x$ oppure $n|y\ ]$ $\iff$ n è primo.

Concludiamo con un'utile caratterizzazione degli ideali primi.

Proposizione 2.27. *Sia P un ideale proprio di A; allora sono equivalenti:*
i) P è primo;
ii) se I e J sono ideali di A tali che $IJ \subseteq P$, allora $I \subseteq P$ oppure $J \subseteq P$;
iii) se $n \in \mathbb{N}^*$ e $I_1, \ldots, I_n$ sono ideali di A tali che $I_1 \cdots I_n \subseteq P$, allora esiste $j \in \{1, \cdots, n\}$ tale che $I_j \subseteq P$.

Dimostrazione.
$(i) \Rightarrow (ii)$ Supponiamo che $I \not\subseteq P$. Chiaramente deve essere $I \neq (0_A)$, quindi esiste $0_A \neq x \in I$ e $x \notin P$. Dall'ipotesi $IJ \subseteq P$ segue che $xy \in P$ per ogni $y \in J$. Essendo P un ideale primo, dalla definizione segue che necessariamente $y \in P$ per ogni $y \in J$, cioè $J \subseteq P$.
$(ii) \Rightarrow (i)$ Siano $x, y \in A$ tali che $xy \in P$. Vogliamo provare che $x \in P$ oppure $y \in P$.
Si considerino gli ideali principali $I := (x)$ e $J := (y)$. È immediato vedere che il loro prodotto è

$$IJ = (x)(y) = (xy) \subseteq P.$$

Dunque per ipotesi si ha: $I \subseteq P$ oppure $J \subseteq P$, cioè $(x) \subseteq P$ oppure $(y) \subseteq P$. Pertanto $x \in P$ oppure $y \in P$, come volevamo.
$(ii) \Rightarrow (iii)$ Si prova per induzione su n. Per $n = 2$ è vero in quanto la tesi è esattamente l'ipotesi (ii). Supponiamo che l'affermazione sia vera per $n - 1$ e proviamola per n. Siano $I_1, \ldots, I_n$ ideali tali che $I_1 \cdots I_n \subseteq P$. Chiaramente $I_1 \cdots I_n = (I_1 \cdots I_{n-1})I_n$ e questo è un prodotto di due ideali contenuto in P. Per l'ipotesi (ii) allora o $I_1 \subseteq P$ oppure $I_1 \cdots I_{n-1} \subseteq P$. Nel primo caso si ha la tesi. Nel secondo, per l'ipotesi induttiva, esiste $j \in \{1, \cdots, n-1\}$ tale che $I_j \subseteq P$, e anche in tal caso si ha la tesi.
$(iii) \Rightarrow (ii)$ Ovvio. □

Teorema Cinese dei Resti in un anello commutativo

Vediamo ora una generalizzazione di 1.9 e 1.10, in cui l'ambiente era $\mathbb{Z}$, al caso di un anello commutativo unitario.

Introduciamo una nozione che generalizza quella di numeri interi coprimi.

Definizione. Sia A un anello commutativo, unitario. Due ideali I e J di A si dicono *coprimi* se $I + J = A$.

Lemma 2.28. *Siano $I_1, \cdots, I_n$ ideali di A a due a due coprimi (cioè: $I_j + I_k = A$ se $j \neq k$). Allora*

$$\bigcap_{j=1}^{n} I_j = I_1 \cdot \ldots \cdot I_n.$$

Dimostrazione. Per semplicità dimostriamo il lemma per $n = 2$ cioè proviamo che se I e J sono due ideali di A allora $I + J = A$ implica $I \cap J = IJ$.
Si ricordi che l'inclusione "$\supseteq$" vale sempre, come osservato in 2.3.
"$\subseteq$" Si noti che $I \cap J = A(I \cap J) = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J)$ dove l'ultima uguaglianza segue dalla distributività del prodotto rispetto alla somma di ideali (facile esercizio). Si osservi infine che l'ultimo ideale è somma di due ideali ciascuno contenuto in IJ, dunque esso stesso è contenuto in IJ. □

Teorema 2.29. *(Teorema Cinese dei Resti in un anello). Sia A un anello commutativo unitario e siano $I_1, \cdots, I_n$ suoi ideali propri a due a due coprimi. Allora, posto $I{:=}I_1 \cdot \ldots \cdot I_n$, l'applicazione*

$$f : A/I \longrightarrow A/I_1 \times \cdots \times A/I_n \qquad \textit{definita da} \qquad [x]_I \quad \mapsto \quad ([x]_{I_1}, \ldots, [x]_{I_n})$$

è un isomorfismo di anelli.

Dimostrazione. Consideriamo l'applicazione

$$g : A \longrightarrow A/I_1 \times \cdots \times A/I_n \quad \text{definita da} \quad x \mapsto ([x]_{I_1}, \ldots, [x]_{I_n}).$$

Basta provare che

i) g è un omomorfismo di anelli;
ii) $\ker(g) = I$;
iii) g è suriettiva.

Infatti, in tal caso, per il Primo teorema di omomorfismo di anelli (vedi 0.41) g si fattorizza attraverso l'isomorfismo f definito nell'enunciato.

i) Tenendo conto del fatto che la proiezione canonica $\pi_i : A \longrightarrow A/I_i$ è un omomorfismo di anelli per ogni $i = 1, \ldots, n$, segue facilmente che anche g è un omomorfismo di anelli.
ii) È immediato verificare che $\ker(g) = I_1 \cap \cdots \cap I_n$ e tale intersezione coincide con $I_1 \cdots I_n$ per 2.28.
iii) Proviamo la suriettività di g nel caso $n = 2$. Siano dunque I e J ideali propri coprimi di A, cioè $I + J = A = (1_A)$. Pertanto esistono $i \in I$ e $j \in J$ tali che $i + j = 1_A$. In particolare, $i \notin J$ e $j \notin I$.
Si consideri ora il generico elemento $([x]_I, [y]_J) \in A/I \times A/J$: mostriamo che tale elemento appartiene all'immagine di g. Infatti, sia $z := xj + yi$ e si calcoli

$$g(z) = g(xj + yi) = ([xj + yi]_I, [xj + yi]_J) = ([xj]_I, [yi]_J)$$

dove l'ultima uguaglianza segue dal fatto che $[xj + yi]_I = [xj]_I + [yi]_I = [xj]_I + [0_A]_I$ (analogamente sulla seconda componente). Infine si osservi che

$$1_A = i + j \quad \Rightarrow \quad x = xi + xj \quad \Rightarrow \quad x - xj = xi \in I \quad \Rightarrow \quad [xj]_I = [x]_I$$

e analogamente $[yi]_J = [y]_J$. Pertanto $g(z) = ([x]_I, [y]_J)$.
Il caso generale si prova per induzione su n: il passo iniziale è quello precedente per $n = 2$. Il passo induttivo usa l'isomorfismo stabilito per due ideali e l'ipotesi induttiva, per la quale occorre il Lemma 2.30, di cui omettiamo la dimostrazione. □

Dimostrazione alternativa del **Teorema 2.29.**
Qui vogliamo esplicitare l'isomorfismo f, in quanto è sufficiente provare (i) e (ii) (che bastano per individuare il monomorfismo f) ed esibire l'inversa di f. Vediamo i casi $n = 2$ e $n = 3$.

Caso $n = 2$.
L'omomorfismo f è

$$f : A/IJ \longrightarrow A/I \times A/J \qquad \text{definito da} \qquad [x]_{IJ} \quad \mapsto \quad ([x]_I, [x]_J)$$

e il suo inverso è

$$\tilde{f} : A/I \times A/J \longrightarrow A/IJ \qquad \text{data da} \qquad ([x]_I, [y]_J) \quad \mapsto \quad [xj + yi]_{IJ}$$

dove $i \in I$ e $j \in J$ sono tali che $i + j = 1_A$.

Con questa linea dimostrativa, al posto della suriettività di g della dimostrazione precedente, occorre fare un altro piccolo calcolo. Provare cioè che $\tilde{f}$ è ben definita e che composta con f coincide con l'identità. Se $([x]_I, [y]_J) = ([x']_I, [y']_J)$ allora $x - x' \in I$ e $y - y' \in J$. Pertanto

$$(xj + yi) - (x'j + y'i) = (x - x')j + (y - y')i \in IJ$$

e quindi $[xj+yi]_{IJ} = [x'j+y'i]_{IJ}$, cioè $\tilde{f}$ non dipende dalla scelta dei rappresentanti di $[x]_I$ e $[y]_J$.
Per concludere la dimostrazione, basta mostrare che $f(\tilde{f}(([x]_I,[y]_J))) = ([x]_I,[y]_J)$ (stesso argomento usato in 2.29) e che $\tilde{f}(f([x]_{IJ})) = [x]_{IJ}$, per ogni $x, y \in A$. Riguardo la seconda uguaglianza da provare, è chiaro che

$$\tilde{f}(f([x]_{IJ})) = \tilde{f}([x]_I,[x]_J) = [xj+xi]_{IJ} = [x(i+j)]_{IJ} = [x]_{IJ}$$

dove l'ultima uguaglianza segue da $i+j=1$.

Caso $n=3$.
I tre ideali, a due a due coprimi, siano I, J, K. Dunque si consideri l'omomorfismo (usiamo un nome diverso)

$$F : A/IJK \longrightarrow A/I \times A/J \times A/K \qquad \text{dato da} \qquad [x]_{IJK} \quad \mapsto \quad ([x]_I,[x]_J,[x]_K)\,.$$

Costruiamo $\tilde{F}$ come la composizione dei seguenti isomorfismi:

$$(A/I \times A/J) \times A/K \longrightarrow A/IJ \times A/K \longrightarrow A/IJK$$

dove il primo è $(\tilde{f}, id_{A/K})$ e il secondo è anch'esso ottenuto nel caso $n=2$ (si osservi che il lemma 2.30 garantisce che gli ideali IJ e K siano coprimi). Pertanto $\tilde{F}$ è un isomorfismo. Per scrivere esplicitamente come è definito, procediamo con i due passaggi:

$$([x]_I,[y]_J,[z]_K) \mapsto ([xj+yi]_{IJ},[z]_K) \mapsto [(xj+yi)k+zl]_{IJK}$$

dove $l \in IJ$ e $k \in K$ sono tali che $l+k=1$. □

Esempio 2.29.1. Sia $A=\mathbb{Z}$ e siano $I=(r), J=(s), K=(t)$, con $r,s,t \in \mathbb{N}$ a due a due coprimi.
Allora si verifica che $IJ = I \cap J = (rs)$, dunque $l = i'j'$ con $i' \in I$ e $j' \in J$. Pertanto l'isomorfismo $\tilde{F}$ è

$$\tilde{F} : \mathbb{Z}/(r) \times \mathbb{Z}/(s) \times \mathbb{Z}/(t) \longrightarrow \mathbb{Z}/(rst)$$

definito da

$$([x]_r,[y]_s,[z]_t) \mapsto [(xj+yi)k+zl]_{rst} = [xjk+yik+zi'j']_{rst}$$

ove $i+j=1$ e $i'j'+k=1$.

Lemma 2.30. *Sia A un anello commutativo unitario e siano $I_1,\cdots,I_n$ suoi ideali propri a due a due coprimi. Allora, per ogni $k=1,\ldots,n$, gli ideali I_k e $I_1I_2\cdots\hat{I}_k\cdots I_n$ sono coprimi.* □

Come osservato, dal Teorema 2.29 segue come caso particolare il Teorema 1.10. Infatti $s_1,\ldots,s_n \in \mathbb{Z}$ sono interi a due a due coprimi se e solo se gli ideali principali di $\mathbb{Z}$ corrispondenti, cioè $(s_1),\ldots,(s_n)$, sono ideali a due a due coprimi. Inoltre $(s_1)\cdots(s_n) = (s_1\cdots s_n)$. Quindi, nelle precedenti ipotesi

$$\mathbb{Z}_{s_1\cdots s_n} \quad \cong \quad \mathbb{Z}_{s_1} \times \mathbb{Z}_{s_2} \times \ldots \times \mathbb{Z}_{s_n}.$$

Questo isomorfismo fornisce una interessante conseguenza sulla funzione di Eulero. A tale scopo abbiamo bisogno del seguente risultato preliminare:

Lemma 2.31. *Siano $A_1,\ldots,A_n$ anelli unitari e $A = A_1 \times \cdots \times A_n$ l'anello prodotto. Allora si ha l'uguaglianza di gruppi moltiplicativi (entrambi sottoinsiemi di A):*

$$\mathcal{U}(A) = \mathcal{U}(A_1) \times \cdots \times \mathcal{U}(A_n).$$

Dimostrazione. "$\subseteq$" Mostriamo che se $(x_1,\ldots,x_n) \in \mathcal{U}(A)$ allora $x_i \in \mathcal{U}(A_i)$ per ogni i.
Per ipotesi esiste $(y_1,\ldots,y_n) := (x_1,\ldots,x_n)^{-1} \in A$ cioè

$$(x_1,\ldots,x_n)\cdot(y_1,\ldots,y_n) = (x_1y_1,\ldots x_ny_n) = 1_A = (1_{A_1},\ldots,1_{A_n}).$$

Pertanto x_i è invertibile in A_i per ogni $i=1,\ldots,n$, quindi $(x_1,\ldots,x_n) \in \mathcal{U}(A_1)\times\cdots\times\mathcal{U}(A_n)$.
"$\supseteq$" Viceversa, sia $(x_1,\ldots,x_n) \in \mathcal{U}(A_1)\times\cdots\times\mathcal{U}(A_n)$. Allora $(x_1,\ldots,x_n)$ è invertibile in A, infatti $(x_1,\ldots,x_n)^{-1} = (x_1^{-1},\ldots,x_n^{-1})$. □

Teorema 2.32. *La funzione di Eulero ϕ è moltiplicativa sugli interi coprimi, cioè, se $s_1, ..., s_n \in \mathbb{N}$ sono a due a due coprimi allora*

$$\phi(s_1 \cdots s_n) = \phi(s_1) \cdots \phi(s_n).$$

Dimostrazione. Consideriamo l'isomorfismo descritto sopra: $\mathbb{Z}_{s_1 \cdots s_n} \cong \mathbb{Z}_{s_1} \times \mathbb{Z}_{s_2} \times \cdots \times \mathbb{Z}_{s_n}$. Chiaramente

$$\mathcal{U}(\mathbb{Z}_{s_1 \ldots s_n}) \cong \mathcal{U}(\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_n})$$

e, d'altra parte, per 2.31 si ha

$$\mathcal{U}(\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_n}) = \mathcal{U}(\mathbb{Z}_{s_1}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{s_n}).$$

Pertanto i gruppi $\mathcal{U}(\mathbb{Z}_{s_1 \ldots s_n})$ e $\mathcal{U}(\mathbb{Z}_{s_1}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{s_n})$ sono isomorfi. In particolare hanno lo stesso ordine:

$$\#\,\mathcal{U}(\mathbb{Z}_{s_1 \ldots s_n}) = \#\,(\mathcal{U}(\mathbb{Z}_{s_1}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{s_n})) = \#\,(\mathcal{U}(\mathbb{Z}_{s_1})) \cdots \#\,(\mathcal{U}(\mathbb{Z}_{s_n})).$$

Per 2.10, l'ordine del gruppo moltiplicativo $\#(\mathcal{U}(\mathbb{Z}_n))$ è esattamente la funzione di Eulero $\phi(n)$ calcolata in n, quindi dall'uguaglianza precedente segue che $\phi(s_1 \cdots s_n) = \phi(s_1) \cdots \phi(s_n)$. □

Fattorialità

D'ora in poi sia A un anello communativo, unitario ed integro.

La nozione di numero primo in $\mathbb{N}$ (e quindi in $\mathbb{Z}$) è legata sia al fatto di non avere divisori sia alla proprietà di dividere necessariamente uno dei fattori di un prodotto nel caso in cui divida il prodotto stesso. In un anello qualunque tali nozioni sono distinte anche se legate, come vedremo.

Definizione. Sia $x \in A$; x si dice *irriducibile* se:
- $x \neq 0$;
- $x \notin \mathcal{U}(A)$;
- x non ha divisori propri.

Definizione Sia $x \in A$, x si dice *primo* se:
- $x \neq 0$;
- $x \notin \mathcal{U}(A)$;
- $x \big| (yz) \Leftrightarrow x \big| y$ o $x \big| z$.

Proposizione 2.33. *Sia A dominio e $x \in A^*$ un elemento non invertibile.*
Allora x è primo $\Leftrightarrow$ l'ideale principale (x) è primo.

Dimostrazione. Per definizione x è primo $\Leftrightarrow x \mid yz \Rightarrow x \mid y$ oppure $x \mid z$.
Mentre (x) è un ideale primo $\Leftrightarrow yz \in (x) \Rightarrow y \in (x)$ oppure $z \in (x)$.
Si conclude osservando che, per ogni $\alpha \in A$, $x \mid \alpha$ se e solo se $\alpha \in (x)$. □

Proposizione 2.34. *Siano A un dominio e $x \in A$. Se x è primo allora x è irriducibile.*

Dimostrazione. Osserviamo intanto che, per ipotesi, $x \neq 0$ e $x \notin \mathcal{U}(A)$.
Supponiamo che $x = ab$; allora $a \mid x$ e $b \mid x$.
D'altra parte, da $x = ab$ segue $x \mid (ab)$ e dall'ipotesi che x sia primo si ha che $x \mid a$ oppure $x \mid b$.
Nel primo caso $x \mid a$ e, come osservato prima, $a \mid x$. Dunque, per definizione, x e a sono associati; quindi b è invertibile per 2.14. Pertanto x non ha divisori propri.
Nel secondo caso $x \mid b$ e, con un ragionamento analogo, si conclude ancora che x non ha divisori propri. □

Esempio 2.34.1. Come abbiamo osservato all'inizio, le nozioni di elemento primo e di elemento irriducibile coincidono nei numeri interi. Infatti è immediato verificare che, se $n \in \mathbb{Z}$ allora

n è irriducibile $\Leftrightarrow$ n è un numero primo o un suo opposto $\Leftrightarrow$ n è un elemento primo.

Definizione. Siano $a, b \in A$; diciamo che $d \in A$ è un *massimo comun divisore* di a e b se verifica le seguenti proprietà:
1. $d|a$ e $d|b$;
2. per ogni $e \in A$ tale che $e|a$ ed $e|b$, allora $e|d$.

Osserviamo che in un dominio qualunque non è garantita l'esistenza di un massimo comune divisore di due elementi e, se esiste, non è unico né canonicamente individuato (come accade in $\mathbb{Z}$) poiché in un dominio non c'è, in generale, una relazione d'ordine. Si possono comunque notare alcuni fatti.

Osservazione 2.35. Siano $a, b \in A$ e siano $d, d' \in A$ due massimi comuni divisori di a e b. Allora d e d' sono associati. Viceversa, se $d \in A$ è un massimo comun divisore, allora ogni associato di d lo è.

Pertanto siamo indotti a dare la seguente definizione e relativa notazione.

Definizione. Siano $a, b \in A$; se $d \in A$ è un massimo comun divisore di a e b scriveremo che $d = MCD(a, b)$ e diremo che d è "il" *massimo comun divisore* di a e b (non unico, ma definito a meno di un elemento invertibile).

Osservazione 2.36 Siano $x, y \in A$ e supponiamo che $(x, y) = (d)$. Allora $d = MCD(x, y)$.
Infatti, $x \in (d)$ e $y \in (d)$ quindi $d|x$ e $d|y$. Sia ora $z \in A$ tale che $z|x$ e $z|y$; allora $(x, y) \subseteq (z)$. Ma per ipotesi $(x, y) = (d)$ quindi $(d) \subseteq (z)$ dunque $d \in (z)$ cioè $z|d$. Questo prova che d è un massimo comun divisore per x e y.

In analogia con quanto visto per l'anello degli interi, si introduce la seguente nozione.

Definizione. Siano $a, b \in A$; se si verifica una delle proprietà equivalenti:
1. $MCD(a, b) = 1_A$;
2. esite un massimo comun divisore di a e b che è invertibile in A;
3. ogni massimo comun divisore di a e b è invertibile in A;

allora a e b si dicono *coprimi*.

Anche in generale vale la seguente proprietà, valida in $\mathbb{Z}$.

Osservazione 2.37. Se a e b sono due elementi coprimi di A, l'unico ideale principale contente (a) e (b) è l'ideale da $(1_A) = A$. Infatti, supponiamo che entrambi siano contenuti in un ideale principale (c); dunque $(a)+(b) \subseteq (c)$. Quindi $a = cn$ e $b = cm$, per opportuni $n, m \in A$. Questo implica che c divide un $MCD(a, b)$. Essendo a e b coprimi per ipotesi, si ha che c è invertibile e quindi $(c) = A$.

Definizione. Se per ogni $x, y \in A$ esiste massimo comune divisore tra x e y allora A si dice *dominio con massimo comune divisore (MCD)*.

Ad esempio, $\mathbb{Z}$ è un dominio con MCD per 2.6.

Teorema 2.38. *(Lemma di Euclide). Siano A un dominio con MCD e $x, y, z \in A^*$. Se $x \mid yz$ ed è coprimo con y allora divide z.*

Dimostrazione. Osserviamo dapprima che, se $d = MCD(x, y)$, allora $zd = MCD(xz, yz)$.
Sia ora $x \mid yz$; poiché $x \mid xz$ allora, per definizione di MCD, si ha che $x \mid MCD(xz, yz) = zd$.
Ma se x e y sono coprimi, allora $d = 1_A$ quindi x divide z. □

Corollario 2.39. *Siano A un dominio con MCD e $x \in A$. Allora*

$$x \text{ è primo} \quad \Leftrightarrow \quad x \text{ è irriducibile.}$$

Dimostrazione. "⇒" Per la proposizione 2.34.
"⇐" Si noti dapprima che, comunque scelto $a \in A$, ci sono solo due possibilità per $MCD(x, a)$. Infatti x è irriducibile cioè non ha divisori propri, dunque i suoi divisori non nulli sono invertibili oppure associati a x. Poiché $MCD(x, a)$ è un divisore di x, allora esso è invertibile, e quindi $MCD(x, a) = 1_A$; oppure è associato a x, e quindi $MCD(x, a) = x$.
Dobbiamo provare che x è primo, cioè che $x \mid ab \Rightarrow x \mid a$ oppure $x \mid b$.
Supponiamo x non divida a: per l'osservazione iniziale $MCD(x, a) = 1_A$. Possiamo quindi applicare 2.38 e ottenere che $x \mid b$. □

Definizione. Un anello integro A si dice *dominio a fattorizzazione unica (UFD = Unique Factorization Domain)* o *dominio fattoriale* se valgono le seguenti condizioni:

i) per ogni $x \in A$, $x \neq 0$, $x \notin \mathcal{U}(A)$:

$$x = p_1\, p_2 \cdots p_n$$

per opportuni $n \in \mathbb{N}^*$ e $p_1, p_2, \ldots, p_n$ elementi irriducibili di A (la scrittura precedente viene detta *fattorizzazione in irriducibili*);

ii) se x ammette due fattorizzazioni in irriducibili:

$$x = p_1\, p_2 \cdots p_n \quad \text{e} \quad x = q_1\, q_2 \cdots q_m$$

allora $n = m$ e si possono permutare i nomi dei q_i in modo che q_i e p_i siano associati per ogni $i = 1, \ldots, n$. (tale proprietà si esprime con *"la fattorizzazione in irriducibili è unica a meno di elementi invertibili"*).

Ad esempio in $\mathbb{Z}$ si ha che $15 = (5)(3) = (-5)(-3)$: sono fattorizzazioni distinte ma equivalenti nel senso precedente. Infatti $\mathbb{Z}$ è un dominio a fattorizzazione unica, come vedremo.

Osservazione 2.40. Ogni campo è UFD, infatti nessun elemento del campo soddisfa (i) quindi tutti gli elementi del campo soddisfano la definizione di UFD.

Osservazione 2.41. Se A è un UFD e $x \in A^*$ è non invertibile, allora nella sua fattorizzazione in irriducibili $x = p_1\, p_2 \cdots p_n$ alcuni p_i possono coincidere. Dunque sono univocamente determinati, oltre ai p_i anche i relativi esponenti α_i nella scrittura (unica a meno di elementi invertibili)

$$x = p_1^{\alpha_1} \cdots p_s^{\alpha_s}.$$

Inoltre per ogni $x \in A^*$, x ha un numero finito di divisori non associati tra loro. (Al lettore la facile verifica).

Esempio 2.41.1. In $\mathbb{Z}$ si ha $x = 15 = 5^1 3^1$ e $y = 49 = 7^2$. Se si vogliono far apparire $3, 5, 7$ in entrambe le fattorizzazioni, allora si può scrivere $x = 3^1 5^1 7^0$ e $y = 3^0 5^0 7^2$.

Il seguente risultato stabilisce un legame tra gli anelli fattoriali e quelli con massimo comun divisore.

Teorema 2.42. *Sia A un dominio. Se A è UFD allora A ha MCD.*

Dimostrazione. Siano $x, y \in A$ e si considerino le rispettive fattorizzazioni in irriducibili che coinvolgano i fattori di entrambi (come in 2.41.1):

$$x = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \quad \text{e} \quad y = p_1^{\beta_1} \cdots p_n^{\beta_n}.$$

Dunque un massimo comun divisore di x e y è $d = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$, dove $\gamma_i = \min(\alpha_i, \beta_i)$ per $i = 1, \ldots, n$. □

Corollario 2.43. *Siano A un UFD e $x \in A$. Allora*

$$x \text{ è primo} \quad \Leftrightarrow \quad x \text{ è irriducibile.}$$

Dimostrazione. Immediata da 2.39 e da 2.42. □

Nell'ambito della fattorialità gli anelli a ideali principali svolgono un ruolo particolarmente importante, come emerge dai seguenti risultati.

Teorema 2.44. *Se A è un PID valgono i seguenti fatti:*

a) Siano $x, y \in A^*$. Allora:

$$d = MCD(x, y) \iff (x, y) = (d).$$

b) L'anello A è un dominio con MCD.

c) Se $d = MCD(x, y)$ allora esistono $a, b \in A$ tali che $d = ax + by$ (identità di Bézout).

Dimostrazione.

a) Per 2.36 $(x, y) = (d)$ implica che $d = MCD(x, y)$.

Viceversa, sia $d = MCD(x, y)$. In particolare $d|x$ e $d|y$; allora $x = dh$ e $y = dk$ per opportuni $h, k \in A$. Pertanto $(x, y) \subseteq (d)$. Poiché A è PID si ha che $(x, y) = (z)$ per un opportuno $z \in A$ quindi $z|x$ e $z|y$. Ma d è massimo comun divisore per x e y quindi $z|d$, cioè $d \in (z)$. Pertanto $(d) \subseteq (z) = (x, y)$. Dalla doppia inclusione segue $(x, y) = (d)$.

b) Segue direttamente da (a). Infatti, presi due qualsiasi $m, n \in A$, è sufficiente considerare l'ideale (m, n): essendo A un PID, $(m, n) = (k)$ per un certo $k \in A$. Dunque per il punto (a) si ha che k è un massimo comun divisore di m ed n.

c) Segue direttamente da (a). Infatti $(x, y) = (d)$ dunque $d \in (x, y)$. Tenuto conto che (x, y) è l'insieme delle combinazioni lineari di x ed y, esistono $a, b \in A$ tali che $d = ax + by$. □

Corollario 2.45. *Siano A un PID e $x \in A$. Allora sono equivalenti:*
1) *x è primo;*
2) *x è irriducibile;*
3) *(x) è un ideale primo;*
4) *(x) è un ideale massimale.*

Dimostrazione. Si osservi che $(1), (2), (3)$ sono equivalenti in ogni anello con MCD e dunque in un PID per 2.44 (b).
Infatti $(1) \Leftrightarrow (2)$ per Corollario 2.39. Inoltre $(1) \Leftrightarrow (3)$ vale in ogni dominio per Proposizione 2.33.
Resta da provare che, assumendo che A sia un PID, vale $(3) \Rightarrow (4)$. Tale fatto si prova facilmente con un argomento simile a quello dell'esempio 2.26.1. □

Teorema 2.46. *Ogni PID è UFD.*

Dimostrazione. Omettiamo la dimostrazione della condizione (i) della definizione di UFD. Verifichiamo solo l'unicità della fattorizzazione.
Siano A un PID e $a \in A^*$, $a \notin \mathcal{U}(A)$ tale che

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

con $r \leq s$ e p_i e q_i irriducibili. Per 2.45 tutti i p_i e i q_i sono primi. Dunque $p_1 \mid (q_1 \cdots q_s)$ implica che $p_1 \mid q_j$ per un opportuno j. Riordinando i q_i posso supporre che $p_1 \mid q_1$. Ma l'elemento q_1 è irriducibile, dunque p_1 è divisore improprio ed è associato non essendo invertibile. Quindi si ha $q_1 = u_1 p_1$, con $u_1 \in \mathcal{U}(A)$. Pertanto

$$p_1 \cdots p_r = u_1 \cdot p_1 \cdot q_2 \cdots q_s.$$

Per la legge di cancellazione in un dominio si ottiene

$$p_2 \cdots p_r = u_1 \cdot q_2 \cdots q_s.$$

Iterando il procedimento su p_2 e, successivamente, su ogni p_i restante, otterremo

$$1_A = u_1 \cdot \ldots \cdot u_r \cdot q_{s-r} \cdot \ldots \cdot q_s,$$

ma i q_i sono irriducibili e, dunque, non invertibili. Pertanto $r = s$ e, ordinatamente si ha che p_i e q_i sono associati per ogni $i = 1, \ldots, r$. □

In conclusione, per un dominio valgono le implicazioni

$$PID \quad \Rightarrow \quad UFD \quad \Rightarrow \quad \text{anello con } MCD$$

ma non valgono le implicazioni opposte. Si noti infine che, usando 2.46 e 2.42, si ha immediatamente il Teorema 2.44 (b).

Vediamo come si applica quanto visto in generale agli anelli $\mathbb{Z}$ e $\mathbb{Z}_n$.

Osservazione 2.47. Abbiamo visto in 0.47 che $\mathbb{Z}$ è un PID.
Tale fatto può essere anche provato direttamente, in modo costruttivo, usando il fatto (non dimostrato) che ogni ideale di $\mathbb{Z}$ è finitamente generato. Infatti sia $I = (n_1, \dots, n_r)$ un ideale di $\mathbb{Z}$; si vede facilmente che I è generato dal $MCD(n_1, \dots, n_r)$ dove si definisce ricorsivamente

$$MCD(n_1, \dots, n_r) := MCD(MCD(n_1, \dots, n_{r-1}), n_r).$$

Osservazione 2.48. In $\mathbb{Z}$ due ideali (n) e (m) sono coprimi se vale una delle seguenti:

$$(n) + (m) = \mathbb{Z} \iff (n, m) = (1_{\mathbb{Z}}) \iff MCD(n, m) = 1_{\mathbb{Z}}.$$

Osservazione 2.49. Ricordiamo che, se I è un ideale di A, la proiezione canonica $\pi : A \to A/I$ opera sugli ideali $J \supseteq I$ in modo che $J \mapsto J/I := \{[x] | x \in J\}$ con $J \supseteq I$.
Più precisamente, per 0.42, tutti e soli gli ideali di A/I sono della forma J/I con $J \supseteq I$.

Esempio 2.49.1. Come caso particolare, gli ideali di $\mathbb{Z}_n = \mathbb{Z}/(n)$ sono le proiezioni di tutti e soli gli ideali di $\mathbb{Z}$ contenenti (n), ovvero sono del tipo $(m)/(n)$ con $(m) \supseteq (n)$, o equivalentemente tali che $m \mid n$.
Ad esempio gli ideali di $\mathbb{Z}_{12}$ sono

$$([0]) = \frac{(12)}{(12)}, \frac{(1)}{(12)}, \frac{(2)}{(12)}, \frac{(3)}{(12)}, \frac{(4)}{(12)}, \frac{(6)}{(12)}.$$

L'anello $\mathbb{Z}_n$ è un PIR (cioè a ideali principali) ma è un PID se e solo se n è primo. In tal caso $\mathbb{Z}_n$ è un campo, dunque i suoi ideali sono solo quelli banali.
Vediamo ora che, se n non è primo, quanto si verifica in $\mathbb{Z}$ per gli ideali coprimi (2.48) non accade in $\mathbb{Z}_n$.

Osservazione 2.50. Siano $a, b \in \mathbb{Z}$ due interi coprimi, cioè $MCD(a, b) = 1$. Dunque vale l'identità di Bézout, $1 = ka + hb$ con $k, h \in \mathbb{Z}$ opportuni. Passando alle classi d'equivalenza in $\mathbb{Z}_n$ si ottiene $[1] \in ([a], [b])$, da cui $([a]) + ([b]) = \mathbb{Z}_n$ e quindi gli ideali $([a])$ e $([b])$ sono coprimi.
Viceversa, siano $([a])$ e $([b])$ due ideali coprimi di $\mathbb{Z}_n$, cioè $([a], [b]) = ([1])$. Sia $d = MCD(a, b)$. Per definizione $d|a$ e $d|b$, quindi $[d] \mid [a]$ e $[d] \mid [b]$. Allora $([a], [b]) \subseteq ([d])$ quindi $([1]) \subseteq ([d])$, per cui $[d]$ è invertibile in $\mathbb{Z}_n$. Ciò significa che d ed n sono coprimi. Questo non implica che $MCD(a, b) = 1$, come vedremo nel seguente esempio.

Esempio 2.50.1. Consideriamo in $\mathbb{Z}_{36}$ gli ideali $I = ([15])$ e $J = ([10])$.
In $\mathbb{Z}$ abbiamo $MCD(15, 10) = 5$ dunque $(15, 10) = (5)$, passando a $\mathbb{Z}_{36}$ abbiamo

$$I + J = ([15], [10]) = ([5]).$$

Infatti l'inclusione "$\subseteq$" è ovvia.
Viceversa, per Bézout, $5 = 15m + 10n$ per opportuni m, n. Ad esempio $5 = 15 - 10 \Rightarrow [5] = [15] - [10]$. Pertanto $[5] \in I + J$ e questo prova che I e J sono coprimi. Infatti $([5]) = \mathbb{Z}_{36}$ in quanto $MCD(5, 36) = 1$ (vedi 2.9). Tuttavia 15 e 10 non sono coprimi. Questo accade perché $\mathbb{Z}_{36}$ non è integro.

Pertanto 2.48 non vale in un qualunque PIR, se non è integro.

Il fatto che $\mathbb{Z}_n$ non sia integro fa mancare un'altra fondamentale proprietà che vale invece in $\mathbb{Z}$: la fattorialità.

Osservazione 2.51. In $\mathbb{Z}_{12}$ abbiamo

$$[3][10] = [30] = [6] \quad \text{e anche} \quad [3][6] = [18] = [6].$$

Ma $[10]$ e $[6]$ non sono associati (e neppure $[3]$ e $[6]$). Pertanto $[6] \in \mathbb{Z}_{12}$ è fattorizzabile in due modi distinti. Ciò succede poichè gli elementi in gioco sono zero divisori.

Questa famiglia racchiude come esempi l'anello degli interi, quello degli interi di Gauss e quello dei polinomi (che introdurremo nel prossimo capitolo).

Vedremo che gli anelli euclidei sono, in particolare, a ideali principali. Dunque per essi valgono i fatti visti in precedenza per i PID. Termineremo con una interessante applicazione di Teoria dei numeri, e precisamente con un *Teorema di Fermat* su una famiglia speciale di numeri primi.

L'idea essenziale di anello euclideo è di un dominio dotato di una "valutazione", cioè di una mappa sui numeri naturali, e di una "divisione".

Definizione. Sia A un dominio e $\delta : A^* \longrightarrow \mathbb{N}$ una applicazione tale che per ogni $a, b \in A^*$ si ha:
i) $\delta(a) \leq \delta(ab)$;
ii) esistono $q, r \in A$ tali che $a = bq + r$, con $r = 0$ oppure $\delta(r) < \delta(b)$.

In tal caso diciamo che δ è una *valutazione* e (A, δ) (o A se è chiaro dal contesto) è un *anello euclideo.*

(Si prova facilmente che la prima proprietà segue dalla seconda).

Osservazione 2.52. L'anello $\mathbb{Z}$ con la valutazione data da $\delta(n) := |n|$ è un anello euclideo per 0.45.

Lemma 2.53. *Dati due interi a e b con $b \neq 0$, esistono $q', r' \in \mathbb{Z}$ tali che*

$$a = bq' + r' \quad \textit{con} \quad |r'| \leq |b|/2.$$

Dimostrazione. Per 0.45, esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$ tali che $0 \leq r < |b|$.
Se $r \leq |b|/2$, basta porre $r' = r$ e $q' = q$ e si ha la tesi.
Se invece $|b|/2 < r < |b|$, si ponga $r' := r - |b|$. Risulta $r' < 0$, dunque

$$|r'| = -r' = |b| - r < |b| - |b|/2 = |b|/2 \quad \Rightarrow \quad |r'| < |b|/2.$$

Si ponga inoltre $q' := q + |b|/b$. Dunque

$$bq' + r' = b(q + |b|/b) + r - |b| = bq + r = a,$$

come richiesto. □

Proposizione 2.54. *L'anello $\mathbb{Z}[i]$ degli interi di Gauss, con la valutazione data da $\delta(a + ib) := a^2 + b^2$, è un anello euclideo.*

Dimostrazione. Ovviamente $a^2 + b^2 > 0$.
(i) Segue dalla proprietà (più forte): $\delta(xy) = \delta(x)\delta(y)$. Infatti la valutazione δ è il quadrato della norma in $\mathbb{C}$ e vale, per ogni $z_1, z_2 \in \mathbb{C}$, che $\| z_1 z_2 \| = \| z_1 \| \, \| z_2 \|$.
(ii) Occorre mostrare che per ogni $x, y \in \mathbb{Z}[i]^*$ esistono $q, r \in \mathbb{Z}[i]$ tali che

$$y = xq + r \qquad \text{ove } r = 0 \text{ oppure } \delta(r) < \delta(x). \tag{$*$}$$

Proviamolo nel caso particolare $x \in \mathbb{N}^*$. Se $y = a + ib$, per il Lemma 2.53 esistono $u, v, u_1, v_1 \in \mathbb{Z}$ tali che:

$$a = xu + u_1, \quad b = xv + v_1 \quad \text{con} \quad |u_1| \leq x/2, \ |v_1| \leq x/2.$$

Posti $t := u + iv$ e $r := u_1 + iv_1$ (che appartengono a $\mathbb{Z}[i]$), si ha immediatamente che

$$y = a + ib = (xu + u_1) + i(xv + v_1) = x(u + iv) + (u_1 + iv_1) = xt + r$$

e vale $\delta(r) = \delta(u_1 + iv_1) = u_1^2 + v_1^2 \leq x^2/4 + x^2/4 = x^2/2 < x^2 = \delta(x)$. Quindi $(*)$ è provata se $x \in \mathbb{N}^*$.
In generale consideriamo un qualunque elemento (non nullo) x di $\mathbb{Z}[i]$. Posto $N := \delta(x)$, tale numero naturale non nullo può svolgere il ruolo di x nella dimostrazione precedente. Inoltre a y si sostituisca $Y := y\overline{x}$. Dunque si ha, per $(*)$ nel caso particolare, che esistono $q, r \in \mathbb{Z}[i]$ tali che

$$Y = Nq + R \qquad \text{ove } R = 0 \text{ oppure } \delta(R) < \delta(N). \tag{$**$}$$

Proviamo ora che q determinato in $(**)$ serve per verificare $(*)$. Ovviamente si ha

$$y = xq + r \quad \text{avendo posto} \quad r := y - xq \in \mathbb{Z}[i].$$

Resta da mostrare che, se $r \neq 0$, allora $\delta(r) < \delta(x)$.
Osserviamo anzitutto che $N = \delta(x) = x\overline{x} = \delta(\overline{x})$. Inoltre, essendo N un numero intero, $\delta(N) = N^2$. Le due uguaglianze precedenti implicano che $\delta(N) = N \cdot N = \delta(x)\delta(\overline{x})$. Infine osserviamo che

$$R = Y - Nq = y\overline{x} - x\overline{x}q = \overline{x}(y - xq) = \overline{x}r.$$

Dunque, essendo $x \neq 0$, se $R = 0$ allora $r = 0$. Supponiamo dunque $r \neq 0$. In tal caso, per quanto visto, $R \neq 0$; dunque, per $(**)$, si ha $\delta(R) < \delta(N)$. Per le precedenti espressioni di R e N si ha infine

$$\delta(\overline{x}r) = \delta(R) < \delta(N) = \delta(x)\delta(\overline{x}) \quad \Rightarrow \quad \delta(\overline{x})\delta(r) < \delta(x)\delta(\overline{x})$$

e quindi $\delta(r) < \delta(x)$, come volevamo. □

Teorema 2.55. *Ogni anello euclideo è un PID.*

Dimostrazione. L'ideale nullo è ovviamente principale. Sia dunque I un ideale non nullo di A. Poichè $I \neq (0_A)$, l'immagine $\delta(I)$ è non vuota e dunque ammette minimo per il Principio del Buon Ordinamento. Sia esso n_0 e sia $a_0 \in I^*$ tale che $\delta(a_0) = n_0$.
Si osservi che $(a_0) \subseteq I$ per definizione di ideale. Proviamo che vale anche l'altra inclusione.
Scegliamo un qualunque elemento $a \in I$. Per l'assioma (ii), esistono $q, r \in A$ tali che $a = a_0q + r$, con $r = 0$ oppure $\delta(r) < \delta(a_0)$. Ma $a, a_0 \in I$ dunque anche $r \in I$. La condizione $\delta(r) < \delta(a_0)$ è impossibile, in quanto a_0 è un elemento di I avente valutazione minima. Dunque $r = 0$ e quindi $a \in (a_0)$. Pertanto $I \subseteq (a_0)$. □

Esempio 2.55.1. Non vale il viceversa; un esempio di PID che non sia un anello euclideo è

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right],$$

cioè l'insieme delle espressioni del tipo $a+\alpha b$, con $a, b \in \mathbb{Z}$ e $\alpha = \frac{1+\sqrt{-19}}{2}$. Omettiamo però la dimostrazione.

Osservazione 2.56. In conclusione, per un dominio valgono le implicazioni

$$\text{euclideo} \quad \Rightarrow \quad PID \quad \Rightarrow \quad UFD \quad \Rightarrow \quad \text{anello con } MCD.$$

Una interessante proprietà riguarda gli elementi non invertibili: essi fanno "aumentare" la valutazione.

Proposizione 2.57. *Sia A un anello euclideo e $b \in A^* \setminus \mathcal{U}(A)$. Allora $\delta(a) < \delta(ab)$ per ogni $a \in A^*$.*

Dimostrazione. Per definizione di anello euclideo $\delta(a) \leq \delta(ab)$ e, dividendo a per ab, si ha $a = q(ab) + r$, dove $r = 0$ oppure $\delta(r) < \delta(ab)$. Supponiamo $\delta(a) = \delta(ab)$; se r fosse non nullo, allora $\delta(r) < \delta(ab) = \delta(a)$. D'altra parte $r = a - qab = a(1 - qb)$; dunque sempre tenendo conto che A è euclideo, $\delta(a) \leq \delta(r)$. Ma questo è impossibile, quindi $r = 0$.
In tal caso $a = qab$ e, per la legge di cancellazione in un dominio, $1_A = qb$, dunque b è invertibile. □

Come ovvia conseguenza del fatto precedente, se $b \in A^*$ è un elemento non invertibile di un anello euclideo, allora $\delta(b) > \delta(1_A)$. Se $A = \mathbb{Z}[i]$, ciò implica immediatente il seguente

Corollario 2.58. *Se $a + ib \in \mathbb{Z}[i]$ è un elemento non nullo e non invertibile, allora $a^2 + b^2 \neq 1$.* □

Possiamo ora provare due risultati preliminari al teorema principale

Lemma 2.59. *Sia $p \in \mathbb{Z}$ un numero primo. Siano $c, x, y \in \mathbb{Z}$ tali che $MCD(c, p) = 1$ e*

$$cp = x^2 + y^2.$$

Allora esistono $a, b \in \mathbb{Z}$ tali che

$$p = a^2 + b^2.$$

Dimostrazione.
Step 1. Mostriamo che p non è primo in $\mathbb{Z}[i]$. Altrimenti, poiché p divide $x^2+y^2=(x+iy)(x-iy)$, dovrebbe dividere $x+iy$ oppure $x-iy$. Nel primo caso, in $\mathbb{Z}$ si avrebbe che $p|x$ e $p|y$, dunque si avrebbe che $p|(x-iy)$ in $\mathbb{Z}[i]$ (analogamente nel secondo caso). Pertanto p^2 divide $x^2+y^2=cp$ e questo implica $p|c$, contro l'ipotesi.
Step 2. Come visto $\mathbb{Z}[i]$ è euclideo e quindi un dominio con MCD. Pertanto gli elementi primi sono tutti e soli quelli irriducibili (vedi....).
Step 3. Per i precedenti passi, p non è irriducibile in $\mathbb{Z}[i]$, quindi ammette una fattorizzazione non banale

$$p=(a+ib)(f+ig)$$

dove i due fattori $a+ib$ e $f+ig$ non sono invertibili. Per 2.58 si ha dunque che $a^2+b^2\neq 1\neq f^2+g^2$. Inoltre p è reale, dunque dalla precedente fattorizzazione si ha che $bf+ag=0$, quindi si verifica che vale anche

$$p=(a-ib)(f-ig).$$

Dalle due uguaglianze precedenti, si ottiene l'uguaglianza (in $\mathbb{Z}$):

$$p^2=(a^2+b^2)(f^2+g^2).$$

Ma $\mathbb{Z}$ è fattoriale e dunque, essendo i fattori a destra non invertibili come osservato prima e p primo, necessariamente

$$a^2+b^2=p=f^2+g^2$$

come richiesto. □

Lemma 2.60. *Sia $p\in\mathbb{N}$ un numero primo della forma $4n+1$. Allora la congruenza*

$$x^2\equiv -1 \pmod{p}$$

ha soluzioni.

Dimostrazione. Poiché $p=4n+1$ allora $p-1$ è multiplo di 4 e quindi $\frac{p-1}{2}$ è intero positivo pari. Quindi il numero

$$x:=\left(\frac{p-1}{2}\right)!$$

è prodotto di un numero pari di fattori:

$$x=1\cdot 2\cdot 3\cdots\frac{p-1}{2}.$$

Quindi vale anche

$$x=(-1)\cdot(-2)\cdot(-3)\cdots\left(-\frac{p-1}{2}\right).$$

Poiché per ogni intero k vale $(p-k)\equiv -k \pmod{p}$, dalla precedente uguaglianza segue che

$$x\equiv_p (p-1)\cdot(p-2)\cdot(p-3)\cdots\left(p-\frac{p-1}{2}\right).$$

Tenendo conto che $p-\frac{p-1}{2}=\frac{p+1}{2}$ è consecutivo a $\frac{p-1}{2}$, si ha in conclusione che

$$x^2\equiv_p 1\cdot 2\cdot 3\cdots\frac{p-1}{2}\cdot\frac{p+1}{2}\cdots(p-3)\cdot(p-2)\cdot(p-1)=(p-1)!.$$

Si conclude con la cosiddetta "uguaglianza di Wilson" che afferma

$$(p-1)!\equiv -1 \pmod{p}.$$

Infatti nel gruppo moltiplicativo $\mathcal{U}(\mathbb{Z}_p)$, a parte $[1]$ e $[p-1]$, che coincidono col proprio inverso, gli altri $p-3$ elementi si possono raggruppare in coppie del tipo $[\alpha]$ e $[\alpha]^{-1}$. Quindi $[p-1]!=[p-1]$ e dunque $(p-1)!\equiv_p (p-1)\equiv_p -1$. □

Teorema 2.61 (Fermat). *Sia $p \in \mathbb{N}$ un numero primo della forma $4n+1$. Allora*

$$p = a^2 + b^2$$

per opportuni $a, b \in \mathbb{Z}$.

Dimostrazione. Per 2.60, esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv_p -1$. Si può scegliere tale elemento in modo che $0 \leq x \leq p-1$. Anzi in modo che $x \leq p/2$. Infatti, se $x > p/2$, sia $y := p - x$. Allora $0 \leq y \leq p/2$ e y è ancora soluzione della precedente equazione modulare in quanto

$$y^2 = (p-x)^2 = p^2 - 2px + x^2 \equiv_p x^2.$$

Pertanto esiste $x \in \mathbb{N}$ tale che $x^2 \equiv_p -1$ e $0 \leq x \leq p/2$. Dunque $x^2 + 1$ è multiplo di p ovvero esistono $x, c \in \mathbb{N}$ tali che

$$x^2 + 1 = cp \qquad \text{con} \quad 0 \leq x \leq p/2. \tag{$*$}$$

Pertanto $x^2 + 1 \leq p^2/4 + 1 < p^2$ e quindi, per $(*)$, $cp < p^2$ in $\mathbb{Z}$. Da cui si ha $c < p$. Essendo p un numero primo, questo implica che c e p sono coprimi. Quindi possiamo applicare 2.59 a $(*)$, ottenendo la tesi. □

Capitolo 3 - Anelli di polinomi *

Polinomi a coefficienti in un anello

Definizione. Se S è un insieme non vuoto, si dice *successione ad elementi in* S un'applicazione $f : \mathbb{N} \to S$ che ad ogni elemento $i \in \mathbb{N}$ associa un elemento $c_i \in S$. Indicheremo le successioni nei seguenti modi:

$$(c_0, c_1, \ldots, c_n, \ldots) \quad \text{o anche} \quad (c_i)_{i\in\mathbb{N}} \quad \text{o brevemente} \quad (c_i).$$

L'insieme di tutte le successioni ad elementi in S si indica con $S^{\mathbb{N}}$.

Sia A un anello commutativo unitario; nell'insieme $A^{\mathbb{N}}$ di tutte le successioni ad elementi in A, introduciamo le seguenti operazioni (in maniera puntuale): la *somma*, definita da

$$(a_i) + (b_i) = (c_i), \quad \text{dove} \quad c_i := a_i +_A b_i.$$

Rispetto tale somma $A^{\mathbb{N}}$ è un gruppo commutativo, come si verifica facilmente.
Definiamo il *prodotto di Cauchy* di due successioni come

$$(a_i)(b_i) = (d_i), \quad \text{dove} \quad d_i := \sum_{n+m=i} a_n\, b_m.$$

Si vede che tale prodotto è associativo, commutativo e dotato di elemento neutro e che $A^{\mathbb{N}}$, dotato di tali operazioni, è un anello commutativo unitario. Osserviamo solo che $0_{A^{\mathbb{N}}}$ è la *successione nulla* (con $a_i = 0_A$ per ogni $i \in \mathbb{N}$) e che $1_{A^{\mathbb{N}}}$ è la *successione identità* (con $a_0 = 1_A$ e $a_i = 0_A$ per ogni $i \in \mathbb{N}^*$).

Definizione. Una successione $(a_i) \in A^{\mathbb{N}}$ si dice *quasi ovunque nulla* se a_i è diverso da zero per un numero finito di indici, o equivalentemente, se esiste j tale che per ogni $i > j$: $a_i = 0$. Scriveremo $(a_0, \ldots, a_j, 0, \to)$. Si indica con P_A il sottoinsieme di $A^{\mathbb{N}}$ delle successioni quasi ovunque nulle ad elementi in A.

Osserviamo che la successione nulla $0_{A^{\mathbb{N}}}$ e la successione $1_{A^{\mathbb{N}}}$ sono successioni quasi ovunque nulle.
Si riesce a provare che P_A è un sottogruppo additivo rispetto alla somma precedentemente definita, e che è chiuso rispetto al prodotto di Cauchy, e che quindi è un sottoanello unitario di $A^{\mathbb{N}}$.

Lasciamo al lettore la dimostrazione della seguente

Proposizione 3.1. *L'applicazione $f : A \to P_A$ che ad ogni $a \in A$ associa la successione quasi ovunque nulla $(a, 0, \to)$ è un monomorfismo di anelli.* □

Dunque P_A contiene, come sottoanello, una copia isomorfa di A. L'immagine di $a \in A$ tramite f è la successione $(a, 0, \to)$, che verrà anche denotata con $\overline{a}$. L'anello P_A contiene un elemento speciale, che non appartiene all'immagine di f, ed è la successione $X := (0_A, 1_A, 0_A, \to)$.

Proposizione 3.2. *Con le precedenti notazioni, si hanno i seguenti fatti:*
i) P_A è il più piccolo sottoanello di $A^{\mathbb{N}}$ contenente A ed X;
ii) ogni elemento di P_A può essere scritto nel seguente modo:

$$(c_0, c_1, \ldots, c_n, 0, \to) = \overline{c}_0 + \overline{c}_1 X + \ldots + \overline{c}_n X^n.$$

Dimostrazione. *i)* Lasciata al lettore.
ii) È sufficiente dimostrare che

$$(c_0, c_1, \ldots, c_n, 0, \to) = (c_0, 0, \to) + (0, c_1, 0, \to) + \ldots + (0, \ldots, c_n, 0, \to) \tag{1}$$

e

$$(0, \ldots, 0, c_s, 0, \to) = \overline{c}_s X^s, \quad \forall s. \tag{2}$$

La (1) è vera per definizione di somma in P_A. Proviamo la (2) nel caso in cui $s = 2$: a tale scopo si osservi preliminarmente che, applicando la definizione di prodotto di Cauchy, si ha

$$X^2 = (0_A, 1_A, 0_A, \to)(0_A, 1_A, 0_A, \to) = (0_A, 0_A, 1_A, 0_A, \to).$$

Dunque, per ogni $c \in A$, abbiamo che

$$\overline{c}X^2 = (c, 0, \to)(0_A, 0_A, 1_A, 0_A, \to) = (0, 0, c, 0, \to)$$

come richiesto. □

* Versione 10.5.2017

Notazione. Per brevità scriveremo c al posto di $\bar{c} = f(c) = (c, 0, \to)$, quando non sia necessario altrimenti. Con tale notazione e per 3.2, ogni elemento di P_A è del tipo $c_0 + c_1X + c_2X^2 + \ldots + c_nX^n$.

Definizione. Un'espressione del tipo $c_0 + c_1X + c_2X^2 + \ldots + c_nX^n$ con $n \in \mathbb{N}$ si dice *polinomio a coefficienti in A nell'indeterminata X* e l'anello commutativo unitario P_A si dice *anello dei polinomi a coefficienti in A* e verrà indicato con $A[X]$. L'elemento $0_{A[X]}$ si dice *polinomio nullo*, mentre gli elemente del tipo $\bar{c}$, che denoteremo semplicemente con c, sono detti *polinomi costanti*.

Osservazione 3.3. Si noti che nell'anello commutativo unitario $A[X]$ la somma e il prodotto definiti all'inizio del capitolo, sono esattamente le note operazioni tra polinomi. In particolare il prodotto di Cauchy è il ben noto prodotto tra polinomi:

$$\left(\sum_{i=0}^{n} a_iX^i\right)\left(\sum_{j=0}^{m} b_jX^j\right) = \sum_{k=0}^{n+m} c_kX^k$$

dove $c_k := \sum_{i+j=k} a_ib_j$.

Principio di identità dei polinomi 3.4. *Due polinomi in $A[X]$ sono uguali se e solo se i loro coefficienti sono ordinatamente uguali.* □

Definizione. Sia $p(X) = a_0 + a_1X + \ldots + a_nX^n$ un polinomio non nullo in $A[X]$.
Ogni elemento (anch'esso un polinomio) a_iX^i si dice *monomio* e i viene detto il suo *grado*.
Se $a_n \neq 0$, il monomio a_nX^n si dice *monomio (termine) direttore* di $p(X)$ e a_n si dice *coefficiente direttore (direttivo) di $p(X)$*. Diremo infine che n è il *grado* di $p(X)$ e scriveremo $\deg(p) = n$. Se $p(X)$ è il polinomio nullo, poniamo $\deg(p) = -1$.

Si osservi che i polinomi di grado zero sono tutte e sole le costanti non nulle.

Teorema 3.5. *L'anello A è un dominio se e solo se l'anello dei polinomi $A[X]$ è un dominio.*

Dimostrazione. Supponiamo che A sia un dominio e consideriamo due generici polinomi non nulli, di gradi n e m rispettivamente:

$$f(X) = \sum_{i=0}^{n} a_iX^i, \quad g(X) = \sum_{j=0}^{m} b_jX^j.$$

Per 3.3 il loro prodotto è un polinomio avente come monomio direttore $a_nb_mX^{n+m}$, che è non nullo in quanto $a_n \neq 0_A$ e $b_m \neq 0_A$ per ipotesi e $a_nb_m \neq 0_A$ in quanto A è un dominio. Dunque il prodotto di $f(X)$ e $g(X)$ è non nullo.
Viceversa, A è un sottoanello di $A[X]$ per 3.1 e $A[X]$ è un dominio per ipotesi. Quindi A è un dominio. □

Proposizione 3.6. *(Formula del grado). Siano $f(X)$ e $g(X)$ due elementi di $A[X]^*$, tali che la loro somma e il loro prodotto non siano nulli. Allora valgono le seguenti disuguaglianze:*

$$\deg(f + g) \leq \max[\deg(f), \deg(g)] \tag{3}$$

$$\deg(fg) \leq \deg(f) + \deg(g). \tag{4}$$

In particolare, se A è un dominio, vale

$$\deg(fg) = \deg(f) + \deg(g). \tag{4bis}$$

Dimostrazione. Siano $f(X) = \sum_{i=0}^{n} a_i X^i$ e $g(X) = \sum_{j=0}^{m} b_j X^j$ con $\deg(f) = n$ e $\deg(g) = m$. Supponiamo $n \geq m$. Dalla definizione di somma tra polinomi si ha

$$f(X) + g(X) = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{n} (a_i + b_i) X^i$$

dove si è posto, ovviamente, $b_i = 0$ per ogni $i = m+1, \ldots, n$. Chiaramente tale polinomio ha grado al più $n = \max[\deg(f), \deg(g)]$ e questo prova la (3) (si osservi che il grado potrebbe essere strettamente minore nel caso in cui $n = m$ e $a_n + b_n = 0$).
Siano $f(X)$ e $g(X)$ come sopra. Per definizione di prodotto di Cauchy tra polinomi si ha che

$$f(X)g(X) = \sum_{i=0}^{n+m} c_i X^i, \quad \text{dove} \quad c_i = \sum_{r+s=i} a_r b_s.$$

Chiaramente tale polinomio ha grado al più $n + m = \deg(f) + \deg(g)$ e questo prova la (4).
Infine, se A è un dominio, allora $a_n \neq 0 \neq b_m$ implica che anche $c_{n+m} = a_n b_m$ è non nullo e dunque è il coefficiente direttore del polinomio prodotto $f(X)g(X)$. Pertanto anche (4*bis*) è dimostrata. □

Esempio 3.6.1. Si considerino i seguenti polinomi in $\mathbb{Z}_6[X]$:

$$f(X) = \bar{2}X \quad \text{e} \quad g(X) = \bar{3}X + \bar{1}$$

È facile vedere che $\deg(f(X) \cdot g(X)) = 1 \leq 2 = \deg(f(X)) + \deg(g(X))$.

Esempio 3.6.2. Sia $j : \mathbb{Z} \hookrightarrow \mathbb{R}$ l'inclusione canonica. Questa induce l'omomorfismo iniettivo di anelli

$$i : \mathbb{Z}[X] \longrightarrow \mathbb{R}[X]$$

definito da: $n \mapsto j(n)$ se $n \in \mathbb{Z}$, $X \mapsto X$ ed esteso in modo polinomiale. Più semplicemente, l'inclusione $\mathbb{Z} \subset \mathbb{R}$ induce una inclusione $\mathbb{Z}[X] \subset \mathbb{R}[X]$.
Vedremo che tale situazione si generalizza a un omomorfismo qualunque tra anelli.

Polinomi invertibili, irriducibili e primi

Se non diversamente indicato, si assume che A sia un dominio di integrità.

Ci poniamo il problema di individuare gli elementi invertibili di $A[X]$. Chiaramente, se $a \in A$ è invertibile in A, lo è anche in $A[X]$.

Viceversa, sia $f(X) \in A[X]$ un elemento invertibile; allora esiste $g(X) \in A[X]$ tale che $f(X)g(X) = 1_{A[X]} = 1_A$. Applicando la Formula del grado (4*bis*) di 3.6, abbiamo che

$$\deg(f(X)) + \deg(g(X)) = \deg(f(X)g(X)) = \deg(1_A) = 0.$$

Quindi necessariamente $\deg(f(X)) = \deg(g(X)) = 0$. Ne segue che il polinomio $f(X)$ ha grado zero, ovvero è un polinomio costante diverso dal polinomio nullo. E come elemento di A deve essere invertibile.

Abbiamo così provato la seguente:

Proposizione 3.7. *Sia A un dominio. Allora $\mathcal{U}(A[X]) = \mathcal{U}(A)$.* □

Esempio 3.7.1. In $\mathbb{R}[X]$ i polinomi invertibili sono tutti e soli le costanti non nulle.
In $\mathbb{Z}[X]$ i polinomi invertibili sono i polinomi costanti 1 e -1.

Esempio 3.7.2. Si consideri il polinomio $f(X) = \bar{2}X + \bar{1} \in \mathbb{Z}_4[X]$. Si calcola facilmente che $(f(X))^2 = \bar{1}$, ovvero $f(X)$ ha come inverso se stesso. Quindi è invertibile anche se non è costante. Questo accade perchè $\mathbb{Z}_4$ non è un dominio, quindi non si applica 3.7.

Corollario 3.8. *In $A[X]$ due polinomi $f(X)$ e $g(X)$ sono associati se e solo se esiste $u \in \mathcal{U}(A)$ tale che $f(X) = ug(X)$.*

Dimostrazione. Per 2.15, $f(X), g(X) \in A[X]$ sono associati se e solo se esiste $u(X) \in \mathcal{U}(A[X])$ tale che $f(X) = u(X)g(X)$. Poiché A è integro, per 3.7 si ha $\mathcal{U}(A[X]) = \mathcal{U}(A)$, da cui la tesi. □

Esempio 3.8.1. Poichè gli elementi invertibili di $\mathbb{Z}$ sono 1 e -1 allora, come precedentemente osservato, $\mathcal{U}(\mathbb{Z}[X]) = \mathcal{U}(\mathbb{Z}) = \{1, -1\}$. Dunque $f(X), g(X) \in \mathbb{Z}[X]$ sono elementi associati se e solo se $f(X) = \pm g(X)$.

Esempio 3.8.2. Sia K un campo e siano $f(X), g(X) \in K[X]$. Allora $f(X)$ e $g(X)$ sono associati se e solo se $f(X) = cg(X)$, dove $c \in K^*$.

Definizione. Un polinomio in $A[X]$ si dice *monico* se il suo coefficiente direttivo è 1_A.

Osservazione 3.9. Verifichiamo che $f(X)$ è associato ad un polinomio monico se e solo se il coefficiente direttivo di $f(X)$ è invertibile in A.
Infatti, se $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ è associato a un polinomio monico $g(X) = \sum_{i=0}^{m} b_i X^i \in A[X]$ con $b_m = 1$ allora per 3.8 possiamo scrivere $f(X) = u \cdot g(X)$ per qualche $u \in \mathcal{U}(A)$.
Risulta allora che $n = m$ e che $a_i = ub_i$ per ogni i. In particolare $a_n = ub_n$ ossia il coefficiente direttore di $f(X)$ è un elemento invertibile di A.
Viceversa, supponiamo che il coefficiente direttore a_n di $f(X)$ sia invertibile in A. Questo conduce a definire $g(X) := a_n^{-1} f(X) = \sum_{i=0}^{n} a_n^{-1} a_i X^i$, il cui coefficiente direttore è $a_n^{-1} a_n = 1_A$. Quindi $f(X)$ è associato a un polinomio monico.

Esempio 3.9.1. In $\mathbb{Q}[X]$ il polinomio $2X^2 + 7X$ è associato al polinomio monico $X^2 + (7/2)X$. Mentre in $\mathbb{Z}[X]$ lo stesso polinomio $2X^2 + 7X$ non è associato ad alcun polinomio monico.

Le nozioni di *irriducibile* e di *primo* in un anello di polinomi sono identiche a quelle relative ad un anello qualunque. Tuttavia le ricordiamo, esprimendole nel linguaggio dei polinomi.

Definizione. Un polinomio $f(X) \in A[X]$ è *irriducibile* se è non nullo, non invertibile e se $f(X) = g(X)h(X)$ implica che uno tra g ed h è invertibile.
Un polinomio $f(X) \in A[X]$ è *riducibile* se è nullo oppure se è invertibile oppure se si può scrivere come $f(X) = g(X)h(X)$ con $f(X), g(X) \notin \mathcal{U}(A)$.

Osservazione 3.10. In $A[X]$ i polinomi monici di primo grado sono irriducibili.
Infatti, sia $p(X) = X - \alpha$ con $\alpha \in A$. Se fosse $p(X) = f(X)g(X)$, per la Formula del grado ($4bis$), $1 = \deg(p) = \deg(f) + \deg(g)$; dunque uno tra $f(X)$ e $g(X)$ sarebbe costante. Ad esempio, sia $f(X) = c \in A$ e $\deg(g(X)) = 1$. Quindi $X - \alpha = c(aX + b)$ e dunque $ca = 1_A$; pertanto c è invertibile.

Esempio 3.10.1. Un polinomio di primo grado, se non monico, può essere riducibile. Ad esempio, in $\mathbb{Z}[X]$, il polinomio $p(X) = 3X$ è riducibile infatti $3X = 3 \cdot X$ e sia 3 che X non sono invertibili in $\mathbb{Z}[X]$.

Definizione. Un polinomio si dice *primo* se è non nullo, non invertibile e se $f(X) \mid g(X)h(X)$ implica che $f(X) \mid g(X)$ oppure $f(X) \mid h(X)$.

Nel prossimo paragrafo studieremo le proprietà dell'anello dei polinomi a coefficienti in un campo. Il primo risultato significativo riguarderà la divisione euclidea che si può operare in analogia con quella vista per $\mathbb{Z}$ nel capitolo 2. Tuttavia tale teorema vale più in generale per i polinomi a coefficienti in un dominio (anche se non per tutti...). Pertanto è il risultato conclusivo di questa sezione. Vedremo le sue conseguenze nel paragrafo successivo, nel contesto dei polinomi a coefficienti in un campo.

Teorema 3.11. *(Algoritmo della divisione euclidea). Sia A un dominio. Se $f(X)$ e $g(X)$ sono due polinomi non nulli in $A[X]$ e il coefficiente direttivo di $g(X)$ è invertibile allora esistono e sono unici due polinomi $q(X)$ ed $r(X)$ in $A[X]$ tali che*

$$f(X) = g(X)q(X) + r(X), \quad con \quad \deg(r(X)) < \deg(g(X)).$$

Dimostrazione. Ci sono due possibilità: o $\deg(f) < \deg(g)$ o $\deg(f) \geq \deg(g)$. Denoteremo questi due passi–base dell'algoritmo con (I) e (II).

(I) Se $\deg(f) < \deg(g)$ basta porre $q(X) = 0$ e $r(X) = f(X)$.

(II) Siano $\deg(f) = n, \deg(g) = m$ con $n \geq m$. Siano a_n e b_m rispettivamente i coefficienti direttori di $f(X)$ e $g(X)$ e si ponga $q_1(X) := a_n b_m^{-1} X^{n-m}$. Consideriamo

$$f_1(X) := f(X) - q_1(X)g(X).$$

Se $f_1(X)$ è non nullo allora ha grado minore di n. Se il grado di $f_1(X)$ risulta essere anche minore di m, procediamo col passo (I) applicato alla coppia f_1 e g.
Se invece $\deg(f_1) = n_1 \geq m$, procediamo col passo (II) applicato alla coppia f_1 e g, costruendo in modo analogo $q_2(X)$ e il polinomio

$$f_2(X) := f_1(X) - q_2(X)g(X).$$

Come prima, se $f_2(X)$ è non nullo allora ha grado minore di n_1.
Iterando il procedimento si costruisce una successione di polinomi non nulli $f_i(X)$ che non può essere infinita. Infatti

$$\deg(f) > \deg(f_1) > \deg(f_2) > \cdots > \deg(f_s) > \cdots$$

Per il Principio del minimo in $\mathbb{N}$, esiste un $k \in \mathbb{N}$ tale che $f_k(X) = 0$ oppure $\deg(f_k(X)) < m$. Pertanto

$$\begin{aligned} f(X) &= f_1(X) + q_1(X)g(X) \\ f_1(X) &= f_2(X) + q_2(X)g(X) \\ &\cdots \\ f_{k-1}(X) &= f_k(X) + q_k(X)g(X) \end{aligned}$$

Dunque

$$f(X) = g(X)[q_1(X) + q_2(X) + \cdots + q_k(X)] + f_k(X)$$

dove $f_k(X) = 0$ oppure $\deg(f_k) < \deg(g)$. Ponendo $q(X) := q_1(X) + q_2(X) + \cdots + q_k(X)$ e $r(X) := f_k(X)$ si è provata l'esistenza di quoziente e resto della divisione di $f(X)$ per $g(X)$.
Dimostriamo ora l'unicità di tali $q(X)$ e $r(X)$. Supponiamo che

$$g(X)q(X) + r(X) = f(X) = g(X)\bar{q}(X) + \bar{r}(X).$$

Allora si avrebbe

$$g(X)[q(X) - \bar{q}(X)] = \bar{r}(X) - r(X).$$

Quindi, se $\bar{r}(X) \neq r(X)$, per la formula del grado nel dominio $A[X]$ (vedi (4bis) in 3.6), si ha

$$\deg(\bar{r} - r) = \deg(g) + \deg(q - \bar{q}).$$

D'altra parte, sempre per la formula del grado, vale $\deg(\bar{r} - r) \leq \max[\deg(\bar{r}, \deg(r)] < \deg(g)$. Si arriva quindi a un assurdo. Pertanto deve essere $\bar{r}(X) = r(X)$.
Infine si osservi che, dato che $A[X]$ è un dominio e $g(X)$ è non nullo, allora $\bar{r}(X) - r(X) = 0$ se e solo se $q(X) - \bar{q}(X) = 0$. Questo conclude la dimostrazione. □

Si noti che la condizione $\deg(r(X)) < \deg(g(X))$ espressa nell'enunciato precedente comprende il caso in cui $r(X)$ è nullo e dunque ha grado -1.

In questa sezione, K denoterà un campo.

È chiaro che le ipotesi del Teorema 3.11 sono soddisfatte se il dominio dei coefficienti è K. Pertanto è immediato il seguente risultato.

Proposizione 3.12. *Se $f(X)$ e $g(X)$ sono due polinomi non nulli in $K[X]$ allora esistono, e sono unici, due polinomi $q(X), r(X) \in K[X]$ tali che*

$$f(X) = g(X)q(X) + r(X), \quad \textit{con} \quad \deg(r(X)) < \deg(g(X)).$$ □

Esempio 3.12.1. Determiniamo quoziente e resto della divisione di $f(X)$ per $g(X)$, dove

$$f(X) = 3X^3 - 2X^2 + 2X + 2 \quad \text{e} \quad g(X) = X^2 - X + 1$$

sono polinomi a coefficienti in $\mathbb{Q}$. Calcoliamo

$$q_1(X) = a_n b_m^{-1} X^{n-m} = 3 \cdot 1 \cdot X^{3-2} = 3X.$$

Quindi

$$\begin{aligned} f_1(X) &= f(X) - g(X)q_1(X) = \\ &= (3X^3 - 2X^2 + 2X + 2) - (3X^3 - 3X^2 + 3X) = \\ &= X^2 - X + 2. \end{aligned}$$

In questo caso $\deg(f_1) = \deg(g)$. Quindi si deve operare ancora una divisione e calcolare $q_2(X)$; ma essendo entrambi i polinomi monici, otteniamo che $q_2(X) = 1$. Dunque

$$\begin{aligned} f_2(X) &= f_1(X) - g(X)q_2(X) = \\ &= X^2 - X + 2 - (X^2 - X + 1) = \\ &= 1. \end{aligned}$$

La divisione di $f(X)$ per $g(X)$ è quindi

$$f(X) = g(X)q_1(X) + f_1(X) = g(X)q_1(X) + g(X)q_2(X) + f_2(X) = g(X)[q_1(X) + q_2(X)] + f_2(X)$$

cioè

$$f(X) = g(X)(3X + 1) + 1.$$

Anche il seguente risultato riprende l'analogia tra $K[X]$ e $\mathbb{Z}$: il fatto di avere un algoritmo di divisione euclidea implica che un anello di polinomi a coefficienti in un campo è anch'esso un dominio euclideo e dunque a ideali principali.

Corollario 3.13. *L'anello $(K[X], \delta)$, ove $\delta(p(X)) := \deg(p(X))$ per ogni $p(X) \in K[X]^*$, è euclideo.*

Dimostrazione. Basta osservare che δ è una valutazione euclidea per 3.6 (4bis) e per 3.12. □

Teorema 3.14. *Sia K un campo. Allora:*
i) l'anello dei polinomi $K[X]$ è un PID;
ii) per ogni ideale non nullo $I \subseteq K[X]$ esiste un unico polinomio monico $p(X) \in I$ di grado minimo in I e vale $I = (p(X))$.

Dimostrazione. (i) Segue dal fatto che $K[X]$ è euclideo e da 2.55.
(ii) Per (i), esiste un polinomio non nullo tale che $I = (f(X))$. Per 3.9, poiché il coefficiente direttivo di f è invertibile, $f(X)$ è associato ad un polinomio monico $p(X)$ e chiaramente $I = (p(X))$.
Resta da mostrare che p è di grado minimo in I e che è unico a soddisfare queste proprietà.
Sia $g(X) \in I$, dunque $g(X) = p(X)a(X)$. Per la Formula del grado, $\deg(g) = \deg(p) + \deg(a)$ e quindi $\deg(g) \geq \deg(p)$.
Supponiamo infine che $q(X) \in I$ sia monico e di grado minimo in I. Quindi $\deg(q) = \deg(p)$ e, per quanto visto prima $q(X) = p(X)a(X)$, dove $\deg(a(X)) = 0$. Pertanto $a(X)$ è una costante $a \in K$. Ma l'uguaglianza $q(X) = ap(X)$ e il fatto che $p(X)$ e $q(X)$ siano monici implicano che $a = 1$. □

Esempio 3.14.1. Come visto ora, se K è un campo allora $K[X]$ è un PID. Ci chiediamo se succede anche in altri casi, cioè quando l'anello dei coefficienti non è un campo.
Ad esempio, ci chiediamo se $\mathbb{Z}[X]$ è un PID. Consideriamo a tale scopo i polinomi $f, g \in \mathbb{Z}[X]$, dove

$$f(X) = X^2, \quad g(X) = X + 1.$$

Dividendo $f(X)$ per $g(X)$ si ottiene $X^2 = (X-1)(X+1) + 1$ e dunque vale l'identità di Bézout: $1 = f(X) + (1-X)g(X)$. Pertanto l'ideale $(f(X), g(X))$ è principale e generato da 1. Si considerino ora

$$p(X) = X^2, \quad q(X) = 2X + 1.$$

Non si può dividere p per q, in quanto il coefficiente direttivo di $q(X)$ non è invertibile in $\mathbb{Z}$ e quindi non si può applicare l'algoritmo della divisione euclidea 3.11. Pertanto l'ideale $(p(X), q(X)) = (X^2, 2X + 1)$ non è principale. Si conclude che $\mathbb{Z}[X]$ non è un PID.

Infine ancora una analogia: come per $\mathbb{Z}$ (e per ogni PID: vedi 2.44), anche in $K[X]$ esiste un massimo comun divisore fra due elementi. Ricordiamo che in $\mathbb{Z}$ esso è unico a meno del segno (vedi 2.7). In $K[X]$ è unico a meno di un coefficiente moltiplicativo non nullo (vedi Corollario 3.8); se si richiede che sia monico, è proprio unico. Quindi si ha come diretta conseguenza dei teoremi che riguardano i PID, la seguente proprietà.

Corollario 3.15. *Siano $f(X)$ e $g(X)$ due polinomi a coefficienti in un campo K non nulli. Allora esiste un massimo comune divisore di $f(X)$ e $g(X)$. Precisamente:*

$$d(X) = MCD(f, g) \iff (f(X), g(X)) = (d(X))$$

Pertanto esistono $a(X), b(X) \in K[X]$ tali che $d(X) = a(X)f(X) + b(X)g(X)$. □

Infine si può costruire un algoritmo, simile a quello visto in $\mathbb{Z}$ (vedi 2.8), che permette di determinare il MCD di due polinomi in modo costruttivo. La dimostrazione è del tutto analoga.

Teorema 3.16. *(Algoritmo delle divisioni successive). Siano $f(X)$ e $g(X)$ due polinomi non nulli di $K[X]$. Si considerino le divisioni successive, dove $r_0(X) := g(X)$:*

$$\begin{aligned} f(X) &= g(X)q_1(X) + r_1(X) \\ g(X) &= r_1(X)q_2(X) + r_2(X) \\ r_1(X) &= r_2(X)q_3(X) + r_3(X) \\ &\cdots \\ r_{n-1}(X) &= r_n(X)q_{n+1}(X). \end{aligned}$$

Allora $MCD(f, g) = r_n(X)$. □

Tale algoritmo permette anche di calcolare i coefficienti della corrispondente identità di Bézout.

Esempio 3.16.1. Applichiamo l'algoritmo 3.16 nel caso numerico in cui $K = \mathbb{Q}$,

$$f(X) = X^4 - X^3 - 4X^2 + 4X + 1 \quad \text{e} \quad g(X) = X^2 - X - 1.$$

Ripercorrendo i passaggi precedenti si ottiene

$$\begin{aligned} f(X) &= g(X)(X^2 - 3) + (X - 2) \\ g(X) &= (X - 2)(X + 1) + 1 \\ X - 2 &= 1(X - 2). \end{aligned}$$

Visto che l'ultimo resto non nullo è 1, ne segue che $MCD(f(X), g(X)) = 1$.
In particolare, per 3.16, $(f, g) = (1)$ dunque vale l'identità di Bézout: esistono $\alpha(X), \beta(X) \in \mathbb{Q}[X]$ tali che

$$1 = \alpha(X)f(X) + \beta(X)g(X).$$

Per calcolare i coefficienti di Bézout si utilizzano le divisioni successive operate prima:

$$\begin{cases} 1 &= g(X) - (X-2)(X+1) \\ X - 2 &= f(X) - g(X)(X^2 - 3) \end{cases}$$

da cui

$$1 = g(X) - [f(X) - g(X)(X^2 - 3)](X + 1) = -(X + 1)f(X) + [(X^2 - 3)(X + 1) + 1]g(X)$$

I coefficienti cercati sono dunque: $\alpha(X) = -(X + 1)$ e $\beta(X) = (X^2 - 3)(X + 1) + 1$.

Vediamo ora alcuni esempi e osservazioni riguardo alla irriducibilità, invertibilità di polinomi a coefficienti in un campo. Ovviamente valgono le definizioni e i risultati stabiliti per l'anello dei polinomi a coefficienti in un dominio qualunque, visti nel paragrafo precedente.

Ricordiamo che gli elementi invertibili di $K[X]$ sono le costanti non nulle. Inoltre un polinomio $p(X) \in K[X]$ è irriducibile $\Leftrightarrow$ non è prodotto di polinomi, eccetto le costanti non nulle e i polinomi associati a $p(X)$.

Osservazione 3.17. Un polinomio $p(X) \in K[X]$ è riducibile $\Leftrightarrow$ esistono due polinomi $f(X)$ e $g(X)$, con $\deg(f) < \deg(p)$ e $\deg(g) < \deg(p)$, tali che $p(X) = f(X)g(X)$.

Esempio 3.17.1. Vediamo due esempi di fattorizzazione banale e non banale di un polinomio in $\mathbb{Q}[X]$.
Sia $p(X) = X^2 - 1$. Una sua fattorizzazione banale (sempre possibile) è

$$X^2 - 1 = 3\left(\frac{X^2}{3} - \frac{1}{3}\right).$$

Si noti che $3 \in \mathbb{Q}^*$ è invertibile e che il polinomio $\left(\frac{X^2}{3} - \frac{1}{3}\right)$ è associato a $p(X)$. D'altra parte la fattorizzazione $X^2 - 1 = (X + 1)(X - 1)$ è non banale, in quanto entrambi i fattori hanno grado $1 < \deg(p) = 2$ e quindi $p(X)$ è riducibile in $\mathbb{Q}[X]$.

Osservazione 3.18. Se è chiaro quali sono gli elementi invertibili in $K[X]$ (le costanti non nulle), cerchiamo gli elementi invertibili in un anello quoziente di $K[X]$.
Sia I un ideale proprio e non nullo di $K[X]$. Dunque $I = (m(X))$ con $\deg(m(X)) \geq 1$.
Consideriamo l'anello quoziente $A := K[X]/I$ e denotiamo i suoi elementi con $\overline{f(X)} := f(X) + I$.
Cerchiamo di caratterizzare gli elementi invertibili in A.
Per definizione, $\overline{f(X)} \in A$ è invertibile se e solo se esiste $\overline{g(X)} \in A$ tale che $\overline{f(X)g(X)} = \overline{1}$. Ciò vale se e solo se $f(X)g(X) - 1 \in I$ o , equivalentemente, se e solo se esiste $\alpha(X)$ tale che $f(X)g(X) - 1 = \alpha(X)m(X)$, cioè $f(X)g(X) - \alpha(X)m(X) = 1$. Abbiamo dunque provato che

$$\overline{f(X)} \in \mathcal{U}(A) \iff MCD(f(X), m(X)) = 1,$$

cioè gli elementi invertibili in $K[X]/(m(X))$ sono tutte e sole le classi dei polinomi coprimi con $m(X)$.

Esempio 3.18.1. Nell'anello $\mathbb{Q}[X]/(X + 1)$ l'elemento $\overline{f(X)} = \overline{X^2} = \overline{X}^2$ è invertibile? Basta calcolare il $MCD(X^2, X+1)$. Ma tali polinomi sono coprimi (come visto nell'Esempio 3.14.1), dunque $\overline{f(X)}$ è invertibile.

Un'altra situazione tipica degli anelli quoziente, che non si verifica negli anelli di polinomi a coefficienti in un campo, è la presenza di zero divisori.

Osservazione 3.19. Come prima, sia I un ideale proprio e non nullo di $K[X]$. Dunque $I = (m(X))$ con $\deg(m(X)) \geq 1$. Consideriamo l'anello quoziente $A := K[X]/I$. Per quanto visto in 2.26, 2.33, 2.39, si ottiene che A non è integro se e solo se I non è primo se e solo se $m(X)$ non è primo se e solo se $m(X)$ non è irriducibile. Si noti che l'ultima equivalenza vale in un dominio con MCD e $K[X]$ lo è.

Esempio 3.19.1. Sia $I = (X^2 - 1) \subset \mathbb{Q}[X]$. Allora $\mathbb{Q}[X]/I$ non è integro. Infatti, posti $f(X) = X + 1$ e $g(X) = X - 1$, si ha che

$$f(X) \notin I,\ g(X) \notin I \quad \Rightarrow \quad \overline{f(X)} \neq \overline{0},\ \overline{g(X)} \neq \overline{0}.$$

Ma

$$f(X)g(X) \in I \quad \Rightarrow \quad \overline{f(X)}\,\overline{g(X)} = \overline{f(X)g(X)} = \overline{0}.$$

Ricordiamo che $K[X]$ è un PID per 3.14; di conseguenza è un UFD per 2.46.
Tuttavia enunciamo tale importante risultato nel linguaggio dei polinomi. Lasciamo al lettore la verifica che i fattori irriducibili di un polinomio possono essere scelti monici.

Teorema 3.20. *(Fattorizzazione unica). Se K è un campo e $f(X) \in K[X]$ con $\deg(f) > 0$ allora esistono $c \in K^*$ e $p_1(X), \ldots, p_n(X)$ polinomi monici e irriducibili tali che*

$$f(X) = c\,p_1(X) \cdots p_n(X)$$

e tale fattorizzazione è unica, a meno dell'ordine dei fattori. □

Se A è un qualunque anello (commutativo unitario), abbiamo definito l'anello $A[X]$ dei polinomi a coefficienti in A nell'indeterminata X. Se al posto di A consideriamo $A[X]$, possiamo analogamente definire l'anello dei polinomi nell'indeterminata Y a coefficienti in $A[X]$ e denotarlo con

$$A[X,Y] := (A[X])[Y].$$

Ovviamente anche quest'ultimo è un anello commutativo unitario e il suo generico elemento è:

$$f(X,Y) = \sum_{j=0}^{m} f_j(X)Y^j = \sum_{j=0}^{m} \left(\sum_{i=0}^{h_j} a_{ij}X^i \right) Y^j = \sum_{\substack{i=0,\dots,n \\ j=0,\dots,m}} a_{ij}X^iY^j$$

dove nell'ultima uguaglianza si è posto $n := \max\{h_1, \dots, h_m\}$, avendo denotato con h_j il grado del polinomio $f_j(X)$, per ogni $j = 0, \dots, m$.

In modo del tutto analogo si procede nel costruire l'anello dei polinomi in più indeterminate. Diamo dunque la seguente definizione ricorsiva:

Proposizione - Definizione 3.21. *Sia A un anello e $X_1, \dots, X_n$ indeterminate su A. Si pongano:*

$$\begin{aligned} A_1 &:= A[X_1] \\ A_2 &:= A_1[X_2] \\ &\dots \\ A_n &:= A_{n-1}[X_n] \end{aligned} \quad .$$

Allora A_n, con le consuete operazioni di somma e prodotto, è un anello commutativo unitario detto anello di polinomi a coefficienti in A nelle indeterminate $X_1, \dots, X_n$ e denotato con $A[X_1, \dots, X_n]$.
Il suo generico elemento si dice polinomio a coefficienti in A nelle indeterminate $X_1, \dots, X_n$ e ha la forma

$$f(X_1, \dots, X_n) = \sum a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

dove la somma è intesa per $i_1 = 0, \dots, k_1$, $i_2 = 0, \dots, k_2$ fino a $i_n = 0, \dots, k_n$.

Dimostrazione. Poiché A è un anello commutativo unitario, allora per 3.2 anche A_1 lo è. Applicando ripetutamente il citato risultato, si ottiene che ogni A_i è un anello commutativo unitario. □

Ci sono naturalmente molte analogie tra i polinomi in più variabili e quelli in una.
Ad esempio, vale ancora il Principio di d'identità dei polinomi (che segue da Principio d'identità per i polinomi in una variabile, iterando):

$$f(X_1, \dots, X_n) \equiv 0 \iff \text{tutti i coefficienti di } f \text{ sono nulli.}$$

Inoltre si può ancora parlare di grado, anche se l'analogia col caso di polinomi in una variabile non è totale, come vedremo. È naturale, infatti, dire che il polinomio di $\mathbb{R}[X,Y]$ dato da $X^2Y^3 + 2XY - 7$ ha grado 5. Diamo dunque le seguenti nozioni.

Definizione. Come nel caso di una variabile, si dice *monomio* un polinomio del tipo $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$, dove $a \in A$ si dice *coefficiente del monomio*. Se $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$ è un monomio non nullo (cioè $a \neq 0$) si dice *grado del monomio* l'intero positivo $\alpha_1 + \cdots + \alpha_n$. Infine se $f(X_1, \dots, X_n) \in A[X_1, \dots, X_n]^*$ diremo *grado di f* il massimo grado dei monomi che lo compongono e verrà denotato con $\deg(f(X_1, \dots, X_n))$. Se $f \equiv 0$, come al solito si pone $\deg(f(X_1, \dots, X_n)) = -1$.

Osservazione 3.22. Tuttavia non è sempre possibile individuare un *monomio massimo rispetto al grado* in un polinomio in più variabili.

Esempio 3.22.1. In $\mathbb{R}[X,Y]$ si consideri il polinomio $f(X,Y) = X^2Y^7 + X^3Y^6 - 5XY$. Per la definizione precedente, $\deg(f) = 9$. Ma non è individuato il monomio massimo di f. Occorre decidere quale tra X^2Y^7 e X^3Y^6 è il più grande. A tale scopo, bisogna introdurre una nozione più complessa di quella di "grado".

Notazione - Definizione. Per brevità denoteremo la n-upla delle indeterminate con $\overline{X} = (X_1, \dots, X_n)$, detto *vettore delle indeterminate*.
Se $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$ è un monomio di $A[X_1, \dots, X_n]$, la n-upla $\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ si chiama *multigrado* del monomio e si denota con "mdeg".
Con tale convenzione il monomio suddetto si denota con $a\overline{X}^{\alpha}$ e di scrive $\mathrm{mdeg}(a\overline{X}^{\alpha}) = \alpha$.
Il generico polinomio $f(X_1, \dots, X_n) = \sum a_{\alpha_1 \dots \alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ è una somma di monomi. In ognuno di essi il coefficiente è dotato di un *multiindice* $\alpha_1 \dots \alpha_n$ che coincide col multigrado del monomio. In tal modo la scrittura di un polinomio $f(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ risulta più compatta: $f(\overline{X}) \in A[\overline{X}]$ è della forma

$$f(\overline{X}) = \sum a_{\alpha} \overline{X}^{\alpha}$$

con $a_\alpha \in A$ e $\alpha \in \mathbb{N}^n$.

Tuttavia non è immediato definire il "multigrado" di un polinomio. Come visto sopra, il multigrado di un monomio è una n-upla di numeri naturali. Ma in un polinomio che sia somma di vari monomi, nasce l'esigenza di determinare il monomio "massimo" e quindi il multigrado del polinomio.

Nell'esempio 3.22.1, per decidere se $X^2Y^7 < X^3Y^6$ oppure $X^2Y^7 > X^3Y^6$ bisogna scegliere un ordine su $\mathbb{N}^2$. Uno dei più noti e semplici ordinamenti è quello lessicografico.

Definizione. L'*ordine lessicografico* in $\mathbb{N}^n$ è definito da:

$$(k_1, \dots, k_n) <_{lex} (h_1, \dots, h_n) \iff k_s < h_s, \text{ dove } s \text{ è il più piccolo } i \text{ per cui } k_i \neq h_i.$$

Esempio 3.22.2. In $\mathbb{N}^2$ si ha che $(2,7) <_{lex} (3,6)$. In $\mathbb{N}^4$, sempre con l'ordine lessicografico, si verifica che $(2,4,3,5) <_{lex} (2,4,4,1)$.

In modo naturale, un ordine in $\mathbb{N}^n$ induce un ordine su monomi di $A[X_1, \dots, X_n]$.

Definizione. L'*ordine lessicografico* sui monomi di $A[X_1, \dots, X_n]$ è definito da:

$$\overline{X}^{\alpha} < \overline{X}^{\beta} \iff \alpha <_{lex} \beta.$$

dove α e β sono i multiindici dei monomi $\overline{X}^{\alpha}$ e $\overline{X}^{\beta}$.

Osservazione 3.23. L'ordine lessicografico (sia in $\mathbb{N}^n$ sia nell'insieme dei monomi) è un ordine *totale*: cioè due monomi sono sempre confrontabili.

Esempio 3.23.1. Abbiamo visto in 3.22.2 che $(2,7) <_{lex} (3,6)$, dunque $X^2Y^7 < X^3Y^6$.
Inoltre abbiamo visto che $(2,4,3,5) <_{lex} (2,4,4,1)$, dunque $X_1^2X_2^4X_3^3X_4^5 < X_1^2X_2^4X_3^4X_4^1$.

Definizione. Una volta fissato un ordine in $\mathbb{N}^n$ (e quindi sui monomi) se $f(\overline{X}) = \sum_{k=0}^{n} a_k \overline{X}^k$ è un polinomio non nullo in n variabili, si dice *monomio direttore* il suo monomio massimo e il suo coefficiente si dice *coefficiente direttivo* di f. Infine diremo *multigrado di f* il massimo dei multigradi dei suoi monomi.

Enunciamo, senza dimostrarlo, il risultato analogo di 3.6.

Teorema 3.24. *(Formula del multigrado). Siano $f(\overline{X}), g(\overline{X}) \in A[\overline{X}]$ due polinomi in n variabili. Allora:*

$$\mathrm{mdeg}(f(\overline{X}) + g(\overline{X})) \leq \max\{\mathrm{mdeg}(f(\overline{X})), \mathrm{mdeg}(g(\overline{X}))\}$$

$$\mathrm{mdeg}(f(\overline{X})g(\overline{X})) \leq \mathrm{mdeg}(f(\overline{X})) + \mathrm{mdeg}(g(\overline{X}))$$

Inoltre, se A è un dominio e $f(\overline{X})g(\overline{X}) \neq 0$, vale

$$\mathrm{mdeg}(f(\overline{X})g(\overline{X})) = \mathrm{mdeg}(f(\overline{X})) + \mathrm{mdeg}(g(\overline{X})). \qquad \square$$

È naturale chiedersi se l'ordine lessicografico dei monomi è compatibile col grado.

Osservazione 3.25. Si noti che il grado induce un ordinamento "parziale" nell'insieme dei monomi, cioè ci sono monomi diversi con lo stesso grado. Si potrebbe pensare che il multigrado genera un ordinamento più fine di quello del grado, ma non è così. Vediamo alcuni esempi.

Esempio 3.25.1. In 3.22.1 abbiamo considerato il polinomio $f(X,Y) = X^2Y^7 + X^3Y^6 - 5XY$. In questo caso

$$\deg(X^2Y^7) = \deg(X^3Y^6) = 9 \quad \text{ma} \quad X^2Y^7 <_{lex} X^3Y^6$$

pertanto il monomio massimo di f è X^3Y^6 e quindi

$$\deg(f(X,Y)) = 9 \quad \text{e} \quad \text{mdeg}(f(X,Y)) = (3,6).$$

Si osservi che il monomio massimo è tra quelli di grado massimo , in quanto $3+6 = 9 = \deg(f(X,Y))$.

Esempio 3.25.2. Consideriamo ora il polinomio a coefficienti reali $g(X,Y) = X^2Y^5 + X^3Y^3 + 2XY$. Il suo monomio di grado massimo è il primo (ed è unico in questo esempio) ed ha grado 7. Ma con l'ordinamento lessicografico:

$$XY <_{lex} X^2Y^5 <_{lex} X^3Y^3.$$

Quindi

$$\deg(g(X,Y)) = 7 \quad \text{e} \quad \text{mdeg}(g(X,Y)) = (3,3).$$

In questo caso il monomio massimo non è tra quelli di grado massimo , in quanto $3+3 \neq 7 = \deg(g(X,Y))$.

Campo dei quozienti di un anello di polinomi

Abbiamo osservato in precedenza che, se A è un dominio, l'anello di polinomi $A[\overline{X}]$ nelle indeterminate $\overline{X} = (X_1, \ldots, X_n)$ è un dominio.

Definizione. Sia A un dominio. Allora il campo dei quozienti di $A[\overline{X}]$, cioè

$$Q(A[\overline{X}]) = \left\{ \frac{f(\overline{X})}{g(\overline{X})} \;\middle|\; f, g \in A[\overline{X}], g \neq 0 \right\}$$

è detto *campo delle funzioni razionali a coefficienti in A nelle indeterminate $X_1, \ldots, X_n$.*

Notazione. Se K è un campo, indicheremo $Q(K[\overline{X}])$ anche con $K(\overline{X})$.

Ad esempio, i campi delle funzioni razionali a coefficienti, rispettivamente, in $\mathbb{Q}$ e $\mathbb{R}$, sono $\mathbb{Q}(\overline{X})$ e $\mathbb{R}(\overline{X})$. Ma anche $\mathbb{Z}[\overline{X}]$ è un dominio; dunque esiste il suo campo dei quozienti. Il seguente risultato lo descrive.

Proposizione 3.30. *Sia A un dominio e $\overline{X} = (X_1, \ldots, X_n)$ un vettore d'indeterminate. Allora*

$$Q(A[\overline{X}]) = Q(A)(\overline{X}).$$

Dimostrazione. Sia $Q(A) := K$. Vogliamo mostrare che $Q(A[\overline{X}]) = K(\overline{X})$.
"$\subseteq$" Poiché $A \subseteq K$ allora $A[\overline{X}] \subseteq K[\overline{X}]$. Dunque, per 0.51 si ha $Q(A[\overline{X}]) \subseteq Q(K[\overline{X}])$. Infine $Q(K[\overline{X}]) = K(\overline{X})$ per definizione.
"$\supseteq$" È sufficiente mostrare che $K[\overline{X}] \subseteq Q(A[\overline{X}])$; infatti, in tal caso, per 0.50 si ha la tesi.
Per semplicità di scrittura, proviamo tale inclusione nel caso di una sola indeterminata. Ogni elemento di $K[X]$ è del tipo $f(X) = \sum_{i=0}^{n} p_i X^i$, con $p_i \in K = Q(A)$. Dunque esistono opportuni $a_i, b_i \in A$ tali che $p_i = a_i/b_i$. Pertanto

$$f(X) = \sum_{i=0}^{n} p_i X^i = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i = \frac{\sum_{i=0}^{n} c_i X^i}{b_0 \ldots b_n}$$

dove $c_i = a_i(b_0 \cdots \hat{b}_i \cdots b_n)$. Chiaramente l'ultimo elemento delle uguaglianze precedenti è un quoziente di polinomi di $A[X]$, cioè appartiene a $Q(A[X])$. □

Esempio 3.30.1. Per il teorema precedente il campo dei quozienti di $\mathbb{Z}[\overline{X}]$ è

$$Q(\mathbb{Z}[\overline{X}]) = Q(\mathbb{Z})(\overline{X}) = \mathbb{Q}(\overline{X}).$$

Concludiamo con una semplice proprietà di immediata dimostrazione.

Proposizione 3.31. *Sia A un anello commutativo unitario. Allora $ch(A) = ch(A[X])$.* □

Osservazione 3.32. Se A è un dominio allora $Q(A)$ ha la stessa caratteristica di A, come visto in 2.21. Da tale fatto, dalla proposizione precedente e da 3.30 segue che

$$ch(A) = ch(A[X]) = ch(Q(A[X])) = ch(Q(A)(X)).$$

Esempio 3.32.1. Sia $A = \mathbb{Z}_p$, con p primo; allora $Q(A) = \mathbb{Z}_p$ per 0.49 (ii) e quindi

$$ch(\mathbb{Z}_p(X)) = ch(\mathbb{Z}_p) = p.$$

Questo è un esempio di un campo infinito con caratteristica finita.

Funzioni polinomiali

In quanto segue A e B denotano due anelli commutativi unitari.

Definizione. Sia A un sottanello di B due anelli, $\overline{X} = (X_1, \ldots, X_n)$ un vettore di n indeterminate e $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$. Se

$$f(\overline{X}) = \sum c_{k_1 \cdots k_n} X_1^{k_1} \cdots X_n^{k_n} \quad \in A[\overline{X}]$$

si dice *valore di $f(\overline{X})$ calcolato in α* l'elemento di B

$$f(\alpha) := \sum c_{k_1 \cdots k_n} \alpha_1^{k_1} \cdots \alpha_n^{k_n}.$$

Proposizione - Definizione 3.33. *Con le notazioni precedenti, l'applicazione*

$$v_\alpha : \quad A[\overline{X}] \longrightarrow B \quad \textit{definita da} \quad v_\alpha\left(f(\overline{X})\right) = f(\alpha)$$

è un omomorfismo d'anelli unitari, detto omomorfismo di valutazione in α.

Dimostrazione. Per semplicità dimostriamo il risultato nel caso $n = 1$. Il ragionamento generale è simile. Sia $\alpha \in B$; dobbiamo provare che, comunque scelti $f(X), g(X) \in A[X]$ si ha:

$$v_\alpha\left(f(X) + g(X)\right) = v_\alpha\left(f(X)\right) + v_\alpha\left(g(X)\right) \quad \text{e} \quad v_\alpha\left(f(X)g(X)\right) = v_\alpha\left(f(X)\right)\ v_\alpha\left(g(X)\right).$$

Siano $f(X) = \sum a_i X^i$ e $g(X) = \sum b_i X^i$. Con la convenzione fatta nella dimostrazione di 3.6, scriviamo semplicemente $f(X) + g(X) = \sum (a_i + b_i) X^i$. Si ha dunque

$$v_\alpha(f(X)) + v_\alpha(g(X)) = f(\alpha) + g(\alpha) = \sum a_i \alpha^i + \sum b_i \alpha^i = \sum (a_i + b_i)\alpha^i = v_\alpha\left(f(X) + g(X)\right).$$

Inoltre, poiché $f(X)g(X) = \sum c_i X^i$, dove i c_i sono i coefficienti ottenuti dal prodotto di Cauchy, si ha

$$v_\alpha(f(x))\, v_\alpha(g(x)) = f(\alpha)\, g(\alpha) = \sum a_i \alpha^i \ \sum b_i \alpha^i = \sum c_i \alpha^i = v_\alpha\left(f(X)g(X)\right)$$

dove la penultima uguaglianza si ottiene con le usuali proprietà delle operazioni nell'anello B.
Resta da verificare che $v_\alpha(1_{A[x]}) = 1_B$. Si osservi dapprima che $1_{A[x]}$ è il polinomio costante 1_A, dunque $v_\alpha(1_{A[x]}) = 1_A$. Ma A è sottoanello di B, quindi $1_A = 1_B$.
Pertanto v_α è un omomorfismo di anelli unitari. □

Nel seguito denoteremo l'immagine della valutazione in α con $A[\alpha] = A[\alpha_1, \ldots, \alpha_n]$; chiaramente è un sottoanello di B, detto *estensione polinomiale di A con $\alpha_1, \ldots, \alpha_n$*.

Proposizione 3.34. *$A[\alpha_1, \ldots, \alpha_n]$ è il più piccolo sottoanello di B contenente A e $\alpha_1, \ldots, \alpha_n$.*

Dimostrazione. Osserviamo che $\mathrm{Im}(v_\alpha) = A[\alpha_1, \ldots, \alpha_n]$ contiene A, infatti per ogni $a \in A$ possiamo considerare il polinomio costante $f(\overline{X}) = a$ e ovviamente $v_\alpha\left(f(\overline{X})\right) = a$. Inoltre $\mathrm{Im}(v_\alpha)$ contiene anche $\alpha_1, \ldots, \alpha_n$ in quanto immagini dei polinomi $X_1, \ldots, X_n$, rispettivamente. Dunque $\mathrm{Im}(v_\alpha)$ è un sottoanello di B contenente A e $\alpha_1, \ldots, \alpha_n$.
Sia ora $V \subseteq B$ un sottoanello contenente A e $\alpha_1, \ldots, \alpha_n$. Poiché V è chiuso rispetto alle operazioni di somma e prodotto di B, deve contenere tutte le espressioni del tipo $\sum c_{k_1 \cdots k_n} \alpha_1^{k_1} \cdots \alpha_n^{k_n}$, con $c_{k_1 \cdots k_n} \in A$. Ma tali espressioni sono esattamente $f(\alpha) = v_\alpha(f(\overline{X}))$, dove $f(\overline{X}) = \sum c_{k_1 \cdots k_n} X_1^{k_1} \cdots X_n^{k_n} \in A[\overline{X}]$.
Quindi $V \supseteq \mathrm{Im}(v_\alpha)$. □

L'omomorfismo di valutazione permette di associare ad un polinomio una funzione in n variabili. Consideriamo, in questa costruzione, il caso in cui $B = A$.

Notazione. Denotiamo con $\mathcal{F}(A^n, A)$ l'insieme delle funzioni da A^n in A.

È facile osservare che, con le operazioni definite puntualmente, cioè per ogni $\phi, \psi \in \mathcal{F}(A^n, A)$ si pone

$$\begin{array}{c} (\phi + \psi)(\alpha) := \phi(\alpha) + \psi(\alpha) \\ (\phi\psi)(\alpha) := \phi(\alpha)\,\psi(\alpha) \end{array} \qquad \text{per ogni } \alpha \in A^n$$

l'insieme $\mathcal{F}(A^n, A)$ è un anello commutativo unitario.

Con le notazioni precedenti, possiamo associare a un polinomio una funzione nel seguente modo

$$\begin{array}{rccc} \varphi: & A[\overline{X}] & \longrightarrow & \mathcal{F}(A^n, A) \\ & f(\overline{X}) & \longrightarrow & \varphi_f: \begin{array}{ccc} A^n & \longrightarrow & A \\ \alpha & \mapsto & f(\alpha) \end{array} \end{array}.$$

Vale il seguente fatto:

Proposizione - Definizione 3.35. *L'applicazione φ è un omomorfismo d'anelli, la cui immagine è detta anello delle funzioni polinomiali su A^n.* □

Esempio 3.35.1. Si osservi che φ non è in generale iniettiva, cioè si possono trovare polinomi diversi ai quali corrisponde la stessa funzione polinomiale. Ad esempio, se A è un anello finito di n elementi $a_1, \ldots, a_n$, il polinomio $f(X) = (X - a_1) \cdots (X - a_n)$ è monico, quindi non nullo, ma si annulla su tutti gli elementi di A. Pertanto φ_f è la funzione nulla. D'altro canto, anche al polinomio nullo corrisponde la funzione nulla, quindi in questo caso φ non è iniettiva. Come esempio numerico, si consideri $f(X) \in \mathbb{Z}_3[X]$ dato da $f(X) = X(X-1)(X-2)$. È non nullo ma la funzione polinomiale da esso indotta è la funzione nulla.

Radici di polinomi

Definizione. Siano $A \subseteq B$ due anelli, $f(X) \in A[X]$ e $\alpha \in B$. Diciamo che α è *radice* di $f(X)$ se $f(\alpha) = 0$.

Osservazione 3.36. Si vede facilmente che:
a) Ogni elemento di A è radice del polinomio nullo.
b) Ogni polinomio costante e non nullo in $A[X]$ non ha radici.
c) Polinomi associati in $A[X]$ hanno le stesse radici.
d) Un polinomio $f(X) \in A[X]$ può avere radici in B e non in A. Ad esempio se A è un dominio e $B = Q(A)$ è il suo campo delle frazioni, un polinomio $f(X) = aX + b \in A[X]$ di primo grado ha sempre una radice in B (ovviamente $-ba^{-1}$) che è radice in A se e solo se a è invertibile in A. Ad esempio $2X + 3 \in \mathbb{Z}[X]$ ha una radice $(-3/2)$ in $\mathbb{Q}$ e nessuna in $\mathbb{Z}$.
e) Se A è integro e $f(X) \in A[X]$ si fattorizza come $f(X) = g(X)h(X)$, allora ogni radice di f è radice di g oppure di h.

Teorema 3.37 (Ruffini, 1809). *Sia A un dominio e $f(X) \in A[X]$ non nullo. Se $\alpha \in A$ allora il resto della divisione di $f(X)$ per il polinomio $(X-\alpha)$ è $f(\alpha)$. In particolare, $(X-\alpha)$ divide $f(X)$ se e solo se α è radice di $f(X)$.*

Dimostrazione. Si divida $f(X)$ per $X-\alpha$:

$$f(X) = (X-\alpha)g(X) + r(X)$$

dove $r(X) \equiv 0$ oppure $\deg(r(X)) < \deg(X-\alpha) = 1$. Quindi il resto $r(X)$ è una costante $r \in A$, nulla o non nulla. Dall'uguaglianza $f(X) = (X-\alpha)g(X) + r$ calcolata in α si ottiene $f(\alpha) = r$, come volevamo. La seconda affermazione è un'immediata conseguenza. □

Se $\alpha \in A$, è chiaro che il nucleo dell'omomorfismo di valutazione $v_\alpha : A[X] \longrightarrow A$ contiene il polinomio $X-\alpha$, e dunque contiene l'ideale principale $(X-\alpha)$. Grazie al Teorema di Ruffini è vero anche il viceversa, purché A sia un dominio. Si ha dunque:

Corollario 3.38. *Se A è un dominio, allora per ogni $\alpha \in A$ l'applicazione*

$$A[X]/(X-\alpha) \longrightarrow A$$

definita da $[f(X)] \mapsto f(\alpha)$ è un isomorfismo di anelli.

Dimostrazione. Basta osservare che l'applicazione in questione è esattamente quella indotta dall'epimorfismo di valutazione $v_\alpha : A[X] \longrightarrow A$ attraverso il Primo Teorema di omomorfismo di anelli, assieme al fatto che $\ker(v_\alpha) = (X-\alpha)$. □

Dal fatto precedente segue che $A[X]/(X-\alpha) \cong A$; essendo A un dominio, anche $A[X]/(X-\alpha)$ lo è. Quindi tutti gli ideali del tipo $(X-\alpha)$ sono primi in $A[X]$ e dunque gli elementi $X-\alpha$ sono primi in tale anello. Da ciò segue immediatamente la seguente

Osservazione 3.39. Si consideri $A[X_1, \ldots, X_n] = B_i[X_i]$, dove $B_i := A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. Per quanto visto, tutti gli elementi del tipo $X_i - \beta_i$, con $\beta_i \in B_i$ sono primi in $A[X_1, \ldots, X_n]$.
In particolare, sono primi i polinomi X_i e anche $X_i \pm X_j$.

Ora alcune interessanti conseguenze del Teorema di Ruffini nel caso di polinomi a coefficienti in un campo.

Proposizione 3.40. *Sia K un campo e $f(X) \in K[X]$ un polinomio non nullo. Allora:*
a) il polinomio $f(X)$ ha una radice in K se e solo se ha un fattore di primo grado in $K[X]$;
b) se $\deg(f) = 1$ allora $f(X)$ è irriducibile;
c) se $\deg(f) = 2$ o 3 allora $f(X)$ è riducibile in $K[X]$ se e solo se ha una radice in K.

Dimostrazione.
a) Se $f(x)$ ha una radice $a \in K$ allora, applicando il Teorema di Ruffini (3.37), risulta $f(X) = (X-a)g(X)$. Viceversa, sia $f(X) = (aX+b)q(X)$ con $\deg(q) \geq 0$ e $a, b \in K$. Si conclude immediatamente dato che $-b/a \in K$ risulta essere radice di $f(X)$.

b) Sia $f(X) = g(X)h(X)$ una fattorizzazione di $f(X)$ in $K[X]$. Applicando la Formula del Grado (3.6) e tenendo conto che K è un dominio, si ha

$$\deg(f) = \deg(g) + \deg(h).$$

Se $\deg(f) = 1$, l'unica possibilità è dunque $\deg(g) = 1$ e $\deg(h) = 0$ (o viceversa). Quindi $f(X)$ è irriducibile.

c) Supponiamo che $f(X) = g(X)h(X)$ sia una fattorizzazione non banale di $f(X)$ in $K[X]$, dunque $\deg(g) \geq 1$ e $\deg(h) \geq 1$.
Come nel caso precedente, vale la Formula del Grado; quindi se $\deg(f) = 2$, l'unica possibilità è $\deg(g) = 1 = \deg(h)$. Pertanto f ha un fattore di primo grado.
Se $\deg(f) = 3$, ci sono due possibilità: o $\deg(g) = 1$ e $\deg(h) = 2$ oppure $\deg(g) = 2$ e $\deg(h) = 1$. Anche in

questo caso f ha un fattore di primo grado.
Pertanto, in entrambi i casi, f ha un fattore di primo grado e quindi, applicando (a), si ottiene che $f(X)$ ha una radice in K.
Viceversa, se $f(X)$ ha una radice in K, per (a) si ottiene che $f(X)$ ha un fattore di primo grado in $K[X]$. Poiché $\deg(f) > 1$, necessariamente $f(X)$ è riducibile. □

Esempio 3.40.1. Se A non è un campo, la (a) della Proposizione precedente non vale. Infatti $f(X) = 2X+1$ è un polinomio di primo grado in $\mathbb{Z}[X]$ ma non ha radici in $\mathbb{Z}$.

Esempio 3.40.2. Se A non è un campo, la (b) della Proposizione precedente non vale. Infatti $f(X) = 2X$ ha grado 1 ma è riducibile in $\mathbb{Z}[X]$ in quanto è prodotto dei due polinomi non invertibili 2 e X.

Esempio 3.40.3. Se A non è un campo, la (c) della Proposizione precedente non vale. Infatti $f(X) = (2X + 1)(3X + 1)$ è un polinomio riducibile in $\mathbb{Z}[X]$ ma non ha radici in $\mathbb{Z}$.

Usando ancora il Teorema di Ruffini, si possono dimostrare alcuni fatti notevoli sui polinomi a coefficienti in un dominio.

Corollario 3.41 (Peter Roth, 1608). *Sia A un dominio e $f(X) \in A[X]$ un polinomio di grado $n \geq 1$. Allora $f(X)$ ha al più n radici in A.*

Dimostrazione. Se f non ha radici in A, allora l'affermazione è vera. Altrimenti si prova il teorema per induzione su n. Infatti, sia $\alpha \in A$ una radice di $f(X)$. Allora, per 3.37, $f(X) = (X - \alpha)g(X)$. Chiaramente $\deg(g(X)) = n - 1$, dunque per l'ipotesi induttiva $g(X)$ ha al più $n - 1$ radici in A. Essendo A un dominio, le radici di f sono tutte e sole le radici di g più α. Pertanto f ha al più n radici in A. □

È interessante e inaspettato vedere che, se A non è integro, il numero di radici di un polinomio può superare il suo grado!

Esempio 3.41.1. Il polinomio di $\mathbb{Z}_6[X]$ dato da $f(X) = X(X+\overline{1})$ è di secondo grado e ha 4 radici: $\overline{0}, \overline{2}, \overline{3}, \overline{5}$.

Corollario 3.42. *Sia A un dominio e $f(X), g(X) \in A[X]$ due polinomi di grado al più n, con $n \geq 1$. Se $f(X)$ e $g(X)$ assumono gli stessi valori in $n + 1$ elementi distinti di A, allora $f(X) = g(X)$.*

Dimostrazione. Siano $a_0, \ldots, a_n \in A$ elementi distinti tali che $f(a_i) = g(a_i)$, per ogni $i = 0, \ldots, n$. Allora il polinomio $f(X) - g(X)$ ha $a_0, \ldots, a_n$ come radici. Se fosse non nullo, avrebbe grado $\leq n$ per la formula del grado (vedi 3.6) e quindi, per 3.41 non può avere $n + 1$ radici. □

Infine studiamo una particolare proprietà dei polinomi in più indeterminate a coefficienti in un dominio infinito. Per fare questo, occorre un risultato preliminare di cui omettiamo la dimostrazione.

Proposizione 3.43. *Sia A un dominio e $\overline{X} = (X_1, \ldots, X_n)$ un insieme di indeterminate su A. Se S è un sottoinsieme infinito di A e $f(\overline{X})$ si annulla su S^n, allora $f(\overline{X})$ è il polinomio nullo.* □

Corollario 3.44. *Sia A un dominio con infiniti elementi. Allora l'anello delle funzioni polinomiali su A^n è isomorfo a $A[X_1, \ldots, X_n]$.*

Dimostrazione. Per 3.35 è sufficiente mostrare che l'omomorfismo $\varphi : A[\overline{X}] \longrightarrow \mathcal{F}(A^n, A)$ è iniettivo (in tal modo si prova che è isomorfismo su $\mathrm{Im}(\varphi)$ che è l'anello delle funzioni polinomiali su A^n).
Sia dunque $f(\overline{X}) \in \ker(\varphi)$; cioè $\varphi(f) = 0_{\mathcal{F}(A^n,A)}$. Per definizione

$$\varphi(f) = \varphi_f : \ A^n \longrightarrow A \quad \text{è definita da} \quad \alpha \mapsto f(\alpha).$$

Quindi $\varphi(f)$ è la funzione nulla, cioè $f(\alpha) = 0_A$ per ogni $\alpha \in A^n$. Per ipotesi A ha infiniti elementi, e f si annulla su A^n: per 3.43 necessariamente f è il polinomio nullo. □

Ricordiamo che, per il Teorema di Ruffini, se $\alpha \in A$ è radice di un polinomio $f(X) \in A[X]$, allora $f(X)$ è divisibile per $(X - \alpha)$. Si può dare dunque la seguente

Definizione. Se $\alpha \in A$ è radice di un polinomio $f(X) \in A[X]$, allora esiste $n \geq 1$ tale che $(X-\alpha)^n$ divide $f(X)$ ma $(X-\alpha)^{n+1}$ non divide $f(X)$. Diremo che n è la *molteplicità* di α e scriveremo $m_\alpha(f) := n$.
Se $n \geq 2$ (risp. $n = 1$) diremo che α è una radice *multipla* (risp. *semplice*) di $f(X)$.
Infine si intende che $m_\alpha(f) = 0$ se e solo se α non è una radice di $f(X)$.

Per determinare se una radice è multipla o meno, si può utilizzare una semplice tecnica. Occorre introdurre la seguente nozione:

Definizione. Sia A un dominio e $f(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$. Si dice *polinomio derivato* di f il polinomio di $A[X]$ definito da

$$f'(X) := \sum_{k=1}^{n} k\, a_k\, X^{k-1}.$$

Si osservi che tale definizione è formale e totalmente algebrica. Tuttavia coincide con l'usuale definizione di derivata analitica nel caso in cui $A = \mathbb{R}$. Più precisamente, ricordando che ad ogni polinomio $f(X) \in \mathbb{R}[X]$ si associa una precisa funzione polinomiale $\varphi_f : \mathbb{R} \longrightarrow \mathbb{R}$ definita da $\varphi_f(a) = f(a)$ per ogni $a \in \mathbb{R}$, e osservando che una funzione polinomiale è derivabile (nel senso dell'analisi), si calcola facilmente la funzione derivata di φ_f e risulta che $(\varphi_f)' = \varphi_{(f')}$. (I due simboli di derivazione qui hanno un significato diverso...).

Osservazione 3.45. È facile provare, usando solo la precedente definizione, le formule note (dall'analisi) che descrivono la relazione tra derivazione e operazioni tra polinomi: per ogni $f(X), g(X) \in A[X]$ valgono

$$(f+g)'(X) = f'(X) + g'(X) \quad \text{e} \quad (fg)'(X) = f'(X)g(X) + f(X)g'(X).$$

Di conseguenza l'applicazione "derivazione"

$$D:\ A[X] \longrightarrow A[X] \quad \text{definita da} \quad f(X) \mapsto f'(X)$$

è un omomorfismo di gruppi additivi, ma non di anelli. Se $A = K$ è un campo, D è inoltre un'applicazione lineare tra K-spazi vettoriali.

Proposizione 3.46. *Siano A un dominio, $f(X) \in A[X]$ e $\alpha \in A$ una radice di f. Allora α è una radice multipla se e solo se $f'(\alpha) = 0$.*

Dimostrazione. Sia α una radice multipla cioè $f(X) = (X-\alpha)^2 g(X)$.
Quindi $f'(X) = 2(X-\alpha)g(X) + (X-\alpha)^2 g'(X)$. Dunque $f'(\alpha) = 0$.
Viceversa, sia $f(\alpha) = 0$ e $f'(\alpha) = 0$. Allora $f(X) = (X-\alpha)h(X)$ e $f'(X) = h(X) + (X-\alpha)h'(X)$. Ma $(X-\alpha) | f'(X)$ dall'ipotesi, quindi necessariamente $(X-\alpha) | h(X)$. Pertanto, $(X-\alpha)^2 | f(X)$. □

Esempio 3.46.1. Si osservi che, se $f(X)$ è costante, $f'(X) = 0_{A[X]}$ (come si vede facilmente dalla definizione di polinomio derivato). Il viceversa è vero nel caso di funzioni polinomiali (reali di variabile reale) associate a polinomi di $\mathbb{R}[X]$, come è noto dall'analisi. È falso invece in anelli di caratteristica positiva. Infatti si consideri $f(X) = X^6 \in \mathbb{Z}_3[X]$. Tale polinomio non è costante, ma $f'(X) = 6X^5 = \overline{6}X^5 = \overline{0}$. In generale, i polinomi del tipo $f(X) = X^n \in \mathbb{Z}_p[X]$ hanno polinomio derivato nullo se n è multiplo di p.

Abbiamo visto che due polinomi che hanno uguale valore in un certo numero di elementi dell'anello dei coefficienti sono coincidenti (vedi 3.42). Ma resta da vedere se tale polinomio esiste e, in tal caso, se si riesce a limitarne il grado. Tale problema, relativamente a polinomi a coefficienti in un campo, è risolto dal

Teorema 3.47. *Sia K un campo. Comunque scelte due $(n+1)$-uple di elementi di K*

$$a_0, a_1, \ldots, a_n \quad e \quad b_0, b_1, \ldots, b_n$$

dove gli a_i sono tra loro distinti, esiste un unico polinomio $f(X) \in K[X]$ tale che
-) $f(a_i) = b_i$, per $i = 0, \ldots, n$;
-) $\deg(f) \leq n$.

Prima di dimostrare tale fatto, occorre premettere qualche osservazione.
Ricordiamo che il Teorema Cinese dei Resti in un anello commutativo qualunque A afferma che, se $I_0, \ldots, I_n$ sono ideali di A a due a due coprimi, cioè tali che $I_r + I_s = A$ per ogni $r \neq s$, allora l'applicazione naturale

$$\frac{A}{I_0 \cdots I_n} \longrightarrow \frac{A}{I_0} \times \cdots \times \frac{A}{I_n}$$

è un isomorfismo d'anelli. Equivalentemente, scelti arbitrariamente $v_0, \ldots, v_n$ in A, il sistema di congruenze

$$u \equiv v_j (\mathrm{mod}\, I_j), \quad i = 0, \ldots, n$$

ha una ed una sola soluzione $[\overline{u}] \in A/I_0 \cdots I_n$.

Una rilettura del Teorema Cinese dei Resti nell'anello dei polinomi $K[X]$ è la seguente, tenuto conto del fatto che $K[X]$ è un PID (vedi 3.14) e che due suoi ideali $(p_r(X))$ e $(p_s(X))$ sono coprimi se e solo se i polinomi $p_r(X)$ e $p_s(X)$ sono coprimi (vedi 2.48):

Lemma 3.48. *Sia K un campo, $p_0(X), \ldots, p_n(X) \in K[X]$ polinomi a due a due coprimi e $b_0, b_1, \ldots, b_n \in K$. Allora il sistema di congruenze*

$$f(X) \equiv b_i (\mathrm{mod}\, p_i(X)), \quad i = 0, \ldots, n$$

ha una ed una sola soluzione $[\overline{f}(X)] \in K[X]/(p_0 \cdots p_n)$. □

Un altro fatto utile alla dimostrazione di 3.47 è il seguente

Lemma 3.49. *Sia K un campo e $h(X) \in K[X]$ un polinomio di grado n. Allora in ogni classe non nulla $[f(X)] \in K[X]/(h(X))$ c'è uno ed un solo polinomio di grado minore di n.*

Dimostrazione. Proviamo dapprima l'esistenza. Se $\deg f(X) < n$, allora f è il polinomio richiesto. Se $\deg f(X) \geq n$, possiamo dividere f per h e determinare gli unici polinomi $q(X), r(X) \in K[X]$ tali che $f(X) = h(X)q(X) + r(X)$ e $\deg r(X) < n$ (il caso $r(X) = 0$ non si presenta in quanto $[f(X)] \neq 0$ per ipotesi). Chiaramente $[r(X)] = [f(X)]$ in $K[X]/(h(X))$ e questo prova che $r(X)$ è il polinomio richiesto.
Per provare l'unicità supponiamo che $r_1(X), r_2(X) \in [f(X)]$ ed entrambi abbiano grado minore di n. Allora $r_1(X) - r_2(X) \in (h(X))$. Ma $\deg(r_1(X) - r_2(X)) < n$ mentre $\deg h(X) = n$. Dunque necessariamente $r_1(X) - r_2(X) = 0$. □

Questi due lemmi permettono di provare il teorema precedente.

Dimostrazione. (**Teorema 3.47.**) Osserviamo preliminarmente che, per il Teorema di Ruffini (vedi 3.37), si ha: $f(a) = b \iff f(a) - b = 0 \iff a$ è radice di $f(X) - b \iff (X - a) | (f(X) - b)$. Inoltre è chiaro che ciò equivale a $f(X) - b \equiv 0 \ (\mathrm{mod}\, (X - a))$. Riassumendo:

$$f(a) = b \iff f(X) \equiv b \ (\mathrm{mod}\, (X - a)).$$

Dunque la tesi del teorema si può riformulare come segue: esiste un unico polinomio $f(X) \in K[X]$ tale che $\deg(f) \leq n$ e $f(X) \equiv b_i \ (\mathrm{mod}\, (X - a_i))$, per $i = 0, \ldots, n$.
Si osservi ora che i polinomi $p_1(X) := X - a_1, \ldots, p_n(X) := X - a_n$ sono a due a due coprimi (in quanto primi, per 3.39). Dunque per 3.48 esiste un'unica classe $[f(X)] \in K[X]/(p_0 \cdots p_n)$ tale che $f(X) \equiv b_j \ \mathrm{mod}\ (X - a_j)$ per ogni j. Infine, per 3.49 si può scegliere f in modo che $\deg(f(X)) < \deg(p_0(X) \cdots p_n(X)) = n+1$.
□

Polinomi complessi e reali

In questo paragrafo studieremo alcune notevoli proprietà dei polinomi a coefficienti complessi. Il risultato storicamente più rilevante riguarda le radici di tali polinomi. Agli inizi del Seicento Roth (3.41) ne limita il numero con il grado, ma riguardo all'esistenza si trovano enunciati a metà del XVI secolo. Poi vari matematici si cimentano sul tema, anche in casi speciali (Leibniz, Bernoulli, Goldbach). D'Alembert tenta una dimostrazione a metà del Settecento, e in seguito anche Eulero, Lagrange e Laplace. Ma solo Gauss prova il teorema, noto poi come *Teorema fondamentale dell'algebra*, nel 1799, a ventidue anni, nella sua tesi di dottorato.

Teorema 3.50. *(Teorema fondamentale dell'algebra) Ogni polinomio non costante a coefficienti complessi ha almeno una radice complessa.* □

Omettiamo la dimostrazione di questo risultato, ma esaminiamo la prima conseguenza.

Teorema 3.51. *Se $f(X) \in \mathbb{C}[X]$ è un polinomio di grado $n > 0$, allora esistono $s \in \mathbb{N}$, con $s \leq n$, $c, \alpha_1, \ldots, \alpha_s \in \mathbb{C}$, con gli α_i distinti, e $m_1, \ldots, m_s \in \mathbb{N}$ tali che*

$$f(X) = c\,(X-\alpha_1)^{m_1} \cdots (X-\alpha_s)^{m_s}.$$

In particolare, $f(X)$ ha n radici, se contate ognuna con la sua molteplicità; cioè $m_1 + \cdots + m_s = n$.

Dimostrazione. Per induzione su n.
Se $n = 1$ è ovvio.
Sia dunque $n \geq 1$. Per il teorema 3.50, $f(X)$ ha una radice $\alpha_1 \in \mathbb{C}$. Per il Teorema di Ruffini (vedi 3.37), si ha quindi $f(X) = (X-\alpha_1)f_1(X)$; chiaramente $\deg(f_1(X)) = n-1$. Quindi possiamo applicare l'ipotesi induttiva a f_1: esistono $c, \alpha_2, \ldots, \alpha_s \in \mathbb{C}$, con α_i distinti, e $m_2, \ldots, m_s \in \mathbb{N}$ tali che

$$f_1(X) = c\,(X-\alpha_2)^{m_2} \cdots (X-\alpha_s)^{m_s}$$

e inoltre $m_2 + \cdots + m_s = n-1$. Quindi

$$f(X) = (X-\alpha_1)f_1(X) = c\,(X-\alpha_1)(X-\alpha_2)^{m_2} \cdots (X-\alpha_s)^{m_s}.$$

Se α_1 è diverso da $\alpha_2, \ldots, \alpha_s$ si ha immediatamente la tesi in quanto $1 + m_2 + \cdots + m_s = n$. Altrimenti, con un facile ragionamento (lasciato al lettore), si ottiene ancora la tesi. □

Come osservato in 3.46, se $f(X)$ è un polinomio non costante, le sue radici multiple sono, tra le sue radici, tutte e sole le radici di $f'(X)$. Inoltre si può provare che, essendo $\mathbb{C}$ un campo di caratteristica zero, il polinomio derivato non è il polinomio nullo. Per il Teorema di Ruffini, abbiamo dunque che α è radice multipla di $f(X)$ se e solo se $(X-\alpha)$ divide sia $f(X)$ che $f'(X)$ se e solo se $(X-\alpha)$ divide il loro massimo comun divisore. Questo prova la seguente

Proposizione 3.52. *Sia $f(X) \in \mathbb{C}[X]$ un polinomio di grado positivo. Allora i seguenti insiemi di numeri complessi coincidono:*

$$\left\{ \begin{array}{c} \text{radici multiple di} \\ f(X) \end{array} \right\} = \left\{ \begin{array}{c} \text{radici di} \\ f(X) \text{ e } f'(X) \end{array} \right\} = \left\{ \begin{array}{c} \text{radici di} \\ d(X) \end{array} \right\}$$

dove $d(X) := MCD(f(X), f'(X))$. □

Da questo fatto si deducono interessanti conseguenze.

Corollario 3.53. *Sia $f(X) \in \mathbb{C}[X]$ un polinomio di grado positivo e si ponga $d(X) := MCD(f(X), f'(X))$.*

i) Se α è una radice di $f(X)$ con $m_f(\alpha) = m$, allora $m_{f'}(\alpha) = m-1$ e quindi $m_d(\alpha) = m-1$;
ii) le radici multiple di $f(X)$ sono radici semplici del polinomio $f(X)/d(X)$;
iii) le radici di $f(X)$ sono tutte e sole le radici del polinomio $f(X)/d(X)$ e quest'ultimo ha solo radici semplici.

Dimostrazione. *i*) Per ipotesi $f(X) = (X-\alpha)^m g(X)$, dove $g(\alpha) \neq 0$.
Quindi $f'(X) = m(X-\alpha)^{m-1}g(X) + (X-\alpha)^m g'(X)$, da cui $m_{f'}(\alpha) \geq m-1$. Se tale molteplicità fosse m, allora $(X-\alpha)$ dividerebbe $g(X)$, contro $g(\alpha) \neq 0$.
ii) Sia α una radice di molteplicità m di $f(X)$. Per (i) si ha che $m_d(\alpha) = m-1$. Dunque

$$f(X) = (X-\alpha)^m g(X), \text{ con } g(\alpha) \neq 0$$
$$d(X) = (X-\alpha)^{m-1} h(X), \text{ con } h(\alpha) \neq 0.$$

Pertanto $f(X)/d(X) = (X-\alpha)[g(X)/h(X)]$ e quindi, poiché $g(\alpha) \neq 0$, si ottiene che α è radice semplice di $f(X)/d(X)$.
iii) Sia α una radice semplice di $f(X)$. Per (i) si ha che $m_d(\alpha) = m_f(\alpha) - 1 = 0$. Dunque α non è radice di $d(X)$. Ciò prova che anche le radici semplici di $f(X)$ sono radici (semplici) del polinomio $f(X)/d(X)$. Tale fatto e (ii) dimostrano che

$$\{\text{radici di } f(X)\} \subseteq \{\text{radici di } f(X)/d(X)\}.$$

L'altra inclusione è ovvia. □

Tra i polinomi a coefficienti complessi ci sono quelli a coefficienti reali. Per studiare le loro prime proprietà, ricordiamo alcuni fatti relativi a $\mathbb{C}$. Il *coniugio complesso* è l'applicazione

$$\mathbb{C} \longrightarrow \mathbb{C} \quad \text{definita da} \quad z = a + ib \mapsto \overline{z} := a - ib.$$

Si verifica facilmente che il coniugio è un automorfismo di anelli e anche un isomorfismo di $\mathbb{R}$-spazi vettoriali. È evidente, inoltre, che $z = \overline{z}$ se e solo se $z \in \mathbb{R}$ e che $z + \overline{z}$ e $z\overline{z}$ sono entrambi reali.

Definizione. Se $f(X) \in \mathbb{C}[X]$, si dice *polinomio coniugato* di $f(X) = \sum_{i=0}^n z_i X^i$ il polinomio

$$\overline{f}(X) = \sum_{i=0}^{n} \overline{z}_i \, X^i.$$

Come per i numeri complessi, è chiaro che $f(X) = \overline{f}(X)$ se e solo se $f(X) \in \mathbb{R}[X]$.

Proposizione 3.54. *Se $f(X) \in \mathbb{R}[X]$ e $\alpha \in \mathbb{C}$ è una sua radice, allora anche $\overline{\alpha}$ è una radice di $f(X)$. Inoltre α e $\overline{\alpha}$ hanno la stessa molteplicità.*

Dimostrazione. Per ipotesi $f(\alpha) = 0_{\mathbb{C}}$. Questa è una uguaglianza tra numeri complessi; dunque anche i loro coniugati sono uguali, cioè $\overline{f(\alpha)} = 0_{\mathbb{C}}$. Ma $\overline{f(\alpha)} = \overline{f}(\overline{\alpha})$; infatti, se $f(X) = \sum_{i=0}^n z_i X^i$ allora

$$\overline{f(\alpha)} = \overline{\sum_{i=0}^{n} z_i \alpha^i} = \sum_{i=0}^{n} \overline{z}_i \overline{\alpha}^i = \overline{f}(\overline{\alpha})$$

dove l'uguaglianza centrale è dovuta al fatto che il coniugio è un omomorfismo di anelli.
In conclusione $\overline{f}(\overline{\alpha}) = 0_{\mathbb{C}}$, cioè $\overline{\alpha}$ è radice di $\overline{f}(X)$.
D'altra parte, per ipotesi, f ha coefficienti reali e dunque $f(X) = \overline{f}(X)$. □

Una ovvia conseguenza della proposizione precedente è che un polinomio a coefficienti reali di grado dispari ha almeno una radice reale. Si prova senza difficoltà anche il seguente risultato.

Proposizione 3.55. *Se $f(X) \in \mathbb{R}[X]$ ha grado $n \geq 3$, allora $f(X)$ è riducibile e si può scrivere come prodotto di polinomi di grado 1 o 2.* □

Fattorialità degli anelli di polinomi

In questo paragrafo studiamo i polinomi a coefficienti in un dominio a fattorizzazione unica. Il risultato principale sarà il *Lemma di Gauss*. Una delle dimostrazioni presenti il letteratura utilizza le classi modulo un ideale primo dell'anello dei coefficienti. Premettiamo dunque alcune nozioni.

Proposizione 3.56. *Siano A e B due anelli commutativi unitari e sia $\varphi : A \to B$ un omomorfismo d'anelli. Allora l'applicazione $\varphi^* : A[X_1, \dots, X_n] \longrightarrow B[X_1, \dots, X_n]$ definita da $a \mapsto \varphi(a)$, per ogni $a \in A$, $X_i \mapsto X_i$, per ogni $i = 1, \dots, n$, ed estesa algebricamente su $A[X_1, \dots, X_n]$ è un omomorfismo d'anelli. Inoltre φ è iniettiva o suriettiva se e solo se lo è φ^*, rispettivamente.*

Dimostrazione. La prima affermazione è tautologica, in quanto "estendere algebricamente" φ significa che φ^* è definita da

$$\varphi^* \left(\sum_{i=0}^{n} a_i \, X^i \right) = \sum_{i=0}^{n} \varphi(a_i) \, X^i.$$

ed è immediato verificare che tale applicazione è un omomorfismo di anelli (utilizzando il fatto che φ lo è).
"$\ker(\varphi) = 0 \iff \ker(\varphi^*) = 0$"
Supponiamo che $\ker(\varphi) = 0$ e sia $f(X) \in \ker(\varphi^*)$. Se $f(X) = \sum_{i=0}^{n} a_i \, X^i$ allora $0 = \varphi^*(f) = \sum_{i=0}^{n} \varphi(a_i) \, X^i$. Per il Principio di identità dei polinomi deve essere $\varphi(a_i) = 0$ per ogni $i = 0, \dots, n$. Ma φ è iniettiva per ipotesi, dunque $a_i = 0$ per ogni $i = 0, \dots, n$. Quindi $f(X) = 0$.
Viceversa, supponiamo che $\ker(\varphi^*) = 0$ e sia $a \in \ker(\varphi)$. Poiché a si può pensare come polinomio costante in $A[X_1, \dots, X_n]$ e φ^* estende φ per ipotesi, allora $\varphi^*(a) = \varphi(a) = 0$, dunque $a = 0$ in quanto φ^* è iniettiva.
"$\mathrm{Im}(\varphi) = B \iff \mathrm{Im}(\varphi^*) = B[X_1, \dots, X_n]$"
Si lascia al lettore la facile verifica che $\mathrm{Im}(\varphi^*) = \mathrm{Im}(\varphi)[X_1, \dots, X_n]$.
Quindi "$\Rightarrow$" è immediata. Anche "$\Leftarrow$" è facile ed è lasciata al lettore. □

Un caso particolare di omomorfismo d'anelli $\varphi : A \to B$ è dato dall'omomorfismo di proiezione di un anello su un suo quoziente. Dunque se $I \subseteq A$ è un ideale e $\pi : A \to A/I$ è la proiezione canonica, resta indotto l'epimorfismo di anelli

$$\pi^* : A[X] \longrightarrow (A/I)[X].$$

Ad esempio, se A è un dominio e p è un elemento primo di A, allora l'ideale (p) è primo e $A/(p)$ è anch'esso un dominio. L'omomorfismo (suriettivo)

$$\pi^* : A[X] \longrightarrow (A/(p))[X].$$

assume la forma

$$\sum_{i=0}^{n} a_i \, X^i \quad \mapsto \sum_{i=0}^{n} \overline{a}_i \, X^i$$

e viene detto *riduzione modulo p*.

Definizione. Sia A un UFD e $f(X) = \sum_{i=0}^{n} a_i \, X^i \in A[X]$. Se un $MCD(a_0, \dots, a_n) = 1$ allora diciamo che $f(X)$ è un polinomio *primitivo*.

Osservazione 3.57. Se un polinomio $f(X) \in A[X]$ è irriducibile in A allora è primitivo.
Infatti, se non lo fosse tutti i suoi coefficienti sarebbero divisibili per il loro Massimo Comun Divisore m, con m non invertibile. Si otterrebbe dunque la fattorizzazione non banale

$$f(X) = m\tilde{f}(X).$$

Esempio 3.57.1. In $\mathbb{Z}[X]$ il polinomio $f(X) = 2X^2 + 4X + 6$ non è primitivo, in quanto $MCD(2, 4, 6) = 2$. E infatti si fattorizza in modo non banale come $f(X) = 2(X^2 + 2X + 3)$. Si noti che 2 è un fattore non invertibile e quindi non banale di $f(X)$.

Esempio 3.57.2. Non vale il viceversa dell'Osservazione 3.57: ci sono infatti polinomi primitivi che sono riducibili. Ad esempio, $X^2 - 1 \in \mathbb{Z}[X]$ è primitivo ma riducibile in quanto $X^2 - 1 = (X + 1)(X - 1)$.

Teorema 3.58. *(Lemma di Gauss) Sia A un UFD e $g(X), h(X) \in A[X]$ polinomi primitivi. Allora $f(X) := g(X)h(X)$ è primitivo.*

Dimostrazione. Supponiamo per assurdo che il Massimo Comun Divisore dei coefficienti di f non sia 1_A. Allora avrà un fattore irriducibile p. Essendo A un anello fattoriale, p è primo, dunque l'ideale (p) è primo in A. Pertanto $A/(p)$ e quindi $(A/(p))[X]$ sono integri. Si consideri la riduzione modulo p di $f(X) = g(X)h(X)$:

$$\pi^*(f(X)) = \pi^*(g(X)h(X)) = \pi^*(g(X))\pi^*(h(X)).$$

Poiché p divide tutti i coefficienti di $f(X)$, ovviamente $\pi^*(f(X)) = 0$ in $(A/(p))[X]$, che è un dominio. Dunque necessariamente uno tra $\pi^*(g(X))$ e $\pi^*(h(X))$ è nullo. Supponiamo $\pi^*(g(X)) = 0$. Per il Principio di identità dei polinomi, questo significa che tutti i coefficienti di $g(X)$ sono nulli modulo p, cioè che sono tutti multipli di p, contro all'ipotesi che $g(X)$ sia primitivo. □

Il precedente teorema implica varie conseguenze interessanti: riguardo alla riducibilità dei polinomi (in un dominio fattoriale e nel suo campo delle frazioni) e riguardo al passaggio della fattorialità alle estensioni polinomiali.

Nel resto del paragrafo, A denota un UFD e $K := Q(A)$ il campo dei quozienti di A. Inoltre denoteremo i polinomi di $A[X]$ con lettere minuscole: $f(X), g(X), h(X), \ldots$ e quelli di $K[X]$ con lettere maiuscole: $F(X), G(X), H(X), \ldots$ Infine se $f(X)$ è un polinomio a coefficienti in A, diremo che è riducibile, irriducibile, primitivo, ecc... *su* A oppure *su* K, intendendo che è riducibile, irriducibile, primitivo, ecc... come elemento di $A[X]$ o, rispettivamente, di $K[X]$.

Osservazione 3.59.

a) Se $F(X) \in K[X]$, allora riducendo i coefficienti di F a un denominatore comune $d \in A$, si può scrivere $F(X) = d^{-1}f(X)$, per un opportuno $f(X) \in A[X]$.

b) Se $f(X) \in A[X]$, posto m un MCD dei suoi coefficienti, si ha che $f(X) = m\tilde{f}(X)$, dove $\tilde{f}(X)$ è un polinomio primitivo di $A[X]$.

c) Questi due fatti implicano che, per ogni $F(X) \in K[X]$ esiste $\lambda \in K$ tale che

$$F(X) = \lambda\tilde{f}(X), \quad \text{con } \tilde{f}(X) \in A[X] \text{ polinomio primitivo.}$$

d) Siano $f(X), g(X) \in A[X]$ due polinomi non nulli e primitivi e sia $k \in K$ tale che $f(X) = k\,g(X)$. Allora $k \in \mathcal{U}(A)$. Per provare tale fatto, sia $k = \alpha/\beta$, con $\alpha, \beta \in A^*$ e coprimi. Si osservi inoltre che f e g hanno lo stesso grado dunque

$$f(X) = \sum_{i=0}^{n} a_i\,X^i \quad \text{e} \quad g(X) = \sum_{i=0}^{n} b_i\,X^i \quad \text{per opportuni} \quad a_i, b_i \in A.$$

Pertanto, dall'ipotesi $f(X) = (\alpha/\beta)\,g(X)$, per il Principio di identità dei polinomi si ha che

$$a_i = \frac{\alpha}{\beta}\,b_i \quad \text{per ogni} \quad i = 0, \ldots, n.$$

Ma il fatto che α e β siano coprimi implica, da una parte, che α divide a_i per ogni $i = 0, \ldots, n$. Dall'altra, essendo $a_i \in A$, implica che β divide b_i per ogni $i = 0, \ldots, n$. Essendo $f(X)$ e $g(X)$ primitivi per ipotesi, necessariamente sia α che β sono invertibili in A. Quindi $k \in A$ ed è invertibile in A, come volevamo.

Esempio 3.59.1 Vediamo alcuni esempi nel caso in cui $A = \mathbb{Z}$ e $K = \mathbb{Q}$.
a) Sia

$$F(X) = \frac{2}{3}X^2 + \frac{4}{5}X + 8 \ \in \ \mathbb{Q}[X].$$

Chiaramente $d = 15 \in \mathbb{Z}$ e $f(X) = 10X^2 + 12X + 120 \in \mathbb{Z}[X]$.
b) Se $f(X) = 2X^2 + 4X - 6$ allora $m = 2$ e $\tilde{f}(X) = X^2 + 2X - 3$.
c) Se

$$F(X) = \frac{2}{3}X^2 + \frac{4}{5}X + 8 \ \in \ \mathbb{Q}[X]$$

allora, ancora per 3.59, possiamo scrivere

$$F(X) = \frac{1}{15}(10X^2 + 12X + 120) = \frac{2}{15}(5X^2 + 6X + 60)$$

e quindi $\lambda = \frac{2}{15} \in \mathbb{Q}$ e $\tilde{f}(X) = 5X^2 + 6X + 60$ polinomio primitivo.

Proviamo ora qualche importante conseguenza del Lemma di Gauss:

Corollario 3.60. *Siano A un UFD e $f(X) \in A[X]$ un polinomio non nullo. Se $f(X)$ è riducibile su K, allora lo è anche su A.*

Dimostrazione. Se $f(X)$ non è primitivo allora si ottiene subito una scomposizione non banale in $A[X]$, come visto in 3.57: $f(X) = m\tilde{f}(X)$.
Quindi possiamo assumere che $f(X)$ sia primitivo. Per ipotesi $f(X)$ è riducibile su K, dunque esistono $G(X), H(X) \in K[X]$ tali che $\deg(G) \geq 1$, $\deg(H) \geq 1$ e $f(X) = G(X)H(X)$.
Per Osservazione 3.59 (c), esistono $\lambda, \mu \in K$ tali che $G(X) = \lambda\tilde{g}(X)$ e $H(X) = \mu\tilde{h}(X)$, con $\tilde{g}(X), \tilde{h}(X) \in A[X]$ polinomi primitivi. Pertanto

$$f(X) = (\lambda\tilde{g}(X))(\mu\tilde{h}(X)) = (\lambda\mu)\tilde{g}(X)\tilde{h}(X).$$

Per il Lemma di Gauss, il prodotto $\tilde{g}(X)\tilde{h}(X) \in A[X]$ è primitivo; ma per ipotesi anche $f(X) \in A[X]$ è primitivo. Allora, necessariamente $\lambda\mu$ è un elemento invertibile di A per Osservazione 3.59 (d).
Quindi il polinomio $g(X) := (\lambda\mu)\tilde{g}(X)$ appartiene ad $A[X]$, come $\tilde{h}(X)$.
Pertanto $f(X) = g(X)\tilde{h}(X)$ è una fattorizzazione non banale in $A[X]$. □

Corollario 3.61. *Siano A un UFD e $f(X) \in A[X]$ un polinomio non nullo. Si hanno i seguenti fatti:*
i) se $\deg f = 0$ allora $f(X)$ è irriducibile su A se e solo se è una costante irriducibile di A;
ii) se $\deg f > 0$ allora $f(X)$ è irriducibile su A se e solo se è irriducibile su K e primitivo su A.

Dimostrazione.
i) Se $\deg f = 0$ allora $f(X) = a \in A^*$.
Dalla definizione di elemento irriducibile si ha, da un lato, che a è irriducibile come elemento di $A[X] \iff a = p_1p_2$ con p_1 e p_2 polinomi costanti (per la Formula del grado) non invertibili. D'altra parte, a è irriducibile come elemento di $A \iff a = p_1p_2$ con p_1 e p_2 elementi di A non invertibili. Si conclude ricordando che $\mathcal{U}(A) = \mathcal{U}(A[X])$ per Proposizione 3.7.
ii) Sia $f(X)$ irriducibile su A; allora è irriducibile anche su K per 3.60. Inoltre è primitivo su A per 3.57.
Viceversa supponiamo che $f(X)$ sia irriducibile su K e primitivo su A. Se fosse $f(X) = g(X)h(X)$ una fattorizzazione non banale in $A[X]$ allora si presentano due possibilità: o entrambi $g(X)$ e $h(X)$ sono non costanti oppure uno dei due è costante. Nel primo caso, $f(X) = g(X)h(X)$ sarebbe una fattorizzazione non banale in $K[X]$, contro l'ipotesi che $f(X)$ sia irriducibile su K. Allora deve essere, ad esempio, $\deg(g(X)) = 0$. In tal caso, $g(X) = \lambda \in A$ costante non invertibile in A. Quindi $f(X) = \lambda h(X)$ e questo contraddice l'ipotesi che $f(X)$ sia primitivo su A. Pertanto anche il secondo caso è impossibile.
Ne segue che $f(X)$ è irriducibile su A. □

Esempio 3.61.1 Nella (ii) di 3.61 non è sufficiente supporre che un polinomio sia irriducibile su K perché sia irriducibile su A: l'ipotesi che sia primitivo è essenziale. Infatti $f(X) = 2X^2+4X+8 \in \mathbb{Z}[X]$ è irriducibile su $\mathbb{Q}$ ma non su $\mathbb{Z}$, in quanto $f(X) = 2(X^2 + 2X + 4)$. Questo accade perché f non è primitivo.

Una classica problematica consiste nel valutare quali proprietà di un anello base A si estendono all'anello dei polinomi $A[X]$.

Abbiamo visto che se A è commutativo, allora anche $A[X]$ è commutativo.

Inoltre se A è unitario, allora anche $A[X]$ è unitario.

Tuttavia la proprietà di essere a ideali principali non si estende. Ad esempio, $\mathbb{Z}$ è un PID, ma $\mathbb{Z}[X]$ no. Infatti il suo ideale $(2, X)$ non è principale. Anche $\mathbb{R}[X]$ è un PID, ma $\mathbb{R}[X, Y]$ no.

Una importante proprietà come la fattorialità passa invece alle estensioni polinomiali:

Teorema 3.62. *Se A è un UFD allora anche $A[X]$ è un UFD.*

Per dimostrare questo importante risultato, anch'esso conseguenza del Lemma di Gauss, proveremo dapprima un fatto più debole, che sfrutta la divisibilità dell'anello dei polinomi a coefficienti in un campo.

Teorema 3.63. *Se K è un campo allora $K[X]$ è un UFD. Precisamente ogni polinomio $F(X) \in K[X]$ di grado positivo ammette una fattorizzazione*

$$F(X) = aP_1(X) \cdots P_r(X), \quad a \in K, \quad P_i(X) \text{ monici irriducibili.}$$

e tale fattorizzazione è unica, a meno dell'ordine.

Dimostrazione. Per 3.14, l'anello $K[X]$ è un PID e quindi, per 2.46, è UFD. L'esistenza di una fattorizzazione come nell'enunciato segue facilmente dividendo ogni fattore per il suo coefficiente direttivo e ponendo a il prodotto di tali coefficienti. Per provare l'unicità si supponga che

$$F(X) = aP_1(X)\cdots P_r(X) = bQ_1(X)\cdots Q_s(X). \qquad (*)$$

Poiché i P_i e i Q_j sono monici, è chiaro che $a = b$. Il polinomio $P_1(X)$ è irriducibile, quindi primo (perché $K[X]$ è un dominio con MCD). Pertanto deve dividere uno dei Q_j; supponiamo il primo, senza perdere di generalità. Ma anche $Q_1(X)$ è irriducibile. Questo implica che $P_1(X)$ e $Q_1(X)$ sono associati ed essendo entrambi monici sono uguali. Pertanto, cancellando da ambo i membri $P_1(X) = Q_1(X)$, l'uguaglianza $(*)$ diventa

$$P_2(X)\cdots P_r(X) = Q_2(X)\cdots Q_s(X).$$

Iterando il procedimento si prova che $s = r$ e che $P_i(X) = Q_i(X)$ per ogni $i = 1, \ldots, r$. □

Per provare il Teorema 3.62 utilizzeremo parzialmente il Teorema 3.63, e precisamente solo il fatto che $K[X]$ è UFD, dove $K = Q(A)$, come al solito.

Dimostrazione. (**Teorema 3.62**) Dobbiamo provare che se $f(X) \in A[X]$ è un polinomio non nullo e non invertibile allora esistono $p_1, \ldots, p_s \in A$ elementi irriducibili ed esistono $q_1(X), \ldots, q_t(X) \in A[X]$ polinomi irriducibili tali che

$$f(X) = p_1\cdots p_s \cdot\ q_1(X)\cdots q_t(X)$$

e tale fattorizzazione è essenzialmente unica.

(•) Se $\deg(f) = 0$, allora $f(X) = m$ dove $m \in A$ non è invertibile. Quindi, essendo A un UFD, m si fattorizza in modo unico in un prodotto di elementi irriducibili di A e la tesi è provata.
Se $\deg(f) > 0$, per 3.59 (b) si può scrivere $f(X) = m\tilde{f}(X)$, dove $\tilde{f}(X)$ è un polinomio primitivo di $A[X]$ e $m \in A$ non è invertibile. Come prima, m si fattorizza come $m = p_1\cdots p_s$ con $p_1, \ldots, p_s \in A$ elementi irriducibili. Pertanto

$$f(X) = p_1\cdots p_s\, \tilde{f}(X).$$

(•) Si consideri ora il polinomio primitivo $\tilde{f}(X)$. Chiaramente $\deg \tilde{f}(X) = \deg f(X) > 0$. Inoltre $\tilde{f}(X) \in A[X] \subseteq K[X]$ (che è UFD), dunque si può fattorizzare in $K[X]$ in modo essenzialmente unico come

$$\tilde{f}(X) = Q_1(X)\cdots Q_t(X)$$

con $Q_i(X) \in K[X]$ irriducibili di gradi positivi. Per l'Osservazione 3.59 (c), per ogni $i = 1, \ldots, t$, esistono $k_i \in K$, $q_i(X) \in A[X]$ polinomio primitivo tale che

$$Q_i(X) = k_i q_i(X).$$

Per 3.61, ogni $q_i(X)$ è irriducibile in $A[X]$ perché ogni $Q_i(X)$ è irriducibile e $q_i(X)$ è primitivo. Pertanto

$$\tilde{f}(X) = k_1\cdots k_t\ q_1(X)\cdots q_t(X).$$

Per 3.58 il prodotto dei polinomi primitivi $q_1(X), \ldots, q_t(X)$ è primitivo. Ma anche $\tilde{f}(X)$ è primitivo per costruzione. Quindi, per l'Osservazione 3.59 (d), $\tau := k_1\cdots k_t$ è un elemento invertibile di A. Pertanto si ottiene la fattorizzazione (essenzialmente unica) in polinomi irriducibili di $A[X]$, con $\tau \in \mathcal{U}(A)$:

$$\tilde{f}(X) = \tau q_1(X)\cdots q_t(X).$$

(•) Si conclude componendo le due parti della dimostrazione:

$$f(X) = p_1\cdots p_s\, \tilde{f}(X) = p_1\cdots p_s\ q_1(X)\cdots q_t(X)$$

dove i fattori hanno le proprietà richieste e tale fattorizzazione è essenzialmente unica. □

È conseguenza immediata del precedente risultato l'estensione della fattorialità ad alcuni casi particolari.

Corollario 3.64. *Se A un UFD allora anche $A[X_1, \ldots, X_n]$ è un UFD. In particolare, $\mathbb{Z}[X_1, \ldots, X_n]$ è un UFD e, per ogni campo K, anche $K[X_1, \ldots, X_n]$ è un UFD.* □

Vediamo alcune osservazioni sui polinomi a coefficienti interi.

Osservazione 3.65. Se un polinomio $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ ha una radice razionale r/s (supponendo r e s coprimi) allora $r|a_0$ e $s|a_n$.

Osservazione 3.66. Sia $f(X) \in \mathbb{Z}[X]$ un polinomio non nullo. Se ridotto modulo un primo p ha lo stesso grado ed è irriducibile, allora è irriducibile in $\mathbb{Z}$.

Concludiamo con alcuni esercizi ed esempi relativi ai capitoli 2 e 3.

Esempio 3.E1. Si consideri il dominio $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$, cioè l'anello degli interi di Gauss.
Il suo campo dei quozienti è

$$Q(\mathbb{Z}[i]) = \mathbb{Q}[i] = \{p + iq \,|\, p, q \in \mathbb{Q}\}.$$

Per provarlo, basta osservare che $\mathbb{Q}[i]$ è un campo, e precisamente un campo numerico (lasciato al lettore). Infatti, dimostrato questo, si consideri il monomorfismo canonico di anelli $j : \mathbb{Z}[i] \longrightarrow \mathbb{Q}[i]$ che estende l'inclusione $\mathbb{Z} \subset \mathbb{Q}$. Per 0.50 esiste un unico omomorfismo di anelli $\psi : Q(\mathbb{Z}[i]) \longrightarrow \mathbb{Q}[i]$ tale che $j = \psi \circ i$. Essendo j non nullo anche ψ è non nullo; quindi, tenuto conto che ogni omomorfismo non nullo di campi è iniettivo, allora ψ è iniettivo. Quindi $Q(\mathbb{Z}[i]) \subseteq \mathbb{Q}[i]$.
L'altra inclusione è immediata, osservando che ogni elemento di $\mathbb{Q}[i]$ è del tipo

$$p + qi = \frac{a}{b} + i\,\frac{c}{d} = \frac{ad + ibc}{bd} \in Q(\mathbb{Z}[i]).$$

Esempio 3.E2. Si consideri l'ideale $I = (Y - 1, X^2 + Y - 2) \subset \mathbb{Q}[X, Y]$.
Calcolare l'anello quoziente $\mathbb{Q}[X, Y]/I$ e determinare se I è un ideale primo e/o massimale.

Per il II Teorema di omomorfismo di anelli (0.42) si ha

$$\mathbb{Q}[X, Y]/(Y - 1, X^2 + Y - 2) \cong \frac{\mathbb{Q}[X, Y]/(Y - 1)}{(Y - 1, X^2 + Y - 2)/(Y - 1)}.$$

Ma $\mathbb{Q}[X, Y]/(Y - 1) = \mathbb{Q}[X][Y]/(Y - 1)$. Inoltre per 3.38 si ha l'isomorfismo

$$A[Y]/(Y - \alpha) \to A \qquad (*)$$

con cui Y viene identificato con α. Nel nostro caso $A = \mathbb{Q}[X]$ e Y si identifica con $1 \in \mathbb{Q}[X]$. Dunque

$$\mathbb{Q}[X, Y]/(Y - 1) \cong \mathbb{Q}[X]$$

e l'immagine dell'ideale $(Y - 1, X^2 + Y - 2)/(Y - 1)$ risulta essere $(X^2 + 1 - 2)$, cioè $(X^2 - 1)$. Pertanto

$$\mathbb{Q}[X, Y]/(Y - 1, X^2 + Y - 2) \cong \mathbb{Q}[X]/(X^2 - 1)$$

Tenuto conto che $X^2 - 1 = (X - 1)(X + 1)$ in $\mathbb{Q}[X]$ e che gli ideali $(X - 1)$ e $(X + 1)$ sono coprimi (in quanto primi), si può applicare il Teorema Cinese dei resti, ottenendo

$$\mathbb{Q}[X]/(X^2 - 1) \cong \mathbb{Q}[X]/(X - 1) \times \mathbb{Q}[X]/(X + 1) \cong \mathbb{Q} \times \mathbb{Q}$$

dove l'ultimo isomorfismo si ottiene ancora per $(*)$.
Infine è noto che $\mathbb{Q} \times \mathbb{Q}$ ha zero divisori, cioè non è integro. Pertanto anche l'anello quoziente da cui siamo partiti, ad esso isomorfo, non è integro. In conclusione l'ideale I non è primo. *A fortiori* neanche massimale.

Esempio 3.E3. Si consideri l'isomorfismo di anelli (vedi Teorema Cinese del resto)

$$f : \mathbb{Z}_{15} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \text{dato da} \quad f([u]_{15}) = ([u]_3, [u]_5).$$

Vogliamo trovare l'inversa g di f e precisamente, per ogni $([x]_3, [y]_5) \in \mathbb{Z}_3 \times \mathbb{Z}_5$, trovare una formula per esprimere $g([x]_3, [y]_5)$ come elemento di $\mathbb{Z}_{15}$.

Ripercorrendo la dimostrazione del teorema, gli ideali I e J sono in questo caso (3) e (5). Si prova quindi che un elemento z di $\mathbb{Z}$ la cui immagine sia $([x]_3, [y]_5)$ è ad esempio $z = xj + yi$, dove $i \in I$, $j \in J$ e $i + j = 1$. In questo caso si possono scegliere $i = -9$ e $j = 10$. Pertanto $z = 10x - 9y$. Si verifichi che tale definizione non dipende dai rappresentanti x e y delle rispettive classi...

Esercizio 3.E4. In un mondo fantastico e molto lontano vivono dei folletti.
Essi sono più di 100 e meno di 300 e si spostano di villaggio in villaggio, tutti insieme. Ogni villaggio ha il nome di un numero intero positivo.
I folletti sanno che non subiranno, dopo ogni loro viaggio, i rigori invernali perché ogni villaggio ha dei rifugi distribuiti come segue: per ogni $n \in \mathbb{N}^*$, nel villaggio n ci sono tante casette con n posti, ciascuna delle quali può essere essere usata SOLO se viene riempita (per esempio, nel villaggio 9 una tale casetta non può essere abitata da 7 folletti). Inoltre, in ogni villaggio n vi è una sola casetta X_n con $n-1$ posti, nella quale possono vivere h folletti, per $0 \leq h \leq n-1$ (per esempio, la casetta X_3 può rimanere vuota o essere abitata da uno o due folletti).
Recentemente i folletti sono stati nei villaggi Cinque, Sei e Sette. Sapendo che le casette X_5 e X_6 sono state abitate da 3 folletti e che la casetta X_7 è stata abitata da 5 folletti, si determini il numero totale dei folletti.

Capitolo 4 - Campi *

Ricordiamo quanto visto nella sezione sulla caratteristica di un anello. Se A è un anello commutativo unitario, allora il nucleo dell'omomorfismo di anelli $\alpha : \mathbb{Z} \longrightarrow A$ definito da $m \mapsto m1_A$ può essere nullo (dunque $ch(A) = 0$) oppure un ideale generato da $n \in \mathbb{N}$ (dunque $ch(A) = n$).
L'immagine di α è un sottoanello di A, detto *sottoanello fondamentale*. Come osservato in precedenza, esso è isomorfo, rispettivamente, a $\mathbb{Z}$ o a $\mathbb{Z}_n$. Abbiamo anche osservato che, se A è integro, allora il suo sottoanello fondamentale è isomorfo, rispettivamente, a $\mathbb{Z}$ o a $\mathbb{Z}_p$, dove p è un numero primo. Questo accade, in particolare, se l'anello in questione è un campo K.

È facile provare la seguente

Proposizione 4.1. *Il sottoanello fondamentale di un anello A è il più piccolo sottoanello di A contenente 1_A e coincide con l'intersezione di tutti i sottoanelli (unitari) di A.* □

Questo fatto induce a dare la seguente

Definizione. Si dice *sottocampo fondamentale* di un campo K il più piccolo sottocampo di K o, equivalentemente, l'intersezione di tutti i sottocampi di K e si indica con $F_c(K)$.

Proposizione 4.2. *Il sottocampo fondamentale di un campo K è il campo dei quozienti del sottoanello fondamentale e quindi è isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}_p$, con p primo, a seconda che K abbia caratteristica 0 o p.*

Dimostrazione. Per brevità poniamo $F_a := F_a(K)$ e $F_c := F_c(K)$. Per definizione di sottocampo fondamentale si ha che F_c è un sottoanello di K; quindi $F_a \subset F_c$ per definizione di sottoanello fondamentale. Dunque, per la proprietà universale del campo dei quozienti si ha $Q(F_a) \subseteq F_c$. Ma per definizione di sottocampo fondamentale, si ha $F_c \subseteq Q(F_a)$. In conclusione $F_c = Q(F_a)$.
Poiché F_a è isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_p$ con p primo, a seconda che $ch(K)$ sia 0 o p. Pertanto, se K ha caratteristica nulla, allora $F_c \cong \mathbb{Q}$, mentre se K ha caratteristica p, allora $F_c \cong \mathbb{Z}_p$. □

Esempio 4.2.1. Chiaramente $F_c(\mathbb{Q}) = \mathbb{Q}$ e $F_c(\mathbb{Z}_p) = \mathbb{Z}_p$, per ogni p primo.

Osservazione 4.3. Si prova (facilmente) che ogni sottocampo di K ha lo stesso sottocampo fondamentale di K. In particolare ha la sua stessa caratteristica. Ne segue che ogni campo numerico (cioè ogni sottocampo di $\mathbb{C}$) ha caratteristica 0. Osserviamo infine che ogni campo di caratteristica 0, contenendo una copia isomorfa di $\mathbb{Q}$, è infinito. Equivalentemente, un campo finito ha necessariamente caratteristica finita.

Esempio 4.3.1. Sia $K := \{0, 1, \alpha, \beta\}$ un insieme di 4 elementi distinti un insieme su cui siano definite un'operazione di addizione e una moltiplicazione in modo che:
I) entrambe le operazioni siano commutative e associative;
II) 0 e 1 siano elementi neutri della somma e del prodotto, rispettivamente;
III) il prodotto sia distributivo rispetto alla somma;
e in cui valgano le seguenti relazioni:
i) $2x = 0$ per ogni elemento x di K;
ii) $1 + \alpha = \beta$;
iii) $\alpha^2 = -\beta$.
Proviamo che K risulta essere un campo. Osserviamo dapprima che valgono le seguenti uguaglianze:
1) per i), si ha subito che $x = -x$ qualunque sia $x \in K$ considerato;
2) per ii), $\beta + 1 = \beta - \alpha + \beta = 2\beta - \alpha = -\alpha = \alpha$;
3) $\beta + \alpha = \beta + \beta - 1 = 2\beta - 1 = -1 = 1$.
In tal modo si ha che K è chiuso rispetto alla somma e all'opposto.
Esaminiamo ora il prodotto. Anche in tal caso occorre anzitutto provare che K è chiuso rispetto al prodotto. Per la distributività e per la (i), per ogni $x \in K$ si ha: $x \cdot 0 = x(1 + 1) = x + x = 0$. Inoltre $x \cdot 1 = x$ per (I) e $\alpha^2 = \beta \in K$ per (iii) e (i); dunque resta solo da provare che $\beta^2, \alpha\beta \in K$.
4) $\beta^2 = (1 + \alpha)(1 + \alpha) = 1 + 2\alpha + \alpha^2$. Per (i) e (iii) si ottiene $\beta^2 = 1 + \beta$ e per (2) si ha $\beta^2 = \alpha \in K$;
5) $\beta\alpha = (1 + \alpha)\alpha = \alpha + \alpha^2$ e, applicando (iii), si ha $\beta\alpha = \alpha + \beta = 1$ per il punto (3).
Infine, da (5) segue che l'inverso di ogni elemento non nullo di K è interno a K. Dunque K è un campo.

* Versione 5.6.2017

Da ora in poi si intenderà con termine *campo* un campo non nullo, cioè tale che 1_K e 0_K sono distinti.

Iniziamo ricordando che un omomorfismo tra campi è semplicemente un omomorfismo d'anelli.

È diretta conseguenza della definizione il fatto che, se $\varphi : K \longrightarrow K'$ è un omomorfismo di campi, allora $\varphi(x)^{-1} = \varphi(x^{-1})$ per ogni $x \in K^*$.

Osservazione 4.4. Se $\varphi : K \longrightarrow K'$ è un omomorfismo di campi diverso dall'omomorfismo nullo, allora il suo nucleo è un ideale di K diverso da K stesso. Ma un campo non ha ideali non banali, dunque il nucleo è nullo. Pertanto φ è iniettivo e quindi è naturale dare la seguente

Definizione. Un omomorfismo non nullo di campi campi $\varphi : K \longrightarrow K'$ viene detto *immersione* di K in K'.

Vediamo una semplice generalizzazione di 4.3:

Proposizione 4.5. *Se $\varphi : K \longrightarrow K'$ è una immersione di campi, allora i sottocampi fondamentali di K e di K' sono isomorfi via φ. In particolare, K e K' hanno la stessa caratteristica.*

Dimostrazione. Per 4.3 il sottocampo fondamentale di $\varphi(K)$ coincide con il sottocampo fondamentale di K'. Per completare la dimostrazione basta quindi provare che, se $\varphi : K \longrightarrow K'$ è un isomorfismo di campi allora i rispettivi sottocampi fondamentali sono isomorfi. Infine è chiaro che, a tale scopo, è sufficiente dimostrare che se H è un sottocampo di K allora $\varphi(H)$ è un sottocampo di K'.
Per 0.40, essendo φ un omomorfismo d'anelli e H un sottoanello di K, si ha che $\varphi(H)$ è un sottoanello di K'. Resta quindi da mostrare che, se $0_{K'} \neq y \in \varphi(H)$ allora $y^{-1} \in \varphi(H)$. Poichè φ è un isomorfismo, esiste un unico $x \in H$ tale che $\varphi(x) = y$. Essendo H un campo, $x^{-1} \in H$, quindi $\varphi(x^{-1}) \in \varphi(H)$. Ma $\varphi(x^{-1}) = \varphi(x)^{-1} = y^{-1}$ e questo conclude la dimostrazione. □

Un'altra pecularità del sottocampo fondamentale è la seguente:

Proposizione 4.6. *Se $\varphi : K \longrightarrow K$ è un automorfismo (cioè un isomorfismo di K in sé) allora φ ristretta al sottocampo fondamentale, cioè $\varphi_{|F_c(K)} : F_c(K) \longrightarrow F_c(K)$, coincide con l'identità.*

Dimostrazione. Si osservi che, per 4.5, $\varphi_{|F_c(K)}$ è un isomorfismo di campi.
Per 4.2, il generico elemento del sottocampo fondamentale di K è della forma

$$\frac{m1_K}{n1_K}, \quad \text{con} \quad n \notin (p)$$

dove $p = ch(K)$ (eventualmente anche $p = 0$). Poiché φ è un isomorfismo di campi, $\varphi(1_K) = 1_K$ e quindi

$$\varphi(m1_K) = m\varphi(1_K) = m1_K, \quad \text{per ogni} \quad m \in \mathbb{Z}.$$

Infine si osservi che, essendo un isomorfismo di campi, φ rispetta il prodotto e l'inverso, pertanto

$$\varphi\left(\frac{m1_K}{n1_K}\right) = \frac{\varphi(m1_K)}{\varphi(n1_K)} = \frac{m1_K}{n1_K}$$

dove l'ultima uguaglianza segue da quanto osservato sopra. □

Esempio 4.6.1. Se K è $\mathbb{Q}$ oppure $\mathbb{Z}_p$, il suo unico automorfismo è l'identità. Questo vale poichè $\mathbb{Q}$ (rispettivamente $\mathbb{Z}_p$) è sottocampo fondamentale di sè stesso.

Esercizio 4.6.2. Se K è $\mathbb{R}$, il suo unico automorfismo è l'identità. Infatti $\mathbb{R}$ è un campo ordinato, quindi posso considerare due numeri $r, s \in \mathbb{R}$ tali che $r \geq s$ e quindi $r - s \geq 0$. Per le proprietà di $\mathbb{R}$ si ha che esiste sicuramente un $x \in \mathbb{R}$ tale che $r - s = x^2$. Sia ora φ un automorfismo di $\mathbb{R}$. Chiaramente $\varphi(r) - \varphi(s) = \varphi(r - s) = \varphi(x^2) = \varphi(x)^2$. Ma il quadrato di un elemento di $\mathbb{R}$ è sempre positivo e quindi possiamo dire che $\varphi(r) \geq \varphi(s)$. Abbiamo in tal modo dimostrato che φ preserva l'ordine. Completare...

Esempio 4.6.3. Se K è $\mathbb{C}$, il coniugio è un automorfismo, dunque ci sono automorfismi di $\mathbb{C}$ oltre l'identità. Infatti si ricordi che il coniugio è definito come $\chi : \mathbb{C} \longrightarrow \mathbb{C}$ dove $a + ib \mapsto a - ib$. Si verifica facilmente

che χ è un omomorfismo d'anelli (dunque di campi), evidentemente suriettivo. Basta dunque provare che è iniettivo. Ma ciò segue immediatamente da 4.4, essendo χ non nullo.

Osservazione 4.7. Indicando con $Aut(K)$ il gruppo degli automorfismi di campi di un campo K ($Aut(K)$ è un gruppo rispetto alla composizione), dagli esempi ed esercizi precedenti segue che

$$Aut(\mathbb{Q}) = \{id_{\mathbb{Q}}\}, \quad Aut(\mathbb{Z}_p) = \{id_{\mathbb{Z}_p}\}, \quad Aut(\mathbb{R}) = \{id_{\mathbb{R}}\}, \quad Aut(\mathbb{C}) \supseteq \{id_{\mathbb{C}}, \chi\}.$$

Un ulteriore esempio di endo(auto) morfismo si ha nel caso di un campo di caratteristica positiva.

Proposizione-Definizione 4.8. *Sia K un campo di caratteristica p. L'applicazione*

$$\Phi : K \longrightarrow K \quad \textit{definita da} \quad x \mapsto x^p$$

è un'immersione di campi, detta endomorfismo di Frobenius di K. In particolare, se K è finito, Φ è un automorfismo.

Dimostrazione. È immediato verificare che, per ogni $x, y \in K$: $(x+y)^p = x^p + y^p$ e $(xy)^p = x^p y^p$. Dunque Φ è un omomorfismo di anelli (e quindi di campi). Inoltre per 4.4, essendo non nullo è iniettivo, dunque è una immersione di campi.
L'ultima affermazione segue dal fatto che un'applicazione iniettiva tra due insiemi finiti con lo stesso numero di elementi è anche suriettiva. □

Osservazione 4.9. Con la terminologia dell'Osservazione 4.7, si può sintetizzare il risultato precedente in tal modo: se K è un campo finito di caratteristica p allora $Aut(K) \supseteq \{id_K, \Phi\}$. Questo sembra contraddire il fatto che $Aut(\mathbb{Z}_p) = \{id_{\mathbb{Z}_p}\}$. Ma non è così! Infatti se K è proprio $\mathbb{Z}_p$, allora l'automorfismo di Frobenius è l'identità per il Piccolo Teorema di Fermat (vedi 1.4).

Ampliamenti di campi

Definizione. Se K e K' sono due campi, diciamo che K' è un *ampliamento* di K se esiste un'immersione di K in K'. Identificando K con la sua immagine, scriveremo $K \subseteq K'$.

Osserviamo che ogni campo è un ampliamento del suo sottocampo fondamentale.

Un altro esempio: il campo delle funzioni razionali in n indeterminate $K(X_1, \ldots, X_n)$ è un ampliamento del campo K dei coefficienti.

Consideriamo l'ampliamento $\mathbb{Q} \subset \mathbb{R}$ e il numero reale $\sqrt{2} \notin \mathbb{Q}$. In analogia con quanto visto per il sottocampo fondamentale, possiamo considerare l'intersezione di tutti i sottocampi di $\mathbb{R}$ contenenti $\mathbb{Q}$ e $\sqrt{2}$. Tale campo contiene $\mathbb{Q}$ ed è contenuto strettamente in $\mathbb{R}$. Indicando tale campo con $\mathbb{Q}(\sqrt{2})$, si ha dunque

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}.$$

Vediamo di generalizzare e precisare tale situazione.

Definizione. Se $K \subseteq K'$ è un ampliamento di K e S è un sottoinsieme di K', il più piccolo sottocampo di K' contenente K ed S viene detto *ampliamento di K in K' generato da S* e si denota con $K(S)$. Diremo, in particolare che tale ampliamento è *finitamente generato* se esiste un insieme finito $\alpha_1, \ldots, \alpha_n \in K'$ tale che tale ampliamento ha la forma $K(\alpha_1, \ldots, \alpha_n)$. Infine se $n = 1$ e dunque ha la forma $K(\alpha)$, diremo che tale ampliamento è *semplice*.

Osservazione 4.10. (a) Si noti che se $S \subset K$, allora $K(S) = K$.
(b) E' chiaro dalla definizione che se $K \subseteq K' \subseteq K''$ sono due ampliamenti e S è un sottoinsieme di K', allora l'ampliamento di K in K' generato da S e l'ampliamento di K in K'' generato da S coincidono. Questo è coerente con la notazione che denota (entrambi!) con $K(S)$.

Cerchiamo di esplicitare gli elementi di $K(\alpha_1, \ldots, \alpha_n)$, ove gli α_i sono elementi dell'ampliamento K'.

Si osservi che $K(\alpha_1, \ldots, \alpha_n)$, essendo chiuso rispetto a somma e prodotto, contiene tutte le espressioni polinomiali in $\alpha_1, \ldots, \alpha_n$ a coefficienti in K, dunque contiene $K[\alpha_1, \ldots, \alpha_n]$ e tale anello è l'immagine dell'omomorfismo di valutazione

$$v_\alpha : K[X_1, \ldots, X_n] \longrightarrow K'$$

dove

$$f(X_1, \ldots, X_n) \mapsto f(\alpha_1, \ldots, \alpha_n).$$

D'altra parte, se un campo contiene un anello, allora contiene anche il suo campo delle frazioni cioè

$$K(\alpha_1, \ldots, \alpha_n) \supseteq Q\left(K[\alpha_1, \ldots, \alpha_n]\right).$$

Quest'ultimo è un campo, contiene K e contiene $\alpha_1, \ldots, \alpha_n$. Ma, per definizione, $K(\alpha_1, \ldots, \alpha_n)$ è il più piccolo campo con questi requisiti: pertanto l'inclusione precedente è un'uguaglianza.
Abbiamo dunque provato la seguente

Proposizione 4.11. *Se $K \subseteq K'$ è un ampliamento di K e $\alpha_1, \ldots, \alpha_n \in K'$ allora $K(\alpha_1, \ldots, \alpha_n)$ è il campo delle frazioni dell'estensione polinomiale $K[\alpha_1, \ldots, \alpha_n]$. In particolare*

$$K \subseteq K[\alpha_1, \ldots, \alpha_n] \subseteq K(\alpha_1, \ldots, \alpha_n) \subseteq K'. \qquad \square$$

Esempio 4.11.1. Se K è un campo numerico e $\alpha \in \mathbb{C} \setminus K$ è tale che $\alpha^2 \in K$, allora l'ampliamento semplice di K in $\mathbb{C}$ generato da α è

$$K(\alpha) = \{a + \alpha b \mid a, b \in K\}.$$

Infatti, si osservi dapprima che $K[\alpha] = \{a + \alpha b \mid a, b \in K\}$, in quanto ogni elemento di $K[\alpha]$ è del tipo

$$\begin{aligned} a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n &= \sum(\text{potenze pari di } \alpha) + \sum(\text{potenze dispari di } \alpha) \\ &= \sum(\text{potenze pari di } \alpha) + \alpha \sum(\text{potenze pari di } \alpha) \end{aligned}.$$

Per ipotesi $\alpha^2 \in K$, dunque anche la somma di potenze pari di α appartiene a K. Questo prova che $K[\alpha] = \{a + \alpha b \mid a, b \in K\}$.
Il successivo passaggio è osservare che tale anello è un campo; questo, assieme a 4.11, prova l'affermazione iniziale.
Per provare che ogni elemento non nullo di $K[\alpha]$ è invertibile, basta notare che per ogni $a + \alpha b \neq 0$ esiste $x + \alpha y$, con $x, y \in K$, tale che

$$(a + \alpha b)(x + \alpha y) = 1.$$

Con semplici conti si prova che l'unica soluzione di tale equazione è

$$x = \frac{a}{a^2 - \alpha^2 b^2} \quad , \quad y = \frac{-b}{a^2 - \alpha^2 b^2}.$$

Esempio 4.11.2. Come caso particolare del precedente esempio, con $K = \mathbb{R}$ e $\alpha = i$, si ha che $\mathbb{C} = \mathbb{R}(i)$.

Esempio 4.11.3. Un altro caso particolare è dato dall'ampliamento semplice di $\mathbb{Q}$ in $\mathbb{R}$ generato da $\sqrt{2}$

$$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}.$$

Ovviamente, per 4.10 (b), coincide con l'ampliamento di $\mathbb{Q}$ in $\mathbb{C}$ generato da $\sqrt{2}$.

Esempio 4.11.4. L'ampliamento $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ è finitamente generato. Ma è semplice?
Iniziamo a esprimerlo con una successione di ampliamenti semplici:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

A) Osserviamo anzitutto che le inclusioni precedenti sono strette. Infatti è noto che $\sqrt{2}$ non è razionale. Inoltre $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Altrimenti, grazie alla descrizione di 4.11.3, esisterebbero due numeri razionali a e b tali che

$$\sqrt{3} = a + b\sqrt{2} \quad \Rightarrow \quad 3 = a^2 + 2b^2 + 2ab\sqrt{2}$$

da cui risulterebbe $\sqrt{2} \in \mathbb{Q}$.
Infine si verifica l'ultima uguaglianza come segue.
"$\supseteq$" È chiaro che $\left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$ contiene $\mathbb{Q}$, $\sqrt{2}$, $\sqrt{3}$. Dunque contiene il più piccolo campo che li contiene, cioè $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
"$\subseteq$" Per quanto visto in 4.11.1

$$\left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3}) = \left\{x + y\sqrt{3} \mid x, y \in \mathbb{Q}(\sqrt{2})\right\} = \left\{(a + b\sqrt{2}) + (a' + b'\sqrt{2})\sqrt{3} \mid a, b, a', b' \in \mathbb{Q}\right\}$$

quindi è immediata l'inclusione $\left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3}) \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Pertanto $\left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, come volevamo.
B) Quest'ultima espressione di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ci fa intuire che anche questo ampliamento è semplice. Infatti, posto $\alpha = \sqrt{2} + \sqrt{3}$ si ha che

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha).$$

Infatti l'inclusione "$\supseteq$" è ovvia. Per provare l'altra basta dimostrare che $\sqrt{2} \in \mathbb{Q}(\alpha)$ e $\sqrt{3} \in \mathbb{Q}(\alpha)$.
A tale scopo si osservi che $\sqrt{3} = \alpha - \sqrt{2}$; elevando al quadrato si ha $3 = \alpha^2 - 2\alpha\sqrt{2} + 2$. Quindi

$$\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha)$$

e quindi si ha anche che $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$.

Esempio 4.11.5. Ci sono ampliamenti finitamente generati che non sono semplici. Ad esempio $K \subset K(X, Y)$ non è semplice. Più avanti questo sarà giustificato dal fatto che X ed Y sono particolari elementi, detti trascendenti su K.

Esempio 4.11.6. Si osservi che negli esempi precedenti $K(\alpha) = K[\alpha]$. Ma questo non accade se α non è algebrico. Ad esempio, $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$.

Elementi algebrici e trascendenti

Definizione. Sia $K \subseteq K'$. Un elemento $\alpha \in K'$ si dice *algebrico su* K se è radice di un polinomio non nullo $f(X) \in K[X]$. Altrimenti si dice *trascendente su* K.

Osservazione 4.12.

a) Se $\alpha \in K$ è banalmente algebrico su K.

b) Il Principio d'identità dei polinomi si può sintetizzare (anche se in modo impreciso, in quanto una indeterminata non è un elemento di un campo...) dicendo che "ogni indeterminata su un campo K è trascendente su K".

c) Se $K \subseteq K' \subseteq K''$ un elemento $\alpha \in K''$ può essere algebrico su K' ma non su K. Ad esempio siano $K = \mathbb{Q}$, $K' = \mathbb{Q}(\pi^2)$ e $K'' = \mathbb{Q}(\pi)$. Dunque

$$\mathbb{Q} \subseteq \mathbb{Q}(\pi^2) \subseteq \mathbb{Q}(\pi).$$

Chiaramente $\pi \in \mathbb{Q}(\pi)$ è trascendente su $\mathbb{Q}$ ma è algebrico su $\mathbb{Q}(\pi^2)$. Infatti è radice del polinomio

$$X^2 - \pi^2 \in \left(\mathbb{Q}(\pi^2)\right)[X].$$

Definizione. Un numero complesso si dice semplicemente *algebrico* (risp. *trascendente*) se lo è su $\mathbb{Q}$.

Ad esempio, se $d \in \mathbb{N}$ allora $\sqrt[n]{d}$ è un numero reale algebrico in quanto radice del polinomio $X^n - d \in \mathbb{Q}[X]$. È pure noto che $i \in \mathbb{C}$ è algebrico in quanto radice del polinomio $X^2 + 1 \in \mathbb{Q}[X]$.

Osservazione 4.13. Se $K \subseteq K'$ è un ampliamento di campi e $\alpha \in K'$, allora (per definizione): α è algebrico su K se e solo se esiste $f(X) \in K[X]$ tale che $f(\alpha) = 0$ se e solo se $\ker(v_\alpha) \neq 0$, dove

$$v_\alpha : K[X] \longrightarrow K'$$

è la valutazione in α. Ricordiamo che $K[X]$ è un PID, dunque anche il nucleo di v_α (che consiste di tutti i polinomi che si annullano in α) è un ideale principale.
Si osservi inoltre che ogni generatore di tale ideale ha grado minimo tra tutti i polinomi che si annullano in α; inoltre uno solo tra questi è monico (vedi 3.14).

Definizione. Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$ algebrico su K. Se $\ker(v_\alpha) = (m(X))$ e $m(X)$ è monico, allora $m(X)$ si dice *polinomio minimo di α su K*. In particolare se $n := \deg(m(X))$, diciamo che α è *algebrico di grado n su K*.

Proposizione 4.14. *Siano $K \subseteq K'$ un ampliamento di campi, $\alpha \in K'$ algebrico su K e $p(X) \in K[X]$ un polinomio che si annulla su α. Allora*

$$p(X) \text{ è il polinomio minimo di } \alpha \iff p(X) \text{ è monico e irriducibile.}$$

Dimostrazione. Denotiamo con n il grado di $p(X)$.
"$\Rightarrow$" Il polinomio $p(X)$ è monico per definizione. Supponiamo che $p(X)$ sia riducibile cioè che si possa fattorizzare in $K[X]$ in modo non banale come $p(X) = f(X)g(X)$, con $\deg(f) < n$ e $\deg(g) < n$.
Valutando tale polinomio in α si avrebbe che $0 = p(\alpha) = f(\alpha)g(\alpha)$ in K. Quindi $f(\alpha) = 0$ oppure $g(\alpha) = 0$, il che risulta essere assurdo poiché $p(X)$ è il polinomio minimo di α su K.
"$\Leftarrow$" Poiché il polinomio $p(X)$ è monico per ipotesi, basta provare che ha grado minimo tra quelli che si annullano in α. Supponiamo che esista $h(X) \in K[X]$ tale che $h(\alpha) = 0$, che $h(X)$ sia di grado minimo tra i polinomi che si annullano su α e che $\deg(h) < n$. Possiamo dividere $p(X)$ per $h(X)$ e in tal modo otteniamo $p(X) = h(X)q(X) + r(X)$, con $\deg(r) < \deg(h)$ oppure $r = 0$.
Valutando tale polinomio in α e tenendo conto che $p(\alpha) = 0 = h(\alpha)$, si ottiene immediatamente che $r(\alpha) = 0$. Ma questo non è possibile se r è non nullo, in quanto $h(X)$ è di grado minimo tra i polinomi che si annullano su α. Pertanto $r(X) = 0_{K[X]}$ e quindi $p(X) = h(X)q(X)$, il che contraddice l'ipotesi che $p(X)$ sia irriducibile. Quindi $p(X)$ è il polinomio minimo di α su K. □

Corollario 4.15. *Sia $K \subseteq \mathbb{C}$ un campo numerico. Ogni polinomio monico e irriducibile di $K[X]$ è il polinomio minimo di ogni sua radice complessa.* □

Osservazione 4.16.

i) Si considerino due ampliamenti $K \subseteq K' \subseteq K''$ e $\alpha \in K''$. Se α è algebrico di grado n su K allora è algebrico di grado m su K', dove $m \leq n$.

ii) Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$. Allora α è algebrico su K di grado 1 se e solo se $\alpha \in K$.

iii) Ogni $\alpha \in \mathbb{C} \setminus \mathbb{R}$ è algebrico di grado 2 su $\mathbb{R}$. Infatti se $\alpha = a + ib$, allora α è radice del polinomio

$$f(X) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} \in \mathbb{R}[X].$$

Esempio 4.16.1 Come esempio della situazione descritta in 4.16 (i), si considerino gli ampliamenti

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

e l'elemento $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Vediamo che α è algebrico di grado 2 su $\mathbb{Q}(\sqrt{2})$, essendo radice del polinomio (irriducibile)

$$X^2 - 2\sqrt{2}X - 1 \in \mathbb{Q}(\sqrt{2})[X].$$

Invece α è algebrico di grado 4 su $\mathbb{Q}$, essendo radice del polinomio

$$X^4 - 10X^2 + 1 \in \mathbb{Q}[X].$$

Tale polinomio, inoltre, è irriducibile su $\mathbb{Q}$ mentre è riducibile su $\mathbb{Q}(\sqrt{2})$:

$$X^4 - 10X^2 + 1 = (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1).$$

Nel seguito può essere utile modificare la notazione finora adottata per l'omomorfismo di valutazione, restringendone il codominio in modo che sia sempre suriettivo. Precisamente, se $K \subseteq K'$ è un ampliamento di campi e $\alpha \in K'$, poniamo

$$v_\alpha : K[X] \longrightarrow K[\alpha] \quad (\subseteq K')$$

definito come al solito da $f(X) \mapsto f(\alpha)$.

Teorema 4.17. *(Teorema di Kronecker, 1882). Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$. Si hanno i seguenti fatti:*

i) se α è trascendente su K allora v_α è un isomorfismo; in particolare $K[X] \cong K[\alpha]$ e $K(X) \cong K(\alpha)$.

ii) se α è algebrico su K allora v_α ha per nucleo $(m(X))$, dove $m(X)$ è il polinomio minimo di α su K; dunque $K[\alpha] = K(\alpha)$.

Dimostrazione. *i)* Se α è trascendente su K allora non ci sono polinomi non nulli che hanno α come radice, cioè $\ker(v_\alpha) = (0)$. Pertanto v_α è iniettiva ed essendo suriettiva per definizione, è un isomorfismo di anelli:

$$v_\alpha : K[X] \xrightarrow{\cong} K[\alpha] \quad \text{che si estende a} \quad K(X) = Q(K[X]) \xrightarrow{\cong} Q(K[\alpha]) = K(\alpha).$$

ii) Da 4.13 e dalla definizione di polinomio minimo, segue la prima affermazione. Pertanto, per il I teorema di omomorfismo di anelli, v_α induce un isomorfismo di anelli

$$\overline{v}_\alpha : K[X]/(m(X)) \xrightarrow{\cong} K[\alpha].$$

Come osservato in 4.14, il polinomio $m(X)$ è irriducibile dunque l'ideale da esso generato è massimale. Pertanto $K[X]/(m(X))$ è un campo e quindi anche $K[\alpha]$ lo è. Questo prova che $K[\alpha]$ coincide col suo campo dei quozienti $K(\alpha)$. □

Corollario 4.18. *Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$. Allora*

$$\alpha \text{ è algebrico su } K \iff K[\alpha] = K(\alpha).$$

In tal caso, posto n il grado di α su K, si hanno i seguenti fatti:

i)

$$K[\alpha] = K(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_i \in K\};$$

ii) $K[\alpha] = K(\alpha)$ è un K-spazio vettoriale di dimensione n.

Dimostrazione. "⇒" Segue immediatamente da 4.17 (*ii*).
"⇐" Segue da 4.17 (*i*): se α fosse trascendente, allora $K[X] \cong K[\alpha]$ e $K(X) \cong K(\alpha)$, quindi $K[\alpha] \neq K(\alpha)$.
(*i*) Per il teorema di Kronecker, $K(\alpha) = K[\alpha] \cong K[X]/(m(X))$ e tale isomorfismo è definito come estensione polinomiale di $\alpha \mapsto \overline{X}$. Quindi ci siamo ricondotti a dimostrare che

$$K[X]/(m(X)) = \{c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} \mid c_i \in K\}.$$

E questo segue dal fatto (vedi 3.49) che in ogni classe di equivalenza del quoziente c'è un polinomio di grado minore di $n = \deg(m(X))$.
(*ii*) Per la parte precedente e per il teorema di Kronecker, si ha

$$K[\alpha] = K(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_i \in K\}$$

dunque il K-spazio vettoriale $K[\alpha]$ è generato da $1, \alpha, \ldots, \alpha^{n-1}$ su K. Per provare che tali elementi sono anche linearmente indipendenti (e quindi costituiscono una base) basta osservare che i loro corrispondenti $1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1} \in K[X]/(m(X))$, via l'isomorfismo $\overline{v}_\alpha$, sono linearmente indipendenti su K. Sia dunque

$$\overline{0} = c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} = \overline{c_0 + c_1X + \cdots + c_{n-1}X^{n-1}}.$$

Questo implica che $c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in (m(X))$. Poiché $m(X)$ ha grado n, questo implica che il polinomio in questione è nullo. Quindi $c_i = 0$ per ogni i. □

Per 4.18 si ha in particolare che, se α è algebrico su K, allora $K[\alpha]$ è un K-spazio vettoriale di dimensione finita. È ancora una conseguenza del Teorema di Kronecker il viceversa.

Corollario 4.19. *Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$. Se $K[\alpha]$ è un K-spazio vettoriale di dimensione finita, allora α è algebrico su K.*

Dimostrazione. Se α fosse trascendente su K allora, per 4.17, si avrebbe $K[\alpha] \cong K[X]$ che, come è noto, è un K-spazio vettoriale di dimensione infinita. □

Gli ultimi due risultati mostrano l'equivalenza di tre condizioni su un elemento di un ampliamento. Introduciamo ora una quarta condizione, legata alla seguente nozione.

Definizione. Sia $K \subseteq K'$ un ampliamento di campi. La dimensione di K' come K-spazio vettoriale si dice *grado di K' su K* e si indica con $[K' : K]$. Se tale dimensione è finita diremo che K' è un *ampliamento di grado finito di K* o semplicemente che K' è *finito su K*.

In altre parole, K' è un ampliamento finito di K se è un K-spazio vettoriale finitamente generato.
È evidente che $[K' : K] = 1$ se e solo se $K = K'$. Il primo esempio non banale di ampliamento finito è $\mathbb{C}$ su $\mathbb{R}$, infatti $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2$. Invece $K(X)$ non è un ampliamento finito di K, cioè $[K(X) : K] = \infty$.

Proposizione 4.20. *Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$. Sono equivalenti:*
i) α è algebrico su K;
ii) $K[\alpha] = K(\alpha)$;
iii) $K[\alpha]$ è un K-spazio vettoriale di dimensione finita;
iv) $[K(\alpha) : K] < \infty$.
Inoltre se valgono le precedenti proprietà, allora il grado di α su K è $[K(\alpha) : K]$.

Dimostrazione. $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ per 4.18 e 4.19. Inoltre ovviamente $(ii) + (iii) \Rightarrow (iv)$.
Resta da provare che la quarta implica una delle tre precedenti.
$(iv) \Rightarrow (iii)$ Poiché $K[\alpha]$ è un sotto-K-spazio vettoriale di $K(\alpha)$, vale

$$\dim_K K[\alpha] \leq \dim_K K(\alpha)$$

dunque essendo $\dim_K K(\alpha)$ finita per ipotesi anche $\dim_K K[\alpha]$ è finita. □

È immediato il seguente corollario, che è una riformulazione dell'equivalenza tra (i) e (iv) di 4.20.

Corollario 4.21. *Siano $K \subseteq K'$ un ampliamento di campi e $\alpha \in K'$. Allora α è trascendente su K se e solo se $K(\alpha)$ ha grado infinito su K.* □

Il grado di un ampliamento gode della proprietà moltiplicativa, di cui omettiamo la dimostrazione.

Proposizione 4.22. *(Legge della torre). Siano $K \subseteq K' \subseteq K''$ ampliamenti di campi. Allora*

$$K'' \text{ è finito su } K \iff K'' \text{ è finito su } K' \text{ e } K' \text{ è finito su } K$$

e in tal caso vale

$$[K'' : K] = [K'' : K'] \, [K' : K].$$ □

Esempio 4.22.1 Si consideri la situazione di 4.16.1 che descrive gli ampliamenti

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

dove le inclusioni sono strette. Posto $\alpha := \sqrt{2} + \sqrt{3}$, abbiamo visto che α è algebrico di grado 2 (risp. 4) su $\mathbb{Q}(\sqrt{2})$ (risp. $\mathbb{Q}$), avendo come polinomio minimo su $\mathbb{Q}(\sqrt{2})$ (risp. su $\mathbb{Q}$):

$$X^2 - 2\sqrt{2}X - 1 \in \mathbb{Q}(\sqrt{2})[X] \quad \text{e, rispettivamente,} \quad X^4 - 10X^2 + 1 \in \mathbb{Q}[X].$$

Dunque, per 4.20, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 2$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Infine è noto che $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
In tal modo si verifica direttamente la Legge della torre:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Corollario 4.23. *Siano $K \subseteq K' \subseteq K''$ ampliamenti di campi. Se $[K'' : K] = p$ numero primo, allora o $K'' = K'$ oppure $K' = K$.* □

Proposizione 4.24. *Sia $K \subseteq K'$ un ampliamento finito e $\alpha \in K'$. Allora α è algebrico su K.*

Dimostrazione. Si considerino gli ampliamenti di campi

$$K \subseteq K(\alpha) \subseteq K'.$$

Per 4.22, anche $K \subseteq K(\alpha)$ è un ampliamento finito. Quindi, per 4.20, α è algebrico su K. □

Dalla proposizione 4.24, ogni elemento di un ampliamento finito di K è algebrico su K. È naturale dunque dare la seguente

Definizione. Sia $K \subseteq K'$ un ampliamento di campi. Diciamo che K' è un *ampliamento algebrico* di K se ogni elemento di K' è algebrico su K.

È quindi immediata la seguente fondamentale proprietà:

Proposizione 4.25. *Ogni ampliamento finito è algebrico.* □

Esempio 4.25.1. Poiché $[\mathbb{C} : \mathbb{R}] = 2$, chiaramente $\mathbb{C}$ è algebrico su $\mathbb{R}$ (già visto in 4.16 in modo esplicito).

Esempio 4.25.2. Anche l'ampliamento $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ è finito, in quanto $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Dunque tale ampliamento è algebrico dunque ogni elemento di $\mathbb{Q}(\sqrt{2})$ è algebrico e non solo $\sqrt{2}$.

Esempio 4.25.3. Invece l'ampliamento $\mathbb{Q} \subset \mathbb{R}$ non è algebrico (e quindi non finito): contiene infatti numeri trascendenti, ad esempio π.

Una domanda naturale è chiedersi se vale il viceversa di 4.25. Vedremo che non è così. Tuttavia con i risultati precedenti si prova la seguente importante caratterizzazione degli ampliamenti finiti, che mostra "quanto manca" ad un ampliamento algebrico per essere finito.

Teorema 4.26. *Sia $K \subseteq K'$ un ampliamento di campi. Sono equivalenti:*
i) K' è finito su K;
ii) K' è algebrico su K e finitamente generato su K;
iii) $K' = K(\alpha_1, \ldots, \alpha_n)$ dove α_i algebrico su K per ogni $i = 1, \ldots, n$.

Dimostrazione. $(i) \Rightarrow (ii)$ Per 4.25, si ha che K' è algebrico su K. Se $(v_1, \ldots, v_n)$ è una base di K' come K-spazio vettoriale, si ha che $K' \subseteq K(v_1, \ldots, v_n)$. L'altra inclusione è ovvia: segue la tesi.
$(ii) \Rightarrow (iii)$ Ovvio.
$(iii) \Rightarrow (i)$ Poiché α_i è algebrico su K allora lo è su $K(\alpha_1, \ldots, \alpha_{i-1})$, per ogni $i = 1, \ldots, n$. Quindi, per 4.20 il grado $[K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]$ è finito per ogni i. Per la *Legge della torre* (4.22) si ha pertanto che $[K(\alpha_1, \ldots, \alpha_n) : K]$ è finito. □

Per trovare un ampliamento algebrico che non sia finito, dobbiamo quindi cercare un ampliamento algebrico non finitamente generato. Iniziamo questo studio con il seguente risultato preliminare.

Proposizione - Definizione 4.27. *Se $K \subseteq K'$ è un ampliamento di campi, l'insieme di tutti gli elementi di K' algebrici su K è un sottocampo di K', detto chiusura algebrica di K in K' e denotato con $\overline{K}_{K'}$.*

Dimostrazione. Siano $\alpha, \beta \in K'$ algebrici su K. È sufficiente mostrare che $\alpha - \beta$ e $\alpha\beta^{-1}$ sono elementi di K' (e questo è ovvio) algebrici su K.
Si osservi che $\alpha - \beta \in K(\alpha, \beta)$ e anche $\alpha\beta^{-1} \in K(\alpha, \beta)$. Ma $K(\alpha, \beta)$ è un ampliamento finito di K per 4.26; dunque è un ampliamento algebrico per 4.25. In particolare tutti i suoi elementi sono algebrici su K. □

Esempio 4.27.1. Consideriamo gli ampliamenti $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. I reali algebrici e i complessi algebrici sono, rispettivamente, le chiusure algebriche di $\mathbb{Q}$ in $\mathbb{R}$ e in $\mathbb{C}$. Ed è chiaro che

$$\overline{\mathbb{Q}}_{\mathbb{R}} = \mathbb{R} \cap \overline{\mathbb{Q}}_{\mathbb{C}}.$$

L'esempio precedente ci permette di trovare un caso in cui non vale il viceversa di 4.25.

Proposizione 4.28. *L'ampliamento*

$$\mathbb{Q} \subset \overline{\mathbb{Q}}_{\mathbb{R}}$$

è algebrico ma non finito.

Dimostrazione. Usiamo il fatto (che non proveremo) che per ogni $n \geq 2$, il polinomio $X^n - 2$ è irriducibile in $\mathbb{Q}[X]$ ed ammette una radice reale $\gamma_n := \sqrt[n]{2}$.

L'elemento γ_n è algebrico di grado n su $\mathbb{Q}$ e quindi $[\mathbb{Q}(\gamma_n) : \mathbb{Q}] = n$ per 4.20.
Se per assurdo $[\overline{\mathbb{Q}}_{\mathbb{R}} : \mathbb{Q}]$ fosse un certo M finito, allora per 4.22, si avrebbe che n divide M per ogni $n \geq 2$, ma questo è assurdo. □

Definizione. Sia $K \subseteq K'$ un ampliamento di campi. Diciamo che K è *algebricamente chiuso in* K' se coincide con la propria chiusura algebrica in K', cioè se

$$K = \overline{K}_{K'}.$$

Un campo si dice *algebricamente chiuso* se lo è in ogni suo ampliamento.

Una semplice ma importante caratterizzazione di tale nozione è il seguente risultato:

Proposizione 4.29. *Se K è un campo, le seguenti condizioni sono equivalenti:*
i) K è algebricamente chiuso;
ii) ogni polinomio non costante di $K[X]$ ha almeno una radice in K;
iii) ogni polinomio non costante di $K[X]$ ha tutte le radici in K;
iv) ogni polinomio non costante di $K[X]$ si fattorizza in polinomi di primo grado in $K[X]$;
v) i soli polinomi irriducibili di $K[X]$ sono quelli di primo grado.

Dimostrazione. *i)* $\Rightarrow$ *iii)* $\Rightarrow$ *ii)*: Ovvie.
ii) $\Rightarrow$ *iii)* Per induzione sul grado del polinomio e per il teorema di Ruffini (analogo a 3.51).
iii) $\Rightarrow$ *iv)* Ancora per il teorema di Ruffini.
iv) $\Rightarrow$ *v)* Ovvio.
v) $\Rightarrow$ *i)* Basta provare che, se K' è un ampliamento algebrico di K, allora $K' = K$. Sia $\alpha \in K'$; essendo algebrico su K, esiste il suo polinomio minimo in $K[X]$. Per 4.14 tale polinomio è irriducibile in $K[X]$, dunque di primo grado per ipotesi. Pertanto $\alpha \in K$. □

Esempio 4.29.1. La chiusura algebrica $\overline{\mathbb{Q}}_{\mathbb{R}}$ di $\mathbb{Q}$ in $\mathbb{R}$ è algebricamente chiusa *in* $\mathbb{R}$, ma non è algebricamente chiusa. Infatti non coincide, ad esempio, con $\overline{\mathbb{Q}}_{\mathbb{C}}$: l'elemento $i \in \mathbb{C}$ appartiene a $\overline{\mathbb{Q}}_{\mathbb{C}}$, essendo radice del polinomio $X^2 + 1$ a coefficienti razionali; ma non appartiene a $\overline{\mathbb{Q}}_{\mathbb{R}}$, non essendo reale.
Si può provare, inoltre, che $\overline{\mathbb{Q}}_{\mathbb{C}}$ è la chiusura algebrica di $\overline{\mathbb{Q}}_{\mathbb{R}}$ in $\mathbb{C}$, cioè

$$\overline{\left(\overline{\mathbb{Q}}_{\mathbb{R}}\right)}_{\mathbb{C}} = \overline{\mathbb{Q}}_{\mathbb{C}}.$$

Esempio 4.29.2. Il *Teorema fondamentale dell'algebra* (3.50) equivale ad affermare che $\mathbb{C}$ è algebricamente chiuso. Essendo inoltre un campo algebrico su $\mathbb{R}$, ne segue che $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$ in $\mathbb{C}$.

Come la nozione di campo algebricamente chiuso è sia relativa (ad un ampliamento) sia assoluta (v. Definizione precedente), analogamente si può dare una nozione assoluta di chiusura algebrica.

Definizione. Se K è un campo, si dice *chiusura algebrica* di K un campo che sia algebricamente chiuso e algebrico su K. Si denota con $\overline{K}$.

Per quanto visto in 4.29.2, $\mathbb{C}$ è *la* chiusura algebrica di $\mathbb{R}$.

Si può dimostrare che ogni campo possiede una chiusura algebrica e che le sue chiusure algebriche sono "essenzialmente" isomorfe tra loro.

Per quanto precede, si può pensare alla chiusura algebrica di un campo come al suo più grande ampliamento algebrico.

Infine si tenga conto che la chiusura algebrica di $\mathbb{Q}$ è la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$, cioè $\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_{\mathbb{C}}$. Dunque $\overline{\mathbb{Q}}_{\mathbb{C}}$ è algebricamente chiuso.
Tra $\overline{\mathbb{Q}}_{\mathbb{C}}$ e $\mathbb{C}$ ci sono infiniti campi algebricamente chiusi: le chiusure algebriche di ampliamenti trascendenti di $\mathbb{Q}$; ad esempio $\overline{\mathbb{Q}(\pi)}$.

Per quanto visto in 4.29, se K è un campo algebricamente chiuso, ogni polinomio a coefficienti in K si fattorizza totalmente in polinomi di primo grado in $K[X]$. Chiaramente ciò accade anche se K non è algebricamente chiuso: basta fattorizzare il polinomio nella sua chiusura algebrica (che è un campo algebricamente chiuso). Precisamente: se $f(X) \in K[X]$ è un polinomio di grado n, esistono $\alpha_1, \dots, \alpha_n \in \overline{K}$ e $c \in K$ tali che

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n).$$

Ad esempio, se $K = \mathbb{R}$ e quindi $\overline{K} = \mathbb{C}$, ogni polinomio a coefficienti reali si fattorizza completamente in $\mathbb{C}$.

È chiaro che, se si vuole fattorizzare *ogni* polinomio di $K[X]$ è necessario porsi all'interno della chiusura algebrica $\overline{K}$. Ma se si vuole fattorizzare un preciso polinomio? È sufficiente un ampliamento di K più piccolo della sua chiusura algebrica? Risponde a queste domande la seguente nozione:

Definizione. Se K è un campo e $f(X) \in K[X]$ è un polinomio di grado $n \geq 1$, un ampliamento K' di K si dice *campo di spezzamento di $f(X)$ su K* se esistono $\alpha_1, \dots, \alpha_n \in K'$ e $c \in K$ tali che
(-) $f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$ in $K'[X]$;
(-) $K' = K(\alpha_1, \dots, \alpha_n)$.

Occorre un risultato preliminare, la cui dimostrazione riprende la linea di quelle di 4.17 e 4.18.

Teorema 4.30. *Siano $f(X) \in K[X]$ un polinomio irriducibile di grado $n \geq 1$ e $K' := K[X]/(f(X))$; allora:*
i) K' è un ampliamento semplice di K, cioè $K' = K(\alpha)$, dove $\alpha = \overline{X}$;
ii) $f(X)$ ha una radice in K' e precisamente $f(\alpha) = 0$;
iii) $K' = K(\alpha) = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} \mid c_i \in K\}$
iv) $[K' : K] = n$;

Dimostrazione. Osserviamo dapprima che $f(X)$ è un polinomio irriducibile dunque primo; perciò l'ideale $(f(X))$ è primo e quindi massimale. Pertanto il quoziente $K' := K[X]/(f(X))$ è un campo.
i) La restrizione della proiezione $\pi : K[X] \longrightarrow K[X]/(f(X))$ al campo K risulta un'immersione $K \to K'$. Inoltre è chiaro che $K' = K[\overline{X}] = K(\overline{X})$.
ii) Ovviamente $\pi(f(X)) = 0$ cioè $f(\alpha) = 0$.
iii) Essendo $f(X)$ irriducibile, è il polinomio minimo di α su K, a meno di una costante moltiplicativa di K. Quindi α è algebrico su K di grado n. La tesi segue da 4.18.
iv) La tesi segue ancora da 4.18, dove si prova che $\dim_K K[\alpha]$ coincide col grado di α su K. □

Ora possiamo provare l'esistenza di un campo di spezzamento di un polinomio, cioè del più piccolo ampliamento algebrico del campo dei coefficienti contenente tutte le radici del polinomio.

Teorema 4.31. *Se K è un campo e $f(X) \in K[X]$ è un polinomio di grado $n \geq 1$, allora esiste un campo di spezzamento K' di $f(X)$ su K. Inoltre K' è finito su K e $[K' : K] \leq n!$.*

Dimostrazione. Se $f(X)$ ha tutte le radici in K allora $K' = K$ e la tesi è vera.
Supponiamo dunque che $p(X)$ sia un fattore irriducibile di $f(X)$ di grado ≥ 2. Allora per 4.30

$$K[X]/(p(X)) = K(\alpha_1) =: K_1$$

è un ampliamento semplice di K di grado $\deg(p) \leq n$. Ovviamente in $K_1[X]$ il polinomio si fattorizza come

$$f(X) = (X - \alpha_1)f_1(X).$$

Se $f_1(X)$ ha tutte le radici in K_1 allora $K' = K_1$ e la tesi è vera. Altrimenti, sia $p_1(X)$ un fattore irriducibile di $f_1(X)$ di grado ≥ 2. Si definisce $K_1[X]/(p_1(X)) = K_1(\alpha_2) = K(\alpha_1, \alpha_2) =: K_2$, che risulta essere un ampliamento semplice di K_1 di grado pari a $\deg(p_1) \leq n - 1$.
Iterando il procedimento si arriva a costruire il campo $K_n := K(\alpha_1, \dots, \alpha_n)$, dove eventualmente qualche α_i appartiene a K. Inoltre ad ogni passo si verificano:

$$[K_1 : K] \leq n, \quad [K_2 : K_1] \leq n - 1, \dots, \quad [K_{i+1} : K_i] \leq n - i, \dots$$

e applicando la Legge della torre si ottiene $[K_n : K] \leq n(n-1) \cdots 3 \cdot 2 = n!$. Inoltre in K_n vale

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$$

e quindi, ponendo $K' := K_n$, si conclude la dimostrazione. □

Si può dimostrare facilmente che due campi di spezzamento di un polinomio sono isomorfi (ogni isomorfismo tra due campi di spezzamento è l'identità sugli elementi di K e permuta le radici del polinomio considerato). Quindi si può parlare *del* campo di spezzamento di un polinomio.

Esempio 4.31.1. Il polinomio $f(X) = X^2 - 2\sqrt{2}X + 3$ può essere visto sia come elemento di $\mathbb{Q}(\sqrt{2})[X]$ sia come elemento di $\mathbb{R}[X]$. Il suo campo di spezzamento nei due casi è diverso.
Notiamo dapprima che le sue radici complesse sono $\sqrt{2} + i$ e $\sqrt{2} - i$. Pertanto l'ampliamento

$$\mathbb{Q}(\sqrt{2}) \quad \subset \quad \mathbb{Q}(\sqrt{2}, i)$$

è il campo di spezzamento di $f(X)$ su $\mathbb{Q}(\sqrt{2})$, in quanto $\mathbb{Q}(\sqrt{2}, i) = \big(\mathbb{Q}(\sqrt{2})\big)\,(\sqrt{2} + i, \sqrt{2} - i)$.
D'altra parte, guardando a $f(X)$ come a un polinomio a coefficienti reali, l'ampliamento

$$\mathbb{R} \quad \subset \quad \mathbb{R}(i) = \mathbb{C}$$

è il campo di spezzamento di $f(X)$ su $\mathbb{R}$, in quanto $\mathbb{R}(i) = \mathbb{R}(\sqrt{2} + i, \sqrt{2} - i)$.

Esempio 4.31.2. Sia $f(X) \in K[X]$ un polinomio irriducibile di grado 3. Ripercorrendo la dimostrazione di 4.31, poste $\alpha_1, \alpha_2, \alpha_3$ le sue radici (ad esempio in $\overline{K}$), si ha la successione di ampliamenti

$$K \;\subset\; K(\alpha_1) \;\subseteq\; K(\alpha_1, \alpha_2) \;\subseteq\; K(\alpha_1, \alpha_2, \alpha_3) = K'$$

dove K' è il campo di spezzamento di $f(X)$ su K. Per la Legge della torre si ha

$$[K' : K] = [K(\alpha_1, \alpha_2, \alpha_3) : K(\alpha_1, \alpha_2)]\;[K(\alpha_1, \alpha_2) : K(\alpha_1)]\;[K(\alpha_1) : K].$$

Come osservato nella dimostrazione

$$[K(\alpha_1) : K] \leq 3, \quad [K(\alpha_1, \alpha_2) : K(\alpha_1)] \leq 2, \quad [K(\alpha_1, \alpha_2, \alpha_3) : K(\alpha_1, \alpha_2)] \leq 1.$$

Si osservi però che essendo $f(X)$ irriducibile su K allora è il polinomio minimo (a parte una costante moltiplicativa) di α_1. Dunque $[K(\alpha_1) : K] = 3$.
Inoltre nessun grado è minore di uno, dunque $[K(\alpha_1, \alpha_2, \alpha_3) : K(\alpha_1, \alpha_2)] = 1$. Pertanto l'unica possibilità di variazione è nel grado dell'ampliamento centrale, che può essere 2 o 1. Ne segue che $[K' : K]$ può essere 3 o 6, come si vede nei seguenti esempi numerici.

Esempio 4.31.3. Sia $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Proviamo che $f(X)$ è irriducibile su $\mathbb{Q}$. Vediamo due dimostrazioni di questo fatto.
(I) È sufficiente mostrare che $f(X)$ non ha radici razionali (in quanto $\deg(f) = 3$). Per 3.66, essendo $f(X) \in \mathbb{Z}[X]$, se fosse $r/s \in \mathbb{Q}$ una sua radice, allora $r|1$ e $s|1$. Dunque tale radice sarebbe necessariamente 1, che è falso.
(II) Se $f(X)$ fosse riducibile su $\mathbb{Q}$ allora lo sarebbe su $\mathbb{Z}$, per 3.60. Ma, in tal caso, per 3.66, sarebbe riducibile su $\mathbb{Z}_p$ (dove chiaramente mantiene il suo grado, essendo un polinomio monico) per ogni p primo. Scegliendo, ad esempio, $p = 2$ si vede immediatamente che $f(X)$ non ha radici in $\mathbb{Z}_2$ ed è quindi irriducibile in quanto $\deg(f) = 3$.

Sia dunque $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ una sua radice. Una facile verifica mostra che

$$\beta := \alpha^2 - 2, \quad \gamma := -\alpha^2 - \alpha + 2$$

sono le altre radici. Pertanto

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \gamma) = \mathbb{Q}(\alpha, \beta, \gamma)$$

è il campo di spezzamento di $f(X)$ su $\mathbb{Q}$ e è un ampliamento di grado 3 su $\mathbb{Q}$.

Esempio 4.31.4. Sia $f(X) = X^3 - 2 \in \mathbb{Q}[X]$. Si verifica che $f(X)$ ha per radici

$$\alpha, \alpha z, \alpha z^2, \quad \text{dove} \quad \alpha = \sqrt[3]{2},\ z = \frac{-1 + i\sqrt{3}}{2}.$$

Come visto nel caso generale in 4.31.2,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3, \quad [\mathbb{Q}(\alpha, \alpha z, \alpha z^2) : \mathbb{Q}(\alpha, \alpha z)] = 1.$$

L'ultima uguaglianza (vista nel teorema) si può provare direttamente. Infatti $\alpha z^2 \in \mathbb{Q}(\alpha, \alpha z)$, come si verifica facilmente osservando che $z^2 + z = -1$ e dunque $\alpha z^2 = -\alpha z - \alpha \in \mathbb{Q}(\alpha, \alpha z)$.
Resta solo da calcolare $[\mathbb{Q}(\alpha, \alpha z) : \mathbb{Q}(\alpha)]$. Si osservi che

$$\mathbb{Q}(\alpha, \alpha z) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \quad \text{e} \quad \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$$

e chiaramente $i\sqrt{3}$ è algebrico di grado 2 su $\mathbb{Q}(\sqrt[3]{2})$. Pertanto il campo di spezzamento di $f(X)$ su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ che ha grado 6 su $\mathbb{Q}$.

Esempio 4.31.5. Sia $f(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$. Si verifica che $f(X)$ non ha radici in $\mathbb{Z}_2$ ed è dunque irriducibile su tale campo. Chiaramente ha una radice $\alpha = \overline{X} \in \mathbb{Z}_2[X]/(f(X))$. Vediamo che struttura ha il campo $\mathbb{Z}_2[X]/(f(X)) = \mathbb{Z}_2[\alpha] = \mathbb{Z}_2(\alpha)$ e se è un campo di spezzamento per f.
Come è noto, poiché $f(X)$ è il polinomio minimo di α su $\mathbb{Z}_2$, si ha

$$\mathbb{Z}_2(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_2\}$$

dunque tale campo è costituito da 8 elementi. Inoltre

$$f(X) = (X - \alpha)\, g(X)$$

dove ovviamente $g(X)$ non ha radici in $\mathbb{Z}_2$ ed è dunque irriducibile come f.
Si calcola facilmente che $g(X) = X^2 + \alpha X + (1 + \alpha^2)$. Supponiamo che abbia una radice β in $\mathbb{Z}_2(\alpha)$; dunque $\beta = a + b\alpha + c\alpha^2$, per opportuni $a, b, c \in \mathbb{Z}_2$. Sostituendo in $g(X)$ si ottiene

$$(a + b\alpha + c\alpha^2)^2 + \alpha(a + b\alpha + c\alpha^2) + (1 + \alpha^2) = 0.$$

Tenuto conto che i doppi prodotti nel primo quadrato sono nulli, in quanto i coefficienti appartengono a $\mathbb{Z}_2$ e usando l'identità $\alpha^3 = \alpha + 1$ (e quindi $\alpha^4 = \alpha^2 + \alpha$) si ottiene

$$a^2 + b^2\alpha^2 + c^2(\alpha^2 + \alpha) + \alpha a + b\alpha^2 + c(\alpha + 1) + 1 + \alpha^2 = 0$$

da cui

$$(b^2 + b + c^2 + 1)\alpha^2 + (a + c + c^2)\alpha + (a^2 + c + 1) = 0$$

Ma α è algebrico di grado 3 su $\mathbb{Z}_2$ e quindi non è radice di alcun polinomio di grado 2. Quindi tutti e 3 i coefficienti devono essere nulli, dunque devono essere radici (in $\mathbb{Z}_2$) del sistema:

$$\begin{cases} b^2 + b + c^2 + 1 &= 0 \\ a + c + c^2 &= 0 \\ a^2 + c + 1 &= 0 \end{cases}$$

ed è immediato vedere (dalla seconda e terza equazione) che necessariamente $a = 0$ e $c = 1$ in $\mathbb{Z}_2$, mentre b può essere sia 0 che 1. Pertanto $g(X) = X^2 + \alpha X + (1 + \alpha^2)$ ha due radici β e γ in $\mathbb{Z}_2(\alpha)$ che sono $\beta = \alpha^2$ e $\gamma = \alpha + \alpha^2$, come si verifica facilmente per sostituzione.
Questo prova che $\mathbb{Z}_2(\alpha)$ è un campo di spezzamento per f in quanto

$$f(X) = (X - \alpha)(X - \beta)(X - \gamma), \quad \text{dove} \quad \beta = \alpha^2,\ \gamma = \alpha + \alpha^2.$$

Nell'ultimo esempio abbiamo introdotto un campo di 8 elementi (ivi denotato con $\mathbb{Z}_2(\alpha)$). È naturale chiedersi se si può dire qualcosa sul numero di elementi di un campo finito. Ovviamente, se tale campo è di tipo $\mathbb{Z}_p$, con p primo, allora ha p elementi. Ma il campo dell'esempio precedente non è certo di questo tipo in quanto 8 non è primo. Il seguente risultato risolve tale problema.

Teorema 4.32. *Se K è un campo finito di caratteristica p allora ha p^n elementi, per qualche $n \in \mathbb{N}$.*

Dimostrazione. Come visto in 4.2, K ha come sottocampo fondamentale $\mathbb{Z}_p$. Dunque, considerando l'ampliamento $\mathbb{Z}_p \subseteq K$, si ha che K è uno spazio vettoriale su $\mathbb{Z}_p$. Essendo K un insieme finito, deve avere dimensione finita, diciamo n, su $\mathbb{Z}_p$. Pertanto, per un noto teorema sugli spazi vettoriali, esiste un isomorfismo di $\mathbb{Z}_p$-spazi vettoriali

$$K \cong (\mathbb{Z}_p)^n.$$

In particolare, tali insiemi finiti hanno la stessa cardinalità. □

Si osservi che, nella situazione del teorema precedente, $[K : \mathbb{Z}_p] = n$. Inoltre si deduce che non esistono campi finiti il cui ordine non sia potenza di un primo. Resta la questione se esistano sempre campi di ordine p^n, dove p è un primo qualunque e n un intero positivo qualunque.

Iniziamo a costruire un campo finito in analogia con quanto visto nell'esempio 4.31.5, dove il campo $\mathbb{Z}(\alpha)$ ha $8 = 2^3$ elementi.

Esempio 4.32.1. Sia $f(X) = X^2 + X + 1 \in \mathbb{Z}_2[X]$. Si verifica che $f(X)$ non ha radici in $\mathbb{Z}_2$ ed è dunque irriducibile su tale campo. Con l'usuale identificazione $\alpha = \overline{X}$ si ha

$$\frac{\mathbb{Z}_2[X]}{(f(X))} = \mathbb{Z}_2[\overline{X}] = \mathbb{Z}_2[\alpha] = \mathbb{Z}_2(\alpha)$$

dove l'ultima uguaglianza è dovuta al fatto che α è algebrico su $\mathbb{Z}_2$ in quanto è radice di $f(X)$, che risulta il suo polinomio minimo. Il campo suddetto ha dunque la forma

$$K := \mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\}$$

e in K vale $\alpha^2 = \alpha + 1$. Chiaramente K ha caratteristica 2, $[K : \mathbb{Z}_2] = 2$ e K ha ordine $2^2 = 4$.

Esempio 4.32.2. Sia $f(X) = X^3 + 2X^2 + 4X + 2 \in \mathbb{Z}_5[X]$. Si verifica che $f(X)$ non ha radici in $\mathbb{Z}_5$ ed è dunque irriducibile su tale campo. Procedendo come prima, si ha

$$K := \frac{\mathbb{Z}_5[X]}{(f(X))} = \mathbb{Z}_5(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_5\}$$

e in K vale $\alpha^3 = -2\alpha^2 - 4\alpha - 2$. Chiaramente K ha caratteristica 5, $[K : \mathbb{Z}_5] = 3$ e K ha ordine $5^3 = 125$.

Esempio 4.32.3. Nel campo K dell'esempio precedente è possibile calcolare l'inverso di ogni elemento utilizzando le divisioni successive e l'identità di Bézout.
Sia β un elemento di $\mathbb{Z}_5(\alpha)$ di cui si vuole trovare l'inverso; ad esempio sia $\beta = \alpha^2 + 3\alpha + 1$.
Consideriamo il corrispondente polinomio $g(X) = X^2 + 3X + 1 \in \mathbb{Z}_5[X]$. Poiché $f(X)$ è irriducibile, $(f(X), g(X)) = 1$ (si noti che ciò accade per ogni $g(X) \in \mathbb{Z}_5[X]$ che non sia multiplo di $f(X)$) e dunque, con le divisioni successive, si ricava la corrispondente identità di Bézout:

$$1 = (-X)f(X) + (X^2 + 4X + 1)g(X).$$

Nell'anello quoziente $\frac{\mathbb{Z}_5[X]}{(f(X))}$ si ha quindi

$$\overline{1} = \overline{X^2 + 4X + 1}\,\overline{g(X)}$$

e identificando come al solito $\alpha = \overline{X}$ si ha l'uguaglianza in $\mathbb{Z}_5(\alpha)$:

$$\overline{1} = (\alpha^2 + 4\alpha + 1)(\alpha^2 + 3\alpha + 1)$$

pertanto $\beta^{-1} = \alpha^2 + 4\alpha + 1$.

È possibile generalizzare quanto visto in 4.32.1 e 4.32.2? Cerchiamo, cioè, un modo per costruire un campo di ordine $q = p^n$, per ogni primo p e per ogni numero naturale n. Ci chiediamo, inoltre, se tale campo è unico (a meno di isomorfismi). Con il prossimo risultato troveremo una risposta affermativa a entrambe le questioni.

Teorema 4.33. *(Esistenza e unicità dei campi finiti). Per ogni primo p e per ogni numero naturale n, esiste un campo finito contenente p^n elementi che è campo di spezzamento del polinomio $X^q - X$ (dove $q = p^n$) su $\mathbb{Z}_p$. Inoltre tale campo è unico a meno di isomorfismi.*

Dimostrazione.
Esistenza. Consideriamo il polinomio $X^q - X \in \mathbb{Z}_p[X]$ e sia K il suo campo di spezzamento su $\mathbb{Z}_p$.
Questo polinomio ha q radici distinte in K in quanto il suo polinomio derivato è $qX^{q-1} - 1 \in \mathbb{Z}_p[X]$ e dunque costantemente uguale a -1.
Sia ora $S = \{a \in K \mid a^q - a = 0\}$ l'insieme di tutte le radici di $X^q - X$. Per quanto osservato, S ha esattamente q elementi.
Si osservi che S è un sottocampo di K; infatti, se $a, b \in S$ allora $(a + b)^q = a^q + b^q$ in quanto i coefficienti binomiali $\binom{q}{i}$ sono multipli di q per ogni $1 \leq i \leq (q - 1)$ e dunque nulli, essendo multipli di p e tenuto conto del fatto che $ch(K) = p$. Pertanto $a + b \in S$. Infine è evidente che S è chiuso anche rispetto al prodotto.
Pertanto S è un sottocampo di K sul quale il polinomio dato si spezza: di conseguenza S coincide col campo di spezzamento K. Quindi K ha $q = p^n$ elementi.
Unicità. Sia F un campo finito con $q = p^n$ elementi. Allora, $ch(F) = p$ e dunque F contiene $\mathbb{Z}_p$ come sottocampo fondamentale. Ne segue che F è campo di spezzamento di $X^q - X$ su $\mathbb{Z}_p$, da cui segue l'unicità di F a meno di isomorfismi. □

Da 4.32 e dal risultato precedente, è possibile introdurre una notazione per designare un campo finito di $q = p^n$ elementi (che esiste ed è unico per ogni p ed n): verrà denotato con $\mathbb{F}_q$. In alcuni testi si usa anche la forma $GF(q)$ e la corrispondente denominazione di *campo di Galois* di q elementi.

Da ora in poi, quindi, per ogni primo p, il campo $\mathbb{Z}_p$ verrà denotato anche con $\mathbb{F}_p$.

Introduciamo infine la seguente notazione: se K è un campo finito e $\alpha \in K^*$, indicheremo con $ord(\alpha)$ l'ordine di α nel *gruppo moltiplicativo* K^*.

Il seguente fondamentale risultato descrive la struttura del gruppo moltiplicativo $\mathbb{F}_q^*$ e necessita alcuni fatti preliminari, il primo dei quali è un facile esercizio lasciato al lettore.

Lemma 4.34. *Sia K un campo, $\alpha \in K^*$ e $n = ord(\alpha)$. Allora le potenze $\alpha, \alpha^2, ..., \alpha^{n-1}, \alpha^n = 1_K$ sono elementi distinti di K.* □

Lemma 4.35. *Sia K un campo, $\alpha \in K^*$ e $n = ord(\alpha)$. Allora*

$$\{s \in \mathbb{N} \mid \alpha^s = 1\} = \{\textit{multipli (positivi) di } n\}.$$

Dimostrazione. L'inclusione $\supseteq$ è ovvia, in quanto se $s = nk$ allora $\alpha^s = \alpha^{nk} = (\alpha^n)^k = 1$.
Per provare l'inclusione $\subseteq$, si procede dividendo s per n, ottenendo $s = nq + r$ dove $0 \leq r < n$. Pertanto

$$1 = \alpha^s = \alpha^{nq+r} = \alpha^{nq}\alpha^r = \alpha^r$$

quindi, per definizione di ordine, deve essere $r = 0$. □

Corollario 4.36. *Sia K un campo, $\alpha \in K^*$ e sia $n \in \mathbb{N}$ tale che $\alpha^n = 1$. Se vale*

$$\{s \in \mathbb{N} \mid \alpha^s = 1\} = \{\textit{multipli (positivi) di } n\},$$

allora $n = ord(\alpha)$.

Dimostrazione. Si osservi che l'ipotesi consiste nell'inclusione "$\subseteq$", in quanto l'altra vale sempre (come visto nel lemma precedente). Tale osservazione sarà utilizzata nelle prossime dimostrazioni.
Per 4.35 e per l'ipotesi si hanno le uguaglianze:

$$\{\text{multipli (positivi) di } ord(\alpha)\} = \{s \in \mathbb{N} \mid \alpha^s = 1\} = \{\text{multipli (positivi) di } n\},$$

da cui la tesi segue immediatamente. □

Proposizione 4.37. *Sia K un campo finito, $\alpha \in K^*$ e $n = ord(\alpha)$. Allora per ogni $k \in \mathbb{N}$ si ha:*

$$ord(\alpha^k) = n/MCD(n,k).$$

Dimostrazione. Sia $d := MCD(n,k)$. Ovviamente $(\alpha^k)^{n/d} = (\alpha^n)^{k/d} = 1$. Per mostrare che $ord(\alpha^k)$ è esattamente n/d basta provare, per 4.36 applicato a α^k, che $(\alpha^k)^s = 1$ implica che s è multiplo di n/d . Si osservi che

$$1 = (\alpha^k)^s = \alpha^{ks}$$

dunque, ancora per 4.36 applicato ad α, si ottiene che ks è multiplo di n, ovvero n divide ks. Da cui segue che n/d divide $ks/d = s(k/d)$. Ma n/d e k/d sono ovviamente coprimi; dunque, necessariamente, n/d divide s, come volevamo. □

Proposizione 4.38. *Sia K un campo finito, $\alpha, \beta \in K^*$ con $n = ord(\alpha)$, $m = ord(\beta)$. Se n e m sono coprimi allora*

$$ord(\alpha\beta) = nm.$$

Dimostrazione. Chiaramente $(\alpha\beta)^{nm} = \alpha^{nm}\beta^{nm} = 1$. Per 4.36 basta provare che, se $(\alpha\beta)^s = 1$, allora s è multiplo di nm.
Elevando ambo i membri di $(\alpha\beta)^s = 1$ per n ed m rispettivamente, otteniamo

$$1 = ((\alpha\beta)^s)^n = (\alpha\beta)^{sn} = \alpha^{sn}\beta^{sn} = \beta^{sn}$$

dunque, per 4.35, sn è multiplo di m. Ma n e m sono coprimi, quindi s è multiplo di m. Analogamente

$$1 = ((\alpha\beta)^s)^m = (\alpha\beta)^{sm} = \alpha^{sm}\beta^{sm} = \alpha^{sm}$$

e quindi, sempre per 4.35, sm è multiplo di n. Ma n e m sono coprimi, quindi s è multiplo di n.
In conclusione, s è multiplo sia di n che di m, che sono coprimi; dunque s è multiplo nm, come volevamo. □

Definizione. Sia K un campo finito di ordine q. Sia $\alpha \in K$ tale che $ord(\alpha) = q-1$. Diciamo allora che α è un *elemento primitivo* di K.

Il seguente risultato, assicurando l'esistenza di un tale elemento in ogni campo finito, fornisce una precisa informazione sul gruppo moltiplicativo dei suoi elementi non nulli.

Teorema 4.39. *(Teorema dell'elemento primitivo) In un campo finito K esiste un elemento primitivo e le sue potenze distinte coincidono con tutti gli elementi non nulli del campo. Equivalentemente, K^* è un gruppo ciclico.*

Dimostrazione. Sia $q := |K|$. Se $q = 2$, il teorema è vero (in tal caso l'elemento primitivo è 1_K).
Sia allora $q > 2$ e sia n il massimo ordine degli elementi del campo; dunque $n \leq q-1$ ed esiste un elemento, diciamo α, di ordine n.

(1) Sia $\beta \in K^*$ un elemento distinto da α e denotiamo con m il suo ordine. Vogliamo provare che $m|n$.
Supponiamo che m non divida n; dunque, posto $d := MCD(n,m)$, si ha che $d < m$. Per 4.37 si ha $ord(\beta^n) = m/d > 1$. Poiché n e m/d sono coprimi, per 4.38 otteniamo

$$ord(\alpha\beta^n) = nm/d > n$$

in quanto $m/d > 1$. Pertanto l'elemento $\alpha\beta^n$ ha ordine maggiore di n, che per ipotesi è il massimo degli ordini. Questo è impossibile e dunque $m|n$.

(2) $n = q-1$.
Per ogni $\beta \in K^*$ (compreso α !) si ha, per la parte (1), che $\beta^n = 1$. Quindi tutti i $q-1$ elementi di K^* sono radici dell'equazione $X^n = 1$; poiché tale equazione ha al più n radici distinte, ne segue che $q-1 \leq n$. Pertanto $n = q-1$ ed α è un elemento primitivo di K.

(3) Il gruppo moltiplicativo K^* è ciclico.
Poiché α ha ordine $q-1$, per 4.34 le potenze $\alpha, \alpha^2, ..., \alpha^{q-1} = 1_K$ sono elementi distinti di K^*. Ma K^* ha esattamente $q-1$ elementi, dunque

$$K^* = \{\alpha, \alpha^2, ..., \alpha^{q-1}\} = \langle\alpha\rangle$$

è un gruppo ciclico. □

Esempio 4.39.1. Nel campo $\mathbb{F}_5$, consideriamo le potenze dei suoi elementi non nulli e diversi da 1, cioè di: $2, 3, 4$. I sottogruppi (tutti ciclici) del gruppo moltiplicativo $\mathbb{F}_5^*$ sono dati da:

$$\langle 2\rangle = \{2, 4, 3, 1\}, \quad \langle 3\rangle = \{3, 4, 2, 1\}, \quad \langle 4\rangle = \{4, 1\}.$$

Pertanto 2 e 3 hanno ordine 4 e quindi sono elementi primitivi di $\mathbb{F}_5$, mentre 4 non lo è, pur essendo anch'esso radice dell'equazione $X^4 = 1$.

Corollario 4.40. *Gli elementi di $\mathbb{F}_q$ sono tutte e sole le soluzioni dell'equazione $X^q - X = 0$. In particolare*

$$X^q - X = \prod_{\alpha\in\mathbb{F}_q} (X - \alpha).$$

Dimostrazione. Basta osservare che $X^q - X = X(X^{q-1} - 1)$, dunque le soluzioni dell'equazione devono soddisfare $X = 0$ (che ha per unica soluzione lo zero di $\mathbb{F}_q$) oppure $X^{q-1} - 1 = 0$, che è soddisfatta da tutti gli elementi non nulli del campo, per quanto visto nella dimostrazione di 4.39. □

È chiaro, comunque, che una equazione del tipo $X^n - X = 0$, con $n > q$, non ha tutte le radici nel campo $\mathbb{F}_q$, come mostra il seguente esempio.

Esempio 4.40.1. Non si può fattorizzare $X^3 - 1$ in $\mathbb{F}_2[X]$ come nel corollario precedente. Infatti

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

e il secondo fattore è irriducibile in $\mathbb{F}_2[X]$, come si vede facilmente. In effetti, $\mathbb{F}_2$ non ha "abbastanza" elementi per contenere una radice terza primitiva dell'unità. Occorre individuare un'opportuna estensione (semplice) di $\mathbb{F}_2$. In questo esempio, è sufficiente $\mathbb{F}_4 = \mathbb{F}_2(a)$, dove a è una radice di $X^2 + X + 1$.

Indice

Capitolo 0 - Background 1
Nozioni di base sui gruppi 1
Richiami su gruppi finiti e gruppi ciclici 3
Sottogruppi normali e quozienti 4
Richiami su omomorfismi di gruppi 5
Nozioni di base su anelli e ideali 6
Richiami sugli omomorfismi d'anelli 10
Divisione euclidea e ideali di $\mathbb{Z}$ 11
Campo dei quozienti di un dominio 12

Capitolo 1 - Teoria dei gruppi 15
Cenni di aritmetica modulare 15
Gruppi di matrici 18
Introduzione ai gruppi finiti 20

Capitolo 2 - Teoria degli anelli 24
Operazioni tra ideali - Generatori 25
Divisibilità e Massimo Comun Divisore in $\mathbb{Z}$ 26
Divisibilità in un anello 29
Caratteristica di un anello 30
Ideli primi e massimali 31
Teorema Cinese dei Resti in un anello commutativo 32
Fattorialità 35
Anelli euclidei 40

Capitolo 3 - Anelli di polinomi 44
Polinomi a coefficienti in un anello 44
Polinomi invertibili, irriducibili e primi 46
Polinomi a coefficienti in un campo 49
Polinomi in più indeterminate 52
Campo dei quozienti di un anelli di polinomi 54
Funzioni polinomiali 55
Radici di polinomi 56
Polinomi complessi e reali 61
Fattorialità degli anelli di polinomi 63

Capitolo 4 - Campi 69
Immersioni e isomorfismi di campi 70
Ampliamenti di campi 71
Elementi algebrici e trascendenti 73
Ampliamenti finiti 76
Ampliamenti algebrici 77
Campi di spezzamento 79
Campi finiti 82