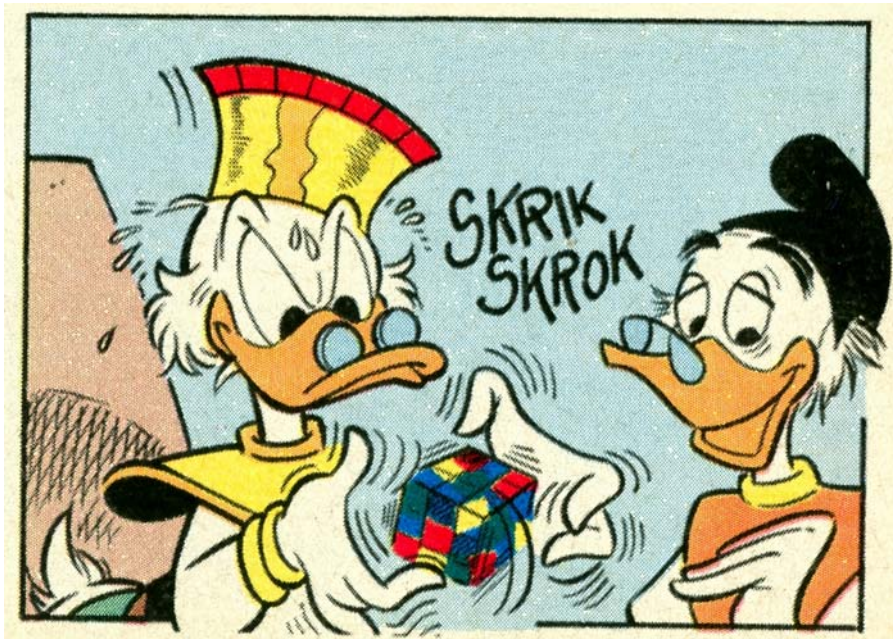


Marco Barlotti

Appunti di
Teoria dei Gruppi
per il corso di laurea triennale in
Matematica

Vers. 2.0
Anno Accademico 2008-2009



In copertina una vignetta (© Disney) di Giuseppe Dalla Santa tratta da I TL 1800-A “Il cubo di Paperubik”.

PERCHE' QUESTI APPUNTI, E COME USARLI

(Prefazione alla vers. 2.0)

Questi appunti nascono come supporto alle lezioni che tengo per l'insegnamento di "Teoria dei Grafi e Applicazioni" per il Corso di Laurea Triennale in Matematica presso la Facoltà di Scienze Matematiche, Fisiche e Naturali all'Università di Firenze, con riferimento a quella parte dell'insegnamento che riguarda le nozioni fondamentali di Teoria dei Gruppi.

Si tratta di una revisione della prima stesura, mirata a rendere il programma del tutto indipendente da quello di Algebra 1 (in particolare, è stata aggiunta una sezione sulla definizione di anello e sugli anelli delle classi di resto). Restano ancora lacune significative (ad esempio, sono quasi del tutto assenti gli esercizi e manca la parte relativa ai gruppi di permutazioni). L'esposizione comunque rispecchia abbastanza fedelmente l'itinerario che mi propongo di percorrere a lezione, e il contenuto di queste pagine dovrebbe essere quasi sufficiente per una buona preparazione relativamente alla prima metà dell'insegnamento.

È certamente inevitabile la presenza di errori materiali; sarò come sempre grato a tutti coloro, e specialmente agli studenti, che vorranno segnalarmi qualunque problema, dai più banali errori di stampa alle oscurità nell'esposizione.

Firenze, 3.11.2008

Marco Barlotti

BIBLIOGRAFIA

- [1] P. R. Halmos
Naive set theory
Van Nostrand, Princeton NJ (1966)

- [2] P. R. Halmos
Teoria elementare degli insiemi
Feltrinelli, Milano (1970)

AVVERTENZA

Tutti i diritti di questa pubblicazione sono dell'autore.

È consentita la riproduzione integrale di questa pubblicazione a titolo gratuito.

È altresì consentita a titolo gratuito l'utilizzazione di parti di questa pubblicazione in altra opera all'inderogabile condizione che ne venga citata la provenienza e che della nuova opera nella sua interezza vengano consentite la riproduzione integrale a titolo gratuito e l'utilizzazione di parti a queste stesse condizioni.

L'uso di questa pubblicazione in qualsiasi forma comporta l'accettazione integrale e senza riserve di quanto sopra.

SOMMARIO

0. - Prerequisiti

0.1 - Che cosa c'è in questo capitolo.	pag.	1
0.2 - Il linguaggio degli insiemi	pag.	1
0.3 - n -ple ordinate. Matrici	pag.	3
0.4 - Relazioni. Funzioni	pag.	5
0.5 - Composizione di funzioni.	pag.	7
0.6 - Cardinalità	pag.	7
0.7 - Relazioni di equivalenza	pag.	8
0.8 - Le classi di resto	pag.	10

1. - Operazioni in un insieme

1.1 - Operazioni in un insieme	pag.	12
1.2 - Chiusura rispetto a un'operazione	pag.	14
1.3 - Associatività e commutatività	pag.	15
1.4 - Elemento neutro	pag.	16
1.5 - Il simmetrico di un elemento	pag.	17
1.6 - La rappresentazione tabulare di un'operazione	pag.	18

2. - Semigrupperi, monoidi, gruppi, anelli

2.1 - Semigrupperi	pag.	20
2.2 - Sottosemigrupperi	pag.	21
2.3 - Omomorfismi e isomorfismi tra semigrupperi.	pag.	22
2.4 - Monoidi	pag.	23
2.5 - Sottomonoidi	pag.	24
2.6 - Omomorfismi e isomorfismi tra monoidi.	pag.	26
2.7 - Gruppi	pag.	27
2.8 - Sottogruppi	pag.	29
2.9 - Omomorfismi e isomorfismi tra gruppi	pag.	29
2.10 - Anelli	pag.	30
2.11 - Omomorfismi e isomorfismi tra anelli	pag.	33
2.12 - L'anello \mathbb{Z}_n	pag.	33
2.13 - I criteri di divisibilità per i numeri interi	pag.	36

3. - Prime proprietà dei gruppi

3.1 - Notazioni	pag. 39
3.2 - Le "leggi di cancellazione"	pag. 40
3.3 - Potenze di un elemento.	pag. 40
3.4 - Ancora sui sottogruppi	pag. 42
3.5 - Gruppi ciclici e loro proprietà	pag. 44

4. - Normalità

4.1 - Classi laterali.	pag. 49
4.2 - Applicazione ai gruppi finiti.	pag. 52
4.3 - Sottogruppi normali	pag. 53
4.4 - Gruppo quoziente	pag. 55
4.5 - Normalizzante	pag. 56
4.6 - Centralizzante di un sottogruppo. Centro di un gruppo	pag. 57
4.7 - Il coniugio. Automorfismi interni.	pag. 59

5. - I teoremi di omomorfismo

5.1 - Nucleo di un omomorfismo	pag. 61
5.2 - Il primo teorema di omomorfismo fra gruppi	pag. 62
5.3 - Il teorema di corrispondenza.	pag. 64
5.4 - Prodotto di sottogruppi	pag. 65
5.5 - Il secondo teorema di omomorfismo fra gruppi	pag. 67
5.6 - Il gruppo degli automorfismi di un gruppo. Il sg degli automorfismi interni	pag. 67

6. - Prodotto diretto di gruppi

6.1 - Definizione e prime proprietà	pag. 69
6.2 - Prodotto diretto di sottogruppi	pag. 71

7. - Azioni di un gruppo su un insieme

7.1 - Definizione e prime proprietà	pag. 73
7.2 - Orbite. Transitività	pag. 74
7.3 - Stabilizzatore.	pag. 75
7.4 - Il caso finito: l'equazione delle orbite	pag. 77
7.5 - Applicazione allo studio dei p -gruppi finiti	pag. 79

8. - I teoremi di Sylow

8.1 - Due lemmi numerici.	pag. 81
8.2 - Il teorema principale.	pag. 83
8.3 - Sottogruppi di Sylow.	pag. 85

0.- PREREQUISITI

0.1 - Che cosa c'è in questo capitolo.

Questo capitolo raccoglie brevemente alcune nozioni che supponiamo note dagli studi precedenti, con lo scopo essenziale di fissare con chiarezza le notazioni adottate.

0.2 - Il linguaggio degli insiemi.

Usiamo la parola “*insieme*” per indicare un ente completamente caratterizzato dagli *elementi* che ad esso *appartengono*, senza però definire i termini “*insieme*”, “*elemento*” e “*appartenere*”. Il lettore interessato a una formalizzazione assiomatica della teoria degli insiemi può consultare utilmente [1], se necessario nella traduzione italiana [2]. Per sgombrare il campo da possibili fraintendimenti, chiariamo subito che

- si usa il termine “elemento” per indicare ciò che “appartiene” ad un “insieme”, senza che ciò prefiguri due mondi distinti, quello degli “elementi” e quello degli “insiemi”: anzi, gli elementi di un insieme possono benissimo essere essi stessi insiemi;
- poiché un insieme resta completamente caratterizzato dai propri elementi, si conviene in particolare che: due insiemi sono lo stesso insieme (si dice anche che *coincidono*) se e solo se hanno gli stessi elementi.

Indichiamo con \emptyset l'*insieme vuoto*, cioè l'unico insieme che non ha elementi.

Siano **A**, **B** insiemi.

Se **a** è un elemento di **A** (ciò si esprime anche dicendo che **a appartiene** ad **A**), scriveremo

$$\mathbf{a} \in \mathbf{A}.$$

Se ogni elemento di **A** è anche elemento di **B**, diremo che **A** è un *sottoinsieme* di **B** (oppure che è *incluso*, o *contenuto* in **B**) e scriveremo

$$\mathbf{A} \subset \mathbf{B}.$$

Se $\mathbf{A} \subset \mathbf{B}$ e $\mathbf{B} \subset \mathbf{A}$, cioè se **A** e **B** hanno gli stessi elementi, **A** e **B** sono lo stesso insieme e scriveremo

$$\mathbf{A} = \mathbf{B}$$

(osserviamo qui esplicitamente che intenderemo sempre l'uguaglianza nel senso “leibniziano” di *identità*).

In generale, se si deve provare che $\mathbf{A} = \mathbf{B}$, il procedimento migliore è appunto quello di mostrare che $\mathbf{A} \subset \mathbf{B}$ e $\mathbf{B} \subset \mathbf{A}$.

Le scritture

$$\mathbf{a} \notin \mathbf{A}, \mathbf{A} \not\subset \mathbf{B}, \mathbf{A} \neq \mathbf{B}$$

indicano la negazione rispettivamente di $\mathbf{a} \in \mathbf{A}$, $\mathbf{A} \subset \mathbf{B}$ e $\mathbf{A} = \mathbf{B}$ (cioè significano rispettivamente: \mathbf{a} non è un elemento di \mathbf{A} , \mathbf{A} non è un sottoinsieme di \mathbf{B} , \mathbf{A} e \mathbf{B} non sono lo stesso insieme; quest'ultimo fatto si esprime anche dicendo che \mathbf{A} e \mathbf{B} sono *diversi* o *distinti*).

Se $\mathbf{A} \subset \mathbf{B}$ e $\mathbf{A} \neq \mathbf{B}$ (ciò si esprime dicendo che \mathbf{A} è *incluso propriamente* in \mathbf{B} , oppure che \mathbf{A} è un *sottoinsieme proprio* di \mathbf{B}), scriveremo anche

$$\mathbf{A} \subsetneq \mathbf{B}.$$

Se $\mathbf{p}(x)$ è una proposizione aperta con variabile libera x su \mathbf{A} , scriviamo

$$\mathbf{A}_1 = \{x \in \mathbf{A} / \mathbf{p}(x)\}$$

(e leggiamo: \mathbf{A}_1 è l'insieme degli x appartenenti a \mathbf{A} tali che $\mathbf{p}(x)$) per indicare il sottoinsieme di \mathbf{A} formato da tutti e soli gli elementi $\mathbf{a} \in \mathbf{A}$ per i quali $\mathbf{p}(\mathbf{a})$ è vera.

L'insieme i cui elementi sono tutti (e soli) i sottoinsiemi di \mathbf{A} si indica con $\mathcal{P}(\mathbf{A})$ e si dice *insieme delle parti* di \mathbf{A} .

Si dice *unione* di \mathbf{A} e \mathbf{B} , e si indica con $\mathbf{A} \cup \mathbf{B}$, l'insieme i cui elementi sono tutti e soli gli elementi di \mathbf{A} e gli elementi di \mathbf{B} .

Si dice *intersezione* di \mathbf{A} e \mathbf{B} , e si indica con $\mathbf{A} \cap \mathbf{B}$, l'insieme degli elementi di \mathbf{A} che appartengono anche a \mathbf{B} , cioè: $\mathbf{A} \cap \mathbf{B} = \{x \in \mathbf{A} / x \in \mathbf{B}\}$.

Se $\mathbf{A} \cap \mathbf{B} = \emptyset$, \mathbf{A} e \mathbf{B} si dicono *disgiunti*.

Si dice *differenza* di \mathbf{A} e \mathbf{B} , e si indica con $\mathbf{A} \setminus \mathbf{B}$, l'insieme degli elementi di \mathbf{A} che non appartengono a \mathbf{B} , cioè: $\mathbf{A} \setminus \mathbf{B} = \{x \in \mathbf{A} / x \notin \mathbf{B}\}$.

Se $\mathbf{B} \subset \mathbf{A}$, l'insieme $\mathbf{A} \setminus \mathbf{B}$ viene detto anche *complementare* di \mathbf{B} in \mathbf{A} , ed è indicato (purché tale notazione non dia luogo ad equivoci) con \mathbf{B}^c .

Un insieme di insiemi si dice anche *una famiglia* di insiemi. Le nozioni di "unione" e "intersezione" si estendono alle famiglie di insiemi: se \mathcal{F} è una famiglia di insiemi, si dice *unione* di \mathcal{F} e si indica con

$$\bigcup_{\mathbf{X} \in \mathcal{F}} \mathbf{X}$$

l'insieme di tutti e soli gli elementi che appartengono ad almeno un elemento di \mathcal{F} ; si dice *intersezione* di \mathcal{F} e si indica con

$$\bigcap_{\mathbf{X} \in \mathcal{F}} \mathbf{X}$$

l'insieme di tutti e soli gli elementi che appartengono a tutti gli elementi di \mathcal{F} .

Si dice *partizione* di \mathbf{A} una famiglia di sottoinsiemi non vuoti di \mathbf{A} a due a due disgiunti la cui unione è \mathbf{A} .

Sia \mathcal{F} una famiglia di sottoinsiemi non vuoti di \mathbf{A} a due a due disgiunti. Un *insieme di rappresentanti* per \mathcal{F} è un sottoinsieme \mathbf{A}^* di \mathbf{A} tale che ogni elemento di \mathbf{A}^* appartiene a un (e, ovviamente, un solo) elemento di \mathcal{F} e per ogni $\mathbf{A}_i \in \mathcal{F}$ esiste uno e un solo $a_i \in \mathbf{A}^*$ tale che $a_i \in \mathbf{A}_i$.

Supporremo noti, e utilizzeremo, i seguenti insiemi numerici: l'insieme \mathbb{N} dei numeri naturali (con le usuali nozioni di *somma, differenza, prodotto, divisione, minore, maggiore*); l'insieme \mathbb{Z} dei numeri interi (con le usuali nozioni di *somma, differenza, prodotto, divisione, minore, maggiore*) nel quale distinguiamo il sottoinsieme \mathbb{Z}^+ dei numeri interi positivi e il sottoinsieme \mathbb{Z}^- dei numeri interi negativi; l'insieme \mathbb{Q} dei numeri razionali (con le usuali nozioni di *somma, differenza, prodotto, divisione, minore, maggiore*) nel quale distinguiamo il sottoinsieme \mathbb{Q}^+ dei numeri razionali positivi e il sottoinsieme \mathbb{Q}^- dei numeri razionali negativi; l'insieme \mathbb{R} dei numeri reali (con le usuali nozioni di *somma, differenza, prodotto, divisione, minore, maggiore*) nel quale distinguiamo il sottoinsieme \mathbb{R}^+ dei numeri reali positivi e il sottoinsieme \mathbb{R}^- dei numeri reali negativi; l'insieme \mathbb{C} dei numeri complessi (con le usuali nozioni di *somma, differenza, prodotto, divisione*).

Come è usuale, identificheremo $\mathbb{Z}^+ \cup \{0\}$ con \mathbb{N} . Analogamente, identificheremo \mathbb{Z} con un opportuno sottoinsieme di \mathbb{Q} , \mathbb{Q} con un opportuno sottoinsieme di \mathbb{R} e \mathbb{R} con un opportuno sottoinsieme di \mathbb{C} . Ci sentiremo pertanto liberi di scrivere

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Osservazione 0.2.1

Comunque presi $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$, restano univocamente determinati due numeri interi q, r tali che

$$a = bq + r \quad \text{e} \quad 0 \leq r < b.$$

Essi si dicono rispettivamente *quoziente* e *resto* della *divisione euclidea* di a per b .

Osservazione 0.2.2

Siano $a, d \in \mathbb{Z}^+$; se il resto della divisione euclidea di a per d è 0 (zero), si dice che d è un *divisore* di a (oppure che d *divide* a , o anche che a è *multiplo* di d).

Siano $a, b \in \mathbb{Z}^+$; si dice *massimo comun divisore* di a e b un numero intero positivo d_0 tale che

- d_0 divide a e b ;

- ogni numero intero positivo che divide sia a che b divide anche d_0 .

Il massimo comun divisore di a e b si indica con $\text{MCD}(a, b)$ o anche, quando non vi sia rischio di equivoci, semplicemente con (a, b) .

Si dimostra senza difficoltà che, detto r il resto della divisione euclidea di a per d , ogni numero che divida sia a che b divide anche r e, viceversa, ogni numero che divida sia b che r divide anche a ; pertanto $\text{MCD}(a, b) = \text{MCD}(b, r)$. È poi chiaro che $\text{MCD}(a, b) = b$ se e soltanto se b divide a . Da queste considerazioni segue subito l'algoritmo detto "delle divisioni successive", che non solo dimostra l'esistenza del massimo comun divisore fra due qualsiasi numeri interi positivi a e b ma costituisce anche il metodo più efficiente per calcolarlo:

ripeti

sia r il resto della divisione euclidea di a per b ;

indica con a il numero che era indicato con b ;

indica con b il numero che era indicato con r

finché $b = 0$;

il numero che a questo punto è indicato con a è il massimo comun divisore cercato.

Poiché il resto è sempre strettamente minore del divisore, il numero indicato con b nell'algoritmo delle divisioni successive diminuisce ad ogni divisione, quindi in un numero finito di passi deve raggiungere zero: questo prova la convergenza dell'algoritmo e l'esistenza del massimo comun divisore di due qualsiasi numeri interi positivi.

0.3 - n -ple ordinate. Matrici.

Siano \mathbf{A} , \mathbf{B} insiemi.

Se $a \in \mathbf{A}$ e $b \in \mathbf{B}$, l'insieme $\{a, \{a, b\}\}$ si dice *coppia ordinata con prima componente a e seconda componente b* , e si indica con (a, b) . Nel seguito per lo più non ci servirà la definizione rigorosa di "coppia ordinata" ma sarà sufficiente tener presente che essa è caratterizzata non solo dai suoi elementi ma anche dall'ordine in cui si considerano: dunque

- se $a, a' \in \mathbf{A}$ e $b, b' \in \mathbf{B}$, si ha $(a, b) = (a', b')$ se e solo se $a = a'$ e $b = b'$;

in particolare:

- se $a \neq b$, si ha sempre $(a, b) \neq (b, a)$.

L'insieme di tutte le coppie ordinate (a, b) con $a \in \mathbf{A}$ e $b \in \mathbf{B}$ si dice *prodotto cartesiano* di \mathbf{A} per \mathbf{B} e si indica con $\mathbf{A} \times \mathbf{B}$.

Analogamente, si può considerare un ente caratterizzato da 3, 4, ..., n elementi (detti *componenti*), e dall'ordine in cui questi vengono considerati: si parla rispettivamente di *terna ordinata*, *quaterna ordinata*, ..., *n -pla ordinata*. Ad esempio, siano dati tre insiemi \mathbf{A}_1 , \mathbf{A}_2 , \mathbf{A}_3 e siano $a_1 \in \mathbf{A}_1$, $a_2 \in \mathbf{A}_2$, $a_3 \in \mathbf{A}_3$: la terna ordinata individuata da a_1, a_2, a_3 (in questo ordine) si indica con (a_1, a_2, a_3) e non è altro che l'elemento $((a_1, a_2), a_3)$ dell'insieme $(\mathbf{A}_1 \times \mathbf{A}_2) \times \mathbf{A}_3$ (che, per semplicità, si indica a sua volta con $\mathbf{A}_1 \times \mathbf{A}_2 \times \mathbf{A}_3$).

Particolare importanza rivestirà per noi il caso delle n -ple ordinate di elementi di uno stesso insieme \mathbf{A} (l'insieme di tali n -ple si indica con \mathbf{A}^n).

Sia \mathbf{A} un insieme, e siano m, n numeri interi positivi. Si dice *matrice* $m \times n$ a elementi in \mathbf{A} una m -pla ordinata di n -ple ordinate di elementi di \mathbf{A} , ossia un elemento di $(\mathbf{A}^n)^m$. Una matrice $m \times n$ potrebbe essere identificata con una mn -pla ordinata; in pratica, quando si parla di matrice gli elementi vengono scritti in una "tabella"

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}$$

nella quale si evidenziano le n -ple ordinate $(a_{1,1}, a_{1,2}, \dots, a_{1,n}), \dots, (a_{2,1}, a_{2,2}, \dots, a_{2,n}), \dots, (a_{m,1}, a_{m,2}, \dots, a_{m,n})$, dette *righe* della matrice, e le m -ple ordinate $(a_{1,1}, a_{2,1}, \dots, a_{m,1}), \dots, (a_{1,2}, a_{2,2}, \dots, a_{m,2}), \dots, (a_{1,n}, a_{2,n}, \dots, a_{m,n})$, dette *colonne* della matrice. Sinteticamente, la matrice di termine generico $a_{i,j}$ si indica con $(a_{i,j})$; le sue righe si indicano con $a_{1,*}, a_{2,*}, \dots, a_{m,*}$ e le sue colonne con $a_{*,1}, a_{*,2}, \dots, a_{*,n}$.

Se $m = n$ (cioè se il numero delle righe è uguale al numero delle colonne) una matrice $n \times n$ si dice *quadrata* (di ordine n). Una matrice quadrata di ordine n $(a_{i,j})$ si dice *simmetrica* se $a_{i,j} = a_{j,i}$ per ogni i, j in $\{1, \dots, n\}$.

L'insieme di tutte le matrici $m \times n$ a elementi in \mathbf{A} si indica con $\mathbf{A}^{m,n}$.

0.4 - Relazioni. Funzioni.

Siano \mathbf{A}, \mathbf{B} insiemi.

Si dice *relazione* tra \mathbf{A} e \mathbf{B} un sottoinsieme del prodotto cartesiano $\mathbf{A} \times \mathbf{B}$. Intuitivamente, una relazione tra \mathbf{A} e \mathbf{B} è una "legge" che a ogni elemento di \mathbf{A} associa qualche elemento di \mathbf{B} (eventualmente nessuno).

Sia ρ una relazione tra \mathbf{A} e \mathbf{B} , cioè sia $\rho \subset \mathbf{A} \times \mathbf{B}$; se $(a, b) \in \rho$, si dice che gli elementi a (di \mathbf{A}) e b (di \mathbf{B}) sono in relazione (secondo ρ), e si scrive $a\rho b$. In pratica si usa sempre la notazione $a\rho b$ anziché $(a, b) \in \rho$.

Se ρ è una relazione tra \mathbf{A} e \mathbf{B} , si dice *relazione inversa* di ρ e si indica con ρ^{-1} la relazione tra \mathbf{B} e \mathbf{A} definita dalla condizione

$$b\rho^{-1}a \text{ se e soltanto se } a\rho b.$$

Si dice *funzione* (o *applicazione*) da \mathbf{A} in \mathbf{B} una relazione \mathbf{f} tra \mathbf{A} e \mathbf{B} tale che per ogni $a \in \mathbf{A}$ esiste esattamente un $b \in \mathbf{B}$ tale che $a\mathbf{f}b$, cioè tale che ogni elemento di \mathbf{A} è in relazione (secondo \mathbf{f}) con esattamente un elemento di \mathbf{B} . Ciò si esprime scrivendo

$$\mathbf{f}: \mathbf{A} \rightarrow \mathbf{B}.$$

Intuitivamente, una funzione da \mathbf{A} in \mathbf{B} è una "legge" che ad ogni elemento di \mathbf{A} associa uno e un solo elemento di \mathbf{B} .

L'insieme \mathbf{A} si dice *dominio* di \mathbf{f} .

Per ogni $a \in \mathbf{A}$, l'unico elemento b di \mathbf{B} tale che $a \mathbf{f} b$ si indica spesso con $\mathbf{f}(a)$; si dice che b *proviene* da a (o anche che b è l'*immagine* di a) mediante \mathbf{f} . In pratica non si usa mai la notazione $a \mathbf{f} b$ ma piuttosto si scrive $\mathbf{f}(a) = b$ come noi faremo in tutto il resto di questi appunti.

Se $\mathbf{A}_1 \subset \mathbf{A}$, si dice *immagine* di \mathbf{A}_1 (mediante \mathbf{f}) il sottoinsieme $\mathbf{f}(\mathbf{A}_1)$ di \mathbf{B} formato dalle immagini (mediante \mathbf{f}) degli elementi di \mathbf{A}_1 , cioè

$$\mathbf{f}(\mathbf{A}_1) = \{b \in \mathbf{B} / b = \mathbf{f}(a) \text{ per qualche } a \in \mathbf{A}_1\}.$$

L'immagine $\mathbf{f}(\mathbf{A})$ di \mathbf{A} si dice anche semplicemente *immagine* di \mathbf{f} .

Se $\mathbf{B}_1 \subset \mathbf{B}$, si dice *immagine inversa* di \mathbf{B}_1 (mediante \mathbf{f}) il sottoinsieme $\mathbf{f}^{-1}(\mathbf{B}_1)$ di \mathbf{A} formato dagli elementi le cui immagini (mediante \mathbf{f}) appartengono a \mathbf{B}_1 , cioè

$$\mathbf{f}^{-1}(\mathbf{B}_1) = \{a \in \mathbf{A} / \mathbf{f}(a) \in \mathbf{B}_1\}.$$

[Osservazione 0.4.1]

Sia \mathbf{A} un insieme, e sia \mathbf{f} una funzione con dominio \mathbf{A} . Per ogni sottoinsieme \mathbf{B}_1 di $\mathbf{f}(\mathbf{A})$, si ha

$$\mathbf{f}(\mathbf{f}^{-1}(\mathbf{B}_1)) = \mathbf{B}_1.$$

Se $\mathbf{f}(\mathbf{A}) = \mathbf{B}$ (ossia se per ogni $\mathbf{b} \in \mathbf{B}$ esiste almeno un $\mathbf{a} \in \mathbf{A}$ tale che $\mathbf{f}(\mathbf{a}) = \mathbf{b}$; cioè se ogni elemento di \mathbf{B} proviene mediante \mathbf{f} da almeno un elemento di \mathbf{A}), \mathbf{f} si dice *suriettiva*. In tal caso, si dice che \mathbf{f} è una funzione da \mathbf{A} su \mathbf{B} .

Se comunque presi $\mathbf{a}, \mathbf{a}' \in \mathcal{D}(\mathbf{f})$ con $\mathbf{a} \neq \mathbf{a}'$ è $\mathbf{f}(\mathbf{a}) \neq \mathbf{f}(\mathbf{a}')$ (ossia se comunque presi $\mathbf{a}, \mathbf{a}' \in \mathcal{D}(\mathbf{f})$ da $\mathbf{f}(\mathbf{a}) = \mathbf{f}(\mathbf{a}')$ segue $\mathbf{a} = \mathbf{a}'$; cioè se ogni elemento di \mathbf{B} proviene da al più un elemento di \mathbf{A}), \mathbf{f} si dice *iniettiva*.

Se \mathbf{f} è iniettiva e suriettiva si dice che \mathbf{f} è *biiettiva* (o anche che \mathbf{f} è una *biiezione*, o una *corrispondenza biunivoca tra \mathbf{A} e \mathbf{B}*). Una funzione iniettiva è sempre una corrispondenza biunivoca tra il proprio dominio e la propria immagine. Una corrispondenza biunivoca tra \mathbf{A} e \mathbf{A} si dice *permutazione* su \mathbf{A} .

Se $\mathbf{f} : \mathbf{A} \rightarrow \mathbf{B}$ è iniettiva, la relazione inversa \mathbf{f}^{-1} di \mathbf{f} è una funzione (necessariamente biiettiva) di $\mathbf{f}(\mathbf{A})$ su \mathbf{A} , che si dice *funzione inversa* di \mathbf{f} . Si noti che, se $\mathbf{B}_1 \subset \mathbf{f}(\mathbf{A})$, l'immagine di \mathbf{B}_1 mediante \mathbf{f}^{-1} coincide con l'immagine inversa di \mathbf{B}_1 mediante \mathbf{f} , e quindi non c'è ambiguità nella notazione $\mathbf{f}^{-1}(\mathbf{B}_1)$. Se \mathbf{f} è una corrispondenza biunivoca tra \mathbf{A} e \mathbf{B} , la sua inversa \mathbf{f}^{-1} è una corrispondenza biunivoca tra \mathbf{B} e \mathbf{A} . In particolare, l'inversa di una permutazione su \mathbf{A} è anch'essa una permutazione su \mathbf{A} .

Per ogni insieme \mathbf{A} , la funzione $\mathbf{id}_{\mathbf{A}} : \mathbf{A} \rightarrow \mathbf{A}$ che ad ogni elemento associa se stesso è una corrispondenza biunivoca detta *funzione identica* o anche *identità* di \mathbf{A} .

Sia \mathbf{f} una funzione da \mathbf{A} in \mathbf{A} . Un elemento a di \mathbf{A} si dice un *punto fisso* per \mathbf{f} se $\mathbf{f}(a) = a$. Ogni elemento di \mathbf{A} è un punto fisso per $\mathbf{id}_{\mathbf{A}}$.

Siano \mathbf{A} , \mathbf{B} insiemi, sia $\mathbf{f} : \mathbf{A} \rightarrow \mathbf{B}$ e sia $\mathbf{A}_1 \subset \mathbf{A}$. Si dice *restrizione* di \mathbf{f} ad \mathbf{A}_1 la funzione $\mathbf{f}|_{\mathbf{A}_1} : \mathbf{A}_1 \rightarrow \mathbf{B}$ così definita: $\mathbf{f}|_{\mathbf{A}_1} := \mathbf{f} \cap (\mathbf{A}_1 \times \mathbf{B})$ (si ricordi che \mathbf{f} è un sottoinsieme di $\mathbf{A} \times \mathbf{B}$). Questa definizione è molto "tecnica", perché nella sostanza $\mathbf{f}|_{\mathbf{A}_1}$ "opera" esattamente come \mathbf{f} (l'unica differenza è che "opera" solo su \mathbf{A}_1); certe proprietà possono però essere verificate da $\mathbf{f}|_{\mathbf{A}_1}$ e non da \mathbf{f} , e viceversa.

0.5 - Composizione di funzioni.

Siano \mathbf{A} , \mathbf{B} , \mathbf{C} insiemi, e siano $\mathbf{f} : \mathbf{A} \rightarrow \mathbf{B}$, $\mathbf{g} : \mathbf{B} \rightarrow \mathbf{C}$ funzioni.

Si dice *composizione* di \mathbf{f} con \mathbf{g} e si indica con $\mathbf{g} \circ \mathbf{f}$ (attenzione all'ordine in cui si scrivono \mathbf{f} e \mathbf{g} !) la funzione $\mathbf{A} \rightarrow \mathbf{C}$ definita ponendo

$$(\mathbf{g} \circ \mathbf{f})(a) := \mathbf{g}(\mathbf{f}(a)) \quad \forall a \in \mathbf{A}.$$

Osservazione 0.5.1

Siano \mathbf{A} , \mathbf{B} insiemi, sia $\mathbf{f} : \mathbf{A} \rightarrow \mathbf{B}$ iniettiva e sia $\mathbf{f}^{-1} : \mathbf{B} \rightarrow \mathbf{A}$ la funzione inversa di \mathbf{f} . Si ha

$$\mathbf{f}^{-1} \circ \mathbf{f} = \mathbf{id}_{\mathbf{A}} \quad \text{e} \quad \mathbf{f} \circ \mathbf{f}^{-1} = \mathbf{id}_{\mathbf{f}(\mathbf{A})}.$$

Osservazione 0.5.2

Siano \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{D} insiemi, e siano $\mathbf{f} : \mathbf{A} \rightarrow \mathbf{B}$, $\mathbf{g} : \mathbf{B} \rightarrow \mathbf{C}$, $\mathbf{h} : \mathbf{C} \rightarrow \mathbf{D}$ funzioni. Si ha

$$(\mathbf{h} \circ \mathbf{g}) \circ \mathbf{f} = \mathbf{h} \circ (\mathbf{g} \circ \mathbf{f}).$$

0.6 - Cardinalità.

Siano \mathbf{A} , \mathbf{B} insiemi. Si dice che \mathbf{A} e \mathbf{B} sono equipotenti se esiste una corrispondenza biunivoca tra \mathbf{A} e \mathbf{B} .

Per ogni $n \in \mathbb{N}$, sia $\mathbf{I}_n := \{x \in \mathbb{N} / 1 \leq x \leq n\}$.

Si dimostra che gli insiemi \mathbf{I}_n (al variare di $n \in \mathbb{N}$), \mathbb{N} e \mathbb{R} a due a due non sono equipotenti.

Sia \mathbf{A} un insieme.

Se esiste $n \in \mathbb{N}$ tale che \mathbf{A} è equipotente a \mathbf{I}_n , si dice che la cardinalità di \mathbf{A} è n e si scrive

$$|\mathbf{A}| = n.$$

In questo caso si dice anche che *il numero degli elementi di \mathbf{A} è n* .

Se \mathbf{A} è equipotente a \mathbb{N} , si dice che la cardinalità di \mathbf{A} è \aleph_0 (si legge: "aleph con zero") e si scrive

$$|\mathbf{A}| = \aleph_0.$$

In questo caso si dice anche che \mathbf{A} è *numerabile*.

Se \mathbf{A} è equipotente a \mathbb{R} , si dice che la cardinalità di \mathbf{A} è c e si scrive

$$|\mathbf{A}| = c.$$

In questo caso si dice anche che \mathbf{A} *ha la potenza del continuo*.

Notiamo esplicitamente che possono verificarsi infiniti altri casi, anche se quelli sopra considerati saranno sufficienti per i nostri scopi.

Sia \mathbf{A} un insieme.

Se esiste $n \in \mathbb{N}$ tale che $|\mathbf{A}| = n$, si dice che \mathbf{A} è un insieme finito; in caso contrario, si dice che \mathbf{A} è un insieme infinito (e la sua cardinalità può essere \aleph_0 , c oppure una delle infinite altre che non abbiamo considerato!).

0.7 - Relazioni di equivalenza.

Sia \mathbf{A} un insieme.

Si dice *relazione in \mathbf{A}* una relazione tra \mathbf{A} e \mathbf{A} (cioè un sottoinsieme del prodotto cartesiano $\mathbf{A} \times \mathbf{A}$).

Sia \sim una relazione in \mathbf{A} . Essa si dice *di equivalenza* se è

- *riflessiva*, cioè $a \sim a \quad \forall a \in \mathbf{A}$;
- *simmetrica*, cioè $a \sim b \Rightarrow b \sim a \quad \forall a, b \in \mathbf{A}$;
- *transitiva*, cioè $(a \sim b \wedge b \sim c) \Rightarrow (a \sim c) \quad \forall a, b, c \in \mathbf{A}$.

Sia \sim una relazione di equivalenza in \mathbf{A} . Se $a \in \mathbf{A}$, si dice *classe di equivalenza* di a (o anche, quando ciò non dia luogo ad equivoci, semplicemente *classe di equivalenza* di a) il sottoinsieme $[a]$ di \mathbf{A} definito come segue:

$$[a] = \{x \in \mathbf{A} / x \sim a\}.$$

Osservazione 0.7.1

Per ogni $a \in \mathbf{A}$, si ha $a \in [a]$.

Dimostrazione – Infatti $a \sim a$, perché \sim è riflessiva.

Osservazione 0.7.2

Comunque presi $a, b \in \mathbf{A}$, si ha $[a] = [b]$ se e solo se $a \sim b$.

Dimostrazione – Se $[a] = [b]$, poiché $a \in [a]$ (per l'osservazione 0.7.1) si ha $a \in [b]$ e dunque $a \sim b$ (per definizione di $[b]$).

Viceversa, sia $a \sim b$; dobbiamo provare che $[a] \subset [b]$ e che $[b] \subset [a]$.

Sia $x \in [a]$; allora $x \sim a$. Ma $a \sim b$ per ipotesi e dunque $x \sim b$ (perché \sim è transitiva), cioè $x \in [b]$. Per l'arbitrarietà di x in $[a]$, si è provato che $[a] \subset [b]$.

Sia ora $x \in [b]$; allora $x \sim b$. Poiché $b \sim a$ (essendo $a \sim b$ per ipotesi, ed essendo \sim simmetrica) e poiché \sim è transitiva, si ha $x \sim a$, cioè $x \in [a]$. Per l'arbitrarietà di x in $[b]$, si è così anche provato che $[b] \subset [a]$ e dunque che $[a] = [b]$.

Osservazione 0.7.3

Sia $a \in \mathbf{A}$. Per ogni $x \in [a]$, è $[x] = [a]$.

Dimostrazione – Per definizione di $[a]$, se $x \in [a]$ è $x \sim a$; dunque $[x] = [a]$ per l'osservazione 0.7.2.

Sia $a \in \mathbf{A}$. Per ogni $x \in [a]$, si dice che x *rappresenta* $[a]$, o anche che x è un *rappresentante* di $[a]$. Ciò è giustificato da quanto si è visto nell'osservazione 0.7.3.

Osservazione 0.7.4

Comunque presi $a, b \in \mathbf{A}$, se $[a] \neq [b]$ è $[a] \cap [b] = \emptyset$.

Dimostrazione – Sia $[a] \neq [b]$. Procediamo per assurdo, supponendo che esista $x \in [a] \cap [b]$. In tal caso $x \sim a$ (perché $x \in [a]$) e $x \sim b$ (perché $x \in [b]$); per l'osservazione 0.7.2 si ha allora $[a] = [x] = [b]$, contro l'ipotesi.

Osservazione 0.7.5

L'insieme delle classi di equivalenza di \mathbf{A} è una partizione di \mathbf{A} .

Dimostrazione – Le classi di equivalenza sono a due a due disgiunte per l'osservazione 0.7.4; per l'osservazione 0.7.1 esse sono non vuote e la loro unione è \mathbf{A} .

L'insieme delle classi di \sim – equivalenza di \mathbf{A} si dice *insieme quoziente* di \mathbf{A} rispetto a \sim , e si indica con $\frac{\mathbf{A}}{\sim}$. La funzione (suriettiva) $\pi: \mathbf{A} \rightarrow \frac{\mathbf{A}}{\sim}$ che ad ogni elemento di \mathbf{A} associa la sua classe di equivalenza si dice *proiezione canonica* di \mathbf{A} su $\frac{\mathbf{A}}{\sim}$.

0.8 - Le classi di resto.

In tutta la sezione 0.8 supporremo fissato un numero intero positivo n .

Siano $a, b \in \mathbb{Z}$; si dice che a è *congruo a b modulo n* e si scrive

$$a \equiv b \pmod{n}$$

sse $(\exists k \in \mathbb{Z})(a - b = kn)$, ossia sse $a - b$ è multiplo di n .

Si è così definita una relazione in \mathbb{Z} , detta "*congruenza modulo n* ". Tale relazione è stata studiata fin dall'antichità: sono celebri le opere in proposito del matematico ellenista Diofanto, vissuto nel terzo secolo d. C..

Teorema 0.8.1

La congruenza modulo n è una relazione di equivalenza in \mathbb{Z} .

Dimostrazione – In primo luogo, la congruenza modulo n è riflessiva, ossia

$$a \equiv a \pmod{n} \quad \text{per ogni } a \in \mathbb{Z}.$$

Infatti, $a - a = 0 \cdot n$ con $0 \in \mathbb{Z}$.

Inoltre, la congruenza modulo n è simmetrica: siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e proviamo che $b \equiv a \pmod{n}$. In effetti, se $a \equiv b \pmod{n}$ esiste $k \in \mathbb{Z}$ tale che $a - b = kn$; ma allora $b - a = (-k)n$ con $-k \in \mathbb{Z}$, e dunque $b \equiv a \pmod{n}$.

Infine, la congruenza modulo n è transitiva: siano $a, b, c \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, e proviamo che $a \equiv c \pmod{n}$. In effetti, se $a \equiv b \pmod{n}$ esiste $k_1 \in \mathbb{Z}$ tale che $a - b = k_1n$; se $b \equiv c \pmod{n}$ esiste $k_2 \in \mathbb{Z}$ tale che $b - c = k_2n$; ma allora

$$a - c = (a - b) + (b - c) = k_1n + k_2n = (k_1 + k_2) \cdot n$$

con $k_1 + k_2 \in \mathbb{Z}$, e dunque $a \equiv c \pmod{n}$.

Per quanto provato nel teorema 0.8.1, se $a \equiv b \pmod{n}$ si può dire che a, b sono *congrui modulo n* senza porre attenzione all'ordine in cui si citano a e b .

Esercizio 0.8.2

Trovare due numeri interi che sono congrui modulo 5 ma non sono congrui modulo 10. Esistono due numeri interi che siano congrui modulo 10 ma non siano congrui modulo 5?

Teorema 0.8.3

Sia $a \in \mathbb{Z}$, e sia r il resto della divisione euclidea di a per n . Allora $a \equiv r \pmod{n}$.

Dimostrazione – Per definizione di divisione euclidea (cfr. osservazione 0.2.1), esiste $q \in \mathbb{Z}$ tale che $a = qn + r$
e dunque $a - r = qn$ con $q \in \mathbb{Z}$, da cui l'asserto.

Le classi di equivalenza rispetto alla relazione di congruenza modulo n si dicono *classi di resto modulo n* . L'insieme delle classi di resto modulo n (cioè l'insieme quoziente di \mathbb{Z} rispetto alla relazione di congruenza modulo n) si indica con \mathbb{Z}_n .

Esercizio 0.8.4

Si deduca dal teorema 0.8.3 che due numeri interi a, b sono congrui modulo n se e solo se la divisione euclidea di a per n e la divisione euclidea di b per n danno lo stesso resto.

Teorema 0.8.5

L'insieme \mathbb{Z}_n ha n elementi, precisamente: $[0], [1], \dots, [n-1]$.

Dimostrazione – Per il teorema 0.8.3, ogni numero intero appartiene a una delle classi $[0], [1], \dots, [n-1]$. Resta da provare che tali classi sono tutte distinte.

Se fosse $[i] = [j]$ con $0 \leq i < j < n$, per l'osservazione 0.7.2 sarebbe $i \equiv j \pmod{n}$ ossia esisterebbe $k \in \mathbb{Z}$ tale che $j - i = kn$.

Ma $j - i > 0$ (perché $j > i$) e $j - i < n$ (perché $j < n$ e $i \geq 0$), dunque $j - i$ non può essere multiplo di n . Abbiamo così ottenuto una contraddizione; ne segue che le classi $[0], [1], \dots, [n-1]$ sono tutte distinte, come si voleva.

Esercizio 0.8.6

Si studi la congruenza modulo 1, la congruenza modulo 2, la congruenza modulo 3, la congruenza modulo 10, la congruenza modulo 12 e la congruenza modulo 24; in particolare, per ciascuna di tali relazioni si scrivano esplicitamente le classi di resto e si precisi come opera la proiezione canonica.

1.- OPERAZIONI IN UN INSIEME

1.1 - Operazioni in un insieme.

Sia \mathbf{A} un insieme non vuoto.

Si dice *operazione (binaria, interna)* in \mathbf{A} una funzione da $\mathbf{A} \times \mathbf{A}$ in \mathbf{A} (cioè, intuitivamente, una "legge" che ad ogni coppia ordinata di elementi di \mathbf{A} associa un elemento di \mathbf{A}).

Se \star è un'operazione in \mathbf{A} e $a, b \in \mathbf{A}$, scriviamo $a \star b$ anziché $\star(a, b)$: così

$$a \star b = c$$

significa che c è l'immagine di (a, b) mediante \star , ossia che \star associa alla coppia ordinata (a, b) di elementi di \mathbf{A} l'elemento c di \mathbf{A} .

Esempi

1.1.1 La somma e il prodotto sono operazioni in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.

1.1.2 Per ogni insieme \mathbf{A} , la composizione definita in 0.5 è un'operazione nell'insieme di tutte le funzioni $\mathbf{A} \rightarrow \mathbf{A}$.

1.1.3 Nell'insieme \mathbb{Z} , la sottrazione è un'operazione, la divisione non lo è.

1.1.4 Nell'insieme \mathbb{N} è un'operazione la \star definita come segue:

$$a \star b = a(b + 1) \quad \forall a, b \in \mathbb{N}.$$

1.1.5 Nell'insieme $\{a, b, c\}$ è un'operazione la \star definita come segue:

$$a \star a = a, a \star b = b, a \star c = c, b \star a = b, b \star b = a, b \star c = a, c \star a = c, c \star b = a, c \star c = b.$$

1.1.6 Sia \mathbf{A} un insieme. La funzione che a due sottoinsiemi di \mathbf{A} associa la loro unione è un'operazione in $\mathcal{P}(\mathbf{A})$ che si indica con \cup .

1.1.7 Sia \mathbf{A} un insieme. La funzione che a due sottoinsiemi di \mathbf{A} associa la loro intersezione è un'operazione in $\mathcal{P}(\mathbf{A})$ che si indica con \cap .

1.1.8 Sia n un numero intero positivo. Nell'insieme $\mathbb{Z}^{n,n}$ delle matrici quadrate $n \times n$ a elementi in \mathbb{Z} si definisce un'operazione \cdot (detta *prodotto righe per colonne*) come segue:

$$(a_{i,j}) \cdot (b_{i,j}) := \left(\sum_{k=1}^n a_{i,k} b_{k,j} \right).$$

Allo stesso modo si definisce il prodotto righe per colonne fra due elementi di $\mathbb{Q}^{n,n}$, fra due elementi di $\mathbb{R}^{n,n}$ o fra due elementi di $\mathbb{C}^{n,n}$. Di fatto, allo stesso modo si definisce il prodotto righe per colonne fra due elementi di $\mathbf{A}^{n,n}$ per qualsiasi anello \mathbf{A} (cfr. sez. 2.10).

Siano \mathbf{A} un insieme non vuoto e \star un'operazione in \mathbf{A} .

Se $a \in \mathbf{A}$ e $\mathbf{B} \subset \mathbf{A}$, si pone:

$$a \star \mathbf{B} := \{x \in \mathbf{A} / x = a \star b \text{ con } b \in \mathbf{B}\};$$

$$\mathbf{B} \star a := \{x \in \mathbf{A} / x = b \star a \text{ con } b \in \mathbf{B}\}.$$

Se $\mathbf{B}, \mathbf{C} \subset \mathbf{A}$, si pone

$$\mathbf{B} \star \mathbf{C} := \{x \in \mathbf{A} / x = b \star c \text{ con } b \in \mathbf{B} \text{ e } c \in \mathbf{C}\}.$$

Esempio 1.1.9

Sia $\mathbf{A} := \mathbb{N}$, e sia \cdot l'usuale prodotto fra numeri naturali. Se $n_0 \in \mathbb{N}$, per quanto sopra convenuto la scrittura $n_0 \cdot \mathbb{N}$ indica l'insieme

$$\{x \in \mathbb{N} / x = n_0 \cdot n \text{ con } n \in \mathbb{N}\}$$

cioè l'insieme dei numeri naturali multipli di n_0 . Poiché, quando ciò non dia luogo ad equivoci, il prodotto si usa indicare con la semplice giustapposizione dei fattori, nel seguito scriveremo $n_0\mathbb{N}$ anziché $n_0 \cdot \mathbb{N}$.

Analogamente, se $k \in \mathbb{Z}$ indicheremo con la scrittura $k\mathbb{Z}$ l'insieme dei numeri interi multipli di k .

Siano \mathbf{A} un insieme non vuoto e \star un'operazione in \mathbf{A} . Un elemento $a \in \mathbf{A}$ si dice *idempotente* se $a \star a = a$.

Esempio 1.1.10

Sia $\mathbf{A} := \mathbb{Z}^{2,2}$, e sia \cdot il prodotto "righe per colonne" definito in 1.1.8. Gli elementi

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

sono idempotenti.

1.2 - Chiusura rispetto a un'operazione.

Sia \mathbf{A} un insieme nel quale è definita un'operazione \star , e sia $\mathbf{B} \subset \mathbf{A}$.

Si dice che \mathbf{B} è *chiuso* rispetto a \star se comunque presi $b, b' \in \mathbf{B}$ è anche $b \star b' \in \mathbf{B}$. Se \mathbf{B} è chiuso rispetto a \star , la restrizione di \star a $\mathbf{B} \times \mathbf{B}$ è un'operazione in \mathbf{B} che si dice *indotta* da \star e (di solito, poiché ciò non dà luogo ad equivoci) si indica ancora con \star .

Esempi

1.2.1 \mathbb{Q}^+ è chiuso rispetto alla somma e al prodotto.

1.2.2 Il sottoinsieme di \mathbb{N} formato dai numeri dispari è chiuso rispetto al prodotto ma non rispetto alla somma.

1.2.3 Siano \mathbf{I} un insieme e \mathbf{A} l'insieme di tutte le funzioni da \mathbf{I} in \mathbf{I} . Il sottoinsieme di \mathbf{A} costituito dalle corrispondenze biunivoche (cioè l'insieme delle *permutazioni* su \mathbf{I} , cfr. sezione 0.4) è chiuso rispetto alla composizione.

Teorema 1.2.4

Sia \mathbf{A} un insieme nel quale è definita un'operazione \star . Se \mathcal{F} è una famiglia di sottoinsiemi di \mathbf{A} chiusi rispetto a \star , anche $\bigcap_{\mathbf{X} \in \mathcal{F}} \mathbf{X}$ è chiuso rispetto a \star .

Dimostrazione – Siano $x, y \in \bigcap_{\mathbf{X} \in \mathcal{F}} \mathbf{X}$. Allora, per ogni $\mathbf{X} \in \mathcal{F}$ si ha $x, y \in \mathbf{X}$ e dunque (poiché per ipotesi \mathbf{X} è chiuso rispetto a \star) $x \star y \in \mathbf{X}$. Ma allora $x \star y \in \bigcap_{\mathbf{X} \in \mathcal{F}} \mathbf{X}$; l'asserto è così provato per l'arbitrarietà di x e y in $\bigcap_{\mathbf{X} \in \mathcal{F}} \mathbf{X}$.

Osservazione 1.2.5

La proprietà espressa per l'intersezione dal teorema 1.2.4 non si può in generale estendere all'unione, nemmeno nel caso di due soli insiemi. Si consideri infatti, per esempio, l'insieme \mathbb{Z} dei numeri interi con l'usuale operazione $+$ di somma, e siano $2\mathbb{Z}$ e $3\mathbb{Z}$ i sottoinsiemi formati rispettivamente dai multipli di 2 e dai multipli di 3 (cfr. esempio 1.1.9). È facile verificare che sia $2\mathbb{Z}$ che $3\mathbb{Z}$ è chiuso rispetto alla somma; tuttavia $2\mathbb{Z} \cup 3\mathbb{Z}$ non è chiuso rispetto alla somma: $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ ma $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

1.3 - Associatività e commutatività.

Sia \mathbf{A} un insieme.

Un'operazione \star in \mathbf{A} si dice *associativa* se

$$a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in \mathbf{A}.$$

Un'operazione \star in \mathbf{A} si dice *commutativa* se

$$a \star b = b \star a \quad \forall a, b \in \mathbf{A}.$$

Esempi

Le operazioni considerate in 1.1.1, 1.1.6 e 1.1.7 sono associative e commutative; quella considerata in 1.1.2 è associativa ma in generale non commutativa; quella considerata in 1.1.5 è commutativa ma non associativa (infatti $(b \star b) \star c \neq b \star (b \star c)$); quella considerata in 1.1.4 non è né associativa né commutativa.

Il "prodotto righe per colonne" in $\mathbf{A}^{n,n}$ considerato in 1.1.8 è associativo, ma in generale non commutativo, per ogni scelta di \mathbf{A} e di n .

Sia \mathbf{A} un insieme, e sia \star un'operazione associativa in \mathbf{A} . Per ogni scelta di elementi $a, b, c \in \mathbf{A}$ la scrittura

$$a \star b \star c$$

non dà luogo ad ambiguità, perché le sue due possibili interpretazioni ($a \star (b \star c)$ e $(a \star b) \star c$) hanno lo stesso valore. Con un po' di attenzione si riesce anche a dimostrare che (purché \star sia associativa!) comunque preso un numero arbitrario di elementi $a_1, a_2, \dots, a_n \in \mathbf{A}$ tutte le possibili interpretazioni della scrittura

$$a_1 \star a_2 \star \dots \star a_n$$

hanno lo stesso valore, e quindi una tale scrittura può essere usata senza dar luogo ad equivoci.

1.4 - Elemento neutro.

Siano \mathbf{A} un insieme e \star un’operazione definita in \mathbf{A} .

Un elemento n di \mathbf{A} si dice *elemento neutro* per \star se $a\star n = n\star a = a \quad \forall a \in \mathbf{A}$.

Se l’operazione \star è detta *somma*, l’elemento neutro si indica con “0” e si chiama “zero”; se è detta *prodotto*, si indica con “1” e si chiama “uno” oppure “unità”.

Teorema 1.4.1

Siano \mathbf{A} un insieme e \star un’operazione definita in \mathbf{A} . Se esiste un elemento neutro per \star , questo è unico.

Dimostrazione – Siano n, n' elementi neutri per \star . Allora $n = n\star n' = n'$, come si voleva dimostrare.

Esempi

1.4.2 L’operazione \star considerata in 1.1.4 non ha elemento neutro. Si noti che $a\star 0 = a$ per ogni $a \in \mathbb{N}$, ma in generale $0\star a \neq a$.

1.4.3 Le operazioni di somma considerate in 1.1.1 hanno come elemento neutro il numero 0.

1.4.4 Le operazioni di prodotto considerate in 1.1.1 hanno come elemento neutro il numero 1.

1.4.5 L’operazione \star considerata in 1.1.5 ha come elemento neutro l’elemento \mathbf{a} .

1.4.6 Le operazioni di unione e intersezione considerate in 1.1.6 e 1.1.7 hanno come elemento neutro rispettivamente \emptyset e \mathbf{A} .

1.4.7 L’operazione di composizione considerata in 1.1.2 ha come elemento neutro la funzione $\mathbf{id}_{\mathbf{A}}$ (“identità su \mathbf{A} ”) già ricordata nella sezione 0.4.

1.4.8 Il “prodotto righe per colonne” in $\mathbf{A}^{n,n}$ considerato in 1.1.8 ha elemento neutro se e soltanto se in \mathbf{A} c’è l’elemento neutro 1 rispetto al prodotto (quindi certamente se \mathbf{A} è \mathbb{Z} , \mathbb{Q} , \mathbb{R} o \mathbb{C}) e tale elemento neutro è la matrice $(\delta_{i,j})$ dove $\delta_{i,j}$ è il cosiddetto “simbolo di Kröneker”, ossia

$$\delta_{i,j} := \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j. \end{cases}$$

1.5 - Il simmetrico di un elemento.

Siano \mathbf{A} un insieme e \star un'operazione definita in \mathbf{A} per la quale esiste l'elemento neutro n .

Per ogni $a \in \mathbf{A}$, si dice *simmetrico di a* (rispetto a \star) un elemento $\bar{a} \in \mathbf{A}$ tale che sia

$$a \star \bar{a} = \bar{a} \star a = n.$$

Se l'operazione \star è detta *somma*, il simmetrico di a si dice *opposto* di a , e si indica con $-a$; se è detta *prodotto*, si dice *inverso* di a , e si indica con a^{-1} .

Teorema 1.5.1

Siano \mathbf{A} un insieme, \star un'operazione definita in \mathbf{A} per la quale esiste l'elemento neutro n , e $a \in \mathbf{A}$.

Se a ha simmetrico \bar{a} , anche \bar{a} ha simmetrico, e il simmetrico di \bar{a} è a .

Dimostrazione – Le stesse uguaglianze ($a \star \bar{a} = \bar{a} \star a = n$) che esprimono il fatto che \bar{a} è simmetrico di a ci dicono anche che a è simmetrico di \bar{a} .

Teorema 1.5.2

Siano \mathbf{A} un insieme e \star un'operazione associativa definita in \mathbf{A} per la quale esiste l'elemento neutro n .

Per ogni $a \in \mathbf{A}$, se esiste un simmetrico questo è unico.

Dimostrazione – Siano $\bar{a}, \bar{\bar{a}}$ simmetrici di a . Allora

$$\bar{a} = \bar{a} \star n = \bar{a} \star (a \star \bar{\bar{a}}) = (\bar{a} \star a) \star \bar{\bar{a}} = n \star \bar{\bar{a}} = \bar{\bar{a}}.$$

Teorema 1.5.3

Siano \mathbf{A} un insieme e \star un'operazione associativa definita in \mathbf{A} per la quale esiste l'elemento neutro n , e $a \in \mathbf{A}$.

Se a è idempotente e ha simmetrico \bar{a} , allora $a = n$.

Dimostrazione – Si ha infatti

$$n = a \star \bar{a} = (a \star a) \star \bar{a} = a \star (a \star \bar{a}) = a \star n = a.$$

Esempi

1.5.4 Rispetto all’operazione \star definita in 1.1.5 (che non è associativa), l’elemento b ha due distinti simmetrici: se stesso e l’elemento b .

1.5.5 In \mathbb{Z} , per ogni elemento esiste l’opposto (cioè, il simmetrico rispetto alla somma) ma solo per $+1$ e -1 esiste l’inverso (cioè, il simmetrico rispetto al prodotto).

1.5.6 Rispetto alle operazioni di “unione” e “intersezione” considerate in 1.1.6 e 1.1.7, non esiste in generale il simmetrico di un elemento di $\mathcal{P}(A)$.

1.5.7 Rispetto all’operazione di “composizione” considerata in 1.1.2 non esiste in generale il simmetrico di una funzione. Tuttavia, se f è una corrispondenza biunivoca di A in sé la funzione f^{-1} ricordata nella sezione 0.4 è il simmetrico di f rispetto alla composizione (cfr. osservazione 0.5.1).

1.6 - La rappresentazione tabulare di un’operazione.

Nel caso, certamente particolare ma assolutamente non irrilevante, in cui si considera un’operazione in un insieme finito, questa può essere descritta mediante una *tabella*.

Sia $A = \{a_1, a_2, \dots, a_n\}$

un insieme di cardinalità n ($\in \mathbb{N}$), e sia \star un’operazione in A . Si dice *tabella* (“*tavola pitagorica*”?) di \star la matrice $(n+1) \times (n+1)$ a elementi in $A \cup \{\star\}$ così definita:

- l’elemento di posto $(1, 1)$ è \star ;
- per ogni $i := 1, \dots, n$, l’elemento di posto $(1, i+1)$ e l’elemento di posto $(i+1, 1)$ coincidono con a_i ;
- per ogni $i, j := 1, \dots, n$, l’elemento di posto $(i+1, j+1)$ coincide con $a_i \star a_j$.

La $(i+1)$ – sima riga [colonna] si dice *riga [colonna] corrispondente all’elemento a_i* ; si usa anche dire che il risultato dell’operazione \star fra due elementi dati *si legge all’incrocio fra la riga e la colonna corrispondenti* a tali elementi.

Alcune proprietà di \star si traducono immediatamente in proprietà della sua tabella. Ad esempio, \star è commutativa se e soltanto se la sua tabella è una matrice simmetrica. È anche facile stabilire con la tabella di \star se un dato elemento è elemento neutro per \star ; se poi \star ha l’elemento neutro, basta scorrere la riga e la colonna corrispondenti a un elemento a_i per decidere (si stabilisca per esercizio con che criterio!) se a_i possiede o non possiede simmetrico rispetto a \star . Non c’è invece un modo “veloce” per decidere mediante la tabella se \star è associativa.

Di solito nella rappresentazione grafica della tabella di un'operazione si evidenziano la prima riga e la prima colonna. Ecco ad esempio come si potrebbe presentare la tabella dell'operazione \star descritta in 1.1.5:

\star	a	b	c
a	a	b	c
b	b	a	a
c	c	a	b

Nella descrizione di un'operazione mediante una tabella è implicito l'insieme in cui essa è definito: lo si può infatti leggere nella prima riga (o nella prima colonna).

Un esame dell'operazione può suggerire di rinominare gli elementi dell'insieme in modo da rendere più espressiva la tabella; ad esempio, nell'operazione \star appena considerata si può rinominare a in n (perché a risulta essere l'elemento neutro) e b in c^2 (avendosi $c \star c = b$). La tabella diventa allora

\star	n	c	c^2
n	n	c	c^2
c	c	c^2	n
c^2	c^2	n	n

Le due tabelle che abbiamo scritto rappresentano operazioni definite in insiemi diversi ($\{a, b, c\}$ e $\{n, c, c^2\}$), ma per come abbiamo ottenuto la seconda a partire dalla prima è lecito affermare che rappresentano *la stessa operazione*. Uno dei primi problemi che dovremo affrontare sarà proprio quello di chiarire quando insiemi diversi, magari con operazioni dal nome diverso (*what's in a name?*) debbano essere "identificati" dal nostro punto di vista.

Esempio 1.6.1

\cdot	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab	ab	b	a^2b	a	1	a^2
a^2b	a^2b	ab	b	a^2	a	1

2.- SEMIGRUPPI, MONOIDI, GRUPPI, ANELLI

2.1 - Semigrupperi.

Siano S un insieme e \star un'operazione in S .

Si dice che la coppia (S, \star) è un semigruppero (o anche, più confidenzialmente, che S è un *semigruppero* rispetto a \star) se:

G.1 l'operazione \star è associativa.

Se inoltre

G.4 l'operazione \star è commutativa

il semigruppero si dice *commutativo*.

Esempi

2.1.1 L'insieme \mathbb{Z} dei numeri interi è un semigruppero commutativo rispetto alla somma. Anche $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$, tanto per citare gli insiemi numerici più conosciuti, sono semigrupperi (commutativi) rispetto alla somma: tutti questi esempi però sono molto "ricchi" (col linguaggio che introdurremo nella sez. 2.7, si tratta di *gruppi commutativi*). Negli esempi 2.1.2 e 2.1.3 presentiamo semigrupperi "poveri" (che cioè non sono *gruppi* e nemmeno sono *monoidi*, cfr. sez. 2.4).

2.1.2 Sia $2\mathbb{Z}$ l'insieme dei numeri interi *pari* (cfr. esempio 1.1.9). L'insieme $(2\mathbb{Z})^{2,2}$ delle matrici 2×2 a coefficienti in $2\mathbb{Z}$ è un semigruppero rispetto all'operazione di "prodotto righe per colonne" definita in 1.1.8.

Si noti che $(2\mathbb{Z})^{2,2}$ **non** è commutativo, perché

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

2.1.3 L'insieme $2\mathbb{Z}$ è un semigruppero commutativo rispetto all'usuale operazione di prodotto.

2.2 - Sottosemigruppi.

Sia \mathbf{S} un semigruppato rispetto a una data operazione \star .

Si dice *sottosemigruppo* di \mathbf{S} un sottoinsieme non vuoto di \mathbf{S} che sia chiuso rispetto a \star . Si noti che: se \mathbf{S}_1 è un sottosemigruppo di \mathbf{S} , allora \mathbf{S}_1 è un semigruppato rispetto all'operazione indotta da \star ; infatti la restrizione a un sottoinsieme di un'operazione associativa non può che essere associativa.

Esempi

2.2.1 Gli insiemi \mathbb{Z}^+ (dei numeri interi positivi) e \mathbb{Z}^- (dei numeri interi negativi) sono sottosemigruppi di $(\mathbb{Z}, +)$.

2.2.2 Il sottoinsieme di $(2\mathbb{Z})^{2,2}$ (cfr. esempio 2.1.2) formato dalle matrici in cui è nullo l'elemento di posto $(2,1)$ (cioè l'elemento individuato dalla seconda riga e dalla prima colonna) è un sottosemigruppo di $(2\mathbb{Z})^{2,2}$. Quanto già osservato in 2.1.2 mostra che questo sottosemigruppo **non** è commutativo.

2.2.3 L'insieme $4\mathbb{Z}$ (dei multipli di 4) è un sottosemigruppo del semigruppato commutativo considerato in 2.1.3.

Teorema 2.2.4

Sia \mathbf{S} un semigruppato. Per ogni famiglia \mathcal{F} di sottosemigruppi di \mathbf{S} ,

$$\bigcap_{\mathbf{T} \in \mathcal{F}} \mathbf{T} \text{ se non è } \emptyset \text{ è un sottosemigruppo di } \mathbf{S}.$$

Dimostrazione – Per definizione di sottosemigruppo, questo teorema è immediata conseguenza del teorema 1.2.4.

Osservazione 2.2.5

Come si è osservato nell'esempio 2.2.1, \mathbb{Z}^+ e \mathbb{Z}^- sono sottosemigruppi di $(\mathbb{Z}, +)$. La loro intersezione è però \emptyset e quindi non è un sottosemigruppo di $(\mathbb{Z}, +)$.

Osservazione 2.2.6

Lo stesso esempio considerato nell'osservazione 1.2.5 mostra che, in generale, l'unione di due sottosemigruppi può non essere un sottosemigruppo.

Sia \mathbf{S} un semigruppato, e sia $\mathbf{X} \subset \mathbf{S}$. Si dice *sottosemigruppato di \mathbf{S} generato da \mathbf{X}* l'intersezione di tutti i sottosemigruppato di \mathbf{S} contenenti \mathbf{X} .

Osservazione 2.2.7

Sia \mathbf{S} un semigruppato, e sia $\mathbf{X} \subset \mathbf{S}$. Il sottosemigruppato di \mathbf{S} generato da \mathbf{X} contiene \mathbf{X} ed è contenuto in ogni sottosemigruppato di \mathbf{S} contenente \mathbf{X} (si dice anche che è *il minimo sottosemigruppato di \mathbf{S} contenente \mathbf{X}*). Infatti la famiglia dei sottosemigruppato di \mathbf{S} contenenti \mathbf{X} non è vuota, perché vi appartiene certamente \mathbf{S} .

Teorema 2.2.8

Sia \mathbf{S} un semigruppato rispetto all'operazione \star , e sia $\mathbf{X} \subset \mathbf{S}$. Il sottosemigruppato di \mathbf{S} generato da \mathbf{X} è l'insieme degli elementi di \mathbf{S} che si possono scrivere nella forma

$$x_1 \star x_2 \star \dots \star x_k$$

con $k \in \mathbb{Z}^+$ (eventualmente $k = 1$) e gli x_i appartenenti a \mathbf{X} non necessariamente distinti fra loro.

Dimostrazione – Sia \mathbf{S}_1 l'insieme degli elementi di \mathbf{S} che si possono scrivere nella forma descritta dall'enunciato del teorema (che, ricordiamo, non è ambigua per l'associatività di \star !), e sia \mathbf{S}_2 il sottosemigruppato di \mathbf{S} generato da \mathbf{X} .

Per definizione di \mathbf{S}_1 , $\mathbf{X} \subset \mathbf{S}_1$; inoltre, \mathbf{S}_1 è chiuso rispetto a \star e dunque è un sottosemigruppato di \mathbf{S} contenente \mathbf{X} : per definizione di \mathbf{S}_2 , ne segue che $\mathbf{S}_2 \subset \mathbf{S}_1$.

Viceversa, sia \mathbf{S}_0 un sottosemigruppato di \mathbf{S} contenente \mathbf{X} ; allora ogni elemento di \mathbf{S} della forma descritta dall'enunciato del teorema deve appartenere a \mathbf{S}_0 (perché \mathbf{S}_0 deve essere chiuso rispetto a \star), cosicché deve essere $\mathbf{S}_1 \subset \mathbf{S}_0$. Per l'arbitrarietà di \mathbf{S}_0 , deve essere $\mathbf{S}_1 \subset \mathbf{S}_2$ cosicché l'asserto è completamente provato.

2.3 - Omomorfismi e isomorfismi tra semigruppato.

Siano (\mathbf{S}, \star) e (\mathbf{T}, \circ) semigruppato.

Si dice *omomorfismo* tra (\mathbf{S}, \star) e (\mathbf{T}, \circ) (o anche, più semplicemente, tra \mathbf{S} e \mathbf{T}) una funzione $\mathbf{f}: \mathbf{S} \rightarrow \mathbf{T}$ tale che

$$\mathbf{f}(x \star y) = \mathbf{f}(x) \circ \mathbf{f}(y) \quad \forall x, y \in \mathbf{S}.$$

Si dice *isomorfismo* un omomorfismo biiettivo.

2.4 - Monoidi.

Siano \mathbf{M} un insieme e \star un'operazione in \mathbf{M} .

Si dice che la coppia (\mathbf{M}, \star) è un *monoide* (o anche, più confidenzialmente, che \mathbf{M} è un *monoide* rispetto a \star) se valgono le seguenti proprietà:

G.1 l'operazione \star è associativa;

G.2 esiste in \mathbf{M} l'elemento neutro per \star .

Se inoltre

G.4 l'operazione \star è commutativa

il monoide si dice *commutativo*.

Esempi

2.4.1 L'insieme $\mathbb{R}^{2,2}$ delle matrici 2×2 a coefficienti reali è un monoide rispetto all'operazione di "prodotto righe per colonne" definita in 1.1.8. L'elemento neutro è

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Si noti che $\mathbb{R}^{2,2}$ **non** è commutativo, perché

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

2.4.2 Più in generale: per ogni numero naturale n , l'insieme $\mathbb{R}^{n,n}$ delle matrici $n \times n$ a coefficienti reali è un monoide (non commutativo) rispetto all'operazione di "prodotto righe per colonne" definita in 1.1.8. L'elemento neutro è la matrice $(\delta_{i,j})$ dove $\delta_{i,j}$ è il già citato "simbolo di Kröneker" (cfr. 1.4.8).

2.4.3 Sia \mathbf{A} un insieme. L'insieme $\mathcal{P}(\mathbf{A})$ è un monoide commutativo rispetto all'operazione di unione definita in 1.1.6 (cfr. 1.4.6).

2.4.4 Sia \mathbf{A} un insieme. L'insieme $\mathcal{P}(\mathbf{A})$ è un monoide commutativo rispetto all'operazione di intersezione definita in 1.1.7 (cfr. 1.4.6).

2.5 - Sottomonoidi.

Sia (\mathbf{M}, \star) un monoide.

Si dice *sottomonoide* di \mathbf{M} un sottoinsieme di \mathbf{M} che sia chiuso rispetto a \star e a cui appartenga l'elemento neutro di \mathbf{M} . Si noti che: se \mathbf{M}_1 è un sottomonoide di \mathbf{M} , allora \mathbf{M}_1 (è un sottoinsieme di \mathbf{M} e) è un monoide rispetto all'operazione indotta da \star , ma non vale il viceversa (cfr. esempio 2.5.3 ed esercizio 2.5.4).

Esempi

2.5.1 Il sottoinsieme di $\mathbb{R}^{2,2}$ formato dalle matrici in cui è nullo l'elemento di posto (2, 1) (cioè l'elemento individuato dalla seconda riga e dalla prima colonna) è un sottomonoide di $\mathbb{R}^{2,2}$. L'esempio già visto in 2.4.1 mostra che questo sottomonoide **non** è commutativo.

2.5.2 Sia \mathbf{A} un insieme. Se $\mathbf{A}_1 \subset \mathbf{A}$, $(\mathcal{P}(\mathbf{A}_1), \cup)$ è un sottomonoide di $(\mathcal{P}(\mathbf{A}), \cup)$.

2.5.3 Sia \mathbf{A} un insieme. Se $\mathbf{A}_1 \subsetneq \mathbf{A}$, $(\mathcal{P}(\mathbf{A}_1), \cap)$ è un sottosemigruppo di $(\mathcal{P}(\mathbf{A}), \cap)$ ed è un monoide, ma non è un sottomonoide di $(\mathcal{P}(\mathbf{A}), \cap)$; infatti l'elemento neutro di $\mathcal{P}(\mathbf{A}_1)$ è \mathbf{A}_1 , che non è elemento neutro per $\mathcal{P}(\mathbf{A})$, mentre l'elemento neutro di $\mathcal{P}(\mathbf{A})$ è \mathbf{A} , che non appartiene a $\mathcal{P}(\mathbf{A}_1)$.

Esercizio 2.5.4

Si dimostri che il sottoinsieme \mathbf{M}_1 del monoide $\mathbb{R}^{2,2}$ formato dalle matrici della forma

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

(cioè quelle in cui è nullo ogni elemento tranne eventualmente quello di posto (1, 1)) è un sottosemigruppo di $\mathbb{R}^{2,2}$ ed è un monoide, ma non è un sottomonoide di $\mathbb{R}^{2,2}$.

Teorema 2.5.5

Sia \mathbf{M} un monoide. Per ogni famiglia non vuota \mathcal{F} di sottomonoidi di \mathbf{M} ,

$$\bigcap_{\mathbf{N} \in \mathcal{F}} \mathbf{N} \text{ è un sottomonoide di } \mathbf{M}.$$

Dimostrazione – Per definizione di sottomonoide, l'elemento neutro di \mathbf{M} appartiene a ogni elemento di \mathcal{F} e quindi anche a $\bigcap_{\mathbf{N} \in \mathcal{F}} \mathbf{N}$. A questo punto il teorema è immediata conseguenza del teorema 1.2.4.

Osservazione 2.5.6

Lo stesso esempio considerato nell'osservazione 1.2.5 mostra che, in generale, l'unione di due sottomonoidi può non essere un sottomonoide.

Sia \mathbf{M} un monoide, e sia $\mathbf{X} \subset \mathbf{M}$. Si dice *sottomonoide di \mathbf{M} generato da \mathbf{X}* l'intersezione di tutti i sottomonoidi di \mathbf{M} contenenti \mathbf{X} .

Osservazione 2.5.7

Sia \mathbf{M} un monoide, e sia $\mathbf{X} \subset \mathbf{M}$. Il sottomonoide di \mathbf{M} generato da \mathbf{X} contiene \mathbf{X} ed è contenuto in ogni sottomonoide di \mathbf{M} contenente \mathbf{X} (si dice anche che è *il minimo sottomonoide di \mathbf{M} contenente \mathbf{X}*). Infatti la famiglia dei sottomonoidi di \mathbf{M} contenenti \mathbf{X} non è vuota, perché vi appartiene certamente \mathbf{M} .

Teorema 2.5.8

Sia \mathbf{M} un monoide rispetto all'operazione \star con elemento neutro n , e sia $\mathbf{X} \subset \mathbf{M}$. Il sottomonoide di \mathbf{M} generato da \mathbf{X} è l'insieme degli elementi di \mathbf{M} che si possono scrivere nella forma

$$x_1 \star x_2 \star \dots \star x_k$$

con $k \in \mathbb{Z}^+$ (eventualmente $k = 1$) e gli x_i appartenenti a $\mathbf{X} \cup \{n\}$ non necessariamente distinti fra loro.

Dimostrazione – Sia \mathbf{M}_1 l'insieme degli elementi di \mathbf{M} che si possono scrivere nella forma descritta dall'enunciato del teorema (che, ricordiamo, non è ambigua per l'associatività di \star !), e sia \mathbf{M}_2 il sottomonoide di \mathbf{M} generato da \mathbf{X} .

Per definizione di \mathbf{M}_1 , $\mathbf{X} \subset \mathbf{M}_1$; inoltre, $n \in \mathbf{M}_1$ e \mathbf{M}_1 è chiuso rispetto a \star ; dunque \mathbf{M}_1 è un sottomonoido di \mathbf{M} contenente \mathbf{X} : per definizione di \mathbf{M}_2 , ne segue che $\mathbf{M}_2 \subset \mathbf{M}_1$.

Viceversa, sia \mathbf{M}_0 un sottomonoido di \mathbf{M} contenente \mathbf{X} ; allora ogni elemento di \mathbf{M} della forma descritta dall'enunciato del teorema deve appartenere a \mathbf{M}_0 (perché deve essere $n \in \mathbf{M}_0$ e \mathbf{M}_0 deve essere chiuso rispetto a \star), cosicché deve essere $\mathbf{M}_1 \subset \mathbf{M}_0$. Per l'arbitrarietà di \mathbf{M}_0 , deve essere $\mathbf{M}_1 \subset \mathbf{M}_2$ cosicché l'asserto è completamente provato.

Teorema 2.5.9

Sia (\mathbf{M}, \star) un monoide. Se a, b sono elementi di \mathbf{M} dotati di simmetrico (rispettivamente \bar{a} e \bar{b}) anche $a \star b$ ha simmetrico $\overline{a \star b}$, e si ha

$$\overline{a \star b} = \bar{b} \star \bar{a}.$$

Dimostrazione – Detto n l'elemento neutro, si ha

$$(a \star b) \star (\bar{b} \star \bar{a}) = a \star (b \star \bar{b}) \star \bar{a} = a \star n \star \bar{a} = a \star \bar{a} = n$$

e allo stesso modo

$$(\bar{b} \star \bar{a}) \star (a \star b) = \bar{b} \star (\bar{a} \star a) \star b = \bar{b} \star n \star b = \bar{b} \star b = n$$

cosicché l'asserto è completamente provato.

Teorema 2.5.10

Sia (\mathbf{M}, \star) un monoide. L'insieme degli elementi di \mathbf{M} dotati di simmetrico è un sottomonoido di \mathbf{M} .

Dimostrazione – L'elemento neutro è il simmetrico di se stesso, dunque appartiene all'insieme considerato; l'asserto segue allora immediatamente dal teorema 2.5.9.

2.6 - Omomorfismi e isomorfismi tra monoidi.

Siano (\mathbf{M}, \star) e (\mathbf{N}, \circ) monoidi.

Si dice *omomorfismo* tra (\mathbf{M}, \star) e (\mathbf{N}, \circ) (o anche, più semplicemente, tra \mathbf{M} e \mathbf{N}) una funzione $\mathbf{f}: \mathbf{M} \rightarrow \mathbf{N}$ tale che

$$- \quad \mathbf{f}(x \star y) = \mathbf{f}(x) \circ \mathbf{f}(y) \quad \forall x, y \in \mathbf{M}$$

e

$$- \quad \text{se } n \text{ è l'elemento neutro di } \mathbf{M}, \mathbf{f}(n) \text{ è l'elemento neutro di } \mathbf{N}.$$

Si dice *isomorfismo* un omomorfismo biiettivo.

Esempio 2.6.1

Sia \mathbf{M} un monoide con elemento neutro n e sia \mathbf{M}_1 un sottosemigruppo di \mathbf{M} che è anch'esso un monoide ma con elemento neutro $n_1 \neq n$ (quindi in particolare $n \notin \mathbf{M}_1$); si vedano l'esempio 2.5.3 e l'esercizio 2.5.4. Sia f la restrizione a \mathbf{M}_1 dell'identità di \mathbf{M} (cfr. sez. 0.4). Indicando con \circ l'operazione definita in \mathbf{M} e con \star quella da essa indotta in \mathbf{M}_1 , è immediato verificare che f è un omomorfismo fra i *semigrupperi* (\mathbf{M}_1, \star) e (\mathbf{M}, \circ) ma **non** è un omomorfismo fra i *monoidi* (\mathbf{M}_1, \star) e (\mathbf{M}, \circ) perché $f(n_1) = n_1$ **non** è l'elemento neutro di \mathbf{M} .

2.7 - Gruppi.

Siano \mathbf{G} un insieme e \star un'operazione in \mathbf{G} .

Si dice che \mathbf{G} è un *gruppo* rispetto a \star , oppure (più correttamente!) che la coppia (\mathbf{G}, \star) è un gruppo, se valgono le seguenti proprietà:

- G.1** l'operazione \star è associativa;
- G.2** esiste in \mathbf{G} l'elemento neutro per \star ;
- G.3** per ogni $g \in \mathbf{G}$ esiste il simmetrico di g rispetto a \star .

Se inoltre

- G.4** l'operazione \star è commutativa

il gruppo si dice *commutativo*. Per i gruppi si usa spesso come sinonimo di "commutativo" l'aggettivo *abeliano* in onore del matematico Niels Henrik Abel (1802-1829).

Esempi

2.7.1 \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} sono gruppi abeliani rispetto alla somma.

2.7.2 \mathbb{N} non è un gruppo rispetto alla somma (non esiste in generale l'opposto di un elemento).

2.7.3 \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} non sono gruppi rispetto al prodotto (non esiste l'inverso di 0).

2.7.4 $\mathbb{Q} \setminus \{0\}$, \mathbb{Q}^+ , $\mathbb{R} \setminus \{0\}$, \mathbb{R}^+ e $\mathbb{C} \setminus \{0\}$ sono gruppi abeliani rispetto al prodotto.

[2.7.5] Per ogni insieme \mathbf{A} , l'insieme $\mathbf{Sym}(\mathbf{A})$ delle permutazioni su \mathbf{A} (sezione 0.4) è un gruppo (in generale non abeliano) rispetto alla composizione di funzioni. Infatti è chiuso rispetto a tale operazione (come si è visto nell'esempio 1.2.3), la quale è associativa (osservazione 0.5.2) e ha come elemento neutro la funzione $\mathbf{id}_{\mathbf{A}} : \mathbf{A} \rightarrow \mathbf{A}$ che ad ogni elemento associa se stesso; infine, l'esistenza del simmetrico per ogni permutazione su \mathbf{A} è già stata segnalata in 1.5.7.

[2.7.6] Sia \mathbf{A} un insieme. $\mathcal{P}(\mathbf{A})$ (cfr. 3.5) non è un gruppo né rispetto all'unione né rispetto all'intersezione; è però un gruppo abeliano rispetto all'operazione \star (detta *differenza simmetrica*) definita come segue:

$$\mathbf{X} \star \mathbf{Y} = (\mathbf{X} \cup \mathbf{Y}) \setminus (\mathbf{X} \cap \mathbf{Y}) \quad \forall \mathbf{X}, \mathbf{Y} \in \mathcal{P}(\mathbf{A}).$$

[2.7.7] Per ogni monoide \mathbf{M} , il sottomonoide degli elementi di \mathbf{M} dotati di simmetrico (cfr. teorema 2.5.10) è un gruppo.

[Osservazione 2.7.8]

Un gruppo è un monoide in cui ogni elemento ha simmetrico.

[Teorema 2.7.9]

Sia (\mathbf{G}, \star) un gruppo. L'unico elemento idempotente di \mathbf{G} è l'elemento neutro.

Dimostrazione – Per definizione di "gruppo", l'operazione \star è associativa e ogni elemento di \mathbf{G} ha simmetrico rispetto a \star . L'asserto segue perciò immediatamente dal teorema 1.5.3.

[Teorema 2.7.10]

Sia (\mathbf{G}, \star) un gruppo. Se ogni elemento di \mathbf{G} coincide col proprio simmetrico, \mathbf{G} è abeliano.

Dimostrazione – Siano $x, y \in \mathbf{G}$; dobbiamo provare che $x \star y = y \star x$. Per ipotesi, $\overline{x \star y} = x \star y$; per il teorema 2.5.9, $x \star y = \overline{y \star x}$. Dunque

$$x \star y = \overline{x \star y} = \overline{y \star x} = y \star x$$

tenendo ancora conto dell'ipotesi.

2.8 - Sottogruppi.

Sia (\mathbf{G}, \star) un gruppo.

Si dice *sottogruppo* di \mathbf{G} un sottoinsieme di \mathbf{G} chiuso rispetto a \star che sia un gruppo rispetto all'operazione indottavi da \star .

Esempi

2.8.1 \mathbb{Z}^+ non è un sottogruppo di $(\mathbb{Z}, +)$, pur essendo chiuso rispetto alla somma.

2.8.2 \mathbb{Q}^+ è un sottogruppo di $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Teorema 2.8.3

Sia (\mathbf{G}, \star) un gruppo, e sia \mathbf{H} un sottogruppo di \mathbf{G} . L'elemento neutro per \star in \mathbf{H} coincide con l'elemento neutro per \star in \mathbf{G} (e quindi, per ogni $h \in \mathbf{H}$ il simmetrico di h in \mathbf{H} coincide col simmetrico di h in \mathbf{G}).

Dimostrazione – L'elemento neutro per \star in \mathbf{H} è idempotente; dunque (per il teorema 2.7.9) esso coincide con l'elemento neutro per \star in \mathbf{G} . Possiamo ora applicare il teorema 1.5.2 e concludere che per ogni $h \in \mathbf{H}$ il simmetrico di h in \mathbf{H} coincide con il simmetrico di h in \mathbf{G} .

2.9 - Omomorfismi e isomorfismi tra gruppi.

Siano (\mathbf{G}, \star) e (\mathbf{H}, \circ) gruppi.

Una funzione $f: \mathbf{G} \rightarrow \mathbf{H}$ si dice un *omomorfismo* tra (\mathbf{G}, \star) e (\mathbf{H}, \circ) (o anche, più semplicemente, tra \mathbf{G} e \mathbf{H}) se

$$f(x \star y) = f(x) \circ f(y) \quad \forall x, y \in \mathbf{G}.$$

Un omomorfismo iniettivo si dice *monomorfismo*; un omomorfismo suriettivo si dice *epimorfismo*; un omomorfismo biiettivo si dice *isomorfismo*.

Sia (\mathbf{G}, \star) un gruppo. Un omomorfismo tra (\mathbf{G}, \star) e (\mathbf{G}, \star) si dice un *endomorfismo* di (\mathbf{G}, \star) ; un isomorfismo tra (\mathbf{G}, \star) e (\mathbf{G}, \star) (cioè un endomorfismo biiettivo di (\mathbf{G}, \star)) si dice un *automorfismo* di (\mathbf{G}, \star) .

Teorema 2.9.1

Siano (\mathbf{G}, \star) e (\mathbf{H}, \circ) gruppi, e sia \mathbf{f} un omomorfismo tra \mathbf{G} e \mathbf{H} . Se n è l'elemento neutro per \star in \mathbf{G} , $\mathbf{f}(n)$ è l'elemento neutro per \circ in \mathbf{H} ; inoltre, per ogni $g \in \mathbf{G}$: se \bar{g} è il simmetrico di g rispetto a \star in \mathbf{G} , $\mathbf{f}(\bar{g})$ è il simmetrico di $\mathbf{f}(g)$ rispetto a \circ in \mathbf{H} .

Dimostrazione – Sia n l'elemento neutro per \star in \mathbf{G} . Si ha

$$\mathbf{f}(n) \circ \mathbf{f}(n) = \mathbf{f}(n \star n) = \mathbf{f}(n)$$

cioè $\mathbf{f}(n)$ è un elemento idempotente di \mathbf{H} ; dunque, per il teorema 2.7.9, $\mathbf{f}(n)$ è l'elemento neutro n' per \circ in \mathbf{H} .

Sia ora $g \in \mathbf{G}$, e sia \bar{g} il simmetrico di g rispetto a \star in \mathbf{G} . Si ha

$$\mathbf{f}(\bar{g}) \circ \mathbf{f}(g) = \mathbf{f}(\bar{g} \star g) = \mathbf{f}(n) = n'$$

e analogamente

$$\mathbf{f}(g) \circ \mathbf{f}(\bar{g}) = \mathbf{f}(g \star \bar{g}) = \mathbf{f}(n) = n'$$

come si voleva dimostrare.

Esempio 2.9.2

Sia (\mathbb{R}^+, \cdot) il gruppo dei numeri reali positivi (rispetto all'operazione di prodotto) e sia $(\mathbb{R}, +)$ il gruppo di tutti i numeri reali (rispetto all'operazione di somma). Per ogni $b \in \mathbb{R}^+$, il logaritmo in base b è un isomorfismo tra (\mathbb{R}^+, \cdot) e $(\mathbb{R}, +)$.

Teorema 2.9.3

Siano (\mathbf{G}, \star) e (\mathbf{H}, \circ) gruppi, e sia \mathbf{f} un isomorfismo tra (\mathbf{G}, \star) e (\mathbf{H}, \circ) . La funzione inversa \mathbf{f}^{-1} (cfr. sez. 0.4) è un isomorfismo tra (\mathbf{H}, \circ) e (\mathbf{G}, \star) , detto *isomorfismo inverso* di \mathbf{f} .

Dimostrazione – Si è già osservato nella sez. 0.4 che \mathbf{f}^{-1} è una corrispondenza biunivoca tra \mathbf{H} e \mathbf{G} , quindi resta soltanto da verificare che è un omomorfismo.

Se $h_1, h_2 \in \mathbf{H}$, esistono $g_1, g_2 \in \mathbf{G}$ tali che $\mathbf{f}(g_1) = h_1$ e $\mathbf{f}(g_2) = h_2$; inoltre, poiché \mathbf{f} è un omomorfismo, si ha $\mathbf{f}(g_1 \star g_2) = \mathbf{f}(g_1) \circ \mathbf{f}(g_2) = h_1 \circ h_2$. Ne segue, per definizione di funzione inversa, che $\mathbf{f}^{-1}(h_1) = g_1$, $\mathbf{f}^{-1}(h_2) = g_2$ e $\mathbf{f}^{-1}(h_1 \circ h_2) = g_1 \star g_2$.

Dunque, comunque presi $h_1, h_2 \in \mathbf{H}$, si ha

$$\mathbf{f}^{-1}(h_1 \circ h_2) = \mathbf{f}^{-1}(h_1) \star \mathbf{f}^{-1}(h_2)$$

come si voleva dimostrare.

Esercizio 2.9.4

Sia $(\mathbb{R}, +)$ il gruppo di tutti i numeri reali (rispetto all'operazione di somma) e sia (\mathbb{R}^+, \cdot) il gruppo dei numeri reali positivi (rispetto all'operazione di prodotto). Per ogni $b \in \mathbb{R}^+$, si descriva l'isomorfismo tra $(\mathbb{R}, +)$ e (\mathbb{R}^+, \cdot) inverso di quello considerato nell'esempio 2.9.2.

2.10 - Anelli.

Sia \mathbf{A} un insieme con almeno due elementi, e siano $+$, \cdot due operazioni in \mathbf{A} (che chiameremo rispettivamente *somma* e *prodotto*).

Si dice che \mathbf{A} è un *anello* rispetto a $+$ e \cdot , oppure (più correttamente!) che la terna $(\mathbf{A}, +, \cdot)$ è un anello, se

A.1 $(\mathbf{A}, +)$ è un gruppo commutativo;

A.2 il prodotto è associativo;

A.3 il prodotto è distributivo rispetto alla somma.

Se inoltre

A.4 esiste in \mathbf{A} un elemento neutro per il prodotto

oppure

A.5 il prodotto è commutativo

si dice (rispettivamente) che \mathbf{A} è un *anello con unità* (e l'elemento neutro per il prodotto si dice l'*unità* di \mathbf{A}) oppure che \mathbf{A} è un *anello commutativo*. Naturalmente, se valgono sia la **A.4** che la **A.5** si dice che \mathbf{A} è un *anello commutativo con unità*.

Convenzionalmente, gli elementi neutri per la somma e il prodotto si indicano rispettivamente con "0" e "1"; qualora possa esservi confusione con i numeri naturali 0 e 1, si usano le notazioni " $0_{\mathbf{A}}$ " e " $1_{\mathbf{A}}$ ". Inoltre, l'opposto di un elemento x si indica con $-x$, l'inverso di un elemento x (se esiste) si indica con x^{-1} .

Esempi

2.10.1 \mathbb{Z} e \mathbb{Q} sono anelli commutativi con unità rispetto alle ordinarie operazioni di somma e prodotto.

2.10.2 L'insieme dei polinomi a coefficienti in \mathbb{Z} (oppure in \mathbb{Q}) nell'indeterminata x è un anello commutativo con unità rispetto alle usuali operazioni di somma e prodotto.

2.10.3 L'insieme dei numeri interi pari (cioè della forma $2k$ con $k \in \mathbb{Z}$) è un anello commutativo senza unità rispetto alle ordinarie operazioni di somma e prodotto.

Osservazione 2.10.4

Sia $(\mathbf{A}, +, \cdot)$ un anello. Per ogni $a \in \mathbf{A}$, si ha $a \cdot 0 = 0 \cdot a = 0$.

Dimostrazione – Ricordiamo che abbiamo convenuto di indicare con 0 l'elemento neutro di \mathbf{A} rispetto alla somma. Si ha

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

da cui (sommando ad ambo i membri l'opposto di $a \cdot 0$) si ricava che $0 = a \cdot 0$. Allo stesso modo si trova che $0 \cdot a = 0$.

Osservazione 2.10.5

Sia $(\mathbf{A}, +, \cdot)$ un anello con unità. Si ha $1 \neq 0$

ossia, l'elemento neutro per il prodotto è necessariamente distinto dall'elemento neutro per la somma.

Dimostrazione – Se fosse $1 = 0$, per ogni $a \in \mathbf{A}$ sarebbe (in base all'osservazione 2.10.4)

$$a = a \cdot 1 = a \cdot 0 = 0$$

e dunque in \mathbf{A} esisterebbe solo l'elemento 0, contro l'ipotesi che \mathbf{A} sia un anello (e che dunque appartengano ad \mathbf{A} almeno due elementi).

Osservazione 2.10.6

Sia $(\mathbf{A}, +, \cdot)$ un anello con unità. Non esiste in \mathbf{A} l'inverso di 0.

Dimostrazione – Se $a \in \mathbf{A}$, è $a \cdot 0 = 0$ per l'osservazione 2.10.4, e dunque (per l'osservazione 2.10.5) non può essere $a \cdot 0 = 1$.

Osservazione 2.10.7

Sia $(\mathbf{A}, +, \cdot)$ un anello con unità. Si ha

$$(-1) \cdot (-1) = 1;$$

inoltre, per ogni $a \in \mathbf{A}$, si ha

$$(-1) \cdot a = -a.$$

Dimostrazione – Per l'osservazione 2.10.4 si ha (applicando la proprietà distributiva) $0 = 0 \cdot (-1) = (1 + (-1)) \cdot (-1) = 1 \cdot (-1) + (-1) \cdot (-1) = -1 + (-1) \cdot (-1)$ e dunque, sommando 1 ad ambo i membri, la prima parte dell'asserto. Inoltre, sempre applicando l'osservazione 2.10.4 e la proprietà distributiva,

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0$$

e, analogamente, $a + (-1) \cdot a = 0$, cosicché $(-1) \cdot a$ è l'opposto di a .

2.11 - Omomorfismi e isomorfismi tra anelli.

Siano $(\mathbf{A}, +, \cdot)$ e $(\mathbf{B}, \oplus, \odot)$ anelli.

Una funzione $\mathbf{f}: \mathbf{A} \rightarrow \mathbf{B}$ tale che $\mathcal{D}(\mathbf{f}) = \mathbf{A}$ si dice un *omomorfismo* tra $(\mathbf{A}, +, \cdot)$ e $(\mathbf{B}, \oplus, \odot)$ (o anche, più semplicemente, tra \mathbf{A} e \mathbf{B}) se

$$\mathbf{f}(\mathbf{x} + \mathbf{y}) = \mathbf{f}(\mathbf{x}) \oplus \mathbf{f}(\mathbf{y}) \quad \text{e} \quad \mathbf{f}(\mathbf{x} \cdot \mathbf{y}) = \mathbf{f}(\mathbf{x}) \odot \mathbf{f}(\mathbf{y}) \quad \forall \mathbf{x}, \mathbf{y} \in \mathbf{A}.$$

Un omomorfismo che sia anche una corrispondenza biunivoca si dice *isomorfismo*.

Esempio 2.11.1

Un esempio significativo di omomorfismo tra anelli sarà dato in 2.12 (teorema 2.12.11).

Esercizio [*] 2.11.2

Siano $(\mathbf{A}, +, \cdot)$ e $(\mathbf{B}, \oplus, \odot)$ anelli, e sia $\mathbf{f}: \mathbf{A} \rightarrow \mathbf{B}$ un isomorfismo tra \mathbf{A} e \mathbf{B} . Si dimostri che la funzione inversa $\mathbf{f}^{-1}: \mathbf{B} \rightarrow \mathbf{A}$ è un isomorfismo tra $(\mathbf{B}, \oplus, \odot)$ e $(\mathbf{A}, +, \cdot)$.

2.12 - L'anello \mathbb{Z}_n .

In tutta la sezione 2.12 supporremo fissato un numero intero positivo n .

Definiamo nell'insieme \mathbb{Z}_n delle classi di resto modulo n (cfr. sez. 0.8) due operazioni: le indicheremo con “+” e “·”, e le chiameremo rispettivamente *somma* e *prodotto*.

Se $[a], [b] \in \mathbb{Z}_n$, poniamo

$$[a] + [b] := [a + b]$$

e

$$[a] \cdot [b] := [a \cdot b].$$

Si noti che con lo stesso simbolo “+” abbiamo indicato a sinistra l'operazione che stiamo definendo in \mathbb{Z}_n e a destra la ben nota operazione di somma in \mathbb{Z} ; analogamente per il simbolo “·” (che, per di più, spesso si omette, proprio come in \mathbb{Z}). Ciò usualmente non dà luogo ad ambiguità né a confusione.

Si noti inoltre che abbiamo definito la “somma” (e il “prodotto”) di due classi di resto mediante la somma (o, rispettivamente, il prodotto) dei loro rappresentanti: poiché tali rappresentanti non sono univocamente determinati, è importante assicurarsi che la definizione sia “ben posta”, ossia dipenda solo dalle classi considerate e non dai rappresentanti scelti in esse (cfr., più avanti, l'esempio 2.12.2). Ciò avviene mediante il

Teorema 2.12.1

Siano $a, b, a', b' \in \mathbb{Z}$. Se $[a] = [a']$ e $[b] = [b']$, allora $[a + b] = [a' + b']$ e $[ab] = [a'b']$.

Dimostrazione – Per l'osservazione 0.7.2, se $[a] = [a']$ e $[b] = [b']$ deve essere

$$a \equiv a' \pmod{n} \quad \text{e} \quad b \equiv b' \pmod{n},$$

ossia devono esistere $h, k \in \mathbb{Z}$ tali che

$$a - a' = hn \quad \text{e} \quad b - b' = kn.$$

Allora

$$(a + b) - (a' + b') = (a - a') + (b - b') = hn + kn = (h + k)n$$

e dunque

$$a + b \equiv a' + b' \pmod{n}$$

ossia, ancora per l'osservazione 0.7.2, $[a + b] = [a' + b']$ come si voleva dimostrare.

Inoltre,

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a') = akn + b'hn = (ak + b'k)n$$

e dunque

$$ab \equiv a'b' \pmod{n}$$

ossia, ancora per l'osservazione 0.7.2, $[ab] = [a'b']$ come si voleva dimostrare.

Esempio 2.12.2

Sia $n = 3$.

Si ha $[2] = [5]$, tuttavia $[2^2] = [1] \neq [2] = [2^5]$. Non sarebbe dunque possibile definire, analogamente a come si è fatto per somma e prodotto, un "elevamento a potenza" in \mathbb{Z}_n ponendo $[a]^{[b]} := [a^b]$.

Analogamente, per $n = 5$, si ha $[3] = [8]$, tuttavia $[2^3] = [8] = [3] \neq [1] = [256] = [2^8]$.

Teorema 2.12.3

$(\mathbb{Z}_n, +)$ è un gruppo abeliano.

Dimostrazione – Proviamo in primo luogo che la somma in \mathbb{Z}_n è associativa. Se $[a], [b], [c]$ appartengono a \mathbb{Z}_n (con $a, b, c \in \mathbb{Z}$), si ha

$$\begin{aligned} ([a] + [b]) + [c] &= [a + b] + [c] = [(a + b) + c] = \\ &= [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]) \end{aligned}$$

perché la somma in \mathbb{Z} è associativa.

Si ha poi

$$[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a]$$

per ogni $[a] \in \mathbb{Z}_n$, e dunque $[0]$ è l'elemento neutro per la somma in \mathbb{Z}_n .

Se $[a] \in \mathbb{Z}_n$ (con $a \in \mathbb{Z}$), si ha $[a] + [-a] = [-a] + [a] = [0]$ e dunque $[-a]$ è l'opposto di $[a]$.

Proviamo infine che la somma in \mathbb{Z}_n è commutativa. Se $[a]$ e $[b]$ appartengono a \mathbb{Z}_n (con $a, b \in \mathbb{Z}$), si ha $[a] + [b] = [a + b] = [b + a] = [b] + [a]$ perché la somma in \mathbb{Z} è commutativa. L'asserto è così completamente provato.

Esercizio [*] 2.12.4

Si dimostri che $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo con unità.

Esempio 2.12.5

Sia $n = 6$.

Si ha $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$; dunque in \mathbb{Z}_6 non vale la legge di annullamento del prodotto.

Esempio 2.12.6

Sia $n = 4$.

Si ha $[2] \cdot [2] = [2 \cdot 2] = [4] = [0]$; dunque in \mathbb{Z}_4 l'elemento $[2] \neq 0$ ha per quadrato 0.

Esempio 2.12.7

Sia $n = 3$.

Il polinomio $x^3 + [2]x$ si annulla per ogni elemento di \mathbb{Z}_3 , ma non è il polinomio nullo.

Esempio 2.12.8

Sia $n = 6$.

Si ha $[4] = [4] \cdot [4] = [4] \cdot [4] \cdot [4] = [4] \cdot [4] \cdot \dots [4]$.

Esercizio 2.12.9

Sia $n = 6$.

Risolvere, se è possibile, le seguenti equazioni in \mathbb{Z}_6 nell'incognita x :

$$[3] \cdot x = [2];$$

$$[4] \cdot x = [2];$$

$$[5] \cdot x = [1];$$

$$x^2 = [2];$$

$$x^2 + [1] = [0];$$

$$[3] \cdot x = [3];$$

$$[4] \cdot x = [3];$$

$$[5] \cdot x = [2];$$

$$x^2 = [3];$$

$$x^2 + [2] = [0];$$

$$x^5 + [3] \cdot x^4 + x^3 + [3] \cdot x^2 + [4] \cdot x = [0].$$

Esercizio 2.12.10

Sia $n = 7$.

Risolvere, se è possibile, le seguenti equazioni in \mathbb{Z}_7 nell'incognita x :

$$\begin{aligned} [3] \cdot x &= [2]; \\ [3] \cdot x &= [3]; \\ [4] \cdot x &= [2]; \\ [4] \cdot x &= [3]; \\ [5] \cdot x &= [1]; \\ [5] \cdot x &= [2]; \\ x^2 &= [2]; \\ x^2 &= [3]; \\ x^2 + [1] &= [0]. \end{aligned}$$

Teorema 2.12.11

La proiezione canonica $\mathbb{Z} \rightarrow \mathbb{Z}_n$ è un omomorfismo fra anelli.

Dimostrazione – Siano $a, b \in \mathbb{Z}$. Si ha $[a + b] = [a] + [b]$ e $[ab] = [a][b]$ per definizione di somma e prodotto in \mathbb{Z}_n , e ciò prova l'asserto.

2.13 - I criteri di divisibilità per i numeri interi.

Come applicazione della teoria sviluppata nella sez. 2.12, dimostriamo i classici criteri di divisibilità per i numeri interi.

In tutta questa sezione, indichiamo con m un numero intero e con n un numero intero positivo. Ci proponiamo di stabilire condizioni necessarie e sufficienti affinché m sia divisibile per n , ossia (cfr. teorema 0.8.3 ed esercizio 0.8.4) affinché si abbia

$$m \equiv 0 \pmod{n}.$$

Poiché numeri opposti hanno gli stessi divisori, possiamo supporre che sia $m > 0$.

I nostri criteri faranno riferimento alle cifre della rappresentazione posizionale di m in base 10; sia dunque

$$m = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \dots + c_3 \cdot 10^3 + c_2 \cdot 10^2 + c_1 \cdot 10 + c_0.$$

Per ogni numero intero a , indicheremo con $[a]$ la classe di resto modulo n a cui appartiene a ; per il teorema 2.12.11, possiamo scrivere

$$(\star) \quad [m] = [c_k] \cdot [10]^k + [c_{k-1}] \cdot [10]^{k-1} + \dots + [c_3] \cdot [10]^3 + [c_2] \cdot [10]^2 + [c_1] \cdot [10] + [c_0].$$

Teorema 2.13.1

Sia c_0 l'ultima cifra di m . Si ha

$$m \equiv c_0 \pmod{2}$$

$$m \equiv c_0 \pmod{5}$$

e

$$m \equiv c_0 \pmod{10}.$$

Pertanto: m è divisibile per 2 sse l'ultima cifra di m è 0, 2, 4, 6 oppure 8; m è divisibile per 5 sse l'ultima cifra di m è 0 oppure 5; m è divisibile per 10 sse l'ultima cifra di m è 0.

Dimostrazione – Se $n = 2$ oppure $n = 5$ oppure $n = 10$, è $[10] = [0]$ e quindi dalla (★), ricordando l'osservazione 2.10.4, si ricava che

$$[m] = [c_0]$$

ossia (cfr. osservazione 0.7.2) $m \equiv c_0 \pmod{n}$.

Le uniche cifre divisibili per 2 sono 0, 2, 4, 6 e 8; le uniche cifre divisibili per 5 sono 0 e 5; e l'unica cifra divisibile per 10 è 0. L'asserto è così completamente provato.

Teorema 2.13.2

Siano c_2, c_1 e c_0 le ultime tre cifre di m . Si ha

$$m \equiv c_1 \cdot [10] + c_0 \pmod{4}$$

e

$$m \equiv c_2 \cdot [10]^2 + c_1 \cdot [10] + c_0 \pmod{8}.$$

Pertanto: m è divisibile per 4 sse è divisibile per 4 il numero formato dalle ultime due cifre di m ; m è divisibile per 8 sse è divisibile per 8 il numero formato dalle ultime tre cifre di m .

Dimostrazione – Dalla (★) si ricava che

$$\begin{aligned} [m] &= [h_0] \cdot [1000] + [c_2] \cdot [10]^2 + [c_1] \cdot [10] + [c_0] = \\ &= [h_1] \cdot [100] + [c_1] \cdot [10] + [c_0]. \end{aligned}$$

Se $n = 8$, è $[1000] = [0]$ e quindi (ricordando l'osservazione 2.10.4)

$$[m] = [c_2] \cdot [10]^2 + [c_1] \cdot [10] + [c_0];$$

Se $n = 4$, è $[100] = [0]$ e quindi (ricordando ancora l'osservazione 2.10.4)

$$[m] = [c_1] \cdot [10] + [c_0]$$

come si voleva.

Teorema 2.13.3

Sia m un numero intero, e siano $c_k, c_{k-1}, \dots, c_2, c_1$ e c_0 le cifre di m . Si ha

$$m \equiv (c_k + c_{k-1} + \dots + c_2 + c_1 + c_0) \pmod{3}$$

e

$$m \equiv (c_k + c_{k-1} + \dots + c_2 + c_1 + c_0) \pmod{9}$$

Pertanto: m è divisibile per 3 [risp.: per 9] sse è divisibile per 3 [risp.: per 9] la somma delle sue cifre.

Dimostrazione – Se $n = 3$ oppure $n = 9$, è $[10] = [1]$ e quindi dalla (★) si ricava che

$$\begin{aligned} [m] &= [c_k] \cdot [1]^k + [c_{k-1}] \cdot [1]^{k-1} + \dots + [c_2] \cdot [1]^2 + [c_1] \cdot [1] + [c_0] = \\ &= [c_k] + [c_{k-1}] + \dots + [c_2] + [c_1] + [c_0] = [c_k + c_{k-1} + \dots + c_2 + c_1 + c_0]. \end{aligned}$$

Dall'osservazione 0.7.2 segue l'asserto.

Osservazione 2.13.4

Sia $n = 9$.

Per il teorema 2.12.11, se $a = b + c$ allora è anche $[a] = [b] + [c]$; se $a = b - c$ allora è anche $[a] = [b] - [c]$; se $a = b \cdot c$ allora è anche $[a] = [b] \cdot [c]$; se $a = bq + r$ allora è anche $[a] = [b][q] + [r]$. Attenzione: non vale il viceversa!

Il teorema 2.13.3 giustifica la cosiddetta "prova del 9" per la somma, la sottrazione, la moltiplicazione e la divisione euclidea.

Esercizio 2.13.5

Sia $n = 9$.

Si trovino dei numeri interi a, b e c tali che $a \neq bq + r$ ma $[a] = [b][q] + [r]$, mostrando così che la "prova del 9" fornisce una condizione necessaria ma non sufficiente per l'esattezza del calcolo.

Esercizio [*] 2.13.6

Si enunci una "prova del 3" analoga a quella "del 9". Si può enunciare analogamente una "prova del 2"? E una "prova dell' 8"? E una "prova del 10"? E una "prova del 6"? Perché la più diffusa è la "prova del 9"?

Teorema 2.13.7

Siano $c_k, c_{k-1}, \dots, c_2, c_1$ e c_0 le cifre di m , e supponiamo k pari (ponendo $c_k := 0$ qualora m abbia un numero pari di cifre). Si ha

$$m \equiv (c_k - c_{k-1} + \dots + c_2 - c_1 + c_0) \pmod{11}$$

ossia $m \equiv (c_k + c_{k-2} + \dots + c_2 + c_0) - (c_{k-1} + c_{k-3} + \dots + c_1) \pmod{11}$.

Pertanto: m è divisibile per 11 sse è divisibile per 11 la differenza tra la somma delle sue cifre "di posto dispari" e la somma delle sue cifre "di posto pari".

Dimostrazione – Se $n = 11$ si ha $[10] = -[1]$, da cui (per il teorema 2.12.11)

$$[10]^h = -[1] \quad \text{se } h \text{ è dispari} \quad \text{e} \quad [10]^h = [1] \quad \text{se } h \text{ è pari.}$$

Ancora per il teorema 2.12.11, e ricordando che abbiamo scelto c_k in modo che k sia pari, dalla (★) si ricava che

$$\begin{aligned} [m] &= [c_k] \cdot [1]^k + [c_{k-1}] \cdot (-[1]) + \dots + [c_2] \cdot [1] + [c_1] \cdot (-[1]) + [c_0] = \\ &= [c_k] - [c_{k-1}] + \dots + [c_2] - [c_1] + [c_0] = [c_k - c_{k-1} + \dots + c_2 - c_1 + c_0]. \end{aligned}$$

Dall'osservazione 0.7.2 segue l'asserto.

3.- PRIME PROPRIETÀ DEI GRUPPI

3.1 - Notazioni.

Nei gruppi che considereremo da qui in avanti chiameremo di regola “prodotto” l’operazione, e la indicheremo senza un simbolo esplicito ma con la semplice giustapposizione degli elementi: questo anche quando considereremo contemporaneamente gruppi distinti, cosicché, ad esempio, il fatto che f sia un omomorfismo tra i gruppi \mathbf{G} e \mathbf{H} sarà espresso scrivendo

$$\mathbf{f}(g_1 g_2) = \mathbf{f}(g_1) \mathbf{f}(g_2) \quad \forall g_1, g_2 \in \mathbf{G}.$$

Coerentemente con questa convenzione, indicheremo con 1 (eventualmente: $1_{\mathbf{G}}$ nel caso in cui possano sorgere equivoci) l’elemento neutro di \mathbf{G} ; se $g \in \mathbf{G}$, il simmetrico di g sarà detto *inverso* di g e sarà indicato con g^{-1} .

Continueremo ad usare una notazione diversa per l’operazione del gruppo in tutti i casi in cui possano sorgere equivoci; va inoltre tenuto presente che per i gruppi abeliani l’operazione di solito si chiama somma e si indica col simbolo “+”: si dice in questo caso che *si usa la notazione additiva*; l’elemento neutro di \mathbf{G} si indica allora con 0 (eventualmente: $0_{\mathbf{G}}$ nel caso in cui possano sorgere equivoci) e il simmetrico di un elemento $g \in \mathbf{G}$ si dice *opposto* di g e si indica con $-g$. L’uso della notazione additiva comporta anche qualche diversa convenzione nelle notazioni che introdurremo più avanti: lo faremo presente caso per caso. Noi utilizzeremo la notazione additiva essenzialmente per i gruppi $(\mathbb{Z}, +)$ e $(\mathbb{Q}, +)$ e per quelli ottenuti a partire da essi.

Introduciamo anche una notazione standard sulla cardinalità di un gruppo \mathbf{G} : se \mathbf{G} ha infiniti elementi, diremo che \mathbf{G} è *un gruppo infinito* (nei casi che studiamo in questi appunti, non ci interesserà distinguere fra le varie possibili cardinalità di \mathbf{G}); se invece $|\mathbf{G}| = n$ con $n \in \mathbb{Z}^+$, diremo che \mathbf{G} è *un gruppo finito* (di *ordine* n).

3.2 - Le "leggi di cancellazione".

Teorema 3.2.1

Sia \mathbf{G} un gruppo, e siano $x, y, z \in \mathbf{G}$.

- Se $xz = yz$, allora $x = y$ (legge di "cancellazione a destra");
- se $zx = zy$, allora $x = y$ (legge di "cancellazione a sinistra").

Dimostrazione – Sia $xz = yz$. Moltiplicando a destra ambo i membri dell'uguaglianza per z^{-1} , si trova che $xzz^{-1} = yzz^{-1}$, cioè $x1 = y1$ e infine $x = y$ come si voleva.

Allo stesso modo si dimostra la legge di "cancellazione a sinistra".

Osservazione 3.2.2

Se in un monoide ogni elemento ha simmetrico (e quindi il monoide è un gruppo!), valgono le leggi di cancellazione, come si è visto col teorema 3.2.1; ma non vale il viceversa: cioè, se in un monoide valgono le leggi di cancellazione non è detto che ogni elemento abbia il simmetrico (e che quindi il monoide sia un gruppo). Si pensi a (\mathbb{Z}, \cdot) .

3.3 - Potenze di un elemento.

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$. Si pone $g^0 := 1$ e, induttivamente, per $n \in \mathbb{Z}^+$:

$$g^n := gg^{n-1}.$$

Teorema 3.3.1

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$. Per ogni scelta di $m, n \in \mathbb{N}$ si ha

- (a) $g^{m+n} = g^m g^n$;
- (b) $(g^m)^n = g^{mn}$.

Dimostrazione – Proviamo entrambe le affermazioni procedendo per induzione.

Consideriamo la (a), e procediamo per induzione su m . Per $m := 0$, si ha in effetti $g^{0+n} = g^n = 1g^n = g^0 g^n$. Supponiamo ora che, per l'ipotesi di induzione, sia $g^{(m-1)+n} = g^{m-1} g^n$.

Allora

$$g^{m+n} = gg^{(m+n)-1} = gg^{(m-1)+n} = gg^{m-1} g^n = g^m g^n.$$

Ora consideriamo la (b), e questa volta procediamo per induzione su n . Per $n := 0$, si ha in effetti $(g^m)^0 = 1 = g^0 = g^{m \cdot 0}$. Supponiamo ora che, per l'ipotesi di induzione, sia $(g^m)^{(n-1)} = g^{m(n-1)}$. Allora

$$(g^m)^n = g^m (g^m)^{(n-1)} = g^m g^{m(n-1)}$$

e quindi, tenendo conto della (a) (già dimostrata)

$$(g^m)^n = g^m g^{m(n-1)} = g^{m+m(n-1)} = g^{m+mn-m} = g^{mn}.$$

Che cosa possiamo dire delle potenze di g con esponente negativo? Ovviamente, per un minimo di coerenza notazionale, g^{-1} deve indicare l'inverso di g . Per esponenti interi minori di -1 ci soccorre il seguente risultato:

Teorema 3.3.2

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$. Per ogni $n \in \mathbb{N}$ si ha

$$(g^{-1})^n = (g^n)^{-1}.$$

Dimostrazione – L'uguaglianza è banalmente vera se $n = 0$, dunque possiamo dimostrarla per induzione su n . Supponiamo che sia $(g^{-1})^{n-1} = (g^{n-1})^{-1}$. Allora

$$(g^{-1})^n = g^{-1}(g^{-1})^{n-1} = g^{-1}(g^{n-1})^{-1} \stackrel{(2.5.9)}{=} (g^{n-1}g)^{-1} \stackrel{(3.3.1)}{=} (g^n)^{-1}$$

come si voleva.

Confortati dal teorema 3.3.2, porremo per $z \in \mathbb{Z}^+$

$$g^{-z} := (g^{-1})^z (= (g^z)^{-1}).$$

È facile adesso verificare che il teorema 3.3.2 vale per ogni $n \in \mathbb{Z}$. Se $n = -z$ con $z \in \mathbb{Z}^+$, si ha infatti

$$(g^{-1})^{-z} = \left((g^{-1})^{-1} \right)^z = g^z = \left((g^z)^{-1} \right)^{-1} = (g^{-z})^{-1}.$$

Lasciamo per esercizio la verifica che anche il teorema 3.3.1 si estende agli esponenti (tutti o in parte) negativi, cosicché vale il

Teorema 3.3.3

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$. Per ogni scelta di $m, n \in \mathbb{Z}$ si ha

- (a) $g^{m+n} = g^m g^n$;
- (b) $(g^m)^n = g^{mn}$.

Nel caso della notazione additiva (che, ricordiamo, si usa esclusivamente per i gruppi abeliani, e nemmeno sempre!) la nozione di *multiplo* di un elemento sostituisce quella di "potenza".

Si pone $0g := 0$ e, induttivamente, per $n \in \mathbb{Z}^+$:

$$ng := g + (n - 1)g.$$

Naturalmente, $(-1)g$ è $-g$, cioè l'opposto di g . Il teorema 3.3.3 diventa

Teorema 3.3.3 in notazione additiva

Sia $(\mathbf{G}, +)$ un gruppo, e sia $g \in \mathbf{G}$. Per ogni scelta di $m, n \in \mathbb{Z}$ si ha

- (a) $(m + n)g = mg + ng$;
- (b) $n(mg) = (nm)g$.

3.4 - Ancora sui sottogruppi.

Sia (\mathbf{G}, \cdot) un gruppo. Ricordiamo dalla sez. 2.8 che si dice *sottogruppo* di \mathbf{G} un sottoinsieme di \mathbf{G} chiuso rispetto a \cdot che sia un gruppo rispetto all'operazione indotta da \cdot .

Se \mathbf{S} è un sottogruppo di \mathbf{G} , si scrive

$$\mathbf{S} \leq \mathbf{G}.$$

Teorema 3.4.1

Siano \mathbf{G} un gruppo e \mathbf{H} un sottoinsieme non vuoto di \mathbf{G} . Sono fatti equivalenti:

- (i) $\mathbf{H} \leq \mathbf{G}$;
- (ii) comunque presi $x, y \in \mathbf{H}$, $xy^{-1} \in \mathbf{H}$;
- (iii) comunque presi $x, y \in \mathbf{H}$, $xy \in \mathbf{H}$; e comunque preso $x \in \mathbf{H}$, $x^{-1} \in \mathbf{H}$.

Dimostrazione – Proveremo il teorema mostrando che $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$ e $(iii) \Rightarrow (i)$.

Mostriamo che $(i) \Rightarrow (ii)$. Supponiamo che \mathbf{H} sia un sottogruppo di \mathbf{G} , e siano $x, y \in \mathbf{H}$. Poiché \mathbf{H} è un gruppo, esiste in \mathbf{H} l'inverso di y ; e per il teorema 2.8.3 esso coincide con l'inverso di y in \mathbf{G} , cioè con y^{-1} . Dunque appartengono a \mathbf{H} sia x che y^{-1} ; poiché \mathbf{H} è chiuso rispetto al prodotto, deve essere $xy^{-1} \in \mathbf{H}$, come si voleva.

Mostriamo che $(ii) \Rightarrow (iii)$. Supponiamo che valga la (ii) , e siano $x, y \in \mathbf{H}$; in primo luogo si osservi che deve essere $1 = xx^{-1} \in \mathbf{H}$; di conseguenza, $x^{-1} = 1x^{-1} \in \mathbf{H}$ e $y^{-1} = 1y^{-1} \in \mathbf{H}$. Ma allora deve esser anche $xy = x(y^{-1})^{-1} \in \mathbf{H}$.

Mostriamo infine che $(iii) \Rightarrow (i)$. Per la (iii) , \mathbf{H} è chiuso rispetto al prodotto, e certamente la restrizione del prodotto a \mathbf{H} è associativa. Poiché $\mathbf{H} \neq \emptyset$, esiste in \mathbf{H} un elemento x ; ma allora per la (iii) si ha $x^{-1} \in \mathbf{H}$ e dunque anche $1 = xx^{-1} \in \mathbf{H}$: l'unità di \mathbf{G} è dunque anche unità per \mathbf{H} . Per ogni $x \in \mathbf{H}$ la (iii) ci assicura poi che $x^{-1} \in \mathbf{H}$, e x^{-1} è inverso di x anche in \mathbf{H} (perché, come abbiamo provato, \mathbf{H} ha la stessa unità di \mathbf{G}).

Teorema 3.4.2

Sia \mathbf{G} un gruppo. Per ogni famiglia non vuota \mathcal{F} di sottogruppi di \mathbf{G} ,

$$\bigcap_{\mathbf{S} \in \mathcal{F}} \mathbf{S} \text{ è un sottogruppo di } \mathbf{G}.$$

Dimostrazione – Poniamo $\mathbf{S}_0 := \bigcap_{\mathbf{S} \in \mathcal{F}} \mathbf{S}$, e dimostriamo che \mathbf{S}_0 verifica la condizione (ii) del teorema 3.4.1. Siano $x, y \in \mathbf{S}_0$; allora $x, y \in \mathbf{S}$ per ogni $\mathbf{S} \in \mathcal{F}$. Poiché $\mathbf{S} \leq \mathbf{G}$, deve essere $xy^{-1} \in \mathbf{S}$ per la (ii) del teorema 3.4.1; poiché ciò deve avvenire per ogni \mathbf{S} in \mathcal{F} , possiamo concludere che $xy^{-1} \in \mathbf{S}_0$ come si voleva.

Osservazione 3.4.3

Lo stesso esempio considerato nell'osservazione 1.2.5 mostra che, in generale, l'unione di due sottogruppi può non essere un sottogruppo.

Sia \mathbf{G} un gruppo, e sia $\mathbf{X} \subset \mathbf{G}$. La famiglia dei sottogruppi di \mathbf{G} contenenti \mathbf{X} non è vuota, perché vi appartiene certamente \mathbf{G} . L'intersezione di tutti i sottogruppi di \mathbf{G} contenenti \mathbf{X} (che, per il teorema 3.4.2, è un sottogruppo di \mathbf{G}) si dice *sottogruppo di \mathbf{G} generato da \mathbf{X}* e si indica, quando non ci sia rischio di ambiguità, con $\langle \mathbf{X} \rangle$.

Osservazione 3.4.4

Sia \mathbf{G} un gruppo, e sia $\mathbf{X} \subset \mathbf{G}$. Il sottogruppo di \mathbf{G} generato da \mathbf{X} contiene \mathbf{X} ed è contenuto in ogni sottogruppo di \mathbf{G} contenente \mathbf{X} ; si dice anche che $\langle \mathbf{X} \rangle$ è *il minimo sottogruppo di \mathbf{G} contenente \mathbf{X}* .

Teorema 3.4.5

Sia \mathbf{G} un gruppo, e sia $\emptyset \neq \mathbf{X} \subset \mathbf{G}$. Il sottogruppo di \mathbf{G} generato da \mathbf{X} è l'insieme degli elementi di \mathbf{G} che si possono scrivere nella forma

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$$

con $k \in \mathbb{Z}^+$ (eventualmente $k = 1$), $\varepsilon_i \in \mathbb{Z}$ e gli x_i appartenenti a \mathbf{X} (non necessariamente distinti fra loro).

Dimostrazione – Sia \mathbf{S}_0 l'insieme degli elementi di \mathbf{G} che si possono scrivere nella forma descritta dall'enunciato del teorema. Per definizione di \mathbf{S}_0 , $\emptyset \neq \mathbf{X} \subset \mathbf{S}_0$; inoltre, tenendo conto dei teoremi 2.5.9 e 3.3.3, è immediato verificare che \mathbf{S}_0 verifica la condizione (iii) del teorema 3.4.1. Pertanto, \mathbf{S}_0 è un sottogruppo di \mathbf{G} contenente \mathbf{X} e dunque $\langle \mathbf{X} \rangle \subset \mathbf{S}_0$.

Viceversa, sia \mathbf{S} un sottogruppo di \mathbf{G} contenente \mathbf{X} ; allora ogni elemento di \mathbf{G} della forma descritta dall'enunciato del teorema deve appartenere a \mathbf{S} (per la (iii) del teorema 3.4.1), cosicché deve essere $\mathbf{S}_0 \subset \mathbf{S}$. Per l'arbitrarietà di \mathbf{S} , deve essere $\mathbf{S}_0 \subset \langle \mathbf{X} \rangle$ cosicché $\langle \mathbf{X} \rangle = \mathbf{S}_0$ e l'asserto è completamente provato.

Riveste particolare interesse il caso in cui $\mathbf{X} := \{g\}$ con $g \in \mathbf{G}$; si scrive di solito $\langle g \rangle$ anziché $\langle \{g\} \rangle$.

Teorema 3.4.6

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$. Allora

$$\langle g \rangle = \{x \in \mathbf{G} / x = g^n \text{ con } n \in \mathbb{Z}\}.$$

Dimostrazione – Segue immediatamente dal teorema 3.4.5 tenendo conto del teorema 3.3.3.

3.5 - Gruppi ciclici e loro proprietà.

Sia \mathbf{G} un gruppo. Si dice che \mathbf{G} è ciclico se esiste $g \in \mathbf{G}$ tale che $\mathbf{G} = \langle g \rangle$.

Osservazione 3.5.1

Ogni gruppo ciclico è un gruppo commutativo.

Dimostrazione – Sia $\mathbf{G} = \langle g \rangle$ un gruppo ciclico; siano $x, y \in \mathbf{G}$ e dimostriamo che $xy = yx$. Per il teorema 3.4.6, esistono $n_1, n_2 \in \mathbb{Z}$ tali che $x = g^{n_1}$ e $y = g^{n_2}$; allora, ricordando la (a) del teorema 3.3.3,

$$xy = g^{n_1}g^{n_2} = g^{n_1+n_2} = g^{n_2}g^{n_1} = yx .$$

Teorema 3.5.2

Sia $\mathbf{G} = \langle g \rangle$ un gruppo ciclico. Se per ogni $n \in \mathbb{Z}^+$ si ha $g^n \neq 1$, gli elementi g^n con $n \in \mathbb{Z}$ sono tutti distinti fra loro e \mathbf{G} è un gruppo infinito; in caso contrario, detto n_0 il minimo intero positivo tale che $g^{n_0} = 1$, si ha

$$\langle g \rangle = \{1, g, g^2, \dots, g^{n_0-1}\}$$

e dunque $|\mathbf{G}| = n_0$.

Dimostrazione – Supponiamo in primo luogo che per ogni $n \in \mathbb{Z}^+$ sia $g^n \neq 1$. Se ci fossero due numeri interi distinti n_1 e n_2 (con, per fissare le idee, $n_1 > n_2$) tali che $g^{n_1} = g^{n_2}$, sarebbe (ricordando il teorema 3.3.3)

$$1 = (g^{n_1})(g^{n_1})^{-1} = (g^{n_1})(g^{n_2})^{-1} = (g^{n_1})(g^{-n_2}) = g^{n_1-n_2}$$

con $n_1 - n_2 \in \mathbb{Z}^+$ (perché $n_1 > n_2$) contro quanto supposto. Dunque gli elementi g^n con $n \in \mathbb{Z}$ sono tutti distinti fra loro e \mathbf{G} ha infiniti elementi, come si voleva dimostrare.

Supponiamo ora che esista $\bar{n} \in \mathbb{Z}^+$ tale che $g^{\bar{n}} = 1$, e sia n_0 il minimo numero intero positivo tale che $g^{n_0} = 1$. Allora certamente gli elementi g^1, g^2, \dots, g^{n_0} sono tutti a due a due distinti fra loro: se fosse $g^{n_1} = g^{n_2}$ con $n_0 \geq n_1 > n_2 \geq 1$ si otterrebbe, come si è fatto sopra, che $1 = g^{n_1-n_2}$ con $0 < n_1 - n_2 < n_0$, assurdo per come si è scelto n_0 . Resta da verificare che $g^1, g^2, \dots, g^{n_0-1}$ e $1 (= g^{n_0})$ esauriscono gli elementi di \mathbf{G} . Ogni elemento di \mathbf{G} è della forma g^n con $n \in \mathbb{Z}$; detti q e r rispettivamente il quoziente e il resto della divisione euclidea di n per n_0 , si ha che

$$g^n = g^{qn_0+r} = (g^{n_0})^q g^r = 1^q g^r = g^r \quad \text{con } 0 \leq r < n_0$$

e quindi $g^n \in \{1, g, g^2, \dots, g^{n_0-1}\}$ come si voleva.

Questo risultato sarà precisato col teorema 5.2.3.

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$.

Se $\langle g \rangle$ ha per ordine un numero intero positivo n , si dice che g ha periodo n (oppure anche che g ha ordine n), e si scrive $o(g) = n$. Per il teorema 3.5.2, n è il minimo intero positivo tale che $g^n = 1$.

Se $\langle g \rangle$ è un gruppo infinito, si dice che g ha periodo infinito (oppure anche che g ha ordine infinito), e si scrive $o(g) = \infty$.

Teorema 3.5.3

Sia \mathbf{G} un gruppo, e sia $g \in \mathbf{G}$. Se $g^h = 1$ con $h \in \mathbb{Z}$, $o(g)$ divide h .

Dimostrazione – Siano rispettivamente q e r il quoziente e il resto della divisione euclidea di h per $o(g)$. Allora si ha, ricordando il teorema 3.3.3,

$$1 = g^h = g^{o(g) \cdot q + r} = (g^{o(g)})^q \cdot g^r = 1^q \cdot g^r = g^r.$$

Poiché $0 \leq r < o(g)$, e poiché $o(g)$ è il minimo intero positivo tale che $g^{o(g)} = 1$, deve essere $r = 0$.

Teorema 3.5.4

Sia \mathbf{G} un gruppo, sia $g \in \mathbf{G}$ e sia $o(g) = n$ con $n \in \mathbb{Z}^+$. Per ogni $k \in \mathbb{Z}^+$,

$$o(g^k) = \frac{n}{(k, n)}.$$

Dimostrazione – Si ha, ricordando la (b) del teorema 3.3.3,

$$(g^k)^{\frac{n}{(k, n)}} = g^{k \cdot \frac{n}{(k, n)}} = (g^n)^{\frac{k}{(k, n)}} = 1^{\frac{k}{(k, n)}} = 1$$

cosicché (per il teorema 3.5.3) $o(g^k)$ divide $\frac{n}{(k, n)}$. Resta da provare che $\frac{n}{(k, n)}$ divide $o(g^k)$.

Si ha

$$1 = (g^k)^{o(g^k)} = g^{k \cdot o(g^k)}$$

cosicché (sempre per il teorema 3.5.3) $n (= o(g))$ divide $k \cdot o(g^k)$ ossia esiste $n_1 \in \mathbb{Z}^+$ tale che

$$n_1 \cdot n = k \cdot o(g^k).$$

Possiamo dividere ambo i membri di questa uguaglianza per (k, n) ; ricordando che sia $\frac{n}{(k, n)}$ che $\frac{k}{(k, n)}$ sono numeri interi, si trova che

$$n_1 \cdot \frac{n}{(k, n)} = \frac{k}{(k, n)} \cdot o(g^k).$$

Dunque $\frac{n}{(k, n)}$ divide il prodotto $\frac{k}{(k, n)} \cdot o(g^k)$; poiché $\frac{n}{(k, n)}$ è primo con $\frac{k}{(k, n)}$, esso deve dividere $o(g^k)$ come si voleva dimostrare.

Teorema 3.5.5

Sia $\mathbf{G} = \langle g \rangle$ un gruppo ciclico. Allora

(1) ogni sottogruppo di \mathbf{G} è ciclico.

(2) Se \mathbf{G} è ciclico infinito, ogni sottogruppo di \mathbf{G} è ciclico infinito; se $|\mathbf{G}| = n$ con $n \in \mathbb{Z}^+$, per ogni divisore d di n esiste esattamente un sottogruppo di \mathbf{G} di ordine d , precisamente

$$\langle g^{\frac{n}{d}} \rangle.$$

(3) Se \mathbf{G} è ciclico infinito, g^k è generatore di \mathbf{G} se e soltanto se $k = \pm 1$; se $|\mathbf{G}| = n$ con $n \in \mathbb{Z}^+$, g^k è generatore di \mathbf{G} se e soltanto se $(k, n) = 1$.

Dimostrazione – Proviamo la (1).

Sia \mathbf{H} un sottogruppo di \mathbf{G} . Ogni elemento di \mathbf{H} è anche elemento di \mathbf{G} , e quindi è della forma g^k con $k \in \mathbb{Z}$; per la (iii) del teorema 3.4.1 e per il teorema 3.3.2, esiste in \mathbf{H} un elemento della forma g^k con $k \in \mathbb{Z}^+$. Sia k_0 il minimo intero positivo tale che $g^{k_0} \in \mathbf{H}$, e proviamo che $\mathbf{H} = \langle g^{k_0} \rangle$.

Per definizione di $\langle g^{k_0} \rangle$ è immediato che $\langle g^{k_0} \rangle \subset \mathbf{H}$, cosicché resta da provare che $\mathbf{H} \subset \langle g^{k_0} \rangle$. Sia g^k (con $k \in \mathbb{Z}$) un elemento di \mathbf{H} , e siano rispettivamente q e r il quoziente e il resto della divisione euclidea di k per k_0 . È

$$g^k = g^{k_0 q + r} = (g^{k_0})^q \cdot g^r$$

da cui

$$g^r = ((g^{k_0})^q)^{-1} \cdot g^k \in \mathbf{H}$$

con $0 \leq r < k_0$. Poiché k_0 è il minimo intero positivo tale che $g^{k_0} \in \mathbf{H}$, ne segue che $r = 0$ e quindi che $g^k = g^{k_0 q} = (g^{k_0})^q \in \langle g^{k_0} \rangle$. Per l'arbitrarietà di g^k in \mathbf{H} si è così provato che $\mathbf{H} \subset \langle g^{k_0} \rangle$ come si voleva.

Proviamo la (2).

Supponiamo in primo luogo che g abbia periodo infinito, e sia $\langle g^k \rangle$ (cfr. la (1), già dimostrata) un sottogruppo di $\langle g \rangle$. Se esistesse $n_0 \in \mathbb{Z}^+$ tale che $1 = (g^k)^{n_0} = g^{kn_0}$, g avrebbe periodo finito contro l'ipotesi; dunque anche g^k ha periodo infinito.

Se invece g ha periodo $n \in \mathbb{Z}^+$, sia d un divisore di n : per il teorema 3.5.4, il periodo di $g^{\frac{n}{d}}$ è $\frac{n}{(d, n)}$, cioè d (infatti se d è un divisore di n anche $\frac{n}{d}$ lo è, quindi $(\frac{n}{d}, n) = \frac{n}{d}$) e dunque $\langle g^{\frac{n}{d}} \rangle$ è un sottogruppo di $\langle g \rangle$ di ordine d ; resta da provare che è l'unico. Sia $\langle g^{k_0} \rangle$ (cfr. la (1), già dimostrata) un sottogruppo di $\langle g \rangle$ di ordine d . Allora

$$1 = (g^{k_0})^d = g^{k_0 d}$$

cosicché (per il teorema 3.5.3) $k_0 d = n_1 n$ con $n_1 \in \mathbb{Z}$. Ne segue che $k_0 = n_1 \frac{n}{d}$ e quindi

$$g^{k_0} = g^{n_1 \frac{n}{d}} = (g^{\frac{n}{d}})^{n_1} \in \langle g^{\frac{n}{d}} \rangle.$$

Ma allora $\langle g^{k_0} \rangle$ è (per definizione) contenuto in $\langle g^{\frac{n}{d}} \rangle$. Poiché $\langle g^{k_0} \rangle$ e $\langle g^{\frac{n}{d}} \rangle$ hanno lo stesso ordine d , essi necessariamente coincidono, come si voleva dimostrare.

Proviamo infine la (3).

Supponiamo in primo luogo che g abbia periodo infinito. Se g^k genera $\langle g \rangle$, deve esistere in particolare $x \in \mathbb{Z}$ tale che $(g^k)^x = g$, ossia $g^{kx} = g^1$, cioè (poiché gli elementi g^n con $n \in \mathbb{Z}$ sono tutti distinti fra loro, cfr. teorema 3.5.2)

$$kx = 1$$

e questa equazione nella x ha soluzione intera se e soltanto se $k = \pm 1$; d'altro lato è immediato che ciascuno degli elementi g^1 e g^{-1} (cioè g e il suo inverso) genera $\langle g \rangle$.

Se invece g ha periodo finito $n \in \mathbb{Z}^+$, g^k (con $k \in \mathbb{Z}$) è un generatore di $\langle g \rangle$ se e soltanto se ha anch'esso periodo n ; ma sappiamo dal teorema 3.5.4 che $o(g^k) = \frac{n}{(k, n)}$. Dunque g^k (con $k \in \mathbb{Z}$) è un generatore di $\langle g \rangle$ se e soltanto se $(k, n) = 1$, come si voleva dimostrare.

Esempio 3.5.6

Sia $n \in \mathbb{Z}^+$. L'insieme delle radici n -sime di 1 in \mathbb{C} è un gruppo ciclico finito di ordine n ; i suoi generatori si dicono *radici n -sime primitive* di 1.

Esempio 3.5.7

Sia $n \in \mathbb{Z}^+$, e sia \mathcal{P} un fissato n -gono regolare nel piano. L'insieme delle rotazioni che mutano \mathcal{P} in sé è un gruppo ciclico finito di ordine n .

Esempio 3.5.8

Sia $n \in \mathbb{Z}^+$, e sia \mathcal{P} un fissato n -gono regolare nel piano. L'insieme delle isometrie del piano che mutano \mathcal{P} in sé è un gruppo ma non è un gruppo ciclico.

Teorema 3.5.9

Se un gruppo non ha sottogruppi propri, esso è ciclico e il suo ordine è 1 oppure è un numero primo.

Dimostrazione – Sia \mathbf{G} un gruppo con più di un elemento che non ha sottogruppi propri. Scelto in \mathbf{G} un elemento $g \neq 1_{\mathbf{G}}$, poiché $\langle g \rangle$ è un sottogruppo di \mathbf{G} e $\langle g \rangle \neq \{1_{\mathbf{G}}\}$ deve essere $\langle g \rangle = \mathbf{G}$: dunque \mathbf{G} è ciclico. Posto $n := |\mathbf{G}|$, se n non fosse un numero primo avrebbe un divisore proprio d e in \mathbf{G} ci sarebbe (per la (2) del teorema 3.5.5) un sottogruppo di ordine $\frac{n}{d}$, cioè un sottogruppo proprio, contro la nostra ipotesi: dunque n è primo, come si voleva dimostrare.

4.- NORMALITÀ

4.1 - Classi laterali.

Siano \mathbf{G} un gruppo, $\mathbf{H} \leq \mathbf{G}$ e $g \in \mathbf{G}$. Si dice classe laterale destra di \mathbf{H} (in \mathbf{G}) individuata da g l'insieme $\mathbf{H}g$ (cfr. sez. 1.1).

Teorema 4.1.1

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Le classi laterali destre di \mathbf{H} in \mathbf{G} sono le classi di equivalenza rispetto alla relazione di equivalenza ϱ definita in \mathbf{G} ponendo

$$x\varrho y \Leftrightarrow xy^{-1} \in \mathbf{H}.$$

In particolare, le classi laterali destre di \mathbf{H} in \mathbf{G} sono una partizione di \mathbf{G} .

Dimostrazione – Proviamo in primo luogo che ϱ è una relazione di equivalenza in \mathbf{G} .

Essa è riflessiva: per ogni $x \in \mathbf{G}$, $xx^{-1} = 1 \in \mathbf{H}$ (perché $\mathbf{H} \leq \mathbf{G}$) e dunque $x\varrho x$.

Essa è simmetrica: siano $x, y \in \mathbf{G}$ tali che $x\varrho y$; allora $xy^{-1} \in \mathbf{H}$ e quindi (per la (iii) del teorema 3.4.1)

$$yx^{-1} = (xy^{-1})^{-1} \in \mathbf{H}$$

ossia $y\varrho x$.

Infine essa è transitiva: siano $x, y, z \in \mathbf{G}$ tali che $x\varrho y$ e $y\varrho z$; allora $xy^{-1} \in \mathbf{H}$ e $yz^{-1} \in \mathbf{H}$; poiché \mathbf{H} (in quanto sottogruppo di \mathbf{G}) deve essere chiuso rispetto al prodotto, ne segue che

$$xz^{-1} = (xy^{-1})(yz^{-1}) \in \mathbf{H}$$

ossia $x\varrho z$.

Proviamo ora che per ogni $g \in \mathbf{G}$ la classe di ϱ – equivalenza $[g]$ individuata da g (definita in 0.7) coincide con la classe laterale destra di \mathbf{H} in \mathbf{G} individuata da g .

Se $x \in [g]$, deve essere $x\varrho g$ ossia $xg^{-1} = h \in \mathbf{H}$; ne segue che $x = hg \in \mathbf{H}g$. Per l'arbitrarietà di x in $[g]$, si è provato che $[g] \subset \mathbf{H}g$.

Viceversa, sia $x \in \mathbf{H}g$; allora $x = hg$ con $h \in \mathbf{H}$; ne segue che $xg^{-1} = h \in \mathbf{H}$ ossia $x\varrho g$ e quindi $x \in [g]$. Per l'arbitrarietà di x in $\mathbf{H}g$, si è provato che $\mathbf{H}g \subset [g]$.

Che le classi laterali destre di \mathbf{H} in \mathbf{G} siano una partizione di \mathbf{G} segue a questo punto dall'osservazione 0.7.5.

Teorema 4.1.2

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Le classi laterali destre di \mathbf{H} in \mathbf{G} sono a due a due tutte equipotenti.

Dimostrazione – Basta provare che ogni classe laterale destra è equipotente a \mathbf{H} . Se $g \in \mathbf{H}$, la funzione $\varphi: \mathbf{H} \rightarrow \mathbf{H}g$ definita da

$$\varphi(h) := hg \quad \forall h \in \mathbf{H}$$

è iniettiva (per la legge di "cancellazione a destra", teorema 3.2.1) e suriettiva (per definizione di $\mathbf{H}g$), dunque è una corrispondenza biunivoca, come si voleva dimostrare.

Siano \mathbf{G} un gruppo, $\mathbf{H} \leq \mathbf{G}$ e $g \in \mathbf{G}$. Si dice classe laterale sinistra di \mathbf{H} (in \mathbf{G}) individuata da g l'insieme $g\mathbf{H}$ (cfr. sez. 1.1).

Valgono, con le corrispondenti dimostrazioni, gli analoghi per le classi laterali sinistre dei teoremi 4.1.1 e 4.1.2, cioè

Teorema 4.1.3

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Le classi laterali sinistre di \mathbf{H} in \mathbf{G} sono le classi di equivalenza rispetto alla relazione di equivalenza $\bar{\varrho}$ definita in \mathbf{G} ponendo

$$x\bar{\varrho}y \Leftrightarrow x^{-1}y \in \mathbf{H}.$$

In particolare, le classi laterali sinistre di \mathbf{H} in \mathbf{G} sono una partizione di \mathbf{G} .

Teorema 4.1.4

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Le classi laterali sinistre di \mathbf{H} in \mathbf{G} sono a due a due tutte equipotenti.

Poiché $1\mathbf{H} = \mathbf{H} = \mathbf{H}1$, dai teoremi 4.1.2 e 4.1.4 segue in particolare che ogni classe laterale destra di \mathbf{H} in \mathbf{G} è equipotente a ogni classe laterale sinistra di \mathbf{H} in \mathbf{G} , e dunque

Osservazione 4.1.5

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Tutte le classi laterali (destre e sinistre) di \mathbf{H} in \mathbf{G} sono a due a due equipotenti.

Teorema 4.1.6

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. L'insieme delle classi laterali destre di \mathbf{H} in \mathbf{G} è equipotente all'insieme delle classi laterali sinistre di \mathbf{H} in \mathbf{G} .

Dimostrazione – Dobbiamo costruire una corrispondenza biunivoca φ tra l'insieme delle classi laterali destre di \mathbf{H} in \mathbf{G} e l'insieme delle classi laterali sinistre di \mathbf{H} in \mathbf{G} . Poniamo

$$\varphi(\mathbf{H}g) := g^{-1}\mathbf{H} \quad \forall g \in \mathbf{G}.$$

La φ è ben definita, perché se $\mathbf{H}g_1 = \mathbf{H}g_2$ si ha $g_1g_2^{-1} \in \mathbf{H}$; ma $g_1g_2^{-1} = (g_1^{-1})^{-1}g_2^{-1}$: pertanto, dal fatto che $g_1g_2^{-1} \in \mathbf{H}$ segue che $g_1^{-1}\mathbf{H} = g_2^{-1}\mathbf{H}$.

Analogamente si vede che φ è iniettiva: da $\varphi(\mathbf{H}g_1) = \varphi(\mathbf{H}g_2)$, cioè $g_1^{-1}\mathbf{H} = g_2^{-1}\mathbf{H}$, segue $g_1g_2^{-1} = (g_1^{-1})^{-1}g_2^{-1} \in \mathbf{H}$ e quindi $\mathbf{H}g_1 = \mathbf{H}g_2$.

Infine, φ è suriettiva: ogni classe laterale sinistra di \mathbf{H} in \mathbf{G} è della forma $g\mathbf{H}$ con $g \in \mathbf{G}$ e quindi è immagine mediante φ della classe laterale destra $\mathbf{H}g^{-1}$ (ricordando che $(g^{-1})^{-1} = g$).

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si dice *indice di \mathbf{H} in \mathbf{G}* , e si denota con $|\mathbf{G} : \mathbf{H}|$, la cardinalità dell'insieme delle classi laterali destre di \mathbf{H} in \mathbf{G} (cioè dell'insieme quoziente di \mathbf{G} rispetto alla relazione di equivalenza definita nel teorema 4.1.1). Per il teorema 4.1.6, l'indice di \mathbf{H} in \mathbf{G} è anche la cardinalità dell'insieme delle classi laterali *sinistre* di \mathbf{H} in \mathbf{G} (cioè dell'insieme quoziente di \mathbf{G} rispetto alla relazione di equivalenza definita nel teorema 4.1.3).

Se esiste $n \in \mathbb{Z}^+$ tale che $|\mathbf{G} : \mathbf{H}| = n$, si dice che \mathbf{H} ha *indice finito in \mathbf{G}* ; in caso contrario, si dice che \mathbf{H} ha *indice infinito in \mathbf{G}* .

Esempio 4.1.7

Sia \mathbf{G} il gruppo di tutte le isometrie del piano e sia σ la simmetria assiale che ha per asse l'asse y . Sia $\mathbf{H} := \langle \sigma \rangle$, cosicché $\mathbf{H} = \{1, \sigma\}$ e tutte le classi laterali (destre e sinistre) di \mathbf{H} in \mathbf{G} sono formate da due elementi (per l'osservazione 4.1.5). Sia τ la traslazione che porta l'origine nel punto $\mathbf{A} \equiv (2, 0)$; le classi laterali (destra e sinistra) di \mathbf{H} in \mathbf{G} individuate da τ sono

$$\mathbf{H}\tau = \{\tau, \sigma\tau\} \quad \text{e} \quad \tau\mathbf{H} = \{\tau, \tau\sigma\}.$$

Si osservi che $\sigma\tau \neq \tau\sigma$ (e quindi $\mathbf{H}\tau \neq \tau\mathbf{H}$), perché $\sigma\tau$ lascia fermo il punto di coordinate $(1, 0)$ mentre $\tau\sigma$ lo trasforma nel punto di coordinate $(-3, 0)$.

Esempio 4.1.8

Sia \mathbf{G} il gruppo la cui rappresentazione tabulare è data nell'esempio 1.6.1 e sia $\mathbf{H} := \langle b \rangle$, cosicché $\mathbf{H} = \{1, b\}$ e tutte le classi laterali (destre e sinistre) di \mathbf{H} in \mathbf{G} sono formate da due elementi (per l'osservazione 4.1.5). Le classi laterali (destra e sinistra) di \mathbf{H} in \mathbf{G} individuate da a sono

$$\mathbf{H}a = \{a, a^2b\} \quad \text{e} \quad a\mathbf{H} = \{a, ab\}.$$

Si osservi che $\mathbf{H}a \neq a\mathbf{H}$ (perché $ab \neq a^2b$).

Esempio 4.1.9

Sia \mathbf{G} il gruppo la cui rappresentazione tabulare è data nell'esempio 1.6.1 e sia $\mathbf{H} := \langle a \rangle$, cosicché $\mathbf{H} = \{1, a, a^2\}$ e tutte le classi laterali (destre e sinistre) di \mathbf{H} in \mathbf{G} sono formate da tre elementi (per l'osservazione 4.1.5). Le classi laterali (destre e sinistre) di \mathbf{H} in \mathbf{G} sono:

$$\mathbf{H} = \mathbf{H}1 = \mathbf{H}a = \mathbf{H}a^2 = 1\mathbf{H} = a\mathbf{H} = a^2\mathbf{H} = \{1, a, a^2\};$$

$$\mathbf{H}b = \mathbf{H}ab = \mathbf{H}a^2b = b\mathbf{H} = ab\mathbf{H} = a^2b\mathbf{H} = \{b, ab, a^2b\}.$$

In questo caso, ciascuna classe laterale destra $\mathbf{H}x$ coincide con la corrispondente classe laterale sinistra $x\mathbf{H}$.

4.2 - Applicazione ai gruppi finiti.

Ricordiamo (cfr. sez. 3.1) che un gruppo \mathbf{G} si dice *finito* se esiste $n \in \mathbb{Z}^+$ tale che $|\mathbf{G}| = n$.

Teorema 4.2.1 (Lagrange)

Siano \mathbf{G} un gruppo finito e \mathbf{H} un sottogruppo di \mathbf{G} . Si ha

$$|\mathbf{G}| = |\mathbf{H}| \cdot |\mathbf{G} : \mathbf{H}|$$

e quindi, in particolare:

- (a) l'ordine di \mathbf{H} è un divisore dell'ordine di \mathbf{G} ;
- (b) l'indice di \mathbf{H} in \mathbf{G} è un divisore dell'ordine di \mathbf{G} e vale $\frac{|\mathbf{G}|}{|\mathbf{H}|}$.

Dimostrazione – Poiché (teorema 4.1.1) le classi laterali destre sono una partizione di \mathbf{G} , e poiché (teorema 4.1.2) ognuna di esse ha $|\mathbf{H}|$ elementi, l'asserto segue immediatamente dalla definizione di $|\mathbf{G} : \mathbf{H}|$.

Osservazione 4.2.2

Sia \mathbf{G} un gruppo finito. Se \mathbf{G} è ciclico, in base alla (2) del teorema 3.5.5. per ogni divisore d dell'ordine di \mathbf{G} esiste in \mathbf{G} un sottogruppo di ordine d . In generale, però, la condizione che un numero intero positivo d divida l'ordine di \mathbf{G} è necessaria (per il teorema di Lagrange) ma non sufficiente affinché esista in \mathbf{G} un sottogruppo di ordine d .

Teorema 4.2.3

Siano \mathbf{G} un gruppo finito, \mathbf{H} un sottogruppo di \mathbf{G} e \mathbf{K} un sottogruppo di \mathbf{H} (e quindi anche di \mathbf{G}). Si ha

$$|\mathbf{G} : \mathbf{K}| = |\mathbf{G} : \mathbf{H}| \cdot |\mathbf{H} : \mathbf{K}|.$$

Dimostrazione – Poiché

$$\frac{|\mathbf{G}|}{|\mathbf{K}|} = \frac{|\mathbf{G}|}{|\mathbf{H}|} \cdot \frac{|\mathbf{H}|}{|\mathbf{K}|}$$

l'asserto segue immediatamente dalla (b) del teorema 4.2.1.

4.3 - Sottogruppi normali.

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si dice che \mathbf{H} è un sottogruppo normale di \mathbf{G} , e si scrive

$$\mathbf{H} \triangleleft \mathbf{G}$$

se $\mathbf{H}g = g\mathbf{H} \quad \forall g \in \mathbf{G}$, cioè se ogni classe laterale destra di \mathbf{H} in \mathbf{G} coincide con la corrispondente classe laterale sinistra di \mathbf{H} in \mathbf{G} .

Osservazione 4.3.1

Sia \mathbf{G} un gruppo abeliano; allora $hg = gh$ comunque presi $h, g \in \mathbf{G}$ e dunque $\mathbf{H}g = g\mathbf{H}$ per ogni sottogruppo \mathbf{H} di \mathbf{G} e per ogni $g \in \mathbf{G}$, quindi ogni sottogruppo di \mathbf{G} è un sottogruppo normale di \mathbf{G} . Tuttavia esistono numerosi casi di sottogruppi normali in gruppi non abeliani (si veda l'esempio 4.1.9).

Osservazione 4.3.2

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Se $|\mathbf{G} : \mathbf{H}| = 2$, esistono esattamente due classi laterali destre per \mathbf{H} in \mathbf{G} , che devono essere \mathbf{H} e $\mathbf{G} \setminus \mathbf{H}$; e (per il teorema 4.1.6) esistono esattamente due classi laterali sinistre per \mathbf{H} in \mathbf{G} , che devono essere \mathbf{H} e $\mathbf{G} \setminus \mathbf{H}$. Dunque: ogni sottogruppo di indice 2 è un sottogruppo normale.

Osservazione 4.3.3

Siano \mathbf{G} un gruppo, $\mathbf{H}, \mathbf{K} \subset \mathbf{G}$ e $x \in \mathbf{G}$. Se $\mathbf{H} \subset \mathbf{K}$, allora $x\mathbf{H} \subset x\mathbf{K}$ e $\mathbf{H}x \subset \mathbf{K}x$; se $\mathbf{H} = \mathbf{K}$, allora $x\mathbf{H} = x\mathbf{K}$ e $\mathbf{H}x = \mathbf{K}x$.

Teorema 4.3.4

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Sono fatti equivalenti:

- (i) $\mathbf{H} \triangleleft \mathbf{G}$;
- (ii) $g^{-1}\mathbf{H}g \subset \mathbf{H} \quad \forall g \in \mathbf{G}$;
- (iii) $g^{-1}\mathbf{H}g = \mathbf{H} \quad \forall g \in \mathbf{G}$.

Dimostrazione – Proveremo il teorema mostrando che (i) \Rightarrow (ii), (ii) \Rightarrow (iii) e (iii) \Rightarrow (i).

Mostriamo che (i) \Rightarrow (ii). Supponiamo che sia $\mathbf{H} \triangleleft \mathbf{G}$, e sia $g \in \mathbf{G}$; dobbiamo provare che

$$g^{-1}hg \in \mathbf{H}.$$

Poiché $\mathbf{H} \triangleleft \mathbf{G}$, deve essere $\mathbf{H}g = g\mathbf{H}$; pertanto $hg \in \mathbf{H}g = g\mathbf{H}$ e dunque esiste $h_1 \in \mathbf{H}$ tale che $hg = gh_1$, da cui $g^{-1}hg = g^{-1}gh_1 = h_1 \in \mathbf{H}$ come si voleva.

Mostriamo che (ii) \Rightarrow (iii). Supponiamo che sia $g^{-1}\mathbf{H}g \subset \mathbf{H} \quad \forall g \in \mathbf{G}$, e sia $g_0 \in \mathbf{G}$; in sostanza, ci resta da provare che $\mathbf{H} \subset g_0^{-1}\mathbf{H}g_0$. Poiché $g_0^{-1} \in \mathbf{G}$, per la (ii) si ha

$$(g_0^{-1})^{-1}\mathbf{H}g_0^{-1} \subset \mathbf{H}$$

ossia

$$g_0\mathbf{H}g_0^{-1} \subset \mathbf{H}$$

da cui (moltiplicando ambo i membri a sinistra per g_0^{-1} e a destra per g_0)

$$\mathbf{H} \subset g_0^{-1}\mathbf{H}g_0$$

come si voleva.

Mostriamo infine che (iii) \Rightarrow (i). Supponiamo che sia $g^{-1}\mathbf{H}g = \mathbf{H} \quad \forall g \in \mathbf{G}$; moltiplicando ambo i membri dell'uguaglianza a sinistra per g , si trova che

$$\mathbf{H}g = g\mathbf{H} \quad \forall g \in \mathbf{G}$$

ma questo significa appunto che $\mathbf{H} \triangleleft \mathbf{G}$.

4.4 - Gruppo quoziente.

Siano \mathbf{G} un gruppo e $\mathbf{H} \triangleleft \mathbf{G}$. L'insieme delle classi laterali di \mathbf{H} in \mathbf{G} si indica con

$$\frac{\mathbf{G}}{\mathbf{H}}.$$

Teorema 4.4.1

Siano \mathbf{G} un gruppo e $\mathbf{H} \triangleleft \mathbf{G}$. Esiste in $\frac{\mathbf{G}}{\mathbf{H}}$ un'operazione \cdot in $\frac{\mathbf{G}}{\mathbf{H}}$ tale che

$$(\mathbf{H}x) \cdot (\mathbf{H}y) = \mathbf{H}xy$$

e $(\frac{\mathbf{G}}{\mathbf{H}}, \cdot)$ è un gruppo.

Dimostrazione – Bisogna in primo luogo provare che associando alla coppia $(\mathbf{H}x, \mathbf{H}y) \in \frac{\mathbf{G}}{\mathbf{H}} \times \frac{\mathbf{G}}{\mathbf{H}}$ l'elemento $\mathbf{H}xy$ di $\frac{\mathbf{G}}{\mathbf{H}}$ si ottiene effettivamente un'operazione in $\frac{\mathbf{G}}{\mathbf{H}}$. L'elemento $\mathbf{H}xy$ è infatti individuato dai rappresentanti x e y di $\mathbf{H}x$ e $\mathbf{H}y$; potrebbe accadere che scegliendo rappresentanti diversi (x_1 e y_1) per le stesse classi laterali il loro prodotto (x_1y_1) individuasse una diversa classe laterale di \mathbf{H} in \mathbf{G} (in tal caso si direbbe che l'operazione \cdot in $\frac{\mathbf{G}}{\mathbf{H}}$ non è ben definita).

Siano dunque $x_1, y_1 \in \mathbf{G}$ tali che $\mathbf{H}x_1 = \mathbf{H}x$ e $\mathbf{H}y_1 = \mathbf{H}y$; dobbiamo provare che $\mathbf{H}(x_1y_1) = \mathbf{H}(xy)$. In effetti,

$$\begin{aligned} (x_1y_1)(xy)^{-1} &= x_1y_1y^{-1}x^{-1} = x_1(x^{-1}x)y_1y^{-1}x^{-1} = (x_1x^{-1})x_1y_1y^{-1}x^{-1} = \\ &= (x_1x^{-1})\left((x^{-1})^{-1}(y_1y^{-1})x^{-1}\right) \end{aligned}$$

dove $(x^{-1})^{-1}(y_1y^{-1})x^{-1} \in \mathbf{H}$ per la (ii) del teorema 4.3.4 (essendo $y_1y^{-1} \in \mathbf{H}$) e quindi $(x_1y_1)(xy)^{-1} \in \mathbf{H}$ (ossia $\mathbf{H}(x_1y_1) = \mathbf{H}(xy)$, come si voleva dimostrare).

Resta da provare che $\frac{\mathbf{G}}{\mathbf{H}}$ è un gruppo rispetto a questa operazione. Verifichiamo che vale la proprietà associativa: se $\mathbf{H}x, \mathbf{H}y, \mathbf{H}z \in \frac{\mathbf{G}}{\mathbf{H}}$, si ha

$$((\mathbf{H}x)(\mathbf{H}y))(\mathbf{H}z) = (\mathbf{H}xy)(\mathbf{H}z) = \mathbf{H}xyz = (\mathbf{H}x)(\mathbf{H}yz) = (\mathbf{H}x)((\mathbf{H}y)(\mathbf{H}z)).$$

La classe laterale \mathbf{H} ($= \mathbf{H}1$) è l'elemento neutro di $\frac{\mathbf{G}}{\mathbf{H}}$; e infine è immediato verificare che ogni classe laterale $\mathbf{H}x$ ha per inverso la classe laterale $\mathbf{H}(x^{-1})$.

L'asserto è così completamente provato.

Il gruppo $\left(\frac{\mathbf{G}}{\mathbf{H}}, \cdot\right)$ di cui al teorema 4.4.1 si dice *gruppo quoziente di \mathbf{G} su \mathbf{H}* e il segno “ \cdot ” si omette, indicando l’operazione con la semplice giustapposizione (proprio come per \mathbf{G}).

Teorema 4.4.2

Siano \mathbf{G} un gruppo e $\mathbf{H} \triangleleft \mathbf{G}$. La funzione $\mathbf{f}: \mathbf{G} \rightarrow \frac{\mathbf{G}}{\mathbf{H}}$ definita ponendo

$$\mathbf{f}(g) := \mathbf{H}g \quad \forall g \in \mathbf{G}$$

è un epimorfismo di \mathbf{G} su $\frac{\mathbf{G}}{\mathbf{H}}$.

Dimostrazione – La \mathbf{f} è suriettiva per come è definito $\frac{\mathbf{G}}{\mathbf{H}}$. D’altra parte, se $x, y \in \mathbf{G}$,

$$\mathbf{f}(xy) = \mathbf{H}xy = (\mathbf{H}x)(\mathbf{H}y) = \mathbf{f}(x)\mathbf{f}(y)$$

per come è definito il prodotto in $\frac{\mathbf{G}}{\mathbf{H}}$.

L’epimorfismo di cui al teorema 4.4.2 si dice proiezione canonica di \mathbf{G} su $\frac{\mathbf{G}}{\mathbf{H}}$.

4.5 - Normalizzante.

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si dice *normalizzante* (o anche *normalizzatore*) di \mathbf{H} in \mathbf{G} l’insieme

$$\mathcal{N}_{\mathbf{G}}(\mathbf{H}) := \{x \in \mathbf{G} / x^{-1}\mathbf{H}x = \mathbf{H}\}.$$

Teorema 4.5.1

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si ha

$$\mathbf{H} \triangleleft \mathcal{N}_{\mathbf{G}}(\mathbf{H}) \leq \mathbf{G}$$

e per ogni sottogruppo \mathbf{K} di \mathbf{G} tale che $\mathbf{H} \triangleleft \mathbf{K}$ si ha

$$\mathbf{K} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{H}).$$

Dimostrazione – È immediato che $\mathbf{H} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{H})$, cosicché intanto $\mathcal{N}_{\mathbf{G}}(\mathbf{H}) \neq \emptyset$. Per provare che $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$ è un sottogruppo di \mathbf{G} , verifichiamo le condizioni (iii) del teorema 3.4.1. Siano $x, y \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$ e proviamo che $xy \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$. Si ha, ricordando il teorema 2.5.9,

$$(xy)^{-1}\mathbf{H}(xy) = (y^{-1}x^{-1})\mathbf{H}(xy) = y^{-1}(x^{-1}\mathbf{H}x)y = y^{-1}\mathbf{H}y = \mathbf{H}.$$

Sia $x \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$ e proviamo che $x^{-1} \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$. Moltiplicando ambo i membri della

$$x^{-1}\mathbf{H}x = \mathbf{H}$$

a sinistra per x e a destra per x^{-1} si ottiene la

$$\mathbf{H} = x\mathbf{H}x^{-1}$$

ossia

$$\mathbf{H} = (x^{-1})^{-1}\mathbf{H}x^{-1}$$

che esprime il fatto che $x^{-1} \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$.

Dunque $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$ è un sottogruppo di \mathbf{G} contenente \mathbf{H} ; è immediato che $\mathbf{H} \triangleleft \mathcal{N}_{\mathbf{G}}(\mathbf{H})$ perché, per definizione di $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$, risulta verificata la condizione (iii) del teorema 4.3.4.

Infine, se \mathbf{K} è un sottogruppo di \mathbf{G} tale che $\mathbf{H} \triangleleft \mathbf{K}$, ancora dalla condizione (iii) del teorema 4.3.4 segue che $\mathbf{K} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{H})$.

Teorema 4.5.2

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{K} \leq \mathbf{G}$. Si ha

$$\mathbf{H} \triangleleft \mathbf{K} \quad \text{se e soltanto se} \quad \mathbf{K} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{H});$$

$$\text{In particolare,} \quad \mathbf{H} \triangleleft \mathbf{G} \quad \text{se e soltanto se} \quad \mathcal{N}_{\mathbf{G}}(\mathbf{H}) = \mathbf{G}.$$

Dimostrazione – Basta confrontare la condizione (iii) del teorema 4.3.4 con la definizione di $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$.

4.6 - Centralizzante di un sottogruppo. Centro di un gruppo.

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si dice *centralizzante* di \mathbf{H} in \mathbf{G} l'insieme

$$\mathcal{C}_{\mathbf{G}}(\mathbf{H}) := \{g \in \mathbf{G} / g^{-1}hg = h \quad \forall h \in \mathbf{H}\}.$$

Teorema 4.6.1

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si ha

$$\mathcal{C}_{\mathbf{G}}(\mathbf{H}) \triangleleft \mathcal{N}_{\mathbf{G}}(\mathbf{H}).$$

Dimostrazione – È immediato $1_{\mathbf{G}} \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$, cosicché intanto $\mathcal{C}_{\mathbf{G}}(\mathbf{H}) \neq \emptyset$, e che $\mathcal{C}_{\mathbf{G}}(\mathbf{H}) \subset \mathcal{N}_{\mathbf{G}}(\mathbf{H})$. Per provare che $\mathcal{C}_{\mathbf{G}}(\mathbf{H})$ è un sottogruppo di $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$, basterà dunque verificare le condizioni (iii) del teorema 3.4.1.

Siano $x, y \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$ e proviamo che $xy \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$. Se $h \in \mathbf{H}$ si ha, ricordando il teorema 2.5.9,

$$(xy)^{-1}h(xy) = (y^{-1}x^{-1})h(xy) = y^{-1}(x^{-1}hx)y = y^{-1}hy = h.$$

Sia $x \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$ e proviamo che $x^{-1} \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$. Se $h \in \mathbf{H}$ si ha

$$x^{-1}hx = h$$

da cui, moltiplicando ambo i membri a sinistra per x e a destra per x^{-1} ,

$$h = xhx^{-1}$$

ossia

$$h = (x^{-1})^{-1}hx^{-1}$$

che esprime il fatto che $x^{-1} \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$.

Dunque $\mathcal{C}_{\mathbf{G}}(\mathbf{H})$ è un sottogruppo di $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$; per dimostrare che $\mathcal{C}_{\mathbf{G}}(\mathbf{H}) \triangleleft \mathcal{N}_{\mathbf{G}}(\mathbf{H})$ verifichiamo la condizione (iii) del teorema 4.3.4: siano $c \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$ e $n \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$ e proviamo che $n^{-1}cn \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$. In effetti, per ogni $h \in \mathbf{H}$ si ha

$$(n^{-1}cn)^{-1}h(n^{-1}cn) = (n^{-1}c^{-1}n)h(n^{-1}cn) = n^{-1}(c^{-1}(nhn^{-1})c)n.$$

Poiché $n \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$ (poiché $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$ è un sottogruppo) si ha che $nhn^{-1} \in \mathbf{H}$; poiché $c \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$ è allora

$$c^{-1}(nhn^{-1})c = nhn^{-1}$$

e dunque

$$(n^{-1}cn)^{-1}h(n^{-1}cn) = n^{-1}(c^{-1}(nhn^{-1})c)n = n^{-1}(nhn^{-1})n = (n^{-1}n)h(n^{-1}n) = h$$

cosicché $n^{-1}cn \in \mathcal{C}_{\mathbf{G}}(\mathbf{H})$ come si voleva.

Esercizio 4.6.2

Siano \mathbf{G} un gruppo e $\mathbf{H} \leq \mathbf{G}$. Si dimostri che: condizione necessaria e sufficiente affinché sia

$$\mathbf{H} \leq \mathcal{C}_{\mathbf{G}}(\mathbf{H})$$

è che \mathbf{H} sia un gruppo commutativo.

Sia \mathbf{G} un gruppo. Il centralizzante di \mathbf{G} in \mathbf{G} si dice *centro di \mathbf{G}* e si indica con $\mathbf{Z}(\mathbf{G})$.
Dunque

$$\mathbf{Z}(\mathbf{G}) := \{g \in \mathbf{G} / g^{-1}xg = x \quad \forall x \in \mathbf{G}\}.$$

Teorema 4.6.3

Sia \mathbf{G} un gruppo. Si ha

$$\mathbf{Z}(\mathbf{G}) \triangleleft \mathbf{G}.$$

Dimostrazione – Poiché $\mathcal{N}_{\mathbf{G}}(\mathbf{G}) = \mathbf{G}$, l'asserto è immediata conseguenza del teorema 4.6.1.

Esercizio 4.6.4

Sia \mathbf{G} un gruppo. Si dimostri che: se \mathbf{G} non è un gruppo commutativo (cioè se $\mathbf{Z}(\mathbf{G}) \neq \mathbf{G}$), il gruppo quoziente $\frac{\mathbf{G}}{\mathbf{Z}(\mathbf{G})}$ non è ciclico.

4.7 - Il coniugio. Automorfismi interni.

Siano \mathbf{G} un gruppo e $x, g \in \mathbf{G}$. Si dice *coniugato di x mediante g* l'elemento

$$x^g := g^{-1}xg.$$

Teorema 4.7.1

Siano \mathbf{G} un gruppo e $x, y, g \in \mathbf{G}$. Se y è il coniugato di x mediante g , allora x è il coniugato di y mediante g^{-1} .

Dimostrazione – Se $y = g^{-1}xg$, è immediato che

$$(g^{-1})^{-1}yg^{-1} \stackrel{\text{Teor. 1.7.1}}{=} gyg^{-1} = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1}) = x.$$

Siano \mathbf{G} un gruppo e $x, y \in \mathbf{G}$. Si dice che x, y sono *coniugati in \mathbf{G}* se esiste $g \in \mathbf{G}$ tale che y è il coniugato di x mediante g .

Teorema 4.7.2

Sia \mathbf{G} un gruppo. La relazione \sim in \mathbf{G} definita da

$$x \sim y \Leftrightarrow x, y \text{ sono coniugati in } \mathbf{G}$$

è una relazione di equivalenza in \mathbf{G} .

Dimostrazione – Dobbiamo provare che \sim è riflessiva, simmetrica e transitiva.

- \sim è riflessiva, cioè $x \sim x \forall x \in \mathbf{G}$; infatti $x = (1_{\mathbf{G}})^{-1}x(1_{\mathbf{G}})$;
- \sim è simmetrica per il teorema 4.7.1;
- \sim è transitiva, cioè $((x \sim y) \wedge (y \sim z)) \Rightarrow (x \sim z) \forall x, y, z \in \mathbf{G}$: supponiamo infatti che esistano $g, h \in \mathbf{G}$ tali che $y = g^{-1}xg$ e $z = h^{-1}yh$; allora

$$z = h^{-1}(g^{-1}xg)h = (h^{-1}g^{-1})x(gh) = (gh)^{-1}x(gh).$$

Teorema 4.7.3

Siano \mathbf{G} un gruppo e $g \in \mathbf{G}$. La funzione $\mathbf{f}_g: \mathbf{G} \rightarrow \mathbf{G}$ definita ponendo

$$\mathbf{f}_g(x) := x^g \quad \forall g \in \mathbf{G}$$

è un automorfismo di \mathbf{G} .

Dimostrazione – Proviamo in primo luogo che \mathbf{f}_g è un omomorfismo di \mathbf{G} in \mathbf{G} . Se $x, y \in \mathbf{G}$, si ha in effetti

$$\mathbf{f}_g(xy) := (xy)^g = (x1y)^g = (xgg^{-1}y)^g = g^{-1}(xgg^{-1}y)g = (g^{-1}xg)(g^{-1}yg) = x^g y^g = \mathbf{f}_g(x)\mathbf{f}_g(y).$$

Proviamo ora che \mathbf{f}_g è suriettiva: se $y \in \mathbf{G}$, sia x il coniugato di y mediante g^{-1} ; per il teorema 4.7.1 (tenendo conto del teorema 1.7.1), y è il coniugato di x mediante g , ossia y è l'immagine di x mediante \mathbf{f}_g .

Proviamo infine che \mathbf{f}_g è iniettiva. Siano $x, y \in \mathbf{G}$ tali che $\mathbf{f}_g(x) = \mathbf{f}_g(y)$; ciò significa che $x^g = y^g$, ossia che

$$g^{-1}xg = g^{-1}yg$$

da cui $x = y$ (come si voleva) per le leggi di cancellazione (teor. 3.2.1).

Sia \mathbf{G} un gruppo. Per ogni $g \in \mathbf{G}$, l'automorfismo di \mathbf{G} che a ogni $x \in \mathbf{G}$ associa x^g (cfr. teorema 4.7.3) si dice *automorfismo interno di \mathbf{G} individuato da g* .

5.- I TEOREMI DI OMOMORFISMO

5.1 - Nucleo di un omomorfismo.

Siano \mathbf{G} , \mathbf{H} gruppi, e sia \mathbf{f} un omomorfismo tra \mathbf{G} e \mathbf{H} . Si dice *nucleo* di \mathbf{f} , e si indica con

$$\mathbf{Ker f}$$

il sottoinsieme di \mathbf{G} definito da

$$\mathbf{Ker f} := \{g \in \mathbf{G} / \mathbf{f}(g) = 1\}.$$

Teorema 5.1.1

Siano \mathbf{G} , \mathbf{H} gruppi, e sia \mathbf{f} un omomorfismo tra \mathbf{G} e \mathbf{H} . Il nucleo di \mathbf{f} è un sottogruppo normale di \mathbf{G} .

Dimostrazione – Proviamo innanzitutto che $\mathbf{Ker f} \leq \mathbf{G}$ verificando la (iii) del teorema 3.4.1. Siano $x, y \in \mathbf{Ker f}$; allora $\mathbf{f}(x) = 1$, $\mathbf{f}(y) = 1$, e quindi

$$\mathbf{f}(xy) = \mathbf{f}(x)\mathbf{f}(y) = 11 = 1.$$

Inoltre, ricordando il teorema 2.9.1,

$$\mathbf{f}(x^{-1}) = (\mathbf{f}(x))^{-1} = 1^{-1} = 1$$

e dunque $x^{-1} \in \mathbf{Ker f}$.

Resta da provare che $\mathbf{Ker f} \triangleleft \mathbf{G}$ e lo facciamo verificando la (ii) del teorema 4.3.4. Siano $k \in \mathbf{Ker f}$ e $g \in \mathbf{G}$; allora (ricordando ancora il teorema 2.9.1)

$$\mathbf{f}(g^{-1}kg) = \mathbf{f}(g^{-1})\mathbf{f}(k)\mathbf{f}(g) = \mathbf{f}(g)^{-1}1\mathbf{f}(g) = \mathbf{f}(g)^{-1}\mathbf{f}(g) = 1$$

cosicché $g^{-1}kg \in \mathbf{Ker f}$ come si voleva dimostrare.

Teorema 5.1.2

Siano \mathbf{G}, \mathbf{H} gruppi. Un omomorfismo \mathbf{f} tra \mathbf{G} e \mathbf{H} è iniettivo (e quindi è un monomorfismo) se e soltanto se $\mathbf{Ker f} = \{1\}$.

Dimostrazione – Per il teorema 2.9.1, $\mathbf{f}(1) = 1$. Se \mathbf{f} è iniettiva, da $k \in \mathbf{Ker f}$ (cioè $\mathbf{f}(k) = 1$) segue $k = 1$, quindi $\mathbf{Ker f} = \{1\}$.

Viceversa, sia $\mathbf{Ker f} = \{1\}$. Se $x, y \in \mathbf{G}$ e si ha $\mathbf{f}(x) = \mathbf{f}(y)$,

$$1 = \mathbf{f}(x)(\mathbf{f}(x))^{-1} = \mathbf{f}(x)(\mathbf{f}(y))^{-1} = \mathbf{f}(xy^{-1})$$

ossia $xy^{-1} \in \mathbf{Ker f} = \{1\}$. Dunque $xy^{-1} = 1$ ossia $x = y$ e quindi, per l'arbitrarietà di x e y in \mathbf{G} , \mathbf{f} è iniettiva.

5.2 - Il primo teorema di omomorfismo fra gruppi.

Teorema 5.2.1

Siano \mathbf{G}, \mathbf{H} gruppi. Per ogni omomorfismo \mathbf{f} tra \mathbf{G} e \mathbf{H} , $\mathbf{f}(\mathbf{G})$ è un sottogruppo di \mathbf{H} .

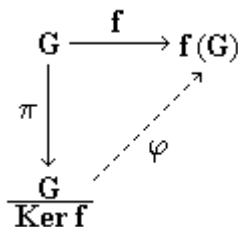
Dimostrazione – Poiché $\mathbf{f}(\mathbf{G})$ non è vuoto, basterà verificare la condizione (ii) del teorema 3.4.1. In effetti, se $\mathbf{f}(x), \mathbf{f}(y) \in \mathbf{f}(\mathbf{G})$, con $x, y \in \mathbf{G}$ si ha (ricordando il teorema 2.9.1)

$$\mathbf{f}(x) \cdot (\mathbf{f}(y))^{-1} = \mathbf{f}(x) \cdot \mathbf{f}(y^{-1}) = \mathbf{f}(xy^{-1}) \in \mathbf{f}(\mathbf{G})$$

come si voleva.

Teorema 5.2.2 ("Primo teorema di omomorfismo per i gruppi")

Siano \mathbf{G}, \mathbf{H} gruppi, e sia \mathbf{f} un omomorfismo tra \mathbf{G} e \mathbf{H} . Esiste un (unico) isomorfismo φ tra $\frac{\mathbf{G}}{\mathbf{Ker f}}$ e $\mathbf{f}(\mathbf{G})$ tale che, detta π la proiezione canonica di \mathbf{G} su $\frac{\mathbf{G}}{\mathbf{Ker f}}$, $\mathbf{f} = \varphi \circ \pi$ ossia, come anche si usa dire, tale che il diagramma



risulta commutativo.

Dimostrazione – Se esiste una funzione φ tra $\frac{\mathbf{G}}{\mathbf{Ker f}}$ e $\mathbf{f}(\mathbf{G})$ tale che $\mathbf{f} = \varphi \circ \pi$, deve essere

$$(*) \quad \varphi(\pi(g)) = \varphi((\mathbf{Ker f})g) = \mathbf{f}(g) \quad \forall g \in \mathbf{G}.$$

Proviamo innanzitutto che la (*) definisce effettivamente una funzione da $\frac{\mathbf{G}}{\mathbf{Ker f}}$ in $\mathbf{f}(\mathbf{G})$, cioè che $\mathbf{f}(g)$ dipende soltanto dalla classe laterale destra $(\mathbf{Ker f})g$: sia cioè $\bar{g} \in \mathbf{G}$ tale che

$$(\mathbf{Ker f})\bar{g} = (\mathbf{Ker f})g$$

e dimostriamo che $\mathbf{f}(\bar{g}) = \mathbf{f}(g)$. Per il teorema 4.1.1, se $(\mathbf{Ker f})\bar{g} = (\mathbf{Ker f})g$ deve essere $\bar{g}g^{-1} \in \mathbf{Ker f}$ ossia (ricordando il teorema 2.9.1)

$$1 = \mathbf{f}(\bar{g}g^{-1}) = \mathbf{f}(\bar{g})\mathbf{f}(g^{-1}) = \mathbf{f}(\bar{g})\mathbf{f}(g)^{-1}$$

e quindi $\mathbf{f}(\bar{g}) = \mathbf{f}(g)$ come si voleva.

Proviamo ora che la funzione φ definita dalla (*) è un omomorfismo. In effetti, se $g_1, g_2 \in \mathbf{G}$ si ha

$$\begin{aligned} \varphi(((\mathbf{Ker f})g_1)((\mathbf{Ker f})g_2)) &= \varphi((\mathbf{Ker f})(g_1g_2)) \stackrel{(*)}{=} \mathbf{f}(g_1g_2) = \\ &= \mathbf{f}(g_1)\mathbf{f}(g_2) \stackrel{(*)}{=} \varphi((\mathbf{Ker f})g_1)\varphi((\mathbf{Ker f})g_2) \end{aligned}$$

ricordando che \mathbf{f} è un omomorfismo.

Resta da provare che φ è suriettiva e iniettiva. Che sia suriettiva è immediato: ogni elemento di $\mathbf{f}(\mathbf{G})$ è della forma $\mathbf{f}(g_0)$ con $g_0 \in \mathbf{G}$, dunque proviene mediante φ da $(\mathbf{Ker f})g_0$. Per dimostrare che è iniettiva, supponiamo che sia

$$\varphi((\mathbf{Ker f})g_2) = \varphi((\mathbf{Ker f})g_1)$$

cioè (ricordando la (*))

$$\mathbf{f}(g_2) = \mathbf{f}(g_1).$$

Ne segue, moltiplicando a destra ambo i membri per $\mathbf{f}(g_2)^{-1}$ e ricordando il teorema 2.9.1, che

$$1 = \mathbf{f}(g_1)\mathbf{f}(g_2)^{-1} = \mathbf{f}(g_1g_2^{-1})$$

e dunque $g_1g_2^{-1} \in \mathbf{Ker f}$ ossia (per il teorema 4.1.1) $(\mathbf{Ker f})g_1 = (\mathbf{Ker f})g_2$ come si voleva.

Teorema 5.2.3

Sia \mathbf{G} un gruppo ciclico. Se \mathbf{G} è un gruppo infinito, \mathbf{G} è isomorfo al gruppo additivo $(\mathbb{Z}, +)$ dei numeri interi. Se $|\mathbf{G}| = n$ con $n \in \mathbb{Z}^+$, \mathbf{G} è isomorfo al gruppo additivo $(\mathbb{Z}_n, +)$ delle classi di resto modulo n .

Dimostrazione – Sia $\mathbf{G} = \langle g \rangle$. Sia $\mathbf{f}: \mathbb{Z} \rightarrow \mathbf{G}$ la funzione definita da

$$\mathbf{f}(n) := g^n \quad \forall n \in \mathbb{Z}.$$

Per la (a) del teorema 3.3.3, \mathbf{f} è un omomorfismo tra $(\mathbb{Z}, +)$ e (\mathbf{G}, \cdot) ; poiché \mathbf{G} è ciclico, \mathbf{f} è un epimorfismo. Per il teorema 3.5.2, se \mathbf{G} è un gruppo infinito \mathbf{f} è un isomorfismo; se invece $|\mathbf{G}| = n$ con $n \in \mathbb{Z}^+$, $\mathbf{Ker f} = n\mathbb{Z}$ e dunque, per il teorema 5.2.2, \mathbf{G} è isomorfo a $\frac{\mathbb{Z}}{n\mathbb{Z}}$ cioè al gruppo additivo \mathbb{Z}_n .

5.3 - Il teorema di corrispondenza.

Teorema 5.3.1 ("Teorema di corrispondenza")

Siano \mathbf{G} , \mathbf{H} gruppi, e sia \mathbf{f} un omomorfismo tra \mathbf{G} e \mathbf{H} . La funzione

$$\mathbf{S} \rightarrow \mathbf{f}(\mathbf{S})$$

che ad ogni sottoinsieme di \mathbf{G} associa la sua immagine mediante \mathbf{f} (e che senza equivoci può essere ancora indicata con \mathbf{f}) è una corrispondenza biunivoca tra l'insieme dei sottogruppi di \mathbf{G} contenenti $\mathbf{Ker f}$ e l'insieme dei sottogruppi di $\mathbf{f}(\mathbf{G})$; inoltre, se \mathbf{S} e \mathbf{T} sono sottogruppi di \mathbf{G} contenenti $\mathbf{Ker f}$, si ha che

$$(a) \mathbf{S} \subset \mathbf{T} \Leftrightarrow \mathbf{f}(\mathbf{S}) \subset \mathbf{f}(\mathbf{T})$$

$$(b) \mathbf{S} \triangleleft \mathbf{G} \Leftrightarrow \mathbf{f}(\mathbf{S}) \triangleleft \mathbf{f}(\mathbf{G}).$$

Dimostrazione – Prima di tutto proviamo la (a).

Sia $\mathbf{S} \subset \mathbf{T}$. Se $y \in \mathbf{f}(\mathbf{S})$, esiste $x \in \mathbf{S}$ tale che $y = \mathbf{f}(x)$; poiché $\mathbf{S} \subset \mathbf{T}$, è $x \in \mathbf{T}$ e dunque $y = \mathbf{f}(x) \in \mathbf{f}(\mathbf{T})$. Per l'arbitrarietà di y in $\mathbf{f}(\mathbf{S})$, si è provato che $\mathbf{f}(\mathbf{S}) \subset \mathbf{f}(\mathbf{T})$.

Viceversa, sia $\mathbf{f}(\mathbf{S}) \subset \mathbf{f}(\mathbf{T})$. Se $x \in \mathbf{S}$, $\mathbf{f}(x) = \mathbf{f}(t)$ per un opportuno $t \in \mathbf{T}$ e quindi

$$1_{\mathbf{H}} = \mathbf{f}(x)(\mathbf{f}(t))^{-1} = \mathbf{f}(xt^{-1})$$

ossia

$$xt^{-1} = k \in \mathbf{Ker f} \subset \mathbf{T}.$$

Ma allora $x = kt \in \mathbf{T}$. Per l'arbitrarietà di x in \mathbf{S} , si è così provato che $\mathbf{S} \subset \mathbf{T}$. La (a) è dunque completamente provata.

Per ogni sottogruppo \mathbf{S} di \mathbf{G} (in base al teorema 5.2.1, applicato alla restrizione di \mathbf{f} a \mathbf{S}) si ha che $\mathbf{f}(\mathbf{S})$ è un sottogruppo di \mathbf{H} (e quindi di $\mathbf{f}(\mathbf{G})$, essendo $\mathbf{f}(\mathbf{S}) \subset \mathbf{f}(\mathbf{G})$). In particolare, \mathbf{f} trasforma sottogruppi di \mathbf{G} contenenti $\mathbf{Ker f}$ in sottogruppi di $\mathbf{f}(\mathbf{G})$.

Per provare che \mathbf{f} è una corrispondenza biunivoca tra l'insieme dei sottogruppi di \mathbf{G} contenenti $\mathbf{Ker f}$ e l'insieme dei sottogruppi di $\mathbf{f}(\mathbf{G})$, dobbiamo mostrare che è iniettiva e suriettiva. Che sia iniettiva a questo punto è immediato: siano infatti \mathbf{S} e \mathbf{T} sottogruppi di \mathbf{G} contenenti $\mathbf{Ker f}$ tali che $\mathbf{f}(\mathbf{S}) = \mathbf{f}(\mathbf{T})$, ossia $\mathbf{f}(\mathbf{S}) \subset \mathbf{f}(\mathbf{T})$ e $\mathbf{f}(\mathbf{T}) \subset \mathbf{f}(\mathbf{S})$: applicando due volte la (a) si ottiene che $\mathbf{S} \subset \mathbf{T}$ e $\mathbf{T} \subset \mathbf{S}$, ossia che $\mathbf{S} = \mathbf{T}$.

Resta da dimostrare che ogni sottogruppo \mathbf{W} di $\mathbf{f}(\mathbf{G})$ è immagine mediante \mathbf{f} di un sottogruppo di \mathbf{G} contenente $\mathbf{Ker f}$. Sia dunque \mathbf{W} un sottogruppo di $\mathbf{f}(\mathbf{G})$: poniamo $\mathbf{S} := \mathbf{f}^{-1}(\mathbf{W})$ (cosicché $\mathbf{f}(\mathbf{S}) = \mathbf{W}$, cfr. osservazione 0.4.1) e proviamo che \mathbf{S} è un sottogruppo di \mathbf{G} contenente $\mathbf{Ker f}$. Se $k \in \mathbf{Ker f}$, $\mathbf{f}(k) = 1 \in \mathbf{W}$ e dunque $k \in \mathbf{f}^{-1}(\mathbf{W}) = \mathbf{S}$; pertanto $\mathbf{Ker f} \subset \mathbf{S}$. Sia poi $x, y \in \mathbf{S}$; ciò significa che $\mathbf{f}(x), \mathbf{f}(y) \in \mathbf{W}$ cosicché (ricordando il teorema 2.9.1 e la (ii) del teorema 3.4.1) $\mathbf{f}(xy^{-1}) = \mathbf{f}(x)(\mathbf{f}(y))^{-1} \in \mathbf{W}$ ossia $xy^{-1} \in \mathbf{S}$: applicando ancora il teorema 3.4.1, si conclude che \mathbf{S} è un sottogruppo di \mathbf{G} , come si voleva.

Dobbiamo infine dimostrare la (b), e lo facciamo utilizzando l'equivalenza fra la (i) e la (ii) del teorema 4.3.4. Sia $\mathbf{S} \triangleleft \mathbf{G}$ e proviamo che $\mathbf{f}(\mathbf{S}) \triangleleft \mathbf{f}(\mathbf{G})$; se $x \in \mathbf{f}(\mathbf{S})$ e $y \in \mathbf{f}(\mathbf{G})$, è $x = \mathbf{f}(s)$ con $s \in \mathbf{S}$ e $y = \mathbf{f}(g)$ con $g \in \mathbf{G}$ cosicché

$$y^{-1}xy = (\mathbf{f}(g))^{-1}\mathbf{f}(s)\mathbf{f}(g) = \mathbf{f}(g^{-1}sg).$$

Poiché $\mathbf{S} \triangleleft \mathbf{G}$, $g^{-1}sg \in \mathbf{S}$ e quindi $y^{-1}xy = \mathbf{f}(g^{-1}sg) \in \mathbf{f}(\mathbf{S})$; per l'arbitrarietà di x in $\mathbf{f}(\mathbf{S})$ e di y in $\mathbf{f}(\mathbf{G})$, possiamo concludere che $\mathbf{f}(\mathbf{S}) \triangleleft \mathbf{f}(\mathbf{G})$. Viceversa, sia $\mathbf{f}(\mathbf{S}) \triangleleft \mathbf{f}(\mathbf{G})$ e proviamo che $\mathbf{S} \triangleleft \mathbf{G}$, ricordando che $\mathbf{Ker} \mathbf{f} \subset \mathbf{S}$. Se $s \in \mathbf{S}$ e $g \in \mathbf{G}$, $\mathbf{f}(g^{-1}sg) = (\mathbf{f}(g))^{-1}\mathbf{f}(s)\mathbf{f}(g) \in \mathbf{f}(\mathbf{S})$ perché $\mathbf{f}(\mathbf{S}) \triangleleft \mathbf{f}(\mathbf{G})$; dunque esiste $s_0 \in \mathbf{S}$ tale che $\mathbf{f}(g^{-1}sg) = \mathbf{f}(s_0)$ e quindi

$$1 = (\mathbf{f}(g^{-1}sg))^{-1}\mathbf{f}(g^{-1}sg) = (\mathbf{f}(s_0))^{-1}\mathbf{f}(g^{-1}sg) = \mathbf{f}(s_0^{-1})\mathbf{f}(g^{-1}sg) = \mathbf{f}(s_0^{-1}g^{-1}sg)$$

ossia

$$s_0^{-1}g^{-1}sg = k \in \mathbf{Ker} \mathbf{f} \subset \mathbf{S}.$$

Se ne deduce che

$$g^{-1}sg = s_0k \in \mathbf{S}$$

e quindi, per l'arbitrarietà di s in \mathbf{S} e di g in \mathbf{G} , che $\mathbf{S} \triangleleft \mathbf{G}$. L'asserto è così completamente provato.

5.4 - Prodotto di sottogruppi.

Teorema 5.4.1

Sia \mathbf{G} un gruppo, e siano \mathbf{A}, \mathbf{B} sottogruppi di \mathbf{G} . Sono fatti equivalenti:

- (i) $\mathbf{AB} = \mathbf{BA}$;
- (ii) \mathbf{AB} è un sottogruppo di \mathbf{G} ;
- (iii) $\langle \mathbf{A}, \mathbf{B} \rangle = \mathbf{AB}$.

Dimostrazione –

(i) \Rightarrow (ii). Supponiamo che sia $\mathbf{AB} = \mathbf{BA}$ e proviamo che \mathbf{AB} è un sottogruppo di \mathbf{G} verificando la (ii) del teorema 3.4.1.

Siano $a_1b_1, a_2b_2 \in \mathbf{AB}$ (con $a_1, a_2 \in \mathbf{A}$ e $b_1, b_2 \in \mathbf{B}$) e proviamo che

$$(a_1b_1)(a_2b_2)^{-1} \in \mathbf{AB}.$$

Si ha

$$(a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}$$

dove $b_1b_2^{-1} \in \mathbf{B}$ (perché \mathbf{B} è un sottogruppo) e $a_2^{-1} \in \mathbf{A}$ (perché \mathbf{A} è un sottogruppo), cosicché $b_1b_2^{-1}a_2^{-1} \in \mathbf{BA} = \mathbf{AB}$, ossia $b_1b_2^{-1}a_2^{-1} = a_3b_3$ con $a_3 \in \mathbf{A}$ e $b_3 \in \mathbf{B}$; pertanto,

$$(a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = a_1a_3b_3 \in \mathbf{AB}$$

essendo $a_1a_3 \in \mathbf{A}$ perché \mathbf{A} è un sottogruppo.

(ii) \Rightarrow (iii). Si ha sempre $\mathbf{AB} \subset \langle \mathbf{A}, \mathbf{B} \rangle$ (per il teorema 3.4.5). Se vale la (ii) è però anche $\langle \mathbf{A}, \mathbf{B} \rangle \subset \mathbf{AB}$, per definizione di $\langle \mathbf{A}, \mathbf{B} \rangle$.

(iii) \Rightarrow (ii). Ovvio, essendo $\langle \mathbf{A}, \mathbf{B} \rangle$ un sottogruppo di \mathbf{G} (per il teorema 3.4.2).

(ii) \Rightarrow (i). Supponiamo che \mathbf{AB} sia un sottogruppo di \mathbf{G} . Dobbiamo provare che $\mathbf{AB} \subset \mathbf{BA}$ e che $\mathbf{BA} \subset \mathbf{AB}$: siano dunque $a \in \mathbf{A}$ e $b \in \mathbf{B}$, e proviamo che $ab \in \mathbf{BA}$ e $ba \in \mathbf{AB}$. Applicheremo ripetutamente la seconda parte della condizione (iii) del teorema 3.4.1.

Poiché deve essere $(ab)^{-1} \in \mathbf{AB}$, esistono $a_1 \in \mathbf{A}$ e $b_1 \in \mathbf{B}$ tali che $(ab)^{-1} = a_1 b_1$ e quindi (per il teorema 1.5.1) $ab = (a_1 b_1)^{-1} = b_1^{-1} a_1^{-1} \in \mathbf{BA}$, come si voleva. Poiché \mathbf{A} e \mathbf{B} sono sottogruppi di \mathbf{G} , è anche $a^{-1} \in \mathbf{A}$ e $b^{-1} \in \mathbf{B}$ cosicché $a^{-1} b^{-1} \in \mathbf{AB}$; poiché \mathbf{AB} è un sottogruppo di \mathbf{G} , deve essere $(a^{-1} b^{-1})^{-1} \in \mathbf{AB}$ ossia $ba \in \mathbf{AB}$, come si voleva.

Teorema 5.4.2

Sia \mathbf{G} un gruppo, e siano \mathbf{A}, \mathbf{B} sottogruppi di \mathbf{G} . Se $\mathbf{A} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$ (oppure $\mathbf{B} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{A})$), valgono le (i), (ii) e (iii) del teorema 5.4.1.

Dimostrazione – Supponiamo, per fissare le idee, che sia $\mathbf{A} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$ e proviamo che \mathbf{AB} è un sottogruppo di \mathbf{G} verificando la (ii) del teorema 3.4.1.

Siano $a_1 b_1, a_2 b_2 \in \mathbf{AB}$ (con $a_1, a_2 \in \mathbf{A}$ e $b_1, b_2 \in \mathbf{B}$) e proviamo che

$$(a_1 b_1)(a_2 b_2)^{-1} \in \mathbf{AB}.$$

Si ha

$$(a_1 b_1)(a_2 b_2)^{-1} = a_1 b_1 b_2^{-1} a_2^{-1} = a_1 (a_2^{-1} a_2) b_1 b_2^{-1} a_2^{-1} = (a_1 a_2^{-1})(a_2^{-1})^{-1} b_1 b_2^{-1} a_2^{-1}$$

dove $a_1 a_2^{-1} \in \mathbf{A}$ (perché \mathbf{A} è un sottogruppo), $b_1 b_2^{-1} \in \mathbf{B}$ (perché \mathbf{B} è un sottogruppo) e $(a_2^{-1})^{-1} b_1 b_2^{-1} a_2^{-1} \in \mathbf{B}$ (perché $\mathbf{A} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$), cosicché $(a_1 a_2^{-1})(a_2^{-1})^{-1} b_1 b_2^{-1} a_2^{-1} \in \mathbf{AB}$ come si voleva dimostrare.

Osservazione 5.4.3

Il teorema 5.4.2 non è invertibile, cioè se per due sottogruppi \mathbf{A}, \mathbf{B} di un gruppo \mathbf{G} valgono le (i), (ii) e (iii) del teorema 5.4.1 può darsi che non sia né $\mathbf{A} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$ né $\mathbf{B} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{A})$.

Siano ad esempio $\mathbf{G} := \mathbf{S}_3$ (il gruppo di tutte le permutazioni sull'insieme $\{1, 2, 3\}$), $\mathbf{A} := \langle (1\ 2\ 3\ 4), (1\ 3) \rangle = \{\mathbf{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (1\ 4)(2\ 3), (2\ 4), (1\ 2)(3\ 4)\}$, $\mathbf{B} := \langle (1\ 2\ 3) \rangle = \{\mathbf{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Allora $\mathbf{AB} = \mathbf{G}$, ma $\mathbf{A} \not\leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$ (perché $(2\ 4)(1\ 2\ 3)(2\ 4) = (1\ 4\ 3) \notin \mathbf{B}$) e $\mathbf{B} \not\leq \mathcal{N}_{\mathbf{G}}(\mathbf{A})$ (perché $(1\ 3\ 2)(1\ 2\ 3\ 4)(1\ 2\ 3) = (1\ 4\ 2\ 3) \notin \mathbf{A}$).

5.5 - Il secondo teorema di omomorfismo fra gruppi.

Teorema 5.5.1

Sia \mathbf{G} un gruppo, e siano \mathbf{A}, \mathbf{B} sottogruppi di \mathbf{G} . Se $\mathbf{A} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$, si ha che

- (a) \mathbf{AB} è un sottogruppo di \mathbf{G} ;
- (b) $\mathbf{B} \triangleleft \mathbf{AB}$;
- (c) $\mathbf{A} \cap \mathbf{B} \triangleleft \mathbf{A}$;
- (d) la funzione $a(\mathbf{A} \cap \mathbf{B}) \rightarrow a\mathbf{B}$ è un isomorfismo tra $\frac{\mathbf{A}}{\mathbf{A} \cap \mathbf{B}}$ e $\frac{\mathbf{AB}}{\mathbf{B}}$.

Dimostrazione – La (a) segue dal teorema 5.4.2; poiché banalmente $\mathbf{B} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$, si ha che $\mathbf{AB} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{B})$ e quindi la (b). Per provare la (c) e la (d) basterà mostrare che la restrizione π ad \mathbf{A} della proiezione canonica di \mathbf{AB} su $\frac{\mathbf{AB}}{\mathbf{B}}$ ha nucleo $\mathbf{A} \cap \mathbf{B}$ e applicare il teorema 5.2.2.

Se $x \in \mathbf{A} \cap \mathbf{B}$ è in particolare $x \in \mathbf{B}$ e dunque $\pi(x) = x\mathbf{B} = \mathbf{B}$ ossia $x \in \mathbf{Ker} \pi$, dunque $\mathbf{A} \cap \mathbf{B} \subset \mathbf{Ker} \pi$.

Viceversa, sia $x \in \mathbf{Ker} \pi$: poiché il dominio di π è \mathbf{A} , deve essere $x \in \mathbf{A}$; poiché $\mathbf{B} = \pi(x) = x\mathbf{B}$, deve essere $x \in \mathbf{B}$. Pertanto $x \in \mathbf{A} \cap \mathbf{B}$ e dunque $\mathbf{Ker} \pi \subset \mathbf{A} \cap \mathbf{B}$.

Si è così provato che $\mathbf{Ker} \pi = \mathbf{A} \cap \mathbf{B}$, da cui la (c) per il teorema 5.1.1. Dal teorema 5.2.2 segue infine la (d).

5.6 - Il gruppo degli automorfismi di un gruppo. Il sottogruppo degli automorfismi interni.

Teorema 5.6.1

Sia \mathbf{G} un gruppo. L'insieme $\mathbf{Aut}(\mathbf{G})$ degli automorfismi di \mathbf{G} è un sottogruppo del gruppo $\mathbf{Sym}(\mathbf{G})$ di tutte le permutazioni su \mathbf{G} . L'insieme $\mathbf{Inn}(\mathbf{G})$ degli automorfismi interni di \mathbf{G} (cfr. sez. 4.7) è un sottogruppo di $\mathbf{Aut}(\mathbf{G})$.

Dimostrazione – Per definizione, $\mathbf{Aut}(\mathbf{G}) \subset \mathbf{Sym}(\mathbf{G})$, e $\mathbf{Aut}(\mathbf{G})$ non è vuoto perché $\mathbf{id}_{\mathbf{G}}$ (cfr. sez. 0.4) è certamente un automorfismo di \mathbf{G} ; quindi basterà verificare la (iii) del teorema 3.4.1.

Siano $\alpha, \beta \in \mathbf{Aut}(\mathbf{G})$; per dimostrare che $\beta \circ \alpha \in \mathbf{Aut}(\mathbf{G})$, per quanto già osservato nell'esempio 1.2.3 basterà mostrare che comunque presi $x, y \in \mathbf{G}$ si ha

$$(\beta \circ \alpha)(xy) = (\beta \circ \alpha)(x)(\beta \circ \alpha)(y).$$

In effetti,

$$(\beta \circ \alpha)(xy) = \beta(\alpha(xy)) = \beta(\alpha(x)\alpha(y)) = \beta(\alpha(x))\beta(\alpha(y)) = (\beta \circ \alpha)(x)(\beta \circ \alpha)(y)$$

come appunto si voleva.

Che l'inverso di un automorfismo di \mathbf{G} sia anch'esso un automorfismo di \mathbf{G} è conseguenza immediata del teorema 2.9.3. Si è così completamente provato che $\mathbf{Aut}(\mathbf{G})$ è un sottogruppo di $\mathbf{Sym}(\mathbf{G})$.

Si applica ancora il teorema 3.4.1 per verificare che $\mathbf{Inn}(\mathbf{G})$ (che certamente non è vuoto) è un sottogruppo di $\mathbf{Aut}(\mathbf{G})$. È infatti una facile verifica controllare che, comunque presi $x, y \in \mathbf{G}$, la composizione degli automorfismi interni individuati da x e y coincide con l'automorfismo interno individuato da xy , e l'inverso dell'automorfismo interno individuato da x coincide con l'automorfismo interno individuato da x^{-1} .

Esercizio 5.6.2

Sia \mathbf{G} un gruppo. Dimostrare che $\mathbf{Inn}(\mathbf{G}) \triangleleft \mathbf{Aut}(\mathbf{G})$.

Teorema 5.6.3

Sia \mathbf{G} un gruppo. $\mathbf{Inn}(\mathbf{G})$ è isomorfo a $\frac{\mathbf{G}}{\mathbf{Z}(\mathbf{G})}$.

Dimostrazione – Questo fatto è conseguenza pressoché immediata del primo teorema di omomorfismo (teorema 5.2.2). Sia infatti $\mathbf{f}: \mathbf{G} \rightarrow \mathbf{Inn}(\mathbf{G})$ la funzione che a ogni $g \in \mathbf{G}$ associa l'automorfismo interno di \mathbf{G} da lui individuato; per definizione di $\mathbf{Inn}(\mathbf{G})$, $\mathbf{f}(\mathbf{G}) = \mathbf{Inn}(\mathbf{G})$ e quindi per poter dedurre il nostro asserto dal teorema 5.2.2 dobbiamo soltanto verificare che $\mathbf{Ker f} = \mathbf{Z}(\mathbf{G})$. In effetti, si ha $g \in \mathbf{Ker f}$ se e soltanto se $x^g = x \forall x \in \mathbf{G}$, cioè se e soltanto se $g \in \mathbf{Z}(\mathbf{G})$ (cfr. sez. 4.6).

6.- PRODOTTO DIRETTO DI GRUPPI

6.1 - Definizione e prime proprietà.

Siano \mathbf{H} , \mathbf{K} gruppi. Si dice *prodotto diretto di \mathbf{H} per \mathbf{K}* il prodotto cartesiano $\mathbf{H} \times \mathbf{K}$ con l'operazione definita ponendo

$$(h_1, k_1)(h_2, k_2) := (h_1 h_2, k_1 k_2).$$

Teorema 6.1.1

Siano \mathbf{H} , \mathbf{K} gruppi. Il prodotto diretto di \mathbf{H} per \mathbf{K} è un gruppo; posto

$$\bar{\mathbf{H}} := \{(h, k) \in \mathbf{H} \times \mathbf{K} / k = 1_{\mathbf{K}}\} \quad \text{e} \quad \bar{\mathbf{K}} := \{(h, k) \in \mathbf{H} \times \mathbf{K} / h = 1_{\mathbf{H}}\}$$

si ha che

- $\bar{\mathbf{H}}$ è isomorfo a \mathbf{H} ;
- $\bar{\mathbf{K}}$ è isomorfo a \mathbf{K} ;
- (a) $\bar{\mathbf{H}} \triangleleft \mathbf{H} \times \mathbf{K}$;
- (b) $\bar{\mathbf{K}} \triangleleft \mathbf{H} \times \mathbf{K}$;
- (c) $\bar{\mathbf{H}} \cap \bar{\mathbf{K}} = \{1_{\mathbf{H} \times \mathbf{K}}\}$;
- (d) $\mathbf{H} \times \mathbf{K} = \bar{\mathbf{H}} \bar{\mathbf{K}}$;

(e) ogni elemento di $\mathbf{H} \times \mathbf{K}$ si esprime in uno e un sol modo come prodotto di un elemento di $\bar{\mathbf{H}}$ e un elemento di $\bar{\mathbf{K}}$;

(f) $(h, 1_{\mathbf{K}})(1_{\mathbf{H}}, k) = (1_{\mathbf{H}}, k)(h, 1_{\mathbf{K}})$ per ogni $(h, 1_{\mathbf{K}}) \in \bar{\mathbf{H}}$, $(1_{\mathbf{H}}, k) \in \bar{\mathbf{K}}$.

Dimostrazione – L'operazione definita in $\mathbf{H} \times \mathbf{K}$ è associativa perché se $h_1, h_2, h_3 \in \mathbf{H}$ e $k_1, k_2, k_3 \in \mathbf{K}$ si ha

$$\begin{aligned} ((h_1, k_1)(h_2, k_2))(h_3, k_3) &= ((h_1 h_2, k_1 k_2))(h_3, k_3) = ((h_1 h_2)h_3, (k_1 k_2)k_3) = \\ &= (h_1(h_2 h_3), k_1(k_2 k_3)) = (h_1, k_1)((h_2 h_3, k_2 k_3)) = (h_1, k_1)((h_2, k_2)(h_3, k_3)). \end{aligned}$$

L'elemento $(1_{\mathbf{H}}, 1_{\mathbf{K}})$ è l'elemento neutro di $\mathbf{H} \times \mathbf{K}$, perché se $h \in \mathbf{H}$ e $k \in \mathbf{K}$ si ha

$$(h, k)(1_{\mathbf{H}}, 1_{\mathbf{K}}) = (h1_{\mathbf{H}}, k1_{\mathbf{K}}) = (h, k)$$

e

$$(1_{\mathbf{H}}, 1_{\mathbf{K}})(h, k) = (1_{\mathbf{H}}h, 1_{\mathbf{K}}k) = (h, k).$$

Infine, se $h \in \mathbf{H}$ e $k \in \mathbf{K}$, l'inverso di (h, k) è (h^{-1}, k^{-1}) perché

$$(h, k)(h^{-1}, k^{-1}) = (hh^{-1}, kk^{-1}) = (1_{\mathbf{H}}, 1_{\mathbf{K}})$$

e

$$(h^{-1}, k^{-1})(h, k) = (h^{-1}h, k^{-1}k) = (1_{\mathbf{H}}, 1_{\mathbf{K}}).$$

È immediato verificare che la funzione che ad ogni $h \in \mathbf{H}$ associa l'elemento $(h, 1_{\mathbf{K}})$ di $\overline{\mathbf{H}}$ è un isomorfismo tra \mathbf{H} e $\overline{\mathbf{H}}$, e che la funzione che ad ogni $k \in \mathbf{K}$ associa l'elemento $(1_{\mathbf{H}}, k)$ di $\overline{\mathbf{K}}$ è un isomorfismo tra \mathbf{K} e $\overline{\mathbf{K}}$.

Proviamo la (a) verificando la condizione (ii) del teorema 4.3.4. Se $(h_0, 1_{\mathbf{K}}) \in \overline{\mathbf{H}}$ e $(h, k) \in \mathbf{H} \times \mathbf{K}$, si ha infatti

$$(h, k)^{-1}(h_0, 1_{\mathbf{K}})(h, k) = (h^{-1}, k^{-1})(h_0, 1_{\mathbf{K}})(h, k) = (h^{-1}h_0h, k^{-1}1_{\mathbf{K}}k) = (h^{-1}h_0h, 1_{\mathbf{K}}) \in \overline{\mathbf{H}}.$$

La (b) si prova in modo del tutto analogo, mentre la (c) è immediata. Per provare la (d) c'è solo da mostrare che $\mathbf{H} \times \mathbf{K} \subset \overline{\mathbf{H}}\overline{\mathbf{K}}$; sia allora $(h, k) \in \mathbf{H} \times \mathbf{K}$ con $h \in \mathbf{H}$ e $k \in \mathbf{K}$: si ha

$$(h, k) = (h, 1_{\mathbf{K}})(1_{\mathbf{H}}, k) \in \overline{\mathbf{H}}\overline{\mathbf{K}}$$

come si voleva.

Per la (d), ogni elemento di $\mathbf{H} \times \mathbf{K}$ si può scrivere in almeno un modo come prodotto di un elemento di $\overline{\mathbf{H}}$ e un elemento di $\overline{\mathbf{K}}$. Se $(h_1, 1_{\mathbf{K}})(1_{\mathbf{H}}, k_1) = (h_2, 1_{\mathbf{K}})(1_{\mathbf{H}}, k_2)$ con $h_1, h_2 \in \mathbf{H}$ e $k_1, k_2 \in \mathbf{K}$, è $(h_1, k_1) = (h_2, k_2)$ e quindi $h_1 = h_2$ e $k_1 = k_2$ ossia $(h_1, 1_{\mathbf{K}}) = (h_2, 1_{\mathbf{K}})$ e $(1_{\mathbf{H}}, k_1) = (1_{\mathbf{H}}, k_2)$: pertanto, ogni elemento di $\mathbf{H} \times \mathbf{K}$ si può scrivere in un solo modo come prodotto di un elemento di $\overline{\mathbf{H}}$ e un elemento di $\overline{\mathbf{K}}$, e la (e) è così completamente provata.

Infine, se $(h, 1_{\mathbf{K}}) \in \overline{\mathbf{H}}$ e $(1_{\mathbf{H}}, k) \in \overline{\mathbf{K}}$ si ha

$$(h, 1_{\mathbf{K}})(1_{\mathbf{H}}, k) = (h, k) = (1_{\mathbf{H}}, k)(h, 1_{\mathbf{K}})$$

e anche la (f) è provata.

6.2 - Prodotto diretto di sottogruppi.

Teorema 6.2.1

Sia \mathbf{G} un gruppo, e siano \mathbf{H}, \mathbf{K} sottogruppi di \mathbf{G} . Sono fatti equivalenti:

(i) valgono le condizioni:

$$(a) \mathbf{H} \triangleleft \mathbf{G};$$

$$(b) \mathbf{K} \triangleleft \mathbf{G};$$

$$(c) \mathbf{H} \cap \mathbf{K} = \{1\};$$

$$(d) \mathbf{G} = \mathbf{H}\mathbf{K};$$

(ii) valgono le condizioni:

(e) ogni elemento di \mathbf{G} si esprime in uno e un sol modo come prodotto di un elemento di \mathbf{H} e un elemento di \mathbf{K} ;

$$(f) hk = kh \text{ per ogni } h \in \mathbf{H}, k \in \mathbf{K}.$$

Inoltre, se valgono le (a), (b), (c), (d), (e), (f), allora \mathbf{G} è (isomorfo al) prodotto diretto di \mathbf{H} per \mathbf{K} .

Dimostrazione – Proviamo in primo luogo che (i) \Rightarrow (ii).

Supponiamo che valgano le (a), (b), (c) e (d). Per la (d), ogni elemento di \mathbf{G} si esprime in almeno un modo come prodotto di un elemento di \mathbf{H} e un elemento di \mathbf{K} ; se $h_1k_1 = h_2k_2$ con $h_1, h_2 \in \mathbf{H}$ e $k_1, k_2 \in \mathbf{K}$, è anche

$$h_2^{-1}h_1k_1k_1^{-1} = h_2^{-1}h_2k_2k_1^{-1}$$

ossia

$$h_2^{-1}h_1 = k_2k_1^{-1} \in \mathbf{H} \cap \mathbf{K} = 1$$

cosicché

$$h_1 = h_2 \text{ e } k_1 = k_2.$$

Si è così provato che ogni elemento di \mathbf{G} si esprime in un solo modo come prodotto di un elemento di \mathbf{H} e un elemento di \mathbf{K} , completando così la dimostrazione della (e).

Siano ora $h \in \mathbf{H}$ e $k \in \mathbf{K}$. Poiché $\mathbf{H} \triangleleft \mathbf{G}$ e $\mathbf{K} \triangleleft \mathbf{G}$,

$$h^{-1}k^{-1}hk = h^{-1}(k^{-1}hk) = h^{-1}h_1 \in \mathbf{H}$$

$$h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k = k_1k \in \mathbf{K}$$

e quindi

$$h^{-1}k^{-1}hk \in \mathbf{H} \cap \mathbf{K} = \{1\}$$

ossia

$$h^{-1}k^{-1}hk = 1$$

da cui, moltiplicando a sinistra per kh ,

$$kh(h^{-1}k^{-1}hk) = kh1$$

cioè

$$hk = kh$$

provando così la (f) per l'arbitrarietà di h in \mathbf{H} e k in \mathbf{K} .

Proviamo adesso che $(ii) \Rightarrow (i)$.

Per dimostrare la (a) , utilizziamo come al solito il teorema 4.3.4. Sia $g \in \mathbf{G}$; dobbiamo provare che $g^{-1}\mathbf{H}g \subset \mathbf{H}$, cioè che $g^{-1}hg$ per ogni $h \in \mathbf{H}$. Per la (e) , esistono $h_0 \in \mathbf{H}$ e $k_0 \in \mathbf{K}$ tali che $g = h_0k_0$; dunque

$$g^{-1}hg = (h_0k_0)^{-1}h(h_0k_0) = k_0^{-1}h_0^{-1}hh_0k_0 = k_0^{-1}(h_0^{-1}hh_0)k_0 = k_0^{-1}h_1k_0$$

avendo posto $h_1 := h_0^{-1}hh_0 \in \mathbf{H}$. Applicando adesso la (f) , si ottiene che

$$g^{-1}hg = k_0^{-1}h_1k_0 = h_1k_0^{-1}k_0 = h_1 \in \mathbf{H}$$

come si voleva. Analogamente si prova la (b) .

Per dimostrare la (c) , supponiamo per assurdo che in $\mathbf{H} \cap \mathbf{K}$ esista un elemento $x \neq 1$; allora tale elemento si potrebbe scrivere come $x \cdot 1$ (con $x \in \mathbf{H}$ e $1 \in \mathbf{K}$) oppure come $1 \cdot x$ (con $1 \in \mathbf{H}$ e $x \in \mathbf{K}$) contraddicendo la (e) . Sempre dalla (e) segue poi immediatamente la (d) .

Proviamo infine che se valgono le (a) , (b) , (c) , (d) , (e) , (f) , allora \mathbf{G} è (isomorfo al) prodotto diretto di \mathbf{H} per \mathbf{K} . Supponiamo in particolare che valgano la (e) e la (f) e costruiamo un isomorfismo \mathbf{f} tra \mathbf{G} e $\mathbf{H} \times \mathbf{K}$. Se $g \in \mathbf{G}$, per la (e) esistono esattamente un $h \in \mathbf{H}$ ed esattamente un $k \in \mathbf{K}$ tali che $g = hk$; se poniamo $\mathbf{f}(g) := (h, k)$, la \mathbf{f} è dunque una funzione ben definita tra \mathbf{G} e $\mathbf{H} \times \mathbf{K}$. Proviamo che \mathbf{f} è un omomorfismo: se $g_1 (= h_1k_1)$ e $g_2 (= h_2k_2)$ sono elementi di \mathbf{G} , si ha

$$\mathbf{f}(g_1g_2) = \mathbf{f}(h_1k_1h_2k_2) \stackrel{(f)}{=} \mathbf{f}(h_1h_2k_1k_2) = (h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = \mathbf{f}(g_1)\mathbf{f}(g_2)$$

e quindi \mathbf{f} è un omomorfismo tra \mathbf{G} e $\mathbf{H} \times \mathbf{K}$.

È immediato che \mathbf{f} è suriettivo; per provare che è anche iniettivo (e che quindi è un isomorfismo), applichiamo il teorema 5.1.2: se $g (= hk)$ appartiene a $\mathbf{Ker} \mathbf{f}$, è

$$(1_{\mathbf{H}}, 1_{\mathbf{K}}) = 1_{\mathbf{H} \times \mathbf{K}} = \mathbf{f}(g) = \mathbf{f}(hk) = (h, k)$$

da cui $h = k = 1$ e pertanto $g = hk = 1$ come si voleva.

Esercizio 6.2.2

Dimostrare che il prodotto diretto fra un gruppo ciclico di ordine n e un gruppo ciclico di ordine m è ciclico se e soltanto se m e n sono primi fra loro.

7.- AZIONI DI UN GRUPPO SU UN INSIEME

7.1 - Definizione e prime proprietà.

Siano \mathbf{G} un gruppo e Ω un insieme. Si dice *azione di \mathbf{G} su Ω* un omomorfismo di \mathbf{G} nel gruppo $\mathbf{Sym}(\Omega)$ di tutte le permutazioni su Ω . Un'azione di \mathbf{G} su Ω si dice *fedele* se è iniettiva, cioè se è un monomorfismo di \mathbf{G} in $\mathbf{Sym}(\Omega)$. Se è data un'azione di \mathbf{G} su Ω , si dice che \mathbf{G} *opera su Ω* (mediante la data azione).

Osservazione 7.1.1

Siano \mathbf{G} un gruppo, Ω un insieme e φ un'azione di \mathbf{G} su Ω . Detta π la proiezione canonica di \mathbf{G} su $\mathbf{Ker} \varphi$, per il primo teorema di omomorfismo (teorema 5.2.2) esiste un'(unica) azione fedele ψ di $\frac{\mathbf{G}}{\mathbf{Ker} \varphi}$ su Ω tale che $\varphi = \psi \circ \pi$.

Teorema 7.1.2

Siano \mathbf{G} un gruppo e Ω un insieme. Sia data un'applicazione $\Omega \times \mathbf{G} \rightarrow \Omega$ che ad ogni coppia ordinata (ω, g) con $\omega \in \Omega$ e $g \in \mathbf{G}$ associa un elemento $\omega^g \in \Omega$ e che verifica le seguenti condizioni:

$$(7.1.2.a) \quad \omega^{1_{\mathbf{G}}} = \omega \quad \forall \omega \in \Omega;$$

$$(7.1.2.b) \quad \omega^{(g_1 g_2)} = (\omega^{g_1})^{g_2} \quad \forall \omega \in \Omega, \forall g_1, g_2 \in \mathbf{G}.$$

Allora la funzione $\varphi: \mathbf{G} \rightarrow \Omega^\Omega$ definita da

$$\varphi(g)(\omega) := \omega^g$$

è un'azione di \mathbf{G} su Ω .

Dimostrazione – La condizione (7.1.2.b) esprime il fatto che $\varphi(g_1 g_2) = \varphi(g_2) \circ \varphi(g_1)$, quindi per provare l'asserto c'è soltanto da verificare che $\varphi(g)$ è una permutazione su Ω per ogni $g \in \mathbf{G}$.

Sia dato $g \in \mathbf{G}$, e proviamo che $\varphi(g)$ è suriettiva. Se $\omega_0 \in \Omega$, posto $\omega_1 := \omega_0^{g^{-1}}$ si ha

$$\varphi(g)(\omega_1) = \omega_1^g = \left(\omega_0^{g^{-1}}\right)^g \stackrel{(7.1.2.b)}{=} \omega_0^{g^{-1}g} = \omega_0^{1_{\mathbf{G}}} \stackrel{(7.1.2.a)}{=} \omega_0$$

e dunque ω_0 proviene da ω_1 mediante $\varphi(g)$.

Infine, sia dato $g \in \mathbf{G}$ e proviamo che $\varphi(g)$ è iniettiva. Se $\varphi(g)(\omega_1) = \varphi(g)(\omega_2)$ con $\omega_1, \omega_2 \in \Omega$, è $\omega_1^g = \omega_2^g$ e quindi $(\omega_1^g)^{g^{-1}} = (\omega_2^g)^{g^{-1}}$, ossia

$$\omega_1 \stackrel{(7.1.2.a)}{=} \omega_1^{1_{\mathbf{G}}} = \omega_1^{gg^{-1}} \stackrel{(7.1.2.b)}{=} (\omega_1^g)^{g^{-1}} = (\omega_2^g)^{g^{-1}} \stackrel{(7.1.2.b)}{=} \omega_2^{gg^{-1}} = \omega_2^{1_{\mathbf{G}}} \stackrel{(7.1.2.a)}{=} \omega_2$$

come si voleva.

Nel seguito utilizzeremo spesso il teorema 7.1.2 per definire un'azione di un gruppo su un'insieme, e comunque ne adotteremo sistematicamente la "notazione esponenziale": pertanto, se è data un'azione del gruppo \mathbf{G} sull'insieme Ω , scriveremo sempre ω^g per indicare l'immagine di ω mediante la permutazione associata a $g \in \mathbf{G}$.

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Un elemento ω di Ω si dice un *punto fisso* per la data azione di \mathbf{G} su Ω se $\omega^g = \omega$ per ogni $g \in \mathbf{G}$.

7.2 - Orbite. Transitività.

Teorema 7.2.1

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . La relazione \sim in Ω definita da

$$\omega_1 \sim \omega_2 \quad \Leftrightarrow \quad \text{esiste } g \in \mathbf{G} \text{ tale che } \omega_1^g = \omega_2$$

è una relazione di equivalenza in Ω .

Dimostrazione – La \sim è riflessiva perché $\omega^{1_{\mathbf{G}}} = \omega$ per ogni $\omega \in \Omega$ (teorema 2.9.1); è simmetrica perché se $\omega_1 \sim \omega_2$ esiste $g \in \mathbf{G}$ tale che $\omega_1^g = \omega_2$ e quindi $\omega_1 = (\omega_1^g)^{g^{-1}} = \omega_2^{g^{-1}}$ ossia $\omega_2 \sim \omega_1$; ed è transitiva perché se $\omega_1 \sim \omega_2$ e $\omega_2 \sim \omega_3$ esistono $g, h \in \mathbf{G}$ tali che $\omega_1^g = \omega_2$ e $\omega_2^h = \omega_3$ cosicché $\omega_1^{gh} = (\omega_1^g)^h = \omega_2^h = \omega_3$ ossia $\omega_1 \sim \omega_3$.

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Le classi di equivalenza individuate in Ω dalla relazione di equivalenza \sim considerata nel teorema 7.2.1 si dicono le *orbite* dell'azione di \mathbf{G} su Ω . Se $\omega \in \Omega$, l'orbita dell'azione di \mathbf{G} su Ω a cui appartiene ω si indica con $O_{\mathbf{G}}(\omega)$.

Teorema 7.2.2

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Le orbite dell'azione di \mathbf{G} su Ω sono una partizione di Ω .

Dimostrazione – Ovvio per il teorema 7.2.1 e l'osservazione 0.7.5.

Siano \mathbf{G} un gruppo e Ω un insieme. Un'azione di \mathbf{G} su Ω per la quale esista una sola orbita si dice *transitiva*. Se l'azione di \mathbf{G} su Ω è transitiva, si dice che \mathbf{G} *opera transitivamente* su Ω .

7.3 - Stabilizzatore.

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Se $\omega \in \Omega$, si dice *stabilizzatore di ω in \mathbf{G}* (rispetto alla data azione di \mathbf{G} su Ω) l'insieme

$$\mathbf{G}_{\omega} := \{g \in \mathbf{G} / \omega^g = \omega\}.$$

Teorema 7.3.1

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Per ogni $\omega \in \Omega$, lo stabilizzatore in \mathbf{G} di ω è un sottogruppo di \mathbf{G} .

Dimostrazione – Sia $\omega \in \Omega$; Poiché certamente $1_{\mathbf{G}} \in \mathbf{G}_{\omega}$, e quindi \mathbf{G}_{ω} non è vuoto, possiamo dimostrare che \mathbf{G}_{ω} è un sottogruppo di \mathbf{G} verificando la condizione (iii) del teorema 3.4.1. Siano $g_1, g_2 \in \mathbf{G}_{\omega}$ (ossia $\omega^{g_1} = \omega^{g_2} = \omega$); allora $\omega^{g_1 g_2} = (\omega^{g_1})^{g_2} = \omega^{g_2} = \omega$, cosicché $g_1 g_2 \in \mathbf{G}_{\omega}$. Infine, se $g \in \mathbf{G}_{\omega}$ (ossia $\omega^g = \omega$) si ha $\omega = \omega^{1_{\mathbf{G}}} = \omega^{g g^{-1}} = (\omega^g)^{g^{-1}} = \omega^{g^{-1}}$ cioè $g^{-1} \in \mathbf{G}_{\omega}$ come si voleva.

Teorema 7.3.2

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Per ogni $\omega \in \Omega$, la cardinalità dell'orbita a cui appartiene ω è uguale all'indice in \mathbf{G} dello stabilizzatore in \mathbf{G} di ω , ossia

$$|O_{\mathbf{G}}(\omega)| = |\mathbf{G} : \mathbf{G}_{\omega}|.$$

Dimostrazione – Si tratta di dimostrare che c'è una corrispondenza biunivoca fra l'insieme delle classi laterali destre di \mathbf{G}_{ω} in \mathbf{G} e l'orbita a cui appartiene ω .

Se $g \in \mathbf{G}$, poniamo

$$\varphi(\mathbf{G}_{\omega}g) := \omega^g$$

e dimostriamo che φ è ben definita, è iniettiva ed è suriettiva.

Per dimostrare che φ è ben definita, supponiamo che sia $\mathbf{G}_{\omega}x = \mathbf{G}_{\omega}y$ con $x, y \in \mathbf{G}$ e proviamo che $\omega^x = \omega^y$. In effetti, poiché $\mathbf{G}_{\omega}x = \mathbf{G}_{\omega}y$ si ha $xy^{-1} \in \mathbf{G}_{\omega}$ ossia $\omega^{xy^{-1}} = \omega$ da cui $\omega^x = \omega^{(xy^{-1}y)} = (\omega^{xy^{-1}})^y = \omega^y$ come si voleva.

Per dimostrare che φ è iniettiva, supponiamo che sia $\varphi(\mathbf{G}_{\omega}x) = \varphi(\mathbf{G}_{\omega}y)$ con $x, y \in \mathbf{G}$ e proviamo che $\mathbf{G}_{\omega}x = \mathbf{G}_{\omega}y$. Per definizione di φ , se $\varphi(\mathbf{G}_{\omega}x) = \varphi(\mathbf{G}_{\omega}y)$ si ha $\omega^x = \omega^y$ e dunque

$$\omega^{(xy^{-1})} = (\omega^x)^{y^{-1}} = (\omega^y)^{y^{-1}} = \omega^{(yy^{-1})} = \omega^{1_{\mathbf{G}}} = \omega$$

ossia $xy^{-1} \in \mathbf{G}_{\omega}$; ciò prova, come si voleva, che $\mathbf{G}_{\omega}x = \mathbf{G}_{\omega}y$.

È infine immediato che φ è suriettiva: ogni elemento dell'orbita di ω è infatti della forma ω^g per un opportuno $g \in \mathbf{G}$, e quindi proviene mediante φ da $\mathbf{G}_{\omega}g$.

Corollario 7.3.3

Se \mathbf{G} è un gruppo che opera transitivamente su un insieme Ω , Ω è equipotente all'insieme delle classi laterali destre in \mathbf{G} (e quindi all'insieme delle classi laterali sinistre in \mathbf{G}) dello stabilizzatore in \mathbf{G} di un qualsiasi elemento di Ω , ossia

$$|\Omega| = |\mathbf{G} : \mathbf{G}_{\omega}| \quad \forall \omega \in \Omega.$$

Dimostrazione – Se \mathbf{G} opera transitivamente su Ω , c'è una sola orbita per l'azione di \mathbf{G} su Ω che quindi coincide con Ω ; a questo punto basta applicare il teorema 7.3.2.

Osservazione 7.3.4

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Per ogni $\omega \in \Omega$, si ha che

$$(\omega \text{ è un punto fisso per l'azione di } \mathbf{G} \text{ su } \Omega) \Leftrightarrow (\mathbf{G}_{\omega} = \mathbf{G}).$$

Teorema 7.3.5

Siano \mathbf{G} un gruppo e Ω un insieme, e sia data un'azione di \mathbf{G} su Ω . Per ogni $\omega \in \Omega$ e per ogni $g \in \mathbf{G}$, si ha

$$\mathbf{G}_{\omega^g} = g^{-1}\mathbf{G}_\omega g.$$

Dimostrazione – Sia $x \in \mathbf{G}_{\omega^g}$ e proviamo che $x \in g^{-1}\mathbf{G}_\omega g$, ossia che $g x g^{-1} \in \mathbf{G}_\omega$. Si ha in effetti

$$\omega^{(g x g^{-1})} = ((\omega^g)^x)^{g^{-1}} = (\omega^g)^{g^{-1}} = \omega^{(g g^{-1})} = \omega^{1_{\mathbf{G}}} = \omega$$

come si voleva.

Sia ora $x \in g^{-1}\mathbf{G}_\omega g$ (ossia $g x g^{-1} \in \mathbf{G}_\omega$) e proviamo che $x \in \mathbf{G}_{\omega^g}$. Si ha in effetti

$$(\omega^g)^x = ((\omega^g)^{g x g^{-1}})^{g^{-1}} = \omega^{(g x g^{-1} g)} = \left(\omega^{(g x g^{-1})} \right)^g = \omega^g$$

come si voleva.

7.4 - Il caso finito: l'equazione delle orbite.

Siano \mathbf{G} un gruppo e Ω un insieme finito, e sia data un'azione di \mathbf{G} su Ω . Se Ω^* è un insieme di rappresentanti per le orbite dell'azione di \mathbf{G} su Ω , si ha ovviamente

(eq. 7.4.a)
$$|\Omega| = \sum_{\omega \in \Omega^*} |\mathbf{O}_{\mathbf{G}}(\omega)|$$

ossia, tenendo conto del teorema 7.3.2,

(eq. 7.4.b)
$$|\Omega| = \sum_{\omega \in \Omega^*} |\mathbf{G} : \mathbf{G}_\omega|.$$

Se, come spesso conviene fare, vogliamo evidenziare il sottoinsieme Ω_0 dei punti fissi di Ω , si considera anziché Ω^* un insieme di rappresentanti Ω^0 per quelle orbite dell'azione di \mathbf{G} su Ω che contengono più di un elemento: le equazioni (eq. 7.4.a) e (eq. 7.4.b) divengono allora rispettivamente

(eq. 7.4.a₀)
$$|\Omega| = |\Omega_0| + \sum_{\omega \in \Omega^0} |\mathbf{O}_{\mathbf{G}}(\omega)|$$

e

(eq. 7.4.b₀)
$$|\Omega| = |\Omega_0| + \sum_{\omega \in \Omega^0} |\mathbf{G} : \mathbf{G}_\omega|.$$

Sia p un numero primo. Un gruppo \mathbf{G} si dice un p -gruppo finito se $|\mathbf{G}| = p^\alpha$ con $\alpha \in \mathbb{N}$.

Nel caso in cui si consideri l'azione su un insieme finito di un p -gruppo finito \mathbf{G} , gli addendi $|\mathbf{G} : \mathbf{G}_\omega|$ che compaiono nella (eq. 7.4.b₀) sono tutti divisibili per p e si possono facilmente ricavare interessanti risultati.

Teorema 7.4.1

Siano p un numero primo, \mathbf{G} un p -gruppo finito e Ω un insieme finito. Se $|\Omega|$ è primo con p , esistono punti fissi per qualsiasi azione di \mathbf{G} su Ω .

Dimostrazione – Se per una data azione di \mathbf{G} su Ω non fossero punti fissi, la (eq. 7.4.b₀) diventerebbe

$$|\Omega| = \sum_{\omega \in \Omega^0} |\mathbf{G} : \mathbf{G}_\omega|$$

ma questa uguaglianza sotto le nostre ipotesi è assurda perché il membro di sinistra è un numero primo con p mentre il membro di destra è una somma di numeri tutti multipli di p e quindi è un multiplo di p .

Teorema 7.4.2

Siano p un numero primo, \mathbf{G} un p -gruppo finito e Ω un insieme finito. Se $|\Omega|$ è divisibile per p , per qualsiasi azione di \mathbf{G} su Ω non può esserci esattamente un punto fisso: o non ce n'è nessuno, o ce n'è un multiplo (positivo) di p .

Dimostrazione – Per l'azione di \mathbf{G} su Ω che si vuole considerare, scriviamo la (eq. 7.4.b₀) nella forma

$$|\Omega_0| = |\Omega| - \left(\sum_{\omega \in \Omega^0} |\mathbf{G} : \mathbf{G}_\omega| \right).$$

Sotto le nostre ipotesi ogni termine al secondo membro è multiplo di p , dunque anche il primo membro è multiplo di p : in particolare, $|\Omega_0| \neq 1$ (e più precisamente: $|\Omega_0| = 0$ oppure $|\Omega_0| = kp$ con $k \in \mathbb{Z}^+$).

7.5 - Applicazione allo studio dei p -gruppi finiti.

Sia \mathbf{G} un gruppo.

Ci sono tre importanti modi in cui \mathbf{G} può operare su se stesso o sull'insieme dei propri sottoinsiemi: mediante *moltiplicazione a destra*, mediante *moltiplicazione a sinistra* e mediante *coniugio*. I primi due sono concettualmente equivalenti fra loro, il terzo è ben diverso.

Per ogni $g \in \mathbf{G}$, se $x \in \mathbf{G}$ e se $\mathbf{S} \subset \mathbf{G}$ poniamo

$$x^g := xg; \quad \mathbf{S}^g := \mathbf{S}g.$$

Per il teorema 7.1.2, è immediato che abbiamo così definito un'azione di \mathbf{G} su se stesso e sull'insieme dei propri sottoinsiemi; si dice in questo caso che \mathbf{G} opera (su se stesso oppure sull'insieme dei propri sottoinsiemi) mediante moltiplicazione a destra.

Per ogni $g \in \mathbf{G}$, se $x \in \mathbf{G}$ e se $\mathbf{S} \subset \mathbf{G}$ poniamo

$$x^g := gx; \quad \mathbf{S}^g := g\mathbf{S}.$$

Per il teorema 7.1.2, è immediato che abbiamo così definito un'azione di \mathbf{G} su se stesso e sull'insieme dei propri sottoinsiemi; si dice in questo caso che \mathbf{G} opera (su se stesso oppure sull'insieme dei propri sottoinsiemi) mediante moltiplicazione a sinistra.

Per ogni $g \in \mathbf{G}$, se $x \in \mathbf{G}$ e se $\mathbf{S} \subset \mathbf{G}$ poniamo

$$x^g := g^{-1}xg; \quad \mathbf{S}^g := g^{-1}\mathbf{S}g.$$

Per il teorema 7.1.2, è immediato che abbiamo così definito un'azione di \mathbf{G} su se stesso e sull'insieme dei propri sottoinsiemi; si dice in questo caso che \mathbf{G} opera (su se stesso oppure sull'insieme dei propri sottoinsiemi) mediante il coniugio.

Nei casi sopra considerati, l'insieme su cui \mathbf{G} opera è \mathbf{G} stesso oppure l'insieme dei propri sottoinsiemi; è chiaro però che \mathbf{G} può operare come visto sopra anche su particolari sottoinsiemi di se stesso o dell'insieme dei propri sottoinsiemi. Ad esempio \mathbf{G} può operare mediante moltiplicazione a destra sull'insieme delle classi laterali destre di un proprio sottogruppo; oppure può operare mediante moltiplicazione a sinistra sull'insieme delle classi laterali sinistre di un proprio sottogruppo; oppure può operare mediante il coniugio su un proprio sottogruppo normale. E ovviamente possiamo considerare la restrizione di tali azioni a qualsiasi sottogruppo di \mathbf{G} .

Teorema 7.5.1

Siano p un numero primo e \mathbf{G} un p -gruppo finito. Se $\{1_{\mathbf{G}}\} \neq \mathbf{N} \triangleleft \mathbf{G}$, allora

$$\mathbf{N} \cap \mathbf{Z}(\mathbf{G}) \neq \{1_{\mathbf{G}}\}.$$

Dimostrazione – Consideriamo l'azione di \mathbf{G} su \mathbf{N} mediante il coniugio: sono verificate le ipotesi del teorema 7.4.2, perché $\Omega(:= \mathbf{N})$ ha ordine multiplo di p . Poiché $1_{\mathbf{G}}$ è un punto fisso per l'azione considerata, ce ne deve essere almeno un altro: dunque in \mathbf{N} esiste $x \neq 1_{\mathbf{G}}$ tale che $g^{-1}xg = x$ (ossia $xg = gx$) per ogni $g \in \mathbf{G}$. Un tale x appartiene quindi a $\mathbf{Z}(\mathbf{G})$ e l'asserto è completamente provato.

Corollario 7.5.2

Siano p un numero primo e \mathbf{G} un p -gruppo finito. Allora $\mathbf{Z}(\mathbf{G}) \neq \{1_{\mathbf{G}}\}$.

Dimostrazione – Basta applicare il teorema 7.5.1 con $\mathbf{N} := \mathbf{G}$.

Esercizio 7.5.3

Sia p un numero primo. Si dimostri che ogni gruppo di ordine p^2 è commutativo.

Teorema 7.5.4

Siano p un numero primo e \mathbf{G} un p -gruppo finito. Se $\mathbf{H} \neq \mathbf{G}$, allora $\mathbf{H} \neq \mathcal{N}_{\mathbf{G}}(\mathbf{H})$.

Dimostrazione – Consideriamo l'azione di \mathbf{H} mediante moltiplicazione a destra sull'insieme delle classi laterali destre di \mathbf{H} in \mathbf{G} : sono verificate le ipotesi del teorema 7.4.2, perché per il teorema 4.2.1 il numero delle classi laterali destre di \mathbf{H} in \mathbf{G} è una potenza di p (e non è 1 perché $\mathbf{H} \neq \mathbf{G}$). Poiché \mathbf{H} stesso è un punto fisso per l'azione considerata, ce ne deve essere almeno un altro: dunque esiste $g \in \mathbf{G}$ tale che $\mathbf{H}g \neq \mathbf{H}$ e $\mathbf{H}g = (\mathbf{H}g)^h := \mathbf{H}gh$ per ogni $h \in \mathbf{H}$. Ma $\mathbf{H}g \neq \mathbf{H}$ significa che $g \notin \mathbf{H}$, e $\mathbf{H}g = \mathbf{H}gh$ (per ogni $h \in \mathbf{H}$) significa che $ghg^{-1} \in \mathbf{H}$ (per ogni $h \in \mathbf{H}$), ossia che $g^{-1} \in \mathcal{N}_{\mathbf{G}}(\mathbf{H})$. Poiché $g \notin \mathbf{H}$, è anche $g^{-1} \notin \mathbf{H}$ e il nostro asserto è così dimostrato.

Sia \mathbf{G} un gruppo. Un sottogruppo \mathbf{M} di \mathbf{G} si dice massimale se (è un elemento massimale nell'insieme dei sottogruppi di \mathbf{G} ordinato rispetto all'inclusione, cioè se) $\mathbf{M} \neq \mathbf{G}$ e per ogni sottogruppo \mathbf{H} di \mathbf{G} tale che $\mathbf{M} \leq \mathbf{H} \leq \mathbf{G}$ si ha $\mathbf{M} = \mathbf{H}$ oppure $\mathbf{H} = \mathbf{G}$.

Corollario 7.5.5

Sia p un numero primo, e sia \mathbf{G} un p -gruppo finito. Ogni sottogruppo massimale di \mathbf{G} è normale in \mathbf{G} e ha indice p in \mathbf{G} .

Dimostrazione – Sia \mathbf{M} un sottogruppo massimale di \mathbf{G} . Poiché $\mathbf{M} \neq \mathbf{G}$, per il teorema 7.5.4 è $\mathbf{M} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{M}) \leq \mathbf{G}$ con $\mathbf{M} \neq \mathcal{N}_{\mathbf{G}}(\mathbf{M})$; per definizione di sottogruppo massimale ne segue che $\mathcal{N}_{\mathbf{G}}(\mathbf{M}) = \mathbf{G}$ cioè che $\mathbf{M} \triangleleft \mathbf{G}$. Consideriamo ora il gruppo quoziente $\frac{\mathbf{G}}{\mathbf{M}}$: se avesse un sottogruppo proprio, esso sarebbe della forma $\frac{\mathbf{H}}{\mathbf{M}}$ con $\mathbf{M} \neq \mathbf{H} \neq \mathbf{G}$, assurdo perché \mathbf{M} è un sottogruppo massimale di \mathbf{G} . Dunque $\frac{\mathbf{G}}{\mathbf{M}}$ non ha sottogruppi propri e quindi per il teorema 3.5.9 il suo ordine è un numero primo. Ma $\left| \frac{\mathbf{G}}{\mathbf{M}} \right| (= |\mathbf{G} : \mathbf{M}|)$ è un divisore di $|\mathbf{G}|$, dunque tale numero primo non può essere che p .

8.- I TEOREMI DI SYLOW

8.1 - Due lemmi numerici.

Riportiamo in questa sezione un paio di risultati "tecnici" che ci serviranno nella sez. 8.2 per la dimostrazione del teorema principale di questo capitolo.

Lemma 8.1.1

Siano a, b numeri interi positivi tali che b divide a . Allora

$$\binom{a}{b} = \frac{a}{b} \binom{a-1}{b-1}.$$

Dimostrazione – Si ha

$$\begin{aligned} \binom{a}{b} &= \frac{a \cdot (a-1) \cdot (a-2) \cdot \dots \cdot (a-(b-1)) \cdot (a-b)}{1 \cdot 2 \cdot \dots \cdot (b-2) \cdot (b-1) \cdot b} = \\ &= \frac{a}{b} \cdot \frac{(a-1) \cdot (a-2) \cdot \dots \cdot ((a-1)-(b-2)) \cdot ((a-1)-(b-1))}{1 \cdot 2 \cdot \dots \cdot (b-2) \cdot (b-1)} = \frac{a}{b} \binom{a-1}{b-1} \end{aligned}$$

Lemma 8.1.2 (Krull)

Siano p un numero primo, k un numero intero positivo e n un numero intero positivo divisibile per p^k . Allora

$$\binom{n-1}{p^k-1} \equiv 1 \pmod{p}.$$

Dimostrazione – Si ha

$$\binom{n-1}{p^k-1} = \frac{(n-1)(n-2)\dots(n-(p^k-1))}{1\cdot 2\cdot \dots\cdot (p^k-1)} = \frac{n-1}{1} \cdot \frac{n-2}{2} \cdot \dots \cdot \frac{n-(p^k-1)}{p^k-1} = \prod_{i=1}^{p^k-1} \left(\frac{n}{i} - 1\right).$$

Poiché $i < p^k$, p^k non divide i per $i := 1, 2, \dots, p^k - 1$. D'altro lato, per ipotesi p^k divide n . Dividendo numeratore e denominatore per la massima potenza di p che divide i , possiamo dunque scrivere

$$\frac{n}{i} = p \frac{x_i}{y_i}$$

con x_i e y_i numeri interi tali che p non divide y_i .

Sviluppando $\prod_{i=1}^{p^k-1} \left(p \frac{x_i}{y_i} - 1\right)$ otteniamo una somma di prodotti, uno dei quali è $(-1)^{p^k-1}$.

Raccogliendo in un unico termine tutti gli altri addendi, con fattore comune p e denominatore v dato dal prodotto di tutti gli y_i , possiamo scrivere

$$\binom{n-1}{p^k-1} = \prod_{i=1}^{p^k-1} \left(p \frac{x_i}{y_i} - 1\right) = (-1)^{p^k-1} + p \frac{u}{v}$$

dove u, v sono interi e v non è divisibile per p (perché nessun y_i lo è). A questo punto ci resta soltanto da mostrare che $\frac{u}{v}$ è un numero intero, dato che $(-1)^{p^k-1} = 1$ per ogni numero primo dispari p , mentre $(-1)^{2^{k-1}} = -1 \equiv 1 \pmod{2}$.

Si ha

$$p \frac{u}{v} = \binom{n-1}{p^k-1} - (-1)^{p^k-1}$$

e dunque $p \frac{u}{v}$ deve essere un numero intero (perché i coefficienti binomiali sono numeri interi), cosicché v divide pu . Ma p è un numero primo che non divide v , quindi necessariamente v divide u e l'asserto è completamente provato.

8.2 - Il teorema principale.

Teorema 8.2.1 (Sylow-Frobenius)

Siano \mathbf{G} un gruppo finito, p un numero primo e k un numero intero positivo tale che p^k divide $|\mathbf{G}|$. Sia \mathcal{X}_{p^k} l'insieme dei sottogruppi di \mathbf{G} che hanno ordine p^k . Allora

$$|\mathcal{X}_{p^k}| \equiv 1 \pmod{p}.$$

In particolare, $\mathcal{X}_{p^k} \neq \emptyset$.

Dimostrazione – Sia d un divisore di $|\mathbf{G}|$ e sia Ω l'insieme dei sottoinsiemi di \mathbf{G} che hanno cardinalità d . Facciamo operare \mathbf{G} su Ω mediante moltiplicazione a destra e cominciamo col raccogliere alcuni risultati sullo stabilizzatore \mathbf{G}_U del generico $U \in \Omega$ in questa azione.

$$\boxed{\text{S}_1}$$

$$\mathbf{G}_U \subset \mathbf{U} \Leftrightarrow 1_{\mathbf{G}} \in \mathbf{U}.$$

$$\boxed{\text{S}_2}$$

$$\mathbf{G}_U = \mathbf{U} \Leftrightarrow \mathbf{U} \text{ è un sottogruppo di } \mathbf{G}.$$

$$\boxed{\text{S}_3}$$

$$\mathbf{U} \cdot \mathbf{G}_U = \mathbf{U}.$$

$$\boxed{\text{S}_4}$$

\mathbf{U} è unione di classi laterali sinistre di \mathbf{G}_U in \mathbf{G} , e quindi $|\mathbf{G}_U|$ divide $|\mathbf{U}|$.

Adesso ragioniamo sulle orbite dell'azione di \mathbf{G} su Ω .

$$\boxed{\text{O}_1}$$

Se Ω_i è l'orbita di U_i , $|\Omega_i| = \frac{|\mathbf{G}|}{d} \cdot \frac{d}{|\mathbf{G}_{U_i}|}$ con $\frac{|\mathbf{G}|}{d}$ e $\frac{d}{|\mathbf{G}_{U_i}|}$ numeri interi.

Dimostrazione – Per ipotesi d divide $|\mathbf{G}|$, e per l'osservazione $\boxed{\text{S}_4}$ (ricordando che $|\mathbf{U}| = d$) $|\mathbf{G}_U|$ divide d .

O_2

Per ogni orbita Ω_i si ha $|\Omega_i| = \frac{|G|}{d}$ se e soltanto se in Ω_i c'è un sottogruppo.

Dimostrazione – Supponiamo in primo luogo che in Ω_i ci sia un sottogruppo: per l'osservazione **S_2** e il teorema 7.3.2, si ha $|\Omega_i| = \frac{|G|}{d}$. Viceversa, sia $|\Omega_i| = \frac{|G|}{d}$ cioè, per il teorema 7.3.2, $|G_U| = d$ per un qualsiasi $U \in \Omega_i$. Scelto $x \in U$, è $1_G \in Ux^{-1} = U_0 \in \Omega_i$. Per l'osservazione **S_1** è $G_{U_0} \subseteq U_0$ ma poiché $|G_{U_0}| = d = |U_0|$ deve essere $G_{U_0} = U_0$ e dunque U_0 è un sottogruppo.

O_3

Se in un'orbita c'è un sottogruppo, ce n'è uno solo.

Dimostrazione – Ovvio, perché se in un'orbita c'è un sottogruppo di G allora tale orbita consiste esattamente delle classi laterali destre in G di quel sottogruppo.

Per l'osservazione **O_1**, l'equazione (eq. 7.4.a) si può riscrivere come

$$(eq. 8.2.1a) \quad |\Omega| = \frac{|G|}{d} \cdot \left(\frac{d}{|G_{U_1}|} + \frac{d}{|G_{U_2}|} + \dots + \frac{d}{|G_{U_t}|} \right)$$

dove $\{U_1, U_2, \dots, U_t\}$ è un insieme di rappresentanti delle orbite di Ω . Tenendo ulteriormente conto delle osservazioni **O_2** e **O_3**, l'equazione (eq. 8.2.1a) diventa

$$(eq. 8.2.1b) \quad |\Omega| = \frac{|G|}{d} \cdot \left(|\mathcal{X}_d| + \frac{d}{|G_{U_{i_1}}|} + \frac{d}{|G_{U_{i_2}}|} + \dots + \frac{d}{|G_{U_{i_z}}|} \right)$$

dove $|\mathcal{X}_d|$ è il numero dei sottogruppi di G di ordine d , $\{U_{i_1}, U_{i_2}, \dots, U_{i_z}\}$ è un insieme di rappresentanti delle orbite di Ω a cui non appartengono sottogruppi, e i numeri interi $\frac{d}{|G_{U_{i_j}}|}$

sono divisori di d diversi da 1.

Esaminiamo ora il membro sinistro dell'equazione (eq. 8.2.1b): il numero dei sottoinsiemi di G con d elementi, cioè $|\Omega|$, è come noto $\binom{|G|}{d}$. Per il lemma 8.1.1,

$$\binom{|G|}{d} = \frac{|G|}{d} \binom{|G| - 1}{d - 1}$$

cosicché possiamo riscrivere l'equazione (eq. 8.2.1b) come

$$(eq. 8.2.1c) \quad \binom{|G| - 1}{d - 1} = |\mathcal{X}_d| + \frac{d}{|G_{U_{i_1}}|} + \frac{d}{|G_{U_{i_2}}|} + \dots + \frac{d}{|G_{U_{i_z}}|}$$

o anche

$$(eq. 8.2.1d) \quad |\mathcal{X}_d| = \binom{|G| - 1}{d - 1} - \left(\frac{d}{|G_{U_{i_1}}|} + \frac{d}{|G_{U_{i_2}}|} + \dots + \frac{d}{|G_{U_{i_z}}|} \right)$$

A questo punto vediamo che cosa accade se $d := p^k$ come nelle ipotesi del nostro teorema.

Tutti gli addendi della forma

$$\frac{p^k}{|G_{U_{i_j}}|}$$

(essendo divisori di p^k diversi da 1) sono congrui a 0 modulo p . L'asserto segue dunque dal lemma 8.1.2.

8.3 - Sottogruppi di Sylow.

Siano \mathbf{G} un gruppo finito, p un numero primo e p^α (con $\alpha \in \mathbb{N}$) la massima potenza di p che divide $|\mathbf{G}|$ (eventualmente $\alpha = 0$ e $p^\alpha = 1$). Si dice *p -sottogruppo di Sylow di \mathbf{G}* ogni sottogruppo di \mathbf{G} che abbia ordine p^α . L'insieme di tutti i p -sottogruppi di Sylow di \mathbf{G} (che non è vuoto per il teorema 8.2.1) si indica con $\mathbf{Syl}_p(\mathbf{G})$.

Osservazione 8.3.1

Ogni endomorfismo di un gruppo, per il "teorema di corrispondenza" (5.3.1), trasforma sottogruppi in sottogruppi. Ogni automorfismo di un gruppo, essendo in particolare una corrispondenza biunivoca, trasforma sottogruppi in sottogruppi della stessa cardinalità. Dunque, ogni automorfismo di un gruppo finito trasforma sottogruppi in sottogruppi dello stesso ordine: in particolare, per ogni numero primo p , ogni automorfismo di un gruppo finito \mathbf{G} muta in sé $\mathbf{Syl}_p(\mathbf{G})$; vedremo adesso (corollario 8.3.3) che $\mathbf{Aut}(\mathbf{G})$ (anzi, addirittura: $\mathbf{Inn}(\mathbf{G})$) opera transitivamente su $\mathbf{Syl}_p(\mathbf{G})$.

Se in un gruppo finito per un particolare numero primo p c'è un solo p -sottogruppo di Sylow, per quanto appena osservato esso è mutato in sé da ogni automorfismo del gruppo; in particolare, esso è mutato in sé da ogni automorfismo interno del gruppo e dunque (teorema 4.3.4) è un sottogruppo normale.

Teorema 8.3.2

Siano \mathbf{G} un gruppo finito, p un numero primo e k un numero intero positivo tale che p^k divide $|\mathbf{G}|$. Siano \mathbf{H} un sottogruppo di \mathbf{G} di ordine p^k e \mathbf{P} un p -sottogruppo di Sylow di \mathbf{G} . Esiste $g \in \mathbf{G}$ tale che

$$\mathbf{H} \subset g^{-1}\mathbf{P}g.$$

Dimostrazione – Sia Ω l'insieme delle classi laterali destre di \mathbf{P} in \mathbf{G} , e facciamo operare \mathbf{H} su Ω mediante moltiplicazione a destra. È $|\Omega| = \frac{|\mathbf{G}|}{|\mathbf{P}|}$ e dunque (poiché \mathbf{P} è un sottogruppo di Sylow di \mathbf{G}) $|\Omega|$ è primo con $|\mathbf{H}|$; per il teorema 7.4.1 c'è almeno un punto fisso per questa azione di \mathbf{H} su Ω , ossia esiste $g \in \mathbf{G}$ tale che

$$(\mathbf{P}g)h = \mathbf{P}g \quad \text{per ogni } h \in \mathbf{H}.$$

Ciò significa che

$$(gh)g^{-1} \in \mathbf{P} \quad \text{per ogni } h \in \mathbf{H}$$

ossia che

$$g\mathbf{H}g^{-1} \subseteq \mathbf{P}$$

e infine che

$$\mathbf{H} \subseteq g^{-1}\mathbf{P}g$$

come si voleva dimostrare.

Corollario 8.3.3

Siano \mathbf{G} un gruppo finito e p un numero primo che divide $|\mathbf{G}|$. Tutti i p -sottogruppi di Sylow di \mathbf{G} sono fra loro coniugati.

Dimostrazione – Siano \mathbf{P}_1 e \mathbf{P}_2 due qualsiasi p -sottogruppi di Sylow di \mathbf{G} . Per il teorema 8.3.2 (con $\mathbf{H} := \mathbf{P}_1$ e $\mathbf{P} := \mathbf{P}_2$), esiste $g \in \mathbf{G}$ tale che

$$\mathbf{P}_1 \subseteq g^{-1}\mathbf{P}_2g.$$

Poiché $|\mathbf{P}_1| = |\mathbf{P}_2|$, ne segue che $\mathbf{P}_1 = g^{-1}\mathbf{P}_2g$, cioè l'asserto.

Corollario 8.3.4

Siano \mathbf{G} un gruppo finito e p un numero primo che divide $|\mathbf{G}|$. Per qualsiasi $\mathbf{P} \in \mathbf{Syl}_p(\mathbf{G})$ si ha

$$|\mathbf{Syl}_p(\mathbf{G})| = |\mathbf{G} : \mathcal{N}_{\mathbf{G}}(\mathbf{P})|.$$

Dimostrazione – Sia $\mathbf{P} \in \mathbf{Syl}_p(\mathbf{G})$. L'orbita a cui appartiene \mathbf{P} per l'azione di \mathbf{G} mediante il coniugio sull'insieme dei suoi sottogruppi è (per il corollario 8.3.3) $\mathbf{Syl}_p(\mathbf{G})$, mentre lo stabilizzatore di \mathbf{P} è (per definizione) $\mathcal{N}_{\mathbf{G}}(\mathbf{P})$. L'asserto è dunque immediata conseguenza del teorema 7.3.2.

Corollario 8.3.5

Sia p^α la massima potenza di p che divide $|\mathbf{G}|$.

Il numero $|\mathbf{Syl}_p(\mathbf{G})|$ dei p -sottogruppi di Sylow di \mathbf{G} è un divisore di $\frac{|\mathbf{G}|}{p^\alpha}$.

Dimostrazione – Ricordando che $\mathbf{P} \leq \mathcal{N}_{\mathbf{G}}(\mathbf{P})$ (per il teorema 4.5.1), dal corollario 8.3.4 e dal teorema 4.2.3 ($\mathbf{H} := \mathcal{N}_{\mathbf{G}}(\mathbf{P})$, $\mathbf{K} := \mathbf{P}$) segue che

$$|\mathbf{Syl}_p(\mathbf{G})| = |\mathbf{G} : \mathcal{N}_{\mathbf{G}}(\mathbf{P})| = \frac{|\mathbf{G} : \mathbf{P}|}{|\mathcal{N}_{\mathbf{G}}(\mathbf{P}) : \mathbf{P}|}$$

da cui l'asserto poiché $|\mathbf{G} : \mathbf{P}| = \frac{|\mathbf{G}|}{p^\alpha}$.