1

Capitolo T23
teoria degli anelli

Contenuti delle sezioni

a. anelli e anelli uniferi: definizioni e primi esempi p. 2
b. ideali p. 7
d. polinomi e anelli di polinomi p. 10
e. anelli di gruppo p. 11
f. anelli principali e fattoriali p. 12

13 pagine

T23 0.01 Le nozioni di anello e di anello unifero, introdotte in B41e e riprese in T15i e in T15j, vengono qui approfondite.
Nelle pagine che seguono viene esposto in modo autosufficiente il complesso delle proprietà della teoria degli anelli maggiormente utilizzato in alcune specializzazioni e in alcune applicazioni.

In particolare sono esaminate le proprietà che servono agli sviluppi della teoria dei campi e della teoria dei moduli, e quelle utilizzate nello studio delle trasformazioni lineari.

T23 a. anelli e anelli uniferi: definizioni e primi esempi

T23 a.01 Definiamo **anello unifero** una struttura algebrica che presenta la forma $\mathsf{R} = \langle R, \mathbf{+}, \mathbf{-}, \mathbf{0}, \mathbf{\cdot}, \mathbf{1} \rangle$, della quale, oltre all'unico terreno R, fanno parte:

l'elemento zero $\mathbf{0}$ e l'elemento unità $\mathbf{1}$;

l'operazione binaria $\ulcorner a, b \in R \mapsto a \mathbf{+} b \urcorner$ che diciamo addizione o somma su $\boldsymbol{R}$;

l'operazione unaria $\ulcorner a \in R \mapsto \mathbf{-}a \urcorner$ che diciamo passaggio all'opposto (additivo);

l'operazione binaria $\ulcorner a, b \in R \mapsto a \mathbf{\cdot} b \urcorner$ che diciamo moltiplicazione o prodotto di $\boldsymbol{R}$.

Per queste entità chiediamo le proprietà che seguono riguardanti $\forall a, b, c \in R$:

[Rng 1] $a\mathbf{+}(b\mathbf{+}c) = (a\mathbf{+}b)\mathbf{+}c$ associatività dell'addizione;

[Rng 2] $a\mathbf{+}b = b\mathbf{+}a$ commutatività dell'addizione;

[Rng 3] $a\mathbf{+}\mathbf{0} = a$ zero elemento neutro per l'addizione;

[Rng 4] $a\mathbf{+}(\mathbf{-}a) = (\mathbf{-}a)\mathbf{+}a = \mathbf{0}$ sottrazione operazione inversa della somma;

[Rng 5] $a\mathbf{\cdot}(b\mathbf{\cdot}c) = (a\mathbf{\cdot}b)\mathbf{\cdot}c$ associatività della moltiplicazione;

[Rng 6] $(a\mathbf{+}b)\mathbf{\cdot}c = a\mathbf{\cdot}c\mathbf{+}b\mathbf{\cdot}c$ distributività da sinistra dell'addizione rispetto alla moltiplicazione;

[Rng 7] $a\mathbf{\cdot}(b\mathbf{+}c) = a\mathbf{\cdot}b\mathbf{+}a\mathbf{\cdot}c$ distributività da destra dell'addizione rispetto alla moltiplicazione.

[Rngu 8] $\mathbf{1}\mathbf{\cdot}a = a\mathbf{\cdot}\mathbf{1} = a$ zero elemento neutro per il prodotto.

T23 a.02

Definiamo **anello** una strutture della forma $\langle R, \mathbf{+}, \mathbf{-}, \mathbf{0}, \mathbf{\cdot} \rangle$ nella quale compaiono tutti i componenti che costituiscono gli anelli uniferi a eccezione dell'elemento neutro per la moltiplicazione e per la quale valgono tutte le proprietà degli anelli uniferi eccettuata la [Rngu 8].

Denotiamo con **RngU** la classe degli anelli uniferi e con **Rng** la classe degli anelli.
Spesso abbrevieremo il termine "anello unifero" con **anello.u**.
Servendoci di un operatore dimenticanza [B41a07] abbiamo $\forall \boldsymbol{R} \in \mathbf{RngU} \ : \ \boldsymbol{Frgt}_6(\boldsymbol{R}) \in \mathbf{Rng}$.

Si dice **anello unifero abeliano**, o anche **anello unifero commutativo** un anello unifero il cui prodotto è commutativo, cioè tale da soddisfare l'ulteriore proprietà

[Rng 9] $a\mathbf{\cdot}b = b\mathbf{\cdot}a$.

Similmente si dice **anello abeliano** o **anello commutativo** un anello per il quale vale la proprietà [Rng 9].
Denotiamo con **RngUAb** la classi degli anelli uniferi e con **RngUAb** la classe degli anelli abeliani.

T23 a.03 Coerentemente con T15h, possiamo affermare che un anello.u è una struttura avente la forma $\langle R, \mathbf{+}, \mathbf{-}, \mathbf{0}, \mathbf{\cdot}, \mathbf{1} \rangle$ nella quale
— $\langle R, \mathbf{+}, \mathbf{-}, \mathbf{0} \rangle$ è un gruppo abeliano,
— $\langle R, \mathbf{\cdot}, \mathbf{1} \rangle$ è un monoide;
— l'operazione somma "$\mathbf{+}$" è distributiva rispetto all'operazione prodotto "$\mathbf{\cdot}$".

Per gli anelli dobbiamo sostituire la seconda delle precedenti proprietà chiedendo che $\langle R, \mathbf{\cdot} \rangle$ sia un semigruppo.

È opportuno segnalare che spesso per le strutture algebriche che stiamo eaminando si usano nomi diversi: una terminologia diffusa chiama anelli quelli che chiamiamo anelli-.niferi mentre chiama "pseudoanelli" quelli che qui sono detti anelli. Inoltre va detto che invece dell'aggettivo unifero spesso si usano "unitale" o "unitario".

Un primo importante esempio di anello.u è fornito dalla sestupla $\mathbb{Z}_{Rngu} := \langle \mathbb{Z}, +, -, 0, \cdot, 1 \rangle$, nella quale i segni $+$, $-$, 0, $\cdot$ e 1 hanno gli usuali significati elementari.

Vi sono invece anelli nei quali non si ha la possibilità di disporre di un elemento neutro per il prodotto. Un primo esempio di tali strutture è fornito dall'insieme dei numeri pari $2 \cdot \mathbb{Z} = \{n \in \mathbb{Z} :| \, 2\,n\}$ munito delle usuali operazioni.

La classe degli anelli che non possono essere muniti di unità moltiplicativa si denota con **RngNu**.

T23 a.04 Un insieme con un solo elemento può essere considerato terreno di un anello.u facendo svolgere al suo elemento sia il ruolo di zero che di unità. Si introduce quindi una entità chiamata **anello.u nullo** il cui unico elemento si scrive $\mathbf{0} = \mathbf{1}$. Questo anello.u è ben definito in quanto non può contenere altri elementi: per ogni suo elemento a si ha
$a = \mathbf{0}\boldsymbol{\cdot}a\mathbf{+}a = (\mathbf{0+1})\boldsymbol{\cdot}a = \mathbf{1}\boldsymbol{\cdot}a = a$ e quindi $a = \mathbf{0}$.
Va segnalato che talora si esclude che questa struttura sia un anello.u, ovvero si chiede che ogni anello.u possegga almeno due elementi.

T23 a.05 Per l'anello.u $\boldsymbol{R} = \langle R, \mathbf{+}, \mathbf{-}, \mathbf{0}, \cdot, \mathbf{1} \rangle$ introduciamo anche l'operazione binaria sottrazione o differenza che possiamo denotare con lo stesso segno $\mathbf{-}$ (il contesto consente di distinguere le notazioni di operatore unario da quelle di operatore binario) ponendo $a\mathbf{-}b := a\mathbf{+}(\mathbf{-}b)$.
Chiaramente $\forall a \in R : \; \mathbf{-}a = \mathbf{0}\mathbf{-}a$.

(1) Prop.: $\mathbf{0+0} = \mathbf{0}$ e $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$. In virtù, risp., di [Rng 3] ed [Rng 6].

(2) Prop.: $\mathbf{-0} = \mathbf{0}$.
Infatti per definizione $\mathbf{-0} = \mathbf{0-0} = [Rng4] = \mathbf{0}$ ∎

(3) Prop.: Per ogni $a \in R$ si ha $zrbf\boldsymbol{\cdot}a = a\boldsymbol{\cdot}\mathbf{0} = \mathbf{0}$.
Infatti $\mathbf{0}\boldsymbol{\cdot}a = [Rng3] = zrbf\boldsymbol{\cdot}a\mathbf{+0} = [Rng4] = \mathbf{0}\boldsymbol{\cdot}a\mathbf{+0}\boldsymbol{\cdot}a\mathbf{-0}\boldsymbol{\cdot}a = (\mathbf{0+0})\boldsymbol{\cdot}a\mathbf{-0}\boldsymbol{\cdot}a = [(1)] = \mathbf{0}\boldsymbol{\cdot}a\mathbf{-}zrbf\boldsymbol{\cdot}a = [Rng4] = \mathbf{0}$ ∎

(4) Prop.: Per ogni $a, b \in R$ si ha $(\mathbf{-}a)b = \mathbf{-}(a \cdot b)$.
Infatti $a\boldsymbol{\cdot}b\mathbf{+}(\mathbf{-}a)\boldsymbol{\cdot}b = (a\mathbf{+}(\mathbf{-}a))\boldsymbol{\cdot}b = \mathbf{0}\boldsymbol{\cdot}b = \mathbf{0}$ ∎

(5) Prop.: $a\boldsymbol{\cdot}(\mathbf{-}b) = \mathbf{-}(a\boldsymbol{\cdot}b)$. La dimostrazione si serve delle espressioni speculari di quelle costituenti la precedente: $a\boldsymbol{\cdot}b\mathbf{+}a\boldsymbol{\cdot}(\mathbf{-}b) = a\boldsymbol{\cdot}(b\mathbf{+}(\mathbf{-}b)) = a\boldsymbol{\cdot}\mathbf{0} = \mathbf{0}$ ∎

(6) Prop.: $\mathbf{-}(\mathbf{-}a) = a$
Infatti [Rng 4] implica $(\mathbf{-}a)\mathbf{+}(\mathbf{-}(\mathbf{-}a)) = zrbf$; sommando a a entrambi i membri e per [Rng 1] si ottiene $a\mathbf{+}(\mathbf{-}a)\mathbf{+}(\mathbf{-}(\mathbf{-}a)) = a$ e quindi l'asserto ∎

(7) Prop.: $(\mathbf{-}a)\boldsymbol{\cdot}(\mathbf{-}b) = a\boldsymbol{\cdot}b$. Infatti $(\mathbf{-}a)\boldsymbol{\cdot}(\mathbf{-}b) = [Rng2] = \mathbf{-}(a\boldsymbol{\cdot}(\mathbf{-}b)) = [Rng2] = \mathbf{-}(\mathbf{-}(a\boldsymbol{\cdot}b)) = \lfloor_{\mathbb{N}}(6)_{\mathbb{N}}\rfloor = a\boldsymbol{\cdot}b$ ∎

T23 a.06 Eserc. Consideriamo un anello unifero $\boldsymbol{R} = \langle R, +, \mathbf{-}, \mathbf{0}, \boldsymbol{\cdot}, 1 \rangle$, un qualsiasi $n \in \mathbb{P}$ e $2\,n$ elementi arbitrari $a_1, a_2, ..., a_n, b_1, b_2, ...b_n \in R$.

Dimostrare le seguenti formule di distributività generalizzata per gli anelli $\boldsymbol{R}$:

(1) $a_1\boldsymbol{\cdot}(b_1\mathbf{+}\cdots\mathbf{+}b_n) = a_1\boldsymbol{\cdot}b_1\mathbf{+}\cdots\mathbf{+}a_1\boldsymbol{\cdot}b_n$;

(2) $(a_1\mathbf{+}\cdots\mathbf{+}a_n)\boldsymbol{\cdot}b_1 = a_1\boldsymbol{\cdot}b_1\mathbf{+}\cdots\mathbf{+}a_n\boldsymbol{\cdot}b_1$;

(3) $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i\, b_j$

Qui il segno Σ denota il costrutto sommatoria derivato dalla somma $\mathbf{+}$.

Dimostrare le distributività per la sottrazione:

(4) $\quad x_1(y_1 - y_2) = x_1\, y_1 - x_1\, y_2 \quad , \quad (x_1 - x_2)y_1 = x_1\, y_1 - x_2\, y_1 \ .$

(2) Eserc. Constatare che un anello abeliano non unifero è fornito da $\mathbb{Z} \times \mathbb{Z}$ munito di somma, passaggio all'opposto (ossia differenza) e prodotto componente per componente; quali sono gli elementi neutri?

(3) Eserc. Osservare che, più in generale, per ogni $m = 2, 3, 4, ...$

$$\mathbb{Z}^{\times m}{}_{Rng} := \langle m \cdot \mathbb{Z}, +^{\times m}, -^{\times m}, 0{\times}m, \cdot^{\times m} \rangle$$

è un anello che non può contenere un elemento neutro per la moltiplicazione, ossia è un anello appartenente a **RngNu**.

T23 a.07 Importanti anelli.u commutativi accostabili a $\mathbb{Z}_{Rngu}$ sono ottenuti arricchendo con le operazioni usuali di somma, differenza e prodotto e con 0 e 1 insiemi numerici di largo uso come $\mathbb{Q}$, $\mathbb{R}_{\mathsf{a}}$, $\mathbb{R}_{\mathsf{c}}$, $\mathbb{R}$ e $\mathbb{C}$.

Altri importanti anelli commutativi sono costituiti, per un qualsiasi intero $m \geq 2$, dagli insiemi $\mathbb{Z}_m$ delle classi di resti modulo m muniti delle operazioni dell'aritmetica modulare.

Per queste strutture si possono usare scritture come

$$\mathbb{R}_{Rngu} := \langle \mathbb{R}, +, -, 0, \cdot, 1 \rangle \quad \text{e} \quad \mathbb{Z}_{m\,Rngu} := \langle \mathbb{Z}_m, +_m, -_m, 0, \cdot_m, 1 \rangle \ .$$

Spesso tuttavia risulta possibile usare per gli anelli senza ambiguità notazioni semplificate nelle quali si confondono le strutture algebriche con i rispettivi terreni e le estensioni cartesiane degli operatori con gli stessi operatori. Si confida infatti che da queste notazioni semplificate il contesto consenta di individuare senza difficoltà le corrispondenti complete, evidentemente più pesanti da scrivere e leggere.

Quindi spesso, per esempio, si scrive $\mathbb{Q}$ per denotare l'anello unifero che più completamente andrebbe individuato da $\mathbb{Q}_{Rngu}$ e si semplificano operatori come $+^{\times m}$ con $+$ o anche con il semplice $+$.

Con atteggiamento simile talora si sostituisce il segno specifico che dovrebbe rappresentare il prodotto con il semplice e generico "$\cdot$" e ancora più spesso si trascura del tutto di segnare la presenza di tale operatore tra due operandi limitandosi a distanziare leggermente i due fattori.

T23 a.08 Un sottoinsieme S del terreno R di un anello $\boldsymbol{R} = \langle R, +, -, 0, \cdot \rangle$ si dice **terreno di un sottoanello** di $\boldsymbol{R}$ sse è chiuso rispetto alle operazioni di somma e prodotto, cioè sse

$$\forall a, b \in S \ : \ a + b \in S \ , \ -a \in S \ , \ a \cdot b \in S \ , \ 0, 1 \in S \ .$$

In questo caso scriviamo $\langle S, +, -, 0, \cdot \rangle \leq_{Rng} \boldsymbol{R}$.
Per essere pignoli va segnalato che non si sono distinti gli operatori definiti in R dalle loro riduzioni a S.
Spesso il contesto consente di semplificare la scrittura precedente nella $S \leq_{Rng} R$.

Scriviamo invece $\langle S, +, -, 0, \cdot \rangle <_{Rng} \boldsymbol{R}$ o $S <_{Rng} R$ per enunciare che S è sottoanello proprio di R, escludendo che possa essere $S = R$.

Un sottoinsieme S del terreno R di un anello.u $\boldsymbol{R}$ si dice **terreno di un sottoanello.u** di $\boldsymbol{R}$ sse è chiuso rispetto alle operazioni di somma e prodotto e contiene l'elemento unità.

Per esprimere questa situazione possiamo usare la scrittura semplificata $S \leq_{Rngu} R$. Scriviamo invece $S <_{Rngu} R$ per enunciare che $S \leq_{Rngu} R$ e $S \subset R$.

T23 a.09 Si dice **centro di un anello.u** $\boldsymbol{R}$ l'insieme dei suoi elementi che commutano con tutti gli elementi di R. Evidentemente del centro fanno parte lo zero e l'unità e insieme a una coppia $\langle a, b \rangle$ di suoi

elementi la loro somma $a+b$, l'opposto $-a$ e il loro prodotto $a \cdot b$. Quindi il centro di ogni anello.u costituisce un suo sottoanello.u.

(1) Eserc. Dimostrare che $\mathbb{Z} <_{Rngu} \mathbb{Q} <_{Rngu} \mathbb{R}_{\mathsf{a}} <_{Rngu} \mathbb{R}_{\mathsf{c}} <_{Rngu} \mathbb{R} <_{Rngu} \mathbb{C}$.

(2) Eserc. Consideriamo $h,k \in \{2,3,4,...\}$. Dimostrare che $(h\,k\,\mathbb{Z})_{Rng} <_{Rng} (h\,\mathbb{Z})_{Rng} <_{Rng} \mathbb{Z}_{Rng}$

T23 a.10 Consideriamo un anello.u $\boldsymbol{R} = \langle R, \boldsymbol{+}, \boldsymbol{-}, \mathbf{0}, \boldsymbol{\cdot}, \mathbf{1} \rangle$ ed un insieme qualsiasi E. Consideriamo l'insieme di funzioni $\lceil E \longmapsto R \rceil$ e muniamo questo terreno con la somma $\boldsymbol{+}^{fe}$, cioè con l'estensione funzionale della somma di $\boldsymbol{R}$, con l'estensione funzionale del passaggio all'opposto $-^{fe}$ e con l'estensione funzionale del prodotto $\cdot^{fe}$.

Eserc. Dimostrare che la struttura $\langle R^E, \boldsymbol{+}^{fe}, \boldsymbol{-}^{fe}, \lceil e \in E \mapsto \mathbf{0} \rceil, \boldsymbol{\cdot}^{fe}, \lceil e \in E \mapsto \mathbf{1} \rceil \rangle$, è un anello.u.

T23 a.11 Le matrici quadrate di ordine finito le cui componenti sono elementi di un anello, unifero o meno, costituiscono anelli ricchi di applicazioni.

A partire da un anello.u $\boldsymbol{R} = \langle R, \boldsymbol{+}, \boldsymbol{-}, \mathbf{0}, \boldsymbol{\cdot}, \mathbf{1} \rangle$ per ogni intero positivo d si definisce l'**anello di matrici** su $\boldsymbol{R}$

$$\mathsf{Mat}(d, \boldsymbol{R})_{Rngu} := \left\langle \mathsf{Mat}_d(\boldsymbol{R}), \boldsymbol{+}^{\times n^2}, \boldsymbol{-}^{\times n^2}, \mathsf{matZr}(d;R), \otimes_{\mathsf{M}}, \mathsf{matId}(d;R) \right\rangle ,$$

dove con $\otimes_{\mathsf{M}}$ denotiamo qui il prodotto righe per colonne delle matrici.

Si constata che la **matrice opposta** di una data $A \in \mathsf{Mat}_d(\boldsymbol{R})$, cioè la sua inversa rispetto alla somma $\boldsymbol{+}^{\times n^2}$, si ottiene modificando tutte le entrate $a_{i,j}$ della A nelle opposte $\boldsymbol{-}a_{i,j}$, mentre l'elemento neutro rispetto alla somma è la matrice quadrata di ordine d $at\mathsf{matZr}(d;R)$ avente tutte le entrate uguali all'elemento neutro $\mathbf{0}$ di $\boldsymbol{R}$.

T23 a.12 Come si è già osservato, gli anelli di matrici su semianelli di ordine maggiore di 1 sono non-commutativi anche se costruiti a partire da un anello commutativo; controesempi alla commutatività si trovano facilmente tra le piccole matrici con componenti intere. Per esempio

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 19 & 43 \\ 22 & 50 \end{bmatrix} \neq \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 31 \\ 34 & 46 \end{bmatrix}$$

T23 a.13 In un anello.u, come in un monoide, si possono avere elementi dotati o meno di inverso [moltiplicativo] a sinistra ed elementi dotati o meno di inverso [moltiplicativo] a destra.

Consideriamo un anello.u $\boldsymbol{R}$ e i suoi elementi dotati sia di un inverso a sinistra che di un inverso a destra. Questo insieme lo denotiamo con $\mathsf{Invelm}(\boldsymbol{R})$. Ovviamente esso non comprende lo zero.

Sia $a \in \mathsf{Invelm}(\boldsymbol{R})$, sia b è un suo inverso a sinistra, cioè sia $b\,a = 1$, e sia c un suo inverso a destra, cioè sia $a\,c = 1$.
Allora $b\,a\,c = b = c$ e quindi a possiede un unico inverso bilatero $b = c$ e l'inverso di questo elemento è lo stesso a.
Dunque $\mathsf{Invelm}(\boldsymbol{R})$ munito del prodotto di $\boldsymbol{R}$ è un gruppo chiamato **gruppo moltiplicativo dell'anello.u** $\boldsymbol{R}$; esso viene denotato con $\boldsymbol{R}^{\mathsf{X}}$.
Evidentemente se $\boldsymbol{R}$ è un anello.u abeliano allora $\boldsymbol{R}^{\mathsf{X}}$ è un gruppo abeliano.

Un anello.u nel quale tutti gli elementi diversi dallo zero sono invertibili è chiamato **anello di divisione**. Denotiamo con RngDiv la classe di queste strutture.

T23 a.14 Gli elementi di un anello.u che sono invertibili solo a sinistra o solo a destra non necessariamente costituiscono un gruppo: un controesempio è fornito dall'anello.u che segue.

Consideriamo l'insieme delle successioni di interi $\lceil \mathbb{N} \longmapsto \mathbb{Z} \rceil$ e denotiamo con $\mathbf{S}$ il monoide ottenuto munendo tale insieme delle operazioni di somma componente per componente $+^{ce}$ e della successione $\lceil \mathbb{N} \nmapsto 0 \rceil$.

Denotiamo con $\mathbf{F_S}$ l'insieme delle funzioni fin $\lceil \mathbf{S} \longmapsto \mathbf{S} \rceil$ additive, cioè delle funzioni tali che

$$\forall \mathbf{s}, \mathbf{t} \in \mathbf{S} \ : \ f(\mathbf{s}+\mathbf{t}) = f(\mathbf{s}) + f(\mathbf{t}) \quad (*) \ .$$

Munendo $\mathbf{F_S}$ dell'operazione di somma componente per componente $+^{ce}$ si ottiene un gruppo abeliano.

$\mathbf{F_S}$ è chiuso rispetto alla composizione $\circ_{rl}$ tra funzioni di $\lceil \mathbf{S} \longmapsto \mathbf{S} \rceil$.

Infatti $\forall f, g \in \mathbf{F_S} \ : \ (f \circ_{rl} g)(\mathbf{s}+\mathbf{t}) = f\Big(g(\mathbf{s}) + g(\mathbf{t})\Big) = f\Big(g(\mathbf{s})\Big) + f\Big(g(\mathbf{t})\Big)$.

$\mathbf{F_S}$ munito del prodotto $\circ_{rl}$, evidentemente associativo e avente come unità $\mathsf{Id}(\mathbf{F_S})$ costituisce un monoide.

Si verifica inoltre che la somma delle funzioni in $\mathbf{F_S}$ è distributiva rispetto a $\circ_{rl}$ e dunque $\mathbf{F_S}$ è terreno di un anello.u.

Questa struttura viene detta **anello.u delle endofunzioni additive di un anello.u**.

Di $\mathbf{F_S}$ fa parte il cosiddetto **operatore di shift** $\lceil \langle a_0, a_1, a_2, ... \rangle \nmapsto \langle 0, a_0, a_1, ... \rangle \rceil$. Si verifica che esso è invertibile a sinistra ma non a destra; quindi non può far parte di un gruppo.

T23 b. ideali

T23 b.01 Per gli anelli.u, oltre ai sottoanelli.u, si possono definire sottostrutture di un'altro importante genere: gli ideali.

Consideriamo dunque un anello.u $\boldsymbol{R} = \langle R, +, -, 0, \cdot, 1 \rangle$ ed il gruppo abeliano $\boldsymbol{R}_{ag} := \langle R, +, -, 0 \rangle$ che costituisce un suo impoverimento.

Si dice **ideale a sinistra dell'anello.u** $\boldsymbol{R}$ un sottoinsieme $I \subseteq R$ che è terreno di un sottogruppo di $\boldsymbol{R}_{ag}$ e tale che $R \cdot I \subseteq I$, ovvero tale che $\forall a \in R \ : \ a \cdot I \subseteq I$, cioè tale che $\forall a \in R \ , \ i \in I \ : \ a \cdot i \in I$.

Dualmente-LR si dice **ideale a destra dell'anello.u** di $\boldsymbol{R}$ un $J \subseteq R$ che è terreno di un sottogruppo di $\boldsymbol{R}_{ag}$ e tale che $J \cdot R \subseteq J$.

Si dice **ideale [bilatero] dell'anello.u** $\boldsymbol{R}$ un $I \subseteq R$ che è sia ideale a sinistra che ideale a destra di $\boldsymbol{R}$.

Evidentemente per un anello abeliano ogni ideale a sinistra è anche un ideale a destra e viceversa; dunque non ha senso parlare di ideali a sinistra o a destra ma solo di ideali bilateri.

Riassumendo un ideale bilatero di $\boldsymbol{R}$ soddisfa queste condizioni:

[Idl 1] I è sottogruppo del gruppo additivo $\boldsymbol{R}_{ag}$;

[Idl 2] è chiuso rispetto alla sottrazione, cioè $\forall a, b \in I \ : \ a - b \in I$;

[Idl 3] $\forall a \in I, \ \forall r \in R \ : \ a \cdot r \in I \ , \ r \cdot a \in I \ .$

L'ultima richiesta è evidentemente più stringente della chiusura di un sottoinsieme rispetto al prodotto: quindi ogni ideale di un anello.u è un suo particolare sottoanello.u .

Sono terreni di ideali bilateri di ogni anello.u (nonnullo) $\boldsymbol{R} = \langle R, +, -, 0, \cdot, 1 \rangle$ i due sottoinsiemi di R l'uno costituito dal solo zero di R e l'altro coincidente con l'intero terreno; essi sono detti, risp., **ideale nullo dell'anello.u** e **ideale improprio dell'anello.u** di $\boldsymbol{R}$. Ogni altro ideale, ammesso che esista, viene chiamato **ideale proprio dell'anello.u** $\boldsymbol{R}$.

Denotiamo con $Idl(\boldsymbol{R})$ la collezione degli ideali bilateri dell'anello $\boldsymbol{R}$.

T23 b.02 Diamo qualche primo esempio di ideali.

Per l'anello.u abeliano degli interi $\mathbb{Z}$ sono ideali propri gli insiemi dei multipli $m \cdot \mathbb{Z}$ per ogni intero $m = 2, 3, 4, ...$

Sia $p(x)$ un polinomio in $\boldsymbol{F}[x]$; L'insieme di tutti i multipli di $p(x)$, per il quale usiamo la notazione $\langle p(x) \rangle \ := \ \{q(x)p(x) \ \ | : \ \ q(x) \in \boldsymbol{F}[x]\}$, è un ideale in $\boldsymbol{F}[x]$.

Questi due esempi si inquadrano opportunamente nel seguente enunciato.

(1) Prop.: Sia $\boldsymbol{R}$ un anello.u e sia a un suo elemento a.
$a \cdot R$ è ideale a destra di $\boldsymbol{R}$;
$R \cdot a$ è ideale a sinistra di $\boldsymbol{R}$;
$R \cdot a \cdot R$ è ideale bilatero di $\boldsymbol{R}$ ∎

T23 b.03 Prop. Ogni ideale sinistro, destro o bilatero I di un anello.u $\boldsymbol{R}$ contiene lo zero di questa struttura.

Dim.: $\forall r \in R \ : \ 0\, r = r\, 0 = 0$ ∎

Si osserva che questo fatto per gli ideali bilateri è conseguenza ben evidente di [Idl 2].

(2) Prop.: Per ogni anello.u dotato di ideali propri l'unità 1 non appartiene ad alcuno di questi sottoanelli.

Dim.: Preso un qualsiasi ideale proprio I dell'anello $\boldsymbol{R}$ e un qualsiasi elemento $r \in R$ non contenuto in I, risulta $1\,r = r\,1 = r$. Se 1 appartenesse ad I si dedurrebbe, dalla definizione di ideale, che anche r apparterrebbe ad I, contro l'ipotesi ∎

T23 b.04 Prop. Un corpo $\boldsymbol{K}$ non possiede alcun ideale proprio.

Dim.: Supponiamo per assurdo che $\boldsymbol{K}$ possegga un ideale proprio I e consideriamo un elemento $i \in I$ diverso dallo zero. Poiché $\boldsymbol{K}$ è un corpo, in $\boldsymbol{K}$ si trova l'inverso di i, i^{-1} e quindi anche $i^{-1}\cdot i = i\cdot i^{-1} = 1$, fatto in contrasto con la precedente proposizione ∎

T23 b.05 Prop. Consideriamo un anello.u $\boldsymbol{R}$, un suo sottoinsieme $S = \{s_1, ..., s_n\}$ e il sottoinsieme

$$\langle S \rangle_R := \bigcup_{\{s_1,...,s_n\}\subseteq S} \{r_1, ..., r_n \in R :|\ r_1 s_1 + \cdots + r_n s_n\}\ .$$

Questo è un ideale in $\boldsymbol{R}$ ed è il più piccolo ideale di $\boldsymbol{R}$ che contiene S.

Dim.: Dato che $\boldsymbol{R}$ contiene zero e unità, si ha $\langle {}_R S \rangle \supseteq S$; inoltre dalla sua espressione si ricava facilmente che soddisfa le tre richieste [Idl 1], [Idl 2] ed [Idl 3] ∎

Il precedente ideale è chiamato **ideale generato** da S.

La notazione $\langle S \rangle_R$ si può accostare a quella usata per i sottogruppi ciclici [T22b10] e come questa può essere abbreviata nella $\langle S \rangle$ nei contesti nei quali si trattano solo anelli.u e loro ideali.

T23 b.06 Prop. Sono particolarmente interessanti gli ideali generati da un singoletto, cioè da un solo elemento s dell'anello.u $\boldsymbol{R}$, ideali aventi la forma $\langle s \rangle_R = \{r \cdot s\ \ |:\ \ r \in R\}$ per qualche elemento $s \in R$; un tale ideale è chiamato **ideale principale**.

T23 b.07 (1) Prop.: L'intersezione di due ideali I_1 e I_2 di un anello.u $\boldsymbol{R}$ è anch'essa un ideale di tale struttura.

Dim.: La richiesta [Idl 1] è soddisfatta in quanto anche l'intersezione di due sottogruppi è sottogruppo. Per la richiesta [Idl 2] basta osservare che $a, b \in I_1 \cap I_2 \implies a - b \in I_1\ ,\ a - b \in I_2$. Considerazione analoga per la [Idl 3] ∎

La precedente dimostrazione si generalizza senza difficoltà alle intersezioni di famiglie di ideali.

(2) Prop.: Consideriamo una famiglia di ideali dell'anello $\boldsymbol{R}$ caratterizzata dall'insieme di indici J $\searrow$ $\{I_j\ \ |:\ \ j \in J\}$; anche l'intersezione di tale famiglia di ideali $\bigcap\{j \in J\ :|\ I_j\}$ è un ideale di $\boldsymbol{R}$ ∎

T23 b.08 Consideriamo una successione di ideali, $\langle I_1, I_2, ... \rangle$ che sia ascendente, cioè tale che $I_1 \subset I_2 \subset I_3 ...$. Allora anche la loro unione $U := \bigcup\{j \in J\ :|\ I_j\}$ è un ideale.

Dim.: Consideriamo $a, b \in U$ ed $r \in R$; siano h il minimo intero per il quale $a \in I_h$, k il minimo intero tale che $b \in I_k$ e $m := \max(h, k)$.
Sia a che b appartengono all'ideale I_m e quindi anche $a + b \in I_m$ e per ogni $r \in R$ $r\,a \in I_m$. Dunque $a + b$ e ogni $r\,a$ appartengono ad U ∎

T23 b.09 Un dominio di integrità $\boldsymbol{R}$ in cui ogni ideale è principale è detto **dominio a ideali principali**.

(1) Prop.: Un qualunque campo $\boldsymbol{F}$ è un anello a ideali principali.

Dim.: $\boldsymbol{F}$ è un anello commutativo che possiede soltanto i due ideali che si possono esprimere come $\langle 0 \langle >$ ed $\langle e \rangle = F$, e quindi che sono ideali principali ∎

Il dominio di integrità degli interi naturali $\mathbb{N}$ è un dominio a ideali principali. Infatti, ogni ideale I è generato dal più piccolo intero positivo m che è contenuto in I, cioè ha la forma $\langle m \rangle$.
Anche l'anello $\boldsymbol{F}[x]$ è un dominio a ideali principali. Infatti ogni ideale I è generato dall'unico polinomio monico contenuto in I e avente grado minimo.

T23 b.10 Si dice **ideale massimale di un anello.u** $\boldsymbol{R}$ un suo ideale I che soddisfa le due seguenti condizioni:

[IdlM 1] I è incluso propriamente in R;

[IdlM 2] I non è incluso propriamente in alcun ideale proprio di $\boldsymbol{R}$ diverso da se stesso.

Per esempio, se $\boldsymbol{K}$ è un corpo, l'ideale $\langle 0 \rangle$ costituito dal solo zero di K è massimale, perché un corpo non possiede ideali propri [b04].

T23 b.11 Un ideale I di un anello.u commutativo $\boldsymbol{R}$ si dice **ideale primo** sse, per ogni due elementi $a, b \in R$ con $a \cdot b \in I$, accade che almeno uno dei due fattori a o b appartiene a I.

(1) Prop.: Sia I un ideale di un anello.u commutativo $\boldsymbol{R}$.
Se I è ideale massimale, esso è anche un ideale primo ∎

T23 b.12 Si chiama **radicale di un ideale** I di un anello $\boldsymbol{R}$, e lo si denota con $\mathsf{Rdcl}(I)$, il sottoinsieme di $\boldsymbol{R}$ costituito dagli elementi b di R, tali che $b^h \in I$ per qualche esponente intero positivo h.

Il radicale di I contiene I, in quanto per ogni $b \in I$, risulta $b^1 \in I$.

(1) Prop.: Il radicale di un ideale I di un anello.u abeliano $\boldsymbol{R}$ è anch'esso un'ideale di $\boldsymbol{R}$ QED

T23 b.13 Un ideale I di un anello abeliano $\boldsymbol{R}$ si dice **ideale primario** sse, ogniqualvolta il prodotto $a \cdot b$ di due elementi a, b di R appartiene ad I, ed a non sta in I, allora una opportuna potenza b^h di b sta in I, cioè b appartiene al radicale di I.

(1) Prop.: Ogni ideale primo è anche ideale primario ∎

T23 d. polinomi e anelli di polinomi

T23 d.01 Vengono studiati vari tipi di anelli costituiti da polinomi.

Innanzitutto si hanno gli insiemi dei polinomi in una variabile x sopra il campo dei numeri reali e sul campo dei numeri complessi.
Più in generale si hanno gli anelli dei polinomi in una variabile sopra un campo arbitrario $\mathbb{F}$ e gli anelli dei polinomi in un numero $d = 2, 3, ...$ di variabili.
Si possono inoltre considerare gli anelli dei polinomi in una successione infinita di variabili X_1, X_2, ..., X_d, ...

Quando le variabili delle costruzioni precedenti si considerano variare in un insieme terreno di un campo o di una simile struttura si possono considerare gli anelli.u delle relative funzioni polinomiali.

Anelli che si possono considerare estensioni dei precedenti sono forniti da insiemi di funzioni a valori reali o complessi soggetti a vincoli che si mantengono con l'addizione e il prodotto di tali funzioni.
Per tali anelli.u la somma e il prodotto sono le estensioni funzionali della somma e del prodotto per l'insieme codominio.
Per esempio si trattano gli anelli delle funzioni aventi come dominio un intervallo reale, che assumono valori reali e che sono continue.

T23 e. anelli di gruppo

T23 e.01 Consideriamo un gruppo $\boldsymbol{G}$ e un campo $\boldsymbol{F}$ e denotiamo con $\boldsymbol{F}[\boldsymbol{G}]_\phi$ l'insieme delle combinazioni lineari formali di elementi di $\boldsymbol{G}$ i cui coefficienti appartengono a $\boldsymbol{F}$ e che presentano solo un numero finito di addendi con coefficiente in $\boldsymbol{F}_{nz}$.
Se $\alpha := \sum_{g\in G} a_g\, g$ e $\beta := \sum_{g\in G} b_g\, g$ sono elementi di $\boldsymbol{F}[\boldsymbol{G}]_\phi$, definiamo come loro prodotto

$$\alpha\bullet\beta \;:=\; \sum_{g\in G}\sum_{h\in G} a_g\, b_h\; g\, h \;=\; \sum_{g,h\in G\ tc\ g\,h=k} a_g\, b_h\; k\ . \tag{1}$$

Si verifica facilmente che, munito di questo prodotto, $\boldsymbol{F}[\boldsymbol{G}]_\phi$ è un anello; questo viene chiamato **anello del gruppo $\boldsymbol{G}$** su $\boldsymbol{F}$.

L'espressione del coefficiente di k nell'ultima espressione in (1) è un caso particolare di una costruzione più generale sopra un gruppo.
Se α e β denotano due "opportune" funzioni su $\boldsymbol{G}$ con valori in un campo $\boldsymbol{F}$ o in una "simile" struttura, si definisce **prodotto di convoluzione delle funzioni** α e β

$$(\alpha * \beta) \;:=\; \left\lceil\, k\in G \mapsto \sum_{g,h\in G\ \left[\!\right]\ g\,h=k} \alpha(g)\,\beta(h) \,\right\rceil \;=\; \left\lceil\, k\in G \mapsto \sum_{g\in G} \alpha(g)\,\beta(g^{-1}\,k) \,\right\rceil\ . \tag{2}$$

Alle opportune funzioni su $\boldsymbol{G}$ si chiede che siano in grado di attribuire utilità alle sommatorie delle definizioni, come si è fatto sopra e come si può fare per i gruppi finiti.
Altri interessanti prodotti di convoluzione sono trattati in D47.

T23 f. anelli principali e fattoriali

T23 f.01 Per un anello $\langle R, +, -, 0, \cdot \rangle$ può accadere che presi due elementi $r, s \in R$, diversi dallo zero, il loro prodotto $r \cdot s$ sia uguale allo stesso elemento zero. Tali elementi si dicono **divisori dello zero**.

Consideriamo l'anello.u $\langle \mathbb{Z}_6, +_6, -_6, 0, \cdot_6, 1 \rangle$; in esso $2 \cdot_6 3 = 0$, cioè 2 e 3 sono divisori dello zero. In ogni anello $\mathbb{Z}_m$ con m intero naturale fattorizzabile (maggiore di 3) si trovano divisori dello zero, in quanto se si può scrivere $m = r \cdot s$ con $r, s \in \{2, 3, 4, ...\}$, si ha $[r]_m \cdot_m [s]_m = [0]_m = [m]_m$.

Eserc. Dimostrare che nell'anello $\mathbb{Z}_m$ l'insieme dei divisori dello zero coincide con l'insieme degli interi in $\{2, ..., m-1\}$ che non sono primi con m, cioè che sono dotati di un divisore comune con m.
Concludere che ogni anello $\mathbb{Z}_p$ con p numero primo è privo di divisori dello zero.

T23 f.02 Si trovano molte coppie di matrici 2×2 sui reali che costituiscono divisori dello zero $\mathbf{0}_{2,2}$: in particolare:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \qquad\qquad \begin{bmatrix} a & -a \\ b & -b \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Ricordiamo che si dice **dominio di integrità** ogni anello.u commutativo privo di divisori dello zero.
Denotiamo con **Intdmn** la classe dei domini di integrità.

T23 f.03 Come per un magma abeliano $\langle R, \cdot \rangle$, per un anello abeliano $\langle R, +, -, 0, \cdot \rangle$ si dice che vale la **legge di cancellazione per un anello abeliano** sse

$$\forall a, b \in R \ , \ r \in R \setminus \{0\} \ : \ r \cdot a = r \cdot b \Longrightarrow a = b \ .$$

Vi sono anelli abeliani nei quali la legge di cancellazione non vale.
Per esempio in $\mathbb{Z}_4$ si ha $2 \cdot_4 3 = 2 \cdot_4 1 = 2 \implies 3 = 1$.

(1) Prop.: Sia $\boldsymbol{R}$ un anello abeliano.

$$\boldsymbol{R} \text{ è un dominio di integrità} \iff \text{per } \boldsymbol{R} \text{ vale la legge di cancellazione .}$$

Dim.: "$\Longrightarrow$": se $\boldsymbol{R}$ è un dominio di integrità si ha: $r \neq 0 \wedge r \cdot a = r \cdot b \implies r \cdot (a - b) = 0 \implies a - b = 0 \implies a = b$.

"$\Longleftarrow$": in $\boldsymbol{R}$ valga la legge di cancellazione e sia $a \cdot b = 0$, allora:
se $a \neq 0$, $a \cdot 0 = 0 = a \cdot b$ e quindi $b = 0$;
se viceversa $b \neq 0$, $0 \cdot b = 0 = a \cdot b$ e quindi $r = 0$ ∎

La legge di cancellazione apre la possibilità di numerose utili elaborazioni; i domini di integrità sono quindi da considerare come anelli che forniscono strumenti elaborativi particolarmente efficaci.

La legge di cancellazione può anche essere usata per sistemi di assiomi per la specie di strutture anello unifero che costituiscono varianti di quello presentato in a01.

T23 f.04 Come per un magma dotato di uno zero 0, un elemento q diverso dallo zero di un anello (o di un anello.u) $\boldsymbol{R}$ viene chiamato **elemento nilpotente di un anello** sse si trova un intero positivo h tale che la sua potenza q^h è uguale allo zero della struttura.
Il più piccolo di tali h viene detto **grado di nilpotenza** dell'elemento q.

Un interessante esempio di elementi nilpotenti di un anello.u è fornito dalle matrici triangolari strette sopra un monoide.

Come per un magma unifero o per un monoide, un elemento q diverso dall'unità di un anello.u $\boldsymbol{R}$ per il quale esiste un intero positivo h tale che $q^h = \mathbf{1}$ si dice **elemento periodico**; se h è il più piccolo intero

positivo per cui questo si verifica, si dice che q ha **periodo di un elemento di un anello** h (talora si dice invece che q ha "ordine" h).

L'unità ha sempre periodo 1, lo zero di qualsiasi anello non è periodico.
In $\mathbb{Z}_5$: $\mathrm{prd}(2) = 3$, $\mathrm{prd}(3) = 2$ e $\mathrm{prd}(4) = 4$.
In $\mathbb{Z}_6$: $\mathrm{prd}(5) = 5$, mentre 2, 3 e 4 non sono periodici.
In $\mathbb{Z}_7$: $\mathrm{prd}(2) = 4$, $\mathrm{prd}(3) = 5$, $\mathrm{prd}(4) = 4$, $\mathrm{prd}(5) = 3$ e $\mathrm{prd}(6) = 6$.

T23 f.05 Ricordiamo che si dice **corpo** un anello.u $\boldsymbol{R}$, in cui gli elementi diversi dallo zero formano gruppo rispetto all'operazione prodotto.
Denotiamo con **Krp** la classe dei corpi. In formule:

$$\mathsf{Krp} \;:=\; \big\{ \boldsymbol{R} = \langle R, \bullet, -, \mathbf{0}, \bullet, \mathbf{1} \rangle \in \mathsf{Rng} \;\P\; \langle R \setminus \{\mathbf{0}\}, \bullet, inv(\bullet), \mathbf{1} \rangle \in \mathsf{Grp} \big\}$$

$$\boldsymbol{R} = \langle R, \bullet, -, \mathbf{0}, \bullet, \mathbf{1} \rangle \in \mathsf{Rng} \;,\; \langle R \setminus \{\mathbf{0}\}, \bullet, inv(\bullet), \mathbf{1} \rangle \in \mathsf{Grp} \implies \boldsymbol{R} \in \mathsf{Krp} \;.$$

L'anello.u binario $\langle \mathbb{B}, +_2, +_2, 0, \cdot, 1 \rangle$, oltre a essere l'anello.u nonnullo più piccolo, è anche il corpo più piccolo.

L'insieme degli elementi del corpo $\boldsymbol{R}$ diversi dallo zero, prende il nome di **gruppo moltiplicativo del corpo** $\boldsymbol{R}$; e, come si è detto [:a13] si denota localmente con $\boldsymbol{R}^{\mathsf{X}}$.

Un corpo in cui il prodotto sia commutativo viene detto **corpo commutativo** o **campo**. Un corpo non-commutativo viene anche chiamato **corpo sghembo** (*skewfield*).
Denotiamo con **Fld** la classe dei campi e con **KrpNab** la classe dei corpi sghembi.

Testo fruibile in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php