Anelli, domini d'integrità e campi.

di Antonino Giambò

1. Riprendo un precedente articolo (*Strutture algebriche "rare"*) al fine di approfondire alcune questioni riguardanti gli anelli.

In quell'articolo ho accennato alle difficoltà di trovare anelli non commutativi. In questo ne propongo uno in particolare, che dovrebbe dare la misura di quelle difficoltà.

L'articolo, comunque, ha come scopo preminente quello di evidenziare il legame che sussiste fra anello, dominio d'integrità e campo, e per questo c'è una breve dissertazione su un settore della Matematica che si presta allo scopo: l'aritmetica modulare.

Conclude l'articolo una nota sulla vita di Emmy Noether, la geniale matematica che fondamentali contributi ha dato allo sviluppo dell'algebra moderna. La nota aggiunge qualcosa a quanto pubblicato da Emilio Ambrisi su questa stessa rubrica il 9 settembre u. s..

Ripropongo per prima cosa la definizione di anello.

*Un **anello** è un insieme A di elementi con due operazioni, "$\perp$" e "$*$", tali che:*

- *la struttura* $(A, \perp)$ *è un gruppo commutativo* $\begin{cases} A \text{ è chiuso rispetto a } \perp \\ \perp \text{ è associativa} \\ A \text{ contiene l'elemento neutro rispetto a } \perp \\ \text{Ogni elemento di } A \text{ è simmetrizzabile rispetto a } \perp \\ \perp \text{ è commutativa} \end{cases}$
- *la struttura* $(A, *)$ *è un semigruppo* $\begin{cases} A \text{ è chiuso rispetto a } * \\ * \text{ è associativa} \end{cases}$
- *la seconda operazione,* $*$*, è distributiva rispetto alla prima,* $\perp$ *.*

In un anello, dunque, può mancare l'elemento neutro rispetto alla seconda operazione, nel qual caso gli elementi non sono simmetrizzabili rispetto a questa operazione. Ma tali elementi potrebbero essere non simmetrizzabili anche se l'anello contenesse l'elemento neutro rispetto alla seconda operazione.

Quando l'anello presenta l'elemento neutro rispetto alla seconda operazione, detto più comunemente *elemento unità*, allora si parla di *anello unitario*. La seconda operazione, poi, può essere commutativa: se così è, l'anello si dice *commutativo* o *abeliano*.

Qualche esempio per chiarire:

- La struttura $(\mathbb{Z}, +, \cdot)$, dove $\mathbb{Z}$ è l'insieme degli interi, è un anello commutativo e unitario (l'elemento neutro rispetto alla seconda operazione è il numero 1), ma gli elementi, fatta eccezione proprio per il numero 1, non sono simmetrizzabili rispetto a questa operazione.
- La struttura $(2\mathbb{Z}, +, \cdot)$, dove $2\mathbb{Z}$ è l'insieme degli interi pari, è un anello commutativo non unitario.
- La struttura $(\mathrm{M}, +, \times)$, dove M è l'insieme delle matrici quadrate (per esempio del secondo ordine), con coefficienti nell'insieme dei numeri interi, è un anello non commutativo ma unitario, ma i suoi elementi non sono simmetrizzabili rispetto alla seconda operazione.
- Se M è invece l'insieme delle matrici quadrate (per esempio del secondo ordine), con elementi nell'insieme degli interi pari, la struttura $(\mathrm{M}, +, \times)$ è ancora un anello non commutativo ma non è unitario, per cui neppure adesso gli elementi sono simmetrizzabili rispetto alla seconda operazione.

2. Solitamente, l'elemento neutro di un anello rispetto alla prima operazione si denomina 0 e può accadere che esistano nell'anello coppie di elementi x, y diversi da 0, tali però che risulti $x * y = 0$. Due elementi siffatti si dicono *divisori dello zero*.

Ora, **se nell'anello non vi sono divisori dello 0**, vale a dire se:

$$x * y = 0 \;\Rightarrow\; (x = 0 \vee y = 0),$$

allora l'anello è denominato ***anello integro*** (o ***anello d'integrità***).

- Per esempio, riprendiamo l'insieme $2\mathbb{Z}$ dei numeri interi pari. Ebbene, la struttura algebrica $(2\mathbb{Z}, +, \cdot)$ è un anello integro ed è anche commutativo.

- Riprendiamo invece, come controesempio, l'insieme M delle matrici quadrate del secondo ordine con coefficienti in $\mathbb{Z}$: la struttura $(M, +, \times)$ è ancora un anello, come già detto, ma non è un anello integro, poiché vi sono dei divisori dello 0. In realtà, ci sono infiniti divisori dello zero nella struttura. Presi infatti due qualsiasi numeri interi a, b, non contemporaneamente nulli, si ha:

$$\begin{Vmatrix} 6\,a & 12\,a \\ 2\,b & 4\,b \end{Vmatrix} \times \begin{Vmatrix} 4 & -8 \\ -2 & 4 \end{Vmatrix} = \begin{Vmatrix} 24\,a - 24\,a & -48\,a + 48\,a \\ 8\,b - 8\,b & -16\,b + 16\,b \end{Vmatrix} = \begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix}.$$

E si capisce che, al variare di a, b si ottengono infiniti divisori dello zero.

- Fermiamo adesso l'attenzione sulla ricerca di un anello integro che sia non commutativo.

Questa ricerca, come si costaterà, conduce ad un risultato non certamente intuitivo e dà la misura delle difficoltà cui si va incontro nella ricerca di tali anelli.

Consideriamo allora l'insieme F [x,y] delle funzioni f(x,y) tali che risulti:

$$f[x,y] = p[x,y] \cdot x + q[x,y] \cdot y,$$

dove p [x,y] e q [x,y] sono polinomi nelle indeterminate x, y con coefficienti interi e termini noti uguali a 0, nei quali polinomi però sia $x \cdot y \neq y \cdot x$.

Ebbene, la struttura algebrica $(F[x,y], +, \cdot)$ soddisfa a tutti gli assiomi che ne fanno un anello integro non commutativo.

La precedente affermazione, non essendo propriamente intuitiva, richiede una spiegazione.

Dobbiamo dunque far vedere anzitutto che le due operazioni "+" e "·" sono operazioni interne all'insieme F [x,y] e poi che la struttura $(F[x,y], +)$ è un gruppo commutativo, che la struttura $(F[x,y], \cdot)$ è un semigruppo non commutativo, che la seconda operazione è distributiva rispetto alla prima e infine che non ci sono divisori dello 0.

Incominciamo a verificare che l'operazione "+" è un'operazione interna all'insieme F [x,y].

Presi al riguardo due qualsiasi funzioni:

$$f_1[x,y] = p_1[x,y] \cdot x + q_1[x,y] \cdot y\,, \quad f_2[x,y] = p_2[x,y] \cdot x + q_2[x,y] \cdot y\,,$$

si ha:

$$f_1[x,y] + f_2[x,y] = \{p_1[x,y] \cdot x + q_1[x,y] \cdot y\} + \{p_2[x,y] \cdot x + q_2[x,y] \cdot y\} =$$
$$= (p_1[x,y] + p_2[x,y]) \cdot x + \{q_1[x,y] + q_2[x,y]\} \cdot y = p[x,y] \cdot x + q[x,y] \cdot y,$$

avendo posto: $p[x,y] = p_1[x,y] + p_2[x,y]$ e $q[x,y] = q_1[x,y] + q_2[x,y]$ ed essendo consapevoli che la somma di due polinomi in x, y e un polinomio nelle stesse indeterminate.

Avendo capito, a questo punto, come si possa procedere, risulta abbastanza semplice spiegare che la struttura $(F[x,y], +)$ è un gruppo commutativo, ossia che la somma è associativa e commutativa, che esiste l'elemento neutro (è il polinomio nullo 0, che può immaginarsi nella forma $0 \cdot x + 0 \cdot y$) e che di ogni funzione f [x,y] esiste la funzione simmetrica rispetto all'operazione "+" (è la funzione –f [x,y]).

Verifichiamo adesso che l'operazione "·" è un'operazione interna alla struttura F [x,y].

Presi al riguardo due qualsiasi funzioni:

$$f_1[x,y] = p_1[x,y] \cdot x + q_1[x,y] \cdot y\,, \quad f_2[x,y] = p_2[x,y] \cdot x + q_2[x,y] \cdot y\,,$$

si ha:

$$f_1[x,y] + f_2[x,y] = \{p_1[x,y] \cdot x + q_1[x,y] \cdot y\} \cdot \{p_2[x,y] \cdot x + q_2[x,y] \cdot y\} =$$
$$= p_1[x,y] \cdot p_2[x,y] \cdot x^2 + p_1[x,y] \cdot q_2[x,y] \cdot x \cdot y + q_1[x,y] \cdot p_2[x,y] \cdot y \cdot x + q_1[x,y] \cdot q_2[x,y] \cdot y^2 =$$
$$= \{p_1[x,y] \cdot p_2[x,y] \cdot x + q_1[x,y] \cdot p_2[x,y] \cdot y\} \cdot x + \{p_1[x,y] \cdot q_2[x,y] \cdot x + q_1[x,y] \cdot q_2[x,y] \cdot y\} \cdot y =$$
$$= p[x,y] \cdot x + q[x,y] \cdot y,$$

avendo posto:

$$p[x,y] = p_1[x,y] \cdot p_2[x,y] \cdot x + q_1[x,y] \cdot p_2[x,y] \cdot y\,,$$
$$q[x,y] = p_1[x,y] \cdot q_2[x,y] \cdot x + q_1[x,y] \cdot q_2[x,y] \cdot y\,.$$

Anche adesso, avendo capito come procedere, ma con un po' più di fatica rispetto a prima, si può verificare che la struttura $(F[x,y], \cdot)$ è un semigruppo non commutativo, vale a dire che il prodotto è associativo ma non commutativo (questo per avere ipotizzato che sia $x \cdot y \neq y \cdot x$).

Bisogna ancora verificare che il prodotto è distributivo rispetto alla somma e siccome non è commutativo, bisogna verificare che lo è sia a destra sia a sinistra. Il procedimento si sviluppa più o meno come sopra, ma è piuttosto noioso.

Che non esistano divisori dello 0 in F[x,y] è semplice da capire, dal momento che il prodotto di due polinomi con termini noti nulli giammai può essere il polinomio 0.

3. Riprendiamo i due modelli di anello integro riportati sopra. In alcuno di essi esiste l'elemento neutro rispetto alla seconda operazione, per cui nessuno di essi è un anello unitario. Spieghiamolo:

- L'elemento neutro non esiste nell'anello degli interi pari poiché dovrebbe essere il numero 1, che però non è pari e quindi non appartiene all'insieme $2\mathbb{Z}$.
- Non esiste nell'insieme F [x,y] poiché dovrebbe essere il polinomio 1, che però è un polinomio con termine noto non nullo e quindi non appartenente all'insieme F [x,y].

Se tuttavia l'anello integro è un anello unitario e se inoltre la seconda operazione è commutativa, insomma se la struttura $(A, *)$ è un monoide unitario commutativo, allora l'anello è denominato più propriamente ***dominio d'integrità***.

Riepiloghiamo.

*Un **dominio d'integrità** è un insieme A di elementi con due operazioni, "$\perp$" e "$*$", tali che:*

- *A è chiuso rispetto ad entrambe le operazioni;*
- *la struttura $(A, \perp)$ è un gruppo commutativo;*
- *la struttura $(A, *)$ è un monoide unitario commutativo;*
- *la seconda operazione, "$*$", è distributiva rispetto alla prima;*
- *non ci sono divisori dello 0.*

Per esempio, è un dominio d'integrità la struttura algebrica $(\mathbb{Z}, +, \cdot)$, dove $\mathbb{Z}$ è l'insieme dei numeri interi. Infatti valgono tutti gli assiomi che caratterizzano questa tipologia di struttura e, in particolare, non ci sono divisori dello 0 dal momento che il prodotto di due interi è 0 se e solo se almeno uno di essi è 0. Si tratta, fra l'altro, di un dominio d'integrità in senso stretto, nel senso cioè che non è un campo giacché la struttura $(\mathbb{Z}_0, \cdot)$ non è un gruppo.

Per capire meglio quest'ultima affermazione, osserviamo che anche la struttura algebrica $(\mathbb{Q}, +, \cdot)$, dove $\mathbb{Q}$ è l'insieme dei numeri razionali, è un dominio d'integrità, ma non lo è in senso stretto, essendo per l'appunto un campo.

Anche la struttura algebrica $(\mathbb{Z}[x], +, \cdot)$, dove $\mathbb{Z}[x]$ indica l'insieme dei polinomi nell'indeterminata x, con coefficienti nell'insieme $\mathbb{Z}$ degli interi, è un dominio d'integrità in senso stretto.

Così come è un dominio d'integrità in senso stretto la struttura $(J, +, \cdot)$, dove J è l'insieme di numeri reali aventi la forma $a+b\sqrt{2}$, essendo a, b numeri interi.

4. Devo riprendere adesso un argomento, anch'esso affrontato nell'articolo succitato per un approfondimento, ancorché limitato a ciò che è funzionale al presente articolo.

Siano allora a, b due numeri interi qualsiasi e sia m un qualunque numero naturale non nullo. Il numero a si dice *congruo* di b rispetto al *modulo* m se esiste un intero k tale che:

$$a - b = k\,m\,.$$

Si scrive:

$$a \equiv b \pmod{m} \quad \text{o anche} \quad a \equiv_m b$$

e si legge: «a è congruo di b rispetto al modulo m».

Per esempio: 7 è congruo di 4 rispetto al modulo 3; 2 è congruo di 10 rispetto al modulo 4.

Vale il seguente teorema.

TEOREMA. **Dati i numeri interi a, b, e il numero naturale m non nullo, risulta $a \equiv_m b$ se e solo se a, b, divisi per m, danno lo stesso resto**.

DIMOSTRAZIONE. Se a, b, divisi per m, danno lo stesso resto r, indicati con p, q i rispettivi quozienti, si ha: $a=pm+r$ e $b=qm+r$, da cui segue facilmente: $a-b=km$, dove $k=p-q$. Perciò; $a \equiv_m b$.

Se, viceversa, $a \equiv_m b$, dividendo a, b per m, e indicando con q_1, q_2 i relativi quozienti e con r_1, r_2 i relativi resti, si ha: $a=mq_1+r_1$, $b=mq_2+r_2$, da cui segue:

$$a - b = m\,(q_1 - q_2) + (r_1 - r_2).$$

Siccome, per essere $a \equiv_m b$, risulta $a-b=km$, dove k è un intero, allora la precedente relazione implica la seguente uguaglianza:

$$m\,[k-(q_1-q_2)]=r_1-r_2.$$

In base alla quale si deve concludere che m divide r_1-r_2. Questo, dal momento che r_1 e r_2 sono entrambi minori di m, può accadere solo se $r_1-r_2=0$, ossia se $r_1=r_2$.

La teoria che si occupa in maniera completa di questa questione è conosciuta come ***aritmetica modulare***.

Fu creata dal matematico tedesco C. F. Gauss (1777-1855), il quale ne trattò diffusamente nella sua opera *Disquisitiones Arthmeticae* (1801), precisamente nelle sezioni I e II.

Ha interessanti applicazioni non solo nella teoria dei numeri ma anche in altri campi, come, tanto per fare un esempio, la sicurezza di Internet.

La relazione "$\Re$", definita nell'insieme $\mathbb{Z}$ dei numeri interi, tale che:

$$a\ \Re\ b \text{ se e solo se } a \equiv b \pmod m$$

si chiama relazione di *congruenza* rispetto al modulo m.

Si dimostra facilmente che essa è riflessiva, simmetrica e transitiva; è pertanto una relazione di equivalenza.

Di conseguenza, opera una partizione dell'insieme $\mathbb{Z}$ in m classi di equivalenza, ciascuna delle quali è formata da tutti i numeri interi congrui fra loro rispetto al modulo m.

Poiché ogni classe di equivalenza può essere rappresentata da un suo qualsiasi elemento, possiamo scegliere come rappresentati delle m classi l'insieme di numeri $0, 1, 2, \ldots, m-2, m-1$.

Cosicché, indicato con la scrittura $\mathbb{Z}_{/m}$ tale insieme, detto ***insieme delle classi di resto modulo m***, si ha:

$$\mathbb{Z}_{/m}=\{\,[0],\ [1],\ [2],\ \ldots,\ [m-1]\,\},$$

oppure, scrivendo per comodità gli elementi di tale insieme senza le parentesi:

$$\mathbb{Z}_{/m}=\{\,0,\ 1,\ 2,\ \ldots,\ m-1\,\}.$$

In figura (figura 1) è sintetizzata la procedura su descritta, quantunque riferita al caso particolare m=3.

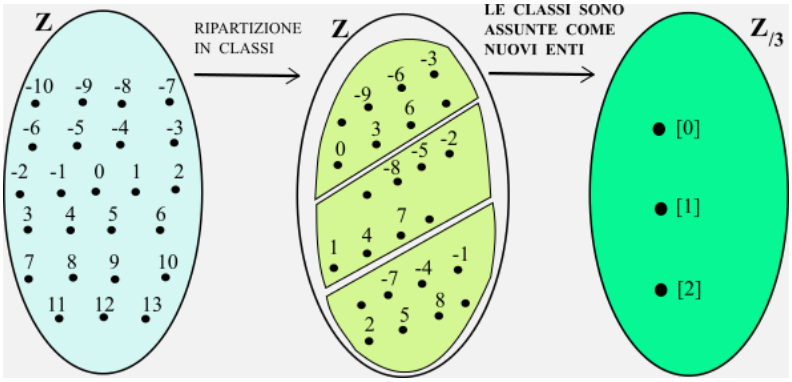

figura 1

Per un generico m lo schema che evidenzia le m classi di equivalenza può essere rappresentato come nella tabella sottostante (tabella 1).

[0]	[1]	[2]	.....	[m – 2]	[m – 1]
.....	.....	.....	.....	.....	.....
– 2 m	– 2 m + 1	– 2 m + 2	.....	– m – 2	– m – 1
– m	– m + 1	– m + 2	.....	– 2	– 1
0	**1**	**2**	**.....**	**m – 2**	**m – 1**
m	m + 1	m + 2	.....	2 m – 2	2 m – 1
2 m	2 m + 1	2 m + 2	.....	3 m – 2	3 m – 1
.....	.....	.....	.....	.....	.....

tabella 1

Nell'insieme $\mathbb{Z}_{/m}$ si possono introdurre due operazioni, che chiamiamo "addizione cerchiata" e "moltiplicazione cerchiata", indicate rispettivamente con i simboli "$\oplus$" e "$\odot$" tali che:

$$a \oplus b = a + b\,, \quad a \odot b = a \cdot b\,.$$

Naturalmente, ogni volta che $a + b$ o $a \cdot b$ sono maggiori di m, si prende il resto della divisione di tali numeri per m.

Per esempio:

- nell'insieme $\mathbb{Z}_{/3}$: $2 \oplus 1 = 0$, $2 \odot 2 = 1$;
- nell'insieme $\mathbb{Z}_{/6}$: $5 \oplus 4 = 3$, $3 \odot 4 = 0$.

Le due operazioni, per il modo stesso in cui sono state definite, godono delle medesime proprietà di cui godono le corrispondenti operazioni in $\mathbb{Z}$, vale a dire che sono commutative, associative e rispetto a ciascuna di esse l'insieme $\mathbb{Z}_{/m}$ ammette l'elemento neutro, che è evidentemente 0 per l'operazione "$\oplus$" e 1 per l'operazione "$\oplus$".

Ma tali operazioni godono anche di altre proprietà.

Infatti, ogni elemento dell'insieme $\mathbb{Z}_{/m}$ non solo ammette il simmetrico rispetto a "$\oplus$", come accade anche nell'insieme $\mathbb{Z}$ e come mostra un'apposita tabella (tabella 2) ancorché costruita per m=5; ma, diversamente da ciò che accade nell'insieme $\mathbb{Z}$, può ammettere l'inverso anche rispetto alla seconda operazione.

Precisamente, per quanto riguarda l'operazione "$\odot$", ogni elemento dell'insieme $\mathbb{Z}_{/m}-\{0\}$ ammette il simmetrico rispetto ad essa se e solo se il numero m è un numero primo (tab 3b – dove m=5), mentre se m è un numero composto questo simmetrico può esistere oppure no (tab. 3a – dove m=4).

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

tabella 2

$\odot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

(a)

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(b)

tabella 3

Con riferimento alla tabella 3a, possiamo constatare poi che si ha $2 \odot 2 = 0$, per cui esistono divisori dello 0.

La tabella 3b mostra invece che in questo caso non esistono divisori dello 0.

Ebbene, **in ogni struttura $(\mathbb{Z}_{/m}, \oplus, \odot)$ esistono divisori dello 0 se m è un numero composto, non ne esistono se m è un numero primo.**

Cosicché, nel primo caso la struttura è un anello unitario commutativo ma non è un dominio d'integrità; nel secondo caso è un dominio d'integrità, ma non lo è in senso stretto. Infatti si può verificare facilmente che in questo caso la struttura è un campo.

In realtà, quando l'insieme sostegno è un insieme finito, non esiste un dominio d'integrità che lo sia in senso stretto, dal momento che è sempre e comunque un campo. Vale, infatti, il seguente teorema.

TEOREMA (di Wedderburn [1]). **Ogni dominio d'integrità finito è un campo**.

DIMOSTRAZIONE. Esistono dimostrazioni sofisticate che presuppongono proprietà iniettive e monomorfismi, ma io ne voglio proporre una, diciamo, terra terra.

Per dimostrare che il dominio d'integrità $(A, \perp, *)$ è un campo, bisogna dimostrare semplicemente che ogni elemento di A, fatta eccezione per l'elemento neutro e_1 rispetto alla prima operazione, è simmetrizzabile rispetto alla seconda operazione.

In altri termini, preso un qualunque $x \in A$, con $x \neq e_1$, bisogna dimostrare che esiste in A l'elemento y tale che $x * y = y * x = e_2$, essendo e_2 l'elemento neutro rispetto alla seconda operazione.

Supponiamo che sia $A = \{a_1, a_2, a_3, \ldots, a_n\}$ l'insieme sostegno della struttura. Preso uno qualsiasi degli elementi di A, che indichiamo con x, componiamo questo elemento con ciascuno degli n elementi di A (è indifferente che la composizione sia fatta a sinistra o a destra, dal momento che l'operazione è commutativa). Otteniamo i seguenti valori:

---

1 Wedderburn, Joseph Henry MacLagan, matematico scozzese, 1882-1948.

$$a_1 * x,\ \ a_2 * x,\ \ a_3 * x,\ \ \ldots\ , a_n * x.$$

Essi sono ovviamente distinti l'uno dagli altri, per cui, considerato che l'operazione "$*$" è ovunque definita in A, tali elementi sono, a parte l'ordine, gli stessi n elementi dell'insieme A.

D'altro canto, c'è nell'insieme A l'elemento neutro e_2 rispetto all'operazione "$*$". Questo significa che uno dei precedenti valori deve essere uguale ad e_2. Poniamo che questo valore sia $a_k * x$. Deve essere dunque: $a_k * x = e_2$.

Siccome poi l'operazione è commutativa, si ha: $a_k * x = x * a_k = e_2$. Cosicché a_k è il simmetrico di x rispetto all'operazione "$*$".

Dal momento che x è stato scelto in maniera del tutto arbitraria, possiamo concludere che ogni elemento di A è simmetrizzabile rispetto all'operazione "$*$". [c.v.d]

5. Ancora una considerazione relativamente alla struttura di campo.

Sappiamo [2] che la struttura $(M_r, +, \times)$, dove M_r è l'insieme delle matrici quadrate regolari (per esempio di ordine 2), con coefficienti in $\mathbb{Q}$, è un corpo non commutativo e perciò non è un campo.

Così come è un corpo non commutativo, e dunque non è un campo, la struttura $(H, +, \cdot)$, dove H è l'insieme dei quaternioni di Hamilton, con coefficienti in $\mathbb{R}$.

Costatiamo però un fatto significativo: entrambi gli insiemi sostegno di queste due strutture sono infiniti.

E questa precisazione non è superflua, poiché in effetti non esiste un corpo finito che sia non commutativo. Vale infatti il seguente teorema, anch'esso solitamente attribuito a Wedderburn.

TEOREMA. **Ogni corpo finito è commutativo (e perciò è un campo).**

La dimostrazione di questo teorema è alquanto complessa, per cui la ometto. Chi volesse comunque prenderne visione lo può fare consultando l'opera [1, pag. 27].

La stessa dimostrazione, in [1], è preceduta da alcune riflessioni di carattere storico che riporto integralmente (le notizie biografiche in nota sono opera mia):

« Questo splendido teorema, generalmente attribuito a MacLagan Wedderburn, è stato dimostrato da diverse persone usando approcci assai diversi. Lo stesso Wedderburn fornì tre dimostrazioni nel 1905 ed un'altra dimostrazione fu data da Leonard E. Dickson [3] nello stesso anno. Altre dimostrazioni furono date in seguito da Emil Artin [4], Hans Zassenhaus [5], Nicolas Bourbaki [6], e molti altri. C'è una dimostrazione che si distingue tuttavia per semplicità ed eleganza. Fu trovata da Ernst Witt [7] nel 1931 e combina due idee elementari per estrarne una brillante conclusione. »

Ed è questa dimostrazione che gli autori dell'opera [1] riportano.

6. Mi piace concludere questo contributo con qualche curiosità riguardante la vita di una delle più brillanti menti matematiche, la tedesca Emmy Noether (1882-1935), che allo studio degli anelli non commutativi ha dedicato parte della sua vita e ne ha fatto uno dei settori di studio più importanti dell'algebra moderna.

Amalie Emmy Noether nacque a Erlangen, cittadina tedesca situata a pochi chilometri a nord di Norimberga, e nella cui Università suo padre, Max (1844-1921), era stimato professore ordinario di Matematica, una delle figure preminenti nella geometria algebrica del suo tempo. In quella università insegnava anche Felix Klein (1849-1925), il quale, peraltro, l'aveva resa famosa con la presentazione, nel 1872, del celebre *Programma di Erlangen*.

Emmy cominciò a frequentare l'Università di Erlangen all'età di 18 anni, ma, siccome le donne non vi erano ammesse, non lo poté fare da studentessa ma da semplice uditrice. Dopo un paio d'anni si trasferì all'Università di

---

2 Cfr.: articolo *Strutture algebriche "rare"*, già citato.

3 Dickson, Leonard Eugene, matematico statunitense, 1874-1954.

4 Artin, Emil, matematico austriaco, 1898-1962.

5 Zassenhaus, Hans Julius, matematico tedesco, 1912-1991.

6 Nicolas Bourbaki, eteronimo con cui si firma un gruppo di matematici, per lo più francesi, autori di importanti opere matematiche composte fra la prima e la seconda metà del Novecento. Fra i bourbakisti più illustri si segnalano André Weil (1906-1998) e Jean Dieudonné (1906-1992).

7 Ernst Witt, matematico tedesco, 1911-1991.

Gottinga, dove seguì le lezioni di David Hilbert 1862-1943) e Felix Klein. Quando, nel 1904, la legge tedesca cambiò e le donne furono ammesse alla regolare frequenza di corsi universitari, Emmy tornò ad Erlangen, dove poté laurearsi in matematica nell'anno 1907. Ad Erlangen lavorò all'Istituto di Matematica per 7 anni, fino al 1915, ma senza ricevere alcun compenso.

Nel 1915 fu di nuovo invitata a Gottinga da Hilbert e Klein, i quali si adoperarono inutilmente per farla ammettere all'esame di abilitazione, il cosiddetto *Privatdozent*, che le avrebbe consentito di ricoprire una cattedra universitaria. Si era in piena guerra (la Prima Guerra Mondiale) e coloro che, nel Senato Accademico, si opponevano così commentavano:

> « *Che cosa penseranno i soldati del proprio Paese quando, ritornando a casa, vedranno che tutti si aspettano che essi imparino ai piedi di una donna?* »

La risposta di Hilbert fu piuttosto caustica:

> « *Non vedo come il sesso di una candidata possa essere il requisito per la sua ammissione come Privatdozent. In fondo l'Università non è uno stabilimento balneare* ».

Per capire la frase di Hilbert, bisogna sapere che a quell'epoca negli stabilimenti balneari donne e uomini erano separati.

Comunque, al momento non ci fu nulla da fare, ma Emmy, pur non essendo stata assunta dall'Università, tenne conferenze a nome di Hilbert e come sua collaboratrice. Fino a che, nel 1919, a guerra finita, le fu concesso di abilitarsi e di insediarsi all'Università di Gottinga. Continuò però ad insegnare senza essere pagata fino al 1923, quando fu assunta, con una piccola retribuzione, come "docente associata non ufficiale". Aveva superato i 40 anni e, nonostante si fosse segnalata come una matematica di primo livello, conosciuta e stimata in tutto il mondo accademico per i suoi lavori originali e innovativi, non riuscì ad ottenere una cattedra.

Tanto per dire, la sua fama era tale che nel 1908 fu invitata a far parte del Circolo Matematico di Palermo, che a quell'epoca era il principale punto di riferimento della comunità matematica internazionale; nel 1909 fu invitata a far parte dell'Associazione dei Matematici Tedeschi; addirittura nel 1932 fu invitata a tenere una conferenza generale al Congresso Internazionale di Matematica, svoltosi a Zurigo: prima donna a ricevere questo importantissimo invito [8].

Con la salita al potere dei nazisti [9], i quali le impedirono di insegnare in quanto ebrea, Emmy nel 1933 fu costretta ad abbandonare Gottinga. Si stabilì negli USA, al *Bryan Mawr College* [10], dove ottenne un posto d'insegnante. In seguito fu invitata a tenere lezioni anche all'*Institute for Advanced Study* di Princeton.

I principali contributi di Emmy Noether alla matematica riguardano in parte la fisica teorica, dove stabilì importanti connessioni fra leggi di conservazione e simmetria, ma soprattutto l'algebra moderna. Ella fece di questa branca della matematica una disciplina fondamentale, tanto che Emmy Noether è considerata "la madre dell'algebra moderna". Così perlomeno la definì il matematico canadese naturalizzato statunitense Irving Kaplansky (1917-2006).

In particolare, i suoi studi sugli anelli risalgono al periodo che va dal 1920 al 1926. Ma è tra il 1933 e il 1935 che Emmy concentra la sua attenzione nello studio degli anelli non commutativi.

Il suo lavoro sulla teoria degli invarianti ebbe un ruolo significativo nella teoria della relatività di Einstein.

---

8 Una seconda donna solo nel 1990, 58 anni dopo, avrebbe avuto questo stesso onore. Si tratta di Karen Uhlenbeck (n. 1942), originaria di Cleveland (Ohio, USA), invitata al Congresso di Kyoto, in Giappone.

9 L'ascesa al potere dei nazisti depauperò l'Università di Gottinga, dalla quale furono scacciati, nel 1933, professori e studenti ebrei o sospettati di essere tali. Fra loro: Max Born (1882-1970) e Richard Courant (1888-1972). In questo modo, fu distrutto in un amen, tutto ciò che era stato costruito in tanti anni di duro lavoro, con il contributo di matematici del calibro di Gauss, Dirichlet, Riemann, Hilbert, Klein.
«*Come va la matematica a Gottinga, ora che è stata liberata dall'influenza ebrea*?» pare che abbia chiesto ad Hilbert il Ministro dell'Educazione durante un congresso di autorità tedesche svoltosi nel 1934.
Questa fu la risposta di un amareggiato Hilbert: «*Matematica a Gottinga? Veramente, non esiste più*».

10 Il *Bryn Mawr College*, nello stato della Pennsylvania, è un college privato femminile, fondato dai quaccheri nel 1885. È una delle prime istituzioni statunitensi create per l'istruzione superiore delle donne. In questa istituzione aveva insegnato anche, fin dalla sua fondazione, dapprima come professore associato e poi come professore ordinario, un'altra matematica europea alla quale era inibito l'insegnamento in patria e che per questo si era trasferita negli USA: Charlotte Angas Scott (1858-1931), la prima donna inglese ad ottenere una laurea (1882). Fu tra i fondatori della *American Mathematical Society* ed editrice della rivista *American Journal of Mathematics.*

Pochi giorni dopo la sua morte, avvenuta quando aveva appena 53 anni per complicazioni postoperatorie, il *New York Times* pubblicava un necrologio scritto proprio da Albert Einstein (1879-1955), in cui si potevano leggere queste parole:

> « *Nel giudizio dei matematici più competenti, la signorina Noether era il più significativo e creativo genio matematico apparso finora da quando è iniziata l'educazione universitaria delle donne* …»

Emmy ispirava simpatia per la sua cordialità e disponibilità. Non era una bella donna, era sovrappeso, vestiva fuori moda e non si curava minimamente di mostrare la sua femminilità, non le interessava proprio.

Offensivo e volgare, oltre che falso, fu il commento del matematico tedesco Hermann Weyl (1885-1955), non tanto su di lei a dire il vero, quanto soprattutto sulla connazionale Sonia (o Sofia) Kovalevskaja (1850-1891) e, più in generale, sul ruolo delle donne in matematica:

> « *Ci sono state solo due donne matematiche nella storia: Sofia Kovalevskaja e Emmy Noether: la prima non era una matematica, la seconda non era una donna* .»

Ma quel commento, che certamente era offensivo nei confronti della Kovalevskaja, forse, riguardo Emmy, voleva essere un complimento, anche se goffo, almeno a mio parere. Di fatto, lo stesso Weil, durante una cerimonia religiosa in memoria della Noether, tenutasi una quindicina di giorni dopo la sua morte, pronunciò un discorso elogiativo molto commovente.

Il matematico e statistico statunitense Norbert Wiener (1894-1964), padre della cibernetica, diede di Emmy Noether le seguenti definizioni:

> « *Uno dei dieci o dodici matematici più importanti di questa generazione in tutto il mondo* .»
> « *La più grande donna matematica che sia mai vissuta.* »

BIBLIOGRAFIA**.**

[1] Martin Aigner – Günter M. Ziegler, *Proofs from THE BOOK*, Edizione italiana a cura di Alfio Quarteroni, Milano, Springer, 2006.

[2] Eric T. Bell, *I grandi matematici*, Biblioteca Sansoni, Firenze, 1966.

[3] Armando Chiellini – Roberto Giannarelli, *L'esame orale di matematica nei concorsi a cattedre di scuole secondarie*, Roma, Libreria Eredi Virgilio Veschi, 1962, pagg. 96-102.

[4] Raúl Ibañez Torres, *L'origine dell'algebra astratta*: *Cayley*, Collana "Geni della Matematica", RBA Italia, Milano, 2017

[5] A. J. Lopez Moreno, *La creazione dell'algebra astratta*: *Noether*, Collana "Geni della Matematica", RBA Italia, Milano, 2017.

[6] John Yarnelle, *Strutture matematiche finite*, Collana "Parlando di matematica", Milano, Progresso Tecnico Editoriale, 1967.