CORSO DI ALGEBRA 1

FABRIZIO CASELLI

Contents

Premessa 1
1. Insiemi e relazioni 2
2. Principio del buon ordinamento e il principio di induzione 9
3. Divisibilità in $\mathbb{Z}$ e numeri primi 10
4. Cardinalità 16
5. La ϕ di Eulero e il teorema cinese del resto 21
6. Congruenze e sistemi di congruenze lineari 24
7. Crittografia (non svolta) 27
8. Sottogruppi e generatori di un gruppo 31
9. I gruppi diedrali 36
10. Il gruppo simmetrico 38
11. Il coniugio 43
12. Classi laterali e teorema di Lagrange 48
13. Omomorfismi, sottogruppi normali e quozienti di un gruppo 49
14. Prodotti diretti e semidiretti 54
15. Qualche osservazione sui quozienti 56
16. Azioni di gruppi 57
17. Il teorema di Sylow 61

Premessa

Queste note sono gli appunti del docente per le lezioni e NON sostituiscono i libri consigliati e sono state redatte per venire incontro agli studenti in mancanza di un libro di testo unico seguito durante il corso. Contengono alcune (poche) cose non trattate in aula e mancano di tanti particolari che invece sono stati visti a lezione. Sfogliare e leggere più libri è sempre una buona prassi quando si studia matematica. È molto probabile che questi appunti contengano numerosi errori e chiedo ai miei studenti-lettori di segnalarmeli.

1. Insiemi e relazioni

Un insieme è per noi un concetto primitivo, cioè un concetto intuitivo cui non diamo una definizione formale. Tuttavia rimane necessario comunicare cosa intendiamo con insieme e soprattutto cosa vuol dire che due insiemi sono uguali.

Per noi un *insieme* è una collezione, o raccolta, o gruppo, di oggetti di qualsiasi natura, detti *elementi*, con un criterio univoco per stabilire quali questi elementi siano.

Ad esempio "gli studenti belli" non formano un insieme, mentre "gli studenti belli secondo il prof" formano un insieme: infatti in questo caso sarà sufficiente chiedere al prof quali secondo lui siano gli studenti che fanno parte di questo insieme.

Classici insiemi numeri che conosciamo da tempo sono:

- i numeri *naturali*: $\mathbb{N} = \{0, 1, 2, \ldots\}$;
- i numeri *interi*: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$;
- i numeri *razionali*: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\, b \neq 0\}$.

Notiamo come in questi primi esempi abbiamo utilizzato le parentesi *graffe* per racchiudere gli elementi dell'insieme (come per $\mathbb{N}$ o per $\mathbb{Z}$) o per descriverne una proprietà che li caratterizza (come per $\mathbb{Q}$). Scriveremo $a \in A$ (leggendo "a è un elemento di A", o a appartiene ad A) per indicare che a è un elemento dell'insieme A. La convenzione di usare lettere minuscole per gli elementi e lettere maiuscole per gli insiemi è una consuetudine, ma non è di certo una regola! Indicheremo con $\emptyset$ l'insieme *vuoto*, cioè l'insieme che non contiene alcun elemento.

Se A e B sono insiemi diciamo che A è un sottoinsieme di B e scriveremo $A \subseteq B$ (leggendo "A è sottoinsieme di B", o "A è contenuto in B") se ogni elemento di A è anche un elemento di B, cioè se vale la seguente implicazione logica

$$a \in A \Leftrightarrow a \in B.$$

Osserviamo che ogni insieme A è sottoinsieme di se stesso, cioè $A \subseteq A$ per ogni insieme A e che l'insieme vuoto è un sottoinsieme di ogni insieme, cioè $\emptyset \subseteq A$ per ogni insieme A.

Se A è un qualunque insieme i suoi sottoinsiemi $\emptyset$ e A si dicono sottoinsieme *banali* di A.

Eviteremo di utilizzare la notazione $A \subset B$ perché è utilizzata con diverse accezioni in letteratura. Scriveremo invece $A \subsetneq B$ per indicare che A è un sottoinsieme di B ma che $A \neq B$.

Abbiamo appena utilizzato la notazione $A \neq B$ che è la negazione di $A = B$, ma forse vale la pensa soffermarsi un attimo su cosa voglia dire $A = B$. Coerentemente con il nostro concetto primitivo di insieme diciamo che due insiemi A e B sono uguali se contengono gli stessi elementi, cioè se vale la cosiddetta doppia inclusione: $A \subseteq B$ e $B \subseteq A$. Sarà questo il metodo standard per stabilire quando due insiemi sono uguali.

Esempio 1.1. Siano $A = \{1, 2\}$ e $B = \{x : x \text{ è soluzione di } x^3 - 4x^2 + 5x - 2 = 0\}$.Vogliamo capire se effettivamente $A = B$. La prima inclusione $A \subseteq B$ non è difficile da stabilire perchè effettivamente possiamo facilmente verificare che sia 1 che 2 sono soluzioni dell'equazione $x^3 - 4x^2 + 5x - 2 = 0$.

L'inclusione $B \subseteq A$ è invece più difficile da verificare perchè comporta la risoluzione di un'equazione di terzo grado. Tuttavia una scomposizione di routine tramite Ruffini (e se non la sai fare forse è il caso di andarla a rivedere) mostra che effettivamente le soluzioni sono proprio 1 e 2.

Esempio 1.2. Consideriamo gli insiemi $A = \{1, 2, 1, 3\}$, $B = \{1, 3, 2\}$, $C = \{1, 2, 3\}$. Osserviamo che in base alla definizione abbiamo $A = B = C$, coerentemente con il nostro concetto primitivo di insieme per cui un insieme è dato dagli elementi che lo compongono, senza considerare "ordine" o "molteplicità". Per dimostrare che $A = B$ ad esempio dobbiamo mostrare che ogni elemento di A sta anche in B e viceversa: gli elementi di A sono $1, 2, 3$ che stanno effettivamente anche in B, e viceversa.

Vediamo ora le definizioni di alcune operazioni standard che effettuiamo tra insiemi.

Definizione. Siano A, B due sottoinsiemi di un insieme U.

(1) L'unione tra A e B è
$$A \cup B = \{x \in U : x \in A \text{ o } x \in B\};$$
(2) l'intersezione tra A e B è
$$A \cap B = \{x \in A : x \in B\};$$
(3) il complementare di A è
$$A^C = \{x \in U : x \notin A\}.$$

Se A e B sono insiemi qualunque definiamo il loro prodotto cartesiano
$$A \times B = \{(a, b) : a \in A, b \in B\}$$
come l'insieme delle coppie ordinate la cui prima coordinata è un elemento di A e la seconda un elemento di B.

Osserviamo che se A e B sono insiemi finiti abbiamo $|A \times B| = |A| \cdot |B|$. Il prodotto cartesiano può essere generalizzato al caso di più di due fattori in modo naturale, ad esempio con tre insiemi abbiamo
$$A \times B \times C = \{(a, b, c) : a \in, b \in B, c \in C\}.$$
Il prodotto cartesiano di un insieme A con se stesso n volte viene detto potenza cartesiana e si indica con A^n.

Esercizio 1.3. Consideriamo tre sottoinsiemi A, B, C di un insieme universo U. Vale allora la seguente proprietà distributiva dell'unione rispetto all'intersezione
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Possiamo fare un passo di astrazione in più e considerare insiemi i cui elementi sono a loro volta insiemi.

Definizione. Data un insieme A l'insieme dei sottoinsiemi o insieme delle parti $\mathcal{P}(A)$ è
$$\mathcal{P}(A) = \{X : X \subseteq A\}$$

Ad esempio, se $A = \{1, a, \pi\}$ abbiamo

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{a\}, \{\pi\}, \{1, a\}, \{1, \pi\}, \{a, \pi\}, A\} :$$

in questo caso l'insieme $\mathcal{P}(A)$ ha quindi cardinalità 8. Notare l'uso delle partentesi graffe sia all'interno che all'esterno. Dimostriamo subito una proposizione di fondamentale importanza.

Proposizione 1.4. *Sia A un insieme finito, $|A| = n$. Esiste una corrispondenza biunivoca tra $\mathcal{P}(A)$ e $\{0, 1\}^n$.*

Dimostrazione. Siccome A ha n elementi possiamo assumere per semplicità che $A = \{1, 2, \ldots, n\}$. Consideriamo la seguente funzione

$$F : \mathcal{P}(A) \longrightarrow \{0, 1\}^n$$

definita in questo modo: se $X \in \mathcal{P}(A)$ è un sottoinsieme di A poniamo $F(X) = (s_1, \ldots, s_n)$, dove

$$s_i = \begin{cases} 1 & \text{se } i \in X \\ 0 & \text{altrimenti.} \end{cases}$$

Ad esempio, se $n = 4$ e $X = \{2, 3\}$ allora $F(X) = (0, 1, 1, 0)$.

Consideriamo ora $G : \{0, 1\}^n \to \mathcal{P}(A)$ data da

$$G((s_1, \ldots, s_n)) = \{i : s_i = 1\}.$$

Ad esempio, se $S = (1, 0, 1, 0)$ allora $G(S) = \{1, 3\}$. Ci si convince facilmente che F e G sono una l'inversa dell'altra e quindi sono delle corrispondenza biunivoche.

□

Esempio 1.5. Se $A = \{1, 2, 3\}$ le applicazioni F e G descritte nella precedente proposizione agiscono nel modo seguente

$$\begin{array}{ccc} \emptyset & \leftrightarrow & (0,0,0) \\ \{1\} & \leftrightarrow & (1,0,0) \\ \{2\} & \leftrightarrow & (0,1,0) \\ \{3\} & \leftrightarrow & (0,0,1) \\ \{1,2\} & \leftrightarrow & (1,1,0) \\ \{2,3\} & \leftrightarrow & (0,1,1) \\ \{1,3\} & \leftrightarrow & (1,0,1) \\ \{1,2,3\} & \leftrightarrow & (1,1,1) \end{array}$$

Dalla proposizione precedente possiamo dedurre che se $|A| = n$ allora $\{\mathcal{P}(A)\} = 2^n$.

Il seguente è un concetto fondamentale che diamo in modo astratto

Definizione. Una relazione R su un insieme A è un sottoinsieme di $A \times A$.

Se la coppia $(a, b) \in R$ diciamo che a è in relazione con b e scriviamo anche $a_R b$ (leggendo a è in relazione R con b).

Esempio 1.6. Se A sono i bambini di un asilo potremmo considerare le relazioni

$$R = \{(a, b) : a, b \in A,\ a \text{ ha dato una spinta a } b\}$$

$$S = \{(a, b) : a, b \in A,\ a \text{ ha giocato con } b\}$$

Una relazione fondamentale in questo corso è la seguente:

Definizione (Congruenza modulo n)**.** La congruenza modulo n è la relazione su $\mathbb{Z}$ data da "a è in relazione con b" se $a - b$ è multiplo di n. Scriveremo in questo caso

$$a \equiv b \mod n$$

e diremo ch a è congruente a b modulo n, o semplicemente che a è congruente a b qualora il modulo fosse sottinteso.

Le relazioni assumono un interesse particolare se soddisfano alcune delle seguenti proprietà

(R) Proprietà riflessiva: $a_R a$ per ogni $a \in A$;
(S) Proprietà simmetrica: per ogni $a, b \in A$ tali che $a_R b$ si ha $b_R a$;
(A) Proprietà antisimmetrica: per ogni $a, b \in A$, se $a_R b$ e $b_R a$ allora $a = b$;
(T) Proprietà transitiva: per ogni $a, b, c \in A$ tali che $a_R b$ e $b_R c$ si ha $a_R c$.

Esercizio 1.7. Sia A un insieme. Mostrare che l'unica relazione R che soddisfa le quattro proprietà è l'identità, cioè si ha

$$R = \{(a, a) : a \in A\}.$$

Definizione.

- Una relazione R si dice *relazione d'ordine* se soddisfa le proprietà (R), (A), (T).
- Una relazione d'ordine si dice *totale* se per ogni $a, b \in A$ si ha $a_R b$ oppure $b_R a$.
- Una relazione si dice di *equivalenza* se soddisfa le proprietà (R), (S), (T).

Esercizio 1.8.

- La relazione su $\mathbb{Z}$ data da $a_R b$ se $a \leq b$ è una relazione d'ordine totale;
- La relazione su $\mathcal{P}(A)$ data da $X_R Y$ se $X \subseteq Y$ è una relazione d'ordine non totale (se A ha almeno due elementi);
- la relazione di congruenza modulo n è una relazione d'equivalenza su $\mathbb{Z}$.

Se R è una relazione d'ordine si è soliti utilizzare una notazione del tipo $a \preceq b$, o $a \leq b$, o $a \subseteq b$ piuttosto che $a_R b$ in modo da porre in evidenza l'ordinamento degli elementi dato dalla relazione stessa.

Un modo tradizionale di rappresentare una relazione d'ordine $\preceq$ su un insieme finito A è quello di considerare il suo *diagramma di Hasse*. Questo diagramma viene costruito nel seguente modo:

1) Si rappresenta ogni elemento di A come un vertice del diagramma;

2) Se $a \prec b$ e non esiste c tale che $a \prec c \prec b$ si disegna un segmento da a a b con l'accortezza di disegnare il punto a più in basso del punto b. Grazie alla proprietà transitiva della relazione d'ordine possiamo dedurre che per ogni $x, y \in A$ abbiamo $x \prec y$ se e solo

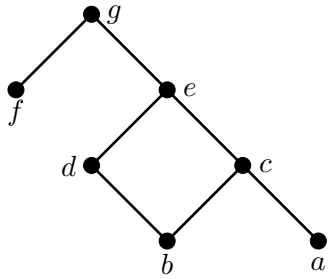

FIGURE 1. Diagramma di Hasse di una relazione d'ordine sull'insieme $A = \{a, b, c, d, e, f\}$.

se esiste un cammino da x a y nel diagramma che non va mai verso il basso. Ad esempio nella relazione d'ordine rappresentata in Figura 1 abbiamo $a \prec g$, ma $a \not\prec f$ e $f \not\prec a$.

Ci concentriamo ora sulle relazioni d'equivalenza, di gran lunga le più importanti in questo corso. Sia quindi R una relazione d'equivalenza su un insieme A.

Definizione. Sia $a \in A$. La classe di equivalenza di A è

$$[a]_R = \{b \in A : b_R a\}.$$

Esempio 1.9. consideriamo l'insieme $\mathbb{N}$ con la relazione

$$a_R b \Leftrightarrow a \text{ e } b \text{ hanno la stessa parità.}$$

Abbiamo

$$[4]_R = \{0, 2, 4, \ldots\}.$$

Chiaramente abbiamo ad esempio $[4]_R = [10]_R = [0]_R$.

Le considerazioni fatte in questo esempio si generalizzano ad ogni relazione d'equivalenza.

Proposizione 1.10. *Sia R una relazione d'equivalenza su un insieme A e siano $a, b \in A$. Allora*

$$a_R b \text{ se e solo se } [a]_R = [b]_R.$$

Dimostrazione. Lasciata per esercizio (ma fatta in aula; è importante da fare osservando che si utilizzano tutte e tre le proprietà di una relazione d'equivalenza). □

Ogni elemento di una classe di equivalenza viene comunemente detto *rappresentante* della classe.

Riprendiamo la relazione di congruenza modulo n: quante e quali sono le classi di equivalenza in questo caso? Prendiamo ad esempio $n = 6$. Noi sappiamo (?) che ogni intero si può dividere per 6 dando un resto compreso tra 0 e 5. Osserviamo che due interi che danno lo stesso resto sono congruenti: infatti, se $a = 6q_1 + r$ e $b = 6q_2 + r$ allora $a - b = 6(q_1 - q_2)$ è un multiplo di 6. Da qui deduciamo che abbiamo *al più* 6 classi e queste sono $[0]_6, [1]_6, [2]_6, \ldots, [5]_6$. D'altra parte notiamo che i numeri da 0 a 5 non

sono congruenti perché le loro differenze non sono mai multiplo di 6. Concludiamo che effettivamente abbiamo esattamente 6 classi.

L'insieme delle classi di equivalenza di $\mathbb{Z}$ rispetto alla congruenza modulo 6 si indica con

$$\mathbb{Z}_{/6} = \{[0]_6, [1]_6, \dots, [5]_6\}$$

ed è quindi un insieme con 6 elementi.

Chiaramente possiamo ripetere questo discorso per un qualunque intero $n > 1$ al posto di 6 ottenendo un insieme con n elementi (i.e., classi):

$$\mathbb{Z}_{/n} = \{[0]_n, [1]_n, \dots, [n-1]_n\}.$$

L'insieme delle classi di congruenza modulo n può essere dotato di una struttura algebrica molto ricca, dotata di due operazioni: somma e prodotto.

Definizione. Definiamo su $\mathbb{Z}_{/n}$ le seguenti operazioni di somma e prodotto: poniamo, per ogni $a, b \in \mathbb{Z}$,

- $[a]_n + [b]_n = [a+b]_n$;
- $[a]_n \cdot [b]_n = [a \cdot b]_n$.

Osservazione 1. In questa definizione abbiamo utilizzato i rappresentanti per definire le operazioni su $\mathbb{Z}_{/n}$. Ciò è legittimo purché la definizione non dipenda dal rappresentante scelto della classe, o come si dice solitamente, la definizione sia *ben posta*.

Facciamo un esempio di operazione mal posta. Definiamo la seguente operazione su $\mathbb{Z}_{/6}$:

$$[a]_6 * [b]_6 = \left[\lfloor \frac{a+b}{2} \rfloor\right]_6,$$

dove $\lfloor x \rfloor$ indica la parte intera di x, cioè il più grande intero $\leq x$. Osserviamo che

$$[2] * [3] = [3] \text{ e } [2] * [9] = [5].$$

Questo mostra che la definizione è mal posta perchè $[3] = [9]$ e quindi il risultato cambia a seconda del rappresentante scelto. Verifichiamo che somma e prodotto sono invece ben poste: Supponiamo $a \equiv a'$ e $b \equiv b'$ dobbiamo mostrare che $[a+b] = [a'+b']$ e che $[ab] = [a'b']$. Osserviamo che $a' = a + kn$ e $b' = b + hn$ per opportuni interi h e k. Abbiamo quindi

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

per cui $[a+b] = [a'+b']$ e

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b'-b) + b(a'-a) = a'hn + bkn = n(a'h + bk)$$

per cui $[a'b'] = [ab]$.

Facciamo un esempio. In $\mathbb{Z}_{/6}$ abbiamo $[2] = [8]$ e $[5] = [10]$. Proviamo a calcolare un prodotto usando diversi rappresentanti:

$$[2][5] = [10], \ [8][11] = [88]$$

e effettivamente $[10] = [88] = [4]$.

Le operazioni di somma e prodotto danno a $\mathbb{Z}_{/n}$ la struttura di anello, che non definiamo ora ma che vedrete in dettaglio nel corso di Algebra 2.

Osserviamo che [0] e [1] sono elementi neutri rispetto alla somma e al prodotto in $\mathbb{Z}_{/n}$ rispettivamente. Mentre ogni elemento $[a]$ ha un "opposto" rispetto alla somma dato da $[-a]$ non è detto che un elemento abbia un inverso rispetto al prodotto. Ad esempio in $\mathbb{Z}_{/4}$ abbiamo che $[3]_4$ è inversa di se stessa in quanto $[3]_4 \cdot [3]_4 = [1]_4$, mentre $[2]_4$ non ammette inversa (perché?). Se ogni elemento di $\mathbb{Z}_{/n}$ diverso da [0] é invertibile diciamo che $\mathbb{Z}_{/n}$ è un *campo*: vedremo in seguito che questo capita se e solo se n è un numero primo.

Il concetto di partizione di un insieme è strettamente correlato a quello di relazione di equivalenza.

Definizione. Una *partizione* di un insieme A è un insieme $P = \{A_i,\, i \in I\}$ i cui elementi sono sottoinsiemi di A tale che

(1) $A_i \neq \emptyset$ per ogni $i \in I$;
(2) $A_i \cap A_j = \emptyset$ per ogni $i \neq j$;
(3) $\cup_{i\in I} A_i = A$

In altre parole una partizione altri non è che una suddivisione di un insieme. I sottoinsiemi A_i si dicono talvolta *blocchi* della partizione.

Proposizione 1.11. *Le classi di equivalenza di una relazione di equivalenza formano una partizione. Viceversa, data una partizione, la relazione definita da $a_R b$ se a e b appartengono allo stesso blocco è una relazione di equivalenza le cui classi sono i blocchi della partizione stessa.*

Dimostrazione. □

Abbiamo già considerato l'insieme delle classi di equivalenza (o, equivalentemente, la partizione associata) nel caso della congruenza modulo n. Possiamo generalizzare questo concetto ad una relazione d'equivalenza qualsiasi.

Definizione. Data una relazione d'equivalenza R su un insieme A *l'insieme quoziente* è semplicemente l'insieme delle classi di equivalenza. Lo indicheremo

$$A/R,\;\; A/\sim,\;\; A/\equiv$$

a seconda di come indichiamo la relazione di equivalenza.

Una funzione $F : A \to B$ di dominio un insieme A e codominio un insieme B associa ad ogni elemento a di A uno e un solo elemento dell'insieme B denotato con $F(a)$. L'immagine di F è il sottoinsieme di B

$$Im(F) = \{F(a) :\, a \in A\}$$

e la funzione si dice suriettiva se $B = Im(F)$.

Proposizione 1.12. *Sia $F : A \to B$ una funzione. La relazione $\sim$ su A data da $a \sim b$ se $F(a) = F(b)$ è una relazione d'equivalenza. Inoltre la funzione indotta*

$$\bar{F} : A/\sim \to Im(F)$$

data da $\bar{F}([a]) = F(a)$ è ben definita ed è una corrispondenza biunivoca.

Dimostrazione. Esercizio. □

Esempio 1.13. Consideriamo la funzione $F : \mathbb{Z} \to \mathbb{Z}$ data da $F(n) = n^2$. Abbiamo $Im(F) = \{0, 1, 4, 9, 16 \ldots\}$. Le classi di equivalenza associate sono $[0] = \{0\}$, $[1] = \{1, -1\}$, $[2] = \{-2, 2\}$ e la corrispondenza biunivoca é data da $\bar{F}([n]) = n^2$.

Esempio 1.14. Sia $A = \mathbb{N} \times \mathbb{N}$ e consideriamo la funzione

$$F : A \to \mathbb{Z}$$

data $F((a, b)) = a - b$. La funzione F è suriettiva e la relazione d'equivalenza associata è $(a, b) \sim (c, d)$ se $a + d = c + b$. Come è fatta la classe di $(1, 3)$? Abbiamo

$$[(1, 3)] = \{(0, 2), (1, 3), (2, 4), (3, 5), \ldots\}.$$

2. Principio del buon ordinamento e il principio di induzione

In matematica ci sono degli enunciati che vengono accettati per buoni senza bisogno di dimostrazione: vengono chiamati principi o assiomi. Una buona teoria matematica cerca di ridurre gli assiomi al minimo e di dimostrare con passaggi logico-deduttivi i teoremi. In questo corso diamo per buono il seguente

Principio 2.1 (di buon ordinamento)**.** *Ogni sottoinsieme A non vuoto di $\mathbb{N}$ ammette un minimo, cioè esiste $a \in A$ tale che $a \leq a'$ per ogni $a' \in A$.*

Penso che un attimo di riflessione ci faccia capire come questo principio sia valido e che quindi possiamo accettarlo per vero. Deduciamo ora dal principio del buon ordinamento un risultato, che chiamiamo anche principio perché talvolta (in una sua riformulazione opportuna) viene utilizzato al posto del principio del buon ordinamento come punto di partenza, e che invece noi dimostriamo come sia una conseguenza. Il principio di induzione è alla base di tante dimostrazioni in algebra e in tutte le branche della matematica. Vediamo il suo enunciato:

Principio 2.2 (di induzione 1)**.** *Sia $P(n)$ una proposizione che abbia senso per ogni intero $n \geq n_0$. Supponiamo che*

- *(passo base)* $P(n_0)$ *è vera;*
- *(passo induttivo)* $P(n)$ *vera implica che anche* $P(n + 1)$ *è vera, per ogni* $n \geq n_0$.

Allora $P(n)$ è vera per ogni $n \geq n_0$.

Dimostrazione. Sia A il sottoinsieme di $\mathbb{N}$ dato da

$$A = \{n \in \mathbb{N} : \ n \geq n_0, \ P(n) \text{ è falsa.}\}$$

Vogliamo dimostrare che $A = \emptyset$ e procediamo per assurdo, cioè supponendo che $A \neq \emptyset$ e trovando una contraddizione. Per il principio del buon ordinamento esiste un elemento minimo $a \in A$. Per definizione di A abbiamo che $P(a)$ è falsa e quindi $a \neq n_0$ perché per ipotesi $P(n_0)$ è vera. Abbiamo quindi $a > n_0$ e per minimalità di a abbiamo che $a - 1 \notin A$ e siccome $a - 1 \geq n_0$ questo vuol dire $P(a - 1)$ vera. Per il passo induttivo (con $n = a - 1$) dovremmo quindi avere $P(a)$ vera, e questa è una contraddizione. □

Il prossimo esempio è tipico di una dimostrazione per induzione.

Esempio 2.3. Si ha $1+2+\cdots+n=\frac{n(n+1)}{2}$ per ogni $n\geq 1$.
Passo base: l'affermazione è vera per $n=1$, infatti in tale caso abbiamo $1=1$.
Supponiamo ora che $P(n)$ sia vera con $n\geq 1$ e mostriamo che anche $P(n+1)$ è vera. Abbiamo,

$$1+2+\cdots+n+(n+1)=(1+2+\cdots+n)+(n+1)=\frac{n(n+1)}{2}+(n+1)=\frac{(n+1)(n+2)}{2}.$$

Talvolta nel passo induttivo si preferisce mostrare che $P(n-1)$ implica $P(n)$: ciè è chiaramente del tutto equivalente.

Esercizio 2.4. Mostrare che per ogni $n\geq 4$ si ha $n!\geq 2^n$.

Il principio di induzione viene spesso utilizzato nella seguente forma equivalente

Principio 2.5 (di induzione 2)**.** *Sia $P(n)$ una proposizione che abbia senso per ogni intero $n\geq n_0$. Supponiamo che*

- *(passo base) $P(n_0)$ è vera;*
- *(passo induttivo) per ogni $n\geq n_0$, se $P(m)$ è vera per ogni $n_0\leq m<n$ allora anche $P(n)$ è vera;*

allora $P(n)$ è vera per ogni $n\geq n_0$.

Esercizio 2.6. I numeri di Fibonacci sono definiti tramite la ricorsione $F_0=0$, $F_1=1$ e $F_n=F_{n-1}+F_{n-2}$. Mostrare che

$$F_n=\frac{((1+\sqrt{5})/2)^n-((1-\sqrt{5})/2)^n}{\sqrt{5}}$$

3. Divisibilità in $\mathbb{Z}$ e numeri primi

Abbiamo visto le relazioni d'equivalenza e come caso particolare $\mathbb{Z}_{/n}$. E in particolare abbiamo già osservato che certe volte è un campo e altre no.

Abbiamo visto le relazioni d'ordine e in particolare la divisibilità tra numeri interi positivi.

Vogliamo ora studiare questi problemi e proprietà "simultaneamente" in modo sistematico arrivando ben presto alle proprietà algebriche di $\mathbb{Z}_{/n}$, della divisibilità tra interi e della fattorizzazione di un numero intero.

Prima di tutto alcune fondamentali definizioni:

Definizione. Un numero intero $p\neq 0,\pm 1$ si dice *primo* se per ogni $a,b\in\mathbb{Z}$ tali che $p|ab$ si ha $p|a$ oppure $p|b$.
Un numero intero $p\neq 0,\pm 1$ si dice *irriducibile* se per ogni $a,b\in\mathbb{Z}$ tali che $p=ab$ si ha $a=\pm 1$ oppure $b=\pm 1$.

In queste definizioni cercheremo sempre di mantenere il linguaggio più generale possibile, in modo che potrà poi essere facilmente esteso al caso di anelli più generali.

Lemma 3.1. *Un numero primo è irriducibile.*

Proof. Se infatti $p = ab$ allora in particolare abbiamo $p \cdot 1 = ab$ e quindi $p|ab$ e quindi per ipotesi $p|a$ oppure $p|b$ e senza perdere generalità possiamo assumere che esista un intero c tale che $pc = a$. Ma allora $p = ab = pcb$ da cui segue, dividendo per p, che $1 = cb$ e quindi $b = \pm 1$. □

Osserviamo che in questa dimostrazione poco abbiamo usato della struttura algebrica di $\mathbb{Z}$, e infatti questo lemma avrà una validità molto più generale. Il fatto che un numero irriducibile sia anche primo è un fatto più peculiare e che sfrutta una proprietà particolare di $\mathbb{Z}$: la divisione con resto.

Proposizione 3.2. *Siano $a, b \in \mathbb{Z}$ con $b \neq 0$; allora esistono $q, r \in \mathbb{Z}$, con $|r| < |b|$ tali che che $a = qb + r$. Il resto r può essere scelto in modo unico se si richiede l'ulteriore condizione $0 \leq r < |b|$.*

Proof. Procediamo per induzione su $|a|$.

Il passo base in questo caso è $|a| = 0$ e in tal caso basta scegliere $q = r = 0$. Vediamo il passo induttivo: supponiamo cioè che l'enunciato sia vero per ogni a, b tali che $|a| < n$ e mostriamo che sia vero anche per una qualunque coppia a, b con $|a| = n$.

Facciamo due casi:
(caso 1) se $|a| < |b|$ basta scegliere $q = 0$ ed $r = a$.
(caso 2) se invece $|a| \geq |b|$ poniamo $\varepsilon \in \{1, -1\}$ tale che $\varepsilon a = |a|$. Poniamo $a' = \varepsilon a - |b|$ e osserviamo a questo punto che $|a'| = |a| - |b| < |a|$ per cui possiamo applicare l'ipotesi induttiva alla coppia (a', b) e quindi esistono q', r' con $|r'| < |b|$ tali che

$$a' = q'b + r'$$

da cui, sostituendo $a' = \varepsilon a - |b|$, otteniamo

$$\varepsilon a = q'b + |b| + r'.$$

Moltiplicando ora per ε e ponendo $\eta b = |b|$ concludiamo che

$$a = (\varepsilon q' + \varepsilon\eta)b + \varepsilon r'.$$

Basta quindi porre a questo punto $q = (\varepsilon q' + \varepsilon\eta)b$ e $r = \varepsilon r'$ e osservare che $|r| = |r'| < |b|$.

L'unicità della seconda parte la lasciamo per esercizio. □

La divisione con resto è una proprietà algebrica molto importante che ci permette da subito di mostrare delle proprietà basilari, tra cui l'esistenza del massimo comun divisore.

Definizione. Dati due interi a, b diciamo che $d \in \mathbb{Z}$ è un massimo comun divisore di a e b se soddisfa le seguenti proprietà:

(1) $d|a$ e $d|b$:
(2) per ogni $d' \in \mathbb{Z}$ tale che $d'|a$ e $d'|b$ si ha $d'|d$.

Osserviamo che l'esistenza di un massimo comun divisore non è automatica finché non viene dimostrata. Possiamo però osservare da subito che se d_1 e d_2 sono entrambi massimi comun divisori allora $d_1|d_2$ e $d_2|d_1$ e quindi $d_1 = \pm d_2$; viceversa, se d è un MCD allora anche $-d$ lo è. Per convenzione si è soliti scegliere come MCD quello ≥ 0.

Possiamo osservare che $MCD(a, 0) = a$ per ogni $a \in \mathbb{Z}$.

Mostriamo l'esistenza del MCD utilizzando la divisione con resto con un algoritmo che ci permette anche di determinarlo. Prima un lemma che lasciamo per esercizio (o forse no?)

Lemma 3.3. *Siano $a, b, c, d, x \in \mathbb{Z}$ tali che $a = bx + c$. Allora $d = MCD(a, b)$ se e solo se $d = MCD(b, c)$.*

Proof. Per simmetria basta mostrare che $d = \mathrm{MCD}(a, b)$ implica $d = \mathrm{MCD}(b, c)$. Infatti $d|b$ e $d|c = a - bx$. Inoltre, se $d'|b$ e $d'|c$ allora $d'|a$ e quindi $d'|d$ perché $d = \mathrm{MCD}(a, b)$. □

Siamo ora pronti a dimostrare l'esistenza del MCD utilizzando la divisione con resto

Teorema 3.4. *Siano $a, b \in \mathbb{Z}$. Allora esiste $d = MCD(a, b)$.*

Dimostrazione. Procediamo per induzione su $\min(|a|, |b|)$ e supponiamo senza perdere generalità che tale minimo sia $|b|$. Il passo base dell'induzione consiste nel considerare il caso $b = 0$: in tal caso abbiamo già osservato che $\mathrm{MCD}(a, 0) = a$.

Passiamo quindi al passo induttivo e assumiamo pertanto $|b| > 0$, cioè $b \neq 0$. Effettuiamo una divisione con resto: abbiamo $a = qb + r$ con $|r| < |b|$. Abbiamo che $\mathrm{MCD}(b, r)$ esiste per ipotesi induttiva e per il Lemma 3.3 abbiamo che anche $\mathrm{MCD}(a, b)$ esiste ed eguaglia $\mathrm{MCD}(b, r)$. □

La dimostrazione del Teorema 3.4 è di tipo "costruttivo" nel senso che determina l'esistenza prescrivendo una ricetta con cui ottenere il MCD: tale ricetta è nota come algoritmo di Euclide

Algoritmo 3.5 (di Euclide)**.** *Siano $a, b \in \mathbb{Z}$, con $|a| \geq |b|$. Allora $MCD(a, b)$ si può determinare nel modo seguente*

- *se $b = 0$ allora $MCD(a, b) = a$*
- *se $b \neq 0$ allora siano q, r con $|r| < |b|$ tali che $a = qb + r$. Allora $MCD(a, b) = MCD(b, r)$.*

Come sempre, un esempio è meglio di tante parole

Esempio 3.6. Vogliamo determinare $d = MCD(4512, 306)$. L'algoritmo dice di effettuare la divisione con resto: otteniamo

$$4512 = 14 \cdot 306 + 228$$

e che $d = MCD(306, 228)$. A questo punto abbiamo un problema analogo, ma con numeri più piccoli e possiamo ricominciare. Abbiamo

$$306 = 1 \cdot 228 + 78$$

e $d = MCD(228, 78)$. Poi abbiamo

$$228 = 2 \cdot 78 + 72$$

e $d = MCD(78, 72)$. Poi abbiamo

$$78 = 1 \cdot 72 + 6$$

e $d = MCD(72, 6)$ e infine

$$72 = 12 \cdot 6 + 0$$

e quindi $d = MCD(6, 0) = 6$.

Nell'esempio precedente abbiamo sempre scelto il resto positivo, ma ricordiamo che possiamo anche scegliere il resto negativo per velocizzare l'algoritmo purchè, in valore assoluto, sia minore del divisore. Avremmo ottenuto

$$4512 = 15 \cdot 306 - 78$$

e poi

$$306 = 4 \cdot 78 - 6$$

e infine

$$78 = 13 \cdot 6 + 0.$$

L'algoritmo di Euclide, oltre a determinare il MCD ha un'altra conseguenza di fondamentale importanza.

Corollario 3.7 (Identità di Bézout)**.** *Siano $a, b \in \mathbb{Z}$ e $d = MCD(a, b)$. Allora esistono $m, n \in \mathbb{Z}$ tali che*

$$d = ma + nb.$$

Viceversa, per ogni $x, y \in \mathbb{Z}$ si ha $d|xa + yb$ e in particolare, se esistono $x, y \in \mathbb{Z}$ tali che $xa + yb = 1$ allora $d = 1$.

Proof. Anche in questo caso facciamo vedere una dimostrazione costruttiva con una procedura ricorsiva basata sull'algoritmo di Euclide. Come ormai siamo abituati a fare procediamo per induzione su $\min(|a|, |b|)$ e supponiamo senza perdere generalità che $|a| \geq |b|$.

Passo base: se $|b| = 0$ allora $d = a$ e basta sceglire $m = 1$ e n qualsiasi.
Passo induttivo: se $|b| > 0$ facciamo la divisione con resto

$$a = qb + r$$

e ricordiamo che $d = MCD(b, r)$; per ipotesi induttiva esistono m', n' tali che $d = m'b + n'r$. Andando ora a sostituire $r = a - qb$ otteniamo $d = m'b + n'(a - qb) = n'a + (m' - qn')b$ per cui ci basterà prendere $m = n'$ e $n = m' - qn'$.

La seconda parte è una semplice osservazione: sappiamo che $d|a$ e che $d|b$ e quindi chiaramente $d|xa + yb$. □

Determiniamo un'identità di Bézout per 4512 e 306, i due numeri visti prima di cui sappiamo già che $MCD(4512, 306) = 6$. Utilizziamo prima la prima sequenza di divisioni. Sarà in questo caso conveniente iniziare dall'ultima divisione perpoi risalire fino alla prima:

abbiamo

$$\begin{aligned} 6 &= 78 - 1 \cdot 72 \\ &= 78 - 1 \cdot (228 - 2 \cdot 78) \\ &= 3 \cdot 78 - 1 \cdot 228 \\ &= 3 \cdot (306 - 228) - 228 \\ &= 3 \cdot 306 - 4 \cdot 228 \\ &= 3 \cdot 306 - 4 \cdot (4512 - 14 \cdot 306) \\ &= 59 \cdot 306 - 4 \cdot 4512 \end{aligned}$$

Chiaramente anche in questo caso potremmo utilizzare i resti negativi ed ottenere un risultato analogo

$$\begin{aligned} 6 &= 4 \cdot 78 - 306 \\ &= 4 \cdot (15 \cdot 306 - 4512) - 306 \\ &= 59 \cdot 306 - 4 \cdot 4512. \end{aligned}$$

Osserviamo comunque che l'identità di Bézout è tutt'altro che unica: ad esempio se $d = ma + nb$ uno può facilmente ottenerne un'altra in questo modo: $d = (m + b)a + (n - a)b$. Nel nostro esempio otterremmo

$$6 = 4571 \cdot 306 - 310 \cdot 4512.$$

Ora vediamo di raccogliere un po' di frutti di questo lavoro

Proposizione 3.8. *Un numero intero irriducibile è anche primo.*

Proof. Sia p un numero irriducibile e supponiamo che $p|ab$. Dobbiamo mostrare che $p|a$ oppure $p|b$. Il $MCD(p, a)$ può essere solo 1 o p perchè p è irriducibile e quindi non ha altri divisori. Se è p allora abbiamo che $p|a$ e abbiamo finito. Se è 1 abbiamo l'identità di Bézout

$$1 = ma + np$$

che moltiplicata per b dà

$$b = mab + npb.$$

Per ipotesi $p|ab$ e quindi divide entrambi gli addendi di destra e concludiamo che divide anche b. □

Possiamo ora facilmente capire quali $\mathbb{Z}_{/n}$ siano campi.

Proposizione 3.9. *Sia $n > 1$ e $a \in \mathbb{Z}$. Allora $[a]$ è invertibile in $\mathbb{Z}_n$ se e solo se $MCD(a, n) = 1$. In particolare $\mathbb{Z}_{/n}$ è un campo se e solo se n è primo.*

Dimostrazione. Supponiamo che $[a]$ sia invertibile in $\mathbb{Z}_{/n}$ e sia $[b]$ la classe inversa cioè tale che

$$[a][b] = [1] \in \mathbb{Z}_{/n}.$$

Ciò vuol dire che esiste $c \in \mathbb{Z}$ tale che

$$ab = 1 + cn;$$

per la seconda parte del Corollario 3.7 abbiamo che $MCD(a, n) = 1$: abbiamo infatti mostrato che esistono $x = b$ e $y = -c$ tali che $xa + yn = 1$.

Viceversa, supponiamo che $MCD(a, n) = 1$: allora per l'identità di Bézout esistono due interi s, t (non li chiamiamo m ed n perché n è già utilizzato) tali che

$$sa + tn = 1$$

e da questa segue che modulo n abbiamo

$$[1] = [sa + tn] = [s][a] + [t][n] = [s][a]$$

□

La dimostrazione precedente è anche costruttiva perché ci indica come determinare l'inverso di una classe invertibile in $\mathbb{Z}_n$:

Esempio 3.10. Determinare l'inverso di $[35]$ in $\mathbb{Z}_{/74}$. Abbiamo bisogno di un'identità di Bézout per cui procediamo con l'algoritmo euclideo. Abbiamo
$74 = 2 \cdot 35 + 4$
$35 = 9 \cdot 4 - 1$ da cui

$$1 = 9 \cdot 4 - 35 = 9 \cdot (74 - 2 \cdot 35) - 35 = 9 \cdot 74 - 19 \cdot 35$$

per cui l'inversa di $[35]$ è $[-19] = [55]$.

Un'ultima questione era rimasta in sospeso

Teorema 3.11 (fondamentale dell'aritmetica)**.** *Ogni numero intero $n > 1$ si scrive in modo unico (a meno dell'ordine) come prodotto di numeri primi positivi.*

Dimostrazione. (*Esistenza.*) Procediamo per induzione su n. Il passo base in questo caso è $n = 2$: in questo caso $n = 2$ che è chiaramente un numero primo.

Vediamo il passo induttivo: se n è primo non c'è niente da dimostrare. Se n non è primo allora non è neanche irriducibile e quindi si può scrivere come $n = ab$ con $1 < a, b < n$: quindi a e b ammettono una scomposizione in numeri primi e il loro prodotto è una scomposizione in primi per n.

(*Unicità.*) L'unicità deriva semplicemente dal fatto che ogni numero irriducibile è anche primo. Infatti, supponiamo che $a = p_1 \cdots p_r = q_1 \cdots q_s$ con $r \leq s$ e procediamo per induzione su r: se $r = 1$ abbiamo $p_1 = q_1 \cdots q_s$. Ma un numero irriducibile non si può fattorizzare nel prodotto di due o più irriducibili e quindi abbiamo $s = 1$ e quindi le due espressioni si riducono a $p_1 = q_1$ e non abbiamo niente da dimostrare. Altrimenti, se $r > 1$ abbiamo che $p_1 | q_1 \cdots q_s$ e quindi p_1, essendo primo, divide almeno uno tra $q_1, \ldots, q_s$. A meno di riordinare e rinominare i fattori q_i, possiamo assumere che p_1 divida q_1. Ma siccome q_1 è irriducibile questo implica che $p_1 = q_1$ e quindi $p_2 \cdots p_r = q_2 \cdots q_s$. Abbiamo quindi l'uguaglianza tra due scomposizioni in fattori irriducibili con $r - 1$ e $s - 1$ fattori

e quindi, per ipotesi induttiva, abbiamo che $r-1=s-1$, (cioè $r=s$) e che, a meno dell'ordine, $p_i=q_i$ per ogni $i=2,\dots,r$. □

Osserviamo che in questa dimostrazione abbiamo usato sia la primalità che l'irriducibilità: l'irriducibilità nell'esistenza e la primalità nell'unicità.

Chiaramente il teorema fondamentale dell'aritmetica si può estendere ai numeri interi: un intero $n\neq 0,\pm 1$ si scrive in modo unico come prodotto di interi primi a meno dell'ordine e a meno del segno.

Esercizio 3.12. Siano $a=p_1^{m_1}\cdots p_r^{m_r}$ e $b=p_1^{n_1}\cdots p_r^{n_r}$ dove i p_i sono primi distinti e gli esponenti m_i,n_i sono interi non negativi. Mostrare che

$$MCD(a,b)=p_1^{\min(m_1,n_1)}\cdots p_r^{\min(m_r,n_r)}$$

Esercizio 3.13. Dati due interi a,b diciamo che c è un loro minimo comune multiplo se $a|c$, $b|c$ e per ogni intero c' tale che $a|c'$ e $b|c'$ si ha $c|c'$. Mostrare che il minimo comune multiplo esiste e che, nella notazione dell'esercizio precedente si ha

$$mcm(a,b)=p_1^{\max(m_1,n_1)}\cdots p_r^{\max(m_r,n_r)}.$$

Non possiamo a questo punto non ricordare la celeberrima dimostrazione di Euclide dell'infinita dei numeri primi basata sul teorema fondamentale dell'aritmetica.

Teorema 3.14. *I numeri primi sono infiniti.*

Dimostrazione. Supponiamo per assurdo che i numeri primi (positivi) siano finiti e chiamiamoli $p_1,\dots,p_r$. Consideriamo il numero intero $n=p_1\cdots p_r+1$. Osserviamo che in particolare $[n]=[1]\in\mathbb{Z}_{/p_i}$ per ogni i. Il numero n avrà una sua fattorizzazione in primi, ma in questa non può comparire nessuno dei p_i altrimenti avremmo $[n]=[0]\in\mathbb{Z}_{/p_i}$ contraddicendo il teorema fondamentale dell'aritmetica. □

4. Cardinalità

Abbiamo parlato nella primissima lezione di cardinalità di un insieme: finché l'insieme è finito non abbiamo molto da aggiungere, ma quando l'insieme è infinito fenomeni abbastanza sorprendenti possono accadere.

Prima di tutto abbiamo bisogno di un po' di nomenclatura che avete già visto e che quindi non stiamo a ripetere il significato delle parole funzione, dominio, codominio, immagine, iniettiva, suriettiva, biiettiva, corrispondenza biunivoca.

Vogliamo dare un senso alle affermazioni "un insieme (infinito) è più grande di in un altro" o "due insiemi (infiniti) sono grandi uguali". Procediamo con ordine e iniziamo dalla seconda affermazione.

Definizione. Diciamo che due insiemi (infiniti) A e B hanno la stessa cardinalità se esiste una corrispondenza biunivoca tra di loro. Scriviamo in questo caso $\mathrm{Card}(A)=\mathrm{Card}(B)$.

Si vede facilmente che, dato un insieme di insiemi, "avere la stessa cardinalità" è una relazione di equivalenza (esercizio).

Definizione. Un insieme A si dice numerabile se ha la stessa cardinalità di $\mathbb{N}$, cioè $\mathrm{Card}(A) = \mathrm{Card}(\mathbb{N})$. Talvolta per dire che A è numerabile si scrive $\mathrm{Card}(A) = \aleph_0$ (leggi alef zero, ma non non lo faremo mai).

Esercizio 4.1. Mostrare che ogni sottoinsieme infinito di $\mathbb{N}$ è numerabile.

Per stabilire se un insieme A è numerabile dobbiamo riuscire ad "elencare" in un elenco infinito gli elementi di A dicendo chi è il primo, chi il secondo e così via. Questo è esattamente quello che produce una corrispondenza biunivoca di un insieme con $\mathbb{N}$.

Esempio 4.2. L'insieme $\mathbb{Z}$ dei numeri interi è numerabile. Infatti possiamo scrivere

$$\mathbb{Z} = \{0, +1, -1, +2, -2, \ldots\}.$$

Analogamente possiamo mostrare che l'unione di due insiemi finiti e' numerabile. Per induzione, otteniamo che l'unione di un numero finito di insiemi numerabili e' numerabile. L'insieme $\mathbb{Q}_{>0}$ costituito dai numeri razionali positivi è anche numerabile, infatti,

$$\mathbb{Q}_{>0} = \{0, 1, \frac{1}{2}, 2, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, 3, \frac{1}{4}, \frac{3}{4}, \frac{4}{3}, 4 \ldots\}.$$

Gli elementi di $\mathbb{Q}$ li abbiamo elencati in questo modo: abbiamo prima scritto tutti i numeri razionali che si possono scrivere utilizzando 1 (cioè solo 1) sia al numeratore che al denominatore; poi abbiamo scritto in ordine crescente tutti i numeri razionali che si possono ottenere utilizzando anche il numero 2 (cioè $1/2$ e 2), poi quelli che utilizzano anche il 3 cioè $\frac{1}{3}, \frac{2}{3}, \frac{3}{2}, 3$ e così via. È chiaro che in questo modo possiamo elencare tutti i numeri razionali positivi. Chiaramente questo non è l'unico modo per farlo e anzi ce ne sono infiniti.

Esercizio 4.3. Mostrare che che anche $\mathbb{Q}$ è numerabile.

L'esempio di $\mathbb{Q}$ si può generalizzare in modo naturale nel prossimo famoso risultato.

Teorema 4.4 (delle diagonali di Cantor)**.** *Il prodotto cartesiano di due insiemi numerabili è numerabile. L'unione numerabile di insiemi numerabili è ancora numerabile, ovvero se A_n al variare di $n \in \mathbb{N}$ sono insiemi numerabili allora $\cup A_n$ è un insieme numerabile.*

Dimostrazione. In classe e' stato mostrato il primo enunciato. Mostriamo il secondo, la cui dimostrazione e' del tutto analoga. Siccome ogni A_n è numerabile possiamo scrivere i suoi elementi in un elenco infinito:

$$A_n = \{a_{n0}, a_{n1}, a_{n2}, \ldots\}.$$

Possiamo ora riarrangiare tutti gli elementi dei vari A_n in una tabella infinita nel seguente modo

$$\begin{array}{lllll} a_{00} & a_{01} & a_{02} & a_{03} & \cdots \\ a_{10} & a_{11} & a_{12} & \cdots & \\ a_{20} & a_{21} & \cdots & & \\ a_{30} & \cdots & & & \\ \vdots & & & & \end{array}$$

in modo che gli elementi delle prima riga siano quelli di A_0, quelli della seconda riga quelli di A_1 e così via. Possiamo a questo punto leggere gli elementi dell'unione degli A_i lungo le diagonali che vanno da sud-ovest a nord-est. Nella prima diagonale abbiamo solo a_00 nella seconda abbiamo a_{10}, a_{01}, nella terza abbiamo a_{20}, a_{11}, a_{02}... In questo modo modo possiamo "elencare" tutti gli elementi di dell'unione degli A_n nel seguente modo

$$\bigcup_{n\in\mathbb{N}} A_n = \{a_{00}, a_{10}, a_{01}, a_{20}, a_{11}, a_{20}, a_{30}, \ldots\}.$$

□

Due parole di attenzione riguardo questa dimostrazione: abbiamo implicitamente supposto che gli insiemi A_n siano disgiunti, cioè che non abbiano elementi in comune. In realtà se ciò accadesse dovremmo solo eliminare dal nostro elenco tutte le ripetizioni per cui rimarrebbe in ogni caso un elenco infinito e la dimostrazione continua a valere. Inoltre, la stessa idea di dimostrazione vale se alcuni degli A_n dovessero essere finiti per cui potremmo più in generale dare il seguente enunciato.

Corollario 4.5. *Un'unione finita o numerabile di insiemi finiti o numerabili è finita o numerabile.*

Potremmo essere tentati di pensare a questo punto che tutti gli insiemi infiniti siano numerabili. Ciò non è vero come mostra il prossimo risultato.

Proposizione 4.6. *L'insieme $\{0,1\}^{\mathbb{N}}$ di tutte le sequenze binarie infinite non è numerabile.*

Dimostrazione. Supponiamo per assurdo che sia possibile elencare tutte le sequenze binarie e quindi scrivere

$$\{0,1\}^{\mathbb{N}} = \{\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}, \ldots\},$$

dove quindi le $\mathbf{b_i}$ sono *tutte* le sequenze binarie.

Costruiamo a questo punto una nuova sequenza binaria $\mathbf{d}$ nel seguente modo:
la prima coordinata di $\mathbf{d}$ è diversa dalla prima coordinata di $\mathbf{b_1}$: ad esempio se $\mathbf{b_1}$ comincia con 0 allora $\mathbf{d}$ comincia con 1 e viceversa.
La seconda coordinata di $\mathbf{d}$ è diversa dalla seconda coordinata di $\mathbf{b_2}$.
La terza coordinata di $\mathbf{d}$ è diversa dalla terza coordinata di $\mathbf{b_3}$ e cosí via. Si ha che la sequenza $\mathbf{d}$ cosí costruita è diversa dalla sequenza $\mathbf{b_i}$ per ogni i avendone la coordinata di posto i diversa. Abbiamo quindi una contraddizione perché avremmo costruito una sequenza binaria infinita che non sta in $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \}$.

□

Si vede facilmente che $\{0,1\}^{\mathbb{N}}$ e' in biezione con l'insieme $\mathcal{P}(\mathbb{N})$ delle parti dei numeri naturali: la biezione e' del tutto analoga a quela costruita nella Proposizione 1.4/

Ci siamo convinti ora che la nozione di cardinalità ha un senso preciso anche per insiemi infiniti, che un sottoinsieme proprio può avere la stessa cardinalità dell'insieme stesso e che esistono insiemi infiniti di cardinalità diversa.

Cosa vuol dire però che un insieme è più grande di un altro? La definizione più naturale che viene in mente è la seguente.

Definizione. Dati due insiemi A e B diciamo che $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ se esiste una funzione iniettiva $f : A \to B$.

La definizione posta in questo modo ha perfettamente senso, ma c'è una domanda naturale la cui risposta è tutt'altro che scontata: è vero che se $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ e $\mathrm{Card}(B) \leq \mathrm{Card}(A)$ allora $\mathrm{Card}(A) = \mathrm{Card}(B)$?

Detto in termini di relazione d'ordine ci stiamo chiedendo se la relazione $\leq$ definita qui sopra sull'insieme delle possibili cardinalità soddisfa la proprietà antisimmetrica e quindi è una relazione d'ordine (le proprietà riflessiva e transitiva sono in questo caso molto semplici). È questo il contenuto del prossimo risultato (che non e' stato dimostrato a lezione, e non fa parte del programma d'esame).

Teorema 4.7 (Schroeder-Bernstein)**.** *Siano A, B insiemi tali che* $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ *e* $\mathrm{Card}(B) \leq \mathrm{Card}(A)$. *Allora* $\mathrm{Card}(A) = \mathrm{Card}(B)$.

Dimostrazione. Siano $f : A \to B$ e $g : B \to A$ funzioni iniettive. Osserviamo che partendo da un elemento di A possiamo applicare f, e poi g, e poi ancora f all'infinito. Se un elemento di A è nell'immagine di g possiamo anche "applicare" g^{-1} (in modo unico per iniettività) e poi eventualmente f^{-1} e così via. Ci sono tre possibilità: (1)ci fermiamo in un punto di A, (2) ci fermiamo in un punto di B o (3) possiamo andare avanti all'infinito. Abbiamo in questo modo formato tre tipi di "stringhe" e ogni elemento di A o di B appartiene ad un'unica stringa.

Definiamo ora una funzione $h : A \to B$ e poi mostriamo che si tratta di una corrispondenza biunivoca.

Poniamo

$$h(a) = \begin{cases} f(a) & \text{se } a \text{ è in una stringa di tipo (1)} \\ g^{-1}(a) & \text{se } a \text{ è in una stringa di tipo (2) o (3)} \end{cases}$$

Osserviamo che $h(a)$ è nella stessa stringa di a per ogni $a \in A$. Mostriamo che h è iniettiva e prendiamo due elementi distinti $a, a' \in A$, con $h(a) = h(a')$. Allora a ed a' stanno nella stessa stringa e quindi $f(a) = f(a')$ oppure $g^{-1}(a) = g^{-1}(a')$. Nel primo caso abbiamo $a = a'$ per iniettività di f, nel secondo per iniettività di g.

Mostriamo che h è suriettiva. Se $b \in B$ è in una stringa di tipo (1) allora la stringa non può iniziare da b e si ha $b = f(a)$ e quindi $b = h(a)$. Se b è in una stringa di tipo (2) o (3) allora $b = h(g(b))$. □

Esempio 4.8. Mostrare che esiste una corrispondenza biunivoca $h : [0, 1] \to [0, 1)$ Abbiamo che $f : [0, 1] \to [0, 1)$ data da $f(x) = x/2$ e $g : [0, 1) \to [0, 1]$ data da $g(x) = x$ sono entrambe iniettive e quindi per il teorema di Schhroeder-Bernstein esiste una corrispondenza biunivoca. Guardando la dimostrazione del teorema abbiamo che gli elementi di $[0, 1]$ in stringhe di tipo 1 sono tutti i numeri del tipo 2^{-n} per ogni $n \geq 0$, mentre tutti gli altri sono in stringhe di tipo (2). La dimostrazione del teorema fornisce

$$h(x) = \begin{cases} x/2 & \text{se } x = 2^{-n} \\ x & \text{altrimenti} \end{cases}$$

Si può verificare anche direttamente che questa h risulta una biiezione.

Teorema 4.9. *L'insieme delle successioni binarie* $\{0,1\}^{\mathbb{N}}$ *è in biezione con l'intervallo aperto* $(0,1)$.

Proof. Costruiamo due applicazioni iniettive e applichiamo il teorema di Schroeder-Bernstein. Una applicazione iniettiva

$$\phi : (0,1) \to \{0,1\}^{\mathbb{N}}$$

è costruita scrivendo ogni numero in base 2 nel modo piu' breve possibile (ovvero senza terminare con 1 periodico), poi associando al numero la sequenza delle sue cifre binarie dopo la virgola. Non e' suriettiva perche', ad esempio $011111\ldots \notin Im(\phi)$ dato che $1/2$ viene scritto come $0,1$ e non come $0,0\overline{1}$.

D'altra parte, una applicazione iniettiva

$$\psi : \{0,1\}^{\mathbb{N}} \to (0,1)$$

è ottenuta trasformando ogni successione di cifre 0 e 1 in una successione di 0 e 2 (sostituendo le cifre 1 con dei 2), poi prendendo il numero reale che scritto in base 3 ha le cifre corrispondenti dopo la virgola. Ad esempio $\psi(1011001\ldots) = 0,2022002\ldots$ che è la scrittura in base 3 del numero $2/3 + 2/27 + 2/81 + \frac{2}{3^7} + \ldots$.

L'applicazione ψ e' chiaramente iniettiva, ma non suriettiva dato che non contiene $1/2$. In effetti la sua immagine è l'insieme di Cantor.

Per il teorema di Schroeder-Bernstein esiste una biezione h tra i due insiemi (anche se scriverla esplicitamente sarebbe tutt'altro che semplice). □

D'altra parte, $(0,1)$ è in biezione con $\mathbb{R}$ (esercizio), quindi $\mathbb{R}$ non è numerabile.

5. La ϕ di Eulero e il teorema cinese del resto

Vogliamo addentrarci ulteriormente nello studio delle classi resto modulo n. Abbiamo già stabilito quando una classe resto è invertibile: la classe $[m]$ è invertibile in $\mathbb{Z}_{/n}$ se e solamente se $MCD(m,n) = 1$ (vedi Proposizione 3.9). Abbiamo anche visto un metodo costruttivo per determinare l'inversa tramite l'identità di Bézout. Un metodo alternativo è basato sui classicissimi teoremi di Eulero e Fermat che andiamo ora a vedere.

Un argomento elementare che non sorprenderà e che utilizzeremo più volte oggi è il seguente: supponiamo che A e B siano due insiemi finiti tali che $|A| = |B|$ e sia $f : A \to B$ una funzione iniettiva. Allora f è una corrispondenza biunivoca tra A e B.

Teorema 5.1 (piccolo di Fermat)**.** *Sia p un primo (positivo) e $a \in \mathbb{Z}$ non divisibile per p. Allora*

$$a^{p-1} \equiv 1 \mod p.$$

Dimostrazione. Consideriamo i primi $p-1$ multipli di a

$$a,\ 2a,\ \ldots,\ (p-1)a$$

e osserviamo che due di questi non possono essere nella stessa classe modulo p. Infatti se così fosse avremmo due indici $0 < i < j \leq p-1$ tali che

$$[ia] = [ja] \mod p.$$

Sappiamo tuttavia che $[a]$ è invertibile in $\mathbb{Z}_{/p}$ e se chiamiamo $[b]$ la sua inversa avremmo

$$[i] = [i][1] = [i][ab] = [iab] = [jab] = [j][ab] = [j][1] = [j] \mod p,$$

che chiaramente è una contraddizione. Abbiamo quindi che questi $p-1$ multipli di a rappresentano classi distinte modulo p e quindi (siccome sono tutte invertibili) rappresentano *tutte* le classi invertibili di $\mathbb{Z}_{/p}$. Abbiamo quindi

$$\{[1],[2],\ldots,[p-1]\} = \{[a],[2a],\ldots,[(p-1)a]\}.$$

Moltiplicando tutte le classi di questo insieme nelle sue due descrizioni otteniamo

$$[1][2]\cdots[p-1] = [a][2a]\cdots[(p-1)a] = [1][2]\cdots[p-1][a^{p-1}].$$

Moltiplicando ora per gli inversi di [1], [2],..., $[p-1]$ otteniamo $[1] = [a^{p-1}]$. □

Il piccolo teorema di Fermat viene talvolta enunciato nella seguente forma equivalente: per ogni primo p e per ogni intero a si ha $a^p \equiv a \mod p$. L'equivalenza è poco più che un'osservazione e la lasciamo per esercizio.

Come anticipato, questo teorema permette di calcolare anche l'inverso di un elemento.

Corollario 5.2. *Sia p un primo e a un intero non divisibile per p. Allora la classe $[a^{p-2}]$ è l'inversa di $[a]$ in $\mathbb{Z}_{/p}$.*

Dimostrazione. Per il piccolo teorema di Fermat abbiamo $[a][a^{p-2}] = [a^{p-1}] = [1]$. □

Ad esempio, se vogliamo determinare l'inversa di $[5]$ in $\mathbb{Z}_{/29}$ possiamo calcolare

$$5^{27} \equiv (5^3)^9 \equiv 9^9 \equiv (9^3)^3 \equiv 4^3 \equiv 6 \mod 29,$$

come era chiaro che fosse visto che $5 \cdot 6 = 30 \equiv 1 \mod 29$. Il piccolo teorema di Fermat è falso in generale se p non è primo. Infatti, ad esempio, in $\mathbb{Z}_{/12}$ $5^{11} \equiv 5 \neq 1 \mod 12$. Sussiste comunque un teorema più generale che ora andiamo a studiare.

Definizione. Per ogni $n \geq 1$ definiamo

$$\begin{aligned}\phi(n) &= |\{m : 1 \leq m \leq n, MCD(m,n) = 1\}| \\ &= |\{[m] \in \mathbb{Z}_{/n} : [m] \text{ è invertibile}\}|.\end{aligned}$$

Questa funzione è nota come la ϕ di Eulero.

Ad esempio abbiamo $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$. Possiamo facilmente mostrare il seguente fatto

Proposizione 5.3. *Se p è un primo e $r > 0$ allora*

$$\phi(p^r) = p^r - p^{r-1}$$

e in particolare $\phi(p) = p - 1$.

Dimostrazione. I numeri $\leq p^r$ coprimi con p^r sono quelli che non sono multipli di p. I multipli di p minori o uguali di p^r sono esattamente p^{r-1} per cui $\phi(p^r) = p^r - p^{r-1}$. □

È apparentemente più complicato calcolare $\phi(n)$ quando n è divisibile per più di un primo. Ricordiamo che due numeri n, m si dicono coprimi se $MCD(n,m) = 1$. Il seguente risultato è famosissimo ed estremamente utile.

Teorema 5.4 (Cinese del resto, forma base)**.** *Siano n, m coprimi. Allora la funzione $\mathbb{Z}_{/nm} \to \mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$ data da*

$$[a]_{nm} \mapsto ([a]_n, [a]_m)$$

è ben posta ed è una corrispondenza biunivoca.

Equivalentemente, dati due interi b, c esiste un unico intero $x \mod mn$ tale che $x \equiv b \mod m$, e $x \equiv c \mod n$. "Unico $\mod mn$" vuol dire che l'insieme degli interi x che soddisfano queste condizioni forma una classe in $\mathbb{Z}_{/mn}$.

Dimostrazione. Lasciamo l'equivalenza tra le due affermazioni per esercizio e dimostriamo la prima.

Cosa vuol dire "è ben posta"? Il dominio della funzione è un insieme di classi di equivalenza (o equivalentemente un insieme quoziente) e per definire la funzione abbiamo utilizzato un rappresentante della classe. Bisogna essere sicuri che la definizione della funzione non dipenda dal rappresentante scelto. Ad esempio, la funzione $F : \mathbb{Z}_{/5} \to \mathbb{Z}$ data da $F([a]) = a^2$ non è ben posta.

In effetti in questo caso è ben posta: se $[a]_{nm} = [a']_{nm}$ allora la differenza $a - a'$ è un multiplo di mn e in particolare è un multiplo sia di m che di n per cui $[a]_m = [a']_m$ e $[a]_n = [a']_n$. Mostriamo che è iniettiva: se $[a]_m = [a']_m$ e $[a]_n = [a']_n$ allora $a - a'$

è un multiplo sia di m che di n e quindi, siccome $MCD(n,m) = 1$ e per il teorema fondamentale dell'aritmetica, $a - a'$ è un multiplo di nm. E quindi è anche suriettiva per ragioni di cardinalità. □

Verifichiamo il teorema cinese nel caso $n = 3$ e $m = 4$. Abbiamo infatti

$$\begin{array}{rcl}
([0]_3, [0]_4) & = & ([0]_3, [0]_4) \\
([1]_3, [1]_4) & = & ([1]_3, [1]_4) \\
([2]_3, [2]_4) & = & ([2]_3, [2]_4) \\
([3]_3, [3]_4) & = & ([0]_3, [3]_4) \\
([4]_3, [4]_4) & = & ([1]_3, [0]_4) \\
([5]_3, [5]_4) & = & ([2]_3, [1]_4) \\
([6]_3, [6]_4) & = & ([0]_3, [2]_4) \\
([7]_3, [7]_4) & = & ([1]_3, [3]_4) \\
([8]_3, [8]_4) & = & ([2]_3, [0]_4) \\
([9]_3, [9]_4) & = & ([0]_3, [1]_4) \\
([10]_3, [10]_4) & = & ([1]_3, [2]_4) \\
([11]_3, [11]_4) & = & ([2]_3, [3]_4)
\end{array}$$

Torneremo su questo risultato tra poco quando studieremo i sistemi di congruenza.

Ma perché questo teorema ci permette di calcolare la ϕ di Eulero su ogni intero n?

Corollario 5.5. *Siano n, m coprimi. Allora*

$$\phi(nm) = \phi(n)\phi(m).$$

Dimostrazione. Contiamo le coppie $([b]_n, [c]_m)$ in $\mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$ tali che sia $[b]_n$ che $[c]_m$ siano invertibili: queste sono chiaramente $\phi(n)\phi(m)$. Per il teorema cinese del resto le possiamo contare anche in un altro modo. Infatti le coppie di $\mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$ le possiamo descrivere anche come $([a]_n, [a]_m)$ al variare di $a = 1, \ldots, nm$. La coppia è formata da due elementi invertibili se e solo se a è coprimo sia con n che con m. E siccome n e m sono coprimi tra loro quest'ultima condizione è equivalente a richiedere che a sia coprimo con mn: tali coppie sono quindi $\phi(nm)$. □

Ad esempio per calcolare $\phi(36) = \phi(3^2)\phi(2^2) = 6 \cdot 2 = 12$ e in effetti i numeri minori di 36 coprimi con 36 sono 12: 1,5,7,11,13,17,19,23,25,29,31,35. Vedremo più avanti delle applicazioni della funzione ϕ di Eulero. Possiamo ora generalizzare il piccolo teorema di Fermat

Teorema 5.6 (di Eulero)**.** *Siano a, n coprimi. Allora*

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

Dimostrazione. La dimostrazione è identica a quella del piccolo teorema di Fermat (e il risultato ne è una generalizzazione ricordando che $\phi(p) = p - 1$ se p è un numero primo). Consideriamo le classi invertibili in $\mathbb{Z}_{/n}$: sappiamo che sono $\phi(n)$ e le indichiamo in questo modo $[b_1], \ldots, [b_{\phi(n)}]$. Moltiplicando queste $\phi(n)$ classi per $[a]$ otteniamo ancora la stesse $\phi(n)$ classi. Infatti $[a][b_i]$ è ancora invertibile e se fosse $[a][b_i] = [a][b_j]$ allora moltiplicando

per l'inversa di $[a]$ avremmo $[b_i] = [b_j]$. Concludiamo quindi che la moltiplicazione per $[a]$ è una corrispondenza biunivoca tra l'insieme delle classi invertibili e se stesso, cioè

$$\{[b_1], \dots, [b_{\phi(n)}]\} = \{[ab_1], \dots, [ab_{\phi(n)}]\}.$$

Moltiplicando tutte le classi di questo insieme nei due modi possibili otteniamo

$$[b_1 \cdots b_{\phi(n)}] = [a^{\phi(n)}][b_1 \cdots b_{\phi(n)}]$$

da cui deduciamo che $[a^{\phi(n)}] = [1]$ cioè $a^{\phi(n)} \equiv 1 \mod n$. □

Il piccolo teorema di Fermat può anche essere enunciato nel seguente modo:

$$a^{\phi(p)+1} \equiv a \mod p$$

per ogni intero a. Espresso in questa forma lo possiamo estendere in un risultato che avrà delle conseguenze basilari in crittografia:

Proposizione 5.7. *Sia n libero da quadrati, cioè $n = p_1 \cdots p_r$ prodotto di primi distinti. Allora per ogni intero a e per ogni intero positivo k si ha*

$$a^{k\phi(n)+1} \equiv a \mod n.$$

Proof. Sia $i \in \{1, \dots, r\}$. Se a non è divisibile per p_i allora per il piccolo teorema di Fermat abbiamo $a^{p_i - 1} \equiv 1 \mod p_i$ e quindi anche $a^{k\phi(n)} \equiv 1 \mod p_i$ perché $k\phi(n)$ è un multiplo di $p_i - 1$ e quindi anche $a^{k\phi(n)+1} \equiv a \mod p_i$.

Se invece a è divisibile per p_i chiaramente $a \equiv 0 \mod p_i$ e quindi $a^{k\phi(n)+1} \equiv a \mod p_i$.

In conclusione abbiamo $a^{k\phi(n)+1} \equiv a \mod p_i$ per ogni i e quindi anche $\mod n$. □

Mostrare per esercizio che se n non è libero da quadrati allora non è possibile trovare un numero q tale che $a^q \equiv a \mod n$ per ogni $a \in \mathbb{Z}$.

6. Congruenze e sistemi di congruenze lineari

Diamo in questa sezione un breve accenno ai sistemi di congruenze lineari. Dati due interi a, b e un intero positivo n risolvere la congruenza

$$ax \equiv b \mod n$$

vuole dire trovare tutti gli interi x che soddisfano questa condizione. Chiaramente se x è una soluzione ogni altro elemento nella classe di x modulo n è un'altra soluzione. Osserviamo anche che la congruenza può essere vista come un'equazione in $\mathbb{Z}_{/n}$:

$$[a][x] = [b].$$

Facciamo qualche piccola osservazione

Lemma 6.1. *Siano a, b interi, $n > 1$ e sia $d = MCD(a, n)$. Allora*

(1) *se $d \not| b$ la congruenza non ammette soluzioni;*

(2) *se $d|b$ allora la congruenza è equivalente alla seguente*

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d}$$

e le soluzioni formano una classe di congruenza modulo $\frac{n}{d}$. In particolare se $d = 1$ l'equazione ammette un'unica soluzione $\mod n$.

Proof. Se x è una soluzione allora esiste $k \in \mathbb{Z}$ tale che $b = ax+kn$ e quindi necessariamente $d|b$, (in quanto $d|a$ e $d|b$). Supponiamo quindi che $d|b$: è chiaro che $ax - b$ è multiplo di n se e solo se $\frac{a}{d}x - \frac{b}{d}$ è multiplo di $\frac{n}{d}$ da cui l'equivalenza tra le due congruenze.

Per quel che riguarda l'ultima affermazione possiamo quindi assumere che abbiamo una congruenza $ax \equiv b \mod n$ e quindi un'equazione

$$[a][x] = [b]$$

con $MCD(a, n) = 1$. Con questa ipotesi $[a]$ è invertibile in $\mathbb{Z}_{/n}$ e quindi, se chiamiamo $[c]$ la sua inversa abbiamo l'unica soluzione

$$[x] = [bc].$$

□

Esempio 6.2. Risolvere le congruenze $6x \equiv 5 \mod 9$, $6x \equiv 6 \mod 9$ e $6x \equiv 5 \mod 7$.

Cosa possiamo dire nel caso in cui abbiamo a che fare con più di una congruenza, cioè con un sistema di congruenze del tipo

$$\begin{cases} a_1x \equiv b_1 & \mod n_1 \\ a_2x \equiv b_2 & \mod n_2 \\ a_3x \equiv b_3 & \mod n_3 \end{cases}$$

Grazie a quanto abbiamo detto prima, se tutte le singole congruenza ammettono soluzioni, possiamo ridurci ad un sistema analogo con $a_1 = a_2 = a_3 = 1$

$$\begin{cases} x \equiv b_1 & \mod n_1 \\ x \equiv b_2 & \mod n_2 \\ x \equiv b_3 & \mod n_3 \end{cases}$$

A questo punto se i moduli n_1, n_2, n_3 sono coprimi abbiamo per il teorema cinese del resto (usato due volte) un'unica soluzione modulo $n_1n_2n_3$. E possiamo anche scriverla esplicitamente. Usando un'identità di Bézout per n_1 e n_2

$$sn_1 + tn_2 = 1$$

abbiamo che il sistema è equivalente a

$$\begin{cases} x \equiv b_2sn_1 + b_1tn_2 & \mod n_1n_2 \\ x \equiv b_3 & \mod n_3 \end{cases}$$

Se invece $MCD(n_1, n_2) = d > 1$ la soluzione potrebbe non esistere. Se ad esempio abbiamo $x \equiv 2 \mod 6$ e $x \equiv 3 \mod 10$ la soluzione non esiste (ad esempio perché la prima equazione implica x pari e la seconda x dispari.) Facciamo prima un'osservazione

Osservazione 2. Siano n_1, n_2 due interi positivi e $d = MCD(n_1, n_2)$. Allora è possibile fattorizzare $d = d_1 d_2$ con $MCD(d_1, n_1/d_1) = 1$ e $MCD(d_2, n_2/d_2) = 1$. Infatti basta scegliere d_1 come il prodotto dei primi che compaiono in n_1 con molteplicità minore o uguale che in n_2 e d_2 è il prodotto dei primi che compaiono in n_2 con molteplicità minore che in n_1. Ad esempio se $n_1 = 24$ e $n_2 = 36$ allora $d = 12$ e possiamo scegliere $d_1 = 3$ e $d_2 = 4$.

Lemma 6.3. *Consideriamo il sistema di due congruenze*

$$\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \end{cases}$$

e sia $d = MCD(n_1, n_2)$. Allora il sistema ammette soluzione se e solo se $b_1 \equiv b_2 \mod d$. In tal caso scriviamo $d = d_1 d_2$ con $MCD(d_1, n_1/d_1) = 1$ e $MCD(d_2, n_2/d_2) = 1$. Allora il sistema è equivalente a

$$\begin{cases} x \equiv b_1 \mod n_1/d_1 \\ x \equiv b_2 \mod n_2/d_2 \end{cases}$$

Proof. Si verifica facilmente che se il sistema ammette soluzione allora $b_1 \equiv b_2 \mod d$: infatti in tal caso x è congruo sia a b_1 che a b_2 modulo d. Vogliamo ora mostrare che in questa ipotesi i due sistemi sono equivalenti: questo ci assicura che la soluzione esiste e che è una classe modulo $n_1 n_2/d = mcm(n_1, n_2)$, grazie al teorema cinese del resto.

Chiaramente se x soddisfa il primo sistema allora soddisfa anche il secondo. Supponiamo quindi che x sia una soluzione del secondo sistema. Abbiamo che esistono tre interi k, k_1, k_2 tali che

$$x = b_1 + k_1 n_1/d_1,\ x = b_2 + k_2 n_2/d_2,\ b_2 = b_1 + kd.$$

Per mostrare che x è soluzione anche del primo sistema dobbiamo verificare che $d_1 | k_1$ e $d_2 | k_2$: per ragioni di simmetria è sufficiente mostare la prima. Dalle tre equazioni qui sopra si deduce facilmente che

$$b_1 + k_1 n_1/d_1 = b_2 + k_2 n_2/d_2 = b_1 + kd + k_2 n_2/d_2$$

da cui ricaviamo

$$k_1 n_1/d_1 = kd + k_2 n_2/d_2.$$

Osserviamo che d_1 divide entrambi gli addendi di destra e quindi divide anche $k_1 n_1/d_1$. Ma $MCD(d_1, n_1/d_1) = 1$ per cui $d_1 | k_1$. □

Esempio 6.4. Consideriamo il sistema

$$\begin{cases} x \equiv 25 \mod 168 \\ x \equiv 49 \mod 180 \end{cases}$$

In questo caso $MCD(168, 180) = 12$ e osserviamo che $25 \equiv 49 \mod 12$ per cui il sistema ammette soluzione. Possiamo (dobbiamo) scegliere $d_1 = 3$ e $d_2 = 4$ e considerare il sistema

$$\begin{cases} x \equiv 25 \mod 56 \\ x \equiv 49 \mod 45, \end{cases}$$

dove possiamo anche sostituire 49 con 4. Per trovare la soluzione abbiamo bisogno dell'identità di Bézout tra 56 e 45:

$56 = 45 + 11$
$45 = 4 \cdot 11 + 1$
da cui $1 = 45 - 4 \cdot 11 = 45 - 4 \cdot (56 - 45) = 5 \cdot 45 - 4 \cdot 56$. La soluzione è quindi

$$x \equiv 25 \cdot 5 \cdot 45 - 4 \cdot 4 \cdot 56 \equiv 4729 \mod 56 \cdot 45 = 2520.$$

e quindi

$$x \equiv -311 \mod 2520.$$

Esercizio 6.5. Risolvere il sistema di congruenze

$$\begin{cases} 3x \equiv 6 \mod 65 \\ 5x \equiv 7 \mod 8 \\ 6x \equiv 30 \mod 26. \end{cases}$$

7. Crittografia (non svolta)

Vogliamo in questa sezione dare delle applicazioni dei risultati visti su $\mathbb{Z}_{/n}$ in crittologia/crittografia, cioè lo studio dell'invio di messaggi cripati che non possono (non dovrebbero poter) essere "letti" da occhi indiscreti.

Chiave 1x1: Un primo metodo sviluppato negli anni 1930 ora è non più applicato, ma è comunque interessante i nostri scopi didattici.

Pensiamo alle lettere come agli elementi in $\mathbb{Z}_{/26}$. Supponiamo di voler inviare il messaggio TANTIXAUGURI, dove la X sta per lo spazio. Pensiamo quindi alla nostra parola come ad una sequenza in $\mathbb{Z}_{/26}$ e la codifichiamo moltiplicando le cifre per una classe invertibile, ad esempio $[5]$. Il nostro messaggio originale

$$-6, 1, -12, 20, 9, -2, 1, -5, 7, -5, -8, 9$$

diventa in questo modo

$$22, 5, 18, 4, 19, 16, 5, 1, 9, 1, 12, 19$$

che, riscritto in lettere, diventa, VERDSPEALIS. Il ricevente quando riceve questo messaggio cosa deve fare per decrittarlo e leggere il messaggio originale? Dovrà semplicemnte moltiplicare il messaggio ricevuto (espresso come sequenza in $\mathbb{Z}_{/26}$) per la classe inversa di $[5]$, cioè $[-5]$. E infatti in questo modo ritroviamo la sequenza originale.

Questo metodo ha innumerevoli difetti e può essere "scoperto" molto facilmente.

Chiave 2x2: Si può rendere questo metodo di crittografia molto più difficile da scoprire utilizzando le lettere a due a due come se fossero dei vettori, e criptandoli moltiplicando per una matrice "invertibile" 2×2, ad esempio la matrice

$$A = \begin{pmatrix} 5 & -2 \\ 1 & 5 \end{pmatrix}.$$

Per decrittare il messaggio bisognerà moltiplicare le lettere ricevute per la matrice "inversa"

$$B = \begin{pmatrix} 5 & 2 \\ -1 & 5 \end{pmatrix}$$

Infatti si verifica facilmente che

$$B\left(A\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} x \\ y \end{pmatrix}.$$

Il nostro messaggio in questo caso viene pensato quindi come una sequenza di vettori di lunghezza 2

$$(-6, 1), (-12, 20), (9, -2), (1, -5), (7, -5), (-8, 9)$$

e moltiplicandoli per la matrice A diventano

Questo metodo è sicuramente molto più sicuro del primo, ma ancora presenta delle debolezze, tra cui la necessità di dover comunicare il codice per decrittare, cioè la matrice B.

Metodo RSA: Un metodo molto più sicuro da questo punto di vista è stato sviluppato negli anni 1970 utilizzando anche i teoremi di Eulero e Fermat che abbiamo visto nella sezione scorsa. Questo metodo prende il nome di RSA dalle iniziali dei suoi inventori.

Ogni lettera ed ogni segno di interpunzione viene pensato come un numero a due cifre, per cui un messaggio può chiaramente essere pensato come ad un numero (bello grande in generale).

In questo metodo, ogni persona che vuole inviare o ricevere un messaggio criptato deve rendere noti a tutti due numeri: n, il suo modulo, ed e il suo esponente.

Il numero n deve essere molto grande e libero da quadrati. Chiaramente se una persona sceglie un numero n deve sapere come si fattorizza in numeri primi, ma non deve comunicare questa fattorizzazione. Conoscendo la fattorizzazione, il nostro partecipante sa facilmente calcolare $\phi(n)$ e deve stare attento che il numero e che comunica sia coprimo con $\phi(n)$.

Supponiamo quindi che A vuole inviare un messaggio a B. Chiamiamo n_A, n_B i moduli di A e B ed e_A e e_B gli esponenti.

Il messaggio M deve essere un numero più piccolo di n_B: se fosse più grande bisognerebbe prima spezzarlo in parole più piccole. A questo punto A deve elevare il messaggio M all'esponente e_B, ottenendo M^{e_B}, e ridurlo modulo n_B ad un intero minore di n_B: questo è il messaggio criptato da inviare $M' \equiv M^{e_B} \mod n_B$.

Come fa ora B a decriptare il messaggio M' e leggere il messaggio M? Siccome e_B è invertibile $\mod \phi(n_B)$ il nostro amico B sarà stato in grado di trovare l'inversa di e_B mod $\phi(n_B)$ e diciamo che sia c_B questa inversa. Allora basterà calcolare

$$M'^{c_B} \equiv M^{e_B c_B} \equiv M^{1+k\phi(n_B)} \equiv M \mod \phi(n_B)$$

dove abbiamo utilizzato il fatto che n_B è libero da quadrati (Proposizione 5.7).

Perché questo metodo è ritenuto sicuro? In fondo un malintenzionato, per decriptare questo messaggio, dovrebbe semplicemente fattorizzare n_B e poi fare quello che ha fatto lo stesso B. Il fatto è che fattorizzare un numero molto grande è un problema computazionalmente estremamente lungo e complesso che anche con i più potenti computer può richiedere anni. Chiaramente più i computer diventano potenti, più ci sarà bisogno di numeri primi grandi per motivi di sicurezza.

Un altro problema fondamentale è stato risolto con questo metodo RSA: come fa B ad essere sicuro che il messaggio gli è stato inviato proprio da A e non da qualche cattivo? Il nostro amico A, diciamo Arturo, può firmare il messaggio scrivendo in fondo al messaggio M' un'ultima parola, la firma. Questa parola è N^{c_A} dove $N = Arturo \mod n_A$. A questo punto B dovrà semplicemente elevare N^{c_A} all'esponente e_A e ridurre modulo n_A per far ricomparire la parola N, la firma di Arturo.

Fare esempi è estremamente laborosioso per cui ne facciamo solo uno, seppur non troppo piccolo. Abbiamo i nostri amici A e B che hanno scelto i seguenti moduli ed esponenenti:

$$\begin{aligned} n_A &= 1147 (= 31 \cdot 37) \\ e_A &= 41 \\ n_B &= 9367 (= 19 \cdot 17 \cdot 29) \\ e_B &= 5 \end{aligned}$$

A può calcolare $\phi(n_A) = 30 \cdot 36 = 1080$ e l'inversa c_A di $e_A \mod 1080$: usando l'identità di Bézout $1 = 3 \cdot 1080 - 79 \cdot 41$ abbiamo che l'inversa di 41 è $-79 = 1001 = c_A \mod 1080$.

Similmente B può calcolare $\phi(n_B) = 18 \cdot 16 \cdot 28 = 8064$ Le chiave per decifrare di B è l'inversa di $5 = e_B$ modulo 8064 cioè $c_B = 1613$.

Abbiamo quindi le due chiavi segrete che solo A e B conoscono rispettivamente

$$\begin{aligned} c_A &= 1001 \\ c_B &= 1613 \end{aligned}$$

Supponiamo che A voglia inviare il messaggio

$$M = 134257$$

e la firma

$$F = 11.$$

Siccome 134257 è maggiore di n_B dovrà spezzarlo in più parole, diciamo 134 e 257. Dovrà a questo punto elevare 134 e 257 all'esponente 5 e poi ridurre modulo 9367. Si ha

$$\begin{aligned} 134^5 \equiv (134^2)^2 \cdot 134 = 17956^2 \cdot 134 = (-778)^2 \cdot 134 = 5796 \cdot 134 = 8570 \\ 257^5 \equiv 3993 \mod 9367 \end{aligned}$$

La firma dovrà invece essere elevata a $c_A \mod n_A$ dove c_A è l'inversa di e_A: La firma sarà quindi

$$11^{1001} \equiv 582 \mod 1147.$$

In conclusione A invierà il messaggio

$$8570\ 9367\ 582.$$

Per decrittare il messaggio B dovrà calcolare

$$8570^{1613} \equiv 134 \mod 9367$$
$$3993^{1613} \equiv 257 \mod 9367$$

e per leggere la firma dovrà calcolare

$$582^{41} = 11 \mod 1147.$$

8. Sottogruppi e generatori di un gruppo

La cardinalità di un gruppo G si indica con $|G|$ e si dice *ordine* del gruppo. Abbiamo imparato che in $\mathbb{Z}_{/n}$ non è lecito "semplificare" come siamo abituati a fare con i numeri reali; ad esempio in $\mathbb{Z}_{/12}$ abbiamo

$$[3][2] = [3][6]$$

ma chiaramente non possiamo semplificare [3]. Un altro esempio lo possiamo osservare con le matrici:

$$\begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} -3 & 2 \\ 4 & -2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}.$$

Tuttavia se siamo in un gruppo la "semplificazione" è sempre consentita:

Lemma 8.1 (Legge di cancellazione.)**.** *Sia $(G, *)$ un gruppo $g, h, k \in G$ tali che*

$$g * h = g * k \text{ oppure } h * g = k * g.$$

Allora $h = k$.

Dimostrazione. Sarà sufficiente moltiplicare per l'inversa di g (nel primo caso a sinistra nel secondo a destra) ed utilizzare la proprietà associativa. □

Utilizzeremo la legge di cancellazione liberamente in un gruppo anche senza citarla esplicitamente.

Abbiamo visto gruppi con diversi tipi di operazioni $\cdot$, $\times$, $*$, $\star$, $+$. Ma da ora in avanti, quando sviluppiamo la teoria generale ci atterremo alla notazione che si usa in tutti i libri: il risultato dell'operazione di gruppo tra due elementi g e h la denoteremo semplicemnte con gh (e talvolta con $g \cdot h$), e la chiameremo prodotto, tenendo bene a mente però che a differenza del prodotto tra numeri reali questo non è necessariamente commutativo.

Certo di volta in volta bisogna stare attenti quando si applicano i risultati ottenuti in generale ad un gruppo additivo, cioè un gruppo abeliano in cui l'operazione si denota con il simbolo $+$.

Usando il prodotto come operazione sarà naturale utilizzare anche la seguente notazione: per ogni $g \in G$ *poniamo* $g^2 = gg$, $g^3 = ggg$ eccetera, ma anche $g^0 = e$, l'elemento neutro del gruppo, $g^{-1} = \tilde{g}$, l'inverso di g, $g^{-2} = \tilde{g}^2$ eccetera.

Notare come nel definire g^n abbiamo fatto implicitamente uso della proprietà associativa.

Esercizio 8.2. Mostrare che per ogni $n, m \in \mathbb{Z}$ si ha $g^n g^m = g^{n+m}$.

Attenzione: quando G è un gruppo additivo l'elemento g^n si indica con ng per ogni $n \in \mathbb{Z}$ e l'inverso di g verrà indicato semplicemente $-g$.

Definizione. Sia G un gruppo. Un sottoinsieme non vuoto $H \subseteq G$ si dice sottogruppo se H è un gruppo rispetto alla stessa operazione di G. Si scrive in questo caso $H \leq G$.

Se G è un gruppo allora G ed $\{e\}$ sono chiaramente sottogruppi di G detti sottogruppi *banali*.

Esempio 8.3. Per ogni $n \in \mathbb{Z}$ si ha che l'insieme $n\mathbb{Z}$ dei multipli di n è un sottogruppo di $\mathbb{Z}$. Tutte le verifiche sono immediate e vengono lasciate al lettore.

Lemma 8.4. *Sia H un sottogruppo di $\mathbb{Z}$. Allora esiste $n \geq 0$ tale che $H = n\mathbb{Z}$.*

Dimostrazione. Se $H = \{0\}$ basta scegliere $n = 0$. Altrimenti H contiene almeno un elemento strettamente positivo. Scegliamo n come il più piccolo intero positivo contenuto in H. Allora, siccome H è un gruppo, esso deve contenere $n\mathbb{Z}$.

Mostriamo ora il viceversa: sia quindi $h \in H$. Effettuiamo la divisione con resto di h per n: otteniamo $h = qn + r$ con $0 \leq r < n$. Ma osserviamo che $r = h - qn$ e quindi $r \in H$. Ma siccome n era il più piccolo elemento positivo di H necessariamente abbiamo $r = 0$ e quindi $h \in n\mathbb{Z}$. □

Possiamo porci delle domande analoghe anche per i gruppi $\mathbb{Z}_{/n}$. La risposta è anche analoga.

Proposizione 8.5. *Per ogni $m \in \mathbb{Z}$ si ha che $H_m = \{[km] : k \in \mathbb{Z}\}$ è un sottogruppo. Inoltre $H_m = H_{m'}$ se e solo se $MCD(m, n) = MCD(m', n)$. Infine, se H è un sottogruppo di $\mathbb{Z}_{/n}$ allora esiste un unico $d > 0$ con $d|n$ tale che $H = H_d$.*

Dimostrazione. Il fatto che H_m sia un sottogruppo è una semplice verifica. Se $d = MCD(m, n) = MCD(m', n)$ allora, sfruttando le relative identità di Bézout, si ha che $[d] = [km] = [k'm']$ per opportuni interi k, k'. Ma da questo segue che $[d] \in H_m \cap H_{m'}$ da cui deduciamo $[m] \in H_{m'}$ e quindi $H_m \subseteq H_{m'}$. Per ragione di simmetria abbiamo anche $H_{m'} \subseteq H_m$.

Viceversa, poniamo $d = MCD(m, n)$ e $d' = MCD(m', n)$ e assumiamo $H_m = H_{m'}$; allora $m = km' + hn$ e quindi $d'|m$ e siccome $d'|n$ abbiamo $d'|d$. Simmetricamente abbiamo anche $d|d'$ per cui $d = d'$.

Se H è un sottogruppo non banale di $\mathbb{Z}_{/n}$ poniamo d il più piccolo intero positivo tale che $[d] \in H$. Sia $[h] \in H$, con $0 < h \leq n$. Dividendo h per d otteniamo $h = qd + r$. Otteniamo quindi $r = 0$ per minimalità di d e quindi $h = qd$. Abbiamo quindi $H = H_d$ e il risultato segue dalla prima parte. □

Vediamo un esempio. Per $n = 6$ i divisori positivi di n sono 1, 2, 3, 6. E infatti otteniamo i seguenti sottogruppi:

d	H_d	$\lvert H_d \rvert$
1	$\{[1], [2], [3], [4], [5], [6]\} = \mathbb{Z}_{/6}$	6
2	$\{[2], [4], [0]\}$	3
3	$\{[3], [0]\}$	2
6	$\{[0]\}$	1

Osserviamo in questo esempio, ma anche in generale, che se $d|n$ abbiamo

$$H_d = \left\{[d], [2d], \cdots [\frac{n}{d}d] = [0]\right\}$$

per cui $|H_d| = \frac{n}{d}$ e quindi in $\mathbb{Z}_{/n}$ abbiamo per ogni $d|n$ esattamente un sottogruppo di ordine d. Abbiamo quindi che in $\mathbb{Z}_{/n}$ esiste esattamente un sottogruppo per ogni divisore di n. Vedremo più avanti che questa è una proprietà caratteristica dei gruppi $\mathbb{Z}_{/n}$.

Esercizio 8.6. Sia H un sottoinsieme non vuoto di un gruppo G. Mostrare che H è un sottogruppo di G se e solo se $h^{-1}k \in H$ per ogni $h, k \in H$.

Vediamo altri esempi di sottogruppi. Se $G = \mathbb{Z}_{/4} \times \mathbb{Z}_{/8}$ allora $H = \{([0]_4, [0]_8), ([2]_4, [4]_8)\}$ è un sottogruppo di G.

Altri sottogruppi si possono definire in modo astratto all'interno di un qualunque gruppo. Ad esempio

$$Z(G) = \{z \in G : \ zg = gz \text{ per ogni } g \in G\}$$

è un sottogruppo di G, detto centro di G.

Esercizio 8.7. Sia $G = GL_2(\mathbb{R})$. Determinare $Z(G)$.

Avete dato qualche accenno al concetto di sottogruppo generato da un sottoinsieme X. La tentazione in questa casi è quella di dire: "il sottogruppo generato da X è il più piccolo sottogruppo di G che contiene X".

Vorrei darvi una piccola avvertenza quando si usa la locuzione "il più piccolo ... tale che": in questi casi bisogna stare attenti che effettivamente esista questo più piccolo.

Ad esempio non avrebbe senso dire "il più piccolo sottogruppo di G che contiene almeno un elemento di X" (perché non ne esiste in generale uno contenuto in tutti gli altri) e non avrebbe neanche senso dire "il più piccolo sottogruppo che contiene X ma non contiene un certo elemento g" perché potrebbe non esisterne neanche uno! Ad esempio non esiste il più piccolo sottogruppo di $\mathbb{Z}$ che contiene almeno un elemento di $\{2, 3\}$ e non esiste nessun sottogruppo di $\mathbb{Z}$ che contiene $\{24, 36\}$ ma non contiene 48.

È un semplice esercizio verificare che l'intersezione di due sottogruppi è ancora un sottogruppo, mentre l'unione non lo è tranne nel caso banale in cui uno dei due sia contenuto nell'altro. (Avete già visto un risultato analogo per gli spazi vettoriali?)

Analogamente se intersechiamo una famiglia infinita di sottogruppi otteniamo ancora un sottogruppo. Questo ci permette di dare la seguente definizione

Definizione. Dato un sottoinsieme X di un gruppo G, il sottogruppo $\langle X \rangle$ generato da X è l'intersezione di tutti i sottogruppi che contengono H

$$\langle X \rangle = \bigcap_{H : X \subseteq H \leq G} H.$$

Possiamo in altre parole dire che il sottogruppo generato da X è il più piccolo sottogruppo di G che contiene X.

Ad esempio, in $\mathbb{Z}$ il sottogruppo generato da $X = \{6, 8\}$ è $\langle X \rangle = 2\mathbb{Z}$. Ma vediamo più in generale come è fatto questo sottogruppo.

Proposizione 8.8. *Sia $X \subseteq G$. Allora*

$$\langle X \rangle = \{t_1 t_2 \cdots t_r : r \geq 0, \ t_i \in X \text{ oppure } t_i^{-1} \in X, \forall i = 1, \ldots, r\}.$$

Dimostrazione. Sia $K = \{t_1 t_2 \cdots t_r : t_i \in X \text{ oppure } t_i^{-1} \in X, \forall i = 1, \ldots, r\}$ e mostriamo la doppia inclusione.

$\langle X \rangle \subseteq K$: è evidente che $X \subseteq K$ e quindi è sufficiente mostrare che K è un sottogruppo e quindi è uno di quelli che intersechiamo nella definizione di $\langle X \rangle$. Osserviamo che $e \in K$ (basta prendere $r = 0$) nella definizione e chiaramente se motiplichiamo due elementi $t_1 \cdots t_r$ e $t'_1 \cdots t'_s$ di H anche il loro prodotto $t_1 \cdots t_r t'_1 \cdots t'_s$ sta in K. Inoltre l'inversa di $t_1 \cdots t_r$ è $t_r^{-1} \cdots t_1^{-1}$ che chiaramente sta ancora in K.

$\langle X \rangle \supseteq K$: in questo caso bisogna mostrare che ogni sottogruppo che contiene X contiene anche K: questo viene direttamente dal fatto che un sottogruppo deve essere chiuso rispetto al prodotto e all'inversione. □

Definizione. Un gruppo G generato da un solo elemento (cioè tale che esiste $g \in G$ per cui $G = \langle g \rangle$) è detto gruppo *ciclico*.

Ad esempio $\mathbb{Z}$ e $\mathbb{Z}_{/n}$ sono esempi di gruppi ciclici. Ne esistono altri (non isomorfi a questi)? Il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico. Ognuno dei tre elementi diversi dall'identità genera un sottogruppo con due elementi.

Il gruppo con 10 elementi $\mathbb{Z}^*_{/11} = \mathbb{Z}_{/11} \setminus \{[0]\}$ con l'operazione di prodotto è un gruppo ciclico: infatti possiamo osservare che ogni elemento di $\mathbb{Z}^*_{/11}$ è una potenza di $[2]$ per cui

$$\mathbb{Z}^*_{/11} = \langle [2] \rangle.$$

Osserviamo che se il gruppo è finito allora ogni elemento ha ordine finito: infatti se $g^n = g^m$, con $n \geq m$ allora $g^{n-m} = e$. Sussiste anche il seguente risultato più preciso

Proposizione 8.9. *Sia G un gruppo e $g \in G$. Se g ha ordine infinito allora $g^a \neq g^b$ per ogni $a \neq b$. Se g ha ordine finito, diciamo n, allora $g^a = g^b$ se e solo se $a \equiv b \mod n$. In particolare*

$$\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$$

ha esattamente n elementi distinti. Osserviamo anche che, in particolare, $g^r = e$ se e solamente se $n|r$.

Ricordiamo che un elemento $g \in G$ ha ordine finito se esiste un intero positivo n tale che $g^n = e$. L'ordine $o(g)$ di g è in tal caso il più piccolo intero positivo tale che $g^n = e$.

Dimostrazione. Se g ha ordine infinito e $g^a = g^b$ con $a > b$ allora $g^{a-b} = e$ per la legge di cancellazione, assurdo. Supponiamo ora che $o(g) = n$ e supponiamo $g^a = g^b$ con $a > b$. Allora $g^{a-b} = e$ e dobbiamo mostrare che $a \equiv b \mod n$. Dividiamo con resto $a - b$ per n ed otteniamo $a - b = qn + r$, con $0 \leq r < n$ da cui deduciamo

$$e = g^{a-b} = g^{qn} g^r = (g^n)^q g^r = g^r.$$

E siccome n è il più piccolo intero tale che $g^n = e$ necessariamente abbiamo $r = 0$ e quindi $a - b \equiv 0 \mod n$. Viceversa, se $a \equiv b \mod n$ allora si ha $a = b + kn$ per cui $g^a = g^b g^{kn} = g^b$. □

Corollario 8.10. *Sia G un gruppo ciclico. Allora se $|G| = +\infty$ abbiamo $G \cong \mathbb{Z}$ e se $|G| = n$ allora $G \cong \mathbb{Z}_{/n}$.*

Dimostrazione. Se $|G| = \infty$ allora per la Proposizione 8.9 abbiamo che l'elemento g che genera G ha ordine infinito e

$$G = \{\dots, g^{-2}, g^{-1}, g^0, g, g^2, g^3, \dots\}.$$

Possiamo a questo punto definire la funzione $\varphi : \mathbb{Z} \to G$ data da

$$\varphi(n) = g^n;$$

la funzione φ è evidentemente una corrispondenza biunivoca. Verifichiamo che si tratta di un omomorfismo e quindi di un isomorfismo:

$$\varphi(n+m) = g^{n+m} = g^n g^m = \varphi(n) \cdot \varphi(m).$$

Similmente possiamo agire nel caso in cui G sia finito. Se $|G| = n$ allora per la Proposizione 8.9 abbiamo che l'elemento g che genera G ha ordine n e

$$G = \{e = g^0, g, \dots, g^{n-1}\}.$$

Allora la funzione

$$\varphi : \mathbb{Z}_{/n} \to G$$

data da $\varphi([a]) = g^a$ è ben posta, e una corrispondenza biunivoca per la Proposizione 8.9. Osserviamo infine che anche in questo caso φ è un omomorfismo e quindi un isomorfismo:

$$\varphi([a] + [b]) = \varphi([a+b]) = g^{a+b} = g^a g^b = \varphi([a])\varphi([b]).$$

□

Per studiare un gruppo ciclico è quindi sufficiente considerare a meno di isomorfismi $\mathbb{Z}$ o $\mathbb{Z}_{/n}$. Ci poniamo la seguente naturale domanda: quanti e quali sono i generatori di $\mathbb{Z}$ e di $\mathbb{Z}_{/n}$? Nel primo caso la risposta è semplice: sono solo $+1$ e -1. Nel secondo caso la situazione è un po' più intricata.

Facciamo qualche esempio: in $\mathbb{Z}_{/4}$ i generatori sono $[1]_4$ e $[3]_4$, in $\mathbb{Z}_{/5}$ ogni elemento diverso da $[0]_5$ è un generatore, in $\mathbb{Z}_{/6}$ i generatori sono $[1]_6$ e $[5]_6$. Osserviamo che i generatori in queti tre esempi sono dati proprio dagli elementi invertibili. Sarà sempre vero? La risposta è affermativa e discende dal seguente risultato.

Proposizione 8.11. *Sia G un gruppo ciclico di ordine n generato da un elemento g. Allora per ogni $a \in \mathbb{Z}$ si ha*

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

In particolare g^a è un generatore se e solo se $MCD(n,a) = 1$, cioè se e solo se $[a]$ è invertibile in $\mathbb{Z}_{/n}$.

Proof. Vogliamo determinare il più piccolo intero positivo x tale che $(g^a)^x = g^{ax} = e$. Per la Proposizione 8.9 questo è equivalente a risolvere la congruenza

$$ax \equiv 0 \mod n.$$

Sappiamo che questa congruenza ammette un'unica soluzione modulo $\frac{n}{d}$, dove $d = MCD(a,n)$ ed è equivalente alla seguente

$$\frac{a}{d}x \equiv 0 \mod \frac{n}{d}.$$

Di conseguenza, per unicità , la soluzione della congruenza è $x \equiv 0 \mod \frac{n}{d}$ e quindi la più piccola soluzione intera positiva è proprio $\frac{n}{d}$.

In alternativa possiamo assumere $G = \mathbb{Z}_{/n}$ e ottenere questo risultato anche sfruttando la Proposizione 8.5. Se $d = MCD(n, a)$ abbiamo che $H_a = H_d$ e di conseguenza $o(a) = o(d) = n/d$, perché d è un divisore di n. Il risultato segue.

□

Da questa Proposizione discende un'altra formula ricorsiva per poter calcolare la ϕ di Eulero:

Corollario 8.12. *Sia $n > 0$, Allora*

$$n = \sum_{d|n} \phi(d).$$

Proof. Per ogni $d|n$ sappiamo che in $\mathbb{Z}_{/n}$ esiste esattamente un sottogruppo di ordine d (generato da n/d) e non ci sono altri sottogruppi. In particolare l'ordine di un qualunque elemento è necessariamente un divisore di n. Contiamo ora quanti sono gli elementi di ordine d. Sia $m(d)$ il numero di elementi di ordine d. Ognuno di questi elementi genera un sottogruppo di ordine d. Ma noi sappiamo che esiste un unico sottogruppo di $Z_{/n}$ di ordine d e che questo sottogruppo è isomorfo a $\mathbb{Z}_{/d}$. Di conseguenza gli elementi di ordine d sono proprio i generatori di questo sottogruppo e questi sono esattamente $\phi(d)$. In conclusione, per ogni $d|n$ abbiamo esattamente $\phi(d)$ elementi di ordine d e quindi il numero totale di elementi, n, è proprio uguale a $\sum_{d|n} \phi(d)$. □

Illuatriamo la precedente dimostrazione con un esempio. Poniamo $n = 12$. I divisori di 12 sono $d = 1, 2, 3, 4, 6, 12$. Per ognuno di questi d abbiamo esattamente un sottogruppo di ordine d: ad esempio per $d = 4$ tale sottogruppo è $H = \{[0], [3], [6], [9]\}$; questo sottogruppo, essendo ciclico di ordine 4 è isomorfo a $\mathbb{Z}_{/4}$ e quindi ha $\phi(4) = 2$ generatori (che sono [3] e [9]). Abbiamo quindi $\phi(1)$ elementi di ordine 1, $\phi(2)$ elementi di ordine 2 e così via.

9. I gruppi diedrali

Il gruppo diedrale D_n (talvolta indicato D_{2n}) è il gruppo delle isometrie del piano che lasciano invariato un n-agono regolare. È costituito da esattamente $2n$ elementi: di questi ne abbiamo n che lasciano la stessa faccia del poligono verso l'alto e altri n che scambiano la faccia. In figura, con $n = 5$ abbiamo i primi 5 rappresentati nella prima riga e gli altri 5 nella seconda riga.

In alternativa se numeriamo i vertici da 1 a n in senso orario i primi sono quelli che lasciano la numerazione in senso orario, i secondi quelli che la trasformano in senso antiorario. D'altra parte abbiamo n rotazioni (che non cambiano faccia) e n riflessioni assiali (che cambiano faccia) e quindi queste sono "tutte" le trasformazioni possibili. Ancora una volta possiamo notare le rotazioni nella prima riga e le riflessioni nella seconda.

Se chiamiamo r la rotazione oraria di $360/n$ gradi ed s una riflessione assiale (in figura abbiamo scelto la riflessione che fissa il vertice 1) qualunque abbiamo che $r^0, \ldots, r^{n-1}$ e

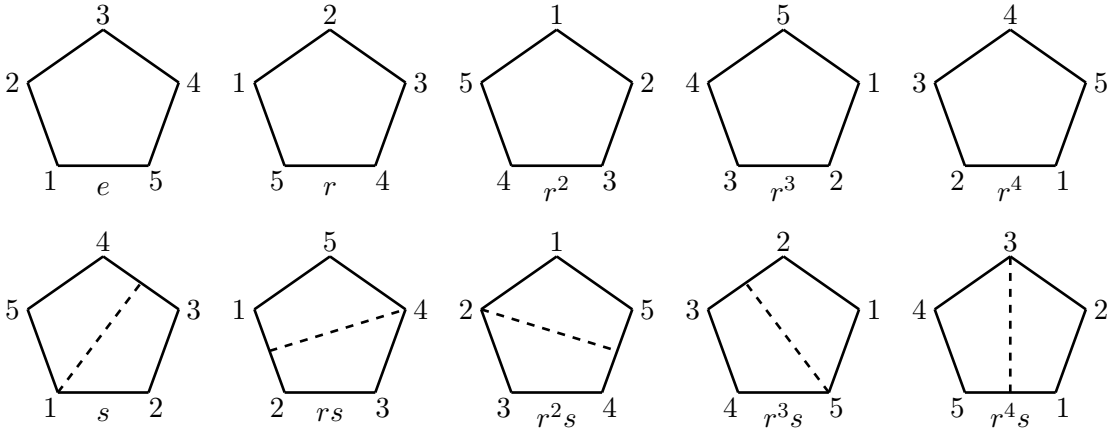

FIGURE 2. Il gruppo diedale D_5

$s, rs, r^2s, \ldots, r^{n-1}s$ sono tutte trasformazioni distinte (le prime n sono le rotazioni le altre sono le riflessioni) e quindi abbiamo che

$$D_n = \langle r, s \rangle.$$

Possiamo dire anche qualcosa in più sul prodotto di questi elementi. Sappiamo ad esempio che ogni elemento della forma $r^k s$ è una riflessione per cui $(r^k s)^{-1} = r^k s$. D'altra parte abbiamo anche $(r^k s)^{-1} = sr^{n-k}$ da cui deduciamo $r^k s = sr^{n-k}$ regola che ci permette di effettuare facilmente il prodotto tra due elementi qualunque di D_n "algebricamente" senza bisogno di pensare alla loro interpretazione geometrica. Ad esempio se $n = 6$ i nostri 12 elementi sono

$$D_6 = \{e, r, \ldots, r^5, s, rs, \ldots, r^5 s\}$$

e ad esempio abbiamo

$$(r^4 s)r^2 = r^4(sr^2) = r^4 r^4 s = r^2 s$$

perché $r^6 = e$ o anche

$$(r^2 s)(rs) = r^2(sr)s = r^2 r^5 ss = r.$$

In conclusione possiamo dire che D_n è generato da due elementi r ed s che soddisfano le seguenti condizioni:

$$s^2 = e,\ r^n = e,\ sr^i = r^{n-i}s$$

per ogni $i = 1, \ldots, n$. Riprenderemo queste osservazioni più avanti quando parleremo di sottogruppi normali e di gruppi presentati per generatori e relazioni.

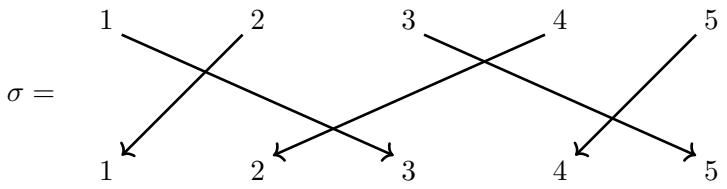

FIGURE 3. La notazione con le freccette

10. Il gruppo simmetrico

Abbiamo già visto che per ogni insieme A le funzioni biiettive $F : A \to A$ formano un gruppo rispetto alla composizione, detto gruppo simmetrico su A. Studieremo in questa sezione il caso in cui A è un insieme finito e, senza perdita di generalità , supporremo che $A = \{1, 2, \ldots, n\}$ e indicheremo questo gruppo simmetrico semplicemente con $\mathfrak{S}(n)$. Gli elementi di $\mathfrak{S}(n)$ si dicono anche permutazioni.

Ricordiamo intanto che $|\mathfrak{S}(n)| = n!$ Esistono diverse notazioni per indicare una permutazione, ognuna delle quali ha pregi e difetti a seconda dell'uso che se ne vuole fare.

La notazione con le *freccette*: in questa notazione viene disegnato un diagramma in cui viene indicato tramite freccette l'immagine di ogni elemento in $\{1, 2, \ldots, n\}$. Ad esempio la permutazione σ mostrata in Figura 3 soddisfa $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 5$, $\sigma(4) = 2$ e $\sigma(5) = 4$.

Una permutazione σ può anche essere rappresentata con la sua notazione *a due righe*:

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

Nella prima riga vengono inseriti tutti i valori da 1 a n e nella seconda le rispettive immagini tramite σ. In questa notazione non è necessario che i numeri nella prima riga siano inseriti in ordine crescente.

Attenzione: la composizione $\sigma\tau$ tra due permutazioni viene effettuata con la usuale convenzione tra le funzioni, cioè bisogna prima applicare τ e poi σ. Ad esempio se

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}$$

allora

$$\sigma\tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}, \quad \tau\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}$$

Osserviamo che l'inversa nella notazione a due righe si ottiene scambiando le due righe per poi riordinare le colonne. Ad esempio

$$\sigma^{-1} = \begin{bmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}.$$

La notazione a due righe non è tuttavia molto conveniente da un punto di vista pratico (e tipografico), anche perché la prima riga può sempre essere riordinata in modo crescente:

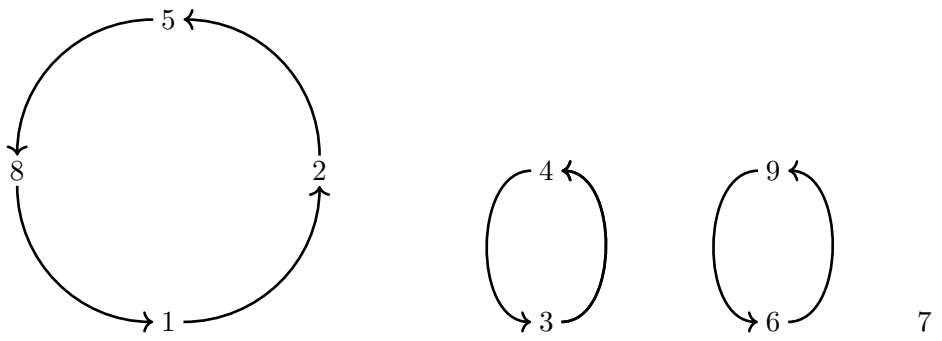

FIGURE 4. Orbite e cicli

si predilige quindi la cosiddetta notazione *ad una riga* (corrispondente alla seconda riga della notazione a due righe quando la prima è ordinata in modo crescente):

$$\sigma = [\sigma(1), \ldots, \sigma(n)].$$

Se ad esempio $\sigma = [2, 4, 5, 1, 3]$ allora $\sigma^2 = [4, 1, 3, 2, 5]$, $\sigma^3 = [1, 2, 5, 4, 3]$, $\sigma^4 = [1, 2, 3, 1, 5]$, $\sigma^5 = [4, 1, 5, 2, 3]$, $\sigma^6 = [1, 2, 3, 4, 5]$ per cui $o(\sigma) = 6$ e quindi σ genera un sottogruppo ciclico di ordine 6 in $\mathfrak{S}(5)$.

Studieremo più avanti il concetto di azione di un gruppo su un insieme. Siamo qui in presenza dell'azione per antonomasia di un gruppo: si dice che $\mathfrak{S}(n)$ "agisce" sull'insieme $\{1, 2, \ldots, n\}$ perché ad ogni elemento di $\mathfrak{S}(n)$ viene associata una trasformazione di questo insieme.

Fissato un elemento σ possiamo definire le sue orbite: l'orbita di i tramite σ è data da

$$\mathcal{O}_\sigma(i) = \{j : \text{ esiste } r \text{ per il quale } \sigma^r(i) = j\}.$$

Se $\sigma = [2, 5, 4, 3, 8, 9, 7, 1, 6]$ allora le orbite di σ sono $\{1, 2, 5, 8\}$, $\{3, 4\}$, $\{6, 9\}$ e $\{7\}$ e sono raffigurate in Figura 4.

Si verifica facilmente che se $k \in \mathcal{O}_\sigma(i)$ allora $\mathcal{O}_\sigma(i) = \mathcal{O}_\sigma(k)$ e quindi le orbite di σ formano una partizione di $\{1, 2, \ldots, n\}$.

Ad esempio, se $\sigma = [4, 1, 5, 2, 3]$ abbiamo due orbite associate a σ: un'orbita è $\{1, 2, 4\}$, l'altra $\{3, 5\}$. Se invece scegliamo $\tau = [2, 3, 4, 5, 1]$ abbiamo un'unica orbita formata da tutti e 5 gli elementi.

Una permutazione si dice *ciclo* se tutte le sue orbite tranne una sono formate da un solo elemento. Ad esempio la permutazione $\tau = [3, 2, 4, 1, 5]$ è un ciclo perché ha un'orbita $\{1, 3, 4\}$ costituita da tre elementi, e due orbite $\{2\}$ e $\{5\}$ banali.

Un ciclo τ si rappresenta nel seguente modo: si scrivono gli elementi dell'unica orbita non banale tra parentesi tonde in modo che l'immagine tramite τ di ogni coefficiente sia il successivo, e l'immagine dell'ultimo sia il primo. Ad esempio il ciclo $\tau = [3, 2, 4, 1, 5]$ verrà rappresentato nel seguente modo

$$\tau = (1, 3, 4)$$

proprio perché $\tau(1) = 3$, $\tau(3) = 4$, $\tau(4) = 1$. Gli elementi che non compaiono in questa scrittura sono da ritenere fissati dalla permutazione. Chiaramente la scrittura di τ non è unica: ad esempio potremmo scrivere anche

$$\tau = (3, 4, 1) = (4, 1, 3).$$

Notare l'uso delle parentesi tonde anziché le parentesi quadre quando utilizziamo la scrittura in cicli anziché la notazione ad una una riga. Il concetto di orbita ci permette di definire i cicli di una permutazione: un ciclo di una permutazione σ è una permutazione che agisce come σ su un'orbita non banale di σ e come l'identità su tutti gli altri elementi.

Ad esempio se $\sigma = [4, 1, 5, 2, 3]$ abbiamo $(1, 4, 2)$ è il ciclo associato all'orbita $\{1, 4, 2\}$. Chiaramente anche $(4, 2, 1)$ rappresenta lo stesso ciclo, mentre $(1, 2, 4)$ rappresenta un altro ciclo. In questo caso σ ha un'altra orbita non banale, $\{3, 5\}$, e il ciclo associato ad essa sarà $(3, 5)$.

Se noi conosciamo il ciclo di ogni orbita di σ possiamo risalire a σ e quindi introduciamo la seguente notazione.

Notazione tramite prodotto di cicli disgiunti: scriveremo una permutazione come prodotto di cicli, uno per ogni sua orbita. Ad esempi la permutazione $\sigma = [4, 1, 5, 2, 3]$ la scriveremo anche come

$$\sigma = (1, 4, 2)(3, 5) = (1, 4, 2)(5, 3) = (3, 5)(2, 1, 4) = \cdots$$

La permutazione $\sigma = [2, 5, 4, 3, 8, 9, 7, 1, 6]$ rappresentata in Figura 4 si può scrivere come prodotto di cicli disgiunti $\sigma = (1, 2, 5, 8)(3, 4)(6, 9)$. I cicli di lunghezza 1 vengono solitamente omessi.

Proposizione 10.1. *Ogni permutazione è prodotto dei suoi cicli. Viceversa, se una permutazione è prodotto di cicli disgiunti allora questi sono i cicli della permutazione.*

Dimostrazione. Qui c'è poco da dimostrare. È chiaro che una permutazione agisce su un elemento i come il ciclo dell'orbita che contiene i, mentre tutti gli altri cicli agiscono come l'identità sia su di esso che su $\sigma(i)$. Vediamolo più formalmente: se $\sigma = \gamma_1 \cdots \gamma_k$ □

Proposizione 10.2. *Ogni permutazione è prodotto di cicli di lunghezza 2 (detti anche trasposizioni).*

Dimostrazione. Siccome ogni permutazione è prodotto di cicli basterà mostrare che ogni ciclo é prodotto di trasposizioni. E infatti ci basta osservare che

$$(a_1, a_2, \ldots, a_n) = (a_1, a_n) \cdots (a_1, a_3)(a_1, a_2).$$

□

Proposizione 10.3. *L'ordine di una permutazione è il mcm delle lunghezze dei suoi cicli.*

Moltiplicare una permutazione per una trasposizione a destra e a sinistra.

Definizione. Parità di una permutazione. Diciamo che una permutazione è pari se è possibile scriverla come prodotto di un numero pari di trasposizioni. Similmente definiamo una trasposizione dispari.

In questa definizione sembra si dia per scontato un fatto che scontato non è :

Teorema 10.4. *Non esistono permutazioni sia pari che dispari.*

Questo risultato è così importante che ne vediamo due dimostrazioni, una algebrica e una combinatorica.

Dimostrazione "algebrica" del Teorema 10.4. Dato un polinomio $p(x_1, \dots, x_n)$ e una permutazione $\sigma \in S_n$ possiamo definire il polinomio $\sigma(p)$ ottenuto da p permutando le variabili:

$$\sigma(p)(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Ad esempio, se $p = x_1^2 - x_2x_3$ e $\sigma = [2, 3, 1]$ allora $\sigma(p) = x_2^2 - x_1x_3$. Osserviamo che se $\sigma = \tau_1\tau_2$ allora

$$\sigma(p) = \tau_1(\tau_2(p)) :$$

infatti

$$\begin{aligned}\sigma(p) &= p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \\ &= p(x_{\tau_1\tau_2(1)}, \dots, x_{\tau_1\tau_2(n)}) \\ &= \tau_1(p(x_{\tau_2(1)}, \dots, x_{\tau_2(n)})) \\ &= \tau_1(\tau_2(p)).\end{aligned}$$

Grazie a queste considerazioni ci sarà sufficiente trovare un polinomio non nullo p tale che $t(p) = -p$ per ogni trasposizione t: questo infatti implica che se $\sigma = t_1 \cdots t_r$ allora

$$\sigma(p) = (-1)^r p$$

per cui la parità di r è univocamente determinata da σ.

Il polinomio che ci risolve questo problema è il seguente:

$$\begin{aligned}p(x_1, \dots, x_n) &= \prod_{1 \le i < j \le n} (x_i - x_j) \\ &= (x_1 - x_2)(x_1 - x_3) \cdots (x_{n-1} - x_n)\end{aligned}$$

Osserviamo subito che $\sigma(p) = \pm p$: infatti i fattori che compaiono in $\sigma(p)$ sono gli stessi, a meno del segno, di quelli che compaiono in p.

Consideriamo ora una trasposizione $t = (i, j)$: chiaramente i fattori di p che non coinvolgono i e j rimangono invariati in $t(p)$ e andiamo a vedere quindi come cambiano quelli che coinvolgono i o j (o entrambi)

Fattore originale	Fattore trasformato	Segno
$x_h - x_i$ (con $h < i$)	$x_h - x_j$	$+1$
$x_h - x_j$ (con $h < i$)	$x_h - x_i$	$+1$
$x_i - x_h$ (con $i < h < j$)	$x_j - x_h$	-1
$x_h - x_j$ (con $i < h < j$)	$x_h - x_i$	-1
$x_i - x_h$ (con $h > j$)	$x_j - x_h$	$+1$
$x_j - x_h$ (con $h > j$)	$x_i - x_h$	$+1$
$x_i - x_j$	$x_j - x_i$	-1

I contributi della terza e quarta riga si annullano e quindi rimane solo il contributo dell'ultima riga da cui segue il risultato.

□

Vediamo ora un metodo più combinatorico per dimostrare il Teorema 10.4. L'idea di fondo è sostanzialmente la stessa per cui abbiamo una seconda chance di capire anche la dimostrazione algebrica.

Data una permutazione $\sigma = [\sigma_1, \dots, \sigma_n]$ definiamo l'insieme delle inversioni di σ tramite

$$\mathrm{Inv}(\sigma) = \{\{i, j\} : i < j,\, \sigma_i > \sigma_j\}.$$

Ad esempio $\mathrm{Inv}([1, 2, 3, 4, 5]) = \emptyset$,

$$\mathrm{Inv}([3, 5, 1, 4, 2]) = \{(1, 3), (1, 5), (2, 3), (2, 4), (2, 5), (4, 5)\}$$

Proposizione 10.5. *Sia σ una permutazione. Se σ è una permutazione pari allora $|\mathrm{Inv}(\sigma)|$ è pari e se σ è una permutazione dispari allora $|\mathrm{Inv}(\sigma)|$ è dispari.*

Dimostrazione. Sia $\sigma = t_1 t_2 \cdots t_r$ dove le t_i sono tutte trasposizioni. Procediamo per induzione su r.

Passo base: $r = 0$. In questo caso $\sigma = e$ e $\mathrm{Inv}(e) = \emptyset$.

Passo induttivo: supponiamo $r > 0$ e che l'enunciato sia vero per tutte le permutazioni che si possono scrivere come prodotto di $r - 1$ trasposizioni.

Supponiamo $t_r = (i, j)$ con $i < j$. Se $\sigma = [\sigma_1, \dots, \sigma_n]$ allora sappiamo che la notazione ad una riga di $\tau = t_1 \cdots t_{r-1}$ si ottiene da quella di σ scambiando σ_i e σ_j:

$$\tau = [\sigma_1, \dots, \sigma_{i-1}, \sigma_j, \sigma_{i+1}, \dots, \sigma_{j-1}, \sigma_i, \sigma_{j+1}, \dots, \sigma_n]$$

Facciamo un esempio: sia $\sigma = [3, 5, 2, 4, 1]$ e sia $\sigma = (1, 3)(2, 3)(2, 5)$ una sua scrittura come prodotto di trasposizioni. Allora la notazione ad una riga di $\tau = (1, 3)(2, 3)$ è $\tau = [3, 1, 2, 4, 5]$ è ottenuta da quella di σ scambiando i numeri in posizione 2 e 5.

Che legame c'è tra le inversioni di σ e quelle di τ? Una coppia (h, k) che non coinvolge né i né j è un'inversione di σ se e solo se è un'inversione di τ.

Vogliamo dimostrare che $|\mathrm{Inv}(\sigma)| + |\mathrm{Inv}(\tau)| \equiv 1 \mod 2$. Infatti una coppia (h, k) che non coinvolge né i né j è un'inversione di σ se e solo se è un'inversione di τ e quindi non dà contributo a $|\mathrm{Inv}(\sigma)| + |\mathrm{Inv}(\tau)| \mod 2$.

Se $h < i < j$ allora (h, i) è un'inversione di σ se e solo se (h, j) è un'inversione di τ e analogamente scambiando i e j: il contributo di tutte queste coppie è quindi ancora nullo in $|\mathrm{Inv}(\sigma)| + |\mathrm{Inv}(\tau)| \mod 2$.

Se $i < j < h$ il discorso é del tutto analogo al caso precedente.

Se $i < h < j$ abbiamo che (i, h) è un'inversione di σ se e solo se (h, j) *non* è un'inversione di τ e analogamente con j al posto di i: il contributo totale in $|\mathrm{Inv}(\sigma)| + |\mathrm{Inv}(\tau)|$ è

$$|\{(i, h) : i < h < j\} \cup \{(h, j) : i < h < j\}| = 2(j - i - 1) \equiv 0 \mod 2.$$

L'unica coppia che non abbiamo ancora considerato è (i, j) che chiaramente é un'inversione per σ se e solo se non lo è per τ e quindi concludiamo che

$$|\mathrm{Inv}(\sigma)| + |\mathrm{Inv}(\tau)| \equiv 1 \mod 2$$

□

Grazie al teorema 10.4 possiamo definire il segno di una permutazione σ ponendo

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{se } \sigma \text{ è pari,} \\ -1 & \text{se } \sigma \text{ è dispari} \end{cases}$$

e abbiamo

Corollario 10.6. *Sia σ una permutazione. Allora*

$$\varepsilon(\sigma) = (-1)^{|\operatorname{Inv}(\sigma)|}.$$

Un'altra conseguenza del Teorema 10.4 è la seguente:

Corollario 10.7. *La funzione $\varepsilon : S_n \to \{+1, -1\}$ è un omomorfismo di gruppi (dove $\{+1, -1\}$ è pensato come gruppo moltiplicativo.)*

Corollario 10.8. *Sia*

$$A_n = \{\sigma \in S_n : \varepsilon(\sigma) = +1\}.$$

Allora A_n è un sottogruppo (detto gruppo alterno) di S_n di ordine $\frac{n!}{2}$ per ogni $n \geq 2$.

Dimostrazione. Chiaramente l'identità è pari, il prodotto di permutazioni pari è pari e l'inversa di una permutazione pari è pari: per quest'ultima proprietà basta osservare che

$$1 = \varepsilon(e) = \varepsilon(\sigma)\varepsilon(\sigma^{-1}).$$

Per la seconda parte osserviamo che, se $n \geq 2$, la moltiplicazione a sinistra per la trasposizione $(1, 2)$ (o una qualunque altra trasposizione) è una biezione tra le permutazioni pari e quelle dispari. □

11. Il coniugio

Se τ è una permutazione di S_n, possiamo associare a τ un automorfismo di S_n detto coniugio tramite τ:

$$c_\tau : S_n \to S_n$$

definito ponendo $c_\tau(\sigma) = \tau\sigma\tau^{-1}$. Ad esempio, se $\tau = (1, 2, 3)$ e $\sigma = (2, 4, 1, 3)$ abbiamo

$$c_\tau(\sigma) = (1, 2, 3)(2, 4, 1, 3)(1, 3, 2) = (1, 3, 4, 2)$$

Osserviamo che per ogni τ, τ' abbiamo

$$c_{\tau\tau'} = c_\tau \circ c_{\tau'} : \tag{1}$$

infatti

$$c_{\tau\tau'}(\sigma) = \tau\tau'\sigma(\tau\tau')^{-1} = \tau(\tau'\sigma(\tau')^{-1})\tau^{-1} = \tau c_{\tau'}(\sigma)\tau^{-1} = c_\tau(c_{\tau'}(\sigma))$$

Lemma 11.1. *Per ogni $\tau \in S_n$ abbiamo che c_τ è un automorfismo di S_n (cioè un isomorfismo da S_n a S_n) la cui inversa è proprio $c_{\tau^{-1}}$.*

Proof. Dobbiamo mostrare che $c_\tau(\sigma_1\sigma_2) = c_\tau(\sigma_1)c_\tau(\sigma_2)$. Infatti,

$$c_\tau(\sigma_1\sigma_2) = \tau\sigma_1\sigma_2\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1} = c_\tau(\sigma_{-1})c_\tau(\sigma_2).$$

L'iniettività deriva facilmente dala legge di cancellazione, la suriettività segue dal fatto che S_n è finito (oppure si può verificare facilmente). In alternativa basta verificare che l'inversa di c_τ è proprio $c_{\tau^{-1}}$, e questo è una conseguenza di (1). □

Diciamo che σ è coniugata a σ' se esiste una permutazione τ tale che

$$\sigma' = \tau\sigma\tau^{-1}.$$

Osserviamo che la relazione su S_n data da "σ è in relazione con σ' se σ è coniugata a σ'" è effettivamente una relazione d'equivalenza.

- Proprietà riflessiva: basta σ è coniugata a se stessa: basta scegliere $\tau = e$.
- Proprietà simmetrica: se $\sigma' = c_\tau(\sigma)$ allora $\sigma = c_{\tau^{-1}}(\sigma')$.
- Proprietà transitiva: se $\sigma' = c_\tau(\sigma)$ e $\sigma'' = c_{\tau'}(\sigma')$ allora

$$\sigma'' = c_{\tau'}(\sigma') = c_{\tau'}(c_\tau(\sigma)) = c_{\tau'\tau}(\sigma).$$

e quindi diremo più semplicemente in questo caso che σ e σ' sono coniugate. Le classe di equivalenza di permutazioni coniugate prendono il nome di classi di coniugio. Vediamo le classi di coniugio di S_3. Chiaramente l'identità forma una classe di coniugio da sola. Vediamo chi sono gli elementi nella classe di coniugio della trasposizione $\sigma = [2, 1, 3]$, Abbiamo

$$c_e(\sigma) = c_{(1,2)}(\sigma) = [2, 1, 3]$$
$$c_{(1,3)}(\sigma) = c_{(1,2,3)}(\sigma) = [1, 3, 2]$$
$$c_{(2,3)}(\sigma) = c_{(1,3,2)}(\sigma) = [3, 2, 1]$$

per cui la classe di coniugio di $(1, 2)$ è data da $\{[2, 1, 3], [1, 3, 2], [3, 2, 1]\} = \{(1, 2), (1, 3), (2, 3)\}$.

Osserviamo anche che $c_{(1,2)}([2, 3, 1]) = [3, 1, 2]$ per cui neessariamente abbiamo l'ultima classe di coniugio formata dai due 3-cicli:

$$\{[2, 3, 1], [3, 1, 2]\} = \{(1, 2, 3), (1, 3, 2)\}.$$

Come si fa a capire se due permutazioni sono coniugate? Avete visto in geometria un concetto analogo al coniugio: la similitudine tra matrici. In quel caso il problema della similitudine è tutt'altro che banale da risolvere (e lo risolverete solo al termine del corso quando farete la forma canonica di Jordan). Nel caso delle permutazioni la risposta è decisamente più semplice. Facciamo un esempio di calcolo di un coniugio in cui scriviamo σ come prodotto di cicli disgiunti e τ nella notazione ad una riga: ad esempio $\sigma = (3, 8, 1, 6, 2)(4, 9, 7)(5, 10)$ e $\tau = [3, 5, 1, 7, 9, 2, 4, 8, 10, 6]$ e quindi $\tau^{-1} = [3, 6, 1, 7, 2, 10, 4, 8, 5, 9]$ e abbiamo

$$\begin{aligned}\tau\sigma\tau^{-1} &= [3, 5, 1, 7, 9, 2, 4, 8, 10, 6](3, 8, 1, 6, 2)(4, 9, 7)(5, 10)[3, 6, 1, 7, 2, 10, 4, 8, 5, 9] \\ &= (1, 8, 3, 2, 5)(4, 7, 10)(6, 9) \\ &= (1, 8, 3, 2, 5)(7, 10, 4)(9, 6)\end{aligned}$$

Nell'ultimo passaggio abbiamo riscritto i cicli coinvolti in un altro ordine. Perché mai? Il motivo è l'osservazione seguente: se noi scriviamo le due permutazioni σ e $c_\tau(\sigma)$ una sopra l'altra

$$\sigma = (3,8,1,6,2)(4,\ 9,\ 7)(5,10)$$
$$c_\tau(\sigma) = (1,8,3,2,5)(7,10,4)(9,\ 6)$$

notiamo che togliendo le parentesi otteniamo la notazione a due righe di una permutazione

$$\begin{bmatrix} 3 & 8 & 1 & 6 & 2 & 4 & 9 & 5 & 10 \\ 1 & 8 & 3 & 2 & 5 & 7 & 10 & 9 & 6 \end{bmatrix}$$

e questa permutazione è proprio τ! Questo chiaramente non è un caso, ma è il contentuto della prossima proposizione. Prima però introduciamo ancora un po' di nomenclatura.

Definizione. Dato $n > 0$, una *partizione* di n è una sequenza di numeri interi positivi $\lambda = (\lambda_1, \dots, \lambda_r)$ tale che $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_r > 0$ e $\lambda_1 + \cdots + \lambda_r = n$.

Ad esempio, se $n = 5$ abbiamo che le partizioni di 5 sono

$$(5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1).$$

Definizione. Data una permutazione $\sigma \in S_n$ e una partizione $\lambda = (\lambda_1, \dots, \lambda_r)$ di n diciamo che σ ha struttura ciclica λ se le orbite di σ (a meno di essere riordinate) hanno rispettivamente cardinalità $\lambda_1, \dots, \lambda_r$. Equivalentemente, se i cicli di λ (includendo anche i cicli di lunghezza 1) hanno rispettivamente ordine $\lambda_1, \dots, \lambda_r$.

Facciamo un piccolo esempio. Se $\sigma = [3,2,1,5,6,7,8,4]$ allora $\sigma = (1,3)(2)(4,5,6,7,8)$ e quindi la struttura ciclica di σ è $\lambda = (5,2,1)$.

Proposizione 11.2. *Sia $\sigma = (i_1, \dots, i_r)$ un ciclo e $\tau \in S_n$ una qualunque permutazione. Allora*

$$c_\tau(\sigma) = (\tau(i_1), \tau(i_2), \dots, \tau(i_r)).$$

Dimostrazione. Vogliamo calcolare $\tau\sigma\tau^{-1}(j)$ per ogni j. Se j non è del tipo $\tau(i_k)$ per qualche k allora $\tau^{-1}(j)$ non è del tipo i_k per cui $\sigma\tau^{-1}(j) = \tau^{-1}(j)$ e quindi

$$\tau\sigma\tau^{-1}(j) = j.$$

Se invece esiste k tale che $j = \tau(i_k)$ allora

$$\tau\sigma\tau^{-1}(j) = \tau\sigma(i_k) = \tau(i_{k+1})$$

dove abbiamo posto $i_{r+1} = i_1$. □

Facciamo un esempio. Vogliamo determinare τ tale che $c_\tau((1,3,2,5,4)) = (1,2,5,4,3)$. Basterà scegliere $\tau = [1,5,2,3,4]$. Non è questa l'unica possibilità : quali sono le altre? La proposizione appena dimostrata può essere estesa in modo immediato al caso in cui σ non sia necessariamente un ciclo. Infatti, se ad esempio $\sigma = (i_1, \dots, i_k)(i_{k+1}, \dots, i_{k+l})$ è prodotto di due cicli disgiunti di lunghezza k ed l allora

$$\begin{aligned} c_\tau(\sigma) &= c_\tau((i_1, \dots, i_k))c_\tau((i_{k+1}, \dots, i_{k+l})) \\ &= (\tau(i_1), \dots, \tau(i_k))(\tau(i_{k+1}), \dots, \tau(i_{k+l})) \end{aligned}$$

è anche prodotto di due cicli disgiunti di lunghezza h ed l. Più in generale, se σ è prodotto di r cicli disgiunti di lunghezza $k_1, \dots, k_r$, allora ogni coniugato di σ è prodotto di r cicli disiguntì di lunghezza $k_1, \dots, k_r$. Il seguente risultato ci mostra che vale anche il viceversa.

Teorema 11.3. *Siano σ_1 e σ_2 due permutazioni di S_n. Allora σ_1 e σ_2 sono coniugate se e solo se hanno la stessa struttura ciclica.*

Dimostrazione. Aggiungendo eventualmente anche cicli di lunghezza 1 possiamo assumere che $k_1 + \cdots + k_r = n$. Scriviamo, per fissare la notazione

$$\sigma_1 = (a_{11}, \dots, a_{1k_1})(a_{21}, \dots, a_{2k_2}) \cdots (a_{r1}, \dots, a_{rk_r})$$
$$\sigma_2 = (b_{11}, \dots, b_{1k_1})(b_{21}, \dots, b_{2k_2}) \cdots (b_{r1}, \dots, b_{rk_r})$$

Poniamo

$$\tau = \begin{bmatrix} a_{11} & \dots & a_{1k_1} & a_{21} & \dots & a_{2k_2} & \dots & a_{r1} & \dots & a_{rk_r} \\ b_{11} & \dots & b_{1k_1} & b_{21} & \dots & b_{2k_2} & \dots & b_{r1} & \dots & b_{rk_r} \end{bmatrix}$$

Allora, usando prima il fatto che c_τ è un omomorfismo e poi la Proposizione 11.2 abbiamo che

$$\begin{aligned} c_\tau(\sigma_1) &= c_\tau((a_{11}, \dots, a_{1k_1})(a_{21}, \dots, a_{2k_2}) \cdots (a_{r1}, \dots, a_{rk_r})) \\ &= c_\tau((a_{11}, \dots, a_{1k_1}))c_\tau((a_{21}, \dots, a_{2k_2})) \cdots c_\tau((a_{r1}, \dots, a_{rk_r})) \\ &= (\tau(a_{11}), \dots, \tau(a_{1k_1}))(\tau(a_{21}), \dots, \tau(a_{2k_2})) \cdots (\tau(a_{r1}), \dots, \tau(a_{rk_r})) \\ &= (b_{11}, \dots, b_{1k_1})(b_{21}, \dots, b_{2k_2}) \cdots (b_{r1}, \dots, b_{rk_r}) \\ &= \sigma_2. \end{aligned}$$

□

Concludiamo il nostro studio del gruppo simmetrico presentando alcuni insiemi di generatori di S_n minimali. Abbiamo già osservato che l'insieme di tutte le trasposizioni genera S_n. Vogliamo estrarne due sottoinsiemi minimali di generatori. Nei prossimi risultati useremo ripetutamente la Proposizione 11.2 senza ricordarlo esplicitamente.

Proposizione 11.4. *Fissato $i \in \{1, \dots, n\}$ l'insieme di $n-1$ trasposizioni*

$$\{(i, j) : j = 1, \dots, \hat{i}, \dots, n\}$$

è un insieme (minimale) di generatori.

Dimostrazione. Infatti, dati $j < k$ diversi da i abbiamo

$$(j, k)c_{(i,k)}((i, j)).$$

□

Il prossimo risultato mostra un altro insieme di trasposizioni che genera S_n che per motivi che forse un giorno vedrete è decisamente più importante del precedente.

Proposizione 11.5. *L'insieme di $n-1$ trasposizioni*

$$S = \{(i, i+1) : i = 1, \dots, n-1\}$$

è un insieme di generatori. Queste trasposizioni vengono anche chiamate traposizioni semplici.

Dimostrazione. Per la Proposizione precedente basterà mostrare che per ogni $i \geq 2$ la trasposizione $(1, i)$ appartiene al sottogruppo generato da S.

Procediamo per induzione su i. Se $i = 2$ abbiamo $(1, 2) \in S$ e quindi non c'è niente da dimostrare.

Vediamo il passo induttivo: sia quindi $i > 2$ e supponiamo che $(1, i-1) \in \langle S \rangle$. Allora

$$c_{(i-1,i)}(1, i-1) = (1, i) \in \langle S \rangle.$$

In alternativa, senza utilizzare la proposizione precedente possiamo direttamente mostrare per induzione su $k - j$ che ogni trasposizione (j, k) con $j < k$ appartiene al sottogruppo generato da S.

Passo base: se $k - j = 1$ allora $k = j + 1$ e il risultato è ovvio.

Passo induttivo: se $k - j > 1$

$$(j, k) = c_{(j,j+1)}(j+1, k)$$

□

Mostrare per esercizio che S_n non può essere generato da meno di $n-1$ trasposizioni. Tuttavia, possiamo osservare che S_n può essere generato da solo due permutazioni.

Proposizione 11.6. *S_n è generato da $\{(1, 2), (1, 2, \dots, n)\}$.*

Proof. Detto $\sigma = (1, 2, \dots, n)$ abbiamo

$$(i, i+1) = c_{\sigma^{i-1}}((1, 2)).$$

□

12. Classi laterali e teorema di Lagrange

Consideriamo un sottogruppo H di un gruppo G.

Definizione. Dato un elemento $g \in G$ il sottoinsieme di G

$$gH = \{gh : h \in H\}$$

si dice un H-laterale sinistro, o una classe laterale di sinistra di H.

Definiamo similmente gli H-laterali destri $Hg = \{hg : h \in H\}$. Prima di fare un esempio vediamo delle proprietà elementari dei laterali.

Lemma 12.1. *Per ogni $g \in G$ abbiamo $g \in gH$. Per ogni $g_1, g_2 \in G$ si ha*

$$g_1H \cap g_2H = \emptyset \text{ oppure } g_1H = g_2H.$$

In particolare l'insieme dei laterali sinistri è una partizione di G.

Dimostrazione. La prima parte è ovvia, basta scegliere $h = e$. Per la seconda parte supponiamo che i due laterali si intersechino, cioè che esistano $h_1, h_2 \in H$ tali che $g_1h_1 = g_2h_2$. Consideriamo un qualunque elemento $k \in g_1H$ cioè $k = g_1h$ per un opportuno elemento $h \in H$. Allora

$$k = g_1h = g_1h_1h_1^{-1}h = g_2h_2h_1^{-1}h \in g_2H,$$

e quindi $g_1H \subseteq g_2H$. Per simmetria abbiamo anche $g_2H \subseteq g_1H$. □

Di conseguenza abbiamo che appartenere ad uno stesso H-laterale sinistro è una relazione di equivalenza su G. È un semplice esercizio verificare che due elementi g_1, g_2 appartengono allo stesso laterale sinistro se e solo se $g_2^{-1}g_1 \in H$. Analogamente, g_1 e g_2 appartengono allo stesso laterale destro se e solo se $g_2g_1^{-1} \in H$.

Esempio 12.2. Consideriamo in S_3 il sottogruppo $H = \{e, (1,2)\}$ e determiniamone i laterali sinistri. Abbiamo

- $eH = \{e, (1,2)\}$;
- $(1,3)H = \{(1,3), (1,3)(1,2)\} = \{(1,3), (1,2,3)\}$;
- $(2,3)H = \{(2,3), (2,3)(1,2)\} = \{(2,3), (1,3,2)\}$.

Esercizio 12.3. Determinare i laterali destri di H e verificare che un laterale destro in generale non è anche un laterale sinistro.

Esempio 12.4. Sia $G = GL(2, \mathbb{R})$ e $H = SL(2, \mathbb{R})$ il sottogruppo delle matrici di determinante 1. In questo caso due matrici M_1, M_2 stanno nello stesso H-laterale sinistro se e solo se $M_1^{-1}M_2 \in H$ e quindi per il teorema di Binet M_1 ed M_2 stanno nello stesso laterale sinistro se e solo se hanno lo stesso determinante. Abbiamo quindi esattamente un laterale per ogni numero reale non nullo.

Osservare che avremmo ottenuto la stessa condizione considerando i laterali destri per cui in questo caso laterali destri e sinistri coincidono.

Definizione. Se i laterali sinistri sono finiti indichiamo con $[G : H]$ il numero di laterali sinistri. Se sono infiniti scriviamo $[G : H] = +\infty$. In ogni caso $[G : H]$ viene detto *indice* di H in G. Il motivo di questa notazione è contenuto nei prossimi risultati.

Proposizione 12.5. *Esiste una corrispondenza biunivoca tra l'insieme dei laterali sinistri e l'insieme dei laterali destri (per cui avremmo potuto definire l'indice $[G : H]$ anche utilizzando i laterali destri anziché i sinistri). Inoltre ogni classe laterale ha la stessa cardinalità di H.*

Dimostrazione. La funzione $gH \mapsto Hg^{-1}$ è una biiezione tra laterali destri e laterali sinistri (mentre $gH \mapsto Hg$ non è neanche ben definita in generale).

Mostriamo che è ben posta: se $g_1H = g_2H$ allora $g_2^{-1}g_1 \in H$. Per mostrare che $Hg_1^{-1} = Hg_2^{-1}$ dobbiamo verificare che $(g_1^{-1})(g_2^{-1})^{-1} \in H$ e questa è chiaramente equivalente alla precedente.

Per mostrare che è biunivoca è sufficiente osservare che la funzione $Hg \mapsto g^{-1}H$ ne è l'inversa.

Infine, mostriamo che $H \to gH$ data da $h \mapsto gh$ è una biiezione. Questa à suriettiva per definizione di laterale ed è iniettiva per la legge di cancellazione.

□

Corollario 12.6 (Teorema di Lagrange)**.** *Se G è un gruppo finito e H un suo sottogruppo allora*

$$|G| = [G : H]|H|$$

In particolare sia H che $[G : H]$ sono divisori di $|G|$.

Dimostrazione. Per la Proposizione precedente G è unione di $[G : H]$ laterali sinistri (disgiunti) ognuno dei quali ha cardinalità $|H|$. Il risultato segue. □

Corollario 12.7. *Se G è un gruppo finito e $g \in G$ allora $o(g) \,\big|\, |G|$ e in particolare $g^{|G|} = e$.*

Proof. Basta ricordare che se $H = \langle g \rangle$ allora $|H| = o(g)$. □

Possiamo anche osservare come il teorema di Eulero sia un caso particolare di questo corollario. Se infatti consideriamo il gruppo $G = U(\mathbb{Z}_{/n})$ abbiamo $|G| = \phi(n)$ per cui per ogni $[a] \in G$ (e quindi per ogni $a \in \mathbb{Z}$ tale che $MCD(a, n) = 1$) abbiamo

$$[a]^{\phi(n)} = [1]$$

cioè

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

13. Omomorfismi, sottogruppi normali e quozienti di un gruppo

Ricordiamo che dati due gruppi G, G' un omomorfismo

$$\varphi : G \to G'$$

è una funzione che rispetta le operazioni dei gruppi, cioè $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ per ogni $g_1, g_2 \in G$, dove a sinistra il prodotto tra g_1 e g_2 è quello di G, mentre a destra il prodotto tra $\varphi(g_1)$ e $\varphi(g_2)$ è quello di G'.

Definiamo nucleo e immagine di un omomorfismo $\varphi : G \to G'$ nel seguente modo

$$\mathrm{Im}(\varphi) = \{\varphi(g) : g \in G\}$$

e

$$\mathrm{Ker}(\varphi) = \{g \in G : \varphi(g) = e'\}.$$

Esercizio 13.1. Verificare che $\mathrm{Ker}(\varphi)$ è un sottogruppo di G e $\mathrm{Im}(\varphi)$ è un sottogruppo di G'.

Come per gli spazi vettoriali possiamo verificare facilmente che un omomorfismo è iniettivo se e solo se il suo nucleo è banale. Inoltre, se $\varphi : G \to G'$ è iniettivo allora $G \cong \mathrm{Im}(G)$. Abbiamo il seguente teorema.

Teorema 13.2 (Cayley)**.** *Sia G un gruppo finito, $|G| = n$. Allora G è isomorfo ad un sottogruppo di S_n.*

Proof. Abbiamo chiaramente $S(G) \cong S_n$ (dove $S(G)$ è il gruppo delle permutazioni di G pensato come insieme) per cui è sufficiente mostrare che esiste un omomorfismo iniettivo $\lambda : G \to S(G)$. Dobbiamo quindi associare ad ogni elemento g di G una funzione (invertibile)

$$\lambda_g : G \to G.$$

Definiamo λ_g ponendo $\lambda_g(x) = gx$, cioè λ_g è la moltiplicazione a sinistra per g.

Mostriamo intanto che effettivamente $S(G)$ è un codominio per λ, cioè che $\lambda_g \in S(G)$ e quindi che λ_g è invertibile. Per questo basta osservare che $\lambda_{g^{-1}}$ è l'inversa di λ_g cioè

$$\lambda_g \circ \lambda_{g^{-1}} = \lambda_{g^{-1}} \circ \lambda_g = Id_G,$$

dove Id_G indica l'identità su G, che ec l'elemento neutro di $S(G)$.

Una volta stabilito che λ è effettivamente una funzione $\lambda : G \to S(G)$ dobbiamo verificare che è anche un omomorfismo iniettivo di gruppi.

Vediamo che si tratta di un omomorfismo:

$$\lambda_{gg'}(x) = gg'x = g(\lambda_{g'}(x) = \lambda_g(\lambda_{g'}(x))$$

per cui $\lambda_{gg'} = \lambda_g \circ \lambda_{g'}$ e quindi λ è un omomorfismo. Mostriamo che λ è iniettivo: se $g \in \mathrm{Ker}(\lambda)$ allora $\lambda_g = Id_G$ per cui $g = ge = \lambda_g(e) = Id_G(e) = e$ e concludiamo che $g = e$ per la legge di cancellazione. □

Osserviamo che se $\varphi : G \to G'$ è un omomorfismo allora $N = \mathrm{Ker}(\varphi)$ è un sottogruppo che soddisfa una ulteriore proprietà algebrica notevole: per ogni $g \in G$ si ha che il laterale destro Ng e il laterale sinistro gN coincidono per ogni $g \in G$. Infatti possiamo verificare che in entrambi i casi abbiamo $Ng = \{x \in G : \varphi(x) = \varphi(g)\} = gN$.

Questa proprietà del nucleo di un omomorfismo motiva la seguente definizione

Definizione. Un sottogruppo $N \leq G$ si dice *normale* se per ogni $g \in G$ si ha $gN = Ng$.

Osserviamo che se il gruppo è abeliano allora ogni sottogruppo è normale, ma abbiamo già verificato che non tutti i sottogruppi sono normali.

Esempio 13.3. Un sottogruppo di indice 2 è normale. Ad esempio il gruppo alterno A_n ha indice due in S_n e quindi è normale.

Osservazione 3. Un sottogruppo N è normale se (e solo se) tutti i coniugati dei suoi elementi sono ancora suoi elementi. Infatti la definizione può anche essere riletta come $gNg^{-1} = N$. Equivalentemente possiamo dire che un sottogruppo è normale se e solo se è unione di classi di coniugio.

La definizione di sottogruppo normale è strettamente correlata a quella di gruppo quoziente. Ma cosa vuol dire fare un gruppo quoziente? Vuol dire dare una struttura di gruppo in modo naturale all'insieme quoziente rispetto ad una relazione d'equivalenza.

Definizione. Sia G un gruppo e $\sim$ una relazione d'equivalenza. Diciamo che $\sim$ è una relazione d'equivalenza *compatibile* se per ogni $x, y, x', y' \in G$ tali che $x \sim x'$ e $y \sim y'$ si ha $xy \sim x'y'$.

Non è difficile verificare che se $\sim$ è una relazione d'equivalenza compatibile allora possiamo dare all'insieme quoziente $G/\sim$ la struttura di gruppo utilizzando l'operazione di G, cioè ponendo:

$$[x][y] = [xy].$$

Tutte le verifiche sono immediate.

Proposizione 13.4. *Se N è un sottogruppo normale allora la relazione data da $x \sim y$ se $xy^{-1} \in N$ (cioè se x ed y appartengono allo stesso N-laterale) è una relazione d'equivalenza compatibile. Viceversa, sia $\sim$ una relazione d'equivalenza compatibile. Allora esiste un sottogruppo normale N tale che $x \sim y$ se e solo se $xy^{-1} \in N$.*

Dimostrazione. Per la prima parte siano $x \sim x'$ e $y \sim y'$ cioè $x'x^{-1} \in N$ e $y'y^{-1} \in N$. Sia quindi $x' = nx$ con $n \in N$ (dove abbiamo sfruttato che N è normale). Allora

$$x'y'(xy)^{-1} = x'(y'y^{-1})x^{-1} = nx(y'y^{-1})x^{-1}$$

è il prodotto tra un elemento di N e il coniugato di un elemento di N che sta quindi ancora in N.

Vediamo la seconda parte e sia quindi $\sim$ una relazione d'equivalenza compatibile. *Definiamo* N come la classe di equivalenza di e e mostriamo che N è un sottogruppo normale. Infatti siano $n_1, n_2 \in N$, cioè $n_1 \sim n_2 \sim e$. Allora

$$n_1 \cdot n_2 \sim e \cdot e = e$$

per cui $n_1 n_2 \in N$. Similmente, se $n \in N$ abbiamo

$$e = n \cdot n^{-1} \sim e \cdot n^{-1}$$

e quindi anche $n^{-1} \in N$. Per la normalità sia $n \in N$ e $g \in G$. Allora

$$g \cdot n \cdot g^{-1} \sim g \cdot e \cdot g^{-1} = e$$

per cui $gng^{-1} \in N$ e quindi N è normale.

Rimane da verificare che $x \sim y$ se e solo se $xy^{-1} \in N$. Infatti, se $x \sim y$, abbiamo

$$x \cdot y^{-1} \sim y \cdot y^{-1} = e$$

per cui $xy^{-1} \in N$ e viceversa, se $xy^{-1} \in N$, cioè $xy^{-1} \sim e$, abbiamo

$$x = xy^{-1} \cdot y \sim e \cdot y = y.$$

□

La Proposizione precedente ci permette di concludere che le relazioni d'equivalenza che danno una naturale struttura di gruppo al relativo insieme quoziente sono proprie quelle date dai sottogruppi normali.

Definizione. Sia N un sottogruppo normale di un gruppo G. Allora l'insieme G/N degli N laterali con l'operazione data da

$$xN \cdot yN = xyN.$$

si dice gruppo quoziente di G modulo N.

Abbiamo già visto un esempio cruciale di gruppo quoziente all'inizio del corso. Infatti abbiamo

$$\mathbb{Z}_{/n} = \mathbb{Z}/n\mathbb{Z}$$

è proprio il quoziente del gruppo $\mathbb{Z}$ modulo il suo sottogruppo $n\mathbb{Z}$. Vediamo un altro esempio

Esempio 13.5. Consideriamo il gruppo diedrale D_4. Il sottogruppo $N = \{e, r^2\}$ è un sottogruppo normale. Il relativo quoziente D_4/N è quindi un gruppo di ordine 4

$$D_4/N = \{[e], [r], [s], [sr]\}$$

in cui ogni elemento ha ordine 2. Questo gruppo è quindi isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Definizione. Dato un gruppo G e un suo sottogruppo normale N la funzione $\pi : G \to G/N$ si dice proiezione al quoziente.

Non è difficile mostrare che la proiezione al quoziente è un omomorfismo e che è suriettiva.
Il seguente teorema è di fondamentale importanza (di nome e di fatto)

Teorema 13.6 (fondamentale di omomorfismo)**.** *Sia $\varphi : G \to G'$ un omomorfismo di gruppi. Allora, detto $N = \ker(\varphi)$, la funzione indotta*

$$\overline{\varphi} : G/N \to \operatorname{Im} \varphi$$

data da $\overline{\varphi}(gN) = \varphi(g)$ è ben posta ed è un isomorfismo di gruppi.

Dimostrazione. Vediamo che è ben posta. se $g_1N = g_2N$, cioè esiste $n \in N$ tale che $g_1 = ng_2$ allora

$$\overline{\varphi}(g_1N) = \varphi(g_1) = \varphi(ng_2) = \varphi(n)\varphi(g_2) = \varphi(g_2) = \overline{\varphi}(g_2N).$$

Vediamo che $\overline{\varphi}$ è suriettiva: infatti se $\varphi(g) \in \operatorname{Im} \varphi$ allora $\varphi(g) = \overline{\varphi}(gN)$.
Infine, verifichiamo l'iniettività : se $\overline{\varphi}(gN) = e \in G_1$ allora $\varphi(g) = e$ e quindi $g \in N$ e concludiamo che $gN = N$ è proprio l'elemento neutro del gruppo G/N. □

Esempio 13.7. Sia $G = D_6$ e consideriamo il sottogruppo $N = \{e, r^3\}$. Mostrare che N è normale e che G/N è isomorfo a S_3. Chiamiamo d_1, d_2, d_3 le tre diagonali dell'esagono che uniscono un vertice con il suo opposto. Ogni elemento di D_6 permuta le tre diagonali tra di loro e quindi abbiamo in modo naturale un omomorfismo

$$\varphi : D_6 \to S(d_1, d_2, d_3) \cong S_3.$$

Osservando che questo omomorfismo è suriettivo e che gli unici elementi che fissano le tre diagonali sono proprio e ed r^3 abbiamo che il $\ker(\varphi) = N$ e possiamo quindi concludere.

14. Prodotti diretti e semidiretti

Se H e K sono due gruppi abbiamo già utilizzato in diverse occasioni il concetto di prodotto diretto (esterno): $H \times K$ è come insieme il prodotto cartesiano tra H e K con prodotto dato da

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2).$$

Si dice "esterno" perché è stato formato prendendo due gruppi astratti che non si trovavano a priori all'interno di uno stesso gruppo.

Definizione. Sia G un gruppo e H, K sottogruppi di G. Diciamo che G è prodotto diretto (interno) di H e K se

(1) H e K sono sottogruppi normali di G;
(2) $H \cap K = \{e\}$;
(3) $G = HK = \{hk : h \in H, k \in K\}$.

Osservazione 4. Se G è prodotto diretto interno di H e K allora ogni elemento di G si scrive in modo unico come prodotto di un elemento di H e uno di K. Infatti se $h_1 k_1 = h_2 k_2$ allora $h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$ per cui $h_1 = h_2$ e $k_1 = k_2$.

Proposizione 14.1. *Se G è prodotto diretto interno tra H e K allora*

(1) *$hk = kh$ per ogni $h \in H$ e $k \in K$;*
(2) *$\varphi : G \to H \times K$ dato da $\varphi(hk) = (h, k)$ è un isomorfismo.*

Dimostrazione. Per la prima parte è sufficiente osservare che $khk^{-1}h^{-1} \in H \cap K$. Infatti $khk^{-1} \in H$ perché H è normale e similmente $hk^{-1}h^{-1} \in K$ perché K è normale.

Per la seconda parte: φ è ben definita e iniettiva per l'Osservazione 4. La suriettività deriva dalla definizione di prodotto diretto esterno. Il fatto che sia un omomorfismo segue dalla prima parte: infatti, se $g_1 = h_1 k_1$ e $g_2 = h_2 k_2$ abbiamo

$$\varphi(g_1 g_2) = \varphi(h_1 k_1 h_2 k_2) = \varphi(h_1 h_2 k_1 k_2) = (h_1 h_2, k_1 k_2) = (h_1, k_1) \cdot (h_2, k_2)) = \varphi(g_1)\varphi(g_2).$$

□

Grazie a questa proposizione scriviamo $G = H \times K$ anche nel caso in cui G è prodotto diretto interno dei sottogruppi H e K.

Esempio 14.2. Se $G = \mathbb{Z}_{/6}$, $H = \langle [3] \rangle$ e $K = \langle [2] \rangle$ allora G è prodotto diretto interno tra H e K. E siccome $H \cong \mathbb{Z}_{/2}$ e $K \cong \mathbb{Z}_{/3}$ ritroviamo il teorema cinese del resto. Anzi, ora che abbiamo un po' di nozione dei gruppi possiamo anche rienunciare questo teorema dicendo che se n e m sono coprimi allora la funzione $\mathbb{Z}_{/nm} \to \mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$ data da

$$[a]_{nm} \mapsto ([a]_n, [a]_m)$$

è un isomorfismo di gruppi.

Molto interessante in teoria dei gruppi è una generalizzazione del prodotto diretto che abbiamo già incontrato diverse volte.

Definizione. Sia G un gruppo $H \leq G$ e $K \triangleleft G$. Diciamo che che G è un prodotto semidiretto interno tra H e K se

(1) $H \cap N = \{e\}$;
(2) $HN = G$.

Scriviamo in tal caso $G = H \ltimes N$ o $N \rtimes H$ (il simbolo è un triangolo $\triangleleft$ o $\triangleright$ affiancato da un simbolo $<$ o $>$; il triangolo "punta" verso il sottogruppo normale).

Osservazione 5. Se G è prodotto semidiretto interno di H ed N allora abbiamo anche $G = NH$ (l'inverso di un elemento di HN appartiene ad NH). Come nel caso del prodotto diretto abbiamo unicità di scrittura: se $g \in G$ esistono unici $h_1 \in H$ e $n_1 \in N$ tali che $g = h_1 n_1$; esitono anche unici $h_2 \in H, n_2 \in N$ tali che $g = n_2 h_2$.

Osservazione 6. Se $G = H \ltimes N$ allora

$$\varphi = G/N \to H$$

data da $\varphi(hN) = h$ è un isomorfismo di gruppi.

Esempio 14.3. Rivediamo alcuni esempi che abbiamo incontrato nelle scorse lezioni. In questi esempi abbiamo sempre $G = H \ltimes N$ e quindi $G/N \cong H$.

(1) $G = S_n$, $N = A_n$ e $H = \langle (1,2) \rangle$;
(2) $G = S_4$, $N = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ e $H = S_3$ (pensato come le permutazioni di S_4 che fissano il 4).
(3) $G = \tilde{A}_1$, $N = \{\text{traslazioni}\}$ e $H = \langle s_0 \rangle$.
(4) $G = GL_n(K)$, $N = SL_N(K)$ e

$$H = \left\{ \begin{pmatrix} k & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} : k \in K^* \right\} \cong K^*$$

A differenza del prodotto diretto, il prodotto semidiretto esterno è più complicato da realizzare e anzi talvolta non è neanche possibile (se non richiedendo che anche H sia normale e quindi ottenendo il caso particolare del prodotto diretto). Per capire questo problema facciamo un'osservazione: se $G = H \ltimes N$ allora il coniugio $c : H \to Aut(N)$ $h \mapsto c_h$ è un omomorfismo. Per costruire un prodotto semidiretto abbiamo proprio bisogno di un omomorfismo

$$\varphi : H \to Aut(N),$$
$$h \mapsto \varphi_h$$

per poi far "diventare" questo automorfismo il coniugio nel prodotto semidiretto... Vediamo come si può fare: prendiamo come insieme $G = H \times N$ e vediamo come potremmo definire il prodotto:

$$(h_1, n_1)(h_2, n_2) = h_1 n_1 h_2 k_2 = h_1 h_2 (h_2^{-1} n_1 h_2) n_2 = h_1 h_2 \varphi_{h_2^{-1}}(n_1) n_2$$

Prendiamo quindi come "definizione"

$$(h_1, n_1)(h_2, n_2) = (h_1 h_2, \varphi_{h_2^{-1}}(n_1) n_2).$$

Mostrare per esercizio che questa operazione definisce una struttura di gruppo su G e che G è prodotto semidiretto

15. Qualche osservazione sui quozienti

Vorrei aggiungere qualche osservazione sui legami che ci sono tra un gruppo G ed un suo quoziente G/N. Abbiamo studiato tempo fa i sottogruppi di $\mathbb{Z}_{/n} = \mathbb{Z}/n\mathbb{Z}$: abbiamo visto che sono tutti e soli della forma

$$H_d = \{[kd] : k \in \mathbb{Z}\}$$

dove d è un opportuno divisore di n. Abbiamo quindi che H_d sono le classi modulo n degli interi multipli di d cioè

$$H_d = d\mathbb{Z}/n\mathbb{Z}.$$

(E un esercizio visto per casa ha quindi la suggestiva interpretazione

$$\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/d\mathbb{Z}.)$$

Osserviamo che al variare di d tra i divisori di n abbiamo che $d\mathbb{Z}$ varia tra tutti i sottogruppi di $\mathbb{Z}$ che contengono $n\mathbb{Z}$. Abbiamo quindi che i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono dati dai quozienti dei sottogruppi che contengono $n\mathbb{Z}$, modulo $n\mathbb{Z}$ stesso. Questo fenomeno accade in un qualunque gruppo, come vediamo nella prossima proposizione.

Proposizione 15.1. *Sia H un sottogruppo di G che contiene un sottogruppo normale N di G. Allora*

1. *N è un sottogruppo normale di H;*
2. *H/N è un sottogruppo di G/N.*
3. *H è normale in G se e solo se H/N è normale in G/N.*

La corrispondenza

$$H \mapsto H/N$$

è una corrispondenza biunivoca tra sottogruppi di G che contengono N e i sottogruppi di G/N;

Dimostrazione.

1. Chiaramente N è un sottogruppo di H e siccome $gN = Ng$ per ogni $g \in G$ in particolare $hN = Nh$ per ogni $h \in H$.
2. Ricordiamo che H/N è un sottoinsieme (non vuoto) di G/N: è costituito dai laterali hN degli elementi di H. E siccome il prodotto è definito tramite i rappresentanti abbiamo
$$h_1N \cdot (h_2N)^{-1} = h_1N \cdot h_2^{-1}N = h_1h_2^{-1}N \in H/N$$
per cui H/N è un sottogruppo.
3. H è normale se e solo se per ogni $g \in G$ e $h \in H$ esiste $h' \in H$ tale che $ghg^{-1} = h'$. Similmente H/N è normale in G/N se e solo se per ogni $g \in G$ e $h \in H$ esiste $h' \in H$ tale che $gN \cdot hN \cdot g^{-1}N = h'N$. Ma quest'ultima condizione è equivalente a $ghg^{-1} = h'n$ per un opportuno $n \in N$ e siccome $N \subseteq H$ concludiamo.

La corrispondenza è iniettiva: supponiamo $H_1/N = H_2/N$ dove H_1 e H_2 sono sottogruppi di G che contengono N: questo vuol dire che per ogni $h_1 \in H_1$ esiste $h_2 \in H_2$ tale che $h_1N = h_2N$ e quindi esistono $n_1, n_2 \in N$ tali che $h_1n_1 = h_2n_2$ da cui $h_1 = h_2n_2n_1^{-1} \in H_2$ (ricordando che $N \leq H_2$) e quindi $H_1 \subseteq H_2$. Per simmetria concludiamo $H_1 = H_2$.

La corrispondenza è suriettiva. Sia K un sottogruppo di G/N: dobbiamo mostrare che esiste H sottogruppo di G contenente N tale che $K = H/N$. Il sottogruppo K è un insieme di laterali di G e definiamo H come l'unione di questi laterali. Equivalentemente

$$H = \{h \in G : \ hN \in K\}$$

o ancora H è la controimmagine di K tramite la proiezione $G \to G/N$.

Tutte le verifiche sono elementari:

- $N \subseteq H$: infatti N è l'elemento neutro di G/N e quindi $N \in K$.
- H è un sottogruppo: siano $h_1, h_2 \in H$, cioè $h_1N, h_2N \in K$. Siccome K è un sottogruppo abbiamo $h_1h_2^{-1} \in h_3N \in K$. Di conseguenza $h_1h_2^{-1}$ appartiene ad un laterale che sta in K e quindi $h_1h_2^{-1} \in H$.
- $K = H/N$ questo è chiaro per definizione di H.

□

Facciamo un'osservazione finale, in cui vediamo come sono fatti i quozienti di quozienti:

Teorema 15.2. *Sia G un gruppo e $H \subseteq K$ sottogruppi normali di G. Allora*

$$\frac{G/H}{K/H} \cong G/K.$$

Proof. Consideriamo $\varphi : G/H \to G/K$ dato da $\varphi(gK) = gH$. Mostrare per esercizio che (1) φ è ben definito, (2) φ è un omomorfismo suriettivo (3) che $\ker(\varphi) = K/H$. □

16. Azioni di gruppi

Abbiamo già incontrato diversi esempi di azioni di gruppi nel nostro studio. È arrivato il momento di formalizzare questo concetto.

Definizione. Diciamo che un gruppo G *agisce* su un insieme X (o che abbiamo un'azione di G su X) se è dato un omomorfismo $\varphi : G \to S(X)$. Esplicitamente questo vuol dire che per ogni $g \in G$ è definita una funzione invertibile $\varphi_g : X \to X$ tale che

$$\varphi_{g_1}(\varphi_{g_2}(x)) = \varphi_{g_1g_2}(x)$$

per ogni $x \in X$.

Se G agisce su X si è soliti anche scrivere $\varphi_g(x) = g.x$, ma preferiremo in questo corso mantenere la notazione con la φ.

Chiaramente se abbiamo un'azione di G su X e H è un sottogruppo di G abbiamo automaticamente anche un'azione di H su X per restrizione.

L'esempio base di azione è quello di S_n sull'insieme $\{1, 2, \ldots, n\}$. In questo caso la funzione φ è data semplicemente dall'identità: ogni permutazione $\sigma \in S_n$ "agisce" su $\{1, 2, \ldots, n\}$ per definizione.

Un'altro esempio è dato dal gruppo K^* che agisce su un qualunque K-spazio vettoriale V come moltiplicazione per scalare: $\varphi_c(v) = cv$ per ogni $c \in K^*$: la proprietà di azione fa parte della definizione di spazio vettoriale.

Esempio 16.1 (Coniugio)**.** Abbiamo un'azione di G su G per coniugio data da

$$c_h(g) = hgh^{-1}.$$

La verifica che si tratti di un'azione l'abbiamo già fatta nel caso del gruppo simmetrico e può essere ripetuta mutatis mutandis. Osserviamo che anche in questo caso il coniugio

$$c : G \to S(G)$$

ha l'ulteriore proprietà

$$c : G \to Aut(G),$$

cioè c_g è un automorfismo di G (un isomorfismo da G in sé) per ogni $g \in G$. Talvolta saremo interessati a considerare il coniugio anche su particolari sottoinsiemi di G. Ad esempio se consideriamo l'insieme X dei sottogruppi di G abbiamo un'azione anche su X: se infatti K è un sottogruppo di G allora

$$c_h(K) = hKh^{-1}$$

è anche un sottogruppo di G. Questo deriva dal fatto che c_h à un automorfismo di G e quindi l'immagine di un sottogruppo è ancora un sottogruppo (oppure si può verificare questa proprietà direttamente).

Esempio 16.2 (Moltiplicazione a sinistra)**.** Abbiamo un'azione di G su G per moltiplicazione a sinistra data da

$$\lambda_h(g) = hg.$$

Le verifiche sono ovvie. Anche in questo caso saremo interessati a considerare la moltiplicazione a sinistra su particolari sottoinsiemi di G: se K è un qualunque sottogruppo possiamo considerare l'insieme X dei laterali sinistri di K:

$$X = \{gK : g \in G\}.$$

L'azione di moltiplicazione a sinistra $\lambda_h(gK) = hgK$ definisce un'azione di G su questi laterali. Considereremo anche l'azione λ sull'insieme di tutti i sottoinsiemi di G di data cardinalità.

Esempio 16.3 (Moltiplicazione a destra)**.** Similmente a prima possiamo definire l'azione di moltiplicazione a destra

$$\rho_h(g) = hg^{-1}$$

e possiamo estendere questa azione ai laterali destri o a generici sottoinsiemi di G.

Nello studio delle permutazioni abbiamo parlato di orbite. Possiamo generalizzare questo concetto ad un'azione qualunque:

Definizione. Sia φ un'azione di un gruppo G su un insieme X. L'orbita di un elemento $x \in X$ è

$$\mathcal{O}(x) = \{\varphi_g(x) : g \in G\}.$$

L'orbita di x è quindi costituita da tutti gli elementi di X che posso ottenere applicando tutti i possibili φ_g ad x.

Se consideriamo l'azione naturale di S_n su $\{1, 2, \ldots, n\}$ abbiamo che tutti gli elementi stanno nella stessa orbita: dati i e j senz'altro esiste $\sigma \in S_n$ tale che $\sigma(i) = j$. Se consideriamo invece l'azione naturale del sottogruppo generato da una permutazione $H = \langle\sigma\rangle$ abbiamo

$$\mathcal{O}(i) = \{i, \sigma(i), \sigma^2(i), \ldots\}$$

e quindi ritroviamo quella che avevamo chiamato l'orbita di i tramite σ.

Non dovrebbe sorprendere la seguente

Osservazione 7. Le orbite formano una partizione di X. Equivalentemente abbiamo che "appartenere ad una stessa orbita" definisce una relazione d'equivalenza su X.

Osserviamo che nella moltiplicazione a sinistra (sia sugli elementi di G che sui laterali sinistri di K) abbiamo un'unica orbita. Si dice in questo caso che l'azione è *transitiva*.

Nel caso del coniugio di G su G abbiamo che le orbite sono proprio le classi di coniugio.

Definizione. Se G agisce su un insieme X e $x \in X$ definiamo lo stabilizzatore di x come

$$Stab(x) = \{g \in G : \varphi_g(x) = x\}.$$

È una semplice verifica mostrare che $Stab(x)$ è un sottogruppo di G. Vediamo come sono fatti gli stabilizzatori negli esempi che stiamo studiando.

Nell'azione naturale di S_n abbiamo che lo stabilizzatore di i è dato dalle permutazioni che fissano i per cui è un sottogruppo isomorfo a S_{n-1}.

Nel caso del coniugio abbiamo che

$$Stab(g) = \{h \in G : hgh^{-1} = g\} = \{h \in G : gh = hg\}.$$

Abbiamo quindi che $Stab(g)$ è dato dagli elementi di G che commutano con g: questo sottogruppo prende il nome di centralizzatore di g e viene anche denotato con $Cen(g)$.

Nel caso della moltiplicazione a sinistra su G lo stabilizzatore è sempre banale: $hg = g$ implica $h = e$. Se invece consideriamo la moltiplicazione a sinistra sui laterali di un sottogruppo la stabilizzatore diventa un gruppo interessante: abbiamo

$$Stab(gK) = \{h \in g : hgK = gK\} = \{h \in G : \text{esiste } k \in K \text{ per cui } hg = gk\} = gKg^{-1}.$$

Abbiamo quindi che lo stabilizzatore del laterale gK è proprio $c_g(K)$ il coniugato di K tramite g.

Teorema 16.4 (Formula delle orbite)**.** *Sia G un gruppo che agisce su un insieme finito X. Siano $x_1, \ldots, x_r$ rappresentanti delle orbite dell'azione. Allora gli stabilizzatori hanno tutti indice finito e*

$$|X| = \sum_{i=1}^{r} [G : Stab(x_i)].$$

Dimostrazione. Basterà dimostrare che ogni orbita $\mathcal{O}(x)$ è in biiezione con l'insieme dei laterali sinistri di $Stab(x)$, per cui $|\mathcal{O}(x)| = [G : Stab(x)]$. Definiamo

$$F : \{\varphi_g(x) : g \in G\} \to \{gStab(x) : g \in G\}$$

ponendo $F(\varphi_g(x)) = gStab(x)$. Osserviamo che F è ben posta: se $\varphi_{g_1}(x) = \varphi_{g_2}(x)$ allora applicando $\varphi(g_2^{-1})$ abbiamo $g_2^{-1}g_1 \in Stab(x)$ per cui $g_1Stab(x) = g_2Stab(x)$.

Abbiamo che F è suriettiva per definizione. Vediamo l'iniettività: se $g_1Stab(x) = g_2Stab(x)$ allora $g_1 = g_2h$ con $h \in Stab(x)$ e quindi $\varphi_{g_1}(x) = \varphi_{g_2}(\varphi_h(x)) = \varphi_{g_2}(x)$. □

Esempio 16.5. Consideriamo l'azione naturale di $G = \{e, (1,2,3), (1,3,2)\}$ su $X = \{1,2,3,4\}$. In questo caso abbiamo due orbite: $\{1,2,3\}$ e $\{4\}$. Lo stabilizzatore di $\{1\}$ è $Stab(1) = \{e\}$ e $Stab(4) = G$. E infatti abbiamo

$$4 = |X| = [G : \{e\}] + [G : G] = 3 + 1.$$

Diciamo che un'orbita è banale se è costituita da un solo elemento. In questo caso lo stabilizzatore di questo elemento è dato da tutto il gruppo G. Osserviamo che nel caso in cui l'azione è il coniugio di G su se stesso abbiamo che gli elementi che formano orbite banali sono gli elementi del centro $Z(G)$.

Esempio 16.6. Consideriamo $G = D_6$. In questo caso si può verificare che le classi di coniugio sono

$$\{e\},\ \{r^3\},\ \{r, r^5\}, \{r^2, r^4\}, \{s, sr^2, sr^4\}, \{sr, sr^3, sr^5\}.$$

Scegliamo un elemento per ogni orbita e calcoliamone il centralizzatore. Abbiamo:

$$\begin{aligned} Cen(e) &= Cen(r^3) = D_6 \\ Cen(r) &= Cen(r^2) = \{e, r, r^2, r^3, r^4, r^5\} \\ Cen(s) &= \{e, r^3, s, sr^3\} \\ Cen(sr) &= \{e, r^3, sr, sr^4\}. \end{aligned}$$

Scegliamo in G un insieme di rappresentanti $\{g_1, \ldots, g_s\}$ delle classi di coniugio non banali. Allora la formula delle orbite diventa la famosa

Corollario 16.7 (Formula delle classi)**.** *Si ha*

$$|G| = |Z(G)| + \sum_{i=1}^{s} [G : Cen(g_i)].$$

La formula delle classi ha delle conseguenze immediate rilevanti.

Corollario 16.8. *Sia p un primo. Se un gruppo ha ordine p^n allora il suo centro non è banale. Un gruppo di ordine p^2 è abeliano.*

Proof. Nella formula delle classi gli indici $[G : Cen(g_i)]$ sono potenze (positive) di p. Ne segue che p è un divisore di $Z(G)$.

Dalla prima parte sappiamo che $Z(G)$ è non banale per cui ha almeno p elementi. Supponiamo per assurdo che ci sia almeno un addendo $[G : Cen(g_1)]$ nella formula delle

classi. Il centralizzatore $Cen(g_1)$ deve contenere $Z(G)$ e anche g_1 per cui contiene almeno $p+1$ elementi e quindi deve essere tutto G. Ma questo implicherebbe che ogni elemento commuta con g_1 per cui $g_1 \in Z(G)$, assurdo. □

Mostriamo ora un primo teorema che inverte parzialmente il teorema di Lagrange:

Teorema 16.9 (Cauchy)**.** *Sia G un gruppo finito e p un primo divisore di $|G|$. Allora esiste in G un elemento di ordine p.*

Proof. Procediamo per induzione su $n = |G|$. Il passo base è $n = p$ e sappiamo già che in questo caso $G \cong \mathbb{Z}_{/p}$. Se G avesse un sottogruppo proprio di ordine divisibile per p il teorema seguirebbe per induzione. Supponiamo quindi che ogni sottogruppo proprio abbia ordine non divisibile per p. Vediamo prima il caso in cui G è abeliano. Sia H un sottogruppo non banale (perché siamo sicuri che esiste?). Siccome G è abeliano H è normale e quindi possiamo considerare il quoziente G/H: questo gruppo ha ordine minore di n ancora divisibile per p (perché $|H|$ non è divisibile per p). Nel quoziente esiste quindi un elemento gH di ordine p, cioè esiste un elemento $g \notin H$ tale che $g^p \in H$. Abbiamo inoltre che, se $m = |H|$ allora $(g^p)^m = e$. Ora, se $g^m \neq e$, abbiamo trovato l'elemento di ordine p, cioè proprio g^m. Possiamo quindi assumere che $g^m = e$. Utilizziamo ora l'identità di Bézout tra m e p: $rp + sm = 1$ per dedurre che

$$g = g^{rp+sm} = (g^p)^r (g^m)^s = (g^p)^r \in H$$

perché $g^p \in H$. Abbiamo quindi la contraddizione $g \in H$.

Supponiamo ora che G non sia abeliano. In questo caso $Z(G)$ è un sottogruppo proprio (perché G non è abeliano) e se p divide $|Z(G)|$ concludiamo per ipotesi induttiva; quindi possiamo assumere che $|Z(G)|$ non sia divisibile per p. Di conseguenza esiste g_i tale che $[G : Cen(g_i)]$ non è divisibile per p: questo implica che $Cen(g_i)$ è divisibile per p e il risultato segue per ipotesi induttiva. □

17. Il teorema di Sylow

Il teorema di Cauchy è una conseguenza di un teorema ben più rilevante che riguarda non solo i sottogruppi di ordine p, ma i sottogruppi di ordine una qualunque potenza di p. È questo il contenuto del famoso teorema di Sylow.

Se $n > 1$ e p un primo definiamo la molteplicità di p in n come

$$m_p(n) = \max\{r : p^r | n\}.$$

Teorema 17.1 (Sylow)**.** *Sia p un primo, G un gruppo finito, $|G| = n$ e $m = m_p(n)$. Allora esiste un sottogruppo di G di ordine p^m.*

Se $|G| = n$ e $m = m_p(n)$ allora un sottogruppo di ordine p^m si dice p-sottogruppo di Sylow di G, o p-Sylow di G o anche solo Sylow di G. Prima di addentrarci nelle dimostrazioni vediamo l'esempio più bello di sottogruppi di Sylow.

Proposizione 17.2. *Sia $G = GL_d(\mathbb{Z}_{/p})$ e sia S il sottogruppo di G dato dalle matrici triangolari superiori che hanno tutti 1 sulla diagonale. Allora S è un p-Sylow di G.*

Proof. Dobbiamo prima di tutto determinare $|G|$: sappiamo che $|G|$ è uguale al numero di basi ordinate distinte di $\mathbb{Z}_{/p}^d$: il primo vettore è uno qualunque non nullo (p^d-1 possibilità), il secondo non deve essere proporzionale al primo (p^d-p possibilità), il terzo non deve essere combinazione lineare dei primi due (p^d-p^2 possibilità) ecc. Abbiamo quindi che

$$n = |G| = (p^d-1)(p^d-p)(p^d-p^2)\cdots(p^d-p^{d-1}) = (p^d-1)p(p^{d-1}-1)p^2(p^{d-2}-1)\cdots p^{d-1}(p-1)$$

e di conseguenza

$$m_p(n) = 1 + 2 + \cdots + (d-1).$$

Calcoliamo ora l'ordine di S: in questo caso abbiamo p scelte per ogni coefficiente al di sopra della diagonale principale: questi coefficienti sono $d-1$ nella prima riga, $d-2$ nella seconda,..., 1 nella penultima. Concludiamo che

$$|S| = p^{(d-1)+(d-2)+\cdots 1} = p^{m_p(n)}$$

per cui S è un p-Sylow. □

Vedremo tre dimostrazioni differenti del teorema di Sylow che mettono in luce tre diversi aspetti, ma tutti molto interessanti. Prima di vedere la prima dimostrazione premettiamo un lemma.

Lemma 17.3. *Sia $m = m_p(n)$. Allora il coefficiente binomiale $\binom{n}{p^m}$ non è divisibile per p.*

Dimostrazione. Sia $n = p^m a$ con $p \nmid a$. Abbiamo

$$\binom{n}{p^m} = \frac{p^m a(p^m a-1)(p^m a-2)\cdots(p^m a-p^m+1)}{p^m(p^m-1)(p^m-2)\cdots(p^m-p^m+1)} = a\prod_{i=1}^{p^m-1}\frac{p^m a-i}{p^m-i}.$$

Sarà sufficiente mostrare che in ogni fattore della produttoria vengono semplificati tutti i fattori p. Infatti se $i = p^s j$ con $j \not\equiv 0 \mod p$ e $s < m$ (perché $i < p^m$) abbiamo

$$\frac{p^m a-i}{p^m-i} = \frac{p^m a-p^s j}{p^m-p^s j} = \frac{p^{m-s}a-j}{p^{m-s}-j}$$

e chiaramente il numeratore e il denominatore rimasti sono entrambi $\equiv -j \mod p$ e quindi non sono più divisibili per p. □

Siamo ora pronti per la prima dimostrazione in cui utilizziamo la formula delle orbite per l'azione di moltiplicazione a sinistra su particolari sottoinsiemi di G.

Dimostrazione 1 del teorema di Sylow. Sia X l'insieme di tutti i sottoinsiemi di G con p^m elementi e consideriamo l'azione λ su X.

Osserviamo intanto che ogni stabilizzatore ha al più p^m elementi. Infatti, sia $x \in X$ con $x = \{g_1, \ldots, g_{p^m}\}$ e $g \in Stab(x)$: allora esiste j tale che $gg_1 = g_j$ per cui $g \in \{1, g_2g^{-1}, \ldots, g_{p^m}g^{-1}\}$ e quindi $|Stab(x)| \leq p^m$ per ogni $x \in X$. Ci basterà quindi mostrare che esiste $x_0 \in X$ tale che p^m divide $|Stab(x_0)|$.

Osserviamo che $|X| = \binom{n}{p^m}$ e quindi per il Lemma 17.3 abbiamo $p \nmid |X|$. Per la formula delle orbite abbiamo che esiste $x_0 \in X$ tale che $p \nmid [G : Stab(x_0)]$ e quindi p^m divide $|Stab(x_0)|$.

Concludiamo che $Stab(x_0)$ è un p-Sylow. □

La seconda dimostrazione utilizza la formula delle classi e riprende idee analoghe a quelle che abbiamo visto per la dimostrazione del teorema di Cauchy.

Dimostrazione 2 del teorema di Sylow. Procediamo per induzione su $n = |G|$. Il passo base è $n = 2$ che chiaramente soddisfa il teorema. Possiamo quindi supporre che se H è un sottogruppo proprio di G allora p^m non divide $|H|$ (altrimenti H conterrebbe un p-Sylow che sarebbe anche un p-Sylow di G). Consideriamo la formula delle classi

$$|G| = |Z(G)| + \sum_{i=1}^{s} [G : Cen(g_i)].$$

Siccome p^m non divide $|Cen(g_i)|$ abbiamo che p divide $[G : Cen(g_i)]$ per ogni i e quindi p divide anche $|Z(G)|$. Possiamo a questo punto applicare il teorema di Cauchy per il quale esiste un sottogruppo N di $Z(G)$ di ordine p. Siccome gli elementi di N commutano con tutti gli elementi di G abbiamo che questo sottogruppo N è necessariamente normale e possiamo quindi considerare il quoziente G/N che avrà ordine n/p. Per induzione abbiamo che G/N contiene un p-Sylow, cioè esiste un suo sottogruppo di ordine p^{m-1}. Per la descrizione dei sottogruppi di un quoziente sappiamo che tale sottogruppo è della forma S/N dove S è un sottogruppo di G che contiene N. Ma chiaramente $|S| = |N| \cdot |S/N| = p \cdot p^{m-1}$ per cui S è un p-Sylow. □

L'ultima dimostrazione che vogliamo vedere è per certi aspetti quella più curiosa, e forse anche quella più brillante. Il fatto più rilevante è il seguente.

Proposizione 17.4. *Sia H un sottogruppo di un gruppo G e sia S un p-Sylow di G. Allora esiste $g \in G$ tale che $H \cap gSg^{-1}$ è un p-Sylow di H.*

Proof. Sia X l'insieme dei laterali sinistri di S e consideriamo l'azione λ di G su X. Ricordiamo che in questa azione lo stabilizzatore del laterale gS è $Stab_G(gS) = gSg^{-1}$ per cui è un gruppo di ordine potenza di p. Se restringiamo l'azione di G al sottogruppo H i nuovi stabilizzatori si otterranno da quelli precedenti intersecandoli con H, cioè $Stab_H(gS) = gSg^{-1} \cap H$ per cui saranno ancora dei gruppi di ordine potenza di p.

Consideriamo a questo punto la formula delle orbite per l'azione di H sull'insieme X dei laterali sinistri di S:

$$|X| = \sum_{x_i} [H : Stab(x_i)].$$

La cardinalità di X è l'indice di S in G per cui p non divide $|X|$. Di conseguenza esiste x_i tale che p non divide $[H : Stab(x_i)]$: deduciamo che lo stabilizzatore $Stab(x_i)$ ha ordine divisibile per la massima potenza di p che divide $|H|$ e quindi è necessariamente un p-Sylow di H. □

Premettiamo un'interessante osservazione apparentemente scollegata

Proposizione 17.5. *Per ogni $n > 0$ e per ogni primo p il gruppo simmetrico S_n è isomorfo ad un sottogruppo di $GL_n(\mathbb{Z}_{/p})$.*

Proof. Ricordiamo che $GL_n(\mathbb{Z}_{/p})$ è il gruppo degli endomorfismi invertibili (o automorfismi) dello spazio vettoriale $V = (\mathbb{Z}_{/p})^n$. Ad ogni permutazione $\sigma \in S_n$ associamo l'endomorfismo F_σ di V che permuta gli elementi della base canonica:

$$F_\sigma(e_i) = e_{\sigma(i)}$$

ed è esteso per linearità a tutto V. Tutte le verifiche sono banali. È chiaro che $F_{\sigma^{-1}}$ è l'inversa di F_σ per cui F_σ è invertibile. Dobbiamo mostrare che $F_{\sigma\tau} = F_\sigma \circ F_\tau$: infatti

$$F_\sigma(F_\tau(e_i)) = F_\sigma(e_{\tau(i)}) = e_{\sigma(\tau(i))} = F_{\sigma\tau}(e_i).$$

□

Possiamo scrivere esplicitamente le matrici associate agli endomorfismi F_σ per $n = 3$: abbiamo

$$F_e = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ F_{[2,1,3]} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ F_{[1,3,2]} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$F_{[2,3,1]} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ F_{[3,1,2]} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},\ F_{[3,2,1]} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Osserviamo che p non gioca alcun ruolo in questo fatto.

Dimostrazione 3 del teorema di Sylow. Per il teorema di Cayley sappiamo che G è isomorfo ad un sottogruppo di S_n e per la Proposizione 17.5 abbiamo quindi che G è isomorfo ad un sottogruppo di $GL_n(\mathbb{Z}_{/p})$. Per la Proposizione 17.2 sappiamo che in $GL_n(\mathbb{Z}_{/p})$ esiste un p-Sylow e quindi per la Proposizione 17.4 esiste anche un p-Sylow di G. □

Possiamo anche enunciare la seguente generalizzazione del teorema di Sylow.

Corollario 17.6. *Sia p un primo, G un gruppo, $|G| = n$ e supponiamo $p^r|n$. Allora G contiene un sottogruppo di ordine p^r*

Dimostrazione. Possiamo assumere per il teorema di Sylow che $|G| = p^m$ e procediamo per induzione su m. Il passo base consiste nel caso $m = 1$ per cui il risultato è ovvio. Per il Corollario 16.8 sappiamo che il centro di G non è banale e per il teorema di Cauchy $Z(G)$ contiene un sottogruppo N di ordine p. Questo sottogruppo è necessariamete normale in G come già osservato nella seconda dimostrazione del teorema di Sylow.

Possiamo quindi considerare il gruppo quoziente G/N di ordine p^{m-1}. Per ipotesi induttiva questo gruppo contiene un sottogruppo H/N di ordine p^{r-1}. Il sottogruppo H sarà quindi il sottogruppo di G di ordine p^r cercato. □