

# ALGEBRA DELLE CLASSI DI RESTO 2

## Esercizi di calcolo con le classi di resto...e un po' di teoria di Leonardo Calconi

Possiamo sommare, sottrarre e moltiplicare le classi di resto come fossero numeri ?  
Possiamo calcolare il valore di espressioni aritmetiche sostituendo gli interi con le classi di resto ?  
Possiamo risolvere equazioni nelle quali sia l'incognita che i coefficienti sono classi di resto ?

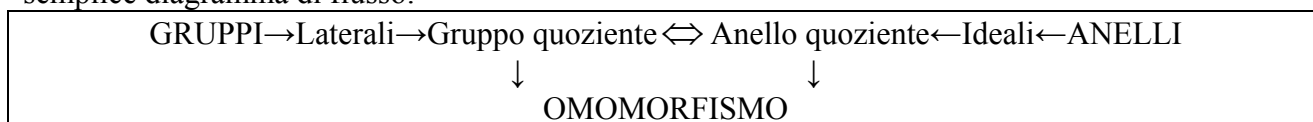
Dimostreremo che la risposta alla prima domanda è affermativa per le operazioni di addizione, sottrazione, moltiplicazione, elevazione a potenza intera ed estrazione di radici perfette, ovvero che queste operazioni valide in  $\mathbb{Z}$  sono altrettanto valide in  $\mathbb{Z}_n$ , ovvero che nel passaggio da  $\mathbb{Z}$  a  $\mathbb{Z}_n$  la struttura algebrica non cambia.

Per quanto riguarda la seconda domanda, implicando essa la divisione, la risposta è negativa ed affermativa ad un tempo; in linea generale ciò non è ovviamente possibile in quanto in  $\mathbb{Z}$  e in ogni suo sottogruppo non esistendo gli inversi manca la chiusura rispetto a questa operazione; pur tuttavia è possibile eseguire la divisione, come vedremo, a determinate condizioni.

Come risposta alla terza domanda, infine, mostreremo che con le opportune condizioni è possibile risolvere equazioni e sistemi in  $\mathbb{Z}_n$ .

Il contenuto di questo lavoro, che considero un'appendice a "Algebra delle classi di resto 1" disponibile all'indirizzo [www.4dmatrix.it/math](http://www.4dmatrix.it/math), è un'esplorazione delle possibilità di eseguire calcoli con le quattro operazioni in  $\mathbb{Z}_n$  ed il suo approccio è quindi in parte euristico.

Per arrivare il più presto possibile al sodo che inizia col capitolo 3, ho evitato di impantanarmi in un pesante lavoro di esposizione delle teorie dei gruppi e degli anelli a colpi di dimostrazioni che avrebbe costituito solo una brutta copia di un buon libro di algebra, preferendo limitarmi al ripasso dei principali concetti di queste teorie che sono indispensabili alla comprensione dei calcoli eseguiti nel capitolo 4 che costituiscono il vero scopo di questo lavoro, ripasso che posso esprimere con un semplice diagramma di flusso:



### Contenuto

#### 1 Elementi di teoria dei gruppi

##### 1.1 Laterali

##### 1.2 Gruppo quoziente

##### 1.3 Omomorfismi di gruppi

###### 1.3.1 Definizione di omomorfismo

###### 1.3.2 Tipi di omomorfismo

###### 1.3.3 Omomorfismo di $G$ su $G/H$

#### 2 Elementi di teoria degli anelli

##### 2.1 Ideali e anello quoziente

##### 2.2 Omomorfismi di anelli

##### 2.3 Altre definizioni utili

#### 3 Le quattro operazioni con le classi di resto

##### 3.1 Addizione

##### 3.2 Opposti ed inversi

##### 3.3 Sottrazione

##### 3.4 Moltiplicazione ed elevazione a potenza

##### 3.5 Divisione

#### 4 Esercizi di calcolo con le quattro operazioni

# 1 ELEMENTI DI TEORIA DEI GRUPPI

## 1.1 Lateralali

Sia  $G$  un gruppo ed  $H$  un suo sottogruppo. Mediante  $H$  noi possiamo effettuare una partizione di  $G$  in classi di equivalenza che lo esauriscono e chiamare tali classi *lateralali destri* di  $H$  in  $G$ . Come fare ?

Iniziamo col costruire un *laterale destro*.

Si prendono tutti gli elementi di  $H$  e se ne effettua il prodotto, secondo l'operazione per il quale  $G$  è definito, con un elemento arbitrario  $a \in G$ :

$Ha = \{ha : h \in H\}$ . Allora  $Ha$  è un laterale destro di  $H$  in  $G$  generato da  $a$ .

E i *lateralali sinistri* ?

Si prende un elemento arbitrario  $a \in G$  e se ne effettua il prodotto con tutti gli elementi di  $H$  secondo l'operazione per il quale  $G$  è definito:

$aH = \{ah : h \in H\}$ . Allora  $aH$  è un laterale sinistro di  $H$  in  $G$  generato da  $a$ .

In genere i laterali destri differiscono dai laterali sinistri, ma se  $G$  è abeliano essi coincidono ed ogni suo sottogruppo  $H$  è detto *normale*.

Ora poniamoci due domande:

1) quanti sono gli elementi di  $Ha$  ?

Ovviamente tanti quanti sono gli elementi di  $H$  :  $o(H)$ .

2) quanti sono i laterali destri di  $H$  in  $G$  ?

Poichè ogni elemento di  $G$  appartiene ad un solo laterale destro, dovrebbe essere evidente che tutti i laterali destri esauriscono  $G$ . Se non è evidente, basta prendere in considerazione un gruppo finito  $G$  di cinque elementi ed un suo sottogruppo di quattro elementi e poi sviluppare la chiusura rispetto all'operazione  $a, b \in G \rightarrow ab \in G$  per rendersi conto che le cose stanno esattamente in questi termini (i numeri rappresentano entità qualsiasi ma tali che  $G$  sia un gruppo finito e  $H$  un suo sottogruppo):

idx	$Ha_0$	$Ha_1$	$Ha_2$	$Ha_3$	$Ha_4$
$h/a$	0	1	2	3	4
0	00	01	02	03	04
1	10	11	12	13	14
2	20	21	22	23	24
3	30	31	32	33	34

Ma allora, detto  $n(Ha)$  il numero dei laterali destri, la decomposizione di  $G$  sarà data da

$$o(G) = n(Ha)o(H)$$

da cui il numero dei laterali destri  $n(Ha) = \frac{o(G)}{o(H)}$

che, per l'esempio precedente vale appunto  $\frac{20}{4} = 5$

e che altro non è che il Teorema di Lagrange per il quale  $o(H) \mid o(G)$  con  $G$  finito.

Ma poichè noi sappiamo che  $G$  è esaurito da una sua partizione in classi di equivalenza, ecco che i laterali destri di  $H$  in  $G$  sono le classi di equivalenza di  $G$ .

## 1.2 Gruppo quoziente

Sia  $G$  il gruppo additivo degli interi e  $H$  un suo sottogruppo formato dai multipli di 5.

Costruiamo una serie di laterali destri che esauriscano  $G$ :

$Ha_0 = H + 0$	...	-10	-5	0	5	10	...
$Ha_1 = H + 1$	...	-9	-4	1	6	11	...
$Ha_2 = H + 2$	...	-8	-3	2	7	12	...
$Ha_3 = H + 3$	...	-7	-2	3	8	13	...
$Ha_4 = H + 4$	...	-6	-1	4	9	14	...

Ci sono altri laterali destri oltre questi? No, infatti

$$Ha_5 = H + 5 = Ha_0$$

$$Ha_6 = H + 6 = Ha_1$$

...

$$Ha_n = H + n = Ha_{n-5}$$

per qualsiasi altro elemento di  $G$ .

Dunque i cinque laterali destri di  $H$  in  $G$  appena costruiti sono tutti quelli possibili e quindi rappresentano le classi di equivalenza in  $G$ , in ossequio al principio che, ripartendo le classi di equivalenza  $G$  in sottoinsiemi disgiunti, due laterali destri o hanno tutti gli elementi in comune o non ne hanno nessuno.

Notare bene che abbiamo detto “di  $H$ ”.

Infatti se cambiamo  $H$  cambia anche il numero dei laterali destri: se  $H$  fosse il sottogruppo dei multipli di 6 avremmo 6 laterali; se fosse il sottogruppo dei multipli di 8 avremmo 8 laterali e così via.

Si verifica facilmente che in questo esempio la costruzione di laterali sinistri porta a  $Ha = aH$  ed allora chiameremo  $H$  *sottogruppo normale* di  $G$  intendendo definire così un sottogruppo i cui laterali destri coincidono con i sinistri, ovvero tale che il prodotto di due laterali destri è ancora un laterale destro (e che il prodotto di due laterali sinistri è ancora un laterale sinistro):

$$HaHb = H(aH)b = H(Ha)b = HHab = Hab$$

$$(HH = H \text{ perchè } H \supset HH \supset He)$$

Ora noi chiameremo l'insieme dei laterali destri  $Ha$  di un gruppo  $G$ , gruppo quoziente  $G/H$  di  $G$  rispetto ad  $H$  che è a sua volta un gruppo e per quanto detto in precedenza si avrà che

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

Verifichiamo che  $G/H$  ha la struttura di gruppo:

- chiusura:

$$\text{se } Ha, Hb \in G/H \text{ sarà } HaHb \in G/H$$

- associatività:

$$\begin{aligned} (HaHb)Hc &= H(ab)HHc = H(ab)Hc = HH(ab)c = H(ab)c = \\ &= Ha(bc) = HHa(bc) = Ha(Hbc) = Ha(HHbc) = Ha(HbHc) \end{aligned}$$

- elemento neutro:  
se  $H = He$  sarà  $HaHe = HHae = Hae = Ha$
- inverso:

$$HaHa^{-1} = HHaa^{-1} = Haa^{-1} = He$$

A questo punto abbiamo dimostrato l'importante teorema che afferma che se  $H$  è un sottogruppo normale di  $G$ , allora  $G/H$  è il gruppo quoziente di  $G$  rispetto ad  $H$

Nell'esempio di questo paragrafo abbiamo ripartito  $G = \mathbb{Z}$  in quelle che nel linguaggio degli anelli si chiamano classi di resto che tutte assieme formano il gruppo quoziente.

E' superfluo dire che se  $G$  fosse moltiplicativo non sarebbe gruppo per l'assenza degli inversi e quindi non sarebbe possibile una sua decomposizione in parti che lo esauriscono per l'impossibilità di costruire laterali destri e quindi un gruppo quoziente.

Per riassumere in una sola affermazioni i risultati fin qui ottenuti possiamo dire di aver trasformato un insieme in un altro insieme che, pur essendo organizzato (ripartito...) in modo differente dal primo, ne conserva la struttura di gruppo.

Pertanto:

1. deve esistere un modo per definire la relazione che lega i due gruppi;
2. è lecito domandarsi se nel passaggio da un gruppo all'altro la struttura algebrica è conservata.

Questi sono gli argomenti del prossimo paragrafo.

### 1.3 Omomorfismi di gruppi

#### 1.3.1 Definizione di omomorfismo

Un omomorfismo è un'applicazione  $\varphi : G \rightarrow G'$  che soddisfa queste *due condizioni*:

1.  $\forall g \in G$  ha un'unica immagine in  $G'$ .

Notare che:

- a. Elementi distinti di  $G$  possono non avere immagini distinte in  $G'$  e quindi l'applicazione non è necessariamente iniettiva.
- b. Elementi di  $G'$  possono non essere immagine di alcun elemento di  $G$  e quindi l'applicazione non è necessariamente suriettiva.
- c. La 1) quindi impone solamente che non ci siano elementi di  $G$  privi di immagine o con immagine multipla in  $G'$ , e poichè questa è la condizione necessaria perchè  $\varphi$  sia un'applicazione, la 1) stessa è tautologica.

2.  $\varphi(ab) = \varphi(a)\varphi(b)$  se  $a \rightarrow a', b \rightarrow b', a, b \in G, a', b' \in G'$ .

Notare che:

- a. La condizione 2) impone che l'operazione per la quale  $G$  è definito si conservi nell'operazione per la quale  $G'$  è definito.
- b. Le operazioni nei due gruppi possono non essere le stesse.
- c. In buona sostanza il risultato dell'operazione in  $G$  deve essere lo stesso dell'operazione in  $G'$ .

#### 1.3.2 Tipi di omomorfismi

Proviamo a classificare e definire i diversi tipi di omomorfismi con alcuni esempi.

##### Omomorfismo generico $\rightarrow$ nè iniettivo nè suriettivo

► Esempio: sia  $G$  il gruppo delle matrici quadrate  $2 \times 2$  con determinante diverso da zero e sia  $G' = \mathbb{R}$ , ambedue moltiplicativi. Sia  $\varphi(A) = \det(A)$ . L'applicazione è un omomorfismo in

quanto per la regola di Binet di ha  $\varphi(AB) = \det(AB) = \varphi(A)\varphi(B) = \det(A)\det(B)$ .

Ma poichè  $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} d & b \\ c & a \end{pmatrix}$  l'omomorfismo non è iniettivo. Del resto poichè

$0 \in G'$  esso non è neanche suriettivo.

► Contro esempio: se i due gruppi fossero additivi anzichè moltiplicativi non ci sarebbe omomorfismo perchè  $\det(A+B) \neq \det(A) + \det(B)$ .

#### **Monomorfismo → omomorfismo iniettivo**

► Esempio: sia  $G = \mathbb{R}$  additivo e  $G' = \mathbb{R}$  moltiplicativo. Sia  $\varphi(a) = e^a$ . L'applicazione è un omomorfismo perchè  $\varphi(a+b) = e^{a+b} = \varphi(a)\varphi(b) = e^a \cdot e^b$ . L'omomorfismo è chiaramente iniettivo, ma essendo  $e^a$  sempre positivo gli elementi non positivi di  $G'$  non sono immagine di alcun elemento di  $G$  e quindi non è suriettivo.

► Contro esempio: l'applicazione è  $\varphi(a) = a^e$  non è un omomorfismo in quanto la seconda condizione non è verificata avendosi  $(a+b)^e \neq a^e \cdot b^e$

#### **Epimorfismo → omomorfismo suriettivo**

► Esempio: sia  $G = \mathbb{R}$  privo dello zero e  $G' = \{1, -1\}$ , ambedue moltiplicativi.

Sia  $\varphi(a) = 1 \Leftrightarrow a^+$ ,  $\varphi(a) = -1 \Leftrightarrow a^-$ . L'applicazione è un omomorfismo perchè

$\varphi(ab) = 1 \cdot 1 = \varphi(a)\varphi(b) = 1$ ,  $\pm 1 \cdot \mp 1 = -1$ ,  $-1 \cdot -1 = 1$ . L'omomorfismo non è iniettivo perchè tutti gli elementi di  $G$  hanno come immagine in  $G'$  o 1 o -1. D'altronde sia 1 che -1 sono immagine di elementi di  $G$  e quindi l'omomorfismo è suriettivo.

► Contro esempio: se  $G$  è completo di zero  $\varphi$  non è un omomorfismo e neanche un'applicazione in quanto lo zero non ha immagine in  $G'$ .

#### **Isomorfismo → omomorfismo biiettivo**

► Esempio: siano  $G = \mathbb{R}^+$  moltiplicativo e  $G' = \mathbb{R}$  additivo. Sia  $\varphi(a) = \log_{10} a$ .

L'applicazione è un omomorfismo perchè

$\varphi(ab) = \log_{10}(ab) = \varphi(a) + \varphi(b) = \log_{10} a + \log_{10} b$  ed è banalmente biunivoca.

► Contro esempio: se fosse  $G' = \mathbb{R}^+$  la prima condizione non sarebbe più verificata in quanto gli elementi di  $G$   $0 < a \leq 1$  non avrebbero immagine in  $G'$  e quindi  $\varphi$  non sarebbe neanche un'applicazione.

#### **Automorfismo → isomorfismo di $G \rightarrow G$**

► Esempio:  $G = G' = \mathbb{R}$  additivo. L'applicazione  $\varphi(x) = x$  è evidentemente e banalmente un isomorfismo di  $G$  su se stesso.

Se ora definiamo come *nucleo*  $K_\varphi$  di un omomorfismo di  $G$  in  $G'$  il sottogruppo normale di  $G$  costituito da tutti quegli elementi che  $\varphi$  trasforma in  $e$  in  $G'$ , avremo a disposizione un bel metodo per riconoscere un isomorfismo.

Se infatti consideriamo il laterale destro-nucleo  $K_\varphi a$  di  $G$  è evidente che tutte le  $ka$  sono immagini inverse dello stesso elemento  $a' \in G'$  e quindi l'applicazione non è iniettiva. Ma se

$K_\varphi$  consta del solo elemento  $e$ , elementi distinti  $ka$  saranno immagini inverse uniche di altrettanti elementi  $a' \in G'$  e l'applicazione sarà iniettiva. Se questo omomorfismo è un epimorfismo siamo allora in presenza di un isomorfismo.

Pertanto due gruppi  $G$  e  $G'$  sono isomorfi se il nucleo dell'omomorfismo dell'uno sull'altro consta del solo elemento neutro:  $K_\varphi = e$

Due gruppi isomorfi sono algebricamente identici variando solo nella scrittura.

### 1.3.3 Omomorfismo di $G$ su $G/H$

Definiamo tale l'applicazione  $\varphi(a) = Ha : G \rightarrow G/H, \forall a \in G$  la cui dimostrazione è implicita in quanto esposto nel paragrafo precedente.

Se ora poniamo  $G = \mathbb{Z}$  e  $G/H = \mathbb{Z}_n$  (rivedere il paragrafo 1.2) avremo stabilito che in  $\mathbb{Z}_n$  viene conservata la struttura algebrica di  $\mathbb{Z}$  e a questo punto del nostro percorso saremo riusciti a trasportare addizione e sottrazione da  $\mathbb{Z}$  a  $\mathbb{Z}_n$ .

Ora possiamo chiederci se, avendo a disposizione qualche proprietà in più oltre quelle offerte dai gruppi, possiamo parlare anche di altre operazioni quali la moltiplicazione o la divisione.

## 2 ELEMENTI DI TEORIA DEGLI ANELLI

### 2.1 Ideali e anello quoziente

$\mathbb{Z}$  e  $\mathbb{Z}_n$  sono oltre che gruppi anche anelli commutativi  $R$  con unità e quindi tutti i sottogruppi sono normali. Allora definiamo *ideali*  $P$  di  $R$  come sottogruppi additivi di  $R$  definiti da  $Pa = aP = \{Pa : \forall p \in P, \forall a \in R\}$ .

Ma allora, analogamente a quanto visto per i gruppi, possiamo definire come *anello quoziente*  $R/P$  l'insieme dei laterali di  $P$  in  $R$  (non si fa distinzione tra laterali destri e sinistri perchè  $R$  è abeliano).

$R/P$  ha già la struttura additiva visto che prima di essere anello è gruppo. Perchè sia realmente anello si deve definire per lui anche una struttura moltiplicativa e fatto questo esso sarà automaticamente omomorfo ad  $R$ .

Nel paragrafo 1.2 abbiamo dimostrato che per i gruppi il prodotto di due laterali destri è ancora un laterale destro:

$$HaHb = H(aH)b = H(Ha)b = HHab = Hab$$

dove per "prodotto" si deve intendere l'addizione e quindi

$$(H+a) + (H+b) = H + (a+b)$$

Quanto sopra vale ovviamente anche per gli anelli e quindi quello che dobbiamo verificare è se è anche vero che il prodotto di due ideali è ancora un ideale:

$$(P+a) \cdot (P+b) = P + (a \cdot b)$$

dove per "prodotto" questa volta intendiamo la moltiplicazione.

La dimostrazione è una di quelle che non possono certo definirsi affascinanti e avremmo potuto ometterla senza danno, comunque eccola qui.

Poniamo  $a' = a + s$  e  $b' = b + t$  con  $a', b' \in R$  e tali che  $a' + p = a + p$  e  $b' + p = b + p$   
 Ora dai due passaggi seguenti

$$a' + p = a + p = (a + s) + p = (a + p) + (s + p)$$

$$b' + t = b + t = (b + t) + p = (b + p) + (t + p)$$

segue che  $s, t \in P$  e quindi

$$(a' + p) \cdot (b' + p) = (a' b') + p = [(ab) + (at) + (sb) + (st)] + p = p + (ab)$$

A questo punto si potranno verificare le proprietà degli anelli per vedere che esse siano rispettate.

## 2.2 Omomorfismi di anelli

C'è poco da dire; in buona sostanza, le definizioni date per gli omomorfismi tra gruppi  $G$  passano tali e quali a quelli tra anelli  $R$  a patto che vengano conservate le *due operazioni*:

$$\varphi(a + b) = \varphi(a') + \varphi(b')$$

$$\varphi(a \cdot b) = \varphi(a') \cdot \varphi(b')$$

## 2.3 Altre definizioni utili

E ciò, con l'aggiunta di alcune definizioni utili, è quanto basta sugli anelli per gli scopi di questo lavoro.

**Caratteristica:** un intero positivo  $q$  tale che  $q \circ a = 0$ ,  $a \in R$ . Ad esempio  $\mathbb{Z}_5$  ha caratteristica 5 in quanto  $[5]$  e tutti i multipli di  $[5]$  sono uguali a  $[0]$ . E' bene ricordare che in  $\mathbb{Z}_n$  esistono soltanto  $n$  elementi da  $[0]$  a  $[n-1]$ .

**Divisori dello zero:** un elemento  $a \neq 0 \in R$  tale che  $ab = ba = 0$

**Anello commutativo con unità:** un anello dotato della proprietà commutativa e dell'elemento neutro moltiplicativi.

**Dominio d'integrità:** un anello commutativo con unità privo di divisori dello zero. Se un dominio d'integrità è finito allora è un campo.

# 3 LE QUATTRO OPERAZIONI CON LE CLASSI DI RESTO

## 3.1 Addizione

Dobbiamo mostrare che l'applicazione  $\varphi(x) = x \equiv a \pmod{n} : \mathbb{Z} \rightarrow \mathbb{Z}_n$  che manda un numero intero  $x \in \mathbb{Z}$  nella classe  $[a] \in \mathbb{Z}_n$  di tutti quei numeri che divisi per  $n$  danno resto  $a$  è o un omorfismo o un isomorfismo.

Controlliamo prendendo come esempio  $\mathbb{Z}_n = \mathbb{Z}_8$

► *Prova dell'omomorfismo:*  $(10 + 8) = 18 \rightarrow [10] + [8] = [2]$ .

Infatti secondo la  $\varphi$  si ha che  $18 \rightarrow [2]$ .

L'omomorfismo pur essendo evidentemente suriettivo non è iniettivo in quanto è  $K \neq \{e\}$ , ovvero il nucleo contiene infiniti elementi di  $\mathbb{Z}$  che tramite  $\varphi$  finiscono nell'elemento neutro di  $\mathbb{Z}_n$ ; nel

nostro esempio  $\{\dots -16, -8, 8, 16, \dots\}$ . Ma per la conservazione dell'operazione non è necessario l'isomorfismo e pertanto la struttura algebrica di  $\mathbb{Z}$  è conservata in  $\mathbb{Z}_n$ .

Ora proviamo a verificare se alcune proprietà dei gruppi additivi da  $\mathbb{Z}$  si trasferiscono in  $\mathbb{Z}_n$ .

► *Associatività*: secondo la  $\varphi$   $18 \rightarrow [2]$ ; infatti

$$3 + (8 + 7) = (3 + 8) + 7 = 18 \rightarrow [3] + ([8] + [7]) = ([3] + [8]) + [7] = [2]$$

► *Cancellazione*:

$$(3 + 15) + \cancel{4} = (12 + 6) + \cancel{4} = 18 \rightarrow ([3] + [15]) + \cancel{[4]} = ([12] + [6]) + \cancel{[4]} = [2]$$

► *Elemento neutro*: è banalmente vero che  $0 \rightarrow [0]$

► *Elemento opposto*: è banalmente vero che  $7 - 7 = [7] - [7] = 0$

Inoltre, poichè  $\mathbb{Z}$  è abeliano e quindi lo è anche  $\mathbb{Z}_n$  che è un suo sottogruppo, possiamo aggiungere la

► *Commutatività additiva*:

$$7 + 3 = 3 + 7 = 10 \rightarrow [7] + [3] = [3] + [7] = [2]$$

### 3.2 Opposti ed inversi

Prima di passare ai paragrafi seguenti bisogna aver ben chiaro cosa sono gli opposti e gli inversi negli anelli delle classi di resto.

Dunque, un elemento di  $\mathbb{Z}_n$  addizionato al suo opposto manda la somma nella classe di resto  $[0]$  che è l'elemento neutro additivo, mentre lo stesso elemento moltiplicato per il suo inverso manda il prodotto nella classe di resto  $[1]$  che è l'elemento neutro moltiplicativo.

Ecco una tabella di esempi; la classe a sinistra è l'*opposto* (o inverso additivo), quella a destra l'*inverso* (o inverso moltiplicativo);  $n$  è primo per assicurare l'esistenza degli inversi:

$i+, i\bullet$	$\mathbb{Z}_5$	$\mathbb{Z}_7$	$\mathbb{Z}_{11}$
$[2]$	$[3], [3]$	$[5], [4]$	$[9], [6]$
$[3]$	$[2], [2]$	$[4], [5]$	$[8], [4]$
$[6]$		$[1], [6]$	$[5], [2]$
$[9]$			$[2], [6]$

### 3.3 Sottrazione

L'esistenza dell'elemento opposto ci garantisce che anche la sottrazione viene conservata in quanto addizione di un elemento con l'opposto di un altro; ad esempio in  $\mathbb{Z}_{11}$  abbiamo

$$9 - 3 = 6 \rightarrow [9] + [3_i] = [9] + [8] = [6]$$

ed infatti secondo la  $\varphi$  è  $6 \rightarrow [6]$ .

### 3.4 Moltiplicazione ed elevazione a potenza

Ma poichè  $\mathbb{Z}$  è un anello commutativo con unità possiamo verificare un numero ben più alto di proprietà che ci permettono di affermare che anche la moltiplicazione (e quindi l'elevazione a potenza intera e l'operazione inversa di estrazione di radice perfetta) è conservata.

Ciò, naturalmente, dopo aver verificato che l'applicazione  $\varphi$  è un omomorfismo anche moltiplicativo. In  $\mathbb{Z}_8$ :

► *Prova dell'omomorfismo*:  $(10 \cdot 8) = 80 \rightarrow [10] \cdot [8] = [2] \cdot [0] = [0]$ .

Infatti secondo la  $\varphi$  si ha che  $80 \rightarrow [0]$ .

► *Associatività moltiplicativa*: secondo la  $\varphi$  è  $168 \rightarrow [0]$ ; infatti

$$3 \cdot (8 \cdot 7) = (3 \cdot 8) \cdot 7 = 168 \rightarrow [3] \cdot ([8] \cdot [7]) = ([3] \cdot [8]) \cdot [7] = [0]$$

► *Cancellazione*:

$$(3 + 15) \cdot \cancel{4} = (12 + 6) \cdot \cancel{4} = 18 \rightarrow ([3] + [15]) \cdot \cancel{[4]} = ([12] + [6]) \cdot \cancel{[4]} = [2]$$

► *Elemento neutro moltiplicativo*: è banalmente vero che  $1 \rightarrow [1]$

► *Distributività*: secondo la  $\varphi$  è  $195 \rightarrow [3]$ ; infatti

$$13 \cdot (6 + 9) = 13 \cdot 6 + 13 \cdot 9 = 13 \cdot 15 = 195 \rightarrow [5] \cdot [7] = [3]$$

► *Commutatività moltiplicativa*: secondo la  $\varphi$   $10 \rightarrow [2]$  e  $21 \rightarrow [3]$ ; infatti

$$7 \cdot 3 = 3 \cdot 7 = 21 \rightarrow [7] \cdot [3] = [3] \cdot [7] = [3]$$

### 3.5 Divisione

Come detto all'inizio, in  $\mathbb{Z}$  e in  $\mathbb{Z}_n$  mancando gli inversi non si può parlare di divisione.

Possiamo comunque provare a vedere se ci sono delle condizioni sotto le quali tale operazione diviene possibile.

In  $\mathbb{Z}$  noi possiamo considerare ogni elemento non nullo come rapporto tra due elementi nel quale il

numeratore sia diviso dal denominatore:  $\frac{4}{2}, \frac{6}{3}, -\frac{144}{12}, \dots$  ovvero come il prodotto di un elemento

per l'inverso di un altro.

Ma se in  $\mathbb{Z}_n$  pensiamo alla divisione come alla moltiplicazione di un elemento per l'inverso di un altro ci accorgiamo che gli anelli commutativi con unità visti finora sono privi di tali inversi.

Dove possiamo trovare gli inversi moltiplicativi?

Li troviamo in un dominio d'integrità che, nel caso di  $\mathbb{Z}_n$  è tale solo quando  $n = p$  primo. E allora, poichè  $\mathbb{Z}_p$  è finito ed un dominio d'integrità finito è un campo, è nel campo  $F_p$  che troveremo per ogni elemento diverso da zero il suo inverso moltiplicativo.

L'applicazione

$$\varphi(x) = x \equiv a \pmod{n} : \mathbb{Z} \rightarrow F_p$$

resta un omomorfismo tra anelli per i quali addizione, sottrazione, moltiplicazione ed elevazione a potenza intera sono conservate.

Se per la divisione imponiamo la condizione che essa sia espressione frazionaria di un intero nella quale il denominatore divide il numeratore, anche questa operazione può dirsi conservata.

► *Esempio in  $F_5$* :  $1224 : 12 = 102 \rightarrow [4] \cdot [2_i] = [4] \cdot [3] = [2]$

Ecco cosa è successo: 1224 va in [4], 12 va in [2] e l'inverso di [2] è [3] perchè  $[2] \cdot [3] = [1]$

Per la verità esistono inversi anche negli anelli con indice non primo. Vedere a questo proposito gli esercizi (4.10) e (4.18) e "Algebra delle classi di resto 1".

#### 4 ESERCIZI DI CALCOLO CON LE QUATTRO OPERAZIONI

Cambio di notazione: d'ora in poi le parentesi quadre ci occorreranno per la gerarchia dei calcoli e pertanto per evitare confusioni una classe di resto  $[a]$  sarà indicata con  $\bar{a}$ .

Per facilitare la comprensione dei calcoli, gli opposti e gli inversi sono in rosso.

(4.1) ► In  $\mathbb{Z}_8$  mandare  $37 \rightarrow \bar{5}$  con l'espressione aritmetica

$$\begin{aligned} & [3 \cdot 2 \cdot (10 - 7 + 2^2) \cdot (7 - 2 + 3) - 2 \cdot 3 - 2] - [(2^3 + 7 - 18) - (7 + 10 - 15) + 13 - 17] - 300 = 37 \rightarrow \\ & \rightarrow [\bar{6} \cdot (\bar{2} + \bar{1} + \bar{4}) \cdot (\bar{7} + \bar{6} + 3) + \bar{2} + \bar{6}] - [(\bar{0} + \bar{7} + \bar{6}) - (\bar{7} + \bar{2} + \bar{1}) + \bar{5} + \bar{7}] + \bar{4} = \\ & = \bar{6} \cdot \bar{7} \cdot \bar{0} + \bar{0} - [\bar{5} + \bar{6} + \bar{5} + \bar{7}] + \bar{4} = \bar{1} + \bar{4} = \bar{5} \end{aligned}$$

(4.2) ► In  $\mathbb{Z}_{20}$  mandare  $-10 \rightarrow \bar{0}$  con l'espressione aritmetica

$$\begin{aligned} & -5 + (7 - 3 + 5 - 2 \cdot 3) - (3 \cdot 2^2 - 5 - 6 + 7) = -10 \rightarrow \\ & \bar{15} + (\bar{7} + \bar{17} + \bar{5} + \bar{14}) - (\bar{12} + \bar{15} + \bar{14} + \bar{7}) = \bar{15} + \bar{3} + \bar{12} = \bar{0} \end{aligned}$$

(4.3) ► In  $\mathbb{Z}_6$  mostrare che  $3^3 + 3^2 \rightarrow \bar{0}$  e che  $3^3 \cdot 3^2 \rightarrow \bar{3}^5 = \bar{3}$

$$\begin{aligned} & [\bar{3} \cdot \bar{3}] \cdot \bar{3} + [\bar{3} \cdot \bar{3}] = \bar{3} \cdot \bar{3} + \bar{3} = \bar{3} + \bar{3} = \bar{0} \text{ e infatti } 3^3 + 3^2 = 36 \rightarrow \bar{0} \\ & [\bar{3} \cdot \bar{3}] \cdot \bar{3} \cdot [\bar{3} \cdot \bar{3}] = \bar{3} \cdot \bar{3} \cdot \bar{3} = \bar{3} \cdot \bar{3} = \bar{3} \text{ e infatti } 3^5 = 243 \rightarrow \bar{3} \end{aligned}$$

(4.4) ► In  $F_{11}$  trovare la soluzione dell'equazione lineare  $\bar{4}\bar{x} + \bar{6} = \bar{3}$

$$\bar{x} = [\bar{3} + \bar{5}] \cdot \bar{3} = \bar{2}$$

Infatti la soluzione di  $4x + 6 = 3$  è  $x = 2 \rightarrow \bar{2}$

(4.5) ► Perché in  $\mathbb{Z}_{10}$  l'equazione dell'esercizio precedente non ha soluzione?

Perché ci occorrono l'opposto di  $\bar{6}$  e l'inverso di  $\bar{4}$  ma ambedue sono divisori dello zero:  
 $\bar{6} + \bar{4} = \bar{0}$ ,  $\bar{4} \cdot \bar{5} = \bar{0}$  ovvero  $(10, 6) = (4, 2) \neq 1$

(4.6) ► Trovare un indice  $n$  non primo di  $\mathbb{Z}_n$  nel quale l'equazione dell'esercizio precedente ha soluzione.

Tale indice deve essere primo con 6 e con 4 e pertanto, ad esempio, va bene 15:

$$\text{In } \mathbb{Z}_{15} \text{ si ha } \bar{x} = [\bar{3} + \bar{9}] \cdot \bar{4} = \bar{3}$$

(4.7) ► In  $F_{11}$  mandare  $-20 \rightarrow \bar{2}$  con un'espressione aritmetica

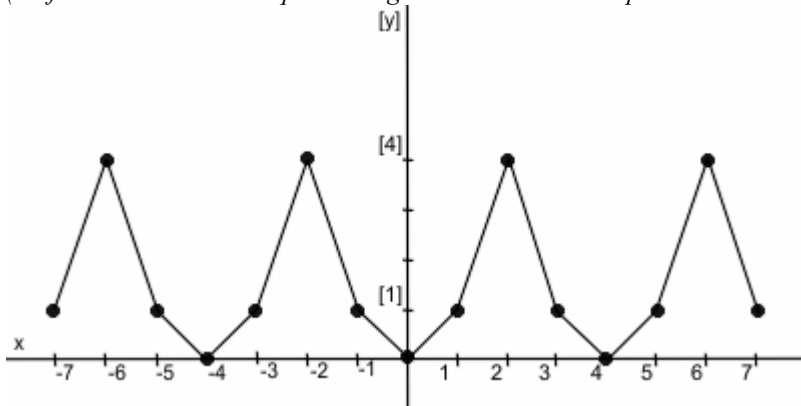
$$-7 - 5 \cdot 2 + 16 : 8 - 5 + 6 - 18 : 3 = -20 \rightarrow \bar{4} + \bar{1} + \bar{5} \cdot \bar{7} + \bar{6} + \bar{6} - \bar{7} \cdot \bar{4} = \bar{5} + \bar{2} + \bar{2} + \bar{4} = \bar{2}$$

(4.8) ► In  $F_{17}$  mostrare che  $\frac{\bar{8}}{\bar{4}} = \frac{\bar{12}}{\bar{6}} \rightarrow \bar{8} \cdot \bar{6} = \bar{12} \cdot \bar{4}$  è vero.

Infatti l'operazione di semplificazione è  $\frac{\overline{8} \cdot \overline{4} \cdot \overline{6}}{\overline{4}} = \frac{\overline{12} \cdot \overline{4} \cdot \overline{6}}{\overline{6}}$  dove  $\frac{\overline{4}}{\overline{4}} = \overline{4} \cdot \overline{13} = \overline{1}$  e  $\frac{\overline{6}}{\overline{6}} = \overline{6} \cdot \overline{3} = \overline{1}$  e pertanto si ha  $\overline{8} \cdot \overline{6} = \overline{12} \cdot \overline{4} = \overline{14}$ . Ma si ha anche che  $\overline{8} \cdot \overline{13} = \overline{12} \cdot \overline{3} = \overline{2}$  da cui semplificando  $\overline{2} \cdot \overline{6} \cdot \overline{4} = \overline{14}$

(4.9) ► Disegnare il grafico dell'applicazione  $\varphi = x^2 : \mathbb{Z} \rightarrow \mathbb{Z}_8$  in modo che essa sia un isomorfismo.

(La funzione è discreta e quindi i segmenti che uniscono i punti hanno un valore esclusivamente decorativo).



(4.10) ► Mostrare che in  $\mathbb{Z}_8$  è possibile mandare  $\frac{14}{7} = 2 \rightarrow \overline{2}$  ma non  $\frac{8}{4} \rightarrow \overline{2}$

La dimostrazione consiste semplicemente nel rilevare che  $\overline{7}_i = \overline{7}$  esiste ed è un inverso banale e che  $\overline{4}_i = ?$  non esiste. Così come anche  $\frac{20}{5} = 4 \rightarrow \overline{5}$  ma non  $\frac{8}{2} = 4 \rightarrow ?$ .

Rileggendo quanto scritto in “Algebra delle classi di resto 1” è evidente che gli elementi di  $\mathbb{Z}_8$  o non hanno inversi o li hanno banali. Ciò accade anche per altri anelli,  $\mathbb{Z}_4$  ad esempio, ma non per tutti gli anelli con l'indice  $n$  di  $\mathbb{Z}$  non primo. In generale se  $n$  non è primo avranno inversi quegli elementi dell'anello che non sono divisori dello zero. Vedere a tal proposito l'esercizio (4.18).

(4.11) ► Mandare in  $\mathbb{Z}_{13}$  il determinante  $\begin{vmatrix} 47 & 21 \\ -5 & 8 \end{vmatrix} = 481$

$\begin{vmatrix} \overline{8} & \overline{8} \\ \overline{8} & \overline{8} \end{vmatrix} = \overline{12} + \overline{1} = \overline{0}$  ed infatti  $13 \mid 481$

(4.12) ► Mandare in  $\mathbb{Z}_6$  il prodotto  $\begin{pmatrix} 2 & 7 \\ -4 & -1 \end{pmatrix} \cdot \begin{pmatrix} -5 & 0 \\ 3 & 11 \end{pmatrix} = \begin{pmatrix} 11 & 77 \\ 17 & -11 \end{pmatrix}$

$\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{2} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{3} & \overline{5} \end{pmatrix} = \begin{pmatrix} \overline{2} + \overline{3} & \overline{0} + \overline{5} \\ \overline{2} + \overline{3} & \overline{0} + \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{5} & \overline{5} \\ \overline{5} & \overline{1} \end{pmatrix}$  ed infatti  $\begin{pmatrix} 11 & 77 \\ 17 & -11 \end{pmatrix} \rightarrow \begin{pmatrix} \overline{5} & \overline{5} \\ \overline{5} & \overline{1} \end{pmatrix}$

(4.13) ► In  $F_{11}$  trovare le soluzioni dell'equazione di 2° grado  $\overline{2}\overline{x}^2 + \overline{4}\overline{x} - \overline{6} = \overline{0}$

$$\overline{x}_{1,2} = \frac{\overline{7} \pm \sqrt{\overline{5} + \overline{4}}}{\overline{2} \cdot \overline{2}} \Rightarrow \overline{x}_1 = \frac{\overline{7} + \overline{3}}{\overline{4}} = \overline{10} \cdot \overline{3} = \overline{8}, \overline{x}_2 = \frac{\overline{7} - \overline{3}}{\overline{4}} = \overline{4} \cdot \overline{3} = \overline{1}$$

Infatti le soluzioni di  $2x^2 + 4x - 6 = 0$  sono  $x_{1,2} = -3, 1 \rightarrow \overline{8}, \overline{1}$

(4.14) ► In  $F_5$  trovare le soluzioni del sistema lineare 
$$\begin{cases} \overline{3}\overline{x} - \overline{y} = \overline{1} \\ \overline{2}\overline{x} + \overline{3}\overline{y} = \overline{3} \end{cases}$$

$$\overline{x} = [\overline{1} + \overline{y}] \cdot \overline{2} = \overline{2} + \overline{2}\overline{y}$$

$$\overline{2} \cdot [\overline{2} + \overline{2}\overline{y}] + \overline{3}\overline{y} = \overline{4} + \overline{2}\overline{y} \Rightarrow \overline{y} = \overline{4} \cdot \overline{3} = \overline{2}$$

$$x = \overline{2} + \overline{2} \cdot \overline{2} = \overline{1}$$

Infatti le soluzioni di 
$$\begin{cases} 3x - y = 1 \\ 2x + 3y = 8 \end{cases}$$
 sono  $x = 1 \rightarrow \overline{1}, y = 2 \rightarrow \overline{2}$

(4.15) ► Stabilire per il sistema dell'esercizio precedente se la soluzione è unica.

$$\begin{vmatrix} \overline{3} & \overline{4} \\ \overline{2} & \overline{3} \end{vmatrix} = \overline{4} + \overline{2} = \overline{1} \neq \overline{0} \text{ quindi il sistema ha soluzione unica.}$$

Allora possiamo adoperare la regola di Cramer per trovare questa soluzione:

$$\overline{x}, \overline{y} = \frac{\begin{vmatrix} \overline{1} & \overline{4} \\ \overline{8} & \overline{3} \end{vmatrix}}{\begin{vmatrix} \overline{3} & \overline{4} \\ \overline{2} & \overline{3} \end{vmatrix}}, \frac{\begin{vmatrix} \overline{3} & \overline{1} \\ \overline{2} & \overline{8} \end{vmatrix}}{\begin{vmatrix} \overline{3} & \overline{4} \\ \overline{2} & \overline{3} \end{vmatrix}} = \frac{\overline{1}}{\overline{1}}, \frac{\overline{2}}{\overline{1}} = \overline{1} \cdot \overline{1}, \overline{2} \cdot \overline{1} = \overline{1}, \overline{2}$$

(4.16) ► Trovare in  $F_3$  le soluzioni dell'equazione di quarto grado  $\overline{2}_i \overline{x}^4 - \overline{1} = -\overline{2}_i \overline{x}^4$

$\overline{x}^4 = \overline{1} \cdot \overline{4}_i = \overline{1} \cdot \overline{4} = \overline{1}$ . La soluzione è unica perchè  $\overline{1}$  è un inverso banale.

Infatti, le soluzioni di  $\frac{x^4}{2} - 250 = 6 - \frac{x^4}{2}$  sono  $\pm 4 \rightarrow \overline{1}, \overline{1} \Rightarrow \overline{1}$

(4.17) ► Mostrare come in  $F_3$  le soluzioni  $\pm 4$  dell'equazione  $x^4 - 7x^2 - 144 = 0$  vadano in  $\overline{1}$

$x^4 - 7x^2 - 144 = 0 \rightarrow \overline{x}^4 - \overline{x}^2 = \overline{0}$  da cui la soluzione unica  $\overline{1} = \overline{1}$ .

(4.18) ► Risolvere in  $F_9$  il sistema simmetrico 
$$\begin{cases} \overline{xy} = \overline{6} \\ \overline{x} + \overline{y} = \overline{5} \end{cases}$$

$$\overline{t}^2 - \overline{5}\overline{t} + \overline{6} = \overline{0} \Rightarrow \overline{t}_{1,2} = (\overline{5} \pm \overline{1}) \cdot \overline{2}_i = (\overline{5} \pm \overline{1}) \cdot \overline{5} = (\overline{3}, \overline{2}) \Rightarrow \overline{x}_{1,2} = (\overline{3}, \overline{2}), \overline{x}_{3,4} = (\overline{2}, \overline{3})$$

Infatti il sistema 
$$\begin{cases} xy = 6 \\ x + y = -5 \end{cases}$$
 ha soluzioni  $x_{1,2} = (3, 2), x_{3,4} = (2, 3)$

Si noti che l'indice dell'anello non è primo; ciò nonostante esiste l'inverso di  $\bar{2}$  perchè non è divisore dello zero. Infatti non esiste alcun elemento  $\bar{a} \neq \bar{0}$  di  $F_9$  tale che  $\bar{2} \cdot \bar{a} = \bar{0}$ , cioè tale che trasformi  $\bar{2}$  in un multiplo di  $\bar{9}$ , perchè  $(9, 2) = 1$ .

(4.19) ► Risolvere in  $F_5$  l'equazione irrazionale  $\sqrt{\bar{x} - \bar{2}} = \bar{x} - \bar{8}$

$$x + 3 = x^2 + 4 + 1x \Rightarrow x^2 + 4 + 2 = 0 \Rightarrow x^2 = 1$$

Infatti l'equazione  $\sqrt{x - 2} = x - 8$  ha come radice  $11 \rightarrow 1$

(4.20) ► Mandare in  $F_7$  ciò che segue:  $x^2 + x - 6 = (x + 3)(x - 2) = 0 \Rightarrow x_{1,2} = (2, -3)$

$$\bar{x}^2 + \bar{x} + \bar{1} = (\bar{x} + \bar{3})(\bar{x} + \bar{5}) = \bar{0}$$

$$\bar{x}_{1,2} = \frac{\bar{6} \mp \sqrt{\bar{1} + \bar{3}}}{\bar{2}} = (\bar{6} \mp \bar{2}) \cdot \bar{4} = (\bar{2}, \bar{4})$$

Infatti  $x_{1,2} = (2, -3) \Rightarrow \bar{x}_{1,2} = (\bar{2}, \bar{4})$

(4.21) ► Mandare in  $F_{11}$  ciò che segue:  $x^3 - 2x^2 - x + 2 = 0 \Rightarrow x_{1,2,3} = (1, 2, -1)$

Possiamo utilizzare la regola di Ruffini per ridurre il grado dell'equazione

$$\bar{x}^3 + \bar{9}\bar{x}^2 + \bar{10}\bar{x} + \bar{2} = \bar{0}$$

Una soluzione dell'equazione è  $\bar{x}_1 = 1$  e quindi applicando Ruffini si ha

$$\begin{array}{r|rrrr} \bar{1} & \bar{9} & \bar{10} & \bar{2} & \\ \bar{1} & \bar{1} & \bar{10} & \bar{9} & \\ \hline \bar{1} & \bar{10} & \bar{9} & \bar{0} & \end{array}$$

da cui  $(\bar{x} + \bar{10})(\bar{x}^2 + \bar{10}\bar{x} + \bar{9}) = \bar{0}$

Le altre due soluzioni sono date da  $\bar{x}_{2,3} = (\bar{1} \pm \sqrt{\bar{1} + \bar{8}}) \cdot \bar{6} = (\bar{2}, \bar{10})$

Infatti  $x_{1,2,3} = (1, 2, -1) \Rightarrow \bar{x}_{1,2,3} = (\bar{1}, \bar{2}, \bar{10})$

Naturalmente, per la risoluzione di questa equazione come delle altre è applicata la condizione che il discriminante sia un quadrato perfetto e che le soluzioni siano esprimibili come rapporti tra interi nei quali il denominatore divide il numeratore.

Leonardo Calconi  
[leo@4dmatrix.it](mailto:leo@4dmatrix.it)  
 15/06/2007

Una versione aggiornata e corretta potrebbe essere disponibile all'indirizzo:  
[www.4dmatrix.it/math](http://www.4dmatrix.it/math)