Appunti delle lezioni del corso di Aritmetica

Michele D'Adderio, Giovanni Gaiffi

17 dicembre 2022

Indice

CAPITOLO 1

I primi passi: i numeri di Fibonacci, l'algoritmo di Euclide e il principio di induzione.

Per questo primo capitolo assumeremo la conoscenza delle proprietà fondamentali dei *numeri naturali* $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ e più in generale degli interi $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

1. I numeri di Fibonacci.

Consideriamo la successione di numeri F_n, con $n \in \mathbb{N}$, così definita:

- $F_0 = 0$
- $F_1 = 1$
- per ogni $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}.$$

Per prima cosa "costruiamo" i primi numeri della successione :
$F_0 = 0$
$F_1 = 1$
$F_2 = F_0 + F_1 = 1$
$F_3 = F_2 + F_1 = 1 + 1 = 2$
$F_4 = 2 + 1 = 3$
$F_5 = 3 + 2 = 5$
$F_6 = 5 + 3 = 8$
$F_7 = 8 + 5 = 13$
$F_8 = 13 + 8 = 21$
e così via.. I numeri F_n si dicono **numeri di Fibonacci** (con riferimento a Leonardo da Pisa, che pubblicò sotto il nome di Fibonacci il suo libro più celebre, *Liber abaci*, nel 1202).

Osserviamo che, per conoscere il numero F_n non ci basta conoscere il numero precedente F_{n-1}, ma bisogna conoscere anche il numero F_{n-2}.

Una successione di questo tipo, ossia in cui il termine ennesimo si costruisce sapendo i termini precedenti, si dice *successione definita per ricorrenza*. Perché la successione sia ben definita, bisogna conoscere i valori iniziali. Per esempio, nel caso di Fibonacci, visto che ogni termine chiama in causa i due precedenti, F_0 e F_1 devono essere noti fin dall'inizio (non possono essere ricavati dalla "regola ricorsiva" $F_n = F_{n-1} + F_{n-2}$ che non li riguarda).

Un altro esempio di successione definita per ricorrenza potrebbe essere: $b_0 = 7$ e, per ogni $n \geq 1$, $b_n = 4b_{n-1}^2$.

2. Una formula per i numeri di Fibonacci

Partiamo da una *successione*[1] $(a_n)_{n\in\mathbb{N}}$, molto semplice, definita per ricorrenza[2]:

$$a_0 = 1$$

[1]La scrittura $(a_n)_{n\in\mathbb{N}}$ denota la successione degli a_n al variare di n in $\mathbb{N}$.
[2]Il simbolo "$\forall$" sta per "per ogni".

$$a_n = 3a_{n-1} \qquad \forall n \geq 1.$$

Sappiamo trovare una *formula* per a_n, ossia una equazione che ci permetta di calcolare a_n direttamente, senza dover calcolare prima a_{n-1}? Proviamo a scrivere i primi termini della successione:
$a_0 = 1$
$a_1 = 3 \cdot 1 = 3$
$a_2 = 3 \cdot 3 = 3^2$
$a_3 = 3 \cdot 3^2 = 3^3$
e così via.. Non ci mettiamo molto a congetturare che la formula giusta per a_n potrebbe essere:

$$a_n = 3^n.$$

Dalla congettura alla dimostrazione in questo caso il passo è breve: ci basta notare che le due successioni $(a_n)_{n\in\mathbb{N}}$ e $(3^n)_{n\in\mathbb{N}}$ soddisfano la stessa regola ricorsiva e la stessa condizione iniziale, dunque si mostra facilmente che devono coincidere termine a termine, ossia $a_n = 3^n$ per ogni $n \in \mathbb{N}$.

Ma torniamo a Fibonacci: come possiamo trovare una formula per i numeri F_n? Memori dell'esempio precedente, possiamo cominciare da un tentativo; proviamo se può funzionare una formula del tipo:

$$F_n = \alpha^n$$

per un qualche $\alpha \in \mathbb{R} - \{0\}$ (certamente $\alpha = 0$ non andrebbe bene, essendo $F_1 = 1$..).
Se fosse così, allora, visto che per $n \geq 2$ vale $F_n = F_{n-1} + F_{n-2}$, dovremmo avere

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2}$$

che, dividendo per α^{n-2}, diventa

$$\alpha^2 = \alpha + 1.$$

Quindi il nostro numero α dovrebbe essere una radice del polinomio $x^2 - x - 1$. Sappiamo che le radici di tale polinomio sono due:

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{e} \quad \beta = \frac{1-\sqrt{5}}{2}.$$

Cominciamo a pensare di essere sulla strada giusta: infatti, rifacendo il ragionamento a ritroso, notiamo che con il nostro tentativo abbiamo trovato due numeri $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ che soddisfano

$$\alpha^2 = \alpha + 1 \quad \text{e} \quad \beta^2 = \beta + 1$$

e quindi anche, per ogni $n \geq 2$:

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2} \quad \text{e} \quad \beta^n = \beta^{n-1} + \beta^{n-2}.$$

Entrambe le successioni $\{\alpha^n\}$ e $\{\beta^n\}$ soddisfano dunque la stessa regola ricorsiva della successione di Fibonacci: per $n \geq 2$, il termine n-esimo è somma dei due termini precedenti.
Il problema è che né $\alpha^1 = \alpha$ né $\beta^1 = \beta$ sono uguali a F_1 che è 1. Inoltre $\alpha^0 = 1$ e $\beta^0 = 1$ non sono uguali a F_0, che è 0.

In altre parole queste successioni non "partono" dagli stessi numeri con cui parte la successione di Fibonacci, dunque i loro termini sono poi molto diversi dai numeri di Fibonacci.

Possiamo rimediare però osservando che anche una successione del tipo $\{a\ \alpha^n + b\ \beta^n\}$, con a e b numeri reali qualunque, soddisfa la richiesta che il termine n-esimo sia somma dei due termini precedenti:

$$a\alpha^n + b\beta^n = \left(a\alpha^{n-1} + b\beta^{n-1}\right) + \left(a\alpha^{n-2} + b\beta^{n-2}\right).$$

Dunque potremmo controllare se è possibile scegliere a e b in modo che $a\alpha^0 + b\beta^0 = 0$ e $a\alpha^1 + b\beta^1 = 1$. Si vede subito che il sistema di equazioni:

$$a\left(\frac{1+\sqrt{5}}{2}\right)^0 + b\left(\frac{1-\sqrt{5}}{2}\right)^0 = 0$$

$$a\left(\frac{1+\sqrt{5}}{2}\right)^1 + b\left(\frac{1-\sqrt{5}}{2}\right)^1 = 1$$

ha come unica soluzione $a = \dfrac{1}{\sqrt{5}}$, $b = -\dfrac{1}{\sqrt{5}}$. Dunque la successione $\{c_n\}$ definita, per ogni $n \in \mathbb{N}$, così:

$$c_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

soddisfa tutte le richieste della successione di Fibonacci.

Ripetiamo allora, per metterlo bene in evidenza, il ragionamento conclusivo: poiché entrambe le successioni soddisfano la stessa legge ricorsiva e le stesse condizioni iniziali, allora coincidono, ossia $c_n = F_n$ per ogni $n \in \mathbb{N}$.

Questo ragionamento non costituisce ancora una dimostrazione formale: quella potremo farla, come facile esercizio, dopo aver introdotto il principio di induzione. Fiduciosi in questo, presentiamo il risultato ottenuto già come teorema:

TEOREMA 1.1. *Dato $n \in \mathbb{N}$, vale la seguente formula per i numeri di Fibonacci:*

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

Suggerimento per una ricerca. Il numero $\alpha = \frac{1+\sqrt{5}}{2}$ è il cosiddetto "rapporto aureo", ossia il rapporto fra la lunghezza di un segmento e quella della sua "sezione aurea". Sapete cosa è?

3. Un metodo per le ricorrenze lineari a coefficienti costanti

Il metodo che abbiamo usato per trovare la formula per i numeri di Fibonacci è partito da un tentativo ("vediamo se per caso vanno bene soluzioni del tipo α^n") ma si è rivelato poi molto efficace. Osserviamo che, ripetendo il ragionamento, il metodo si può generalizzare al caso di successioni definite per ricorrenza in cui la legge ricorsiva sia *lineare e a coefficienti costanti*, ossia del tipo:

$$a_n = \gamma_1 a_{n-1} + \gamma_2 a_{n-2} + \gamma_3 a_{n-3} + \cdots + \gamma_i a_{n-i}$$

dove i γ_j sono numeri complessi.
Per esempio prendiamo, per $n \geq 4$, la legge

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

con le condizioni iniziali

$$a_1 = 4 \quad a_2 = 22 \quad a_3 = 82.$$

Lo stesso ragionamento usato per Fibonacci ci porta a cercare le radici del polinomio $x^3 - 6x^2 + 11x - 6$. Tali radici (che in generale possiamo cercare in $\mathbb{C}$) si trovano in questo caso molto facilmente e sono 1, 2 e 3; allora tutte le successioni del tipo

$$a\ 1^n + b\ 2^n + c\ 3^n.$$

con a, b, c numeri reali qualsiasi soddisfano la legge ricorsiva data. Facendo il sistema di tre equazioni per imporre che valgano le 3 condizioni iniziali si trova che la formula per la successione a_n è, per ogni $n \geq 1$:

$$a_n = -2 \cdot 1^n + (-3) \cdot\ 2^n + 4 \cdot\ 3^n$$

Quindi quando avete di fronte una successione definita per ricorrenza lineare e a coefficienti costanti potete tentare di applicare questo metodo per trovare la formula per il termine ennesimo.
Vi avvertiamo però che, quando cercate le radici del polinomio, possono capitare situazioni che richiedono ulteriori approfondimenti. Per esempio studiamo il caso di una successione che soddisfa, per $n \geq 2$, la legge

$$b_n = 4b_{n-1} - 4b_{n-2}$$

con le condizioni iniziali

$$b_0 = 5 \quad b_1 = 7.$$

Il polinomio associato è $x^2 - 4x + 4$ che è $(x-2)^2$ ossia ha come radice 2 "ripetuta due volte" (detto meglio: con molteplicità due). Questo è dunque un caso che prima non avevamo trattato: qui le successioni che si usano sono $\{2^n\}$ e la sua "derivata" $\{n2^{n-1}\}$. Le successioni del tipo

$$a\ 2^n + b\ n2^{n-1}$$

con a, b numeri reali qualsiasi soddisfano tutte la legge ricorsiva data. Facendo il sistema di due equazioni per imporre che valgano le due condizioni iniziali si trova che la formula per la successione b_n è, per ogni $n \geq 0$:

$$b_n = 5 \cdot\ 2^n - 3 \cdot\ n2^{n-1}$$

Certamente, durante l'applicazione di questo metodo, può sorgere una difficoltà, ossia può risultare molto difficile trovare le radici in $\mathbb{C}$ del polinomio associato alla successione. A questo non c'è rimedio, visto che in generale il problema di trovare radici di polinomi è molto difficile; possiamo però garantirvi che negli esercizi che vi proporremo di svolgere in questo corso i polinomi saranno sempre "alla portata".

Per quello che riguarda il sistema finale che mette in gioco le condizioni iniziali, c'è una buona notizia, perché, come imparerete nel corso di Geometria 1, quel tipo di sistemi ha sempre una unica soluzione (la matrice che descrive il sistema è una *matrice di Vandermonde*).

4. L'algoritmo di Euclide e l'identità di Bézout

Denotiamo con $\mathbb{Z}$ l'insieme dei numeri *interi*, ossia $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

Dati due interi $a, b \in \mathbb{Z}$, diciamo che a *divide* b se esiste $c \in \mathbb{Z}$ tale che $b = ac$. Ad esempio -7 divide 35, infatti $(-7)(-5) = 35$. In futuro useremo spesso la notazione $a \mid b$ per dire "a divide b".

Osserviamo che ogni $a \in \mathbb{Z}$ divide 0, visto che abbiamo sempre $0 = a \cdot 0$. Mentre per $b \in \mathbb{Z}$, $b \neq 0$, abbiamo solo un numero finito di divisori di b: infatti se d divide b, allora $d \leq |b|$. Inoltre, si verifica immediatamente che se d divide b, allora è anche vero che $-d$ divide b, d divide $-b$, e $-d$ divide $-b$.

Dunque, dati due interi $a, b \in \mathbb{Z}$ non entrambi nulli, ossia[3] $(a, b) \neq (0, 0)$, è chiaro che l'insieme dei divisori comuni di a e b è un insieme finito. Inoltre, chiaramente 1 è un divisore comune di a e b, quindi, per le osservazioni precedenti, sappiamo che il *massimo comun divisore* di a e b, denotato con $MCD(a, b)$, è un intero positivo minore o uguale al massimo tra $|a|$ e $|b|$ (non al minimo, ad esempio $MCD(10, 0) = 10$). Dati due interi $a, b \in \mathbb{Z}$ non entrambi nulli, usando la fattorizzazione in fattori primi di a e b (la cui esistenza andrebbe dimostrata), non è difficile calcolare $MCD(a, b)$. Putroppo calcolare la fattorizzazione in fattori primi di un intero è un problema molto difficile computazionalmente (addirittura questa difficoltà è alla base dei sistemi di sicurezza delle carte di credito).

L'*algoritmo di Euclide*, che ci accingiamo a spiegare, permette di calcolare il massimo comun divisore di due interi non entrambi nulli senza passare per la loro fattorizzazione in fattori primi, e risulta essere molto efficiente. Questo algoritmo è basato sulla *divisione con resto* degli interi, detta anche *divisione euclidea*.

Dati due interi $a, b \in \mathbb{Z}$ con $b \neq 0$, esiste un unico $q \in \mathbb{Z}$ tale che[4] $r := a - qb$ soddisfa $0 \leq r < |b|$. Questo si vede immediatamente denotando i multipli di b sulla retta dei reali, e osservando che ogni $a \in \mathbb{Z}$ ha alla sua sinistra un multiplo qb a distanza minore o uguale a $|b| - 1$.

Chiamiamo q il *quoziente* e r il *resto* della divisione (euclidea) di a per b. Notiamo che il resto r è uguale a 0 esattamente quando b divide a.

Ad esempio, se $a = 124$ e $b = -17$, allora quoziente e resto della divisione di a per b sono $q = -7$ e $r = 5$ rispettivamente, in quanto

$$124 = (-7)(-17) + 5 \quad \text{e} \quad 0 \leq 5 < |-17| = 17.$$

Siamo ora pronti a descrivere l'*algoritmo di Euclide* per il massimo comun divisore di interi.

Dati due interi $r_{-1} := a$ e $r_0 := b \neq 0$, siano q_1 e r_1 gli unici interi tali che

$$r_{-1} = q_1 r_0 + r_1 \quad \text{con} \quad 0 \leq r_1 < |r_0|.$$

Se $r_1 = 0$ ci fermiamo. Altrimenti, siano q_2 e r_2 gli unici interi tali che

$$r_0 = q_2 r_1 + r_2 \quad \text{avec } 0 \leq r_2 < |r_1|.$$

Se $r_2 = 0$ ci fermiamo. Altrimenti possiamo iterare, e ottenere in questo modo una successione di interi $q_1, q_2, q_3, \ldots$ e $r_1, r_2, r_3, \ldots$ tali che per ogni $i = 1, 2, 3, \ldots$ si ha

$$r_{i-2} = q_i r_{i-1} + r_i \quad \text{avec } 0 \leq r_i < |r_{i-1}|.$$

Siccome per ogni i si ha $0 \leq r_i < |r_{i-1}|$, questo algoritmo si arresta in un numero finito (in effetti minore o uguale a $|b|$) di passi. Sia k il minimo tale che $r_{k+1} = 0$.

Affermiamo che $|r_k| = MCD(a, b)$.

Infatti, notiamo che ad ogni tappa $r_{i-2} = q_i r_{i-1} + r_i$ dell'algoritmo, ogni divisore comune di r_{i-2} e r_{i-1} deve dividere r_i. Quindi ogni divisore comune di $r_{-1} = a$ e $r_0 = b$ dovrà dividere anche r_k. Viceversa, $r_{k+1} = 0$ implica $r_{k-1} = q_{k+1} r_k$, e quindi r_k divide r_{k-1}. Ma siccome $r_{k-2} = q_k r_{k-1} + r_k$, r_k dovrà dividere anche r_{k-2}. Iterando, ogni $r_{i-2} = q_i r_{i-1} + r_i$ implica che r_k divide r_{i-2}, e quindi dovrà dividere anche $r_{-1} = a$ e $r_0 = b$. Dunque r_k è un divisore comune di a e b, che è diviso da ogni divisore comune di a e b. Quindi necessariamente $|r_k| = MCD(a, b)$ come volevamo.

[3] Denotiamo con (a, b) la coppia ordinata in cui il primo elemento è a e il secondo elemento è b.

[4] Usiamo il simbolo ":=" per indicare che ciò che appare alla sua sinistra è definito da quello che appare alla sua destra.

Esempio 1.2. Siano $a = 124$ e $b = -17$. Allora $q_1 = -7$ e $r_1 = 5$, poichè

$$124 = -7 \cdot (-17) + 5.$$

Ora $q_2 = -4$ e $r_2 = 3$, poichè

$$-17 = -4 \cdot 5 + 3.$$

Allora $q_3 = 1$ e $r_3 = 2$, visto che

$$5 = 1 \cdot 3 + 2.$$

Dunque $q_4 = 1$ e $r_4 = 1$, dato che

$$3 = 1 \cdot 2 + 1.$$

Infine $q_5 = 2$ e $r_5 = 0$, poichè

$$2 = 2 \cdot 1 + 0.$$

Dunque $MCD(124, -17) = 1$.

Andando a ritroso, partendo dall'ultima equazione dell'algoritmo di Euclide, e risalendo fino alla prima, possiamo calcolare esplicitamente due interi y e z tali che

$$ya + zb = MCD(a, b).$$

L'esistenza di questi interi è dunque un utile corollario dell'algoritmo di Euclide, che viene attribuito a Bézout e che enunciamo come teorema.

Teorema 1.3 (detto anche Identità di Bézout o Lemma di Bézout[5]). *Dati due numeri interi a e b con $(a, b) \neq (0, 0)$, esistono due numeri interi y e z tali che*

$$MCD(a, b) = ya + zb$$

Si dice che $MCD(a, b)$ può essere espresso come combinazione lineare a coefficienti interi di a e di b.

Osservazione 1.4. Il teorema dice che esistono y e z tali che $MCD(a, b) = ya + zb$, ma non dice che sono unici. Infatti, come risulterà dalla teoria delle equazioni diofantee lineari, ci sono infinite scelte possibili di una coppia (y, z) tale che $MCD(a, b) = ya + zb$.

Spieghiamo l'algoritmo con l'esempio precedente.

Esempio 1.5. Siano $a = 124$ e $b = -17$. Abbiamo visto esplicitamente l'algoritmo di Euclide in questo caso nell'esempio precedente, che ci ha dato $MCD(124, -17) = 1$.

Per trovare y e z tali che $y \cdot 124 + z \cdot (-17) = 1$ partiamo dalla penultima equazione, che dà

$$1 = 3 - 1 \cdot 2.$$

Ma adesso l'equazione precedente dà

$$2 = 5 - 1 \cdot 3$$

e quindi

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5.$$

Ora l'equazione precedente dà

$$3 = -17 - (-4 \cdot 5),$$

dunque otteniamo

$$1 = 2 \cdot (-17 - (-4 \cdot 5)) - 1 \cdot 5 = 7 \cdot 5 + 2 \cdot (-17).$$

Ancora una volta, l'equazione precedente dà

$$5 = 124 - (-7 \cdot (-17)),$$

[5]Prende il nome dal matematico francese Etienne Bézout, 1730-1783.

e quindi

$$1 = 7 \cdot (124 - (-7 \cdot (-17))) + 2 \cdot (-17) = 7 \cdot 124 + 51 \cdot (-17).$$

Abbiamo dunque trovato $y = 7$ e $z = 51$.

OSSERVAZIONE 1.6. Osserviamo che nell'esempio precedente siamo stati sempre accorti a non semplificare troppo le espressioni, in particolare a non semplificare le occorrenze di a e b e dei resti (ossia gli r_i, in questo caso $124, -17, 5, 3, 2, 1$) dell'algoritmo di Euclide. Facendo i conti precedenti in modo formale, utilizzando le equazioni dell'algoritmo ($r_{i-2} = q_i r_{i-1} + r_i$) si verifica che gli interi y e z del teorema sono polinomi nei quozienti (i q_i, in questo caso $-7, -4, 1, 1, 2$) dell'algoritmo di Euclide, che si calcolano ricorsivamente.

Vediamo una implementazione in SAGE (Sagemath) di tutto ciò che abbiamo visto in questa sezione.

5. Implementazione dell'algoritmo di Euclide per gli interi

Spieghiamo qui una implementazione dell'algoritmo di Euclide per interi positivi. Il caso generale è lasciato come ***esercizio***.

La funzione `floor(x)` de SAGE calcola il più grande intero minore o uguale a `x`. Ad esempio `floor(3/2)` dà 1.

Definiamo la funzione `my_divide_integers` che prende in input due interi `a` e `b` non negativi e restituisce il quoziente e il resto della divisione di `a` per `b`.

```
    # we write a warning message if we try to divide by 0
def my_divide_integers(a,b):
    if b==0:
      out='You cannot divide by 0 !!!'
    else:
      quotient=nsimplify(floor(a/b))
      remainder=nsimplify(a-quotient*b)
      out=[quotient,remainder]
    return out
```

Ad esempio

```
my_divide_integers(13,0)
```

dà

'You cannot divide by 0 !!!',

mentre

```
my_divide_integers(1454,332)
```

dà

[4, 126].

Utilizzando la funzione `my_divide_integers`, definiamo la funzione `my_GCD_for_integers` che calcola il MCD (massimo comun divisore) di due interi non negativi `a` e `b`.

```
    # notice the recursive call of the function my_GCD_for_integers that we are trying
to define
def my_GCD_for_integers(a,b):
    if a==0 and b==0:            # this is in case both a and b are 0
```

```
    out='Both integers are 0 !!!'
  elif b==0:
    out=a
  else:
    qr=my_divide_integers(a,b)
    out=my_GCD_for_integers(b,qr[1]) # recall that in SAGE the positions
                                     # of a list start with 0 !!!
  return out
```

Ad esempio

```
my_GCD_for_integers(15,12)
```

dà

3,

mentre

```
my_GCD_for_integers(36400,43316)
```

dà

364.

Definiamo la funzione `get_integer_quotients` che prende come input due interi positivi `a` e `b` e restituisce la lista dei quozienti dati dall'algoritmo di Euclide.

```
def get_integer_quotients(a,b):
  aa=a
  bb=b
  qlist=[]
  while bb!=0:
    qr=my_divide_integers(aa,bb)
    qlist.append(qr[0])
    aa=bb
    bb=qr[1]
  return qlist
```

Ad esempio

```
get_integer_quotients(3,4)
```

dà

[0, 1, 3]

mentre

```
get_integer_quotients(21,6)
```

dà

[3, 2].

Definiamo la funzione `quotients_to_yz` che prende come input la lista dei quozienti data dall'algoritmo di Euclide applicato a due interi positivi `a` e `b` e restituisce due interi `y` e `z` tali che `ya+zb` è il MCD di `a` e `b`.

```
def quotients_to_yz(qlist):
  k=len(qlist)
  if k==1:
    out=[0,1]
```

```
  if k==2:
    out=[1,-qlist[0]]
  if k>2:
    ax,bx=symbols('ax,bx')      # here we define two global variables ax and bx
    pout=bx-qlist[1]*(ax-bx*qlist[0]) # this is the base case. We use the
                                      # global variables ax and bx
                                      # in place of the integers a and b
    auxrlist=[ax-bx*qlist[0],bx-qlist[1]*(ax-bx*qlist[0])]
    for j in range(k-3):
      pout=auxrlist[0]-qlist[j+2]*auxrlist[1]
      auxrlist[0]=auxrlist[1]
      auxrlist[1]=pout
    out=[pout.coefficient(ax,1),pout.coefficient(bx,1)]
    del(ax,bx)                  # here we unassign ax and bx
  return out
```

Ad esempio

```
qq=get_integer_quotients(123,24)
qq
```

dà

[5, 8]

e quindi

```
quotients_to_yz(qq)
```

dà

[1, −5]

Osserviamo che, utilizzando `reset` nella funzione, abbiamo lasciato `ax` e `bx` non assegnati.

Definiamo la funzione `my_integer_Euclid_theorem` che prende come input due interi non negativi `a` e `b` e che restituisce due interi `y` e `z` tali che `ya+zb` è uguale al MCD di `a` e `b`.

```
def my_integer_Euclid_theorem(a,b):
  if a==0 and b==0:
    out='The two integers are both 0 !!!'
  elif b==0:
    out=[1,0]
  else:
    qlist=get_integer_quotients(a,b)
    out=quotients_to_yz(qlist)
  return out
```

Ad esempio,

```
my_integer_Euclid_theorem(0,0)
```

dà

'The two integers are both 0 !!!'

mentre

```
my_integer_Euclid_theorem(123,24)
```

dà

$$[1,\ -5].$$

6. Il principio di induzione

Alcune argomentazioni che abbiamo utilizzato nei paragrafi precedenti possono essere espresse in maniera più formale utilizzando il principio di induzione. Di cosa si tratta? Innanzitutto 'in gioco' c'è un *predicato* $P(n)$, ossia una frase che contiene il simbolo n, da intendersi come variabile che 'varia' - appunto - fra i numeri naturali. Ma non una frase qualunque: per poterla chiamare *predicato* bisogna che, ogni volta che sostituiamo alla n un preciso numero naturale (per esempio $n = 6$), diventi una *proposizione*, ovvero una frase di cui ha senso dire se sia vera o falsa.

Esempio 1.7. Per esempio sono predicati

$P_1(n)$: 'la somma dei primi n numeri interi positivi è $\frac{n(n+1)}{2}$ '
$P_2(n)$: 'in un poligono regolare con n lati posso tracciare al massimo $n-3$ diagonali che non si intersecano o si intersecano solo nei vertici'
$P_3(n)$: ' $2^n > n^2 + 3n + 1$ '
$P_4(n)$: 'se ho due colori, rosso e blu, e voglio colorare i numeri dell'insieme $\{1, 2, \ldots, n\}$, posso farlo in 2^n modi diversi'
$P_5(n)$: 'Consideriamo n (con $n \geq 2$) punti dati su una circonferenza in modo che i segmenti che li congiungono due a due siano in 'posizione generale', ovvero che all'interno del cerchio non ci sia nessun punto in cui si intersecano tre (o più) di essi. Allora questi segmenti suddividono l'interno del cerchio in 2^{n-1} regioni'
$P_6(n)$: 'n è un numero pari'

mentre *non* sono predicati

$Q_1(n)$: 'quando piove n gatti'
$Q_2(n)$: 'n è maggiore di x' (con x che resta un simbolo non specificato) .

Osservazione 1.8. Sottolineiamo che $P_3(n)$ e $P_6(n)$ sono predicati, anche se per esempio le proposizioni $P_3(0)$ e $P_6(5)$ sono false. Attenzione al predicato $P_5(n)$: si verifica facilmente che $P_5(2)$,$P_5(3)$,$P_5(4)$, $P_5(5)$ sono proposizioni vere, mentre $P_5(6)$ è falsa e così le successive...

Supponiamo di voler dimostrare che, per ogni numero naturale m maggiore o uguale di un certo numero naturale n_0 fissato, la proposizione $P(m)$ è vera. Il principio di induzione ci offre la possibilità di farlo in due passi:

- Primo passo (o *passo base*): controlliamo la 'base dell'induzione', ossia verifichiamo che $P(n_0)$ sia vera;
- Secondo passo (o *passo induttivo*): dimostriamo che, se per un qualsiasi $k \geq n_0$ la $P(k)$ è vera, allora è vera anche la 'successiva', ossia la $P(k+1)$.

A questo punto l'intuizione ci dice che, comunque prendiamo un numero naturale m maggiore o uguale a n_0, la $P(m)$ è vera. Infatti:

$P(n_0)$ è vera perché è stato verificato come base dell'induzione;
siccome è vera $P(n_0)$ allora è vera $P(n_0+1)$ (per il passo induttivo);
siccome è vera $P(n_0+1)$ allora è vera $P(n_0+2)$ (per il passo induttivo);
siccome è vera $P(n_0+2)$ allora è vera $P(n_0+3)$ (per il passo induttivo);
siccome è vera $P(n_0+3)$ allora è vera $P(n_0+4)$ (per il passo induttivo);

... e così via, fino a raggiungere in un numero finito di passi la $P(m)$ desiderata.

Le dimostrazioni per induzione sono proprio la formalizzazione di quel '... e così via' che, senza ulteriore attenta considerazione, è molto insidioso.
Proviamo ad esprimere in modo più preciso (pur lasciando a livello intuitivo la definizione di 'predicato') il ragionamento che abbiamo appena descritto:

Il principio di induzione.
Supponiamo che $P(n)$ sia un predicato che dipende da un numero naturale $n \in \mathbb{N}$. Se, dato un numero naturale n_0, vale che:

(1) *$P(n_0)$ è vera* (base dell'induzione)*;*
(2) *preso un qualsiasi $k \geq n_0$, se è vera la $P(k)$ allora è vera anche la $P(k+1)$* (passo induttivo - la $P(k)$ si chiama ipotesi induttiva)*;*

allora possiamo concludere che: 'P(m) è vera per ogni $m \geq n_0$'.

Come potete notare, nell'enunciare il principio di induzione non abbiamo premesso la voce 'Teorema', o 'Proposizione'. Per noi è come un assioma, ossia un fatto la cui validità sta alla base di tutti i nostri ragionamenti. In effetti il principio di induzione è legato all'esistenza dei numeri naturali, e lo accettiamo così come accettiamo i numeri naturali. Approfondirete questi temi più avanti negli esami di logica matematica.

Esempio 1.9. A titolo di esempio, dimostriamo per induzione la validità di $P_1(n)$ per ogni numero naturale positivo (non è l'unico modo in cui si potrebbe dimostrare, ne avrete di sicuro già visti altri). Ovvero, dimostriamo per induzione che, per ogni numero naturale positivo n, la somma dei numeri interi maggiori o uguali a 1 e minori o uguali a n è $\frac{n(n+1)}{2}$:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2},$$

dove abbiamo utilizzato il simbolo di sommatoria.[6]
(1) *Base dell'induzione.* Per prima cosa si verifica che per $n = 1$ l'affermazione è vera. Infatti

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}.$$

(2) *Passo induttivo.* Supponiamo di sapere che, per un certo intero $k \geq 1$, valga $P_1(k)$, ovvero che:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$

Usando questa ipotesi (l''ipotesi induttiva') vogliamo dimostrare $P(k+1)$:

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}.$$

[6]In generale, dati dei numeri $a_1, a_2, \ldots, a_n$, il simbolo $\sum_{i=1}^{n} a_i$, 'somma per i che varia fra 1 ed n di a_i', è un modo per scrivere $a_1 + a_2 + \cdots + a_n$. Il lettore lo incontrerà altre volte in questo volume.

Procediamo; scriviamo $\sum_{i=1}^{k+1} i$ spezzando la somma così:

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1).$$

Ma l'ipotesi induttiva ci permette di scrivere, al posto di $\left(\sum_{i=1}^{k} i\right)$, il numero $\frac{k(k+1)}{2}$. Dunque otteniamo

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + k + 1$$

che, riorganizzando il secondo membro, è proprio

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

come volevamo. La dimostrazione per induzione è conclusa.

Esempio 1.10. Consideriamo ora il predicato $P_3(n)$ definito all'inizio. Determiniamo per quali numeri naturali n si ha che $P_3(n)$ è vera, ossia per quali n vale $2^n > n^2 + 3n + 1$.

Con dei tentativi scopriamo subito che la disuguaglianza non è vera per $n = 0, 1, 2, 3, 4, 5$, mentre è vera per $n = 6$ in quanto $2^6 = 64 > 6^2 + 3 \cdot 6 + 1 = 55$. Si verifica inoltre che è vera anche per $n = 7, 8, 9$ e che la differenza fra il membro di sinistra e quello di destra della disuguglianza è sempre più grande. Siamo allora portati a sospettare che la disuguaglianza valga per ogni $n \geq 6$.

Proviamo allora a dimostrare per induzione che:

$$\textit{per ogni } n \geq 6 \textit{ vale } 2^n > n^2 + 3n + 1.$$

La base dell'induzione, ossia il caso $n = 6$, è stata già verificata.
Per compiere il passo induttivo sia ora k un intero maggiore o uguale a 6. Supponiamo di sapere che (ipotesi induttiva):

$$2^k > k^2 + 3k + 1$$

e mostriamo che da questo si può ottenere:

$$2^{k+1} > (k+1)^2 + 3(k+1) + 1.$$

Innanzitutto osserviamo che $2^{k+1} = 2 \cdot 2^k$ e allora, usando l'ipotesi induttiva, possiamo scrivere:

$$2^{k+1} = 2 \cdot 2^k > 2(k^2 + 3k + 1).$$

A questo punto ci rendiamo conto che se è vera la disuguaglianza:

$$2(k^2 + 3k + 1) > (k+1)^2 + 3(k+1) + 1$$

abbiamo finito perché abbiamo la catena di disuguaglianze:

$$2^{k+1} = 2 \cdot 2^k > 2(k^2 + 3k + 1) > (k+1)^2 + 3(k+1) + 1.$$

Mostriamo dunque che

$$2(k^2 + 3k + 1) > (k+1)^2 + 3(k+1) + 1.$$

Con qualche calcolo si nota che ciò equivale a

$$2k^2 + 6k + 2 > k^2 + 2k + 1 + 3k + 3 + 1 = k^2 + 5k + 5$$

che, semplificando ancora, diventa:

$$k^2 + k > 3.$$

Visto che stiamo considerando i valori k maggiori o uguali a 6 quest'ultima disuguaglianza è vera (infatti $k^2 + k \geq k \geq 6 > 3$).

ESEMPIO 1.11. Dato un numero intero positivo n, la somma dei primi n numeri dispari è n^2.

SOLUZIONE: Diamo tre dimostrazioni.

La prima si riferisce alla Figura 1. La accenniamo senza scriverla in modo troppo formale: un quadrato di lato n e di area n^2 può essere ottenuto sommando n "cornici" di area dispari, precisamente di area $1, 3, 5, \ldots, 2n - 1$. Potete provare a scriverla in modo formale per induzione.

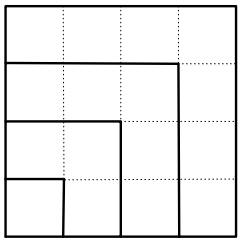

FIGURA 1. Il quadrato di lato 4 e area 4^2 si ottiene sommando "cornici" e quindi la sua area si può calcolare anche con la somma dei primi 4 numeri dispari: $1 + 3 + 5 + 7$.

Proponiamo anche una dimostrazione per induzione scritta più formalmente, che prevede la manipolazione di sommatorie. Come predicato $P(n)$ scegliamo

$$P(n) : \sum_{i=0}^{n-1}(2i + 1) = n^2.$$

BASE. Si verifica subito che $P(1)$ è vera visto che si traduce nell'uguaglianza $1 = 1$.

PASSO INDUTTIVO. Sia $k \geq 1$ un intero. Dobbiamo dimostrare che è vera l'implicazione[7]:

$$\sum_{i=0}^{k-1}(2i + 1) = k^2 \Rightarrow \sum_{i=0}^{k}(2i + 1) = (k + 1)^2.$$

Procediamo; scriviamo $\sum_{i=0}^{k}(2i + 1)$ spezzando la somma così:

$$\sum_{i=0}^{k}(2i + 1) = \left(\sum_{i=0}^{k-1}(2i + 1)\right) + (2k + 1).$$

Ma l'ipotesi induttiva ci permette di scrivere, al posto di $\left(\sum_{i=0}^{k-1}(2i + 1)\right)$, il suo valore k^2. Dunque otteniamo

$$\sum_{i=0}^{k}(2i + 1) = k^2 + 2k + 1$$

[7]Il simbolo "⇒" si usa per indicare che quello appare alla sua sinistra "implica" quello che appare alla sua destra.

che, riorganizzando il secondo membro, è proprio

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2$$

come volevamo.

Dimostriamo infine la formula ancora in un terzo modo. Possiamo esprimere la somma dei primi n numeri dispari con la sommatoria $\sum_{i=1}^{n}(2i-1)$. Alcuni passaggi algebrici ci permettono di scrivere:

$$\sum_{i=1}^{n}(2i-1) = 2\left(\sum_{i=1}^{n} i\right) + \sum_{i=1}^{n}(-1).$$

A questo punto conosciamo entrambe le sommatorie che compaiono nel membro di destra: la prima è uguale (vedi esercizio precedente) a $2\dfrac{n(n+1)}{2}$, la seconda a $-n$. Dunque abbiamo ottenuto che

$$\sum_{i=1}^{n}(2i-1) = n(n+1) - n = n^2.$$

□

Generalizziamo:

Esempio 1.12. Diremo che una successione di numeri reali $a_0, a_1, \ldots, a_n$ è una *progressione aritmetica* se le differenze $a_i - a_{i-1}$ sono tutte uguali fra loro (diciamo che siano tutte uguali al numero a). In generale una progressione aritmetica si può scrivere dicendo che, per ogni $i \in \mathbb{N}$, $a_i = ai + b$ per certi numeri reali fissati a e b.

Quanto vale $\sum_{i=0}^{n}(ai+b)$? Possiamo scrivere

$$\sum_{i=0}^{n}(ai+b) = a\left(\sum_{i=0}^{n} i\right) - \sum_{i=0}^{n} b = a\frac{n(n+1)}{2} - (n+1)b.$$

Occupiamoci ora di un altro tipo di successioni, le *progressioni geometriche*. Cominciamo con questo esercizio:

Esercizio 1.13. Dimostrare che, per ogni $n \in \mathbb{N}$,

$$\sum_{i=0}^{n} 1/2^i = 2 - 1/2^n$$

Soluzione: Possiamo procedere per induzione, scegliendo il predicato

$$P(n) : \sum_{i=0}^{n} 1/2^i = 2 - 1/2^n.$$

La base dell'induzione si riduce alla seguente verifica: $1 = 2 - 1/2^0$. Il passo induttivo richiede, assumendo vero $\sum_{i=0}^{k} 1/2^i = 2 - 1/2^k$, di dimostrare che $\sum_{i=0}^{k+1} 1/2^i = 2 - 1/2^{k+1}$. Possiamo scrivere:

$$\sum_{i=0}^{k+1} 1/2^i = \left(\sum_{i=0}^{k} 1/2^i\right) + 1/2^{k+1}.$$

A questo punto, usando l'ipotesi induttiva, otteniamo

$$\sum_{i=0}^{k+1} 1/2^i = 2 - 1/2^k + 1/2^{k+1}.$$

Visto che $-1/2^k + 1/2^{k+1} = -1/2^{k+1}$ abbiamo trovato l'uguaglianza desiderata[8]. □

ESEMPIO 1.14. Diremo che una successione di numeri reali non nulli $b_0, b_1, \ldots, b_n$ è una *progressione geometrica* se i rapporti $\frac{b_i}{b_{i-1}}$ sono tutti uguali fra loro (diciamo che siano tutte uguali al numero k). In generale una progressione geometrica si può scrivere dicendo che, per ogni $i \in \mathbb{N}$, $b_i = ck^i$ per certi numeri reali non nulli fissati c e k.

Quanto vale $\sum_{i=0}^{n} ck^i$? Possiamo rispondere osservando che $\sum_{i=0}^{n} ck^i = c\sum_{i=0}^{n} k^i$. Se $k = 1$ allora la progressione geometrica è in realtà una successione costante, e la somma vale $ck(n+1)$. Se invece $k \neq 1$, possiamo partire calcolando

$$(1 + k + k^2 + \ldots + k^n)(k - 1).$$

Svolgendo i calcoli si vede che molti termini si cancellano e rimane $k^{n+1} - 1$. Quindi vale:

$$1 + k + k^2 + \ldots + k^n = \frac{k^{n+1} - 1}{k - 1}$$

e possiamo concludere che

$$\sum_{i=0}^{n} ck^i = c\frac{k^{n+1} - 1}{k - 1}.$$

7. Forme equivalenti del principio di induzione: il principio del minimo e il principio di induzione forte

Ci sono altri due modi con cui si può enunciare il principio di induzione: l'assioma del buon ordinamento (detto anche "principio del minimo") e il principio di induzione "forte". Anche se a prima vista non sembrerebbe, si può in realtà dimostrare che il principio di induzione, il principio di induzione forte e l'assioma del buon ordinamento sono equivalenti. Come conseguenza pratica, questo vuol dire che se un problema si può risolvere usando uno di questi tre assiomi, allora c'è sicuramente il modo di risolverlo anche usando uno qualunque degli altri due.

Il principio di induzione forte.
Supponiamo che $P(n)$ sia un predicato che dipende da un numero naturale $n \in \mathbb{N}$. Se, dato un numero naturale n_0, vale che:

- $P(n_0)$ è vera (*questa si chiama BASE dell'induzione*);
- per ogni intero $k \geq n_0$, è vera l'implicazione[9]

  $$(P(n_0) \wedge P(n_0 + 1) \wedge \cdots \wedge P(k)) \Rightarrow P(k + 1)$$

  (*questo si chiama PASSO INDUTTIVO e la* $P(n_0) \wedge P(n_0 + 1) \wedge \cdots \wedge P(k)$ *si chiama IPOTESI INDUTTIVA*);

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

Osserviamo che, in questo caso, la base dell'induzione è la stessa del "normale" principio di induzione, ma il passo induttivo è diverso. Nell'induzione normale, si deve dimostrare che, per ogni intero $k \geq n_0$, è vera l'implicazione $P(k) \Rightarrow P(k+1)$. Questo si traduce nel tentativo di dimostrare $P(k+1)$ assumendo come vera la $P(k)$. Dunque, nel

[8]La somma che abbiamo appena calcolato richiama il paradosso di Zenone di Elea (si tratta in realtà di una variante del celebre paradosso). Quando ci avviciniamo ad un oggetto possiamo osservare il nostro moto così: percorriamo metà della distanza che ci separa, poi metá della distanza rimanente, e così via... Lo raggiungeremo mai?

[9]Il simbolo "$\wedge$" sta per la congiunzione logica "e".

momento in cui dimostriamo la $P(k+1)$, abbiamo un'arma a nostro vantaggio, ossia la $P(k)$.

Nell'induzione forte, invece, il passo induttivo chiede di dimostrare che, per ogni intero $k \geq n_0$, è vera l'implicazione

$$(P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)) \Rightarrow P(k+1)$$

Questo si traduce come prima nel tentativo di dimostrare la $P(k+1)$, ma stavolta si possono assumere come vere tutte le proposizioni $P(n_0), P(n_0+1), \ldots, P(k)$; dunque nel momento in cui dimostriamo la $P(k+1)$ siamo più "forti" (ecco perché si chiama induzione "forte"), perché abbiamo a nostro vantaggio molte armi, non solo la $P(k)$, che avevamo anche nell'induzione normale, ma anche le altre proposizioni $P(n_0), P(n_0+1), \ldots, P(k-1)$ (*ricordatevi però che siamo più forti solo apparentemente, perché in realtà l'induzione forte è equivalente all'induzione semplice*).

Esempio 1.15. Dimostrare usando l'induzione forte che ogni numero intero maggiore o uguale a 2 o è *primo* (ossia gli unici divisori positivi sono 1 e se stesso) oppure si può scrivere come prodotto di numeri primi [10].

Consideriamo il predicato $P(n)$:"il numero n o è primo o si può scrivere come prodotto di numeri primi".

La base, ossia la dimostrazione di $P(2)$, è immediata, perché 2 è appunto un numero primo.
Adesso occupiamoci del passo induttivo. Supponiamo (induzione forte!) che siano vere tutte le proposizioni $P(j)$ con $2 \leq j \leq k$ e cerchiamo di dimostrare che è vera $P(k+1)$, ossia dobbiamo dimostrare che: "il numero $k+1$ o è primo o si può scrivere come prodotto di numeri primi".

Ora si possono verificare due casi: o $k+1$ è primo, e in tal caso la dimostrazione del passo induttivo è già finita, oppure $k+1$ non è primo. In questo secondo caso, allora $k+1$ è *composto*, ossia si può scrivere come prodotto di due numeri a e b, $k+1 = ab$, dove $1 < a < k+1$, e quindi $1 < b < k+1$. Dunque a e b sono tali che le proposizioni $P(a)$ e $P(b)$ risultano vere per ipotesi induttiva, garantendoci che a e b o sono primi o si possono scrivere come prodotto di numeri primi. Di conseguenza $k+1 = ab$ si scrive come prodotto di numeri primi (quelli della decomposizione di a per quelli della decomposizione di $b\ldots$).

Osservazione 1.16. Per dimostrare questa stessa proposizione usando l'induzione semplice, basta cambiare il predicato, quello giusto è $T(n)$:"ogni numero intero maggiore o uguale a 2 e minore o uguale a n è o primo o prodotto di primi". Provate a completare la dimostrazione, che è simile alla precedente....

Quando abbiamo introdotto il principio di induzione abbiamo detto che è legato alla esistenza dei numeri naturali. Questo viene messo particolarmente in luce se enunciamo il principio di induzione in questa forma:

Assioma del buon ordinamento (chiamato anche "Principio del minimo").
Ogni sottoinsieme NON VUOTO di $\mathbb{N}$ ha un elemento minimo.

Vedremo più avanti in questo corso alcune dimostrazioni in cui risulta naturale applicare l'induzione nella forma data dall'assioma del buon ordinamento. Per il momento

[10] Approfondiremo più avanti in un paragrafo apposito

torniamo all'esempio precedente e vediamo come il principio del minimo possa essere usato per dare una variante della dimostrazione.

ESEMPIO 1.17. Dimostrare usando il principio del minimo che ogni numero intero maggiore o uguale 2 o è primo o è prodotto di numeri primi.

Consideriamo il predicato $P(n)$: "il numero n o è primo o è prodotto di numeri primi" e sia S l'insieme dei numeri interi $m \geq 2$ tali che la proposizione $P(m)$ è falsa.

Osserviamo che dimostrare l'enunciato equivale a dimostrare che S è vuoto. Procediamo per assurdo e supponiamo dunque per assurdo che S non sia vuoto. Allora S, che è un sottoinsieme non vuoto di $\mathbb{N}$, per il principio del minimo ha un elemento minimo, che chiamiamo s.

Riassumendo, cosa sappiamo di s? Sappiamo che è un intero maggiore o uguale a 2 tale che $P(s)$ è falsa, ossia che non è né primo né prodotto di primi, e che è il più piccolo numero con queste caratteristiche.

In particolare, non essendo primo si potrà scrivere come prodotto di due numeri a e b, $s = ab$, dove $1 < a < s$, e quindi $1 < b < s$. Dunque a e b, essendo maggiori o uguali a 2 e strettamente minori di s sono tali che le proposizioni $P(a)$ e $P(b)$ sono vere (altrimenti sarebbe uno di loro, e non s, il minimo dell'insieme S..). Questo vuol dire che a e b sono o primi o prodotto di primi e ci permette di ottenere una decomposizione in primi di s. Abbiamo ottenuto un assurdo, perché s per costruzione non può ammettere una decomposizione in primi.

Siccome aver assunto che S sia diverso dall'insieme vuoto ci ha portati ad un assurdo, abbiamo dunque dimostrato che[11] $S = \varnothing$ come volevamo.

8. Qualche esercizio...

ESERCIZIO 1.18. Utilizzare il principio di induzione (o induzione forte, o principio del minimo, a vostra scelta) per dimostrare più formalmente il Teorema 1.1 e il Teorema 1.3 (ossia riscrivete per bene quello che abbiamo detto in classe).

ESERCIZIO 1.19. Sia $(u_n)_{n\in\mathbb{N}}$ la successione così definita:

$$\begin{aligned} u_0 &= 0 \\ u_{k+1} &= 3u_k + 3^k \quad \text{per } k \in \mathbb{N}. \end{aligned}$$

Dimostrare che $u_k = k3^{k-1}$ per ogni $k \in \mathbb{N}$. [Osservazione: la successione proposta non è "lineare a coefficienti costanti" dunque non si applica il metodo descritto nei paragrafi precedenti.]

ESERCIZIO 1.20. Definiamo per ricorrenza $a_0 = 0, a_1 = 12$ e $a_{n+2} = 6a_{n+1} - 9a_n$ per ogni $n \in \mathbb{N}$. Trovare una formula per a_n.

ESERCIZIO 1.21. Consideriamo la successione definita per ricorrenza da $a_0 = 8, a_1 = -1$ e, per ogni numero intero $n \geq 2$, dalla regola:

$$a_n = -a_{n-1} + 2a_{n-2}$$

Trovare un formula per a_n.

ESERCIZIO 1.22. Si definisca una successione tramite la regola $a_0 = 2, a_1 = 1$ e, per ogni $n \geq 1$, $a_{n+1} = a_n + 6a_{n-1}$. Si trovi una formula per il termine a_n.

[11] Il simbolo $\varnothing$ denota l'insieme vuoto.

Esercizio 1.23. Si consideri la successione data da $a_0 = 1$ e $a_{n+1} = 2a_n + 3$ per ogni $n \in \mathbb{N}$.
a) Si dimostri che, per ogni $n \geq 1$, 2^n divide $a_n + 3$.
b) Si trovi una formula per a_n. [Osservazione: la successione proposta non è lineare.]

Esercizio 1.24. Si consideri la successione data da $a_0 = 1$, $a_1 = 1$ e $a_n = a_{n-2} + n$ per $n \geq 2$.
a) Trovare, motivando la risposta, il più piccolo numero $n_0 \in \mathbb{N}$ tale che, per ogni $n \geq n_0$, vale $a_n \geq 2n$.
b) Trovare una formula per a_n.

Esercizio 1.25. Sia a_n una successione di numeri interi tale che $a_0 = 1$, $a_{n+1} \geq 2a_n$ se n è pari, e $a_{n+1} \geq 3a_n$ se n è dispari. Dimostrare che per ogni $n \in \mathbb{N}$, $a_{2n} \geq 6^n$.

Esercizio 1.26. Dato $n \in \mathbb{N} - \{0\}$, sia ST_n il numero di tutte le possibili stringhe (cioè liste ordinate) di cifre binarie (ossia 0 e 1) che hanno le seguenti caratteristiche:

- hanno lunghezza n
- se $n = 1$ la stringa è 0, se $n \geq 2$ la stringa comincia per 01
- non ci sono mai tre cifre uguali consecutive.

Per esempio $ST_5 = 5$ e le stringhe in questione sono 01001, 01010, 01011, 01100, 01101. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$, $ST_n = F_n$.

Esercizio 1.27. Una lista di numeri interi strettamente crescente si dice *di parità alterna* se inizia con un numero dispari, ha come secondo termine un numero pari, poi il terzo termine è dispari, il quarto è pari, e così via. La lista vuota viene considerata anch'essa una lista di parità alterna. Sia $LP(n)$ il numero delle liste di parità alterna i cui termini costituiscono un sottoinsieme di $\{1, 2, \ldots, n\}$. Che relazione c'è fra le successioni $\{LP_n\}$ e $\{F_n\}$?

Esercizio 1.28. Provare che per i numeri di Fibonacci F_n ($n \geq 0$) vale la seguente formula:

$$F_{n+4} = F_3 F_n + F_4 F_{n+1}$$

Esercizio 1.29. Provare che per i numeri di Fibonacci F_n vale la seguente formula ($n \geq 0$ e $m \geq 1$):

$$F_{n+m} = F_{m-1} F_n + F_m F_{n+1}$$

Esercizio 1.30. Provare che per i numeri di Fibonacci si ha che F_n divide F_{mn} ($n \geq 1$, $m \geq 0$).

Esercizio 1.31. Provare che per i numeri di Fibonacci si ha che $F_{n+4} \geq n^2$ per $n \geq 0$.

Esercizio 1.32. Introduciamo i numeri di Lucas[12], definiti così: $L_0 = 2$, $L_1 = 1$ e, per ogni n intero ≥ 2, $L_n = L_{n-1} + L_{n-2}$.
È vero o falso che, per ogni $n \geq 1$, vale $L_n = F_{n-1} + F_{n+1}$?
È vero o falso che, per ogni $n \geq 1$, vale $F_{2n-1}^2 = F_n^2 + F_{n-1}^2$?
È vero o falso che, per ogni $n \geq 1$, vale $L_{2n-1}^2 = L_n^2 + L_{n-1}^2$?

Esercizio 1.33. Data la successione $(a_n)_{n \in \mathbb{N}}$ definita da $a_0 = 1$,

$$a_n = 1 + a_0 + a_1 + \cdots + a_{n-1} \qquad \forall n \geq 1$$

trovare una formula per a_n.

[12] Édouard Lucas, matematico francese, 1842-1891.

Trovare una formula per la successione $(b_n)_{n\in\mathbb{N}}$ definita da $b_0 = 1$,

$$b_n = 1 - b_0 + b_1 - b_2 + \cdots + (-1)^n b_{n-1} \qquad \forall n \geq 1.$$

[Osservazione: le successioni proposte non sono lineari.]

Esercizio 1.34. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$ vale:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Esercizio 1.35. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$ vale:

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Esercizio 1.36. Dimostrare per induzione la seguente formula per la somma dei cubi dei primi n numeri pari positivi:

$$\sum_{k=1}^{n} (2k)^3 = 2n^2(n+1)^2.$$

Esercizio 1.37. Dimostrare che per ogni $n \geq 1$ si ha

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}.$$

Esercizio 1.38. Sia $H_k = \sum_{1=1}^{k} \frac{1}{i}$. Si dimostri che $H_{2^n} \geq 1 + \frac{n}{2}$ per ogni $n \in \mathbb{N}$.

Esercizio 1.39. Dimostrare che per ogni intero $n \geq 1$ vale:

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}.$$

Esercizio 1.40. Dimostrare che, per ogni n intero positivo, esistono almeno n numeri primi distinti che dividono il numero $2^{2^n} - 1$.[Suggerimento: $2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$.]

Esercizio 1.41. Consideriamo la formula

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{an + b}{cn}.$$

Proporre dei valori $a, b, c \in \mathbb{Z}$ per cui questa formula è vera per ogni $n \geq 2$ e dimostrare in tale caso la formula per induzione. La scelta di tali valori è unica? Il numero $\frac{a}{c}$ è univocamente determinato?

Esercizio 1.42. Dimostrare per induzione che per ogni intero $n \geq 14$ esistono interi non negativi $x, y \in \mathbb{N}$ tali che $n = 3x + 8y$.

Esercizio 1.43. Trovare, motivando la risposta, il più piccolo numero $n_0 \in \mathbb{N}$ tale che, per ogni $n \geq n_0$, valga

$$4^n \geq n^2 + 5n + 1.$$

Esercizio 1.44 (Disuguaglianza di Bernoulli). Dimostrare che, per ogni $n \in \mathbb{N}$ e per ogni numero reale $x > -1$ vale

$$(1 + x)^n \geq 1 + nx.$$

Esercizio 1.45. Da un fagiolo magico germoglia una piantina alta un centimetro, che ogni giorno cresce di 1/30 della sua altezza. Dimostrare che dopo un anno la piantina avrà superato i 40 metri di altezza.

Esercizio 1.46. Togliamo una casella da una scacchiera di $2^n \times 2^n$ caselle. Dimostrare che è possibile ricoprire la parte rimanente con tessere tutte uguali fatte a "L" che ricoprono 3 caselle.

Esercizio 1.47. Sia n in intero positivo. Su un circuito ci sono n automobili uguali fra loro, disposte (ferme) in n punti distinti. La somma di tutto il carburante che possiedono è tale che ognuna di loro, se lo possedesse, potrebbe percorrere l'intero circuito. È vero o falso che esiste una macchina che, partendo dalla sua posizione, e prendendo il carburante delle macchine che di volta in volta raggiunge, è in grado di percorrere tutto il circuito?

CAPITOLO 2

Congruenze

Ricordiamo la notazione $a \mid b$ per dire "a divide b".

1. Due osservazioni preliminari

Se dividiamo due numeri per il loro massimo comun divisore, i due quozienti ottenuti sono primi fra loro, ossia non hanno divisori comuni strettamente maggiori di 1:

PROPOSIZIONE 2.1. *Presi due numeri interi a e b non entrambi nulli, se li dividiamo per il loro massimo comun divisore $MCD(a,b)$ otteniamo due numeri*

$$a' = \frac{a}{MCD(a,b)} \qquad b' = \frac{b}{MCD(a,b)}$$

che sono primi fra loro.

DIMOSTRAZIONE. Si può vedere in due modi, entrambi molto semplici. Il primo modo è il seguente: se ci fosse un divisore comune $d > 1$ di a' e b', allora $d \cdot MCD(a,b)$ dividerebbe sia a che b, e sarebbe più grande di $MCD(a,b)$, assurdo.

Il secondo modo parte dall'identità di Bézout

$$MCD(a,b) = am + bn.$$

Dividendo per $MCD(a,b)$ si ottiene

$$1 = a'm + b'n.$$

Osserviamo che $MCD(a',b')$ divide il numero al secondo membro perché divide entrambi gli addendi. Dunque $MCD(a',b')$ divide 1, e allora $MCD(a',b') = 1$.

□

Ecco un'osservazione aritmetica importante, nella cui dimostrazione l'Identità di Bézout gioca un ruolo fondamentale:

TEOREMA 2.2. *Siano $a,b,c \in \mathbb{Z}$. Se $a \mid bc$ e $MCD(a,b) = 1$ allora $a \mid c$.*

DIMOSTRAZIONE. Visto che $MCD(a,b) = 1$ allora per l'Identità di Bézout possiamo trovare $m,n \in \mathbb{Z}$ tali che

$$1 = an + bm.$$

Moltiplicando entrambi i membri per c otteniamo:

$$c = acn + bcm.$$

Questo ci permette di concludere che $a \mid c$. Infatti $a \mid acn$ (ovviamente) e $a \mid bcm$ (visto che $a \mid bc$ per ipotesi), dunque a divide la somma $acn + bcm$ che è uguale a c.

□

OSSERVAZIONE 2.3. La dimostrazione precedente è breve ma non è banale. Il Teorema 2.2 è alla base del fatto che la fattorizzazione in prodotto di primi di un numero intero è unica, come vedremo in seguito.

2. Definizione di congruenza e prime proprietà

Fissiamo un numero m intero positivo, per esempio $m = 12$.

Fare l'*aritmetica modulo* 12 vuol dire considerare tutti gli altri numeri interi da un punto di vista particolare: di ogni numero n ci interesserà solo il suo resto quando facciamo la divisione euclidea per 12. Per esempio, 38 sarà *identificato* al numero 2, visto che:

$$38 = 12 \cdot 3 + 2.$$

Ma anche 62 sarà identificato al 2:

$$62 = 12 \cdot 5 + 2.$$

Altri esempi, dove la freccia indica il resto della divisione per 12:

$$43 \to 7 \qquad 12 \to 0 \qquad -6 \to 6 \qquad -11 \to 1$$

$$15 \to 3 \qquad 27 \to 3 \qquad -8 \to 4 \qquad -12 \to 0.$$

Si dirà per esempio che 38, 62 e 2 sono *congrui modulo* 12, e si scriverà:

$$38 \equiv 62 \equiv 2 \quad (12)$$

Pensandoci bene, questa è una aritmetica molto naturale per le lancette del nostro orologio: se si parte dalla mezzanotte di un certo giorno e si lasciano trascorrere due ore, le lancette indicheranno le 2. Ma anche se facciamo trascorrere 38 ore o 62 ore, le lancette indicheranno sempre le 2. Per le lancette del nostro orologio, i numeri 2, 68 e 38 sono in effetti "identificati"!

Dall'esempio passiamo ad una definizione più generale:

Definizione 2.4. Fissato un numero intero positivo m, diremo che due numeri interi a e b sono *congrui modulo* m se quando facciamo la divisione euclidea di a per m otteniamo lo stesso resto di quando facciamo la divisione euclidea di b per m. Scriveremo:

$$a \equiv b \qquad (m)$$

oppure

$$a \equiv b \qquad \mod m.$$

Se due numeri a e b sono congrui modulo m, possiamo scrivere le loro divisioni euclidee per m, che, come sappiamo, hanno lo stesso resto:

$$a = mq + r \qquad b = ms + r.$$

Notiamo allora che

$$a - b = mq + r - (ms + r) = mq - ms = m(q - s).$$

Questo significa che m divide $a - b$. Viceversa, se prendiamo due numeri a e b che non sono congrui modulo m, possiamo facilmente osservare che $a - b$ non è un multiplo di m. Infatti, poniamo $a = mq + r_1$ e $b = ms + r_2$, dove r_1 e r_2 sono diversi fra loro e possiamo supporre $r_1 > r_2$. Scrivendo

$$a - b = mq + r_1 - (ms + r_2) = m(q - s) + (r_1 - r_2)$$

si nota che la divisione euclidea di $a - b$ per m ha resto $r_1 - r_2$, che è diverso da 0. In conclusione, abbiamo dimostrato:

Proposizione 2.5. *Dato un numero intero positivo m, due numeri interi a e b sono congrui modulo m se e solo se m divide $a - b$ (questo equivale anche a dire che m divide $b - a$).*

OSSERVAZIONE 2.6. Dunque, la condizione "m divide $a-b$" poteva essere presa come definizione di congruenza fra i numeri interi a e b.

TEOREMA 2.7. *Le congruenze "rispettano" somme e prodotti, nel senso che se* $a \equiv a' \bmod m$ *e* $b \equiv b' \bmod m$, *allora* $a+b \equiv a'+b' \bmod m$ *e* $ab \equiv a'b' \bmod m$.

DIMOSTRAZIONE. Supponiamo che $a' = a + km$ e $b' = b + k'm$.
Allora $a' + b' = a + b + (k + k')m$, e quindi $a + b \equiv a' + b' \bmod m$.
Inoltre $a'b' = (a+km)(b+k'm) = ab+kmb+k'ma+kk'm^2$, e siccome $kmb+k'ma+kk'm^2$ è un multiplo di m possiamo concludere $a'b' \equiv ab \bmod m$. □

ESEMPIO 2.8. Trovare il resto della divisione euclidea di $1253423 \cdot 134432$ per 5. Soluzione: Visto che $1253423 \equiv 3 \bmod 5$ e che $134432 \equiv 2 \bmod 5$, possiamo sostituire e scrivere: $1253423 \cdot 134432 \equiv 3 \cdot 2 \equiv 6 \equiv 1 \bmod (5)$. Quindi il resto è 1.

ESEMPIO 2.9. Trovare il resto della divisione euclidea di 2^{99} per 7. Soluzione: $2^{99} = 2^{3 \cdot 33} = 8^{33}$. Ora, 8 è congruo a 1 modulo 7 dunque possiamo continuare sostituendo: $8^{33} \equiv 1^{33} \equiv 1 \bmod 7$. Quindi il resto è 1.

ESEMPIO 2.10. Trovare il resto della divisione di 3^{11} per 5. Soluzione: Modulo 5 abbiamo le seguenti congruenze: $3^{11} \equiv 3^2 3^2 3^2 3^2 3 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \equiv (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot 3 \equiv -3 \equiv 2 \bmod (5)$. Quindi il resto è 2.

3. Calcolo veloce dei resti e basi numeriche

Ricordiamo che quando scriviamo un numero, ad esempio 1234567, implicitamente sottintendiamo che esso è scritto in base 10, ovvero:

$$1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$$

Utilizzando il linguaggio delle congruenze possiamo trovare dei modi rapidi di calcolare il resto della divisione euclidea. I prossimi esempi illustrano il caso in cui il divisore è $3, 9, 11, 4, 7$ (e in particolare ci fanno riottenere i famosi criteri di divisibilità per $3, 4, 7, 11$).

ESEMPIO 2.11. Trovare il resto della divisione di 1234564 per 3. Soluzione: Siccome $10 \equiv 1 \bmod 3$, nel fare le congruenze modulo 3 possiamo sostituire 10 con 1 nell'espansione decimale ottenendo: $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 1 \bmod 3$. Quindi il resto è 1. Se avessimo cercato il resto della divisione di 1234564 per 9, avremmo anche in questo caso sostituito il 10 con 1 ottenendo $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 7 \bmod 9$.

ESEMPIO 2.12. Trovare il resto della divisione di 1234567 per 11. Soluzione: Siccome $10 \equiv -1 \bmod (11)$, nel fare le congruenze modulo 11 possiamo sostituire 10 con -1 nell'espansione decimale ottenendo: $1234567 \equiv 1 - 2 + 3 - 4 + 5 - 6 + 7 \equiv 4 \bmod 11$. Quindi il resto è 4.

ESEMPIO 2.13. Trovare il resto della divisione di 1234567 per 4. Soluzione: Osserviamo che $100 = 25 \cdot 4 \equiv 0 \bmod (4)$. Quindi $1234567 = 12345 \cdot 100 + 67 \equiv 67 \equiv 3 \bmod (4)$.

ESEMPIO 2.14. Trovare il resto della divisione di 1234567 per 7. Soluzione: Osserviamo che $1000 = 7 \cdot 143 - 1 \equiv -1 \bmod (7)$. Quindi $1234567 = 1 \cdot 1000^2 + 234 \cdot 1000 + 567 \equiv 1 - 234 + 567 \equiv 334 \equiv 5 \bmod 7$.

ESEMPIO 2.15. Si dimostri che $\sqrt{1234567}$ non è un intero. Soluzione: per assurdo supponiamo che vi sia un intero x tale che $x^2 = 1234567$. Per l'esercizio precedente $x^2 \equiv 1234567 \equiv 3 \bmod 4$. Quindi basta mostrare che x^2 non può essere congruente a 3

modulo 4. Siccome x è congruo a $0, 1, 2$ o 3 modulo 4, ci sono solo quattro verifiche da fare:

$$\begin{aligned} 0^2 &\equiv 0 \bmod 4 \\ 1^2 &\equiv 1 \bmod 4 \\ 2^2 &\equiv 0 \bmod 4 \\ 3^2 &\equiv 1 \bmod 4 \end{aligned} .$$

Esempio 2.16. Cambiamento di base: verifichiamo che la scrittura 12345 in base 10 e la scrittura 30071 in base 8 indicano lo stesso numero. In simboli $(12345)_{\text{base } 10} = (30071)_{\text{base } 8}$. Infatti

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

I resti danno la scrittura in base 8 richiesta: infatti da quanto abbiamo scritto segue che $12345 = 1543 \cdot 8 + 1 = 192 \cdot 8^2 + 7 \cdot 8 + 1 = 24 \cdot 8^3 + 7 \cdot 8 + 1 = 3 \cdot 8^4 + 7 \cdot 8 + 1$.

4. Inverso di un numero modulo un intero positivo

Gli unici numeri interi che ammettono un inverso moltiplicativo in $\mathbb{Z}$ sono $+1$ e -1. Quando si considera l'aritmetica modulo un intero positivo m, invece sarà naturale trovare vari numeri che ammettono un inverso. Naturalmente, in questo caso per dire che un numero è inverso di un altro non pretendiamo che il prodotto dei due numeri faccia 1, ma ci basta che faccia un qualunque numero congruo a 1 modulo m:

Definizione 2.17. Sia m un intero positivo. Un inverso di un intero a modulo m è un intero x tale che $ax \equiv 1 \bmod m$.

Esempio 2.18. 2 è un inverso di 3 modulo 5 in quanto $2 \cdot 3 = 6 \equiv 1 \bmod 5$. Attenzione, anche 7 è un inverso di 3, e anche -3.... Come potete facilmente verificare, quando un numero ammette un inverso modulo m non ne ammette uno solo, ma infiniti.

Esempio 2.19. Non ci sono inversi di 2 modulo 4.

Teorema 2.20. *Un numero a ha un inverso modulo m se e solo se $MCD(a, m) = 1$.*

Dimostrazione. Se $MCD(a, m) = 1$ per il teorema di Bézout possiamo trovare u, v interi tali che $au + mv = 1$ con u, v interi. Questa uguaglianza, letta modulo m, diventa $au \equiv 1 \bmod m$. Quindi u è un inverso di a modulo m.

Viceversa supponiamo che a abbia un inverso u modulo m, ovvero $au \equiv 1 \bmod m$; questo come sappiamo equivale a dire che esiste k tale che $au - 1 = mk$, da cui ricaviamo $au - mk = 1$. Questo implica che $MCD(a, m) = 1$. □

Non sempre possiamo dividere in una congruenza. Ad esempio $2 \cdot 7 \equiv 2 \cdot 4 \bmod 6$, ma $7 \not\equiv 4 \bmod 6$. In generale, la divisione in una congruenza segue la seguente regola:

Teorema 2.21. *Dato $m \in \mathbb{N} - \{0\}$, per ogni $a \in \mathbb{Z} - \{0\}$, $b_1, b_2 \in \mathbb{Z}$ vale:*

$$a\ b_1 \equiv a\ b_2 \quad (m) \qquad \textit{se e solo se} \qquad b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a, m)}\right)$$

Osservazione 2.22. Quindi, se c'è un numero a che divide entrambi i membri di una congruenza, si può "semplificare", a patto però di dividere anche il modulo m per $MCD(a,m)$. Ad esempio[1]:

$$66 \equiv 42 \quad (8) \quad \Leftrightarrow \quad 11 \equiv 7 \quad (4)$$

dove abbiamo diviso il membro di sinistra e quello di destra per 6 e il modulo per $MCD(6,8) = 2$. Se non avessimo diviso il modulo per 2 avremmo ottenuto

$$11 \equiv 7 \quad (8)$$

che è **falsa**.

Dimostrazione. Ricordiamo che stiamo considerando $a \in \mathbb{Z} - \{0\}$. Supponiamo che

$$a\ b_1 \equiv a\ b_2 \quad (m).$$

Allora per la definizione di congruenza vale che

$$m \mid ab_1 - ab_2$$

ossia esiste un $q \in \mathbb{Z}$ tale che

$$ab_1 - ab_2 = mq.$$

Possiamo dividere per $MCD(a,m)$ e otteniamo

$$\frac{a}{MCD(a,m)}(b_1 - b_2) = \frac{m}{MCD(a,m)}q.$$

Da questo, visto che $\frac{a}{MCD(a,m)}$ e $\frac{m}{MCD(a,m)}$ sono coprimi (ricordate la Proposizione 2.1), segue, per il Teorema 2.2, che

$$\frac{m}{MCD(a,m)} \mid b_1 - b_2$$

ovvero che

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right).$$

Supponiamo ora, viceversa, che sia vero

$$b_1 \equiv b_2 \quad \left(\frac{m}{MCD(a,m)}\right).$$

Allora $\frac{m}{MCD(a,m)} \mid (b_1 - b_2)$, ossia esiste un $t \in \mathbb{Z}$ tale che

$$t\frac{m}{MCD(a,m)} = b_1 - b_2$$

da cui, moltiplicando per $MCD(a,m)$ otteniamo

$$tm = (b_1 - b_2)MCD(a,m).$$

Osserviamo dunque che

$$m \mid (b_1 - b_2)MCD(a,m)$$

da cui a maggior ragione ricaviamo

$$m \mid (b_1 - b_2)a$$

(abbiamo usato il fatto che $MCD(a,m)|a$) che si riscrive come

$$a\ b_1 \equiv a\ b_2 \quad (m).$$

[1]Il simbolo "$\Leftrightarrow$" sta per "se e solo se".

□

COROLLARIO 2.23. *Se* $ac \equiv bc \bmod m$ *e* $MCD(c,m) = 1$*, allora* $a \equiv b \bmod m$*.*

5. Metodo per risolvere le congruenze lineari in una incognita

In questo paragrafo ci occuperemo della risoluzione di equazioni con congruenze lineari con una incognita, ossia del seguente problema:

dati $a, b, m \in \mathbb{Z}$ *con* $m > 0$*, trovare tutti i numeri interi che risolvono la congruenza lineare ad una incognita*

$$ax \equiv b \quad (m). \tag{5.1}$$

Innanzitutto osserviamo che se esiste un intero d che divide a e m ma non divide b, allora l'equazione (5.1) non ha soluzioni. Infatti se (5.1) ha una soluzione $\overline{x}$, allora esiste un intero k tale che $a\overline{x} - b = km$. Da questa uguaglianza si ricava subito che se d divide a e m allora deve dividere anche b.

ESEMPIO 2.24. $6x \equiv 3 \bmod 4$ non ha soluzioni perché 2 divide 6 e 4 ma non divide 3.

In particolare dalla osservazione precedente si deduce che una condizione necessaria perchè l'equazione (5.1) abbia soluzioni è che $MCD(a,m)$ divida b.

Nel prossimo teorema daremo una dimostrazione che fornirà anche un algoritmo per trovare tutte le soluzioni quando esistono. Prima di enunciarlo, però, è bene fare una osservazione sull'equivalenza di due equazioni con congruenze lineari.

OSSERVAZIONE 2.25. Dato un numero k che divide a e b, l'equazione

$$\frac{a}{k}x \equiv \frac{b}{k} \quad \left(\frac{m}{MCD(k,m)}\right)$$

è equivalente alla equazione (5.1), ossia *ha le stesse soluzioni*. Questo segue dalla regola di divisione data dal Teorema 2.21, visto che in base a tale regola un intero $\overline{x}$ soddisfa $a\overline{x} \equiv b \quad (m)$ se e solo se soddisfa

$$\frac{a}{k}\overline{x} \equiv \frac{b}{k} \quad \left(\frac{m}{MCD(k,m)}\right).$$

Analogamente (si può vedere in realtà come caso particolare di quanto appena osservato), se s è un numero primo con m, l'equazione

$$sax \equiv sb \quad (m)$$

è equivalente alla (5.1).

TEOREMA 2.26. *La congruenza*

$$ax \equiv b \quad (m)$$

ha soluzione se e solo se il massimo comun divisore tra a *e* m *divide* b*. In questo caso l'equazione ha infinite soluzioni, precisamente* $MCD(a,m)$ *soluzioni modulo* m*.*

OSSERVAZIONE 2.27. Quando diciamo "l'equazione ha $MCD(a,m)$ soluzioni modulo m" intendiamo dire che l'insieme delle soluzioni dell'equazione è composto da esattamente $MCD(a,m)$ soluzioni $\overline{x}$ che soddisfano $0 \leq \overline{x} < m$ e tutte le altre soluzioni sono i numeri che si ottengono da queste sommando loro un multiplo di m.

DIMOSTRAZIONE. Se $MCD(a,m)$ non divide b sappiamo già che la congruenza non ha soluzioni. Quindi consideriamo il caso in cui $MCD(a,m)$ divide b. In questo caso $MCD(a,m)$ è dunque il massimo divisore positivo comune a tutti e tre i numeri a, b, m; dividendo l'equazione data per $MCD(a,m)$ otteniamo l'equazione

$$a'x \equiv b' \quad (m') \tag{5.2}$$

dove $a' = \dfrac{a}{MCD(a,m)}, b' = \dfrac{b}{MCD(a,m)}, m' = \dfrac{m}{MCD(a,m)}$, che è equivalente alla (5.1) come sappiamo dalla Osservazione 2.25.

A questo punto notiamo che, per costruzione, a' e m' sono coprimi e che, per il Teorema 2.20, a' ha un inverso e' modulo m'. [2] Osserviamo in particolare che, visto che anche e' ha un inverso modulo m', ovvero a', allora sempre per il Teorema 2.20 risulta che e' è primo con m'.

Moltiplicando per e' il membro di sinistra e quello di destra di (5.2) otteniamo

$$e'a'x \equiv e'b' \quad (m'). \tag{5.3}$$

Per l'Osservazione 2.25 sappiamo che l'equazione (5.3) è equivalente alla (5.2).

Visto che $e'a' \equiv 1 \quad (m')$ possiamo riscrivere la (5.3) come

$$x \equiv e'b' \quad (m').$$

A questo punto si osserva subito che le soluzioni di questa equazione (e dunque le soluzioni della (5.1)) sono tutti e soli gli interi della forma $e'b' + km'$ al variare di k in $\mathbb{Z}$. Visto che $m' = \dfrac{m}{MCD(a,m)}$, ci sono esattamente $MCD(a,m)$ interi di questa forma in ogni sequenza di m numeri consecutivi. □

ESEMPIO 2.28. Data l'equazione

$$195x \equiv 6 \quad (42)$$

trovare:
a) tutte le sue soluzioni,
b) le sue soluzioni modulo 42, ossia quelle comprese fra 0 e 41.

SOLUZIONE: Osserviamo che $MCD(195,42) = 3 \mid 6$ dunque l'equazione ha soluzione. Per prima cosa possiamo sostituire 195 con il suo resto modulo 42, ossia 27:

$$27x \equiv 6 \quad (42).$$

Poi possiamo dividere membro di destra, membro di sinistra e modulo per $MCD(195,42) = 3$, ottenendo l'equazione equivalente:

$$9x \equiv 2 \quad \left(\frac{42}{MCD(3,42)} = 14\right).$$

Un possibile modo di procedere adesso è il seguente: si nota "a occhio" che $3 \cdot 9 = 27$ è congruo a -1 modulo 14. Dunque ci conviene moltiplicare il membro di sinistra e quello di destra per 3. Visto che 3 è primo con 14, per l'Osservazione 2.25 sappiamo che l'equazione che otteniamo è equivalente:

$$27x \equiv 6 \quad (14)$$

che si può riscrivere

$$-x \equiv 6 \quad (14).$$

[2] Ricordiamo che, in concreto, si può applicare l'algoritmo per trovare una combinazione di Bézout per ottenere due interi x', y' tali che $1 = a'x' + m'y'$ e poi si prende $e' = x'$.

Moltiplicando adesso per -1 (anch'esso primo con 14), otteniamo:

$$x \equiv -6 \quad (14).$$

Questa scrittura descrive già con chiarezza l'insieme di tutte soluzioni dell'equazione

$$195x \equiv 6 \quad (42)$$

Possiamo comunque anche scriverlo così:

$$\{x = -6 + 14q \mid q \in \mathbb{Z}\}$$

Per rispondere alla domanda b), dobbiamo indicare le soluzioni x con $0 \leq x \leq 41$. Sono tre: $-6+14, -6+2\cdot 14, -6+3\cdot 14$, cioè 8, 22 e 36. □

6. Esempi di risoluzione di una equazione diofantea (usando le congruenze)

Facciamo qualche esempio che illustra la relazione fra le soluzioni (intere) di una *equazione diofantea* (ossia a coefficienti interi) lineare in due variabili e quella delle equazioni lineari con congruenze ad essa associate. Consideriamo l'equazione diofantea:

$$224x + 108y = 700. \tag{6.1}$$

Osservazione 2.29. Se esiste una soluzione (X, Y), il numero intero X deve anche soddisfare

$$224X \equiv 700 \quad (108)$$

(infatti $108Y = 700 - 224X$ dunque $108 \mid 224X - 700$). Viceversa, se un certo numero intero X soddisfa la congruenza $224X \equiv 700 \quad (108)$, questo vuol dire che soddisfa $108 \mid 224X - 700$; allora deve esistere un Y tale che $108Y = 700 - 224X$ e dunque

$$224X + 108Y = 700$$

cioè la coppia (X, Y) risolve l'equazione diofantea (6.1).

In conclusione abbiamo osservato che l'insieme delle soluzioni dell'equazione

$$224x \equiv 700 \quad (108)$$

coincide con l'insieme dato dalle prime componenti ("le X") delle coppie che risolvono l'equazione diofantea (6.1).

Risolviamo allora la congruenza

$$224x \equiv 700 \quad (108).$$

Per prima cosa sostituiamo il 224 e il 700 con dei numeri più piccoli, a loro congrui modulo 108:

$$8x \equiv 160 \quad (108).$$

Ora possiamo dividere per 8, per semplificare[3] :

$$x \equiv 20 \quad \left(\frac{108}{MCD(108, 8)} = 27\right).$$

Dunque l'insieme delle soluzioni di

$$224x \equiv 700 \quad (108)$$

è

$$\{x = 20 + 27q \mid q \in \mathbb{Z}\}.$$

[3]La scelta di sostituire il 700 con 160, anzichè per esempio col 52, è stata dettata proprio dal fatto di aver intravisto la possibilità di questa divisione per 8 che rende la soluzione molto rapida; la conclusione dell'esercizio sarebbe abbastanza veloce anche sostituendo con il 52, verificate.

Possiamo sostituire queste soluzioni al posto della x nella equazione diofantea

$$224x + 108y = 700,$$

che comunque per semplificare possiamo dividere per 4=MCD(224, 108), ottenendo l'equazione diofantea equivalente $56x + 27y = 175$:

$$56(20 + 27q) + 27y = 175.$$

Svolgiamo i conti:

$$27y = -1120 + 175 - 56 \cdot 27q$$
$$27y = -945 - 56 \cdot 27q$$
$$y = -35 - 56q.$$

Abbiamo dunque trovato che l'insieme delle soluzioni di

$$224x + 108y = 700$$

è:

$$\{(20 + 27q\ ,\ -35 - 56q) \mid q \in \mathbb{Z}\}.$$

Esempio 2.30. Trovare tutte le soluzioni intere della equazione diofantea

$$54 = 252x + 198y.$$

Soluzione: Dividendo tutto per $18 = MCD(252, 198)$ otteniamo l'equazione equivalente:

$$3 = 14x + 11y.$$

Risolviamo la congruenza

$$14x \equiv 3 \bmod 11.$$

Moltiplicando per 4 e semplificando otteniamo $x \equiv 1 \bmod 11$, quindi x è della forma $x = 1 + 11k$. Sostituendo nella $14x + 11y = 3$ e facendo i conti si trova $y = -1 - 14k$. Dunque l'insieme delle soluzioni della equazione diofantea data è

$$\{(1 + 11k\ ,\ -1 - 14k) \mid k \in \mathbb{Z}\}.$$

□

7. Esercizi

Esercizio 2.31 (di ripasso, consigliato l'uso del principio del minimo). Dati due numeri interi a e b con $(a, b) \neq (0, 0)$, dimostrare che $MCD(a, b)$ è il più piccolo numero intero positivo ottenibile come combinazione lineare intera di a e di b.

Esercizio 2.32 (di ripasso, sul MCD). Sia $(a_n)_{n \in \mathbb{N}}$ la successione definita per ricorrenza da

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 1 \\ a_{n+1} &= 2a_n + 3a_{n-1} \qquad \forall n \geq 1. \end{aligned}$$

Dimostrare che:

(1) $\mathrm{MCD}(a_n, 3) = 1$ per ogni $n \geq 0$.
(2) $\mathrm{MCD}(a_{n+1}, a_n) = 1$ per ogni $n \geq 0$.

Esercizio 2.33. Premessa: ricordiamo qui la classica dimostrazione del fatto che i numeri primi sono infiniti.

Teorema 2.34. *L'insieme $\mathcal{P}$ dei numeri primi è infinito.*

DIMOSTRAZIONE. Supponiamo per assurdo che $\mathcal{P}$ sia finito e siano dunque

$$p_1, p_2, \ldots, p_N$$

tutti i numeri primi. Consideriamo allora il numero

$$a = (p_1 \cdot p_2 \cdots p_N) + 1$$

Come sappiamo, ogni numero ammette una fattorizzazione in primi, dunque prendiamo un primo p che divide a. Vale allora $a \equiv 0 \mod (p)$. D'altra parte, p deve essere uno dei p_i, visto che questi sono tutti i numeri primi. Allora $p_1 \cdot p_2 \cdots p_N \equiv 0 \mod (p)$ e dunque

$$a = (p_1 \cdot p_2 \cdots p_N) + 1 \equiv 0 + 1 \equiv 1 \mod p.$$

Questo contraddice $a \equiv 0 \mod p$.

□

Dimostrare che l'insieme dei numeri primi congrui a 3 modulo 4 è infinito.[4]

ESERCIZIO 2.35. Consideriamo i numeri interi x tali che $10000000 \leq x < 20000000$. Quanti di questi numeri sono congrui a 1 modulo 3?

ESERCIZIO 2.36. Stabilire se è vero o falso che

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot 12 \cdot 13 \equiv 7 \qquad (17)$$
$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot 12 \cdot 13 \equiv 0 \qquad (1024).$$

In generale è vero o falso che il prodotto di 13 numeri interi consecutivi è sempre divisibile per 1024?

ESERCIZIO 2.37. Consideriamo la successione definita per ricorrenza

$$x_0 = 2,\ x_{n+1} = x_n^2 + 1.$$

Sia r_n il resto della divisione euclidea di x_n per 5.

1) Calcolare i primi 7 valori di r_n.

2) Si dia una regola generale per calcolare r_n e la si dimostri per induzione.

3) Si calcoli r_{10000}.

ESERCIZIO 2.38 (Tornei all'italiana). Supponiamo di avere n squadre di calcio, con n numero pari, e di voler organizzare un torneo all'italiana[5]. Basta pensare al girone d'andata, quello di ritorno poi è automatico, dunque bisogna organizzare $n-1$ turni. Le congruenze possono aiutarci. Possiamo infatti utilizzare la seguente regola:

- al turno i la squadra x, con $1 \leq x \leq n-1$, incontrerà la squadra y dove y soddisfa $1 \leq y \leq n-1$ e
$$x + y \equiv i \mod n-1$$
a meno che questa equazione non dia come soluzione $x = y$. In tal caso la squadra x incontra la squadra n.

Dimostrare che il torneo così preparato è ben organizzato (vedi Tabella 1).

[4]Anche l'insieme dei numeri primi congrui a 1 modulo 4 è infinito, ma di questo parleremo più avanti.

[5]Se avessimo un numero dispari di squadre ci potremmo comunque ricondurre a questo caso aggiungendo una squadra fittizia, con la regola che se una squadra deve incontrarla le tocca invece un turno di riposo.

	Turno 1	Turno 2	Turno 3	Turno 4	Turno 5
squadra 1	vs 5	vs 6	vs 2	vs 3	vs 4
squadra 2	vs 4	vs 5	vs 1	vs 6	vs 3
squadra 3	vs 6	vs 4	vs 5	vs 1	vs 2
squadra 4	vs 2	vs 3	vs 6	vs 5	vs 1
squadra 5	vs 1	vs 2	vs 3	vs 4	vs 6
squadra 6	vs 3	vs 1	vs 4	vs 2	vs 5

TABELLA 1. Esempio: il tabellone del torneo nel caso di 6 squadre.

ESERCIZIO 2.39. Dato un numero naturale m, dimostrare che se $2^m + 1$ è primo allora m è una potenza di 2.

ESERCIZIO 2.40 (I numeri di Fermat). Dato $n \in \mathbb{N}$ definiamo:

$$\mathcal{F}_n = 2^{2^n} + 1.$$

I numeri $\mathcal{F}_n$ si chiamano *numeri di Fermat*. Fermat[6] aveva congetturato che tali numeri fossero tutti primi... ma, come fu mostrato da Eulero[7], la congettura è falsa. Provate anche voi a confutarla:

- Dimostrare che $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ sono primi. Dimostrare che anche $\mathcal{F}_4$ è primo. [Consiglio: non fatelo davvero adesso, $\mathcal{F}_4$ è un numero troppo grande. La cosa diventerà abbordabile con qualche risultato in più che conosceremo nel prossimo capitolo.]
- Dimostrare che $\mathcal{F}_5$ è divisibile per 641. [Traccia: può essere utile osservare che $641 = 2^4 + 5^4 = 1 + 5 \cdot 2^7$]

Possiamo comunque utilizzare i numeri di Fermat per dimostrare, in maniera diversa da quella che già conoscete (ma quale conoscete?), che i numeri primi sono infiniti:

- Dimostrare che se $n \neq m$ allora $\mathcal{F}_n$ e $\mathcal{F}_m$ sono coprimi.
- Dedurre dal punto precedente che i numeri primi sono infiniti.

ESERCIZIO 2.41. Risolvere l'equazione diofantea

$$40x + 252y = 44.$$

[6]Pierre de Fermat, matematico francese, 1601-1665.
[7]Leonhard Euler, matematico svizzero, 1707-1783.

Esistono soluzioni (x, y) con $x \equiv 0 \bmod 7$? E con $x \equiv 0 \bmod 13$?

Esercizio 2.42. Trovare tutte le soluzioni intere dell'equazione

$$341x \equiv 15 \quad (912).$$

Esercizio 2.43. Trovare tutte le soluzioni della congruenza

$$18\ x \equiv 1 \quad (25).$$

Quante sono le soluzioni x con $-10 \leq x \leq 300$?

Esercizio 2.44. a) Trovare tutti i numeri interi che risolvono l'equazione

$$70x \equiv 222 \qquad (24).$$

b) Trovare tutti i numeri interi che risolvono l'equazione

$$(x+1)(x+2) \equiv 0 \qquad (24).$$

Esercizio 2.45. Trovare tutte le soluzioni della congruenza

$$12\ x \equiv 33 \quad (57).$$

Quante sono le soluzioni x con $-10 \leq x \leq 10$?

Esercizio 2.46. Trovare tutte le soluzioni della congruenza

$$1008\ x \equiv 12 \quad (11).$$

Esercizio 2.47. a) Trovare tutte le soluzioni della congruenza

$$546x \equiv 442 \quad (260).$$

b) Trovare tutte le soluzioni della congruenza

$$7x \equiv -46 \quad (58).$$

c) Trovare le soluzioni comuni alle due equazioni. [È una piccola anticipazione di un tema trattato nel prossimo capitolo.]

Esercizio 2.48. Trovare tutte le soluzioni della congruenza

$$44\ x \equiv 10 \quad (105).$$

Esercizio 2.49. Trovare per quali $b \in \mathbb{Z}$ e $m \in \mathbb{N} - \{0\}$ si può risolvere la congruenza

$$2\ x \equiv b \quad (m).$$

Esercizio 2.50. a) Risolvere la congruenza

$$168x \equiv 3080 \quad (455).$$

b) Per quali valori del numero intero positivo m la congruenza

$$168x \equiv 1540 \quad (35m)$$

ammette soluzione?

Esercizio 2.51. Trovare tutte le soluzioni della congruenza

$$420\ x \equiv 91 \quad (119).$$

Quante sono le soluzioni x con $-10 \leq x \leq 300$?

Esercizio 2.52. Trovare tutte le soluzioni della congruenza $42x \equiv 6 \bmod 110$ e stabilire il numero delle soluzioni nell'intervallo $[-1000, 2000]$.

Esercizio 2.53. Trovare tutte le soluzioni della congruenza $9x \equiv 3^{15} \bmod 17$.

Esercizio 2.54. Determinare per quali valori del parametro k la congruenza

$$-6x \equiv 20 \bmod 7k$$

ha soluzione e risolverla per $k = 8$.

Esercizio 2.55. Risolvere l'equazione diofantea

$$40x + 252y = 44.$$

Esercizio 2.56. Trovare tutte le soluzioni della equazione diofantea

$$4060x + 1953y = 49.$$

È vero che per ogni soluzione $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ vale che $x - y$ è un multiplo di 3?

Esercizio 2.57. Si determini l'insieme $A = \{(x, y) \in \mathbb{Z}^2 \mid 102x + 153y = 459\}$. Si determini la cardinalità dell'insieme $B = \{(x, y) \in A \mid |x| + |y| < 100\}$.

Esercizio 2.58. a) Calcolare $MCD(3192, 117)$.
b) Trovare tutti gli $m \in \mathbb{Z}$ che soddisfano

$$3192\ m \equiv 288 \mod 117$$

e tali che $0 \leq m \leq 234$.

Esercizio 2.59. Dire se le seguenti proposizioni sono vere o false e motivare la risposta:

a) per tutti i numeri naturali positivi n, $7^n \equiv n^3 + 3n^2 + 2n + 1 \mod 5$.
b) Per tutti i numeri naturali positivi n, $7^n \equiv n^3 + 3n^2 + 2n + 1 \mod 3$.
c) Per tutti i numeri naturali positivi n, $7^n \geq n^3 + 3n^2 + 2n + 1$.

Esercizio 2.60. a) Trovare tutti gli interi x che soddisfano la congruenza:

$$1386x \equiv 1890 \quad (294).$$

b) Trovare tutti gli interi y che soddisfano la congruenza:

$$1386y^2 \equiv 1890 \quad (294).$$

Esercizio 2.61. a) Risolvere la congruenza

$$396x \equiv 234 \quad (1050).$$

b) Per quali valori dell'intero k la congruenza

$$396x \equiv 234 \quad (105 \cdot k)$$

ha soluzione?

Esercizio 2.62. a) Risolvere la congruenza

$$5920x \equiv 160 \quad (504).$$

b) Per quali valori del numero intero positivo m la congruenza

$$5920x \equiv 160 \quad (56m)$$

ammette soluzione ?

Esercizio 2.63. Trovare tutte le soluzioni di

$$x^2 + 1 \equiv 0 \bmod 65.$$

ESERCIZIO 2.64. Dimostrare che per ogni numero primo p esiste un numero naturale n tale che

$$6n^2 + 5n + 1 \equiv 0 \bmod p.$$

CAPITOLO 3

Il teorema cinese del resto e il piccolo teorema di Fermat

1. Sistemi di congruenze. Il teorema cinese del resto

Proviamo a risolvere un sistema di due equazioni lineari con congruenze:

$$\begin{cases} x \equiv a & (m_1) \\ x \equiv b & (m_2) \end{cases}.$$

Per prima cosa osserviamo che le soluzioni della prima equazione sono tutti e soli i numeri della forma

$$x = a + km_1 \quad \text{con} \quad k \in \mathbb{Z}.$$

Ci chiediamo quando un tale numero risolve anche la seconda equazione. Per saperlo sostituiamo $a + km_1$ alla x nella seconda equazione:

$$a + km_1 \equiv b \qquad (m_2).$$

Qui la variabile è k e otteniamo

$$m_1 k \equiv b - a \qquad (m_2).$$

Questa equazione, come sappiamo, ha soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$. Dunque siamo già arrivati ad una prima conclusione: il sistema di partenza ha soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$.

Nel caso in cui ci siano soluzioni, come fare a trovarle tutte? Prendiamo una soluzione particolare k_0 della equazione

$$m_1 k \equiv b - a \qquad (m_2).$$

Allora $x_0 = a + k_0 m_1$ è una soluzione del sistema di partenza ossia

$$\begin{cases} x_0 \equiv a & (m_1) \\ x_0 \equiv b & (m_2) \end{cases}.$$

Come differisce da un'altra soluzione del sistema di partenza? Se anche x_1 soddisfa

$$\begin{cases} x_1 \equiv a & (m_1) \\ x_1 \equiv b & (m_2) \end{cases}$$

sottraendo opportunamente otteniamo

$$\begin{cases} x_0 - x_1 \equiv 0 & (m_1) \\ x_0 - x_1 \equiv 0 & (m_2) \end{cases}.$$

Dunque $x_0 - x_1$ è un numero che deve essere multiplo di m_1 e anche di m_2. Il più piccolo numero intero positivo che soddisfa tale condizione come sapete si chiama minimo comune

multiplo di m_1 e di m_2 e si indica come $mcm\ (m_1, m_2)$. Ricordiamo anche che tutti e soli i numeri che sono divisi da m_1 e da m_2 sono i multipli di $mcm\ (m_1, m_2)$.[1]

In conclusione, tornando al nostro sistema, abbiamo dimostrato che due soluzioni x_0 e x_1 del sistema differiscono per un multiplo di $mcm\ (m_1, m_2)$. Viceversa si verifica subito che, dato x_0 che soddisfa il sistema e dato un multiplo $s \cdot mcm\ (m_1, m_2)$ di $mcm\ (m_1, m_2)$, anche

$$x_0 + s \cdot mcm\ (m_1, m_2)$$

soddisfa il sistema.

Possiamo riassumere tutto quel che abbiamo detto fin qui nel seguente:

Teorema 3.1 (Teorema cinese del resto per due equazioni con moduli qualunque). *Dato il sistema di equazioni*

$$\begin{cases} x \equiv a & (m_1) \\ x \equiv b & (m_2) \end{cases}$$

tale sistema ammette soluzione se e solo se $MCD(m_1, m_2) \mid (b - a)$. *In tal caso, presa una soluzione* x_0, *tutte le altre soluzioni del sistema sono i numeri della forma*

$$x_0 + s \cdot mcm\ (m_1, m_2) \quad con \quad s \in \mathbb{Z}$$

Osservazione 3.2. Come sappiamo, questo si può esprimere anche dicendo che tutte le soluzioni del sistema sono i numeri x che soddisfano

$$x \equiv x_0 \qquad (mcm\ (m_1, m_2)).$$

In particolare osserviamo che esiste un'unica soluzione x con $0 \leq x < mcm\ (m_1, m_2)$.

Esempio 3.3. Si consideri il sistema:

$$\begin{cases} 14x \equiv 4570 & (30) \\ 45x \equiv 231 & (8) \end{cases}.$$

Innanzitutto studiamo e risolviamo una per una le due equazioni: la prima ha soluzione perché $MCD(14, 30) = 2 \mid 4570$ e la possiamo riscrivere sostituendo a 4570 il suo resto modulo 30:

$$14x \equiv 10 \qquad (30).$$

Dividendo per 2 otteniamo:

$$7x \equiv 5 \qquad (15).$$

Se moltiplichiamo entrambi i membri per 2 otteniamo una equazione equivalente perché 2 è primo con il modulo 15 e così arriviamo a

$$14x \equiv 10 \qquad (15)$$

$$-x \equiv 10 \qquad (15)$$

$$x \equiv -10 \qquad (15)$$

$$x \equiv 5 \qquad (15).$$

[1] Infatti se t è diviso da m_1 e anche da m_2, consideriamo la divisione euclidea di t per $mcm\ (m_1, m_2)$:

$$t = q \cdot mcm\ (m_1, m_2) + r$$

dove $0 \leq r < mcm\ (m_1, m_2)$. Ora, siccome m_1 e m_2 dividono t e $q \cdot mcm\ (m_1, m_2)$, entrambi devono anche dividere r. Allora r deve essere 0, altrimenti sarebbe un numero intero positivo diviso da m_1 e da m_2 ma più piccolo di $mcm\ (m_1, m_2)$ (assurdo).

Per quel che riguarda la seconda equazione, notiamo subito che ha soluzione perché 45 e 8 sono primi fra loro. Sostituiamo ai numeri che compaiono i loro resti modulo 8:

$$5x \equiv 7 \qquad (8).$$

Moltiplicando entrambi i membri per 3 otteniamo l' equazione equivalente

$$15x \equiv 21 \qquad (8)$$

che risolviamo facilmente

$$-x \equiv 5 \qquad (8)$$
$$x \equiv -5 \qquad (8)$$
$$x \equiv 3 \qquad (8).$$

Dunque il sistema dato si può riscrivere come

$$\begin{cases} x \equiv 5 & (15) \\ x \equiv 3 & (8) \end{cases}.$$

Ora possiamo applicare il teorema cinese del resto: il sistema ammette soluzione perché $MCD(15, 8) = 1$ e dunque divide $5 - 3$.

A questo punto dobbiamo trovare una soluzione particolare. Ne esisterà una (e una sola) compresa fra 0 e 119 (infatti $120 = 15 \cdot 8$ è il $mcm\ (15, 8)$). Possiamo cercarla fra i numeri $5, 20, 35, 50, 65, ...$ che sono le soluzioni della prima equazione. Vediamo subito che 35 fa al caso nostro. Dunque, grazie al teorema cinese del resto, possiamo affermare che tutte le soluzioni del sistema sono i numeri della forma

$$35 + 120s \qquad \text{con} \quad s \in \mathbb{Z}.$$

Osservazione 3.4. Se non avessimo "visto" subito il 35 avremmo comunque potuto seguire il metodo standard: la prima equazione ci dice che x deve essere del tipo $x = 5+15k$. Sostituendo nella seconda abbiamo

$$5 + 15k \equiv 3 \qquad (8)$$

ossia

$$15k \equiv -2 \qquad (8)$$
$$-k \equiv -2 \qquad (8)$$
$$k \equiv 2 \qquad (8).$$

Allora $x = 5 + 15 \cdot 2 = 35$ è una soluzione particolare..e abbiamo "ritrovato" il 35.

Riscriviamo ora il teorema nel caso particolare in cui i moduli delle due equazioni sono primi fra loro, come premessa per poi enunciare il teorema cinese del resto nella sua forma classica.

Teorema 3.5 (Teorema cinese del resto per due equazioni con moduli primi fra loro). *Dato il sistema di congruenze*

$$\begin{cases} x \equiv a & (m_1) \\ x \equiv b & (m_2) \end{cases}$$

con $MCD(m_1, m_2) = 1$, tale sistema ammette sempre soluzione ed esiste un'unica soluzione x_0 tale che $0 \le x_0 < m_1 \cdot m_2$. Tutte le altre soluzioni del sistema sono i numeri della forma

$$x_0 + q \cdot m_1 \cdot m_2 \quad \textit{con} \quad q \in \mathbb{Z}.$$

La dimostrazione che abbiamo dato si generalizza facilmente al caso di sistemi di n congruenze in cui i moduli siano a due a due coprimi:

TEOREMA 3.6 (Teorema cinese del resto, forma classica). *Dato il sistema di congruenze*

$$\begin{cases} x \equiv a_1 & (m_1) \\ x \equiv a_2 & (m_2) \\ .. \quad .. \quad .. & .. \\ .. \quad .. \quad .. & .. \\ x \equiv a_{n-1} & (m_{n-1}) \\ x \equiv a_n & (m_n) \end{cases}$$

in cui i moduli sono a due a due coprimi (questo vuol dire che per ogni $i \neq j$ vale $MCD(m_i, m_j) = 1$), tale sistema ammette sempre soluzione ed esiste un'unica soluzione x_0 tale che $0 \leq x_0 < m_1 \cdot m_2 \cdots m_{n-1} \cdot m_n$. Tutte le altre soluzioni del sistema sono i numeri della forma

$$x_0 + q \cdot m_1 \cdot m_2 \cdots m_{n-1} \cdot m_n \quad con \quad q \in \mathbb{Z}\,.$$

ESERCIZIO 3.7. Dimostrare la forma classica del teorema cinese del resto. (Suggerimento: per induzione sul numero n di equazioni del sistema; il caso di sistemi con due congruenze lo abbiamo già studiato...).

Trovate una discussione del teorema cinese del resto nel libro [**DM**], al Capitolo 4, Paragrafo 7 (in alcuni passaggi viene usata la notazione delle classi di resto, che noi introdurremo presto, ma alcuni esempi ed esercizi sono scritti nella stessa notazione che abbiamo usato noi).

2. Coefficienti binomiali

Dato n numero naturale positivo, e $k \in \mathbb{N}$, con $0 \leq k \leq n$, poniamo

$$\binom{n}{k} := \text{ numero di sottoinsiemi di } \{1, 2, \ldots, n\} \text{ con } k \text{ elementi.}$$

Ad esempio, per ogni $n \geq 1$, $\binom{n}{n} = 1$, $\binom{n}{1} = n$ e $\binom{n}{0} = 1$, quest'ultima segue dalla osservazione che c'è un solo sottoinsieme (l'insieme vuoto) con 0 elementi. Inoltre poniamo per convenzione $\binom{0}{0} = 1$ e $\binom{n}{k} = 0$ per ogni $n, k \in \mathbb{N}$ con $k > n$.

I numeri $\binom{n}{k}$ (in inglese leggi "n choose k") sono detti *coefficienti binomiali*; i primi valori sono dati dalla seguente tabella:

$k \backslash n$	0	1	2	3	4	5	6
0	1	1	1	1	1	1	1
1	0	1	2	3	4	5	6
2	0	0	1	3	6	10	15
3	0	0	0	1	4	10	20
4	0	0	0	0	1	5	15
5	0	0	0	0	0	1	6
6	0	0	0	0	0	0	1

Osserviamo che per ogni n numero naturale positivo, e per ogni $k \in \mathbb{N}$, con $1 \leq k \leq n$ vale

$$\binom{n}{k} = \binom{n}{n-k},$$

infatti a ogni sottoinsieme di k elementi di $\{1, 2, \dots, n\}$ corrisponde naturalmente il suo complementare, che è un sottoinsieme di $n-k$ elementi di $\{1, 2, \dots, n\}$.

La seguente formula è solitamente attribuita a Newton[2].

TEOREMA 3.8. *Per $n \in \mathbb{N}$ e x variabile, vale*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{2.1}$$

DIMOSTRAZIONE. La dimostrazione è ovvia: per ottenere x^k dal prodotto degli n fattori $(1+x)^n = (1+x)(1+x)\cdots(1+x)$ dobbiamo scegliere k volte la x e le altre $(n-k)$ volte l'1. □

Esiste una (ben nota) formula chiusa per i binomiali.[3]

PROPOSIZIONE 3.9. *Per $n, k \in \mathbb{N}$ con $n \geq k \geq 0$ vale*

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}, \tag{2.2}$$

dove $k! := k(k-1)\cdots 2 \cdot 1$ denote il fattoriale *di k (convenzionalmente $0! = 1$).*

DIMOSTRAZIONE. Dobbiamo scegliere un sottoinsieme di $\{1, 2, \dots, n\}$ con k elementi: ci sono n scelte per il primo elemento, $n-1$ scelte per il secondo, etc., fino a $n-k+1$ scelte per il k-esimo, ma in questo modo stiamo contando questi insiemi troppe volte (ad esempio sceliere prima 1 e poi 4 o viceversa porta allo stesso sottoinsieme di 2 elementi, ossia $\{1, 4\}$). Infatti ogni sottoinsieme scelto viene contato $k!$ volte, che è il numero di modi di ordinare k elementi distinti: infatti ci sono k possibilità per il primo elemento, $k-1$ per il secondo, etc.. □

ESERCIZIO 3.10. Dimostrare combinatorialmente (ossia senza usare la (2.2)) la seguente ricorrenza: per ogni intero $n \geq 2$ e per ogni intero k con $1 \leq k \leq n-1$ vale

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Questa semplice ricorrenza spiega il famoso *triangolo di Pascal*:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
\therefore & & \therefore & & \therefore & & \vdots & & \ddots & & \ddots & & \ddots
\end{array}$$

[2]Isaac Newton, matematico inglese, 1642 - 1727.

[3]Spesso, in maniera innaturale, la formula (2.2) viene addirittura data come definizione del binomiale.

3. Il piccolo teorema di Fermat

In questa sezione studieremo un importante teorema che riguarda le potenze dei numeri modulo un intero positivo m.

TEOREMA 3.11 (Il piccolo teorema di Fermat). *Se p è un numero primo e a è un numero intero che non è un multiplo di p, allora vale*

$$a^{p-1} \equiv 1 \quad (p)$$

OSSERVAZIONE 3.12. Sia $p = 7$. Il teorema ci garantisce che per ogni $a \in \mathbb{Z}$ che non sia multiplo di 7 vale:

$$a^6 \equiv 1 \quad (7).$$

Avvertiamo subito che può accadere che 6 non sia il più piccolo numero t tale che

$$a^t \equiv 1 \quad (7).$$

Per esempio per $a = 2$ troviamo:

$$2^3 \equiv 1 \quad (7)$$

Invece per $a = 3$ la più piccola potenza che dà un risultato congruo a 1 modulo 7 è effettivamente 6. Infatti le potenze di 3 modulo 7 sono le seguenti:

$$3^1 = 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1$$

Approfondiremo più avanti questa osservazione.

DIMOSTRAZIONE. Dato un intero $a \not\equiv 0 \quad (p)$ consideriamo i numeri

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

Questi $p-1$ numeri sono a due a due non congrui fra loro modulo p. Supponiamo infatti, per assurdo, che esistano i e j $(0 \le i < j \le p-1)$ tali che $ia \equiv ja \quad (p)$.

Ora sappiamo (per il Teorema 2.20) che a ammette un inverso modulo p. Sia dunque b un inverso di a. Moltiplicando per b otteniamo:

$$iab \equiv jab \quad (p)$$

ossia

$$i \equiv j \quad (p)$$

Poiché avevamo supposto $0 \le i < j \le p-1$ abbiamo trovato un assurdo.

Dunque la lista

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

comprende $p-1$ numeri i cui resti nella divisione per p sono tutti diversi da 0 e a due a due distinti. Allora i resti dei numeri $a, 2a, \ldots, (p-1)a$ sono esattamente, a meno di riordinarli, i numeri

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

Possiamo dunque scrivere che

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \qquad (p)$$

Questa congruenza, raccogliendo a sinistra i fattori uguali ad a, equivale alla seguente:

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \qquad (p)$$

Ora osserviamo che $p-1$ è invertibile modulo p (sempre per il Teorema 2.20), e moltiplichiamo entrambi i membri per un suo inverso. Otteniamo

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-2) \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \qquad (p)$$

Poi moltiplichiamo entrambi i membri per un inverso di $p-2$, e così via..

Alla fine troviamo

$$a^{p-1} \equiv 1 \qquad (p)$$

come volevamo dimostrare. □

Diamo adesso una diversa dimostrazione del piccolo teorema di Fermat dovuta ad Eulero.

DIMOSTRAZIONE. Per prima cosa dimostriamo che p divide $\binom{p}{i}$ quando $0 < i < p$. Infatti sappiamo dalla (2.2) che

$$\binom{p}{i} i!\ (p-i)! = p!$$

Ora p, che divide il membro di destra, deve dividere il membro di sinistra. Poiché p è primo con $i!\ (p-i)!$ (visto che si tratta del prodotto di numeri positivi strettamente minori di p) possiamo dedurre, per il Teorema 2.2, che p divide $\binom{p}{i}$.

A questo punto possiamo osservare che, dato un numero intero a, lo sviluppo del binomio $(1+a)^p$ ha, modulo p, una scrittura molto semplificata. Infatti, usando (2.1) vale

$$(1+a)^p = \sum_{i=0}^{p} \binom{p}{i} a^i \equiv a^p + 1^p \equiv a^p + 1 \qquad (p)$$

dato che, appunto, p divide tutti i coefficienti $\binom{p}{i}$ $(0 < i < p)$.

Ora proviamo che, per ogni $a \in \mathbb{Z}$ vale

$$a^p \equiv a \quad (p)$$

Questa relazione, nel caso in cui a non è multiplo di p, ci dà (dividendo per a) l'enunciato del teorema.

Ci basta dimostrare che, per ogni $a \in \mathbb{N}$,

$$a^p \equiv a \quad (p)$$

(il caso dei numeri negativi si ricava poi immediatamente).

Lo dimostriamo per induzione su a.

Il caso base, per $a = 0$,

$$0^p \equiv 0 \quad (p)$$

è banale.

Supponiamo ora che questa relazione sia vera fino ad $a = n$ e proviamo a dimostrare che

$$(n+1)^p \equiv n+1 \quad (p)$$

(se ci riusciamo la nostra dimostrazione è terminata).

Ora, per quanto visto sopra possiamo scrivere che

$$(n+1)^p \equiv n^p + 1 \quad (p)$$

Ma, per ipotesi induttiva, $n^p \equiv n \quad (p)$ per cui

$$(n+1)^p \equiv n+1 \quad (p)$$

□

Mostriamo nel seguente esempio una importante applicazione del piccolo teorema di Fermat al calcolo veloce di potenze modulo un numero primo.

Esempio 3.13. Se vogliamo calcolare

$$15^{1443} \equiv ? \quad (17)$$

possiamo utilizzare il piccolo teorema di Fermat che ci dice che

$$15^{16} \equiv 1 \quad (17).$$

Ora $1443 = 16 \cdot 90 + 3$ dunque

$$15^{1443} \equiv (15^{16})^{90}\, 15^3 \equiv 1^{90}\, 15^3 \quad (17).$$

Ma $15 \equiv -2 \quad (17)$ dunque

$$15^{1453} \equiv (-2)^3 \equiv -8 \equiv 9 \quad (17).$$

Esempio 3.14. Attenzione, se il modulo non è primo, l'enunciato del piccolo teorema di Fermat non vale più: non è vero, per esempio, che $2^5 \equiv 1 \quad (6)$. Infatti

$$2^5 = 32 \equiv 2 \quad (6).$$

Dal piccolo teorema di Fermat si ricava subito questo corollario:

Corollario 3.15. *Se p è un numero primo, per ogni numero intero a vale*

$$a^p \equiv a \quad (p).$$

Dimostrazione. Se a non è multiplo di p per il piccolo teorema di Fermat vale

$$a^{p-1} \equiv 1 \quad (p)$$

da cui si ottiene la tesi moltiplicando per a entrambi i membri. È poi immediato verificare che se $a \equiv 0 \quad (p)$ allora la tesi è vera.

□

Questo ci dà un criterio per decidere se un numero non è primo:

Corollario 3.16. *Se $n > 1$ è un numero intero tale che per qualche numero intero a vale*

$$a^n \not\equiv a \quad (n)$$

allora n non è primo.

Dimostrazione. Si tratta della contronominale del corollario precedente. □

È interessante capire se con questi ragionamenti si può trovare un criterio per dire con certezza se un numero è primo (non solo per dire se un numero NON è primo). Saremmo infatti tentati di pensare che se prendiamo un numero intero $n > 1$ e scopriamo che per tutti i numeri interi a vale

$$a^n \equiv a \quad (n)$$

allora n è primo. Questo non è vero: ci sono infiniti numeri che soddisfano questa proprietà ma non sono primi. Si chiamano *numeri di Carmichael*[4] o *falsi primi*.

Esercizio 3.17. Dimostrare che 561 è un numero di Carmichael (è il più piccolo esistente).

Esercizio 3.18. Dimostrare che 1105 e 1729 sono numeri di Carmichael (sono il secondo e il terzo nella lista dei numeri di Carmichael).

[4]Robert Carmichael, matematico americano, 1878-1967.

4. Un interessante risvolto applicativo: il metodo di crittografia RSA

Consideriamo due numeri primi distinti p e q, e prendiamo un numero e che sia primo con $(p-1)(q-1)$. Sappiamo dunque che e è invertibile modulo $(p-1)(q-1)$, e chiamiamo d un suo inverso.

La seguente semplice proposizione è il cuore del metodo di crittografia che vogliamo descrivere:

PROPOSIZIONE 3.19. *Dati p, q, e, d come sopra, per ogni numero m con $0 \leq m < pq$ vale*

$$(m^e)^d \equiv m \quad (pq).$$

DIMOSTRAZIONE. Osserviamo che per il teorema cinese del resto l'equazione

$$x \equiv m \quad (pq)$$

è equivalente al sistema

$$\begin{cases} x \equiv m & (p) \\ x \equiv m & (q) \end{cases}.$$

Dunque ci basta dimostrare che $(m^e)^d$ è una soluzione del sistema.

Verifichiamo che $(m^e)^d$ è soluzione della prima equazione (per la seconda equazione si procederà in maniera del tutto analoga), ossia verifichiamo che è vera la congruenza:

$$(m^e)^d \equiv m \quad (p)$$

Ora, se $p|m$ la congruenza appena scritta diventa $0 \equiv 0 \quad (p)$ che è vera.

Se invece $p \nmid m$ allora possiamo applicare il piccolo teorema di Fermat. Infatti per costruzione

$$ed \equiv 1 \qquad ((p-1)(q-1))$$

dunque possiamo scrivere

$$ed = 1 + k(p-1)(q-1)$$

per un certo intero k.

Allora

$$(m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} \equiv m \quad (p)$$

dove abbiamo usato il piccolo teorema di Fermat per dire che $m^{p-1} \equiv 1 \quad (p)$.

□

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman inventarono un metodo (detto RSA dalle iniziali dei loro cognomi) per scambiarsi messaggi criptati il cui funzionamento può essere schematicamente riassunto nel seguente modo.[5]

Supponiamo che A voglia inviare un messaggio segreto a B (non occorre pensare a chissà quali contesti di spionaggio e controspionaggio, A per esempio potremmo essere noi mentre digitiamo il codice della nostra carta di credito per fare un acquisto online).

Innanzitutto B ha scelto due numeri primi distinti p e q molto grandi (attualmente si scelgono numeri di circa seicento cifre: osserviamo che la ricerca di numeri primi grandi è un problema matematico di per sé interessante, che ha dunque anche una importante applicazione).

Visto che conosce p e q, B conosce anche $p-1$ e $q-1$ e può dunque facilmente scegliere e e d con le caratteristiche illustrate in questo paragrafo.

[5]Per coloro che sono interessati ad una introduzione divulgativa (non tecnica) alla storia della crittografia fin dalle origini, segnaliamo il libro di S. Singh *Codici e Segreti*.

A questo punto B consegna ad A i numeri pq ed e. Anzi, li può addirittura rendere pubblici, in modo che altri possano inviargli messaggi crittati, non solo A.

Quando A vuole inviare un messaggio, questo messaggio può essere facilmente codificato da un numero m con $0 < m < pq$ (se è un messaggio numerico è già un numero, se è un messaggio con lettere, si può certo trovare un modo di associare ad ogni lettera un numero, dunque il messaggio finale risulterà un numero m, magari molto grande, ottenuto scrivendo uno accanto all'altro tutti i numeri che rappresentano le lettere).[6]

A questo punto A non invia il numero m, ma calcola m^e modulo pq e invia dunque un numero c con $0 < c < pq$ e $c \equiv m^e \pmod{pq}$.

Dunque B riceve il messaggio c. Per decodificarlo calcolerà c^d modulo pq e, per la Proposizione 3.19, ritroverà il messaggio originale m.

Come mai questo sistema è efficace? Ricordiamo che solo B conosce il numero d, e il punto è proprio questo. Il numero d è stato ricavato da e e dalla conoscenza dei numeri $p-1$ e $q-1$, mentre sono pubblici solo i numeri e e il **prodotto** pq. Per ricavare $p-1$ e $q-1$ conoscendo il prodotto pq bisognerebbe saper fattorizzare pq, e questa è una operazione che, al giorno d'oggi, con numeri così grandi, non è possibile eseguire in tempo utile.[7] E non esiste per il momento neppure nessun altro metodo che permetta, dato un numero c che sappiamo essere congruo modulo pq ad una potenza e-esima di un certo numero ignoto, di ritrovare in tempo utile questo numero ignoto.[8]

Nelle poche righe precedenti abbiamo descritto in maniera schematica il metodo RSA, senza discutere le molte accortezze tecniche che occorre usare nella pratica, che non competono a questo corso ma ad un corso di crittografia. Ad ogni modo, una volta che viene applicato con tutte le accortezze del caso, il metodo RSA è ritenuto molto affidabile.

Abbiamo fatto solo un primo accenno alle complesse problematiche della crittografia, ma per voi che intraprendete la carriera di matematici può essere interessante sapere che un teorema di aritmetica elementare, semplice ma profondo, come il piccolo teorema di Fermat, ha ripercussioni applicative così importanti.

Esercizio 3.20. In una prova didattica del metodo RSA, Bob sceglie i numeri primi $p = 7$ e $q = 13$, e rende pubblici il prodotto $pq = 91$ e l'esponente $e = 5$. Riceve da Alice il messaggio 44.
a) Qual è l'esponente 'segreto' d a cui Bob deve elevare 44 per riottenere il messaggio originale?
b) Qual è il messaggio originale m che è stato inviato?

Esercizio 3.21. In una prova didattica del metodo RSA, Bob sceglie i numeri primi $p = 11, q = 19$ e rende pubblici il loro prodotto $n = 209$ e l'esponente $e = 53$. Alice manda a Bob il messaggio cifrato $c = 162$.
a) Qual è l'esponente 'segreto' d al quale Bob deve elevare 162 per decriptare il messaggio?
b) Qual è il messaggio originale m?

[6] Ricordiamo che pq è molto grande, dunque c'è spazio per codificare anche messaggi molto lunghi. Altrimenti A dovrà spezzare il suo messaggio e inviare vari numeri m_1, m_2 etc...

[7] Per vostro divertimento, potete informarvi sul *RSA Factory Challenge* a questo link: https://it.wikipedia.org/wiki/RSA_Factoring_Challenge.

[8] Se siete curiosi potete dare un'occhiata all'articolo *RSA problem* di Rivest e Kaliski: https://people.csail.mit.edu/rivest/RivestKaliski-RSAProblem.pdf.

5. Le classi di resto modulo un intero positivo. Struttura additiva e moltiplicativa.

Cominciamo con un esempio. Consideriamo i possibili resti della divisione euclidea di un numero intero per 10. Abbiamo 10 possibilità: resto uguale a 0,1,2,3,..., 9. Quali sono i numeri che danno resto 1? Eccone alcuni: $1, 11, 21, 31, \ldots, -9, -19, -29, -39, -49 \ldots$.

Chiamiamo $[1]_{10}$ l'insieme costituito da questi numeri:

$$[1]_{10} = \{x \in \mathbb{Z} \mid x \equiv 1 \quad (10)\}.$$

Analogamente, chiamiamo $[2]_{10}$ l'insieme dei numeri interi la cui divisione per 10 dà resto 2, e in generale, per $i = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, chiamiamo $[i]_{10}$ l'insieme dei numeri interi la cui divisione per 10 dà resto i.

Gli insiemi $[0]_{10}$, $[1]_{10}$, $[2]_{10}$,..., $[9]_{10}$ si chiamano "classi di resto modulo 10"; la loro unione è uguale a tutto $\mathbb{Z}$ giacché ogni numero intero appartiene ad una (e ad una sola) delle classi. Chiamiamo ora $\mathbb{Z}_{10}$ l'insieme i cui elementi sono tutte le classi di resto modulo 10:

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, \ldots, [9]_{10}\}.$$

Possiamo arricchire questo insieme definendo due operazioni, una somma e una moltiplicazione.

Prima estendiamo la nostra notazione: fin qui per esempio non abbiamo definito il simbolo $[11]_{10}$. Infatti abbiamo preso in considerazione solo simboli in cui fra le parentesi quadre c'è un resto 0,1,..., 9 di una divisione euclidea per 10. Decidiamo di accettare anche $[11]_{10}$ intendendo che $[11]_{10} = [1]_{10}$. E anche, per esempio, $[127]_{10} = [7]_{10}$. Insomma ci mettiamo d'accordo di poter indicare una classe di resto $[i]_{10}$ anche col simbolo $[s]_{10}$ dove s è un qualunque numero intero tale che

$$s \equiv i \quad (10).$$

Ora siamo pronti a definire la somma e la moltiplicazione di elementi di $\mathbb{Z}_{10}$. Poniamo:

$$[a]_{10} \cdot [b]_{10} = [ab]_{10}$$

$$[a]_{10} + [b]_{10} = [a + b]_{10}.$$

Per esempio:

$$[7]_{10} \cdot [5]_{10} = [35]_{10} = [5]_{10}$$

$$[6]_{10} + [8]_{10} = [14]_{10} = [4]_{10}.$$

Insomma in $\mathbb{Z}_{10}$ "sette" per "cinque" fa "cinque" e "sei" più "otto" fa "quattro".

In realtà, per essere sicuri di aver definito una buona somma e una buona moltiplicazione, bisogna verificare che, se

$$[a]_{10} = [a']_{10}$$

$$[b]_{10} = [b']_{10}$$

allora

$$[a]_{10} \cdot [b]_{10} = [a']_{10} \cdot [b']_{10}$$

$$[a]_{10} + [b]_{10} = [a']_{10} + [b']_{10}$$

insomma che queste operazioni non dipendono dai numeri a e b che mettiamo fra parentesi quadre ma solo dalle loro classi di resto.

ESERCIZIO 3.22. Fate questa verifica. (Suggerimento: visto che $[a]_{10} = [a']_{10}$ allora sarà $a' = a + 10k$ e analogamente $b' = b + 10t$. Dunque per esempio, per quel che riguarda la moltiplicazione, vale $[a']_{10} \cdot [b']_{10} = [(a+10k)(b+10t)]_{10} = [ab + 10bk + 10at + 100kt]_{10} = [ab]_{10} = [a]_{10}[b]_{10}$.)

Con queste operazioni l'insieme $\mathbb{Z}_{10}$ diventa un "anello commutativo con unità". Discuteremo la definizione formale di anello (anche se forse l'avete già vista a Geometria 1) in uno dei prossimi capitoli.

Intanto osserviamo che la somma e la moltiplicazione che abbiamo definito hanno molte delle buone proprietà a cui "siamo abituati" dalla moltiplicazione e dalla somma in $\mathbb{Z}$ (proprietà commutativa e associativa di entrambe le operazioni, proprietà distributive, esistenza dell'elemento neutro per entrambe operazioni, esistenza dell'opposto rispetto alla somma..).

C'è però una cosa nuova in $\mathbb{Z}_{10}$, rispetto a $\mathbb{Z}$. Vale infatti

$$[2]_{10} \cdot [5]_{10} = [10]_{10} = [0]_{10}$$

ossia il prodotto di due elementi diversi da $[0]_{10}$ ha come risultato $[0]_{10}$ (mentre in $\mathbb{Z}$ il prodotto di due interi diversi da zero è sempre diverso da 0). Si dice a questo proposito che $[2]_{10}$ e $[5]_{10}$ sono due *divisori dello zero* in $\mathbb{Z}_{10}$.

Passiamo al caso generale. Sia m un numero intero positivo.
Per ogni $i = 0, 1, 2, \ldots, m-1$ chiamiamo $[i]_m$ la "classe di resto di i modulo m", ossia l'insieme dei numeri che danno resto i quando si considera la loro divisione euclidea per m:

$$[i]_m = \{x \in \mathbb{Z} \mid x \equiv i \pmod{m}\}.$$

Come nell'esempio in cui $m = 10$, osserviamo che le classi di resto modulo m forniscono una *partizione* di $\mathbb{Z}$, ossia sono a due a due disgiunte e la loro unione è uguale a $\mathbb{Z}$.
Chiamiamo $\mathbb{Z}_m$ l'insieme di tutte le classi di resto modulo m:[9]

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Si tratta dunque un insieme di cardinalità m.

Come sopra adottiamo la convenzione per cui possiamo indicare la classe $[i]_m$ anche col simbolo $[s]_m$ dove s è un qualunque numero intero tale che

$$s \equiv i \pmod{m}$$

Per esempio, con $m = 37$:

$$[5]_{37} = [42]_{37} = [412]_{37}.$$

Possiamo allora definire la somma e la moltiplicazione di elementi di $\mathbb{Z}_m$:

$$[a]_m \cdot [b]_m = [ab]_m$$

$$[a]_m + [b]_m = [a+b]_m.$$

Anche questa volta si verifica (fate di nuovo il facile esercizio!) che queste operazioni sono ben definite e che non dipendono dai numeri a e b ma solo delle loro classi di resto, e $\mathbb{Z}_m$ risulterà un anello commutativo con unità.

[9] In vari testi trovate questo insieme indicato con il simbolo $\mathbb{Z}/m\mathbb{Z}$.

OSSERVAZIONE 3.23. Il piccolo teorema di Fermat si può esprimere in modo equivalente utilizzando le classi di resto nel seguente modo: dato p primo, e data la classe $[a]_p$ in $\mathbb{Z}_p$ con $[a]_p \neq [0]_p$ vale che

$$[a]_p^{p-1} = [1]_p$$

Da questo segue in particolare che per ogni classe $[a]_p$ in $\mathbb{Z}_p$ con $[a]_p \neq [0]_p$ esiste un minimo intero positivo b tale che $[a]_p^b = [1]_p$ (certamente $b \leq p-1$). Anticipando una terminologia che verrà introdotto nel prossimo capitolo in un contesto più generale, chiameremo b l'*ordine* moltiplicativo di $[a]_p$ in $\mathbb{Z}_p$. È facile osservare fin d'ora che b ha questa proprietà: se per un certo intero positivo m vale $[a]_p^m = [1]_p$ allora $b|m$ (per dimostrarlo: fate la divisione euclidea $m = qb + r$ e ricavate subito che $[a]_p^r = [1]_p$, a questo punto deducete che r deve essere 0, altrimenti verrebbe contraddetta la minimalità di b). In particolare b divide $p-1$. Questa osservazione sarà utile nel risolvere alcuni degli esercizi del prossimo paragrafo.

6. Esercizi

ESERCIZIO 3.24. a) Trovare il numero naturale m tale che $0 \leq m < 13$ e

$$[2^{(2^{10})}]_{13} = [m]_{13}$$

b) Trovare il numero naturale k tale che $0 \leq k < 3$ e

$$[(138139140141 \ldots 999)^{1987} - 1]_3 = [k]_3$$

ESERCIZIO 3.25. Consideriamo la funzione $g : \mathbb{Z}_5 \times \mathbb{Z}_5 \to \mathbb{Z}_5 \times \mathbb{Z}_5$ che è definita dalla seguente relazione:

$$\forall\ [a],\ [b] \in \mathbb{Z}_5, \quad g(([a],[b])) = ([a-3b],[a+3b])$$

Dire se g è iniettiva, surgettiva, bigettiva.

ESERCIZIO 3.26. a) Trovare l'insieme delle soluzioni della congruenza lineare:

$$327\ x \equiv 416 \qquad \mod (52)$$

b) Dire se la funzione $f : \mathbb{Z}_{52} \to \mathbb{Z}_{52}$ data da

$$f([x]) = [15x]$$

è iniettiva, surgettiva, bigettiva.

ESERCIZIO 3.27 (Teorema di Wilson[10]). Dimostrare che, se p è primo, vale

$$(p-1)! \equiv -1 \qquad (p)$$

Se invece m è un numero non primo, la congruenza

$$(m-1)! \equiv -1 \qquad (m)$$

è vera o falsa?

ESERCIZIO 3.28. Sia p un numero primo dispari. Dimostrare che se $[-1]$ è un quadrato in $\mathbb{Z}_p$ allora p è congruo a 1 modulo 4.

ESERCIZIO 3.29. Dimostrare che, preso un numero primo $p \equiv 1 \bmod 4$ allora

$$\left(\left(\frac{(p-1)}{2}\right)!\right)^2 \equiv -1 \bmod p$$

[10]John Wilson, matematico inglese, 1741-1793.

Esercizio 3.30. Dimostrare che esistono infiniti numeri primi congrui a 1 modulo 4.

Soluzione: [Traccia] Se fossero finiti, diciamo $p_1, p_2, \ldots, p_N$, potremmo considerare il numero $4(p_1 p_2 \cdots p_N)^2 + 1$... □

Esercizio 3.31. Dimostrare che, per ogni $n \in \mathbb{N} - \{0\}$, $17^{16^n} \equiv 4 \mod 7$.

Esercizio 3.32. a) Quante sono tutte le possibili funzioni $f : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$?
b) Quanti sono gli elementi invertibili di $\mathbb{Z}_{15}$? E quelli invertibili di $\mathbb{Z}_{20}$?
c) Quante sono le funzioni $g : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ che mandano elementi invertibili di $\mathbb{Z}_{15}$ in elementi invertibili di $\mathbb{Z}_{20}$?
d) Quante sono le funzioni iniettive $h : \mathbb{Z}_{15} \to \mathbb{Z}_{20}$ che mandano elementi invertibili di Z_{15} in elementi invertibili di $\mathbb{Z}_{20}$?

Esercizio 3.33. Dimostrare che esiste un multiplo di 174 nella cui scrittura decimale appare solo la cifra 6.
[Traccia: $174 = 6 \cdot 29$. C'è un n tale che il numero 66666...66 (il 6 compare n volte) sia divisibile per 174 ? Basta scoprire quando il numero 11111...11 (l'1 compare n volte) è divisibile per 29. Ora, $11111...11 = 1 + 10 + 10^2 + \cdots + 10^{n-1} = \frac{10^n - 1}{10 - 1}$...]

Esercizio 3.34. Sia n un intero positivo dispari la cui espressione decimale non termina per 5. Dimostrare che c'è un multiplo di n che in base dieci si scrive utilizzando solo la cifra 1.

Esercizio 3.35. Qual è l'ultima cifra del numero 3^{13452} scritto in base 10? E del numero 6^{245389}?

Esercizio 3.36. Dimostrare che, per ogni numero naturale n, $n(n^6 - 1)$ è divisibile per 42.

Esercizio 3.37. Dimostrare che, per ogni intero positivo n, $2^{3n+3} - 7n - 8$ è divisibile per 49.

Esercizio 3.38. a) Consideriamo l'insieme $Q = \{a^2 \mid a \in \mathbb{Z}\}$ di tutti i quadrati degli interi. Per ogni primo dispari p, sia R_p l'insieme dei resti delle divisioni degli elementi di Q per p. Dimostrare che R_p ha esattamente $\frac{p+1}{2}$ elementi.
b) Dimostrare che per ogni primo dispari p esistono due interi a e b tali che p divide $a^2 + b^2 + 4$.

Esercizio 3.39 (Difficile). Siano m, n due interi positivi primi fra loro. Dimostrare che

$$\sum_{k=1}^{n-1} \left\lfloor \frac{km}{n} \right\rfloor = \frac{(n-1)(m-1)}{2}$$

dove il simbolo $\lfloor\ \rfloor$ indica la parte intera inferiore.

Esercizio 3.40 (Difficile). Dimostrare che non esiste nessuna funzione $f : \mathbb{N} \to \mathbb{N}$ tale che, per ogni $n \in \mathbb{N}$

$$f(f(n)) = n + 2023$$

Esiste una simile funzione se nella formula precedente si sostituisce 2023 con 2022 ?

Esercizio 3.41 (Difficile). Sia $\mathcal{F}_n$ l'ennesimo numero di Fermat (vedi l'Esercizio 2.40)[11]. Dimostrare che, se q è un primo che divide $\mathcal{F}_n$, allora

$$q \equiv 1 \bmod 2^{n+1}$$

Esercizio 3.42 (Più difficile del precedente). Proviamo a migliorare il risultato dell'esercizio precedente, dimostrando la seguente osservazione, dovuta a Lucas: se q è un primo che divide $\mathcal{F}_n$, con $n > 1$, allora

$$q \equiv 1 \bmod 2^{n+2}$$

Esercizio 3.43 (Difficile). Sia $p > 3$ un numero primo. Scriviamo

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{(p-1)!}$$

Dimostrare che p^2 divide a.

Esercizio 3.44 (Difficile, è una versione debole del teorema di Dirichlet). Sia p un numero primo, sia n un intero positivo, e sia

$$N = \frac{(np)^p - 1}{np - 1}$$

(1) Dimostrare che $MCD(N, np-1) = 1$.
(2) Sia q un primo che divide N. Dimostrare che np è primo con q e determinare l'ordine moltiplicativo di $[np]_q$.
(3) Sia q un primo che divide N. Dimostrare che $q \equiv 1 \quad (p)$.
(4) Dimostrare che esistono infiniti numeri primi congrui a 1 modulo p.

[11] Il risultato di questo esercizio potrebbe fornire una spiegazione di come mai Eulero ha saputo trovare facilmente il numero primo 641 che divide $\mathcal{F}_5$: per cercare un eventuale primo che divide $\mathcal{F}_5$ basta cercare fra i numeri primi congrui a 1 modulo $2^6 = 64$ o, se dimostrate anche il risultato del prossimo esercizio, addirittura fra i numeri primi congrui a 1 modulo $2^7 = 128$.

CAPITOLO 4

Gruppi

1. Gruppi e sottogruppi: prime proprietà

Cominciamo subito scrivendo la definizione formale di gruppo (la avete in realtà già vista a Geometria 1).

DEFINIZIONE 4.1. Un *gruppo* G è un insieme non vuoto dotato di una operazione che ad ogni coppia di elementi $a, b \in G$ associa un elemento di G indicato con $a \cdot b$ e ha le seguenti proprietà:

(1) dati $a, b, c \in G$ vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (proprietà associativa);
(2) esiste un elemento $e \in G$ tale che $a \cdot e = e \cdot a = a$ per ogni $a \in G$ (esistenza dell'elemento neutro, detto anche identità, in G);
(3) per ogni $a \in G$ esiste un elemento $a^{-1} \in G$ tale che $a \cdot a^{-1} = a^{-1} \cdot a = e$ (esistenza dell'inverso in G).

Un gruppo si dice *commutativo* o *abeliano*[1] se, per ogni $a, b \in G$ vale $a \cdot b = b \cdot a$. Un gruppo G si dice finito se l'insieme G ha cardinalità finita.

ESEMPIO 4.2. Ecco alcuni esempi, e controesempi, familiari.

L'insieme $\mathbb{Z}$ considerato con l'operazione + è un gruppo commutativo infinito; rispetto alla moltiplicazione, invece, non è un gruppo perché solo gli elementi 1 e -1 hanno un inverso. L'insieme $\mathbb{N}$ non è un gruppo né con l'addizione né con la moltiplicazione. I campi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sono gruppi commutativi rispetto all'addizione, mentre gli insiemi $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$,$\mathbb{C} - \{0\}$ sono gruppi commutativi rispetto alla moltiplicazione.

Ogni spazio vettoriale V è un gruppo commutativo rispetto alla addizione. In particolare l'insieme $Mat_{m\times n}(K)$ delle matrici $m \times n$ a coefficienti in un campo K è un gruppo commutativo rispetto alla operazione di somma fra matrici.

Osserviamo inoltre che l'insieme $Mat_{n\times n}(K)^*$ delle matrici $n \times n$ *invertibili* a coefficienti in un campo K è un gruppo rispetto all'operazione di prodotto fra matrici. Si tratta di un gruppo non commutativo (se $n \geq 2$).

OSSERVAZIONE 4.3. D'ora in avanti, quando parleremo di un gruppo, ometteremo, tutte le volte che sarà possibile farlo senza creare ambiguità, il simbolo $\cdot$ per la moltiplicazione; scriveremo dunque ab invece di $a \cdot b$, $a^2 = aa$ invece di $a \cdot a$. Inoltre nel fare il prodotto fra n elementi del gruppo scriveremo spesso $a_1 a_2 \cdots a_n$ omettendo le parentesi, visto che vale la proprietà associativa (una facile induzione su n ci mostra che il risultato del prodotto non dipende da come erano collocate le parentesi).

Il seguente teorema, semplice ma importante, mette in luce alcune prime proprietà dei gruppi che derivano immediatamente dalla definizione.

TEOREMA 4.4. *Dimostrare che, se G è un gruppo, allora*

(1) *C'è un solo elemento neutro e.*
(2) *Per ogni $a \in G$ c'è un unico inverso di a.*

[1] In onore di Niels Henrik Abel, matematico norvegese, 1802-1829.

(3) *Per ogni* $a \in G$ *vale* $(a^{-1})^{-1} = a$.
(4) *Per ogni* $a, b \in G$ *vale* $(ab)^{-1} = b^{-1}a^{-1}$.
(5) *Siano* a, b, c *elementi di* G. *Allora l'equazione* $axb = c$ *ha un'unica soluzione* $x = a^{-1}cb^{-1}$ *in* G.

DIMOSTRAZIONE. (1) Supponiamo che ci siano due elementi neutri e ed e'. Allora possiamo scrivere, che $e = ee' = e'$ dove per il primo $=$ abbiamo sfruttato la proprietà di elemento neutro di e' (abbiamo infatti moltiplicato a destra per e') e per il secondo $=$ abbiamo sfruttato la proprietà di elemento neutro di e (abbiamo moltiplicato e' a sinistra per e).
(2) Siano h e k due inversi di a. Allora

$$h = he = h(ak) = (ha)k = ek = k$$

(3) Osserviamo che $(g^{-1})^{-1}g^{-1} = g^{-1}(g^{-1})^{-1} = e$ per definizione di $(g^{-1})^{-1}$. Ma sappiamo anche che $gg^{-1} = g^{-1}g = e$ per definizione di g^{-1}. Dunque osserviamo che sia g sia $(g^{-1})^{-1}$ sono inversi di g^{-1}. Per l'unicità dell'inverso stabilita nel punto (2) possiamo concludere che $g = (g^{-1})^{-1}$.
(4) Basta verificare che $b^{-1}a^{-1}$ è un inverso di ab. Lo faremo moltiplicandolo a sinistra (la dimostrazione moltiplicandolo a destra è analoga).

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$$

dove abbiamo usato in maniera sostanziale la proprietà associativa.
(5) Un elemento $\overline{x}$ soddisfa l'equazione $axb = c$ se e solo se vale $a\overline{x}b = c$. Questa uguaglianza è vera se e solo se è vera $\overline{x}b = a^{-1}c$, come si vede moltiplicando ognuno dei due membri, a sinistra, per a^{-1}. Moltiplicando ognuno dei due membri, a destra, per b^{-1} si vede che questa uguaglianza a sua volta è vera se e solo se è vera $\overline{x} = a^{-1}cb^{-1}$. Dunque le soluzioni della equazione $axb = c$ coincidono con le soluzioni della equazione $x = a^{-1}cb^{-1}$, che, come si vede, sono una sola, ossia $a^{-1}cb^{-1}$.

□

Fra i sottoinsiemi di G rivestono un ruolo particolare quelli che, rispetto all'operazione $\cdot$, sono a loro volta dei gruppi:

DEFINIZIONE 4.5. Un *sottogruppo* H di un gruppo G è un sottoinsieme di G che soddisfa le tre seguenti proprietà:

(1) $e \in H$
(2) $a, b \in H \Rightarrow ab \in H$
(3) $a \in H \Rightarrow a^{-1} \in H$

Per indicare che H è un sottogruppo di G si scrive $H < G$.

OSSERVAZIONE 4.6. In particolare, fra i sottogruppi di un gruppo G ci sono sempre G stesso e il sottogruppo banale $\{e\}$.

Indichiamo subito un importante sottogruppo:

DEFINIZIONE 4.7 (Centro di un gruppo). Dato un gruppo G si chiama *centro* di G il sottoinsieme formato dagli elementi che commutano con tutti gli elementi del gruppo:

$$Z(G) = \{g \in G \mid gh = hg \quad \forall h \in G\}$$

ESERCIZIO 4.8. Dimostrare che $Z(G)$ è un sottogruppo di G.

Osserviamo che se il gruppo G è abeliano allora $Z(G) = G$.

ESEMPIO 4.9. Sia a un elemento di un gruppo G. Consideriamo il sottoinsieme di G

$$(a) = \{a^i \mid i \in \mathbb{Z}\}$$

Spieghiamo bene la notazione. Se $s > 0$ con a^s si intende, come immaginate, il prodotto di a per se stesso s volte. Poi si pone $a^0 = e$. Inoltre se $i > 0$ e scriviamo a^{-i} intendiamo $(a^{-1})^i$. Per il punto (4) del Teorema 4.4 questo è uguale a $(a^i)^{-1}$ (per esempio $a^{-2} = a^{-1}a^{-1} = (a^2)^{-1}$). Il sottoinsieme (a) è un sottogruppo di G e si chiama *sottogruppo ciclico generato da* a. Dalla descrizione data sopra segue che per la moltiplicazione fra elementi di (a) vale la classica regola dell'esponenziale: per ogni $i, j \in \mathbb{Z}$ abbiamo $a^i\, a^j = a^{i+j}$. In particolare (a) è un gruppo commutativo (e rimarchiamo che è un sottogruppo di G, che potrebbe non essere commutativo).

I sottogruppi ciclici di $\mathbb{Z}$ (con l'operazione +) sono, al variare di $m \in \mathbb{Z}$, i sottogruppi

$$(m) = \{km \mid k \in \mathbb{Z}\}$$

che per $m > 0$ coincidono, usando la notazione della scorsa lezione, con le classi di resto $[0]_m$, mentre per $m = 0$ troviamo il sottogruppo 'banale' $\{0\}$.

Concludiamo il paragrafo mettendo in luce con una definizione una famiglia importante di gruppi:

DEFINIZIONE 4.10. Se, per qualche $a \in G$ vale $G = (a)$ allora si dice che G è un *gruppo ciclico*.

ESEMPIO 4.11. Il gruppo $\mathbb{Z}$, con l'operazione di somma, è ciclico, infatti vale $\mathbb{Z} = (1)$ o anche $\mathbb{Z} = (-1)$. Il gruppo $\mathbb{Z}_{20}$, con l'operazione di somma, è ciclico, infatti vale $\mathbb{Z}_{20} = ([1]_{20})$ ma anche per esempio $\mathbb{Z}_{20} = ([3]_{20})$. In generale, per $m \geq 2$, $\mathbb{Z}_m$ con l'operazione di somma, è ciclico, e vale $\mathbb{Z}_m = ([a]_m)$ dove a è un qualunque numero primo con m (scrivete la breve dimostrazione!).

2. Un esempio importante: il gruppo simmetrico

In questo paragrafo presenteremo un importante esempio di gruppo: il gruppo simmetrico. In classe abbiamo descritto in dettaglio S_3, qui nelle dispense tratteremo il caso generale.

DEFINIZIONE 4.12. Dato un numero intero positivo n, una *permutazione dei numeri* $1, 2, \ldots, n$ è una funzione f bigettiva dall'insieme $\{1, 2, \ldots, n\}$ in se stesso. Chiamiamo S_n l'insieme di tali permutazioni.

Osserviamo che l'insieme S_n ha $n!$ elementi. Inoltre, poiché sappiamo che la composizione fra funzioni è associativa, e che una funzione è bigettiva se e solo se ammette un'inversa, è immediato verificare che S_n, con il prodotto dato dalla composizione fra funzioni, è un gruppo.

DEFINIZIONE 4.13. Chiameremo S_n il *gruppo simmetrico* su n elementi.

2.1. La rappresentazione di una permutazione mediante la decomposizione in cicli disgiunti. Per descrivere le permutazioni è molto utile avere a disposizione una notazione efficiente. Una prima possibilità è illustrata dal seguente esempio. Sia $n = 9$; allora col simbolo

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 1 & 7 & 2 & 8 & 5 & 9 \end{pmatrix}$$

indichiamo la permutazione che manda ogni numero in quello che sta sotto di lui: per esempio 1 va in 3, 2 in 4, 3 in 6, 4 in 1, 5 in 7, e così via.

Un altro modo di rappresentare la stessa permutazione è la *decomposizione in cicli disgiunti*:

$$f = (1,3,6,2,4)(5,7,8)(9).$$

Questa scrittura va letta così: il primo ciclo (la prima parentesi) ci dice che la f manda 1 in 3, 3 in 6, 6 in 2, 2 in 4 e 4 in 1, ossia ogni elemento viene mandato in quello che lo segue, tranne l'ultimo, che viene rimandato nel primo (ecco perché si chiamano 'cicli'). Il secondo ciclo dice che 5 viene mandato in 7, 7 in 8 e 8 in 5. L'ultimo ciclo dice che 9 viene mandato in se stesso, ossia viene lasciato fisso dalla f.

Di solito quando un elemento viene lasciato fisso non lo indichiamo; dunque possiamo indicare f anche con la scrittura

$$f = (1,3,6,2,4)(5,7,8)$$

Osservazione 4.14. È facile dimostrare che, data una permutazione f, la si può sempre scrivere come decomposizione di cicli disgiunti (l'aggettivo 'disgiunti' si riferisce, come avrete intuito, al fatto che ogni numero compare al più in un solo ciclo). Infatti si crea tale decomposizione come risultato di un algoritmo finito: si apre un ciclo, per esempio, come sopra, $(1,3,6....$, e i numeri che compaiono, dopo il primo, sono tutte immagini del numero precedente. Per esempio $3 = f(1), 6 = f(3)$ etc.. Poiché f è una funzione iniettiva, nel procedere con l'algoritmo, ogni volta il numero da inserire sarà o un numero 'nuovo', mai comparso prima, oppure il numero da cui eravamo partiti (nell'esempio: 1). Nel primo caso si continua a completare il ciclo, nel secondo caso si chiude il ciclo e si passa a creare un altro ciclo, finchè non si è descritta completamente la permutazione f.

Osservazione 4.15. La notazione introdotta è molto chiara ma non è unica. Per esempio abbiamo scritto:

$$f = (1,3,6,2,4)(5,7,8)$$

ma avremmo potuto anche scrivere anche

$$f = (5,7,8)(1,3,6,2,4)$$

oppure

$$f = (7,8,5)(6,2,4,1,3)$$

potete infatti facilmente verificare che tutte e tre le scritture qui sopra descrivono la stessa funzione f.

2.2. Composizione di permutazioni: qualche esempio per fare pratica. Per acquisire maggiore familiarità con il prodotto in S_n, ossia con la composizione di permutazioni, facciamo adesso un esempio.

Consideriamo $n = 10$; se f è la permutazione $f = (1,3,6,2,4,7)(5,8,10)$ e g è la permutazione

$$g = (1,3)(2,9)$$

qual è la decomposizione in cicli di $g \circ f$?

In concreto, scriviamo

$$(1,3)(2,9) \circ (1,3,6,2,4,7)(5,8,10)$$

Comporre le funzioni equivale a seguire il 'cammino' di un numero, applicandogli i cicli da destra a sinistra. Per esempio il ciclo più a destra manda il 5 in 8, il secondo ciclo lascia l'8 fisso, il terzo e il quarto anche. Dunque $g \circ f$ manda il 5 in 8. Seguiamo adesso

l'8. Il ciclo più a destra lo manda in 10, il secondo ciclo lascia fisso il 10, e così anche il terzo e il quarto. Dunque per ora abbiamo trovato:

$$g \circ f = (5, 8, 10...$$

Continuiamo: il 10 viene mandato in 5 dal ciclo più a destra, e il 5 vene poi lasciato fisso. Dunque abbiamo chiuso il primo ciclo:

$$g \circ f = (5, 8, 10)...$$

Studiamo adesso l'immagine di un altro numero, per esempio il 2 (in questo momento in realtà siamo liberi di partire da un numero qualunque diverso da 5,8,10). Otteniamo

$$g \circ f = (5, 8, 10)(2, 4...$$

Ora dobbiamo seguire il 4

$$g \circ f = (5, 8, 10)(2, 4, 7...$$

Poi il 7, che viene lasciato fisso dal ciclo più a destra, e viene mandato in 1 dal secondo ciclo. Il terzo ciclo lascia fisso l'1 e il quarto manda 1 in 3. Dunque

$$g \circ f = (5, 8, 10)(2, 4, 7, 3...$$

Continuando così arriviamo a

$$g \circ f = (5, 8, 10)(2, 4, 7, 3, 6, 9)(1) = (5, 8, 10)(2, 4, 7, 3, 6, 9)$$

che è la decomposizione in cicli disgiunti che cercavamo.

Osservazione 4.16. È facile vedere che, se $n \geq 3$, non è detto che $g \circ f = f \circ g$. Basta considerare $f = (1, 2)$, $g = (1, 3)$; possiamo calcolare:

$$g \circ f = (1, 3)(1, 2) = (1, 2, 3)$$

$$f \circ g = (1, 2)(1, 3) = (1, 3, 2)$$

e osservare che la permutazione $(1, 2, 3)$ è diversa da $(1, 3, 2)$.

Osservazione 4.17. In S_8, chiamiamo f_1 la permutazione $f_1 = (1, 3, 6, 2, 4)$ e f_2 la permutazione $f_2 = (5, 7, 8)$. Allora f_1 e f_2 commutano (lo potete verificare pensando che 'muovono' due insiemi di numeri che sono disgiunti fra loro) e vale che $f_1 \circ f_2 = f_2 \circ f_1$ coincide con la permutazione che, scritta nella notazione in cicli disgiunti, indicheremmo come $(1, 3, 6, 2, 4)(5, 7, 8)$. In altre parole, quando scriviamo una permutazione con la notazione dei cicli disgiunti, in realtà potremmo mettere fra un ciclo e l'altro il simbolo $\circ$, perché f è anche uguale al prodotto delle permutazioni corrispondenti a ciascuno dei cicli.

3. Laterali sinistri di un sottogruppo. Il teorema di Lagrange. Ordine di un elemento

Definizione 4.18. Sia G un gruppo, H un sottogruppo di G. Chiameremo *H-laterale sinistro*, o *laterale sinistro di H*, o *classe laterale sinistra di H*, un sottoinsieme di G del tipo:

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

dove $g \in G$.

L'insieme i cui elementi sono gli H-laterali sinistri si indica con G/H e la sua cardinalità $|G/H|$ si chiama *indice* di H in G.

In particolare osserviamo che $eH = H$ ossia H è un particolare H-laterale sinistro. A parte questo caso, i laterali sinistri di H non sono sottogruppi (come potete facilmente verificare nel caso in cui $G = \mathbb{Z}$ con l'operazione + e $H = (m)$ per un certo intero positivo m), ma solo sottoinsiemi di G.

ESEMPIO 4.19. Consideriamo per esempio il gruppo S_3 e il sottogruppo $H = \{e, (1,2)\}$. Si verifica direttamente che i laterali sinistri di H in S_3 sono tre:

$$eH = (1,2)H = \{e, (1,2)\} = H$$

$$(1,3)H = (1,2,3)H = \{(1,3), (1,2,3)\}$$

$$(2,3)H = (1,3,2)H = \{(2,3), (1,3,2)\}$$

Come si intuisce anche dall'esempio qui sopra, gli H-laterali sinistri forniscono una partizione di G, ossia G è unione disgiunta degli H-laterali sinistri. Dedichiamo a questo il seguente:

TEOREMA 4.20. *Ogni elemento w di G è contenuto in uno e un solo H-laterale sinistro: wH.*

DIMOSTRAZIONE. Osserviamo subito che $w \in wH$ visto che $e \in H$ e allora $w = we \in wH$. Supponiamo ora che w appartenga anche al laterale γH, dove $\gamma \in G$. Allora $w = \gamma h_1$ per un certo $h_1 \in H$. Ora osserviamo che il laterale wH e il laterale γH coincidono. Infatti:

$$\gamma H = \{\gamma h \mid h \in H\} = \{\gamma h_1 h \mid h \in H\} = \{wh \mid h \in H\} = wH$$

Il secondo =, quello in blu, va spiegato bene. Il punto è che, al variare di h, gli elementi $h_1 h$ descrivono tutti gli elementi del gruppo H: infatti ogni elemento h_2 appartenente ad H può essere ottenuto come $h_1(h_1^{-1}h_2)$, dove $h_1^{-1}h_2$ appartiene ad H visto che H è un sottogruppo. □

OSSERVAZIONE 4.21. Illustriamo la proposizione precedente anche nel caso in cui $G = \mathbb{Z}$ con l'operazione + e $H = (12)$. Il numero 5 appartiene al laterale $5 + (12)$ che, se ci si pensa, è l'insieme che nella lezione scorsa abbiamo chiamato $[5]_{12}$, la classe (laterale) di resto di 5 modulo 12. Ora 5 appartiene anche al laterale $17 + (12)$ ma si verifica subito che i laterali $5 + (12)$ e $17 + (12)$ coincidono (questo è in accordo con la convenzione che avevamo scelto per cui $[5]_{12} = [17]_{12}$).

In conclusione otteniamo la ben nota partizione di $\mathbb{Z}$ in unione disgiunta delle seguenti classi laterali:

$$[0]_{12}, [1]_{12}, [2]_{12}, \ldots, [10]_{12}, [11]_{12}$$

Segue dal precedente teorema che due laterali gH e bH o sono disgiunti o coincidono. Il seguente corollario illustra la situazione:

COROLLARIO 4.22. *Dato un laterale gH, si consideri un laterale bH. Allora bH coincide con gH se e solo se $b \in gH$. Altrimenti i due laterali sono disgiunti.*

DIMOSTRAZIONE. Se $b \in gH$ allora c'è un elemento in comune fra i due laterali. Dunque poiché sappiamo dal Teorema 4.20 che ogni elemento appartiene ad un solo laterale, questo vuol dire che $gH = bH$. Viceversa, se $bH = gH$ allora è immediato concludere che $b \in bH = gH$. □

Svolgete anche l'Esercizio 4.37 che presenta i laterali come classi di equivalenza rispetto ad una relazione.

La partizione di G in unione disgiunta di classi laterali rispetto ad un sottogruppo H ha una importante conseguenza per quel che riguarda le cardinalità, nel caso in cui G sia finito:

TEOREMA 4.23 (Teorema di Lagrange[2]). *Se G è un gruppo finito e H è un sottogruppo di G allora $|H|$ divide $|G|$.*

DIMOSTRAZIONE. Visto che G è finito, G è l'unione disgiunta di un numero finito, diciamo n_H, di laterali sinistri di H. Se dimostriamo che ogni laterale ha cardinalità esattamente $|H|$ allora risulta $|G| = n_H\ |H|$ e dunque $|H|$ divide $|G|$.

Contiamo allora quanti elementi ha il laterale gH, per un qualunque $g \in G$. Visto che gli elementi della forma gh ottenuti al variare di $h \in H$ sono tutti diversi fra loro (se vale $gh_1 = gh_2$ allora moltiplicando a sinistra per g^{-1} abbiamo $h_1 = h_2$), vale che $|gH| = |H|$. □

Segnaliamo subito un importante corollario del teorema di Lagrange.

DEFINIZIONE 4.24. Dato un elemento x di un gruppo G, se esiste un minimo intero positivo n tale che $x^n = e$ allora n si indica con $o(x)$ e si chiama *ordine* di x. Se un tale n non esiste allora si dice che x ha ordine infinito e si scrive $o(x) = \infty$.

COROLLARIO 4.25. *In un gruppo finito G, ogni elemento x ha ordine finito e tale ordine $o(x)$ divide $|G|$.*

DIMOSTRAZIONE. Consideriamo le potenze positive di x di G: $x, x^2, \cdots, x^k, \ldots$. In questa lista ad un certo punto deve comparire e. Infatti, se $x = e$ non c'è nulla da dimostrare. Se $x \neq e$, visto che le potenze sono infinite ma gli elementi del gruppo sono finiti, ad un certo punto deve valere $x^i = x^j$ con $1 \leq i < j$. Allora, moltiplicando per l'inverso di x^i, si ottiene $x^{j-i} = e$.

Sia ora $o(x)$, come abbiamo definito sopra, il più piccolo n per cui $x^n = e$ e consideriamo gli elementi

$$\{e, x, x^2, \ldots, x^{o(x)-1}\}$$

Tali elementi sono tutti distinti: se fosse $x^i = x^j$ con $1 \leq i < j \leq o(x)$ allora varrebbe $x^{j-i} = e$ ma questo non è possibile perché $j - i < o(x)$.

Inoltre osserviamo che $\{e, x, x^2, \ldots, x^{o(x)-1}\}$ coincide con il sottogruppo ciclico (x) generato da x (infatti si nota che $x^{-1} = x^{o(x)-1}$, $x^{-2} = x^{o(x)-2}$ etc...e si verifica subito che tutte le potenze di x e di x^{-1} sono presenti nella lista, visto che si ripetono ciclicamente).

Dunque la cardinalità del sottogruppo (x) è uguale a $o(x)$, e dal teorema di Lagrange segue che $o(x)$ divide $|G|$.

□

COROLLARIO 4.26. *Se x è un elemento di un gruppo finito G vale*

$$x^{|G|} = e.$$

DIMOSTRAZIONE. Infatti per il corollario precedente possiamo scrivere $|G| = k \cdot o(x)$ per un certo intero k. Da questo segue che

$$x^{|G|} = x^{k \cdot o(x)} = \left(x^{o(x)}\right)^k = e^k = e$$

□

[2]Joseph-Louis Lagrange, nato Giuseppe Lodovico Lagrangia, matematico italiano, 1736-1813.

4. Una prima applicazione: la funzione di Eulero.

Il teorema di Lagrange e il Corollario 4.25 hanno una immediata applicazione aritmetica. Fissato un numero intero $m \geq 2$, consideriamo l'anello $\mathbb{Z}_m$. È immediato verificare che gli elementi invertibili di $\mathbb{Z}_m$ (cioè gli $[a]_m$ per cui esiste $[b]_m$ tale che $[a]_m[b]_m = [1]_m$) costituiscono un gruppo *rispetto alla moltiplicazione*. Tale gruppo viene indicato con la notazione $\mathbb{Z}_m^*$.

ESEMPIO 4.27. Se p è un numero primo, $\mathbb{Z}_p^*$ ha $p-1$ elementi, visto che tutte le classi (eccetto la $[0]$) sono invertibili.
Il gruppo Z_{10}^* ha 4 elementi: [1],[3],[7],[9].
Il gruppo Z_{15}^* ha 8 elementi: [1], [2], [4], [7], [8], [11], [13], [14].

DEFINIZIONE 4.28. *La funzione ϕ di Eulero* è la funzione $\phi : \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ definita ponendo $\phi(1) = 1$ e, per $n > 1$,

$$\phi(n) = \text{numero degli interi positivi minori di } n \text{ e primi con } n$$

Dunque, dato $m \geq 2$, la cardinalità di $\mathbb{Z}_m^*$ è uguale a $\phi(m)$. Questo ci permette già di enunciare un teorema che generalizza il piccolo teorema di Fermat:

TEOREMA 4.29. *Fissato un intero positivo m, se a è un intero primo con m vale:*

$$a^{\phi(m)} \equiv 1 \bmod m$$

DIMOSTRAZIONE. Se $m = 1$ l'enunciato è banale (tutti i numeri sono congrui fra loro modulo 1). Sia allora $m \geq 2$. Visto che a ed m sono coprimi, sappiamo che $[a]$ appartiene a $\mathbb{Z}_m^*$. Per il Corollario 4.26 in $\mathbb{Z}_m^*$ vale

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

che equivale a

$$a^{\phi(m)} \equiv 1 \bmod m$$

□

OSSERVAZIONE 4.30. Se $m = p$ è primo ritroviamo l'enunciato del piccolo teorema di Fermat, visto che $\phi(p) = p - 1$ (abbiamo dunque dato, tramite il teorema di Lagrange, un'altra dimostrazione del piccolo teorema di Fermat). In questo caso, come vedremo più avanti, vale anche che $\mathbb{Z}_p^*$ è un gruppo ciclico, ossia esiste un elemento in $\mathbb{Z}_p^*$ di ordine esattamente $p - 1$.

OSSERVAZIONE 4.31. Avremmo potuto dimostrare il Teorema 4.29 anche imitando la dimostrazione del piccolo teorema di Fermat nel caso dei gruppi abeliani finiti, come suggerito dall'Esercizio 4.35. Ma abbiamo preferito introdurre subito il teorema di Lagrange, che ha valore più generale, e i laterali, che avranno anch'essi grande importanza in seguito.

Alla luce di questo teorema, risulta importante saper calcolare in modo efficiente i valori della funzione ϕ che, al momento, è definita in maniera un po' implicita. Ce ne occuperemo nel prossimo capitolo.

5. Esercizi

ESERCIZIO 4.32. Dimostrare che se la cardinalità di un gruppo è un numero primo, allora il gruppo è ciclico.

Esercizio 4.33. Dimostrare che se per due elementi a, b di un gruppo G vale $ab = e$ allora vale anche $ba = e$, e viceversa. Dunque per verificare che b è l'inverso di a basta verificare solo che sia inverso sinistro (o solo che sia inverso destro).

Esercizio 4.34. Quali sono gli elementi di ordine massimo in $\mathbb{Z}_{13}^*$? E in $\mathbb{Z}_{20}^*$?

Esercizio 4.35. Sia G un gruppo abeliano finito di cardinalità n. Dimostrare, senza usare il teorema di Lagrange, e imitando la prima dimostrazione del piccolo teorema di Fermat, che per ogni $g \in G$ vale $g^n = e$. [Nota: seguendo questa strada avremmo potuto dunque dimostrare il Teorema 4.29 senza passare per il teorema di Lagrange.]

Esercizio 4.36. Se H è un sottoinsieme finito non vuoto di un gruppo G e vale che $a, b \in H \Rightarrow ab \in H$, allora H è un sottogruppo di G.

Esercizio 4.37. Dato un sottogruppo H di un gruppo G si consideri la seguente relazione fra gli elementi di G: $x \sim y$ se e solo se $y^{-1}x \in H$.

Dimostrare che si tratta di una relazione di equivalenza e che per due elementi x e y vale $x \sim y$ se e solo se x e y appartengono allo stesso laterale sinistro $xH = yH$.

Esercizio 4.38. Provate a dare una prima dimostrazione di questa formula, su cui torneremo fra due capitoli. Dimostrare che, per ogni intero positivo n vale:

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

CAPITOLO 5

La funzione ϕ di Eulero

Ci eravamo ripromessi di trovare un modo efficiente di calcolare i valori della funzione ϕ di Eulero.

1. Una formula per la funzione ϕ

PROPOSIZIONE 5.1. *Se b e c sono due numeri primi tra loro*

$$\phi(bc) = \phi(b)\phi(c)$$

OSSERVAZIONE 5.2. Dato che ϕ possiede la proprietà scritta qui sopra, appartiene alla famiglia delle funzioni *aritmetiche moltiplicative*.

DIMOSTRAZIONE. Facciamo una breve osservazione preliminare: dati tre numeri interi s, t, m, con $m > 0$, tali che $s \equiv t \quad (m)$, allora s è coprimo con m se e solo se t è coprimo con m. Infatti $s \equiv t \quad (m)$ può essere tradotto nella relazione $s = mq + t$ per un certo intero q, e, come visto nella Sezione 4 del Capitolo 1, è facile osservare che $MCD(s, m) = MCD(m, t)$.

Ora se u è un numero intero positivo coprimo con bc e minore di bc, allora u è in particolare coprimo con b e coprimo con c, ed è dunque soluzione di un sistema di equazioni del tipo:

$$\begin{cases} x \equiv k & (b) \\ x \equiv v & (c) \end{cases}$$

dove k è un intero positivo coprimo con b e $< b$ e v è un intero positivo coprimo con c e $< c$. Viceversa, per il teorema cinese, ogni sistema di equazioni del tipo descritto ha una sola soluzione intera positiva minore di bc, e tale soluzione, essendo coprima con b e con c, è anche coprima con bc.

Dunque i numeri interi positivi coprimi con bc e minori di bc sono tanti quanti i sistemi del tipo descritto, che sono $\phi(b)\phi(c)$ (il prodotto delle possibili scelte di k e v).

□

TEOREMA 5.3. *Consideriamo un intero positivo m. Se $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ è la sua decomposizione in fattori primi, allora*

$$\phi(m) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$$

DIMOSTRAZIONE. Dalla Proposizione 5.1 segue subito che per calcolare $\phi(m)$ basta fare il prodotto dei numeri $\phi(p_i^{a_i})$. Ci resta dunque da sapere quanto vale $\phi(p^n)$ con p numero primo. Osserviamo che i numeri positivi minori di p^n sono tutti primi con p^n a meno che non siano multipli di p. Un semplice calcolo mostra dunque che $\phi(p^n) = p^n - p^{n-1}$. □

OSSERVAZIONE 5.4. In particolare, se p e q sono due distinti numeri primi, $\phi(p^2) = p^2 - p$, $\phi(pq) = (p-1)(q-1)$. Dunque, come avevamo osservato nell'Esempio 4.27, $\phi(10) = 4 \cdot 1 = 4$, $\phi(15) = 4 \cdot 2 = 8$.

Esempio 5.5. Come applicazione immediata dei risultati precedenti possiamo calcolare subito la classe di resto di 2^{365} modulo 225.

Visto che $\phi(225) = (25-5)(9-3) = 120$, per il Teorema 4.29 sappiamo infatti che

$$2^{120} \equiv 1 \bmod 225$$

Dunque

$$2^{365} \equiv (2^{120})^3 \cdot 2^5 \equiv 2^5 \equiv 32 \bmod 225$$

Esempio 5.6. Il Teorema 4.29 ci dice che

$$2^8 \equiv 1 \bmod 15$$

Osserviamo però che l'ordine di $[2]$ in $\mathbb{Z}_{15}^*$ non è 8, ma 4. L'ordine di un elemento divide l'ordine del gruppo (Corollario 4.25): questo esempio mostra che non è detto che coincida con l'ordine del gruppo. Del resto, $[1]$ ha ordine 1 in ogni gruppo $\mathbb{Z}_m^*$, e, se $m > 1$, 1 è diverso da $\phi(m)$.

2. Esercizi

Esercizio 5.7. Dato un numero intero positivo n, sia $\sigma(n)$ la somma dei divisori di n. In particolare dunque $\sigma(1) = 1$.

(1) Quali sono i numeri interi positivi n tali che $\sigma(n)$ è dispari?
(2) Dire se l'equazione
$$3\sigma(n) = 4n - 17$$
ha soluzione per qualche n intero positivo.

Esercizio 5.8. Dimostrare che la funzione $\sigma : \mathbb{N}-\{0\} \to \mathbb{N}-0$ definita nell'esercizio precedente è una funzione aritmetica moltiplicativa.

Esercizio 5.9 (I numeri primi di Mersenne[1]). I numeri primi di Mersenne sono i numeri primi che si trovano fra i numeri della forma $M_n = 2^n - 1$, dove n è un intero positivo. I più piccoli numeri primi di Mersenne sono $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{13} = 8191$, $M_{17} = 131071$, $M_{19} = 524287$.

Attualmente (ottobre 2022) sono noti 51 numeri primi di Mersenne; fra questi c'è il più grande numero primo conosciuto $2^{82589933} - 1$.

a) Dimostrare che se n non è primo allora neppure $M_n = 2^n - 1$ è primo, dunque i numeri primi di Mersenne vanno cercati fra i numeri della forma M_p con p primo.
b) Dimostrare che se p è un primo dispari, allora per ogni numero primo q che divide M_p vale
$$q \equiv 1 \quad (2p)$$

Esercizio 5.10. Sia p un numero primo tale che $M_p = 2^p - 1$ è un primo di Mersenne. Dimostrare che $N_p = 2^{p-1}M_p$ è uguale alla somma dei suoi divisori propri, ossia $\sigma(N_p) = 2N_p$.

Esercizio 5.11 (difficile). Dimostrare che se un intero positivo n è pari e $\sigma(n) = 2n$ allora esiste un primo p tale che $M_p = 2^p - 1$ è un primo di Mersenne e $n = N_p = 2^{p-1}M_p$.

[1] Marin Mersenne, matematico francese (anche teologo e teorico della musica e del suono), 1588-1648.

CAPITOLO 6

Omomorfismi ed esempi

1. Omomorfismi di gruppi

1.1. Definizione di omomorfismo e automorfismo.

DEFINIZIONE 6.1. Dati due gruppi G_1, G_2, una funzione $f : G_1 \to G_2$ si dice *omomorfismo* se per ogni $g, h \in G_1$ vale:

$$f(gh) = f(g)f(h)$$

PROPOSIZIONE 6.2. *Sia $f : G_1 \to G_2$ un omomorfismo. Allora, se chiamiamo e_{G_1} ed e_{G_2} rispettivamente le identità di G_1 e di G_2, vale*

$$f(e_{G_1}) = e_{G_2}$$

Inoltre, per ogni $g \in G_1$ vale

$$f(g^{-1}) = f(g)^{-1}$$

DIMOSTRAZIONE. Osserviamo che possiamo scrivere

$$f(e_{G_1}) = f(e_{G_1}e_{G_1}) = f(e_{G_1})f(e_{G_1})$$

dove per il primo = si è usato il fatto che e_{G_1} è l'identità di G_1 e per il secondo = si è usato il fatto che f è un omomorfismo. Quella che abbiamo ottenuto è una uguaglianza in G_2. Potremmo subito concludere per il punto (5) del Teorema 4.4, visto che la soluzione dell'equazione

$$f(e_{G_1}) = xf(e_{G_1})$$

è unica, e sappiamo che e_{G_2} e $f(e_{G_1})$ entrambi risolvono l'equazione, dunque devono coincidere. Altrimenti (si tratta in realtà dello stessa dimostrazione, ma la presentiamo in due forme così potete scegliere quella a voi più congeniale), possiamo moltiplicare entrambi i membri di

$$f(e_{G_1}) = f(e_{G_1})f(e_{G_1})$$

per l'inverso di $f(e_{G_1})$:

$$f(e_{G_1})^{-1}f(e_{G_1}) = f(e_{G_1})^{-1}f(e_{G_1})f(e_{G_1})$$

ottenendo

$$e_{G_2} = f(e_{G_1})$$

Per quel che riguarda la seconda affermazione che dobbiamo dimostrare, dato $g \in G_1$ possiamo scrivere

$$e_{G_2} = f(e_{G_1}) = f(gg^{-1}) = f(g)f(g^{-1})$$

Dunque, vista l'unicità dell'inverso di un elemento, $f(g^{-1}) = f(g)^{-1}$.

□

DEFINIZIONE 6.3. Dati due gruppi G_1, G_2, se un omomorfismo $f : G_1 \to G_2$ è bigettivo allora è un *isomorfismo*. Se esiste un isomorfismo fra due gruppi G_1 e G_2 si dice che i due gruppi sono *isomorfi* e si scrive

$$G_1 \cong G_2$$

Dato un gruppo G, un isomorfismo $f : G \to G$ si dice anche *automorfismo*. Denoteremo con $Aut(G)$ l'insieme formato dagli automorfismi di un gruppo G.

ESERCIZIO 6.4. Dimostrare che $Aut(G)$ è un gruppo rispetto all'operazione data dalla composizione di funzioni.

ESEMPIO 6.5. La funzione $exp : \mathbb{R} \to \mathbb{R}^{>0}$ definita da $exp(a) = e^a$ per ogni $a \in \mathbb{R}$ è un isomorfismo fra $\mathbb{R}$ pensato come gruppo con l'operazione + e $\mathbb{R}^{>0}$ (con questo simbolo intendiamo i numeri reali positivi) pensato come gruppo con la moltiplicazione.

ESEMPIO 6.6. La funzione $f : \mathbb{Z}_{10} \to \mathbb{Z}_5$ definita da $f([a]_{10}) = [a]_5$ è un omomorfismo surgettivo fra $\mathbb{Z}_{10}$ e $\mathbb{Z}_5$, pensati come gruppi con l'operazione +.

ESEMPIO 6.7. Osserviamo che il sottoinsieme $\{1, -1\}$ di $\mathbb{Z}$, visto con l'operazione data dalla moltiplicazione, è un gruppo. Si tratta di un gruppo isomorfo a $\mathbb{Z}_2$, visto come gruppo rispetto all'operazione +. L'isomorfismo $f : \{1, -1\} \to \mathbb{Z}_2$ è unico, ed è definito da $f(1) = [0]$ e $f(-1) = [1]$ (verificate nei dettagli quest'ultima affermazione).

ESERCIZIO 6.8. Il sottoinsieme $\{1, -1, \imath, -\imath\}$ di $\mathbb{C}$, visto con l'operazione data dalla moltiplicazione, è un gruppo, isomorfo a $\mathbb{Z}_4$, visto come gruppo con l'operazione +. In questo caso ci sono due isomorfismi possibili: quali?

Illustriamo ora un modo per produrre importanti automorfismi di un gruppo:

DEFINIZIONE 6.9. Sia G un gruppo e sia $g \in G$. Consideriamo la funzione $C_g : G \to G$ definita da

$$C_g(h) = ghg^{-1} \qquad \forall h \in G$$

Tale funzione si chiama *coniugio* rispetto all'elemento g.

PROPOSIZIONE 6.10. *Sia G un gruppo e sia $g \in G$. Il coniugio C_g è un automorfismo di G.*

DIMOSTRAZIONE. Per dimostrare che C_g è una funzione bigettiva basta osservare che possiede un'inversa, che è $C_{g^{-1}}$.

Per dimostrare che è un omomorfismo (e dunque un automorfismo), dati $h, k \in G$ si osserva che:

$$C_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = (ghg^{-1})(gkg^{-1}) = C_g(h)C_g(k)$$

□

Osserviamo che nella dimostrazione qui sopra, nel passaggio in cui compare $ghg^{-1}gkg^{-1}$ abbiamo aggiunto nel nostro prodotto il fattore $g^{-1}g$ che è uguale ad e. Si tratta di una tecnica usato molto frequentemente quando si fanno calcoli in un gruppo.

1.2. Nucleo e immagine di un omomorfismo. Ci sono due sottogruppi importanti associati ad un omomorfismo.

DEFINIZIONE 6.11. Dati due gruppi G_1, G_2 e un omomorfismo $f : G_1 \to G_2$ chiamiamo *nucleo* di f l'insieme:

$$Ker f = \{g \in G_1 | f(g) = e_{G_2}\}$$

Denotiamo con $\operatorname{Imm} f$ l'immagine di f:

$$\operatorname{Imm} f = \{f(g) | g \in G_1\}$$

ESERCIZIO 6.12. Dimostrare che $Kerf$ è un sottogruppo di G_1 e Imm f è un sottogruppo di G_2.

Illustriamo subito una importante proprietà di $Kerf$.

TEOREMA 6.13. *Dati due gruppi G_1, G_2, un omomorfismo $f : G_1 \to G_2$ è iniettivo se e solo se $Kerf = \{e_{G_1}\}$.*

DIMOSTRAZIONE. Supponiamo che f sia iniettivo. Se esistesse in $Kerf$ un elemento $u \neq e_{G_1}$ allora varrebbe $f(u) = e_{G_2} = f(e_{G_1})$, dove il secondo $=$ deriva dalla Proposizione 6.2, e questo contraddirebbe l'iniettività.

Viceversa, supponiamo che $Kerf = \{e_{G_1}\}$. Supponiamo per assurdo che f non sia iniettiva. Allora esistono due elementi $g, h \in G_1$, con $g \neq h$ e tali che $f(g) = f(h)$.

Possiamo dunque scrivere, moltiplicando per $f(h)^{-1}$, che $f(h)^{-1}f(g) = e_{G_2}$. A questo punto usando la Proposizione 6.2 e la definizione di omomorfismo otteniamo

$$e_{G_2} = f(h)^{-1}f(g) = f(h^{-1})f(g) = f(h^{-1}g)$$

Questo significa che $h^{-1}g \in Kerf$. Poiché però $Kerf = \{e_{G_1}\}$ allora $h^{-1}g = e_{G_1}$, da cui si ottiene, moltiplicando entrambi i membri per h (a sinistra), $g = h$ che è assurdo perché contraddice l'ipotesi iniziale $g \neq h$.

□

Collegamento con argomenti che vedrete prossimamente a Geometria 1: se si considerano gli spazi vettoriali come gruppi abeliani con l'operazione + allora una applicazione lineare è in particolare un omomorfismo nel senso dei gruppi, e dunque il Teorema 6.13, applicato questo caso, dice appunto che una applicazione lineare è iniettiva se e solo se il suo nucleo è $\{O\}$.

2. Gruppi ciclici

Sia G un gruppo ciclico. Ci poniamo le seguenti domande:
1) Chi sono i generatori di G, ossia gli elementi $g \in G$ tali che $G = (g)$? Quanti sono?
2) Chi sono i sottogruppi di G? Come sono fatti? Quanti sono?

Per rispondere a queste domande cominciamo dalla seguente proposizione.

PROPOSIZIONE 6.14. *Sia G un gruppo ciclico, e sia H un sottogruppo non banale di G. Allora H è ciclico.*

DIMOSTRAZIONE. Sia k il minimo intero postivo tale che $g^k \in H$. Sia ora $g^a \in H$ per qualche $a \in \mathbb{Z}$. Per la divisione Euclidea esistono $q, r \in \mathbb{Z}$ tali che $a = qk + r$ e $0 \leq r < k$, quindi $(g^k)^{-q}g^a = g^{qk+r} = (g^k)^{-q}(g^k)^q g^r = g^r \in H$ poiché H è un sottogruppo. Ma per la minimalità di k questo implica $r = 0$, e dunque $g^a = (g^k)^q \in (g^k)$. Dunque $H = (g^k)$. □

Questa proposizione ci permette di rispondere immediatamente alle nostre domande nel caso infinito: invitiamo il lettore a scrivere i dettagli della dimostrazione del seguente corollario.

COROLLARIO 6.15. *Sia G un gruppo ciclico infinito, e sia $g \in G$ un generatore di G, ossia $G = (g)$. Allora i sottogruppi di G sono tutti e soli i sottogruppi ciclici (g^n) con $n \in \mathbb{N}$, $n \geq 1$. In particolare i generatori di G sono esattamente g e g^{-1}, e $(g_1^n) \subseteq (g^{n_2})$ se e solo se n_2 divide n_1.*

Per trattare il caso finito abbiamo bisogno di una proposizione.

PROPOSIZIONE 6.16. *Sia G un gruppo ciclico finito di ordine $|G| = n$, e sia $g \in G$ un generatore di G, ossia $G = (g)$. Allora per ogni $k \in \mathbb{Z}$, $(g^k) = (g^{MCD(k,n)})$.*

DIMOSTRAZIONE. Sia $d := MCD(k,n)$, sia $k = cd$, con $c \in \mathbb{Z}$, e siano $x, y \in \mathbb{Z}$ tali che $d = xk + yn$: l'esistenza di x e y è garantita dal teorema di Bézout. Allora, se denotiamo con e l'identità di G, abbiamo

$$(g^k) = ((g^d)^c) \subseteq (g^d) = ((g^k)^x (g^n)^y) = ((g^k)^x e^y) = ((g^k)^x) \subseteq (g^k),$$

e dunque $(g^k) = (g^d)$. □

COROLLARIO 6.17. *Sia G un gruppo ciclico finito di ordine $|G| = n \geq 2$, e sia d un divisore positivo di n. Allora*

1) ci sono $\varphi(d)$ elementi di G di ordine d e sono esattamente i generatori del sottogruppo $(g^{\frac{n}{d}})$;

2) in particolare c'è un unico sottogruppo di G di ordine d, ossia $(g^{\frac{n}{d}})$.

Infine, per d_1, d_2 divisori positivi di n, $(g^{d_1}) \subseteq (g^{d_2})$ se e solo se d_2 divide d_1.

DIMOSTRAZIONE. Per la proposizione precedente ogni elemento della forma g^k con $1 \leq k \leq n$ e $MCD(k,n) = d$ è un generatore di (g^d), e dunque ha ordine $\frac{n}{d}$. Per $d = 1$ questo ci dice che ci sono $\varphi(n)$ elementi di G di ordine n, ossia generatori di $G = (g)$. Questo stesso fatto applicato al gruppo ciclico $(g^{n/d})$, che ha chiaramente ordine d, ci dice che ci sono $\varphi(d)$ generatori di $(g^{n/d})$, che per la proposizione sono esattamente gli elementi di G di ordine d. Questo mostra la 1). La 2) e l'ultima osservazione sono ora evidenti. □

Una conseguenza immediata di questo corollario è la seguente formula:

$$\sum_{d|n} \varphi(d) = n, \tag{2.1}$$

infatti, nella notazione del corollario, ogni elemento di G ha ordine un divisore di n, e per ogni divisore d di n il corollario ci dice che abbiamo $\varphi(d)$ elementi di ordine d.

ESEMPIO 6.18. Consideriamo il gruppo ciclico $\mathbb{Z}_{12}$ con l'addizione. Elenchiamo i sottogruppi ciclici generati dai suoi elementi (per semplificare la notazione indichiamo la classe $[a]_{12}$ semplicemente con $[a]$):

$$\begin{aligned}
([0]) &= \{[0]\} \\
([1]) &= \{[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[0]\} = \mathbb{Z}_{12} \\
([2]) &= \{[2],[4],[6],[8],[10],[0]\} \\
([3]) &= \{[3],[6],[9],[0]\} \\
([4]) &= \{[4],[8],[0]\} \\
([5]) &= \{[5],[10],[3],[8],[1],[6],[11],[4],[9],[2],[7],[0]\} = \mathbb{Z}_{12} \\
([6]) &= \{[6],[0]\} \\
([7]) &= \{[7],[2],[9],[4],[11],[6],[1],[8],[3],[10],[5],[0]\} = \mathbb{Z}_{12} \\
([8]) &= \{[8],[4],[0]\} \\
([9]) &= \{[9],[6],[3],[0]\} \\
([10]) &= \{[10],[8],[6],[4],[2],[0]\} \\
([11]) &= \{[11],[10],[9],[8],[7],[6],[5],[4],[3],[2],[1],[0]\} = \mathbb{Z}_{12}\,.
\end{aligned}$$

È ora un facile ed utile **eserczio** verificare le affermazioni del Corollario 6.17 in questo esempio.

È interessante notare che la proprietà 2) del Corollario 6.17 caratterizza i gruppi ciclici finiti.

PROPOSIZIONE 6.19. *Sia G un gruppo finito di ordine n tale che per ogni d divisore positivo di n G ha al più un sottogruppo di ordine d. Allora G è ciclico.*

DIMOSTRAZIONE. Sia d un divisore positivo di n, e sia G_d l'insieme degli elementi di G di ordine d. Se G_d è non vuoto, allora ogni suo elemento genera un sottogruppo ciclico di G di ordine d, che per ipotesi è l'unico tale sottogruppo. Dunque G_d è l'insieme dei generatori di questo unico sottogruppo ciclico di ordine d, quindi per il Corollario 6.17 $|G_d| \leq \varphi(d)$. Ma ora

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n,$$

dove abbiamo usato la (2.1) nell'ultima uguaglianza. Ma questo implica che per ogni d, $|G_d| = \varphi(d)$, e in particolare $|G_n| = \varphi(n)$, dunque G ha un elemento di ordine n, ossia un generatore. □

ESEMPIO 6.20. Sia H il sottoinsieme $\{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ del gruppo simmetrico S_4, dove abbiamo denotato con id l'identità del gruppo. È un facile ed utile **esercizio** verificare che H è un sottogruppo abeliano di S_4. Inoltre, ogni elemento al quadrato fa l'identità, quindi H non ha elementi di ordine 4, e quindi non è ciclico. In accordo con la Proposizione 6.19, H ha 3 (> 1) sottogruppi di ordine 2, ossia $\{id, (1,2)(3,4)\}, \{id, (1,3)(2,4)\}$ e $\{id, (1,4)(2,3)\}$.

In effetti l'esempio precedente è il più piccolo gruppo non ciclico:

ESERCIZIO 6.21. Mostrare che ogni gruppo di ordine ≤ 3 è ciclico.

3. Ancora il gruppo simmetrico

Torniamo al gruppo simmetrico S_n. Avevamo già introdotto due notazioni per i suoi elementi.

La prima notazione è quella come *prodotto di cicli disgiunti*, ad esempio

$$\sigma = (1,3,5)(2,7) = (1,3,5)(2,7)(4)(6) \in S_7.$$

Questa notazione è particolarmente utile in algebra. Ricordiamo che un ciclo di lunghezza 1 è detto *punto fisso*, mentre un ciclo di lunghezza due è detto *trasposizione*.

La seconda notazione è quella come *doppio array*, ad esempio (lo stesso esempio)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 1 & 6 & 2 \end{pmatrix}.$$

In realtà quest'ultima notazione è un po' ridondante. Infatti per ricostruire $\sigma \in S_n$ ci basta tenere traccia della seconda riga, ossia invece di guardare a

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

scriviamo semplicemente $\sigma = \sigma(1)\sigma(2)\cdots\sigma(n)$. Nel nostro esempio 3754162. In questo modo pensiamo a σ come una parola nell'alfabeto $\{1, 2, \ldots, n\}$, e la posizione di una lettera j nella parola è semplicemente $\sigma^{-1}(j)$. Chiamiamo questa notazione *one-line notation*. Questa notazione è particolarmente utile in combinatoria.

3.1. Inversioni e segno di una permutazione. Una terza notazione è la notazione come *treccia*: per $\sigma \in S_n$, scriviamo i numeri $1, 2, \ldots, n$ in due righe consecutive, e uniamo i a $\sigma(i)$ con un segmento (filo), per ogni i.

Ad esempio per $\sigma = 314265 \in S_6$, la sua notazione come treccia appare in Figura 1.

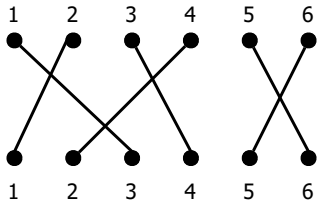

FIGURA 1. La treccia corrispondente a $\sigma = 314265$.

Quest'ultima notazione è particolarmente utile per lavorare con le inversioni.

Una coppia (i, j) è una *inversione* di $\sigma \in S_n$ se $1 \le i < j \le n$ e $\sigma(i) > \sigma(j)$. È un **esercizio** mostrare che (i, j) è un'inversione di σ se e solo se nella treccia corrispondente a σ il segmento (filo) da i a $\sigma(i)$ e quello da j a $\sigma(j)$ si intersecano.

Ad esempio $\sigma = 314265$ ha 4 inversioni: $(1, 2)$, $(1, 4)$, $(3, 4)$ e $(5, 6)$ (vedi Figura 1).

Se denotiamo con $\mathsf{inv}(\sigma)$ il numero di inversioni di $\sigma \in S_n$, allora abbiamo le seguenti proprietà.

PROPOSIZIONE 6.22. *Valgono le seguenti proprietà:*

(1) *l'identità* $id \in S_n$ *ha* $\mathsf{inv}(id) = 0$*;*
(2) *per ogni trasposizione* (i, j) *con* $i < j$ *si ha*

$$\mathsf{inv}((i, j)) = 2(j - i - 1) + 1;$$

(3) $\mathsf{inv}(\sigma) = \mathsf{inv}(\sigma^{-1})$*;*
(4) *se* $\sigma, \tau \in S_n$*, allora*

$$(-1)^{\mathsf{inv}(\sigma)+\mathsf{inv}(\tau)} = (-1)^{\mathsf{inv}(\tau\circ\sigma)}.$$

DIMOSTRAZIONE. La 1) e la 2) si calcolano direttamente, ad esempio usando le trecce. Per la 3), osserviamo che la treccia di σ^{-1} si ottiene dalla treccia di σ riflettendo la figura rispetto a una retta orizzontale. Quindi il numero di inversioni, ossia il numero di intersezioni dei fili della treccia, non cambia.

Per la 4), dobbiamo motrare che $\mathsf{inv}(\sigma) + \mathsf{inv}(\tau)$ e $\mathsf{inv}(\tau \circ \sigma)$ hanno la stessa parità, ossia che sono congrui modulo 2. Osserviamo che la composizione di due trecce si ottiene mettendo le due trecce una dopo l'altra (e poi eventualmente "tendendo" i fili della treccia).

Ad esempio se $\sigma = 314265$ e $\tau = 513642$, allora la treccia della composizione $\tau \circ \sigma = 356124$ appare in Figura 2.

Osserviamo che (i, j) con $1 \le i < j \le n$ è un'inversione di $\tau \circ \sigma \in \mathfrak{S}_n$ se e solo se i fili che partono da i e da j si incrociano nella prima metà del diagramma, ma non nella seconda, oppure si incrociano nella seconda metà del diagramma ma non nella prima. Negli altri casi si incrociano zero o due volte, e questo mostra la proprietà che volevamo. □

Questa semplice proposizione ha una conseguenza non banale. Cominciamo con una osservazione.

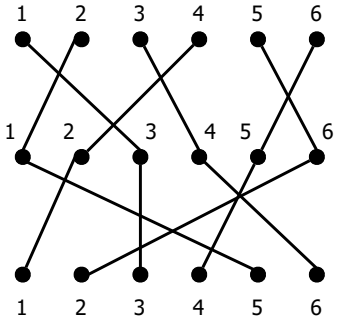

FIGURA 2. La treccia corrispondente alla composizione $\tau \circ \sigma = 356124$.

OSSERVAZIONE 6.23. Ogni permutazione si scrive in almeno un modo (in realtà in infiniti modi) come prodotto di trasposizioni. Infatti, sappiamo già che ogni permutazione si scrive come prodotto di cicli, quindi mi basta mostrare che posso scrivere un ciclo come prodotto di trasposizioni (i cicli di lunghezza 1 sono il prodotto di zero trasposizioni). Ecco due modi di scrivere un ciclo di lunghezza k come prodotto di $k-1$ trasposizioni:

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_2, a_3)\cdots(a_{k-1}, a_k) = (a_1, a_k)(a_1, a_{k-1})\cdots(a_1, a_3)(a_1, a_2).$$

PROPOSIZIONE 6.24. *Se $\sigma \in S_n$ è tale che*

$$\sigma = \tau_1\tau_2\cdots\tau_r = \tau'_1\tau'_2\cdots\tau'_s$$

con τ_i e τ'_j trasposizioni per ogni i e j, allora r e s hanno la stessa parità, ossia sono congrui modulo 2.

DIMOSTRAZIONE. Per la Proposizione 6.22, $\mathsf{inv}(\tau_i)$ è dispari per ogni i, quindi, usando ancora le proprietà dimostrate nella proposizione, otteniamo

$$(-1)^{\mathsf{inv}(\sigma)} = (-1)^{\mathsf{inv}(\tau_1\tau_2\cdots\tau_r)} = (-1)^{\mathsf{inv}(\tau_1)+\mathsf{inv}(\tau_2)+\cdots+\mathsf{inv}(\tau_r)} = (-1)^r.$$

Lo stesso argomento mostra che $(-1)^{\mathsf{inv}(\sigma)} = (-1)^s$. Ma allora $(-1)^r = (-1)^s$, e questo è equivalente a dire che r e s hanno la stessa parità. □

Questa proposizione suggerisce la seguente formula.

PROPOSIZIONE 6.25. *Se $\sigma = \gamma_1\gamma_2\cdots\gamma_r \in S_n$, dove i γ_i sono i cicli della decomposizione in cicli disgiunti di σ. Sia k_i la lunghezza di γ_i per ogni $i = 1, 2, \ldots, r$. Allora*

$$(-1)^{\mathsf{inv}(\sigma)} = (-1)^{\sum_{i=1}^{r}(k_i-1)}.$$

DIMOSTRAZIONE. Per la Proposizione 6.22 abbiamo

$$(-1)^{\mathsf{inv}(\sigma)} = (-1)^{\mathsf{inv}(\gamma_1\gamma_2\cdots\gamma_r)} = (-1)^{\mathsf{inv}(\gamma_1)+\mathsf{inv}(\gamma_2)+\cdots+\mathsf{inv}(\gamma_r)}.$$

È dunque sufficiente mostrare che $(-1)^{\mathsf{inv}(\gamma_i)} = (-1)^{k_i-1}$. Ma abbiamo visto nella Osservazione 6.23 che γ_i si scrive come prodotto di $k_i - 1$ trasposizioni, da cui segue facilmente l'affermazione. □

ESEMPIO 6.26. Per ogni $\sigma \in S_3$ il calcolo di $(-1)^{\mathsf{inv}(\sigma)}$ appare nella seguente tabella:

σ	id	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
$(-1)^{\mathsf{inv}(\sigma)}$	1	-1	-1	-1	1	1

è arrivato il momento di dare una definizione.

DEFINIZIONE 6.27. Dato $\sigma \in S_n$ il *segno* di σ è definito come

$$\operatorname{sgn}(\sigma) := (-1)^{\mathsf{inv}(\sigma)}.$$

Una permutazione $\sigma \in S_n$ è detta *pari* se $\operatorname{sgn}(\sigma) = 1$, mentre è detta *dispari* se $\operatorname{sgn}(\sigma) = -1$.

Consideriamo l'insieme $C_2 := \{1, -1\}$: con l'operazione di prodotto si verifica facilmente che C_2 è un grupo ciclico di ordine 2. Ora la proprietà 4) della Proposizione 6.22 ci dice che la funzione

$$\operatorname{sgn} : S_n \to C_2, \quad \sigma \mapsto \operatorname{sgn}(\sigma)$$

è un omomorfismo di gruppi. Dunque il kernel di sgn, che si denota usualmente con A_n è l'insieme delle permutazioni pari di S_n, e, per quello che abbiamo visto in generale per i kernel di omomorfismi, forma un sottogruppo del gruppo simmetrico S_n, detto *gruppo alterno* (o *alternante*).

OSSERVAZIONE 6.28. Osserviamo che $|A_n| = |S_n|/2 = n!/2$. Un modo per vedere questo fatto è il seguente: chiaramente ogni elemento di $(1,2)A_n = \{(1,2)\sigma \mid \sigma A_n\}$ è una permutazione dispari. Viceversa, data una permutazione dispari τ possiamo scriverla come $(1,2)((1,2)\tau)$, e chiaramente $(1,2)\tau \in A_n$. Dunque $(1,2)A_n$ è esattamente l'insieme delle permutazioni dispari, e la corrispondenza $A_n \to (1,2)A_n$ data da $\sigma \mapsto (1,2)\sigma$ è una bigezione. Siccome S_n è l'unione disgiunta di A_n e $(1,2)A_n$, questo mostra che in effetti $|A_n| = |S_n|/2 = n!/2$.

3.2. Ordine di una permutazione. Una domanda naturale è la seguente: qual è l'ordine di una permutazione $\sigma \in S_n$?

Come spesso accade per le questioni algebriche, per rispondere a questa domanda ci sarà di aiuto guardare alla decomposizione in cicli disgiunti di σ.

Sia $\sigma = \gamma_1\gamma_2\cdots\gamma_r$ la decomposizione in cicli disgiunti di $\sigma \in S_n$, e sia k_i la lunghezza del ciclo γ_i per ogni $i = 1, 2, \ldots, r$. Chiaramente il ciclo γ_i ha ordine k_i. Abbiamo già osservato che possiamo pensare σ come la composizione dei cicli $\gamma_1, \gamma_2, \ldots, \gamma_r$. Inoltre abbiamo anche osservato che i cicli γ_i commutano tra loro: questo semplicemente perché "muovono" insiemi di numeri disgiunti tra loro. Pertanto per ogni $k \in \mathbb{Z}$ abbiamo

$$\sigma^k = \gamma_1^k\gamma_2^k\cdots\gamma_r^k.$$

Affinché $\gamma^k = id$ dobbiamo dunque avere $\gamma_i^k = id$ per ogni i, e questo implica che k_i divide k per ogni i. A questo punto è chiaro che l'ordine di σ è il minimo comune multiplo di $k_1, k_2, \ldots, k_r$.

ESEMPIO 6.29. Ad esempio per $\sigma = (1,3,5)(2,4) \in S_5$ abbiamo

$$\begin{aligned}
\sigma^2 &= (1,3,5)^2(2,4)^2 = (1,5,3)\\
\sigma^3 &= (1,3,5)^3(2,4)^3 = (2,4)\\
\sigma^4 &= (1,3,5)^4(2,4)^4 = (1,3,5)\\
\sigma^5 &= (1,3,5)^5(2,4)^5 = (1,5,3)(2,4)\\
\sigma^6 &= (1,3,5)^6(2,4)^6 = id.
\end{aligned}$$

3.3. Classi di coniugio di S_n. Abbiamo considerato il coniugio nei gruppi. Nel gruppo simmetrico il coniugio ha una formula semplice, che risulta molto utile per fare calcoli.

Siano $\sigma, \tau \in S_n$, e consideriamo la decomposizione in cicli disgiunti di σ:

$$\sigma = (a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2})\cdots.$$

Allora vale la formula

$$\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_{k_1}))(\tau(b_1), \tau(b_2), \dots, \tau(b_{k_2}))\cdots. \tag{3.1}$$

Ad esempio se $\sigma, \tau \in S_5$ con $\sigma = (1,3,5)(2,4)$ e $\tau = (1,4,2,5)$, allora

$$\tau\sigma\tau^{-1} = (\tau(1), \tau(3), \tau(5))(\tau(2), \tau(4)) = (4,3,1)(5,2).$$

Questa formula implica immediatamente che tutti e soli gli elementi della *classe di coniugio* di $\sigma \in S_n$, ossia dell'insieme

$$C(\sigma) := \{\tau\sigma\tau^{-1} \mid \tau \in S_n\}$$

sono tutte e sole le permutazioni di S_n la cui decomposizione in cicli disgiunti ha cicli della stessa lunghezza di σ.

Una domanda naturale è la seguente: quanti elementi ci sono in $C(\sigma)$?

Introduciamo un po' di notazione: denotiamo con $\lambda(\sigma)$ la tupla $(\lambda_1, \lambda_2, \dots, \lambda_k)$ delle lunghezze dei cicli di σ nella sua decomposizione in cicli disgiunti, dove $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k > 0$.

Ad esempio se $\sigma = (1,5,4)(7,2,3)(6)(9,8) = (1,5,4)(7,2,3)(9,8) \in S_9$, allora $\lambda(\sigma) = (3,3,2,1)$.

Dunque, usando questa notazione, abbiamo osservato, grazie alla formula (3.1) che

$$C(\sigma) = \{\tau \in S_n \mid \lambda(\tau) = \lambda(\sigma)\}.$$

Denotiamo adesso con $\alpha_i = \alpha_i(\sigma)$ il numero di cicli di σ di lunghezza i: in formule, se $\lambda(\sigma) = (\lambda_1, \lambda_2, \dots, \lambda_k)$, allora

$$\alpha_i := |\{j \mid \lambda_j = i\}|.$$

PROPOSIZIONE 6.30. *Nella notazione introdotta sopra, abbiamo la formula*

$$|C(\sigma)| = \frac{n!}{1^{\alpha_1}2^{\alpha_2}\cdots n^{\alpha_n}\alpha_1!\alpha_2!\cdots\alpha_n!}.$$

DIMOSTRAZIONE. Il modo più semplice per capire la formula è il seguente: scriviamo una qualsiasi permutazione τ in one-line notation, e poi inseriamo le parentesi e le virgole in modo da ottenere un elemento di $C(\sigma)$.

Ad esempio, se $\sigma \in S_9$ è tale che $\lambda(\sigma) = (3,3,2,1)$, allora prendiamo un elemento

$$\tau = 425138796 \in S_9,$$

e inseriamo parentesi e virgole nella forma di $\lambda(\sigma) = (3,3,2,1)$, ossia $(\_,\_,\_)(\_,\_,\_)(\_,\_)(\_)$, ottenendo

$$(4,2,5)(1,3,8)(7,9)(6)$$

che è un elemento di $C(\sigma)$.

Apparentemente in questo modo otteniamo $n!$ elementi, che è chiaramente troppo. Il problema è che in questo modo otteniamo molte volte lo stesso elemento di $C(\sigma)$.

Ad esempio la permutazione $\tau' = 138542976$ dà lo stesso elemento di $C(\sigma)$ dato da τ nel nostro esempio.

In effetti ci sono due modi in cui stiamo "sovracontando": per ogni $i = 1, 2, \dots, n$, in ogni fissato ciclo di lunghezza i si possono permutare ciclicamente i numeri in i modi, e questo spiega il fattore $1^{\alpha_1}2^{\alpha_2}\cdots n^{\alpha_n}$ al denominatore; e si possono permutare in α_i modi i cicli di lunghezza i tra di loro, e questo spiega il fattore $\alpha_1!\alpha_2!\cdots\alpha_n!$ al denominatore. □

3.4. Esercizi.

Esercizio 6.31. Consideriamo il gruppo simmetrico S_{10}. Qual è l'ordine della permutazione $(2,3,4,5,6,7,8)$? Qual è l'ordine della permutazione $(1,3,5,6)(2,4,8)$? E quello della permutazione $(1,2,3,4,5,6)(7,8,9,10)$?

Esercizio 6.32. Consideriamo la permutazione $g = (2,4,6,1)(3,5,7)(8,9) \in S_9$. Qual è il suo ordine?

Esercizio 6.33. Sia $\sigma \in S_n$, e sia

$$\sigma = \tau_1\tau_2\cdots\tau_r$$

dove τ_i è una trasposizione per ogni $i = 1,2,\ldots,r$. Dimostrare che

$$\sigma^{-1} = \tau_r\tau_{r-1}\cdots\tau_2\tau_1.$$

Esercizio 6.34. Date le permutazioni

$$\alpha = (1,2,3,4,5)(6,7)(8)(9,10,11) \in S_{11}$$
$$\beta = (1,6)(2,7)(3,8,9)(4)(5,10,11) \in S_{11}$$

calcolare $\beta\circ\alpha$, $\alpha\circ\beta$, α^{-1}, β^{-1}, α^2, α^5, α^{1174}, β^2, β^6, β^{27802}.

Esercizio 6.35. Siano α, β e γ le permutazioni di S_7

$$\alpha = (1,2)(3,4,5)(6,7)$$
$$\beta = (1,2,3,4,5,6,7)$$
$$\gamma = (1,6,7)(2)(3,4)(5).$$

Calcolare $\mathsf{inv}(\alpha)$, $\mathsf{inv}(\beta)$, $\mathsf{inv}(\gamma)$, $\mathsf{inv}(\gamma\circ\alpha)$ e $\mathsf{inv}(\gamma\circ\beta)$.

Esercizio 6.36. Siano $\sigma,\tau \in S_n$, e sia $\sigma = a_1a_2\cdots a_n$ la scrittura di σ in one-line notation. Verificare che τ agisce a destra sulle posizioni, e a sinistra sui valori delle a_i, ossia in one-line notation

$$\sigma\tau = a_{\tau(1)}a_{\tau(2)}\cdots a_{\tau(2)}$$

e

$$\tau\sigma = \tau(a_1)\tau(a_2)\cdots\tau(a_n).$$

Verificare queste affermazioni con $\sigma = (1,2)(3,4,5)(6,7)$ e $\tau = (1,6,7)(2)(3,4)(5)$.

Esercizio 6.37. Date $\sigma = (1,2)(3,4,5)(6,7)$ e $\tau = (1,6,7)(2)(3,4)(5)$ in S_7, calcolare la cardinalità delle loro classi di coniugio

$$C(\sigma) := \{\rho\sigma\rho^{-1} \mid \rho \in S_7\} \quad \text{e} \quad C(\tau) := \{\rho\tau\rho^{-1} \mid \rho \in S_7\}.$$

Esercizio 6.38. Calcolare la cardinalità degli insiemi

$$A := \{\sigma \in S_7 \mid \sigma^2 = id\} \quad \text{e} \quad B := \{\sigma \in S_6 \mid \sigma \text{ ha ordine dispari}\}.$$

Esercizio 6.39. Quante sono in S_{12} le permutazioni di ordine 12?

Esercizio 6.40. Dimostrare che, a parte il caso di S_2, il centro del gruppo simmetrico è banale, ossia che per ogni intero positivo $n \neq 2$ vale $Z(S_n) = \{e\}$.

Esercizio 6.41. Dimostrare che, per $n \geq 2$, ogni permutazione di S_n può essere ottenuta come prodotto delle seguenti $n-1$ trasposizioni:

$$(1,2),(1,3),....,(1,n)$$

Qui si intende che nel prodotto ogni trasposizione può comparire anche più volte, o non comparire affatto.

Prima del prossimo esercizio introduciamo una definizione:

DEFINIZIONE 6.42. Dato un gruppo G, e dati $g_1, ..., g_k \in G$, diremo che G *è generato* da $g_1, ..., g_k \in G$ se ogni elemento di g può essere espresso come prodotto degli elementi $g_1, ..., g_k$ e dei loro inversi, eventualmente con ripetizioni. Si dirà che l'insieme $\{g_1, ..., g_k\}$ è un *insieme di generatori* di G.

Sappiamo che l'insieme delle trasposizioni è un insieme di generatori di S_n, per ogni $n \geq 2$. L'esercizio precedente ci mostra che anche l'insieme $\{(1,2),(1,3),....,(1,n)\}$ è un insieme di generatori per S_n. Il prossimo ci chiede di trovare un altro insieme di generatori:

ESERCIZIO 6.43. Dato $n \geq 3$, trovare un insieme di generatori di S_n di cardinalità $n-1$, in cui non tutti gli elementi sono trasposizioni.

ESERCIZIO 6.44. Dimostrare che, per ogni $n \geq 3$ esiste un insieme di generatori di S_n di cardinalità 2.

ESERCIZIO 6.45. Dimostrare che, dato $n \geq 3$, ogni permutazione di A_n può essere ottenuta come prodotto di permutazioni della forma (a,b,c), ossia di permutazioni composte da un unico ciclo di lunghezza 3.

ESERCIZIO 6.46 (L' 'enigma' del gioco del 15). La Figura 3 rappresenta la configurazione di base del famoso gioco del 15: Dimostrare che, seguendo le regole del gioco, ossia

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

FIGURA 3. Configurazione di base del gioco del 15

facendo scorrere i blocchetti nel modo lecito, non è possibile passare dalla configurazione base alla configurazione in cui il blocchetto 15 e il blocchetto 14 sono scambiati fra di loro, mentre tutti gli altri blocchetti sono posti come nella configurazione base.

ESERCIZIO 6.47. Sia G un gruppo ciclico di ordine 72 generato da $g \in G$, ossia $G = (g)$. 1) Elencare tutti i generatori di G. 2) Elencare tutti gli elementi di G di ordine 6. 3) Descrivere tutti i sottogruppi di G di ordine 12.

ESERCIZIO 6.48. Elencare tutti i sottogruppi ciclici di ordine 9 del gruppo simmetrico S_6.

ESERCIZIO 6.49. Sia G un gruppo ciclico generato da $g \in G$, ossia $G = (g)$, e sia G_2 un altro gruppo.

(1) Mostrare che un omomorfismo $f : G \to G_2$ è determinato da $f(g)$, ossia, sapendo chi è $f(g)$, il valore di $f(h)$ è forzato per ogni $h \in G$.
(2) Mostrare che se G è infinito, allora per ogni scelta di $g_2 \in G_2$ esiste un (unico) omomorfismo $f : G \to G_2$ tale che $f(g) = g_2$.
(3) Mostrare che se G è finito di ordine n e $g_2 \in G_2$, allora esiste un (unico) omomorfismo $f : G \to G_2$ tale che $f(g) = g_2$ se e solo se l'ordine di g_2 in G_2 divide n.

(4) Per ogni $n \in \mathbb{N}$, $n \geq 2$ descrivere tutti gli omomorfismi $f : \mathbb{Z}_n \to \mathbb{Z}$. Quanti sono?
(5) Per ogni $k \in \mathbb{N}$, $k \geq 2$ descrivere tutti gli omomorfismi $f : \mathbb{Z} \to \mathbb{Z}_k$. Quanti sono?
(6) Per ogni $k, n \in \mathbb{N}$, $k, n \geq 2$ descrivere tutti gli omomorfismi $f : \mathbb{Z}_n \to \mathbb{Z}_k$. Quanti sono?

CAPITOLO 7

Quozienti

1. Sottogruppi normali e quozienti

DEFINIZIONE 7.1. Sia $H < G$. Diremo che H è un *sottogruppo normale* o semplicemente che è *normale* se per ogni $g \in G$ vale

$$C_g(H) = H$$

In tal caso si scrive $H \lhd G$.

L'insieme $C_g(H)$ si indica comunemente anche come gHg^{-1}. È una notazione molto intuitiva e la useremo spesso anche noi, visto che descrive bene l'insieme

$$C_g(H) = \{ghg^{-1} | h \in H\}$$

OSSERVAZIONE 7.2. Se il gruppo G è abeliano, si verifica immediatamente che ogni suo sottogruppo è normale. Infatti, per ogni $g \in G$, vale in questo caso che C_g è l'identità (ossia l'automorfismo che manda ogni elemento in se stesso).

In realtà abbiamo già incontrato i gruppi normali quando abbiamo discusso i nuclei degli omomorfismi. Come vedremo, un sottogruppo è normale se e solo se esiste un omomorfismo di cui è il nucleo. Cominciamo intanto con una delle due implicazioni:

PROPOSIZIONE 7.3. *Dati due gruppi G_1, G_2 e un omomorfismo $f : G_1 \to G_2$, vale che $Kerf$ è un sottogruppo normale di G_1.*

DIMOSTRAZIONE. Presi $h \in Kerf$ e $g \in G_1$, usiamo il fatto che $f(h) = e_{G_2}$ e le proprietà degli omomorfismi studiate fin qui:

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e_{G_2}f(g)^{-1} = e_{G_2}$$

Abbiamo dunque dimostrato che $C_g(Kerf) \subseteq Kerf$.

Questo vale per ogni $g \in G_1$. Prendendo in particolare l'elemento g^{-1} abbiamo che $C_{g^{-1}}(Kerf) \subseteq Kerf$. Applicando C_g a questi due insiemi otteniamo dunque l'inclusione $C_g(C_{g^{-1}}(Kerf)) \subseteq C_g(Kerf)$ che, visto che C_g e $C_{g^{-1}}$ sono l'uno l'inverso dell'altro, è l'inclusione $Kerf \subseteq C_g(Kerf)$ che restava da dimostrare.

□

OSSERVAZIONE 7.4. Rileggendo la dimostrazione della Proposizione 7.3, si osserva che una parte di essa può essere facilmente generalizzata e adattata a dimostrare il seguente fatto: se per un sottogruppo H di G e per ogni $g \in G$ vale $gHg^{-1} \subseteq H$ allora vale anche, per ogni $g \in G$, $gHg^{-1} = H$. Dunque nella definizione di sottogruppo normale avremmo potuto sostituire la richiesta $C_g(H) = H$ con $C_g(H) \subseteq H$.

Facciamo subito un esempio di sottogruppo che non è normale. Per questo abbiamo bisogno di un gruppo non abeliano. Consideriamo il sottogruppo $H = \{e, (1,2)\}$ di S_3. Vale che

$$(1,3)H(1,3) = \{e, (3,2)\} \neq H$$

dunque H non è normale in S_3.

Ora veniamo al punto cruciale di questo paragrafo: mostreremo che se $H \lhd G$ allora è possibile definire sull'insieme G/H (i cui elementi sono gli H-laterali) un prodotto rispetto al quale G/H diventa un gruppo.

Innanzitutto premettiamo che, dati due sottoinsiemi A ed B di G, esiste già una definizione 'naturale' del prodotto AB come il seguente sottoinsieme di G:

$$AB = \{ab | a \in A, b \in B\}$$

Proviamo a partire da questa definizione di prodotto fra sottoinsiemi, e prendiamo due classi laterali g_1H e g_2H. Il loro prodotto naturale come sottoinsiemi è dunque il seguente sottoinsieme di G:

$$(g_1H)(g_2H) = \{g_1h_1g_2h_2 | h_1 \in H, h_2 \in H\}$$

Ora ci chiediamo: questo insieme è ancora una classe laterale di H in G?

Osserviamo che

$$g_1h_1g_2h_2 = g_1g_2g_2^{-1}h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$$

dove abbiamo usato il trucco di inserire $e = g_2g_2^{-1}$ nel prodotto che stavamo considerando. Ora notiamo che $g_2^{-1}h_1g_2$ è un elemento di H (**qui si usa in maniera cruciale il fatto che H è un sottogruppo normale**), che chiameremo $\overline{h}$. In conclusione,

$$g_1h_1g_2h_2 = g_1g_2\overline{h}h_2$$

Il calcolo appena fatto mostra che il sottoinsieme $(g_1H)(g_2H)$ di G definito sopra è contenuto nella classe laterale g_1g_2H. Inoltre è immediato verificare l'inclusione opposta (esercizio!). Dunque la definizione naturale di $(g_1H)(g_2H)$ produce come risultato il sottoinsieme g_1g_2H di G che è ancora una classe laterale.

Questa osservazione, che si è svolta a livello di sottoinsiemi di G, ci suggerisce che siamo sulla buona strada per definire un prodotto in G/H, quando H è normale. Definiamo il seguente prodotto fra due elementi g_1H e g_2H di G/H:

$$g_1Hg_2H = g_1g_2H$$

Bisogna innanzitutto verificare che questa definizione è ben posta, ossia non dipende dai rappresentanti scelti per le classi laterali g_1H e g_2H. Prendiamo dunque degli altri rappresentanti delle stesse classi laterali: il Corollario 4.22 ci dice che saranno del tipo $g_1h_1H = g_1H$ e $g_2h_2H = g_2H$ con h_1, h_2 elementi di H. Secondo la definizione di prodotto in G/H che abbiamo appena dato vale

$$g_1h_1H\ g_2h_2H = g_1h_1g_2h_2H$$

A questo punto rimane solo da controllare che i due laterali $g_1h_1g_2h_2H$ e g_1g_2H coincidono.

Ma, adottando un ragionamento simile a quello visto sopra, possiamo scrivere

$$g_1h_1g_2h_2H = g_1g_2g_2^{-1}h_1g_2h_2H = g_1g_2(g_2^{-1}h_1g_2)h_2H = g_1g_2\overline{h}h_2H$$

dove $\overline{h} \in H$ per la normalità di H, e dunque infine $g_1g_2\overline{h}h_2H = g_1g_2H$ come volevamo.[1]

La classe laterale $eH = H$ si comporta da identità rispetto al prodotto appena definito in G/H, e per ogni classe gH esiste l'inverso, che è la classe $g^{-1}H$. L'associatività del prodotto è una facile conseguenza dell'associatività del prodotto in G.

[1] Vorremmo rimarcare che il fatto che il prodotto in G/H sia ben definito discende anche direttamente dalla osservazione precedente sul prodotto di sottoinsiemi: sappiamo che il laterale g_1g_2H si può ottenere come prodotto degli insiemi g_1H e g_2H, mentre il laterale $g_1h_1g_2h_2H$ si può ottenere come prodotto degli insiemi dati dai due laterali g_1h_1H e g_2h_2H, che coincidono rispettivamente con g_1H e g_2H. Dunque i laterali $g_1h_1g_2h_2H$ e g_1g_2H coincidono.

DEFINIZIONE 7.5. Dato un gruppo G e un suo sottogruppo normale H chiameremo G/H, munito del prodotto definito sopra, il *gruppo quoziente* di G su H.

Quali sono le proprietà dei gruppi quozienti?

Alcune in qualche modo rispecchieranno le proprietà di G, altre potranno rendere G/H molto diverso da G: basti pensare al caso in cui $G = \mathbb{Z}$ con l'operazione $+$ e $H = (m)$. Osserviamo immediatamente che il gruppo quoziente $G/(m)$ è (isomorfo a) $\mathbb{Z}_m$ con l'operazione $+$. Dunque siamo partiti da un gruppo infinito ($\mathbb{Z}$) e abbiamo ottenuto come quoziente un gruppo finito.

Cominciamo ad esplorare la situazione con il seguente:

TEOREMA 7.6 (Primo teorema di omomorfismo). *Dati due gruppi G_1, G_2 e un omomorfismo $f : G_1 \to G_2$, vale che*

$$G_1/Kerf \cong \operatorname{Imm} f$$

DIMOSTRAZIONE. Osserviamo innanzitutto che il gruppo quoziente $G_1/Kerf$ è ben definito perché, come sappiamo, $Kerf$ è un sottogruppo normale di G_1. Inoltre abbiamo già osservato che $\operatorname{Imm} f$ è un sottogruppo di G_2, dunque in particolare è un gruppo.

Per dimostrare il teorema dobbiamo costruire un isomorfismo $\overline{f} : G_1/Kerf \to \operatorname{Imm} f$. Poniamo, per ogni $g_1 \in G_1$,

$$\overline{f}(g_1 Kerf) = f(g_1)$$

Per prima cosa si verifica che $\overline{f}$ è ben definito: se avessimo scelto un altro rappresentante per il laterale $g_1 Kerf$, lo avremmo indicato (in accordo con il Corollario 4.22) come $g_1 k Kerf$, con $k \in Kerf$. Ma allora secondo la definizione di $\overline{f}$ abbiamo

$$\overline{f}(g_1 k Kerf) = f(g_1 k)$$

Dato che f è un omomorfismo e $k \in Kerf$ possiamo scrivere

$$f(g_1 k) = f(g_1) f(k) = f(g_1) e_{G_2} = f(g_1)$$

dunque $\overline{f}$ è ben definito.

A questo punto possiamo verificare che $\overline{f}$ è un omomorfismo. Dati due laterali $g_1 Kerf, g_2 Kerf \in G_1/Kerf$, dobbiamo dimostrare che:

$$\overline{f}(g_1 Kerf)\overline{f}(g_2 Kerf) = \overline{f}(g_1 Kerf\ g_2 Kerf)$$

Ora osserviamo che:

$$\overline{f}(g_1 Kerf\ g_2 Kerf) = \overline{f}(g_1 g_2 Kerf) = f(g_1 g_2)$$

dove per il primo $=$ abbiamo usato la definizione di prodotto nel gruppo quoziente $G_1/Kerf$ e per il secondo $=$ abbiamo usato la definizione di $\overline{f}$. D'altra parte, sempre per la definizione di $\overline{f}$, vale:

$$\overline{f}(g_1 Kerf)\overline{f}(g_2 Kerf) = f(g_1) f(g_2)$$

Visto che f è un omomorfismo, e dunque $f(g_1 g_2) = f(g_1) f(g_2)$, abbiamo dimostrato che $\overline{f}$ è un omomorfismo.

Resta da dimostrare che $\overline{f}$ è bigettivo. Per l'iniettività, dato il Teorema 6.13, basta studiare $Ker\overline{f}$. Ora, quali classi laterali $gKerf$ vengono mandate da $\overline{f}$ in e_{G_2} (che è anche l'identità di $\operatorname{Imm} f$)? Se vale

$$\overline{f}(gKerf) = f(g) = e_{G_2}$$

allora deve essere $g \in Kerf$ dunque la classe $gKerf$ coincide con la classe $eKerf$, che è l'identità di $G_1/Kerf$. Dunque $Ker\overline{f}$ contiene un solo elemento, l'identità di $G_1/Kerf$: questo prova l'iniettività di $\overline{f}$.

Per quel che riguarda la surgettività, preso un qualunque elemento $y \in \operatorname{Imm} f$, allora possiamo scegliere $g \in G_1$ tale che $f(g) = y$. A questo punto si osserva che

$$\overline{f}(gKerf) = f(g) = y$$

dunque $\overline{f}$ è surgettivo.

□

COROLLARIO 7.7. *Dati due gruppi G_1, G_2 e un omomorfismo surgettivo $f : G_1 \to G_2$, vale che*

$$G_1/Kerf \cong G_2$$

COROLLARIO 7.8. *Dati due gruppi G_1, G_2 e un omomorfismo iniettivo $f : G_1 \to G_2$, vale che*

$$G_1 \cong \operatorname{Imm} \ f$$

Concludiamo questo paragrafo tornando sulla affermazione "un sottogruppo è normale se e solo se esiste un omomorfismo di cui è il nucleo". Abbiamo già dimostrato una delle due implicazioni, ora siamo pronti per dimostrare l'altra:

PROPOSIZIONE 7.9. *Dato un gruppo G_1 e un suo sottogruppo normale H, la funzione $\pi_H : G_1 \to G_1/H$ definita da $\pi(g) = gH$ per ogni $g \in G_1$ è un omomorfismo surgettivo (su G_1/H consideriamo la struttura di gruppo quoziente), con nucleo uguale ad H. Tale omomorfismo si chiama* proiezione al quoziente *di G_1 rispetto ad H.*

DIMOSTRAZIONE. Tutte le proprietà indicate sono di facile dimostrazione. Per esempio, il fatto che π_H sia un omomorfismo richiede la verifica che, dati $g_1, g_2 \in G_1$ vale

$$\pi_H(g_1g_2) = g_1g_2H = g_1Hg_2H = \pi_H(g_1)\pi_H(g_2)$$

dove l' = centrale è dato proprio dalla definizione di prodotto in G_1/H. □

Osserviamo infine che il primo teorema di omomorfismo e la proposizione precedente ci permettono di dire che, dato un gruppo G, ogni suo quoziente rispetto ad un sottogruppo normale è isomorfo all'immagine di G tramite un certo omomorfismo, e viceversa, ogni immagine di G tramite un omomorfismo è isomorfa ad un quoziente di G per un suo sottogruppo normale.

2. Qualche esempio

2.1. Quoziente di un gruppo ciclico. Sia C un gruppo ciclico (finito o infinito), generato da un elemento x: $C = (x)$. Se consideriamo un sottogruppo H di C, questo sarà normale visto che C è commutativo. Vogliamo studiare il gruppo quoziente C/H.

Possiamo per questo considerare l'omomorfismo $\pi_H : C \to C/H$.

Poiché x genera C, allora $\pi_H(x) = xH$ genera C/H, vista la surgettività di π_H e il fatto che $\pi_H(x^j) = \pi_H(x)^j$ per le proprietà di omomorfismo. Dunque C/H è ciclico.

Analizziamo vari casi. Se $H = \{e\}$, dalla Proposizione 7.9 ricaviamo che π_H è iniettiva e surgettiva, dunque si tratta di un isomorfismo: vale allora $C \cong C/H$, cosa che del resto avremmo potuto verificare direttamente in questo caso molto semplice.

Se $H = C$ (il che equivale a dire che $x \in H$), C/H contiene un solo elemento, ed è il gruppo banale formato solo dall'identità.

Supponiamo allora che $\{e\} \subsetneq H \subsetneq C$. Visto che $x \notin H$, possiamo considerare il più piccolo intero positivo m tale che $x^m \in H$ (tale intero deve esistere perchè x genera C). Sappiamo già che C/H è ciclico e generato da xH, ora possiamo aggiungere l'informazione che $x^m H = H$ e che l'ordine di xH è proprio m, dunque C/H ha cardinalità m, ed è costituito dai seguenti elementi:

$$H, xH, x^2H, ..., x^{m-1}H$$

2.2. Una osservazione sui gruppi ciclici finiti. Applichiamo quanto visto nel paragrafo precedente al caso in cui $C = (x)$ sia un gruppo ciclico finito di cardinalità n che possiede un sottogruppo H diverso da $\{e\}$ e da C stesso. Questo ci permetterà di rileggere da un altro punto di vista lo studio sui gruppi ciclici del Paragrafo 2 del Capitolo 6.

Come sappiamo, C/H ha cardinalità m, dove m è il più piccolo intero positivo tale che $x^m \in H$. Da questo segue che H ha cardinalità $\frac{n}{m}$ per considerazioni già comparse nella dimostrazione del Teorema di Lagrange (Teorema 4.23): infatti le classi laterali di H sono m, hanno tutte cardinalità uguale a $|H|$, e costituiscono una partizione dell'insieme C, per cui vale la relazione

$$m\ |H| = n$$

Questo ci permette (di nuovo) di concludere che in C c'è un solo sottogruppo di ordine $d = \frac{n}{m}$, ed è proprio H. Infatti supponiamo che anche H' sia un sottogruppo di ordine $\frac{n}{m}$. Allora il quoziente G/H' deve avere cardinalità m per le considerazioni appena viste sulla cardinalità delle classi di resto. Inoltre, per quello che sappiamo dal paragrafo precedente, m è il più piccolo intero positivo tale che $x^m \in H'$.

Dunque x^m appartiene sia ad H sia ad H'. Inoltre x^m è un elemento di ordine d (se avesse ordine minore, allora x avrebbe un ordine minore di n, assurdo). Questo ci permette di concludere che il sottoinsieme di C:

$$\{e, x^m, (x^m)^2 = x^{2m}, ..., x^{(d-1)m}\}$$

è costituito da d elementi distinti, ed essendo contenuto sia in H sia in H' coincide con entrambi. Da qui ritroviamo immediatamente i risultati del Corollario 6.17.

2.3. Il quoziente $\mathbb{R}/\mathbb{Z}$. Consideriamo la funzione $g : \mathbb{R} \to \mathbb{C}$ definita da $g(\alpha) = \cos 2\pi\alpha + i \sin 2\pi\alpha$ per ogni $\alpha \in \mathbb{R}$.[2]

Si osserva subito che Imm g coincide con il sottoinsieme $\mathcal{C}$ di $\mathbb{C}$ dato dagli elementi di norma 1 (ossia dai punti della circonferenza di raggio 1 centrata nell'origine). Se consideriamo $\mathbb{R}$ come gruppo rispetto all'addizione e $\mathcal{C}$ come gruppo con la moltiplicazione 'ereditata' da $\mathbb{C}$ (è un sottogruppo moltiplicativo di $\mathbb{C}$), le regole della moltiplicazione in $\mathbb{C}$ ci permettono di verificare facilmente che g è un omomorfismo.

Qual è il suo nucleo? Si tratta degli elementi $\alpha \in \mathbb{R}$ tali che $g(\alpha) = \cos 2\pi\alpha + i \sin 2\pi\alpha = 1$, e questo accade se e solo se $\alpha \in \mathbb{Z}$. Dunque per il Teorema 7.6 possiamo concludere che $\mathbb{R}/\mathbb{Z}$ è isomorfo al gruppo $\mathcal{C}$.

3. Esercizi su prodotti diretti, generatori e sottogruppi (lezioni del 3 e 4 novembre)

In questa sezione facciamo alcune considerazioni ed esempi in forma di sequenza di esercizi.

[2]Il numero complesso $\cos 2\pi\alpha + i \sin 2\pi\alpha$ viene indicato come $e^{2\pi i\alpha}$ e la funzione g che stiamo considerando è dunque l'esponenziale complesso che manda $\alpha \in \mathbb{R}$ in $e^{2\pi i\alpha}$.

DEFINIZIONE 7.10. Siano G_1 e G_2 due gruppi. Definiamo il *prodotto diretto (cartesiano)* di G_1 e G_2 come l'insieme $G_1 \times G_2$ con l'operazione definita da

$$(g_1, g_2) \cdot (g_1', g_2') := (g_1 g_1', g_2 g_2')$$

per ogni $(g_1, g_2), (g_1', g_2') \in G_1 \times G_2$.

ESERCIZIO 7.11. Siano G_1 e G_2 due gruppi.

(1) Mostrare che il prodotto diretto $G_1 \times G_2$ è un gruppo.
(2) Mostrare che se $g_1 \in G_1$ ha ordine n_1 e $g_2 \in G_2$ ha ordine n_2, allora $(g_1, g_2) \in G_1 \times G_2$ ha ordine $mcm(n_1, n_2)$.
(3) Mostrare che $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ non sono isomorfi.
(4) Mostrare che ogni gruppo di ordine 4 è isomorfo a $\mathbb{Z}_4$ o a $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(5) Elencare tutti i sottogruppi di ordine 2 e tutti i sottogruppi di ordine 4 di $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
(6) Determinare se $\mathbb{Z}_4 \times \mathbb{Z}_3$ è isomorfo a $\mathbb{Z}_{12}$.
(7) Determinare se $\mathbb{Z}_2 \times \mathbb{Z}_6$ è isomorfo a $\mathbb{Z}_{12}$.

La seguente definizione e i seguenti esercizi approfondiscono il concetto di insieme di generatori di un gruppo o sottogruppo (la definizione di insieme di generatori di un gruppo è già comparsa in queste dispense come premessa ad alcuni esercizi sul gruppo simmetrico, vedi Definizione 6.42).

DEFINIZIONE 7.12. Sia G un gruppo, e sia $X \subseteq G$ un sottoinsieme di G. Denotiamo con X^{-1} l'insieme degli inversi degli elementi di X. Definiamo allora

$$(X) := \{y_1 y_2 \cdots y_k \mid k \in \mathbb{N}, y_i \in X \cup X^{-1} \text{ per ogni } i\} \subseteq G,$$

ossia (X) è l'insieme di tutti i possibili prodotti di elementi (non necessariamente distinti) di X e dei loro inversi. Per convenzione, se $X = \varnothing$, poniamo $(\varnothing) = \{e\}$, dove e è il neutro di G.

ESERCIZIO 7.13. Sia G un gruppo e $X \subseteq G$ un sottoinsieme di G.

(1) Mostrare che (X) è un sottogruppo di G, detto *sottogruppo generato da* X. Se $(X) = G$ diciamo che X *genera* G, e chiamamo gli elementi di X *generatori* di G.
(2) Mostrare che se H è un sottogruppo di G e $X \subseteq H$, allora $(X) \subseteq H$.
(3) Verificare che $(G) = G$, e che se $g \in G$, allora $(g) = (\{g\})$.
(4) Mostrare che se X genera G, ossia $(X) = G$, e Y è un sottoinsieme di G contenente X, ossia $X \subseteq Y \subseteq G$, allora anche Y genera G, ossia $(Y) = G$.
(5) Elencare tutti i sottoinsiemi $X \subseteq \mathbb{Z}_4$ tali che $(X) = \mathbb{Z}_4$.

L'intersezione di sottogruppi è ancora un sottogruppo.

ESERCIZIO 7.14. Sia G un gruppo e sia $\{H_i\}_{i \in I}$ una famiglia di sottogruppi di G (dove I è una famiglia di indici, anche infinita). Allora l'intersezione $\bigcap_{i \in I} H_i$ è un sottogruppo di G.

ESERCIZIO 7.15. Sia G un gruppo e sia $X \subseteq G$ un sottoinsieme di G. Allora (X) è il più piccolo sottogruppo che contiene X, ossia (X) è l'intersezione di tutti i sottogruppi di G che contengono X.

La nozione di generatori di un gruppo è utile in molti modi. In particolare permette di lavorare più facilmente con gli omomorfismi.

ESERCIZIO 7.16. Sia G un gruppo e $X \subseteq G$ un sottoinsieme di G. Mostrare che se $(X) = G$, G_2 è un altro gruppo e $f : G \to G_2$ è un omomorfismo, allora f è determinato dalle immagini $f(y)$ per $y \in X$.

DEFINIZIONE 7.17. Nel piano $\mathbb{R}^2$ consideriamo un poligono regolare P_n con n lati, $n \geq 3$, il cui baricentro è l'origine. Sia D_n l'insieme delle isometrie del piano $\mathbb{R}^2$ che mandano P_n in se stesso. Ad esempio la rotazione $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ di centro l'origine e di angolo $2\pi/n$ in senso antiorario è un elemento di D_n. Un altro elemento di D_n è la riflessione $r : \mathbb{R}^2 \to \mathbb{R}^2$ rispetto a una retta fissata che passa per il centro di P_n e per il punto medio di uno dei suoi lati.

ESERCIZIO 7.18.
(1) Verificare che D_n con la composizione di funzioni è un gruppo, detto *gruppo diedrale*.
(2) Verificare geometricamente la relazione $r\rho r = \rho^{-1}$.
(3) Mostrare che D_n ha $2n$ elementi:

$$D_n = \{Id_{\mathbb{R}^2}, \rho, \rho^2, \dots, \rho^{n-1}, r, r\rho, r\rho^2 \dots, r\rho^{n-1}\}.$$

Il gruppo diedrale si può "incarnare" naturalmente come un sottogruppo di S_n.

ESERCIZIO 7.19. Nel piano $\mathbb{R}^2$ consideriamo un poligono regolare P_n con n lati, $n \geq 3$, il cui baricentro è l'origine. Denotiamo con in numeri $1, 2, \dots, n$ i vertici consecutivi di P_n in senso antiorario, e sia r la riflessione rispetto alla retta passante per il centro di P_n e per il punto medio del lato di vertici 1 e n.

(1) Verificare che D_n agisce su P_n permutando i suoi vertici, e che ogni elemento di D_n è determinato dalla corrispondente permutazione dei vertici, che si può vedere come un elemento di S_n.
(2) Scrivere esplicitamente le permutazioni di S_n corrispondenti a ρ e r, e verificare che queste generano un sottogruppo di S_n di ordine $2n$.
(3) Calcolare il centro $Z(D_n)$ di D_n per ogni n.

4. Esercizi

ESERCIZIO 7.20. Dimostrare che un sottogruppo H di un gruppo G è normale se e solo se gli H-laterali sinistri coincidono con gli H-laterali destri, ossia, per ogni $g \in G$ vale

$$gH = Hg$$

ESERCIZIO 7.21. Sia G un gruppo e siano H_i dei sottogruppi ($i \in I$, dove I è una famiglia di indici, anche infinita). È vero che se tutti gli H_i sono normali allora $\bigcap_{i \in I} H_i$ è normale?

ESERCIZIO 7.22. Dato un gruppo G e un sottogruppo H, dimostrare che se l'insieme G/H ha solo due elementi allora H è normale.

ESERCIZIO 7.23. Dati $A = \{e, (1,2)\}$ e $B = \{e, (2,3)\}$ sottoinsiemi di S_3, dimostrare che AB non è un sottogruppo.

ESERCIZIO 7.24. Siano A e B sottogruppi di un gruppo finito G. Dimostrare che

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

(questo vale anche se AB non è un sottogruppo).

ESERCIZIO 7.25. Dare un esempio di tre gruppi $H < K < G$ tali che K è normale in G, H è normale in K ma H non è normale in G.

Esercizio 7.26. Consideriamo un gruppo G e un suo sottogruppo normale H. Dimostrare che la proiezione $\pi_H : G \to G/H$ induce una corrispondenza bigettiva fra l'insieme dei sottogruppi di G/H e l'insieme dei sottogruppi di G che contengono H.

Esercizio 7.27 (Il sottogruppo di Klein[3]). Si consideri il seguente sottoinsieme di S_4:

$$K = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

Dimostrare che K è un sottogruppo normale di S_4 (viene chiamato *sottogruppo di Klein*), isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Esercizio 7.28. Chiamiamo $A = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ l'insieme dei tre elementi del gruppo di Klein diversi dall'identità. Consideriamo l'insieme $Big(A)$ delle funzioni bigettive da A in sé. Con l'operazione di composizione, è un gruppo isomorfo a S_3. Consideriamo la funzione $f : S_4 \to Big(A)$ definita così: per ogni $\sigma \in S_4$, $f(\sigma)$ è l'elemento di $Big(A)$ tale che per ogni $x \in A$ vale $f(\sigma)(x) = \sigma x \sigma^{-1}$. Dimostrare che f è un omomorfismo di gruppi e, utilizzando il primo teorema di omomorfismo, che $S_4/K \cong S_3$.

Esercizio 7.29. Verificare che il sottogruppo di Klein è sottogruppo di A_4, oltre che di S_4. Dimostrare che $A_4/K \cong \mathbb{Z}_3$.

Esercizio 7.30. Dare un esempio di un gruppo G con due sottogruppi normali H e K tali che $H \cong K$ ma G/H non è isomorfo a G/K. Dimostrare che invece se esiste un $\phi \in Aut(G)$ tale che $\phi(H) = K$ allora G/H è isomorfo a G/K.

Esercizio 7.31. Dare un esempio di quattro gruppi $H_1 < G_1$, $H_2 < G_2$, con $H_1 \cong H_2$, $G_1/H_1 \cong G_2/H_2$ ma G_1 non è isomorfo a G_2.

Esercizio 7.32. Trovare in S_4 tre sottogruppi distinti isomorfi a D_4. Elencare gli elementi di questi sottogruppi.

Esercizio 7.33. Sia $n \geq 1$. Dimostrare che, dato un qualunque sottogruppo H di S_n vale $H < A_n$ oppure $|H \cap A_n| = \dfrac{|H|}{2}$.

[3]Christian Felix Klein, matematico tedesco, 1849 - 1925.

CAPITOLO 8

Anelli e ideali

1. Anelli

1.1. Definizioni. In questo paragrafo presenteremo in maniera formale la definizione di anello con unità, già accennata fin dalle prime lezioni del corso, e discuteremo alcune proprietà fondamentali.

DEFINIZIONE 8.1. Un anello con unità R è un insieme dove sono definite due operazioni, che chiamiamo addizione $(+)$ e moltiplicazione $(\cdot)$, che soddisfano le seguenti proprietà:

- R è un gruppo commutativo rispetto all'operazione $+$. Indicheremo con 0 l'elemento neutro rispetto alla somma, e per ogni $a \in \mathbb{R}$ indicheremo con $-a$ il suo inverso rispetto alla somma, che chiameremo *opposto*.
- $\forall\ a, b, c \in R$ vale $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (proprietà associativa della moltiplicazione).
- esiste un elemento $1 \in R$ tale che $\forall\ a \in R$ vale $a \cdot 1 = 1 \cdot a = a$ (1 è l'elemento neutro per il prodotto).
- $\forall\ a, b, c \in R$ vale $(a + b) \cdot c = a \cdot c + b \cdot c$ e anche $a \cdot (b + c) = a \cdot b + a \cdot c$ (proprietà distributive).

OSSERVAZIONE 8.2. Come sappiamo dalla teoria dei gruppi (vedi Teorema 4.4), l'elemento 0 è unico e inoltre per ogni $a \in \mathbb{R}$ l'opposto di a è unico. Analogamente si dimostra che l'elemento 1 è unico.

Segnaliamo subito che la definizione include anche l'anello banale $A = \{0\}$, in cui tutte le operazioni sono banali e dunque lo 0 funziona da elemento neutro per la somma e anche per la moltiplicazione (0=1).

OSSERVAZIONE 8.3. In questo corso, quando useremo la parola 'anello', intenderemo sempre un anello con unità (in generale si può dare la definizione di anello senza la richiesta che esista l'elemento 1, e in diversi contesti risulta utile lavorare con anelli senza 1).

DEFINIZIONE 8.4. Un anello R che soddisfa anche la seguente proprietà si dice *commutativo*:

- $\forall\ a, b \in R$ vale $a \cdot b = b \cdot a$ (proprietà commutativa della moltiplicazione).

DEFINIZIONE 8.5. Sia R un anello commutativo. Diciamo che $a \in R$ è un *divisore di zero* se esiste $b \in R$, $b \neq 0$ tale che $ab = 0$. In particolare, 0 è un divisore di 0. Un anello commutativo R in cui $0 \neq 1$ e in cui l'unico divisore di 0 è 0 si chiama *dominio* (o *dominio di integrità*).

DEFINIZIONE 8.6. Un elemento u di un anello R si dice *invertibile* se esiste $v \in R$ tale che $u \cdot v = v \cdot u = 1$ (cioè se esiste un inverso sinistro e destro di u rispetto alla moltiplicazione). Denotiamo con R^* l'insieme degli elementi invertibili di R.

ESERCIZIO 8.7. Sia R un anello. Dimostrare che R^* è un gruppo rispetto alla moltiplicazione.

DEFINIZIONE 8.8. Due elementi a, b di un anello commutativo R si dicono *associati* se $a = bu$ con $u \in R^*$.

DEFINIZIONE 8.9. Un anello R in cui $0 \neq 1$ che soddisfa anche la seguente proprietà è detto *corpo*:

- ogni $a \in R - \{0\}$ è invertibile (esistenza dell'inverso rispetto alla moltiplicazione per tutti gli elementi diversi da 0).

Un corpo commutativo viene detto *campo*.

1.2. Primi esempi. Sono esempi di anelli commutativi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_m$ per ogni $m > 1$. Gli anelli $\mathbb{Q}$ ed $\mathbb{R}$ sono anche dei campi mentre $\mathbb{Z}$ non è un campo (non esiste in $\mathbb{Z}$ l'inverso rispetto alla moltiplicazione degli elementi diversi da 1 e -1, per esempio non esiste in $\mathbb{Z}$ l'inverso di 8). Come esempio di un anello non commutativo, avete già visto nel corso di Geometria 1 l'anello $Mat_{n\times n}(K)$ delle matrici $n \times n$ a coefficienti in un campo K. È non commutativo se $n \geq 2$.

Un esempio di corpo che non è un campo è fornito dal corpo $\mathbb{H}$ dei quaternioni (vedi Esercizio 8.34).

Per quel che riguarda gli anelli $\mathbb{Z}_m$ osserviamo che se il numero m non è primo, $\mathbb{Z}_m$ ha dei divisori dello zero diversi da $[0]_m$, dunque non è un dominio. Infatti in tal caso m si fattorizza come $m = k \cdot s$ con $1 < k < m$ e $1 < s < m$ e vale che

$$[k]_m[s]_m = [ks]_m = [m]_m = [0]_m$$

Come conseguenza, se m non è primo, $\mathbb{Z}_m$ non è un campo (vedremo fra poco, nell'Osservazione 8.13, che un campo è automaticamente un dominio, comunque potete fin d'ora mostrare -facile esercizio- che non può esistere l'inverso degli elementi $[k]_m$ e $[s]_m$...). Vale invece il seguente importante teorema:

TEOREMA 8.10. *Se p è un numero primo, $\mathbb{Z}_p$ è un campo.*

DIMOSTRAZIONE. Se prendiamo una classe $[a]_p \neq [0]_p$ in $\mathbb{Z}_p$, visto che p non divide a, vale che $MCD(a, p) = 1$. Allora la congruenza $ax \equiv 1 \quad (p)$ ha soluzione, dunque esiste $b \in \mathbb{Z}$ tale che $ab \equiv 1 \quad (p)$. Come conseguenza in $\mathbb{Z}_p$ vale $[a]_p[b]_p = [ab]_p = [1]_p$. Dunque $[a]_p$ è invertibile in $\mathbb{Z}_p$ e $[b]_p$ è il suo inverso.

□

1.3. Prime osservazioni. Il seguente lemma ci rassicura sul fatto che, a partire dalla definizione di anello, possiamo ricavare alcune proprietà a noi molto familiari (se si moltiplica un elemento per 0 si ottiene 0, 'meno' per 'meno' fa più...etc...).

LEMMA 8.11. *Sia A un anello, allora per ogni a, b in A vale:*

(1) $a \cdot 0 = 0$ *e* $0 \cdot a = 0$
(2) *l'opposto di a è unico e* $-(-a) = a$
(3) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$, *in particolare* $(-1) \cdot a = a \cdot (-1) = -a$.
(4) $(-a) \cdot (-b) = a \cdot b$, *in particolare* $(-1) \cdot (-1) = 1$.

DIMOSTRAZIONE. (1) Dimostriamo che $a \cdot 0 = 0$ (l'altra uguaglianza si dimostra in maniera analoga). Per prima cosa scriviamo $a \cdot (0 + 0) = a \cdot 0$ utilizzando il fatto che 0 è l'elemento neutro per la somma. A questo punto per la proprietà distributiva abbiamo $a\cdot(0+0) = a\cdot0+a\cdot0$. Dunque abbiamo ottenuto $a\cdot0+a\cdot0 = a\cdot0$. Sottraendo a destra e a sinistra l'opposto di $a \cdot 0$ (che esiste appunto perché A è un anello), otteniamo

$$a \cdot 0 = 0$$

(2) Queste proprietà sono state già dimostrate per i gruppi (Teorema 4.4), dunque non vanno ridimostrate. Le abbiamo inserite in questo lemma per comodità, per presentarle nella notazione additiva.
(3) Per dimostrare che $a \cdot (-b) = -(a \cdot b)$, dobbiamo mostrare che $a \cdot b + a \cdot (-b) = 0$. Utilizzando la proprietà distributiva, si scrive $a \cdot b + a \cdot (-b) = a \cdot (b + (-b))$. Ora, visto che $-b$ è l'opposto di b possiamo proseguire:

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

dove l'ultima uguaglianza segue dal punto (1) appena dimostrato.
(4) Applichiamo due volte il punto (3):

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b))$$

Come sappiamo dal punto (2), $-(-(a \cdot b)) = a \cdot b$ e questo conclude la dimostrazione.

□

D'ora in avanti, visto che l'opposto e lo 0 ubbidiscono alle regole a noi familiari, saremo liberi di scrivere $a - b$ invece di $a + (-b)$. Inoltre, ometteremo spesso il segno $\cdot$ della moltiplicazione.

Osservazione 8.12. Dalla proprietà (1) segue in particolare che se in un anello abbiamo $0 = 1$ allora per ogni elemento a possiamo scrivere la $a \cdot 0 = 0$ come $a = a \cdot 1 = a \cdot 0 = 0$ e dunque risulta che l'anello A è l'anello banale. Dunque l'unico anello con unità in cui $0 = 1$ è l'anello banale.

Osservazione 8.13. Un campo è anche automaticamente un dominio: infatti, se in un campo K per assurdo valesse $b \cdot r = 0$ per due elementi b, r diversi da 0 allora potremmo moltiplicare entrambi i membri per l'inverso di b, che chiameremo c, ottenendo

$$c \cdot (b \cdot r) = c \cdot 0$$

da cui, tenendo conto della proprietà associativa, del fatto che $c \cdot b = 1$ e del fatto che $c \cdot 0 = 0$ (punto (1) del Lemma 8.11), abbiamo $r = 0$, assurdo.

Osservazione 8.14. In ogni dominio R vale la *legge di cancellazione*, ossia, se $a \in R$ è diverso da 0, l'uguaglianza

$$ab = ac$$

implica

$$b = c$$

Infatti la $ab = ac$ si può riscrivere come $ab - ac = 0$ e, per la proprietà distributiva, come $a(b - c) = 0$. A questo punto, visto che $a \neq 0$ e che R è un dominio e dunque non ha divisori di 0 diversi da 0, deve valere $b - c = 0$, ovvero $b = c$.

La legge di cancellazione non è vera in generale per gli anelli. Basti pensare per esempio a $\mathbb{Z}_{12}$, dove abbiamo $[3][4] = [3][8]$ ma non è vero che $[4] = [8]$.[1]

Chiudiamo il paragrafo dando la definizione di sottoanello.

Definizione 8.15. Dato un anello R, un *sottoanello* di R è un sottoinsieme $T \subseteq R$ tale che valgano le seguenti tre condizioni:

- $1 \in T$;
- T è un sottogruppo di R rispetto alla operazione $+$;

[1] Come avete visto, abbiamo scritto $[4]$ e non $[4]_{12}$. Ometteremo l'indice per alleggerire la notazione tutte le volte in cui sarà ben chiaro in quale anello stiamo lavorando.

- per ogni $a, b \in T$ vale $ab \in T$.

Se $T \neq R$ si dice che T è un sottoanello *proprio*.

2. Omomorfismi

DEFINIZIONE 8.16. Siano R e S due anelli. Una funzione $\phi : R \to S$ si dice *omomorfismo di anelli* se e solo se, per ogni $a, b \in R$

1) $\phi(a+b) = \phi(a) + \phi(b)$;
2) $\phi(ab) = \phi(a)\phi(b)$;
3) $\phi(1_R) = 1_S$.

Se un omomorfismo ϕ è sia iniettivo che surgettivo si dice *isomorfismo*.

DEFINIZIONE 8.17. Se $\phi : R \to S$ è un omomorfismo di anelli, definiamo *nucleo* di ϕ l'insieme $\ker \phi = \{a \in R \mid \phi(a) = 0_S\}$, dove 0_S è l'elemento neutro rispetto alla somma in S.

LEMMA 8.18. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora $\ker \phi$ è un sottogruppo additivo di R. Inoltre, se $a \in \ker \phi$ e $r \in R$ allora $ar \in \ker \phi$ e $ra \in \ker \phi$.*

DIMOSTRAZIONE. Dal momento che ϕ è, in particolare, un omomorfismo di gruppi additivi, la prima parte è già per noi nota.
Siano ora $a \in \ker \phi$ e $r \in R$. Vediamo che $\phi(ar) = \phi(a)\phi(r) = 0_S\phi(r) = 0_S$, e quindi $ar \in \ker \phi$. Allo stesso modo si dimostra che $ra \in \ker \phi$. □

OSSERVAZIONE 8.19. Sia $\phi : R \to S$ un omomorfismo di anelli. Visto che in particolare ϕ è anche un omomorfismo di gruppi abeliani, il Teorema 6.13 ci dice che ϕ è iniettivo se e solo se $\ker \phi = \{0_R\}$.

L'Esercizio 8.31 vi inviterà a riflettere sul fatto che in generale il nucleo di un omomorfismo di anelli $\phi : R \to S$ non è un sottoanello di R. Infatti nella definizione di omomorfismo fra anelli è inclusa la richiesta che $\phi(1_R) = 1_S$, dunque $1_R \notin Ker\phi$ a meno che S non sia l'anello banale.

Nessuna sorpresa invece per quel che riguarda l'immagine di un omomorfismo fra anelli:

ESERCIZIO 8.20. Sia $\phi : R \to S$ un omomorfismo. Dimostrare che $\phi(R)$ è un sottoanello di S.

3. Ideali di un anello e anelli quoziente

Lo studio dei nuclei degli omomorfismi ha messo in luce che in un anello ci sono alcuni sottoinsiemi notevoli che non sono sottoanelli. La seguente definizione li individua:

DEFINIZIONE 8.21. Un *ideale* I di un anello R è un sottogruppo additivo tale che per ogni $r \in R$ e per ogni $h \in I$ allora $rh \in I$ e $hr \in I$. Se $I \neq R$ si dice che I è un *ideale proprio*.

La proprietà moltiplicativa che caratterizza gli ideali ci dice che I 'assorbe' la moltiplicazione a destra e a sinistra per elementi arbitrari dell'anello (sottolineiamo che la definizione che abbiamo dato è dunque quella di ideale *bilatero*: in questo corso, visto che lavoreremo quasi esclusivamente con anelli commutativi, non avremo bisogno di approfondire il concetto di ideale non bilatero).

OSSERVAZIONE 8.22. Un ideale I non è un sottoanello di R, a parte il caso $I = R$. Infatti se $1 \in I$ allora $I = R$, per la proprietà di 'assorbimento'.

Esempio 8.23. Sia $R = \mathbb{Z}$. L'insieme $6\mathbb{Z} = (6)$ composto da tutti i multipli di 6 ci fornisce l'esempio di un ideale. In generale, dato un anello commutativo R e un elemento $a \in R$, denoteremo (a) l'insieme di tutti gli elementi dell'anello che si possono scrivere come ak per un certo $k \in R$. Si verifica facilmente che (a) è un ideale, e si chiama l'*ideale generato da* a. Notate che, dato un gruppo G e un elemento $g \in G$ avevamo chiamato (g) il sottogruppo ciclico generato da g. Le due notazioni riguardano due concetti diversi, ma non si creerà confusione perché sarà sempre chiaro dal contesto a quale caso ci stiamo riferendo. Per l'appunto se $G = \mathbb{Z}$ le due notazioni coincidono: il sottogruppo ciclico (6) (pensando $\mathbb{Z}$ come gruppo con la $+$) coincide con l'ideale (6) (pensando $\mathbb{Z}$ come anello).

Osservazione 8.24. Abbiamo visto nel Lemma 8.18 che il nucleo di un omomorfismo $\phi : R \to S$ è un ideale di R.

Esercizio 8.25. Dimostrare che se I e J sono due ideali dell'anello R allora anche $I + J = \{i + j \mid i \in I, j \in J\}$ e $I \cap J$ sono ideali di R.

Esercizio 8.26. Dimostrare che se I e J sono due ideali dell'anello R allora anche IJ, l'insieme degli elementi che si possono scrivere come somme finite di elementi della forma ij, con $i \in I$ e $j \in J$, è un ideale di R. Dimostrare inoltre che $IJ \subset I \cap J$ e che l'inclusione può essere stretta.

Dato un ideale I in un anello R denotiamo con R/I l'insieme dei laterali di I in R, considerando I come sottogruppo additivo di R. Possiamo scrivere gli elementi di R/I con la notazione additiva $a + I$, con $a \in R$, e per quanto abbiamo visto nel Paragrafo 1 del Capitolo 7 sappiamo che possiamo dare a R/I una struttura di gruppo additivo, con la somma definita da: $(a + I) + (b + I) = (a + b) + I$.

Per dotare R/I di una struttura di anello dobbiamo definire ora una moltiplicazione. La cosa più naturale è definire $(a + I)(b + I) = ab + I$. Dobbiamo però assicurarci che si tratti di una buona definizione, ovvero dobbiamo verificare che se $a + I = a' + I$ e se $b + I = b' + I$ allora vale $ab + I = a'b' + I$. Dal Corollario 4.22 riformulato con la notazione additiva, sappiamo che se $a + I = a' + I$ allora $a = a' + i_1$ con $i_1 \in I$; analogamente se $b + I = b' + I$ allora $b = b' + i_2$ con $i_2 \in I$. Ne segue

$$ab = (a' + i_1)(b' + i_2) = a'b' + a'i_2 + i_1b' + i_1i_2,$$

ed essendo I un ideale di R abbiamo che per la proprietà di assorbimento (destra e sinistra) $a'i_2, i_1b', i_1i_2 \in I$, e inoltre per il fatto che un ideale è in particolare un sottogruppo additivo abbiamo $a'i_2 + b'i_1 + i_1i_2 \in I$, dunque $ab + I = a'b' + I$. Quindi l'operazione di moltiplicazione è ben definita.

Esercizio 8.27. Verificare che R/I, con le operazioni somma e prodotto definite sopra, è un anello con unità (l'elemento neutro del prodotto è $1 + I$).

Osservazione 8.28. Abbiamo appena *definito* la moltiplicazione nel quoziente con l'uguaglianza $(a + I)(b + I) = ab + I$. Questa è una definizione in cui le classi laterali sono pensate come elementi del quoziente R/I.

Pensiamole invece adesso come sottoinsiemi di R. Osserviamo che in R vale, dal punto di vista insiemistico,

$$(a + I)(b + I) = \{(a + i_1)(b + i_2) \mid i_1, i_2 \in I\} \subseteq ab + I$$

dove l'ultima inclusione può essere stretta. Prendiamo come esempio $\mathbb{Z}$ e l'ideale $I = 6\mathbb{Z}$: si ha $(2 + 6\mathbb{Z})(4 + 6\mathbb{Z}) \subsetneq 8 + 6\mathbb{Z}$. Infatti 14 appartiene al laterale $8 + 6\mathbb{Z}$, ma non può essere scritto come $(2 + 6k)(4 + 6h)$ con h, k interi.

Compiuta la costruzione dell'anello quoziente di un anello rispetto ad un suo ideale possiamo ora enunciare per gli anelli il primo teorema di omomorfismo, analogo a quello per i gruppi. Lasciamo a voi la dimostrazione come utile esercizio di ripasso, visto che è semplicemente una traduzione parola per parola nel linguaggio degli anelli della dimostrazione già vista per i gruppi:

TEOREMA 8.29. *Siano R e S due anelli, e sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

$$R/\ker\phi \cong \text{Imm } \phi$$

ESERCIZIO 8.30. Dimostrare il teorema appena enunciato.

4. Esercizi

ESERCIZIO 8.31. Si consideri la funzione $f : \mathbb{Z} \to \mathbb{Z}_{10}$ definita da $f(x) = [x]_{10}$ per ogni $x \in \mathbb{Z}$. Dimostrare che si tratta di un omomorfismo di anelli e descrivere $Kerf$. Il nucleo $Kerf$ è un sottoanello di $\mathbb{Z}$?

ESERCIZIO 8.32. Se $R = \mathbb{Z}$ e $I = m\mathbb{Z} = (m)$ con m intero positivo, dimostrare che l'anello quoziente R/I è isomorfo a $\mathbb{Z}_m$.

ESERCIZIO 8.33. Dato un anello R ed un ideale I, dimostrare che se R è commutativo allora è commutativo anche R/I. Mostrare invece un esempio di un anello R non commutativo e di un ideale I tali che R/I sia commutativo. [Ovviamente l'ideale $I = R$ funziona per questo esempio. Riuscite a immaginare un esempio con I ideale proprio?]

ESERCIZIO 8.34 (Il corpo dei quaternioni di Hamilton[2]). Il corpo dei quaternioni estende il campo dei numeri complessi. Come insieme è definito così:

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

dove $\mathbf{i}, \mathbf{j}, \mathbf{k}$ sono simboli. La somma è definita da :

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = a + a' + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$$

mentre la moltiplicazione è definita facendo la moltiplicazione come la fareste intuitivamente e raccogliendo poi i termini utilizzando le relazioni:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k},\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i},\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

Qual è l'unità rispetto alla moltiplicazione? Trovare l'inverso di $1 + 2\mathbf{i} + 3\mathbf{j} + 4\mathbf{k}$.

ESERCIZIO 8.35. Siano R e S due anelli, e sia $\phi : R \to S$ un omomorfismo di anelli. Dato un ideale I di S dimostrare che il sottoinsieme Γ di R definito da

$$\Gamma = \{x \in R \mid \phi(x) \in I\}$$

è un ideale di R che contiene $Ker\phi$. [Di solito Γ viene indicato come $\phi^{-1}(I)$.]

ESERCIZIO 8.36. Dimostrare che un dominio di integrità finito è un campo.

[2]William Rowan Hamilton, fisico e matematico irlandese, 1805-1865.

CAPITOLO 9

Polinomi

1. L'algoritmo di Euclide per i polinomi

Sia K un campo, e consideriamo l'insieme $K[x]$ dei polinomi nella variabile x a coefficienti in K. Dunque un elemento $f(x)$ di $K[x]$ è della forma

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

dove $a_i \in K$ per ogni $i = 0, 1, 2, \ldots, n$. Con questa scrittura, nel caso in cui $f(x)$ non è nullo, intendiamo che $a_n \neq 0$ (chiameremo a_n il *coefficiente direttore* di $f(x)$). In questo caso, n è il *grado* del polinomio $f(x)$, che denotiamo con $\deg(f(x))$. Per convenzione, il polinomio costante 0 ha grado $-\infty$. È facile verificare che con le usuali operazioni di somma e prodotto fra polinomi $K[x]$ è un anello, anzi un dominio. Studiamo adesso alcune proprietà legate al grado.

Esercizio 9.1. Sia K un campo, e siano $f(x), g(x) \in K[x]$. Allora

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

Se $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ con $a_n = 1$, diciamo che $f(x)$ è un *polinomio monico*.

Dato K un campo e dati due polinomi $f(x), g(x) \in K[x]$ con $g(x) \neq 0$, esistono unici due polinomi $q(x)$ e $r(x)$ in $K[x]$ tali che

$$f(x) = q(x) \cdot g(x) + r(x) \quad \text{con } \deg(r(x)) \lneqq \deg(g(x)).$$

Chiamiamo $q(x)$ il *quoziente* e $r(x)$ il *resto* della *divisione (Euclidea)* di $f(x)$ per $g(x)$. Se il resto $r(x)$ è uguale a 0, diciamo che $g(x)$ *divide* $f(x)$ (osserviamo che secondo questa definizione $3x^2 + 3$ e $2x^2 + 2$ dividono entrambi $5x^2 + 5$).

L'esistenza di quoziente e resto è dato semplicemente dall'*algoritmo di divisione* di due polinomi che avete imparato a scuola. Ricordiamo come funziona l'algoritmo con un piccolo esempio.

Esempio 9.2. Siano $f(x) = 2x^4 + 5x^3 + 10x^2 + 10x + 3$ e $g(x) = 2x^3 + x^2 + 4x + 2$. Siccome $\deg(f(x)) \geq \deg(g(x))$, per dividere $f(x)$ per $g(x)$ dobbiamo moltiplicare $g(x)$ par un monomio appropriato in modo tale che $f(x)$ meno il prodotto dia un polinomio di grado strettamente più piccolo di $\deg(f(x))$. In altri termini, vogliamo annullare il *monomio direttore* di $f(x)$, ossia il monomio di $f(x)$ che ha grado più alto. Poi iteriamo il processo, fino a quando non otteniamo un polinomio di grado strettamente più piccolo di $\deg(g(x))$.

Possiamo dunque cominciare con

$$f(x) - x \cdot g(x) = 4x^3 + 6x^2 + 8x + 3,$$

e poi

$$f(x) - (x+2)g(x) = f(x) - x \cdot g(x) - 2 \cdot g(x) = 4x^3 + 6x^2 + 8x + 3 - 2 \cdot g(x) = 4x^2 - 1$$

ha un grado strettamente inferiore a $\deg(g(x)) = 3$. Dunque otteniamo che $q(x) = x + 2$ e $r(x) = 4x^2 - 1$ sono i quoziente e il resto della divisione di $f(x)$ per $g(x)$.

Utilizzando questo algoritmo di divisione, possiamo calcolare il *massimo comun divisore* di $f(x)$ e $g(x)$, denotato con $MCD(f(x), g(x))$. Questo è l'unico divisore comune monico di $f(x)$ e $g(x)$ di grado massimale.

Bisogna verificare che questa sia una buona definizione: per prima cosa osserviamo che se si considerano tutti i polinomi monici che dividono sia $f(x)$ sia $g(x)$ possiamo sceglierne uno che ha grado massimale. Lo chiamiamo $MCD(f(x), g(x))$ e mostreremo che è unico (dunque ben definito). Utilizzeremo l'algoritmo di Euclide, che è essenzialmente lo stesso di quello visto per gli interi:

Dati due polinomi $r_{-1}(x) := f(x)$ e $r_0(x) := g(x) \neq 0$ di $K[x]$, siano $q_1(x)$ e $r_1(x)$ gli unici polinomi di $K[x]$ tali che

$$r_{-1}(x) = q_1(x)r_0(x) + r_1(x) \quad \text{con } \deg(r_1(x)) \lneqq \deg(r_0(x)).$$

Se $r_1(x) = 0$, ci fermiamo. Altrimenti, siano $q_2(x)$ e $r_2(x)$ gli unici polinomi di $K[x]$ tali che

$$r_0(x) = q_2(x)r_1(x) + r_2(x) \quad \text{con } \deg(r_2(x)) \lneqq \deg(r_1(x)).$$

Se $r_2(x) = 0$ ci fermiamo. Altrimenti, possiamo iterare, ottenendo due sequenze di polinomi $q_1(x), q_2(x), q_3(x), \dots$ e $r_1(x), r_2(x), r_3(x), \dots$ tali che per ogni $i = 1, 2, 3, \dots$

$$r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x) \quad \text{con } \deg(r_i(x)) \lneqq \deg(r_{i-1}(x)).$$

Siccome per ogni i si ha $\deg(r_i(x)) \lneqq \deg(r_{i-1}(x))$, esiste il più piccolo $k \geq 0$ tale che $r_{k+1}(x) = 0$. Affermiamo che $r_k(x)$ è un polinomio associato a $MCD(f(x), g(x))$ (ossia differisce da $MCD(f(x), g(x))$ solo per moltiplicazione per un elemento di K diverso da 0).

Infatti, da una parte ad ogni passo ogni divisore comune di $r_{i-2}(x)$ e $r_{i-1}(x)$ deve dividere anche $r_i(x)$. Quindi, per induzione, ogni divisore comune di $r_{-1}(x) = f(x)$ e $r_0(x) = g(x)$ deve dividere $r_k(x)$. Allora in particolare $MCD(f(x), g(x))$ divide $r_k(x)$.

Ma dato che $r_{k+1}(x) = 0$, abbiamo $r_{k-1}(x) = q_{k+1}(x)r_k(x)$, e dunque $r_k(x)$ divide $r_{k-1}(x)$. Allora, per la $r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x)$, deve dividere anche $r_{k-2}(x)$. Iterando, usando le $r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x)$, $r_k(x)$ deve dividere tutti i $r_i(x)$, e dunque anche $r_{-1}(x) = f(x)$ e $r_0(x) = g(x)$. Sia ora γ il coefficiente direttore di $r_k(x)$: allora anche $\frac{r_k(x)}{\gamma}$, che ha coefficiente direttore 1, divide $f(x)$ e $g(x)$. Per la definizione di $MCD(f(x), g(x))$ questo significa che $\deg \frac{r_k(x)}{\gamma} \leq \deg MCD(f(x), g(x))$. Deve però valere anche $\deg MCD(f(x), g(x)) \leq \deg \frac{r_k(x)}{\gamma}$ dato che $MCD(f(x), g(x))$ divide $r_k(x)$ e dunque anche $\frac{r_k(x)}{\gamma}$. I due polinomi $MCD(f(x), g(x))$ e $\frac{r_k(x)}{\gamma}$ hanno lo stesso grado, sono entrambi monici, e il primo divide il secondo: questo implica che coincidono. Questo dimostra la nostra affermazione che $r_k(x)$ è un polinomio associato a $MCD(f(x), g(x))$.

Come per gli interi, partendo dall'ultima identità dell'algoritmo e risalendo al contrario, possiamo calcolare esplicitamente due polinomi $y(x)$ e $z(x)$ di $K[x]$ tali che

$$y(x)f(x) + z(x)g(x) = r_k(x)$$

da cui poi, dividendo per il coefficiente direttore γ di $r_k(x)$ si ottiene

$$\lambda(x)f(x) + \mu(x)g(x) = MCD(f(x), g(x))$$

dove $\lambda(x) = \frac{y(x)}{\gamma}$ e $\mu(x) = \frac{z(x)}{\gamma}$. L'esistenza di questi polinomi $\lambda(x)$ e $\mu(x)$ è dunque un utile corollario dell'algoritmo di Euclide, che chiamamo ancora *teorema di Bézout*. La dimostrazione dell'unicità (e dunque della buona definizione) di $MCD(f(x), g(x))$ è a questo punto quasi terminata e la lasciamo come esercizio:

ESERCIZIO 9.3. Dimostrare che tutti i polinomi che dividono $f(x)$ e $g(x)$ e hanno grado massimale sono associati fra loro, e in particolare ne esiste uno solo che ha coefficiente direttore uguale ad 1.

ESEMPIO 9.4. Siano $f(x) = 2x^4+5x^3+10x^2+10x+3$ e $g(x) = 2x^3+x^2+4x+2$. Abbiamo già visto che $q_1(x) := x+2$ e $r_1(x) := 4x^2-1$ sono tali che

$$f(x) = q_1(x)g(x) + r_1(x).$$

Ora per $q_2(x) = (2x+1)/4$ e $r_2(x) = 9(2x+1)/4$ troviamo

$$g(x) - q_2(x)r_1(x) = 2x^3 + x^2 + 4x + 2 - \frac{2x+1}{4}(4x^2-1) = 9(2x+1)/4 = r_2(x).$$

Infine, per $q_3 = (8x-4)/9$ abbiamo

$$r_1(x) = 4x^2 - 1 = \frac{8x-4}{9} \cdot \frac{9(2x+1)}{4} = q_r(x)r_2(x),$$

e dunque $r_3(x) = 0$.

Pertanto $MCD(f(x), g(x)) = 4r_2(x)/18 = (2x+1)/2$.

A partire dalle equazioni

$$\begin{aligned} r_2(x) &= g(x) - q_2(x)r_1(x) = g(x) - q_2(x)(f(x) - q_1(x)g(x)) \\ &= -q_2(x)f(x) + (1 + q_1(x)q_2(x))g(x), \end{aligned}$$

deduciamo che in questo caso abbiamo

$$\lambda(x) = -4q_2(x)/18 = -(2x+1)/18 \quad \text{e} \quad \mu(x) = 4(1 + q_1(x)q_2(x))/18 = (2x^2+5x+6)/18.$$

2. Radici di un polinomio

Sia K un campo. Una *radice* di un polinomio

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

è un $x_0 \in K$ tale che

$$f(x_0) = a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_1 x_0 + a_0 = 0.$$

LEMMA 9.5. *Sia K un campo, sia $f(x) \in K[x]$, e sia $x_0 \in K$ una radice di $f(x)$. Allora*

$$f(x) = (x - x_0)g(x) \text{ con } g(x) \in K[x] \text{ tale che } \deg(g(x)) = \deg(f(x)) - 1.$$

DIMOSTRAZIONE. Facendo la divisione euclidea di $f(x)$ per $x-x_0$ troviamo $q(x), r(x) \in K[x]$ tali che

$$f(x) = q(x)(x - x_0) + r(x) \quad \text{con } \deg(r(x)) < \deg(x - x_0) = 1,$$

dunque $r(x)$ è un polinomio costante. Ora valutando questa equazione in $x = x_0$ otteniamo

$$0 = f(x_0) = q(x_0)(x_0 - x_0) + r(x_0) = r(x)$$

dunque $g(x) = q(x)$ è il polinomio cercato. □

Il *teorema fondamentale dell'algebra*[1] dice che ogni polinomio $f(x) \in \mathbb{C}[x]$ di grado positivo ha una radice z_0 in $\mathbb{C}$. Dunque, per il lemma precedente, $f(x) = (x - z_0)g(x)$

[1]Questo teorema ha tante dimostrazioni, ma nessuna è davvero semplice, quindi rimandiamo la sua dimostrazione a un corso di algebra successivo.

con $g(x) \in \mathbb{C}[x]$ e $\deg(g(x)) = \deg(f(x)) - 1$. Iterando questo ragionamento con $g(x)$, otteniamo che $f(x)$ fattorizza come

$$f(x) = c(x - z_0)(x - z_1)\cdots(x - z_n),$$

dove $n = \deg(f(x))$ e le z_i sono radici di $f(x)$ (notate che le radici non sono necessariamente distinte).

Cosa dice questo teorema sui polinomi a coefficienti reali?

Dato un polinomio a coefficienti complessi

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$$

definiamo

$$\overline{f}(x) := \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0} \in \mathbb{C}[x],$$

dove $\overline{z}$ denote il coniugato del numero complesso $z \in \mathbb{C}$ (ossia se $z = a + bi$ con $a, b \in \mathbb{R}$, allora $\overline{z} = a - bi$).

Supponiamo adesso che $f(x) \in \mathbb{R}[x]$ abbia coefficienti reali e grado positivo. Notate che siccome i coeffienti di $f(x)$ sono tutti reali, ricordando che $\overline{a} = a$ se e solo se $a \in \mathbb{R} \subseteq \mathbb{C}$, abbiamo $\overline{f}(x) = f(x)$.

Ora se $z_0 \in \mathbb{C}$ è una radice complessa di $f(x)$, allora

$$\begin{aligned} 0 = \overline{f(z_0)} &= \overline{= a_n z_0^n + a_{n-1}z_0^{n-1} + \cdots + a_1 z_0 + a_0} \\ &= \overline{a_n z_0}^n + \overline{a_{n-1}z_0}^{n-1} + \cdots + \overline{a_1 z_0} + \overline{a_0} \\ &= \overline{f}(\overline{z_0}) = f(\overline{z_0}), \end{aligned}$$

(dove abbiamo usato le proprietà $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ e $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$ per ogni $z_1, z_2 \in \mathbb{C}$ (**esercizio**)) dunque anche $\overline{z_0}$ è una radice di $f(x)$. Chiaramente se z_0 era un numero reale, questa osservazione non ci dice nulla di nuovo, visto che $z_0 = \overline{z_0}$ in questo caso. Ma se z_0 è una radice di $f(x)$ non reale (ossia $f(z_0) = 0$ e $Im(z_0) \neq 0$)[2], allora affermiamo che il polinomio $(x - z_0)(x - \overline{z_0})$ divide $f(x)$ in $\mathbb{R}[x]$. Infatti, osserviamo innanzitutto che $(x - z_0)(x - \overline{z_0})$ è un polinomio reale, poichè

$$(x - z_0)(x - \overline{z_0}) = x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0} = x^2 - 2Re(z_0)x + |z_0|^2 \in \mathbb{R}[x].$$

Ora facendo la divisione euclidea possiamo trovare due polinomi $q(x), r(x) \in \mathbb{R}[x]$ con $\deg(r(x)) \lneq \deg((x - z_0)(x - \overline{z_0})) = 2$ tali che

$$f(x) = q(x)(x - z_0)(x - \overline{z_0}) + r(x).$$

Adesso se $\deg(r(x)) = 1$, allora $r(x) = ax + b$ con $a, b \in \mathbb{R}$ e $a \neq 0$. Ma la valutazione $x = z_0$ ci dà

$$0 = f(z_0) = q(z_0)(z_0 - z_0)(z_0 - \overline{z_0}) + r(z_0) = r(z_0) = az_0 + b,$$

che è una contraddizione, poichè $Im(az_0 + b) = aIm(z_0) \neq 0$ in quanto $a \neq 0$ e $Im(z_0) \neq 0$. Dunque $\deg(r(x)) \leq 0$, ossia $r(x)$ è costante, ma quindi $r(x) = r(z_0) = 0$, e dunque $(x - z_0)(x - \overline{z_0})$ divide $f(x)$ in $\mathbb{R}[x]$, che è ciò che abbiamo affermato.

Otteniamo quindi il seguente corollario, che è in effetti l'enunciato originale del teorema fondamentale dell'algebra.

COROLLARIO 9.6. *Ogni polinomio $f(x) \in \mathbb{R}[x]$ di grado positivo fattorizza in un prodotto di fattori di grado minore o uguale a 2.*

[2]Ricordiamo che se $z = a + bi$ con $a, b \in \mathbb{R}$, allora $Im(z) = b$ denota la *parte immaginaria* di $z \in \mathbb{C}$, e $Re(z) = a$ denota la *parte reale* di z.

In particolare un polinomio di grado dispari avrà necessariamente una radice reale (in realtà questo fatto si deve dimostrare prima, perchè viene usato sostanzialmente in ogni dimostrazione del teorema fondamentale dell'algebra).

3. Il quoziente $K[x]/(f(x))$

In questa sezione vogliamo capire meglio come funziona il quoziente $K[x]/(f(x))$, dove K è un campo e $f(x) \in K[x]$.

Ci sono due casi banali: se $f(x) = 0$, allora l'ideale $(0) = \{0\}$ è banale, dunque $K[x]/(f(x)) \cong K[x]$ (**esercizio**). Se $f(x) = a \in K$ costante con $a \neq 0$, allora $(a) = K[x]$, e in questo caso il quoziente è banale (ossia l'anello in cui $1 = 0$).

Supponiamo dunque che $\deg(f(x)) = n \geq 1$.

L'idea è che nel quoziente $K[x]/(f(x))$ stiamo imponendo la "relazione $f(x) = 0$". Per capire meglio, vediamo un esempio.

Esempio 9.7. Consideriamo $K = \mathbb{R}$, e $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Allora in $\mathbb{R}[x]/(x^2 + 1)$ "vale la relazione $x^2 + 1 = 0$, ossia $x^2 = -1$" in questo senso: se ad esempio abbiamo un elemento $3x^4 - 5x^3 + x - \sqrt{3} + (f(x))$, allora possiamo sostituire x^2 on -1, ottenendo ad esempio

$$3(x^2)^2 - 5x^3 + x - \sqrt{3} + (f(x)) = 3(-1)^2 - 5x^3 + x - \sqrt{3} + (f(x)).$$

Per verificare questa uguaglianza basta verificare che la differenza dei rappresentanti dei laterali sta nell'ideale, ossia che $f(x) = x^2+1$ divide $3x^4-5x^3+x-\sqrt{3}-(3(-1)^2-5x^3+x-\sqrt{3})$ (**esercizio**). Possiamo quindi continuare ad usare la relazione $x^2 = -1$ ed ottenere ad esempio

$$\begin{aligned} 3x^4 - 5x^3 + x - \sqrt{3} + (f(x)) &= 3(-1)^2 - 5x^3 + x - \sqrt{3} + (f(x)) \\ &= 3(-1)^2 - 5x(-1) + x - \sqrt{3} + (f(x)) \\ &= 5x + 3 - \sqrt{3} + (f(x)). \end{aligned}$$

Rimandiamo alla prossima sezione una più profonda comprensione di $\mathbb{R}[x]/(x^2 + 1)$.

Dall'esempio appena visto è chiaro che facendo questo tipo di sostituzioni, possiamo sempre scegliere un rapprentante di un laterale $g(x) + (f(x)) \in K[x]/(f(x))$ che abbia grado strettamente minore di $f(x)$: infatti basta fare la divisione euclidea, che ci dà

$$g(x) = q(x)f(x) + r(x) \quad \text{con } \deg(r(x)) < \deg(f(x))$$

ed è ora chiaro che

$$g(x) + (f(x)) = q(x)f(x) + r(x) + (f(x)) = r(x) + (f(x)).$$

Dunque ogni elemento del quoziente $K[x]/(f(x))$ è il laterale di un poliomio di grado minore di $\deg(f(x)) = n$. A questo punto vale la pena fare i due seguenti esercizi.

Esercizio 9.8. Sia K un campo, e sia R un anello che contiene K come sottoanello. Allora R è uno spazio vettoriale su K con le operazioni ovvie di somma e prodotto per scalari.

Esercizio 9.9. Sia K un campo, e sia $f(x) \in K[x]$ un polinomio di grado $n \geq 1$. Sia K' il sottoinsieme $\{c + (f(x)) \mid c \in K\}$, ossia K' è l'insieme dei laterali dei polinomi costanti. Allora K' è un sottoanello di $K[x]/(f(x))$ isomorfo a K, e $K[x]/(f(x))$ è uno spazio vettoriale su K' di dimensione n.

Vediamo un altro esempio.

ESEMPIO 9.10. Consideriamo il campo $K = \mathbb{Z}_2$, e sia[3] $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Per l'esercizio precedente, $\mathbb{Z}_2[x]/(x^2 + x + 1)$ è uno spazio vettoriale su $\mathbb{Z}_2$ di dimensione 2, dunque ha quattro elementi: $\overline{0}, \overline{1}, \overline{x}$ e $\overline{x+1}$, dove con $\overline{g(x)}$ denotiamo il laterale $g(x) + (x^2 + x + 1)$ di $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Si verifica facilmente (**esercizio**) che

$$\overline{x}(\overline{x+1}) = \overline{1},$$

dunque $\mathbb{Z}_2[x]/(x^2 + x + 1)$ è un campo... con 4 elementi (!) che chiameremo $\mathbb{F}_4$. Come potete intuire, questa costruzione si potrà generalizzare, e lo faremo nelle prossime lezioni.

Facciamo un'ultima (per ora) importante osservazione. Usiamo la notazione $\overline{g(x)}$ per indicare il laterale $g(x) + (f(x))$ in $K[x]/(f(x))$. Osserviamo dunque che $\overline{x}$ soddisfa l'equazione

$$f(\overline{x}) = \overline{0} \in K[x]/(f(x)).$$

Infatti, se

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x],$$

allora

$$\begin{aligned} f(\overline{x}) &= \overline{a_n}\,\overline{x}^n + \overline{a_{n-1}}\,\overline{x}^{n-1} + \cdots + \overline{a_1}\,\overline{x} + \overline{a_0} \\ \text{(per definizione di quoziente)} &= \overline{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{f(x)} = \overline{0} \in K[x]/(f(x)), \end{aligned}$$

dove notate che $\overline{a_i} = a_i + (f(x))$ denota il laterale del polinomio costante a_i.

Abbiamo quindi costruito un anello (il nostro $K[x]/(f(x))$) che contiene K (o meglio un sottoanello isomorfo a K, ossia l'insieme dei laterali dei polinomi costanti) e in cui $f(x) \in K[x]$ ha una radice...!

4. Morfismi di valutazione

Abbiamo già osservato in precedenza come sia utile valutare i polinomi, ossia porre $x = a$ dove a è un coefficiente. Vale la pena fare un'esercizio generale.

ESERCIZIO 9.11. Sia A un anello commutativo, e sia R un anello che contiene A come sottoanello. Allora per ogni $r \in R$ definiamo la mappa

$$\varphi_r : A[x] \to R, \quad \varphi_r(f(x)) \coloneqq f(r) \text{ per ogni } f(x) \in A[x].$$

Mostrare che φ_r è un omomorfismo di anelli, detto *omomorfismo di valutazione* in r.

Questi omomorfismi di valutazione possono aiutarci a capire meglio i quozienti di $K[x]$. Vediamo un esempio fondamentale.

ESEMPIO 9.12. Consideriamo $K = \mathbb{R}$, $i \in \mathbb{C}$, e sia $\varphi_i : \mathbb{R}[x] \to \mathbb{C}$ l'omomorfismo di valutazione in i. È chiaro che questo omomorfismo è suriettivo: ogni numero complesso $a + bi$ è chiaramente l'immagine di un polinomio in $\mathbb{R}[x]$, ad esempio $\varphi_i(bx + a) = a + bi$. Dunque l'immagine di φ_i è tutto $\mathbb{C}$.

Chi è $Ker(\varphi_i)$? Sicuramente $x^2 + 1$ viene mandato in zero, ossia $\varphi_i(x^2 + 1) = i^2 + 1 = -1 + 1 = 0$, dunque $x^2 + 1 \in Ker(\varphi_i)$. Pertanto $Ker(\varphi_i)$ contiene anche ogni suo multiplo, ossia $Ker(\varphi_i) \supseteq (x^2 + 1)$.

ESERCIZIO 9.13. Mostrare che $Ker(\varphi_i) = (x^2 + 1)$.

[3]Qui, e nel seguito in casi simili, per alleggerire la notazione non usiamo la notazione con le parentesi quadre $[a]_2$ per gli elementi di $\mathbb{Z}_2$.

Fatto l'esercizio, grazie al Teorema 8.29, otteniamo il seguente isomorfismo di anelli:

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

5. Esercizi

Esercizio 9.14. Trovare il MCD di $f(x) = x^2 - x + 4$ e $g(x) = x^3 + 2x^2 + 3x + 2$ in $\mathbb{Z}_3[x]$ ed esprimere in entrambi i casi il MCD come combinazione di Bézout di $f(x)$ e $g(x)$.

Esercizio 9.15. Trovare il MCD di $f(x) = x^6 - 1$ e $g(x) = x^4 + x^3 + x^2 - 4x + 1$ in $\mathbb{Z}_5[x]$ e in $\mathbb{Q}[x]$ ed esprimere in entrambi i casi il MCD come combinazione di Bézout di $f(x)$ e $g(x)$.

Esercizio 9.16. Trovare il MCD di $f(x) = x^9 - 1$ e $g(x) = x^{11} - 1$ in $\mathbb{Z}_2[x]$ e in $\mathbb{Q}[x]$ ed esprimere in entrambi i casi il MCD come combinazione di Bézout di $f(x)$ e $g(x)$.

Esercizio 9.17. Sia $f(x) = x^2 - 3x + 2$ e chiamiamo I l'ideale $(x^2 - 3x + 2) \in \mathbb{Q}[x]$. Trovare (se esiste) l'inverso di $x^2 + x + 1 + I$ in $\mathbb{Q}[x]/I$.

Esercizio 9.18. Sia $f(x) = x^3 + x + 1$ e chiamiamo I l'ideale $(x^3 + x + 1) \in \mathbb{Z}_2[x]$. Trovare (se esiste) l'inverso di $x^2 + x + 1 + I$ in $\mathbb{Z}_2[x]/I$.

Esercizio 9.19. Sia $f(x) = x^4 - 2x^3 + 2x^2 + x + 1$ e chiamiamo I l'ideale $(x^4 - 2x^3 + 2x^2 + x + 1) \in \mathbb{Z}_3[x]$. Trovare (se esiste) l'inverso di $x^2 + x + 1 + I$ in $\mathbb{Z}_3[x]/I$.

CAPITOLO 10

Anelli quoziente. Anelli euclidei

1. Gli anelli $K[x]$ sono ad ideali principali

Sia K un campo. Una proprietà importante che riguarda gli ideali dell'anello $K[x]$ è la seguente:

TEOREMA 10.1. *Sia K un campo e sia I un ideale di $K[x]$. Allora esiste in I un polinomio $f(x)$ tale che*

$$I = (f(x))$$

DIMOSTRAZIONE. Se I è l'ideale banale $\{0\}$ allora vale $I = (0)$.
Sia ora $I \neq \{0\}$ e consideriamo l'insieme dato dai gradi dei polinomi non nulli di I:

$$\{deg\ g(x) \,|\, g(x) \in I, g(x) \neq 0\}$$

Questo è un sottoinsieme non vuoto di $\mathbb{N}$, e per il principio del minimo ammette un minimo $m \in \mathbb{N}$. Possiamo allora scegliere in I un polinomio $f(x)$ tale che $deg\ f(x) = m$. Dimostreremo che $I = (f(x))$. Basterà mostrare che ogni polinomio $h(x) \in I$ è diviso da $f(x)$. Sia dunque $h(x) \in I$ e consideriamo la divisione euclidea di $h(x)$ per $f(x)$:

$$h(x) = f(x)q(x) + r(x)$$

dove o $r(x) = 0$ oppure $r(x) \neq 0$ e $deg\ r(x) < deg\ f(x)$. Quest'ultimo caso non può accadere. Per prima cosa osserviamo che dalla relazione

$$r(x) = h(x) - f(x)q(x)$$

si ricava che $r(x) \in I$. Infatti $h(x) \in I$ e $f(x)q(x) \in I$ per la proprietà di assorbimento degli ideali, visto che $f(x) \in I$. Allora se avessimo $r(x) \neq 0$ e $deg\ r(x) < deg\ f(x)$ risulterebbe che $r(x)$ è un elemento di I di grado minore del grado minimo m, assurdo.

□

In accordo con le definizioni seguenti, abbiamo dunque dimostrato che, se K è un campo, l'anello $K[x]$ è un *dominio ad ideali principali*:

DEFINIZIONE 10.2. Un ideale I di un anello commutativo A si dice *principale* se è generato da un solo elemento, ossia se esiste $a \in A$ tale che $I = (a)$.[1]

DEFINIZIONE 10.3. Un dominio di integrità si dice a *dominio a ideali principali* (PID) se tutti i suoi ideali sono principali.

OSSERVAZIONE 10.4. Consideriamo $K[x, y]$, anello dei polinomi a coefficienti in un campo K e nelle variabili x e y. Questo anello non è a ideali principali: si può mostrare (esercizio!) che l'ideale $I = (x, y)$ generato dalle variabili x e y non può essere generato da un solo elemento.

[1]Questa è la definizione per anelli commutativi, quella che servirà in questo corso. Nel caso in cui l'anello non sia commutativo, si distinguono gli ideali principali sinistri, destri e bilateri.

Osservazione 10.5. Consideriamo $\mathbb{Z}[x]$, anello dei polinomi a coefficienti in $\mathbb{Z}$ nella variabile x. Anche questo anello non è a ideali principali: si può mostrare (esercizio!) che l'ideale $I = (2, x)$ non può essere generato da un solo elemento.

Osservazione 10.6. Come abbiamo visto nel capitolo precedente, dati due polinomi $f(x), g(x) \in K[x]$ non entrambi nulli esiste un massimo comun divisore monico $MCD(f(x), g(x))$. Come sappiamo, l'ideale $(f(x), g(x))$ in $K[x]$ è principale; è facile dimostrare che coincide con l'ideale generato da $MCD(f(x), g(x))$ e che ogni altro generatore dell'ideale è associato a $MCD(f(x), g(x))$.

2. Polinomi irriducibili in $K[x]$ e quozienti

Definizione 10.7. Sia K un campo, e sia $f(x) \in K[x]$ un polinomio di grado ≥ 1. Diremo che $f(x)$ è *irriducibile* se gli unici divisori di $f(x)$ sono i polinomi costanti diversi da 0 o i polinomi associati a $f(x)$.

Un modo equivalente per dare la definizione di irriducibilità è il seguente: un polinomio $f(x) \in K[x]$ di grado ≥ 1 è irriducibile se e solo se quando abbiamo in $K[x]$ una relazione del tipo

$$f(x) = a(x)b(x)$$

questo implica che uno fra i polinomi $a(x)$, $b(x)$ è un polinomio costante diverso da 0. Sarà per noi molto importante avere dei criteri per riconoscere i polinomi irriducibili. Uno dei motivi è dato dal seguente

Teorema 10.8. *Sia K un campo, e sia $f(x) \in K[x]$. Allora il quoziente $K[x]/(f(x))$ è un campo se e solo se $f(x)$ è un polinomio irriducibile.*

Dimostrazione. Sia $f(x) \in K[x]$ irriducibile e poniamo $I = (f(x))$. Per mostrare che $K[x]/(f(x))$ è un campo basta mostrare che se $a(x)+I$ è un elemento di $K[x]/(f(x))$ diverso da $0 + I$ allora ammette un inverso.

Per prima cosa notiamo che $MCD(a(x), f(x)) = 1$. Infatti, dato che $f(x)$ è irriducibile, gli unici divisori di $f(x)$ in $K[x]$ sono, a meno di associati, 1 e $f(x)$. Di questi solo 1 divide anche $a(x)$ perché se $f(x)$ dividesse $a(x)$ allora $a(x)$ apparterrebbe a I e dunque avremmo $a(x) + I = 0 + I$, contraddicendo la scelta di $a(x) + I$.

Per il teorema di Bezout esistono allora $\lambda(x)$ e $\mu(x)$ in $K[x]$ tali che

$$a(x)\lambda(x) + f(x)\mu(x) = 1$$

A questo punto possiamo verificare che $\lambda(x) + I$ è l'inverso di $a(x) + I$ in $K[x]/(f(x))$. Infatti

$$(a(x) + I)(\lambda(x) + I) = a(x)\lambda(x) + I = 1 + I$$

dove la prima uguaglianza deriva dalla definizione del prodotto in $K[x]/(f(x))$ e la seconda dalla osservazione che

$$a(x)\lambda(x) - 1 = f(x)\mu(x) \in I$$

Abbiamo dunque dimostrato che se $f(x) \in K[x]$ è irriducibile allora $K[x]/(f(x))$ è un campo.

Viceversa, se $f(x)$ non è irriducibile, siamo in uno dei seguenti tre casi:

- $f(x) = 0$. Allora si osserva $K[x]/(0) \cong K[x]$ e dunque non è un campo.
- $f(x)$ ha grado 0, ossia $f(x) = k \in K^*$. In tal caso si osserva che $(k) = (1) = K[x]$, e dunque $K[x]/(k) \cong \{0\}$ che non è un campo.

- $f(x)$ si fattorizza come $f(x) = g_1(x)g_2(x)$ con $1 \leq deg\ g_1(x) < degf(x)$ e $1 \leq deg\ g_2(x) < degf(x)$. Allora, ponendo $I = (f(x))$, si verifica subito che le classi $g_1(x) + I$ e $g_2(x) + I$ sono entrambe diverse da $0 + I$ e

$$(g_1(x) + I)(g_2(x) + I) = f(x) + I = 0 + I$$

Visto che in $K[x]/(f(x))$ ci sono dei divisori di 0, non è un dominio e a maggior ragione neppure un campo.

□

Concludiamo questo paragrafo sui quozienti di $K[x]$ segnalando che si potrebbe utilizzare in questo contesto la notazione usata per le congruenze. Prendiamo $m(x) \in K[x]$ e chiamiamo $J = (m(x))$. Si stabilisce che la scrittura

$$a(x) \equiv b(x) \bmod m(x)$$

equivale alla uguaglianza in $K[x]/J$

$$a(x) + J = b(x) + J$$

La nostra conoscenza dei quozienti di $K[x]$ ci permette di concludere che le regole di addizione, moltiplicazione, divisione per le congruenze in $K[x]$ sono del tutto analoghe a quelle viste per le congruenze in $\mathbb{Z}$, e così pure il teorema cinese del resto.

3. Anelli euclidei

Come abbiamo visto, nell'anello $K[x]$ dei polinomi a coefficienti in un campo K si può fare la divisione col resto, che ha molte analogie con la divisione euclidea in $\mathbb{Z}$.

La seguente definizione di anello euclideo raccoglie tutti gli anelli in cui esiste una divisione con le caratteristiche delle due divisioni ricordate qui sopra. Scopriremo alcune proprietà comuni a tutti questi anelli, e descriveremo un anello euclideo il cui studio ci darà interessanti applicazioni aritmetiche.

Definizione 10.9. Un dominio di integrità D si dice *anello euclideo* se esiste una funzione *grado*

$$g : D \setminus \{0\} \to \mathbb{N}$$

tale che

(1) per ogni $a, b \in D$, entrambi non zero, vale $g(a) \leq g(ab)$;
(2) per ogni $a, b \in D$ con $b \neq 0$, esistono $q, r \in D$ tali che $a = qb + r$, dove $r = 0$ o $g(r) < g(b)$.

Osservazione 10.10. Osserviamo che la funzione grado non è definita su 0. L'anello $\mathbb{Z}$ è un esempio di anello euclideo (possiamo prendere come g la funzione valore assoluto, e ignorare il fatto che tale funzione è definita anche su 0). L'anello dei $K[x]$ dei polinomi a coefficienti in un campo K è euclideo (in questo caso possiamo prendere come g la funzione *deg* che associa ad un polinomio il suo grado, e non è definito il grado del polinomio 0).

Lemma 10.11. *In un anello euclideo D siano $a, b \neq 0$. Se $b \mid a$ e $a \nmid b$ allora $g(b) < g(a)$.*[2]

[2]Il concetto di divisibilità negli anelli commutativi è quello ovvio: a divide c se e solo se esiste b tale che $ab = c$.

DIMOSTRAZIONE. Sia $a = bc$. Se a non divide b possiamo scrivere che $b = aq + r$ con $r \neq 0$ e $g(r) < g(a)$. Ma d'altra parte $r = b - aq = b - bcq = b(1 - cq)$ e dunque $g(r) \geq g(b)$. Si conclude che $g(a) > g(b)$.

□

LEMMA 10.12. *In un anello euclideo D vale che $g(1) \leq g(b)$ per ogni $b \in D$ e $g(b) = g(1)$ se e solo $b \in D^*$.*

DIMOSTRAZIONE. Per la prima affermazione è sufficiente osservare che, per ogni $b \in D$, vale $g(b1) \geq g(1)$, e questo mostra che $g(1)$ è il minimo dei gradi degli elementi dell'anello. Per la seconda parte utilizzeremo il fatto che b è invertibile se e solo se $(b) = D$.
($\Longrightarrow$) Supponiamo che $g(b) = g(1)$. Sia $a \in D$, allora $a = qb + r$ con $r = 0$ o $g(r) < g(b)$, ma b ha il grado minimo fra tutti i gradi degli elementi dell'anello e quindi $r = 0$. Quindi $a \in (b)$ per ogni $a \in D$ e dunque $D = (b)$.
($\Longleftarrow$) Supponiamo che $b \in D^*$. Allora $(b) = D$ e quindi per ogni $a \in D$ esisterà $r \in D$ tale che $a = rb$. Si deduce che, per ogni $a \in D$, $g(a) \geq g(b)$ e quindi $g(b)$ è il minimo fra tutti i gradi degli elementi dell'anello: allora $g(b) = g(1)$.

□

Introduciamo un importante esempio di anello euclideo, di cui parleremo in maniera più approfondita nella prossima lezione.

DEFINIZIONE 10.13. L'insieme $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, viene chiamato *anello degli interi di Gauss.*[3]

ESERCIZIO 10.14. Mostrare che $\mathbb{Z}[i]$ è un anello.

PROPOSIZIONE 10.15. *L'anello $\mathbb{Z}[i]$ è euclideo.*

DIMOSTRAZIONE. L'anello $\mathbb{Z}[i]$ è un dominio di integrità visto che è un sottoanello del campo $\mathbb{C}$. Scegliamo come grado g il quadrato del modulo:

$$\begin{array}{rccc} g: & \mathbb{Z}[i]\setminus\{0\} & \longrightarrow & \mathbb{N} \\ & a + bi & \longmapsto & |a + bi|^2 = a^2 + b^2. \end{array}$$

Come avrete subito osservato la funzione g si estende in maniera naturale anche a tutto $\mathbb{Z}[i]$ ma questo per definire il grado di un anello euclideo non ha importanza.

Se $z, w \in \mathbb{Z}[i]\setminus\{0\}$ allora $g(zw) \geq g(z)$: infatti $|zw|^2 \geq |z|^2$ poiché $|w| \geq 1$ ($w = a + bi$ con a e b interi). Adesso siano $z, w \in \mathbb{Z}[i]$ con $w \neq 0$. Dimostriamo che esiste la divisione euclidea di z per w. Consideriamo tutti i multipli di w in $\mathbb{Z}[i]$: questi individuano nel piano complesso un reticolo dato dai vertici di quadrati di lato $|w|$ e ogni punto del piano è in uno di questi quadrati (o in più di uno, se si trova al bordo). In particolare z starà in uno di questi quadrati. Sia $Q = w_0 w$ un vertice del quadrato che ha distanza minima da z. Stimiamo questa distanza: nel peggiore dei casi z è nel centro del quadrato, dunque,

$$|z - w_0 w| \leq \frac{|w|}{\sqrt{2}}.$$

Da questo segue che $g(z - w_0 w) \leq \frac{g(w)}{2} < g(w)$ e quindi possiamo prendere w_0 come quoziente della divisione e $z - w_0 w$ come resto. In altre parole

$$z = w w_0 + (z - w_0 w)$$

è la divisione euclidea che cercavamo.

□

[3]Carl Friedrich Gauss, matematico tedesco, 1777-1855.

Esercizio 10.16. Dimostrare che gli elementi invertibili di $\mathbb{Z}[i]$ sono quattro: 1,-1, i, $-i$. [Si può fare velocemente in maniera diretta, ma ricordiamo che si può usare il Lemma 10.12.]

4. Esercizi sui gruppi (lezione del 17 novembre)

Esercizio 10.17. Siano G_1 e G_2 due gruppi, e siano $X_1 \subseteq G_1$ e $X_2 \subseteq G_2$ tali che $(X_1) = G_1$ e $(X_2) = G_2$.

(i) Mostrare che

$$X_{1,2} := \{(x_1, e_{G_2}) \mid x_1 \in X_1\} \cup \{(e_{G_1}, x_2) \mid x_2 \in X_2\} \subseteq G_1 \times G_2$$

è tale che $(X_{1,2}) = G_1 \times G_2$.

(ii) Generalizzare il punto precedente al prodotto diretto di $k \geq 3$ gruppi.

Esercizio 10.18. (i) Mostrare che ogni sottogruppo normale di un gruppo G è il kernel di un qualche omomorfismo da G a un gruppo.

(ii) È vero che un omomorfismo di gruppi $\varphi : G_1 \to G_2$ è determinato dal suo nucleo $Ker(\varphi)$?

Esercizio 10.19. (i) Determinare tutti gli omomorfismi $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$, i loro nuclei e le loro immagini.

(ii) Determinare tutti gli omomorfismi $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to S_3$, i loro nuclei e le loro immagini.

Esercizio 10.20. (i) Per ogni $n \geq 2$, determinare tutti gli omomorfismi $\varphi : S_3 \to \mathbb{Z}_n$, i loro nuclei e le loro immagini.

(ii) Determinare tutti gli omomorfismi $\varphi : S_3 \to \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, i loro nuclei e le loro immagini.

5. Esercizi

Esercizio 10.21. I due anelli $\mathbb{Z}[\imath]/(3)$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$ sono isomorfi?

Esercizio 10.22. È vero o falso che l'anello $\mathbb{Z}[i]/(1+i)$ è isomorfo a $\mathbb{Z}_2$?

Esercizio 10.23. Determinare gli elementi che sono divisori di zero e gli elementi invertibili in $\mathbb{Q}[x]/(x^2-1)$.

Esercizio 10.24. Enunciare il teorema cinese del resto per sistemi di congruenze in $K[x]$ e verificare che la dimostrazione è del tutto analoga a quella per $\mathbb{Z}$.

Esercizio 10.25. Dimostrare che un anello commutativo che ha come soli ideali $\{0\}$ e se stesso è un campo.

Esercizio 10.26. Sia R un dominio e sia $a \in R$. Dimostrare che $R[x]/(x-a) \cong R$.

Esercizio 10.27. Si consideri in $\mathbb{Z}[x]$ l'ideale I generato da $x-2$ e da 3. Dimostrare che $\mathbb{Z}[x]/I \cong \mathbb{Z}_3$.

Esercizio 10.28. Si può definire sull'anello $K[[x]]$ (le *serie* formali nella variabile x sul campo K) una funzione grado che lo rende un anello euclideo?

Esercizio 10.29 (L'anello degli interi di Eisenstein[4]). Sia $\omega \in \mathbb{C}$ una radice cubica di 1 diversa da 1. È possibile dare una struttura euclidea all'*anello degli interi di Eisenstein* $\mathbb{Z}[\omega]$?

[4]Gotthold Max Eisenstein, matematico tedesco, 1823-1852

CAPITOLO 11

Fattorizzazione negli anelli euclidei

1. Elementi irriducibili e il teorema di fattorizzazione unica

Diamo innazitutto la definizione di elemento irriducibile per un dominio, generalizzando le definizioni per noi già note nei casi particolari di $\mathbb{Z}$ e $K[x]$ (K campo).

DEFINIZIONE 11.1. Un elemento $\pi \neq 0$, $\pi \notin D^*$, di un dominio di integrità D si dice *irriducibile* se, per ogni $\gamma, \delta \in D$, $\pi = \gamma\delta$ implica $\gamma \in D^*$ o $\delta \in D^*$.

Mostreremo che se D è un anello euclideo e $p \in D$ è irriducibile allora p possiede anche la seguente proprietà (che viene chiamata *primalità*): *se $p|ab$ allora o $p|a$ oppure $p|b$.*

Il nostro percorso passerà attraverso una rapida rivisitazione delle proprietà degli anelli euclidei.

TEOREMA 11.2. *Sia D un anello euclideo. Allora D è un dominio a ideali principali.*

DIMOSTRAZIONE. La dimostrazione è identica a quella del Teorema 10.1, utilizzando la funzione grado dell'anello. □

DEFINIZIONE 11.3. Sia D un anello euclideo e siano $a, b \in D$ due elementi non entrambi nulli. Sia d un generatore dell'ideale (a, b). Diremo allora che d è un massimo comun divisore di a e b.

Come avrete notato, questa definizione di massimo comune divisore estende quelle per noi già note in $\mathbb{Z}$ e in $K[x]$ (vedi per esempio l'Osservazione 10.6). In particolare è facile dimostrare che

- $d|a$ e $d|b$
- per ogni elemento c di D che divide sia a sia b vale che $c|d$.

In generale il massimo comune divisore in un anello euclideo D non è unico, né ci sono criteri speciali per sceglierne uno (come abbiamo fatto in $\mathbb{Z}$ e in $K[x]$), ma segue immediatamente dalla definizione appena data che se d_1 e d_2 sono massimi comuni divisori di a e b allora d_1 e d_2 sono associati (**esercizio**).

Se entrambi a e b sono diversi da zero, dato che siamo in un anello euclideo, per trovare operativamente un massimo comune divisore si può eseguire l'algoritmo di Euclide: l'ultimo resto non zero che otterremo, chiamiamolo d, sarà un massimo comune divisore di a e b (**esercizio**). Inoltre, ripercorrendo l'algoritmo a ritroso potremo esprimere d come

$$d = \lambda a + \mu b$$

dove $\lambda, \mu \in D$.

Ci sembra importante sottolineare che dalle considerazioni precedenti sul MCD (sia dalle riflessioni sulla definizione, sia dal metodo operativo) segue la validità del teorema di Bézout; lo evidenziamo enunciandolo:

TEOREMA 11.4 (Teorema di Bézout per anelli euclidei). *Sia D un anello euclideo. Dati $a, b \in D$ non entrambi nulli, sia $MCD(a, b)$ un massimo comun divisore di a, b.*

Allora esistono $\lambda, \mu \in D$ *tali che*

$$MCD(a,b) = \lambda a + \mu b$$

Utilizzando il teorema di Bézout, e ripetendo parola per parola una dimostrazione già svolta per $\mathbb{Z}$ possiamo dimostrare, come annunciato, il seguente:

TEOREMA 11.5. *Sia* D *un anello euclideo, e sia* $p \in D$ *un elemento irriducibile. Dati* $a, b \in D$*, se vale che* $p|ab$ *e* $p \nmid a$*, allora* p *divide* b*.*

In un anello euclideo D ogni elemento a diverso da 0 e non invertibile ammette una fattorizzazione in irriducibili. La dimostrazione è per induzione. Si usa la funzione grado in maniera del tutto analoga a quanto visto per $\mathbb{Z}$ (ricordiamo che per esercizio in $\mathbb{Z}$ avevamo proposto varie versioni, utilizzando varie forme del principio di induzione, incluso il principio del minimo).

Il Teorema 11.5 è un ingrediente fondamentale per dimostrare che la fattorizzazione in irriducibili è unica, a meno di associati. La dimostrazione che illustriamo qui di seguito avremmo potuto svolgerla pressoché identica per $\mathbb{Z}$ già nel primo capitolo, subito dopo aver dimostrato il teorema di Bézout. Abbiamo preferito rimandarla a questo punto del corso per farla una volta sola per anelli euclidei (nel frattempo, come si era detto in classe, abbiamo dato per buono che in $\mathbb{Z}$ la fattorizzazione in primi è unica).

TEOREMA 11.6 (Unicità della fattorizzazione in prodotto di irriducibili in un anello euclideo). *Sia* D *un anello euclideo e sia* a *un elemento di* D *diverso da 0 e non invertibile. Siano*

$$a = p_1 p_2 p_3 \cdots p_r$$

$$a = q_1 q_2 \cdots q_s$$

due fattorizzazioni, dove gli elementi p_i $(i = 1, 2, \ldots, r)$ *e* q_j $(j = 1, 2, \ldots, s)$ *sono irriducibili. Allora vale che* $r = s$ *ed esiste una permutazione* $\sigma \in S_r$ *tale che, per ogni* $i = 1, 2, \ldots, r$*,* p_i *e* $q_{\sigma(i)}$ *sono associati.*

DIMOSTRAZIONE. Sia $r \leq s$ e dimostriamo il teorema per induzione su r. Il passo base $r = 1$ è semplice: s deve essere uguale ad 1 altrimenti a sarebbe contemporaneamente irriducibile $(a = p_1)$ e non irriducibile $(a = q_1 \cdots q_s)$. A quel punto è immediato concludere che $a = p_1 = q_1$.

Per il passo induttivo, supponiamo $r > 1$ e che l'enunciato del teorema sia vero quando la prima fattorizzazione ha $r - 1$ fattori irriducibili. Supponiamo di avere

$$a = p_1 p_2 p_3 \cdots p_r$$

$$a = q_1 q_2 \cdots q_s$$

con $1 < r \leq s$.

Cominciamo considerando l'irriducibile p_1. Visto che p_1 divide $q_1 q_2 \cdots q_s = q_1(q_2 \cdots q_s)$, per il Teorema 11.5 o $p_1|q_1$ oppure $p_1|(q_2 \cdots q_s)$. Se vale $p_1|q_1$ allora, visto che p_1 e q_1 sono entrambi irriducibili, deve valere che a meno di associati $p_1 = q_1$. Diciamo che $q_1 = kp_1$ con $k \in D^*$. Allora possiamo dividere a per p_1 ottenendo

$$a = p_2 p_3 \cdots p_r$$

$$a = k q_2 \cdots q_s$$

dove nella prima equazione abbiamo il prodotto di $r - 1$ fattori irriducibili e nella seconda il prodotto di $s - 1$ fattori irriducibili (notate che k non ci interessa, visto che è invertibile e che dobbiamo dimostrare che le due fattorizzazioni coincidono "a meno di associati"; per esempio kq_2 è un irriducibile associato a q_2).

Per ipotesi induttiva sappiamo che $r-1 = s-1$ e che queste due fattorizzazioni coincidono (a meno di associati) e abbiamo concluso.

Se invece non valesse $p_1|q_1$ allora avremmo $p_1|(q_2 \cdots q_s)$. Da qui, iterando il ragionamento, in un numero finito di passi troviamo un i tale che p_1 è associato a q_i. Si conclude analogamente a prima dividendo per p_1 e usando l'ipotesi induttiva. □

Esercizio 11.7. Alla luce del teorema di esistenza e unicità della fattorizzazione in primi prendiamo in considerazione il seguente metodo per la ricerca del massimo comune divisore fra due elementi a e b in un anello euclideo D che si basa sulla scomposizione di a e b in irriducibili: si scelgono (a meno di associati) gli irriducibili che compaiono in entrambe le fattorizzazioni. Se un irriducibile compare s volte (a meno di associati) nella fattorizzazione di a e t volte nella fattorizzazione di b lo si considera $min(s,t)$ volte. Si fa il prodotto di tutti gli irriducibili scelti. Come mai questo metodo dà effettivamente un $MCD(a,b)$?

Esercizio 11.8. Si consideri il sottoanello A di $\mathbb{R}[x]$ definito così:

$$A = \{f(x) \in \mathbb{R}[x] \mid f(0) \in \mathbb{Q}\}$$

Dimostrare che in questo anello i polinomi x e $\sqrt{2}x$ sono entrambi irriducibili e non sono associati, e dunque le scritture

$$2x^2 = (2x)x$$

$$2x^2 = (\sqrt{2}x)(\sqrt{2}x)$$

rappresentano due distinte fattorizzazioni in irriducibili. [Nota 1: questo mostra che in A la fattorizzazione non è unica, e in particolare permette di concludere che non è euclideo. Nota 2: alla fine dell'esercizio avrete dunque mostrato che x è irriducibile e divide il prodotto $(\sqrt{2}x)(\sqrt{2}x)$, ma non divide nessuno dei due fattori.]

Esercizio 11.9. Ripensate alla classica dimostrazione del fatto che $\sqrt{2}$ non è un numero razionale, evidenziando quale ruolo gioca il fatto che in $\mathbb{Z}$ la fattorizzazione è unica.

2. La fattorizzazione in $\mathbb{Z}[i]$ e le somme di quadrati in $\mathbb{Z}$

In questo paragrafo studieremo l'anello $\mathbb{Z}[i]$ degli interi di Gauss; in particolare individueremo quali sono gli elementi irriducibili e scopriremo che questo è collegato ad una interessante osservazione aritmetica.

Lemma 11.10. *Sia $p \in \mathbb{Z}$ un numero primo dispari che non è un elemento irriducibile in $\mathbb{Z}[i]$; allora p si può scrivere come somma di due quadrati di numeri interi.*

Dimostrazione. Supponiamo che p non sia un elemento irriducibile in $\mathbb{Z}[i]$, allora $p = (a+bi)(c+di)$ con $a+bi$ e $c+di$ appartenenti a $\mathbb{Z}[i]$ non invertibili, e dunque tali che $a^2+b^2 > 1$ e $c^2+d^2 > 1$ (vedi Lemma 10.12).

Osserviamo che, essendo $\overline{p} = p$, si ha anche $p = (a-bi)(c-di)$. Allora moltiplicando membro a membro le due relazioni abbiamo $p^2 = (a^2+b^2)(c^2+d^2)$; visto che $a^2+b^2 > 1$ e $c^2+d^2 > 1$ deve valere $a^2+b^2 = p$ e $c^2+d^2 = p$. □

Lemma 11.11. *Sia $p \in \mathbb{Z}$ un primo della forma $4n+1$. Allora la congruenza $x^2 \equiv -1 \pmod{p}$ ammette soluzione in $\mathbb{Z}$.*

DIMOSTRAZIONE. Per coloro che non hanno già risolto l'Esercizio 3.29: sia $x = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$. Essendo $p - 1 = 4n$, nel prodotto precedente compare un numero pari di termini, per cui $x = (-1)(-2)(-3)\cdots\left(-\frac{p-1}{2}\right)$. A questo punto osserviamo che

$$\begin{aligned} x^2 &= 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot (-1) \cdot (-2) \cdot (-3) \cdots \left(-\frac{p-1}{2}\right) \equiv \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \equiv (p-1)! \equiv -1 \pmod{p}, \end{aligned}$$

dove l'ultimo passaggio segue dal teorema di Wilson (Esercizio 3.27). □

Siamo pronti per enunciare un famoso teorema che riguarda i primi $p \equiv 1 \pmod 4$.

TEOREMA 11.12. *Sia $p \in \mathbb{Z}$ un numero primo della forma $4n + 1$. Allora p non è irriducibile in $\mathbb{Z}[i]$ ed esistono $a, b \in \mathbb{Z}$ tali che $p = a^2 + b^2$.*

DIMOSTRAZIONE. Basta dimostrare che p non è irriducibile in $\mathbb{Z}[i]$, il resto dell'enunciato segue poi dal Lemma 11.10. Scegliamo $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \pmod p$ (tale x esiste per il Lemma 11.11). Dunque $p \mid x^2 + 1 = (x - i)(x + i)$, e se p fosse irriducibile in $\mathbb{Z}[i]$ allora per il Teorema 11.5 dovrebbe valere $p \mid (x + i)$ per esempio. Questo vorrebbe dire che esistono $c, d \in \mathbb{Z}$ tali che $p(c + di) = x + i$. Uguagliando le parti immaginarie, dovrebbe valere $pd = 1$, che è assurdo. □

OSSERVAZIONE 11.13. Possiamo per esempio scrivere: $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$ e così via...

Il fatto che un numero primo del tipo $4n + 1$ si possa scrivere come somma di due quadrati di numeri interi fu enunciato da Fermat, senza dimostrazione, in una lettera a Mersenne datata 25 Dicembre 1640: perciò viene talvolta chiamato 'Fermat's Christmas Theorem'. La prima dimostrazione fu poi scritta da Eulero, mentre quella che usa gli interi di Gauss è dovuta a Dedekind.[1]

Completiamo il quadro mostrando che il risultato non è vero per i numeri primi congrui a 3 modulo 4.

TEOREMA 11.14. *Sia p un primo dispari della forma $4n + 3$. Allora p non può essere scritto come somma di due quadrati.*

DIMOSTRAZIONE. Supponiamo che $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$. Dato che p è dispari deve essere che a e b sono uno pari e l'altro dispari; senza perdita di generalità supponiamo a pari e b dispari. Allora $a^2 \equiv 0 \pmod 4$ e $b^2 \equiv 1 \pmod 4$ (verificate!) e

$$p = a^2 + b^2 \equiv 1 + 0 \equiv 1 \pmod{4},$$

Ma questo è assurdo perché $p \equiv 3 \pmod 4$. □

COROLLARIO 11.15. *I primi della forma $4n + 3$ sono irriducibili in $\mathbb{Z}[i]$.*

DIMOSTRAZIONE. Sappiamo dal Lemma 11.10 che se un primo dispari non è irriducibile in $\mathbb{Z}[i]$ allora può essere scritto come somma di due quadrati. Non potendo i primi della forma $4n + 3$ essere scritti in tal modo, ne segue che devono essere irriducibili in $\mathbb{Z}[i]$. □

TEOREMA 11.16. *Tutti e soli gli irriducibili di $\mathbb{Z}[i]$ sono (a meno di associati) i primi di $\mathbb{Z}$ della forma $4n + 3$ e gli $z \in \mathbb{Z}[i]$ tali che $g(z) = |z|^2$ è un primo di $\mathbb{Z}$.*

[1] Richard Dedekind, matematico tedesco, 1831-1916.

DIMOSTRAZIONE. ($\Longleftarrow$) Se p è un primo della forma $4n+3$ il corollario precedente ci dice che è irriducibile in $\mathbb{Z}[i]$. Se $g(z) = p$, con p primo, allora z è irriducibile perché se scriviamo $z = w_1 w_2$ e consideriamo i quadrati delle norme abbiamo $p = |w_1|^2|w_2|^2$ e quindi una delle due norme deve essere uguale a 1, dunque uno dei fattori di z è invertibile.
($\Longrightarrow$) Sia $z \in \mathbb{Z}[i]$ irriducibile. Intanto $z \mid z\overline{z} = g(z) = q_1 \dots q_s$ dove i q_i sono primi in $\mathbb{Z}$ (ossia abbiamo fattorizzato $g(z)$ in $\mathbb{Z}$). Essendo z irriducibile in $\mathbb{Z}[i]$, per il Teorema 11.5 si ha che $z \mid q_i$ per un certo i. Deve essere dunque $zw = q_i$ per un certo $w \in \mathbb{Z}[i]$. Se w è invertibile allora z è associato a q_i in $\mathbb{Z}[i]$, e dunque q_i è irriducibile in $\mathbb{Z}[i]$. Ma allora, per quanto visto in questo paragrafo, q_i è un primo della forma $4n+3$. Quindi z, a meno di associati, è un primo di tale tipo. Se invece w non è invertibile allora $|w|^2 \neq 1$; passando ai quadrati delle norme, si osserva che

$$|z|^2|w|^2 = q_i^2.$$

da cui si deduce $|w|^2 = q_i$ e $|z|^2 = q_i$. □

3. Complementi (facoltativo): esempio ulteriore di un dominio in cui la fattorizzazione non è unica

La nostra attenzione adesso si sposta sugli anelli del tipo $\mathbb{Z}[\sqrt{n}]$ e $\mathbb{Z}[i\sqrt{n}]$. Gli interi di Gauss appartengono a questa famiglia di anelli.
Intanto osserviamo che se n è un quadrato allora $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$, quindi in questo paragrafo n non sarà un quadrato e anzi sarà un elemento in $\mathbb{Z}$ 'squarefree', ovvero uguale ad un prodotto di primi distinti, tutti con esponente uguale a 1. Inoltre adotteremo la notazione per cui per esempio $\mathbb{Z}[\sqrt{-14}]$ significa $\mathbb{Z}[i\sqrt{14}]$.

Questi anelli, come vedremo, in generale non sono euclidei. È possibile comunque definire su di essi una "seminorma" nel modo seguente

$$\begin{array}{rccc} \ell: & \mathbb{Z}[\sqrt{n}] & \longrightarrow & \mathbb{Z} \\ & a+b\sqrt{n} & \longmapsto & a^2-nb^2 \end{array}.$$

LEMMA 11.17. *L'applicazione ℓ è moltiplicativa.*

DIMOSTRAZIONE. Consideriamo $\mathbb{Z}[\sqrt{n}]$ e due elementi $a+b\sqrt{n}$ e $c+d\sqrt{n}$ dell'anello. Intanto

$$\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right) = ac+bdn+(ad+bc)\sqrt{n},$$

da cui

$$\begin{aligned} \ell\left(\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right)\right) &= (ac+bdn)^2 - n(ad+bc)^2 \\ &= a^2c^2+2abcdn+b^2d^2n^2-a^2d^2n-2abcdn-b^2c^2n = \\ &= c^2(a^2-nb^2)-nd^2(a^2-nb^2) = (a^2-nb^2)(c^2-nd^2) = \\ &= \ell\left(a+b\sqrt{n}\right)\ell\left(c+d\sqrt{n}\right), \end{aligned}$$

□

LEMMA 11.18. *Un elemento $z \in \mathbb{Z}[\sqrt{n}]$ è invertibile se e solo se $\ell(z) \in \{1,-1\}$.*

DIMOSTRAZIONE. ($\Longrightarrow$) Se $z \in \mathbb{Z}[\sqrt{n}]$ ed è invertibile allora $zw = 1$ per qualche $w \in \mathbb{Z}[\sqrt{n}]$. Per il lemma precedente si ha $\ell(z)\ell(w) = \ell(1) = 1$ e dunque $\ell(z) \in \{1,-1\}$.
($\Longleftarrow$) Sia $z = a+b\sqrt{n}$ con $|\ell(z)| = 1$, allora $|a^2-nb^2| = 1$. Ma allora possiamo scrivere $\left(a+b\sqrt{n}\right)\left(a-b\sqrt{n}\right) = 1$ o $\left(a+b\sqrt{n}\right)\left(-a+b\sqrt{n}\right) = 1$, e in ogni caso z è invertibile. □

Studiando gli anelli di questo tipo ci possiamo imbattere per esempio in anelli che non sono a fattorizzazione unica.

LEMMA 11.19. *L'anello* $\mathbb{Z}[\sqrt{10}]$ *non è un dominio a fattorizzazione unica.*

DIMOSTRAZIONE. Per esempio osserviamo che 6 possiamo scriverlo nei due modi che seguono:

$$(4+\sqrt{10})(4-\sqrt{10}) = 6 = 2\cdot 3,$$

ma per concludere che $\mathbb{Z}[\sqrt{10}]$ non è a fattorizzazione unica dobbiamo essere sicuri che gli elementi che appaiono nelle due fattorizzazioni siano irriducibili. Mostriamo che 2 e 3 sono elementi irriducibili; se $2 = (a+b\sqrt{10})(c+d\sqrt{10})$ fosse una fattorizzazione senza invertibili allora

$$\ell(a+b\sqrt{10})\ell(c+d\sqrt{10}) = \ell(2) = 4$$

e quindi le due seminorme a primo membro dovrebbero essere entrambe uguali a 2 o a -2 (non potrebbe essere che una delle due è uguale a ± 1, perché in tal caso l'elemento sarebbe invertibile). Ma ciò non è possibile perché $a^2 - 10b^2 = \pm 2$ non ha soluzioni intere. Procedendo in modo analogo per il 3 si ottiene che anche 3 è irriducibile, visto che $a^2 - 10b^2 = \pm 3$ non ha soluzioni intere. L'irriducibilità di $(4+\sqrt{10})$ e $(4-\sqrt{10})$ è una conseguenza dei conti già svolti. Infatti tali elementi hanno seminorma 6: dunque per esempio se $(4+\sqrt{10})$ avesse una fattorizzazione senza invertibili, i due fattori dovrebbero avere seminorma rispettivamente uguale a 2 e a 3, ma abbiamo già visto che nell'anello non ci sono elementi di questo tipo. □

OSSERVAZIONE 11.20. Osserviamo che nell'esempio precedente 2 è irriducibile e $2 \mid (4+\sqrt{10})(4-\sqrt{10})$ ma non divide nessuno dei due fattori: uno dei tanti modi per vederlo è che se fosse $2(a+b\sqrt{10}) = 4+\sqrt{10}$ allora varrebbe $\ell(2)|\ell(4+\sqrt{10})$ che è falso perché 4 non divide 6.

4. Esercizi

ESERCIZIO 11.21. Sia D un dominio, e sia $p \in D$ un elemento con la proprietà che se $p|ab$ allora o p divide a oppure p divide b. Dimostrare che p è un irriducibile. Se si leva l'ipotesi che D sia un dominio possiamo concludere che p è irriducibile?

ESERCIZIO 11.22. Consideriamo in $\mathbb{R}[x]$ i polinomi $f(x) = x^4+x^3-x-1$, $g(x) = x^{10}-x^7$ e sia I l'ideale $(f(x), g(x))$. Determinare gli ideali di $\mathbb{R}[x]$ che contengono I.

ESERCIZIO 11.23. Fattorizzare come prodotto di irriducibili l'elemento 2 in $\mathbb{Z}[i]$.

ESERCIZIO 11.24. Fattorizzare come prodotto di irriducibili l'elemento $3+4i$ in $\mathbb{Z}[i]$.

ESERCIZIO 11.25. Decidere se 5 è irriducibile in $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}[i]$ (e se volete provate anche in $\mathbb{Z}[i\sqrt{2}]$).

ESERCIZIO 11.26. Fattorizzare $43i - 19$ in prodotto di irriducibili in $\mathbb{Z}[i]$.

ESERCIZIO 11.27. Fare la divisione euclidea in $\mathbb{Z}[i]$ fra $11+10i$ (dividendo) e $4+i$ (divisore).

ESERCIZIO 11.28. Utilizzando i risultati sugli anelli euclidei e quelli del Paragrafo 2 di questo capitolo possiamo anche dimostrare che un numero primo della forma $4n+1$ può essere scritto *in modo unico* come somma di due quadrati di numeri interi?

ESERCIZIO 11.29. Trovare tutte le rappresentazioni di 1105 come somma di due quadrati.

ESERCIZIO 11.30. Trovare tutte le rappresentazioni di 2425 come somma di due quadrati.

Esercizio 11.31. Dimostrare che un numero intero $n \geq 2$ si può scrivere come somma di due quadrati di interi positivi se e solo se nella fattorizzazione di n in $\mathbb{Z}$ i numeri primi congrui a 3 modulo 4 compaiono con esponente pari.

Esercizio 11.32. Dire se l'anello $\mathbb{Z}[i]/(1+2i)$ è o non è un campo e contare quanti elementi ha.

Esercizio 11.33. Dire se l'anello $\mathbb{Z}[i]/(2+2i)$ è o non è un campo e contare quanti elementi ha.

Esercizio 11.34. Dato $a+bi \in \mathbb{Z}[i]$, chiamiamo $N(a+bi)$ il numero di elementi dell'anello $\mathbb{Z}[i]/(a+bi)$.

(1) Dimostrare che se $a \in \mathbb{Z}$, allora $N(a) = a^2$.
(2) Dimostrare che per ogni $a+bi \in \mathbb{Z}[i]$ vale $N(a+bi) = N(a-bi)$.
(3) Dimostrare che per ogni $z, w \in Z[i]$ vale $N(zw) = N(z)N(w)$.
(4) Dimostrare che per ogni $a+bi \in \mathbb{Z}[i]$ vale $N(a+bi) = a^2+b^2$.

Esercizio 11.35. Dato un numero primo p congruo a 1 modulo 4, si consideri l'insieme $S = \{(x,y,z) \in \mathbb{N}^3 \mid x^2+4yz = p\}$. Dimostrare che la funzione $f : S \to S$ definita da

$$f((x,y,z)) = (x+2z, z, y-x-z) \quad \text{se} \quad x < y-z$$
$$f((x,y,z)) = (2y-x, y, x-y+z) \quad \text{se} \quad y-z < x < 2y$$
$$f((x,y,z)) = (x-2y, x-y+z, y) \quad \text{se} \quad x > 2y$$

è una involuzione, ossia $f \circ f$ è l'identità. Dimostrare inoltre che f ha un solo punto fisso. Dunque $|S|$ è dispari, e allora anche l'involuzione $g : S \to S$ data da $g((x,y,z)) = (x,z,y)$ deve avere un punto fisso. Questo dimostra che p si può scrivere come somma di due quadrati.

[Si tratta della 'one sentence proof' del Teorema 11.12 pubblicata da Zagier[2] in The American Mathematical Monthly, Vol. 97, No. 2 (Feb. 1990).]

[2]Don Zagier, matematico americano, 1951-

CAPITOLO 12

Anelli di polinomi, approfondimenti sulla irriducibilità

Abbiamo visto che se K è un campo, allora tutti gli ideali di $K[x]$ sono della forma $(f(x))$ per un qualche $f(x) \in K[x]$. Inoltre, se $f(x)$ è irriducibile, allora $K[x]/(f(x))$ è un campo che contiene (un sottoanello isomorfo a) K (ossia le classi dei polinomi costanti), è uno spazio vettoriale su K di dimensione uguale al grado di $f(x)$, e in questo campo il nostro polinomio ha una radice (la classe di x). Ci poniamo quindi due domande naturali.

1) Cosa succede se $f(x)$ non è irriducibile? Abbiamo già visto che il quoziente $K[x]/(f(x))$ non è un campo in questo caso. Possiamo dire qualcosa di più?

2) Come sono fatti i polinomi irriducibili di $K[x]$? Quanti sono? Come li trovo?

Queste due domande sono piuttosto generali e difficili, ma in questo capitolo faremo alcune importanti considerazioni che ci permetteranno di cominciare a "grattare la superficie" di questi problemi.

1. Il teorema cinese del resto revisited

Sia K un campo, e sia $f(x) \in K[x]$. Denotiamo con $\overline{b(x)} := b(x) + (f(x))$ la classe di $b(x) \in K[x]$ in $K[x]/(f(x))$.

Supponiamo che $f(x)$ sia riducibile, e siano $g(x), h(x) \in K[x]$ tali che $f(x) = g(x)h(x)$, con $\deg(g(x)) \geq 1$ e $\deg(h(x)) \geq 1$. Allora abbiamo già osservato che $\overline{g(x)}$ e $\overline{h(x)}$ sono divisori dello zero non banali, ossia sono non nulli ma il loro prodotto fa zero in $K[x]/(f(x))$.

Cos'altro possiamo dire in questo caso dell'anello $K[x]/(f(x))$?

Per rispondere a questa domanda, diamo prima una definizione, e poi guardiamo a una situazione analoga che abbiamo già studiato.

DEFINIZIONE 12.1. Dati due anelli A_1 e A_2, definiamo il *prodotto diretto* $A_1 \times A_2$ definendo sull'insieme $A_1 \times A_2$ le seguenti operazioni di somma e prodotto:

$$(a_1, a_2) + (b_1, b_2) := (a_1 + a_2, b_1 + b_2) \quad \text{e} \quad (a_1, a_2) \cdot (b_1, b_2) := (a_1 a_2, b_1 b_2)$$

per ogni $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$.

ESERCIZIO 12.2. 1) Mostrare che con le definizioni date sopra $A_1 \times A_2$ è effettivamente un anello.

2) Mostrare che se A_1 e A_2 non sono banali, allora $A_1 \times A_2$ non è mai un campo.

Una situazione analoga l'abbiamo già studiata: consideriamo un elemento $n \in \mathbb{Z}$, con $n \geq 2$, tale che $n = ab$, dove $a, b \in \mathbb{Z}$ sono tali che $a > 1$ e $b > 1$. Proviamo a capire com'è fatto l'anello quoziente $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$. L'osservazione cruciale è che abbiamo una funzione

$$f : \mathbb{Z}/(n) \to \mathbb{Z}/(a) \times \mathbb{Z}/(b)$$

definita da $f([c]_n) := ([c]_a, [c]_b)$ per ogni $[c]_n \in \mathbb{Z}/(n)$. Il fatto che questa funzione sia ben definita è un facile **esercizio**. È altrettanto facile verificare che f è in effetti un omomorfismo di anelli (**esercizio**). Ora quello che il teorema cinese del resto ci dice

è proprio che se $\mathrm{MCD}(a,b) = 1$ allora questa funzione f è una bigezione: **esercizio**. Dunque abbiamo scoperto che se $\mathrm{MCD}(a,b) = 1$ allora abbiamo un isomorfismo di anelli $\mathbb{Z}/(ab) \cong \mathbb{Z}/(a) \times \mathbb{Z}/(b)$.

Torniamo ora a $K[x]/(f(x))$ con $f(x) = g(x)h(x)$, $\deg(g(x)) \geq 1$ e $h(x) \geq 1$. Se $\mathrm{MCD}(f(x), g(x)) = 1$, allora, con ragionamenti del tutto analoghi, si dimostra effettivamente che la funzione

$$\varphi : K[x]/(f(x)) \to K[x]/(g(x)) \times K[x]/(h(x))$$

è un isomorfismo di anelli. Quello che serve per dimostrare questa affermazione è l'analogo per i polinomi del *teorema cinese del resto*, la cui dimostrazione passerà a sua volta per la divisione euclidea e il teorema di Bézout per polinomi: **esercizio**.

2. Irriducibilità in $\mathbb{Z}_p[x]$ e in $\mathbb{Z}[x]$

In generale decidere se un polinomio è irriducibile è un problema difficile. Il teorema fondamentale dell'algebra (e un suo corollario che abbiamo visto) ci dice che in $\mathbb{C}[x]$ gli unici irriducibili sono i polinomi di grado 1, mentre in $\mathbb{R}[x]$ ci sono i polinomi di grado 1 e quelli di grado due con discriminante negativo. Nonostante questo, calcolare la fattorizzazione in irriducibili (che abbiamo visto essere unica a meno di associati) può essere estremamente complicato. Ad esempio ci si può cominciare a chiedere se ci sono fattori lineari, ossia radici nell'anello dei coefficienti. Questo problema, anche in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$, è molto difficile, sia in teoria (non ci sono formule generali, per motivi profondi), sia in pratica (anche sapendo che una radice deve esserci, trovarla o anche solo approssimarla può essere complicato in concreto).

C'è però un insieme di campi K in cui questo problema in $K[x]$ è decisamente più abbordabile: i campi finiti. In questo capitolo ci concentriamo sui campi $\mathbb{Z}_p$.

In $\mathbb{Z}_p[x]$ il problema di decidere se un polinomio è irriducibile non presenta difficoltà teoriche: in fondo c'è un numero finito di polinomi monici di grado $d \in \mathbb{N}$ (sono p^d), e i possibili fattori propri di un polinomio di grado n in $\mathbb{Z}_p[x]$ si dovranno cercare tra questi per $1 \leq d \leq n-1$.

Esempio 12.3. Descriviamo i polinomi irriducibili (monici) di $\mathbb{Z}_2[x]$ di grado piccolo. Oltre agli ovvi x e $x+1$ (che sono quelli di grado 1), fino a grado minore o uguale a 3 basta verificare che il nostro polinomio non ha una radice in $\mathbb{Z}_2$, cosa che richiede due verifiche immediate, ossia se le valutazioni in $[0]_2$ e in $[1]_2$ sono nulle. Troviamo quindi che sono irriducibili anche

$$x^2 + x + 1, \quad x^3 + x^2 + 1 \quad \text{e} \quad x^3 + x + 1.$$

Per quelli di grado 4, oltre a verificare che non ci sono radici, dobbiamo verificare che non ci sono fattori di grado 2; ma c'è solo un irriducibile di grado due, quindi si fa presto...

È questo un momento opportuno per osservare che, a differenza del caso dei polinomi complessi, cercare una radice razionale di un polinomio a coefficienti interi (o razionali) è un problema teoricamente semplice.

Esercizio 12.4. 1) Sia dato un polinomio $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_n \neq 0 \neq a_0$, e sia p/q una radice di $f(x)$, con $p, q \in \mathbb{Z}$, $q \neq 0$ e $\mathrm{MCD}(p,q) = 1$. Mostrare che q divide a_n e p divide a_0.

2) Descrivere un algoritmo che in un numero finito di passi decide se un dato polinomio in $\mathbb{Q}[x]$ ha una radice razionale, e in caso affermativo ne calcola una.

È il momento di fare un altro utile esercizio.

Esercizio 12.5. Siano A_1 e A_2 due anelli, e sia $\varphi : A_1 \to A_2$ un omomorfismo di anelli. Mostrare che la funzione

$$\hat{\varphi} : A_1[x] \to A_2[x]$$

data per ogni $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in A_1[x]$ da

$$\hat{\varphi}(f(x)) := \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0)$$

definisce un omomorfismo di anelli.

Vogliamo usare questo omomorfismo nel caso della proiezione al quoziente $\varphi : \mathbb{Z} \to \mathbb{Z}_p$, dove p è un primo. Diamo prima una definizione.

Definizione 12.6. Un polinomio $f(x) \in \mathbb{Z}[x]$ è detto *primitivo* se il massimo comun divisore dei suoi coefficienti è uguale a 1.

In pratica un polinomio in $\mathbb{Z}[x]$ è primitivo se non ha fattori irriducibili di grado zero.

Proposizione 12.7. *Sia p un primo, sia $\varphi : \mathbb{Z} \to \mathbb{Z}_p = \mathbb{Z}/(p)$ la proiezione al quoziente, e sia $\hat{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ l'omomorfismo descritto sopra. Sia $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ primitivo con $n \geq 1$, e supponiamo che p non divida a_n. Se $\hat{\varphi}(f(x))$ è irriducibile in $\mathbb{Z}_p[x]$, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.*

Dimostrazione. Supponiamo che $f(x)$ sia riducibile, e siano $g(x), h(x) \in \mathbb{Z}[x]$ tali che $f(x) = g(x)h(x)$. Siccome $f(x)$ è primitivo dobbiamo necessariamente avere $\deg(g(x)) \geq 1$ e $\deg(h(x)) \geq 1$. Osserviamo che

$$\hat{\varphi}(f(x)) = \hat{\varphi}(g(x))\hat{\varphi}(h(x))$$

e $\deg(\hat{\varphi}(f(x))) = \deg(f(x)) = n$ poichè per ipotesi $\varphi(a_n) \neq [0]_p$. Dunque dobbiamo avere anche $\deg(\hat{\varphi}(g(x))) = \deg(g(x)) \geq 1$ e $\deg(\hat{\varphi}(h(x))) = \deg(h(x)) \geq 1$, e questo mostra che $\hat{\varphi}(f(x))$ è riducibile in $\mathbb{Z}_p[x]$. □

Osserviamo che l'ipotesi di primitività è necessaria: ad esempio per $p = 2$ e $f(x) = 3x + 3 = 3(x + 1)$ avremmo $\overline{\varphi}(f(x))$ irriducibile, ma $f(x)$ chiaramente non lo è.

Usando la stessa idea si può dimostrare un *criterio* di irriducibilità in $\mathbb{Z}[x]$ molto utile, dovuto ad Eisenstein.

Teorema 12.8 (Eisenstein). *Sia $p \in \mathbb{N}$ un primo, e sia $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ primitivo tale che*

1. *p non divide a_n;*
2. *p divide $a_0, a_1, \ldots, a_{n-1}$;*
3. *p^2 non divide a_0.*

Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

Esempio 12.9. Per il criterio di Eisenstein, il polinomio $x^5 - 4x + 2$ è irriducbile in $\mathbb{Z}[x]$. Infatti, $x^k - 4x + 2$ è irriducbile in $\mathbb{Z}[x]$ per ogni $k \geq 2$, il che mostra che in $\mathbb{Z}[x]$ ci sono polinomi irriducibili in ogni grado (a differenza di quello che succede in $\mathbb{C}[x]$ o in $\mathbb{R}[x]$ ad esempio).

Dimostrazione del criterio di Eisenstein. Supponiamo che $f(x)$ sia riducibile in $\mathbb{Z}[x]$, e siano $g(x), h(x) \in \mathbb{Z}[x]$ tali che

$$f(x) = g(x)h(x).$$

Poichè $f(x)$ è primitivo, $g(x)$ e $h(x)$ saranno due polinomi non costanti.

Applicando l'omomorfismo $\hat{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ della proposizione precedente e l'ipotesi (2), otteniamo

$$[a_n]_p x^n = \hat{\varphi}(f(x)) = \hat{\varphi}(g(x))\hat{\varphi}(h(x)),$$

dove per l'ipotesi (1) $[a_n]_p \neq [0]_p$. Osserviamo (**esercizio**) che in un anello di polinomi a coefficienti in un campo, quale è $\mathbb{Z}_p[x]$, il prodotto di due polinomi è un monomio se e solo se entrambi i fattori sono monomi (basta guardare ai termini di grado minimo e massimo). Siccome $\deg(\hat{\varphi}(f(x))) = \deg(f(x)) = n$, varranno anche $\deg(\hat{\varphi}(g(x))) = \deg(g(x)) \geq 1$ e $\deg(\hat{\varphi}(h(x))) = \deg(h(x)) \geq 1$. Dunque $\hat{\varphi}(g(x))$ e $\hat{\varphi}(h(x))$ sono due monomi di grado positivo. In particolare i termini costanti di $g(x)$ e $h(x)$ sono entrambi divisibili per p. Ma siccome a_0 è il prodotto di questi due coefficienti, dovremmo avere che p^2 divide a_0, e questo contraddice la nostra ipotesi (3). Dunque $f(x)$ non può essere riducibile in $\mathbb{Z}[x]$. □

3. Irriducibilità in $\mathbb{Q}[x]$

Vogliamo ora studiare l'irriducibilità in $\mathbb{Q}[x]$.
Il lemma fondamentale è il seguente.

Lemma 12.10 (Gauss). *Siano $f(x), g(x) \in \mathbb{Z}[x]$ due polinomi primitivi. Allora il loro prodotto $f(x)g(x) \in \mathbb{Z}[x]$ è primitivo.*

Dimostrazione. Siano

$$f(x) = \sum_i a_i x^i \quad \text{e} \quad g(x) = \sum_j b_j x^j$$

con $a_i, b_j \in \mathbb{Z}$ per ogni i e j, e supponiamo che $f(x)g(x)$ non sia primitivo. Sia allora p un primo che divide tutti i coefficienti di $f(x)g(x)$. Siano $a_s x^s$ e $b_r x^r$ i due termini di grado più alto di $f(x)$ e $g(x)$, rispettivamente, che non sono divisibili per p. Allora il coefficiente di x^{r+s} nel prodotto $f(x)g(x)$ è

$$\sum_{i+j=s+r} a_i b_j,$$

e questo deve essere divisibile per p. Ma p divide sicuramente tutti i termini di questa somma, con la sola possibile eccezione di $a_s b_r$. Dunque p dovrà dividere anche $a_s b_r$, e quindi, in quanto primo, dividerà uno tra a_s e b_r. Questa è una cotraddizione, dunque $f(x)g(x)$ deve essere primitivo. □

Abbiamo quindi il seguente importante corollario.

Corollario 12.11. *Un polinomio in $\mathbb{Z}[x]$ di grado positivo è irriducibile in $\mathbb{Z}[x]$ se e solo se è primitivo ed è irriducibile in $\mathbb{Q}[x]$.*

Dimostrazione. Se $f(x) \in \mathbb{Z}[x]$ è primitivo ed irriducibile in $\mathbb{Q}[x]$, allora sarà ovviamente irriducibile in $\mathbb{Z}[x]$. L'implicazione non banale è l'altra.

Se $f(x) \in \mathbb{Z}[x]$ non è primitivo, allora non sarà irriducibile in $\mathbb{Z}[x]$. Quindi possiamo assumere che $f(x) \in \mathbb{Z}[x]$ sia primitivo. Supponiamo che $f(x) = a(x)b(x)$, con $a(x), b(x) \in \mathbb{Q}[x]$ di grado positivo. Vogliamo mostrare che $f(x)$ è riducibile in $\mathbb{Z}[x]$. Possiamo trovare $\alpha, \beta \in \mathbb{Q}$ tali che $a'(x) = \alpha a(x) \in \mathbb{Z}[x]$ e $b'(x) = \beta b(x) \in \mathbb{Z}[x]$, ed entrambi $a'(x)$ e $b'(x)$ sono primitivi (**esercizio**). Allora, per il lemma di Gauss, anche $a'(x)b'(x) = \alpha\beta f(x) \in \mathbb{Z}[x]$ è primitivo. Poichè $f(x)$ è primitivo, dobbiamo avere $\alpha\beta \in \mathbb{Z}$ (**esercizio**), e poichè $\alpha\beta f(x)$ è primitivo, dobbiamo anche avere $\alpha\beta = \pm 1$. Dunque $f(x) = \pm a'(x)b'(x)$, il che mostra che $f(x)$ non è irriducibile in $\mathbb{Z}[x]$, che era quello che volevamo mostrare. □

CAPITOLO 13

Campi

1. Approfondimenti sulle estensioni semplici di campi

Nei capitoli precedenti abbiamo visto come sia possibile, dato un campo K e un polinomio $f(x) \in K[x]$ irriducibile e di grado ≥ 2, 'creare' un nuovo campo, che contiene K, dove $f(x)$ ammette una radice. Ma talvolta noi conosciamo già un campo che contiene K e in cui il polinomio ha una radice: per esempio, nel caso del polinomio $x^3 - 2 \in \mathbb{Q}[x]$, noi sappiamo che tale polinomio non ha radici razionali ma che in $\mathbb{R}$ esiste una radice, cioè $\sqrt[3]{2}$. Che relazione c'è fra il campo $\mathbb{Q}[x]/(x^3 - 2)$ costruito nel paragrafo precedente e la presenza di una radice di $x^3 - 2$ in $\mathbb{R}$?

Per rispondere, affrontiamo la situazione da un punto di vista generale. Premettiamo intanto la definizione di sottocampo:

DEFINIZIONE 13.1. Dati un campo E ed un sottoanello A di E, si dice che A è un *sottocampo* di E se per ogni $a \in A$ diverso da 0 l'inverso di a appartiene ad A.

Sia K un campo e sia L un campo che è una *estensione* di K, ossia vale $K \subseteq L$. Dato $\alpha \in L$, consideriamo adesso tutti i sottocampi di L che contengono K e α. La loro intersezione è ancora un sottocampo di L (facile esercizio) che contiene K e α. Per costruzione, si tratta del minimo sottocampo di L (minimo rispetto all'inclusione) che contiene K e α. Visto che questo minimo sottocampo esiste, lo valorizziamo con una notazione apposita:

DEFINIZIONE 13.2. Dati due campi $K \subseteq L$ e un elemento $\alpha \in L$, indicheremo con $K(\alpha)$ il minimo sottocampo (rispetto all'inclusione) di L che contiene K e α. Si dice che $K(\alpha)$ è una *estensione semplice* di K.

Dati $K \subseteq L$ e $\alpha \in L$, come sopra, possiamo considerare l'omomorfismo di valutazione

$$\psi : K[x] \to L$$

tale che, per ogni $f(x) \in K[x]$, $\psi(f(x)) = f(\alpha)$.

Indicheremo anche con il simbolo $K[\alpha]$ l'immagine di ψ. Possiamo in effetti vedere gli elementi di Imm ψ come i polinomi in α a coefficienti in K.

Qual è il nucleo di ψ? I suoi elementi sono tutti i polinomi $g(x) \in K[x]$ tali che $g(\alpha) = 0$. Sappiamo che $\operatorname{Ker}\psi$ è un ideale e, visto che $K[x]$ è euclideo, $\operatorname{Ker}\psi$ è un ideale principale.

Possiamo allora scrivere

$$\operatorname{Ker}\psi = (f(x))$$

per un certo polinomio $f \in K[x]$.

Ci sono due casi. Il primo è che $\operatorname{Ker}\psi = \{0\}$. Ovvero α non è radice di nessun polinomio a coefficienti in K (a parte ovviamente il polinomio 0). Si dice in tal caso che $\alpha \in L$ è un elemento *trascendente su* K. Per il primo teorema di omomorfismo sappiamo che $K[x] \cong K[\alpha] = \operatorname{Imm}\psi$. In particolare $K[\alpha]$ non è un campo e dunque $K[\alpha] \subsetneq K(\alpha)$.

Osservazione 13.3. Come è noto (ma non lo dimostreremo in questo corso) i numeri reali π ed e, il numero di Eulero base dei logaritmi (detto anche di Nepero[1]) sono due esempi di numeri trascendenti su $\mathbb{Q}$.[2]

L'altro caso è che $\operatorname{Ker}\psi = (f(x)) \neq \{0\}$. In tal caso si dice che α è algebrico su K, nel senso della seguente definizione:

Definizione 13.4. Dati due campi $K \subseteq L$ si dice che un elemento $\alpha \in L$ è *algebrico su* K se esiste un polinomio non nullo in $K[x]$ di cui α è radice, ossia se il nucleo $\operatorname{Ker}\psi$ della valutazione definita sopra è diverso da 0. Un generatore $f(x)$ di $\operatorname{Ker}\psi$ si chiama *polinomio minimo di* α *su* K.

Osservazione 13.5. Un polinomio minimo di α su K, per come è stato definito, divide ogni altro polinomio in $K[x]$ che ha α come radice. Come avrete subito notato, un polinomio minimo non è unico, ma è unico a meno di associati. L'aggettivo 'minimo' si riferisce al fatto che tale polinomio ha grado minimo fra tutti i polinomi di $K[x]$ che hanno α come radice. Talvolta viene usata la convenzione per cui fra tutti i polinomi associati che sono polinomi minimi quello che ha coefficiente direttore uguale a 1 viene chiamato *il* polinomio minimo di α su K.

Continuiamo a studiare il caso in cui α è algebrico su K e pertanto $\operatorname{Ker}\psi = (f(x)) \neq \{0\}$. Osserviamo che allora $f(x)$ è irriducibile in $K[x]$. Si può vedere in molti modi: per esempio se $f(x) = h_1(x)h_2(x)$ fosse una fattorizzazione in $K[x]$ con $h_1(x), h_2(x)$ non costanti, e dunque $deg\ h_1(x) < deg\ f(x)$ e $deg\ h_2(x) < deg\ f(x)$, valutando in α avremmo $f(\alpha) = 0 = h_1(\alpha)h_2(\alpha)$. Allora deve valere $h_1(\alpha) = 0$ oppure $h_2(\alpha) = 0$, ossia $h_1(x) \in \operatorname{Ker}\psi$ oppure $h_2(x) \in \operatorname{Ker}\psi$, che è assurdo perché $f(x)$, generatore dell'ideale $\operatorname{Ker}\psi$, ha grado maggiore di $h_1(x)$ e $h_2(x)$.

Torniamo a studiare il nostro omomorfismo di valutazione ψ nel caso che α sia algebrico su K. Dal fatto che $\operatorname{Ker}\psi = (f(x))$ con $f(x)$ irriducibile e dal primo teorema di isomorfismo ricaviamo che $\operatorname{Imm}\psi = K[\alpha]$ è un campo: più esattamente è un sottocampo di L che contiene K e α, dunque contiene il campo $K(\alpha)$. Si osserva subito anche che tutti i polinomi in α devono appartenere a $K(\alpha)$, dunque $K[\alpha] \subseteq K(\alpha)$, per cui vale $K[\alpha] = K(\alpha)$.

Questo potrebbe suscitare un dubbio.

Per esempio se $K = \mathbb{Q}$, $L = \mathbb{R}$ e $\alpha = \sqrt[3]{2}$, sappiamo che sia $1 + \sqrt[3]{2}$ sia il suo inverso $\dfrac{1}{1+\sqrt[3]{2}}$ devono appartenere al campo $\mathbb{Q}(\sqrt[3]{2})$.

Però abbiamo appena visto che in realtà $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$: vogliamo renderci conto come sia possibile che $\dfrac{1}{1+\sqrt[3]{2}}$ appartenga a $\mathbb{Q}[\sqrt[3]{2}]$.

Per la verità questo caso è semplice, e potremmo subito esibire un polinomio in $\sqrt[3]{2}$ uguale a $\dfrac{1}{1+\sqrt[3]{2}}$, ma sviluppare nei dettagli questo esempio potrà essere illuminante.

Consideriamo dunque l'omomorfismo di valutazione $\psi : \mathbb{Q}[x] \to \mathbb{R}$ che valuta ogni polinomio in $\sqrt[3]{2}$. Si nota subito che il polinomio minimo di $\sqrt[3]{2}$ è $x^3 - 2$, ossia che $\operatorname{Ker}\psi = (x^3 - 2)$. Infatti $(x^3 - 2)$ è incluso in $\operatorname{Ker}\ \psi$ ma si può vedere facilmente che $x^3 - 2$

[1] John Napier, matematico e astronomo scozzese, 1550-1617.

[2] Osservazione per gli amanti dell'infinito: i numeri algebrici sono un sottoinsieme infinito numerabile di $\mathbb{R}$ (potreste provare a dimostrarlo per esercizio), dunque i numeri trascendenti sono in realtà 'di più' dei numeri algebrici (se fossero un infinito numerabile allora $\mathbb{R}$ sarebbe numerabile...).

è irriducibile in $\mathbb{Q}[x]$,[3] dunque è un generatore di $Ker\ \psi$. Infatti sia $g(x)$ un generatore di $Ker\psi$; allora deve dividere x^3-2 ma x^3-2 è irriducibile dunque, a meno di associati, $g(x)=1$ oppure $g(x)=f(x)$: il primo dei due casi si esclude perché implicherebbe $Ker\psi=\mathbb{Q}[x]$, che è assurdo dato che $\psi(1)=1$. [4]

Dunque

$$\mathbb{Q}[\sqrt[3]{2}] \cong Q[x]/(x^3-2)$$

Ora riflettiamo sul quoziente $\mathbb{Q}[x]/(x^3-2)$. Ogni elemento di $\mathbb{Q}[x]/(x^3-2)$ si può rappresentare come

$$ax^2+bx+c+(x^3-2)$$

con $a,b,c\in\mathbb{Q}$. Per esempio consideriamo l'elemento

$$x+1+(x^3-2)$$

Visto che il massimo comun divisore fra $x+1$ e x^3-2 è 1, per il Lemma di Bezout per polinomi è possibile scrivere 1 come combinazione lineare di $x+1$ e x^3-2 a coefficienti in $\mathbb{Q}[x]$. Nel caso in questione è semplicissimo trovare questa combinazione lineare, perchè l'algoritmo di Euclide è molto breve:

$$x^3-2=(x^2-x+1)(x+1)-3$$

dunque dopo una divisione possiamo scrivere

$$1=-\frac{1}{3}(x^3-2)+\frac{1}{3}(x^2-x+1)(x+1)$$

Una immediata verifica ci mostra a questo punto che le due classi $x+1+(x^3-2)$ e $\frac{1}{3}(x^2-x+1)+(x^3-2)$ sono una l'inversa dell'altra in $\mathbb{Q}[x]/(x^3-2)$.

D'altra parte, se valutiamo l'uguaglianza fra polinomi

$$1=-\frac{1}{3}(x^3-2)+\frac{1}{3}(x^2-x+1)(x+1)$$

ponendo $x=\sqrt[3]{2}$, otteniamo

$$1=-\frac{1}{3}((\sqrt[3]{2})^3-2)+\frac{1}{3}((\sqrt[3]{2})^2-\sqrt[3]{2}+1)(\sqrt[3]{2}+1)$$

ossia

$$1=\frac{1}{3}((\sqrt[3]{2})^2-\sqrt[3]{2}+1)(\sqrt[3]{2}+1)$$

Questo ci dice che in $\mathbb{R}$

$$\frac{1}{\sqrt[3]{2}+1}=\frac{1}{3}((\sqrt[3]{2})^2-\sqrt[3]{2}+1)$$

Abbiamo mostrato che l'inverso di $\sqrt[3]{2}+1$ può essere scritto come polinomio in $\sqrt[3]{2}$ ed appartiene pertanto a $\mathbb{Q}[\sqrt[3]{2}]$.

Questo ragionamento, ripetuto per ogni elemento non zero, ci mostra concretamente come mai $\mathbb{Q}[\sqrt[3]{2}]$ è un campo e ci indica come trovare gli elementi inversi.

Una ulteriore domanda che potremmo porci è la seguente. Sappiamo che il polinomio x^3-2 ammette altre due radici in $\mathbb{C}$, ovvero $\sqrt[3]{2}\omega$ e $\sqrt[3]{2}\omega^2$, dove $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}\imath$ è una radice cubica di 1.

---

[3]Questo si può fare osservando che il polinomio ha grado 3 e se fosse riducibile dovrebbe avere un fattore di grado 1, dunque dovrebbe avere una radice razionale. Ma si verifica facilmente che x^3-2 non ammette radici razionali. Un altro modo è usare il criterio di Eisenstein con il primo $p=2$.

[4]Questa osservazione ci fa riflettere sul fatto che, in generale, se abbiamo un omomorfismo di anelli con unità $g: A\to B$, il nucleo di g è uguale ad A se e solo se B è l'anello banale $B=\{0\}$.

Analogamente a quanto visto per $\mathbb{Q}[\sqrt[3]{2}]$, utilizzando l'omomorfismo di valutazione

$$\psi' : \mathbb{Q}[x] \to \mathbb{C}$$

tale che per ogni $g(x) \in \mathbb{Q}[x]$ $\psi(g(x) = g(\sqrt[3]{2}\omega)$, possiamo concludere che $\mathbb{Q}[\sqrt[3]{2}\omega]$ è isomorfo a $\mathbb{Q}[x]/(x^3-2)$.

Dunque abbiamo la seguente situazione

$$\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}\omega]$$

Se chiamiamo $\theta : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}\omega]$ l'isomorfismo che si ottiene, è facile osservare che θ lascia fissi gli elementi di $\mathbb{Q}$ e $\theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ (infatti nell'isomorfismo a sinistra $\sqrt[3]{2}$ viene mandato in $\overline{x}$ e in quello a destra $\overline{x}$ viene mandato in $\sqrt[3]{2}\omega$).

La stessa cosa si può dire di $\mathbb{Q}[\sqrt[3]{2}\omega^2]$. Abbiamo dunque individuato tre sottocampi di $\mathbb{C}$ isomorfi fra loro.

La cosa si può esporre in generale attraverso il seguente teorema:

Teorema 13.6. *Dati due campi $K \subseteq L$, sia $f(x)$ un polinomio irriducibile in $K[x]$ che ha due radici distinte α e β in L. Allora esiste un isomorfismo $\theta : K[\alpha] \to K[\beta]$ fra i campi $K[\alpha]$ e $K[\beta]$ tale che $\theta(\alpha) = \beta$ e θ ristretto a K sia l'identità.*

Dimostrazione. La dimostrazione ricalca esattamente quella illustrata nell'esempio, dunque la lasciamo a voi come esercizio. □

Talvolta può capitare che i campi $K[\alpha]$ e $K[\beta]$ che appaiono nel teorema precedente siano uguali, oltre che isomorfi: per esempio se si considera $K = \mathbb{Q}$, $L = \mathbb{C}$ e $f(x) = x^2 + 1$, si trova che $\mathbb{Q}(\imath) = \mathbb{Q}(-\imath)$.

In generale però $K[\alpha]$ e $K[\beta]$ non coincidono. Tornando al caso di $x^3 - 2$ che stavamo studiando, osserviamo infatti che i tre sottocampi di $\mathbb{C}$ sono tutti distinti: $\mathbb{Q}[\sqrt[3]{2}]$ certamente non coincide né con $\mathbb{Q}[\sqrt[3]{2}\omega]$ né con $\mathbb{Q}[\sqrt[3]{2}\omega^2]$ visto che $\mathbb{Q}[\sqrt[3]{2}]$ è contenuto in $\mathbb{R}$ e gli altri due invece non lo sono. Inoltre non può valere $\mathbb{Q}[\sqrt[3]{2}\omega] = \mathbb{Q}[\sqrt[3]{2}\omega^2]$ altrimenti a tale campo, come si verifica subito, dovrebbero appartenere gli elementi ω (ottenuto dividendo $\sqrt[3]{2}\omega^2$ per $\sqrt[3]{2}\omega$) e $\sqrt[3]{2}$ (ottenuto dividendo $\sqrt[3]{2}\omega$ per ω).

Dunque $\mathbb{Q}[\sqrt[3]{2}\omega] = \mathbb{Q}[\sqrt[3]{2}\omega^2]$ strettamente $\mathbb{Q}[\sqrt[3]{2}]$ e lo conterrebbe strettamente (visto che in $\mathbb{Q}[\sqrt[3]{2}\omega]$ ci sono anche numeri complessi non reali), e questo creerebbe problemi di dimensione: sappiamo infatti che gli spazi vettoriali $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[\sqrt[3]{2}\omega]$ e $Q[\sqrt[3]{2}\omega^2]$ hanno tutti dimensione 3 su $\mathbb{Q}$ essendo isomorfi a $\mathbb{Q}[x]/(x^3-2)$, pertanto se fosse $\mathbb{Q}[\sqrt[3]{2}\omega] = \mathbb{Q}[\sqrt[3]{2}\omega^2]$ tale spazio vettoriale avrebbe dimensione 3 su $\mathbb{Q}$ ma conterrebbe strettamente lo spazio vettoriale $\mathbb{Q}[\sqrt[3]{2}]$ che ha anch'esso dimensione 3 su $\mathbb{Q}$.

2. Creare un campo con tutte le radici di un polinomio

Cominciamo con il precisare che, dato un campo L, un polinomio $f(x) \in L[x]$ di grado $n > 0$ ha al più n radici in L.

Teorema 13.7. *Sia L un campo e sia $f(x) \in L[x]$ un polinomio di grado $n > 0$. Allora $f(x)$ ha al più n radici in L, contate con molteplicità.*

Dimostrazione. Se $f(x)$ non ha radici in L l'enunciato è vero. Se invece $f(x)$ ha una radice α_1, come sappiamo, possiamo fattorizzarlo così:

$$f(x) = (x - \alpha_1) f_1(x)$$

Se $f_1(x)$ ha una radice α_2 proseguiamo, e così via fino a che non troviamo

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_t) h(x)$$

dove $h(x) \in L[x]$ è un polinomio che non ha radici in L, e dunque non ha fattori di primo grado in $L[x]$. Dunque $\alpha_1, \ldots, \alpha_t$ sono t radici in L, con eventuali ripetizioni, e ovviamente, per questioni di grado, $t \leq n$. Per quel motivo siamo sicuri che in L non ci sono altre radici di $f(x)$ oltre a $\alpha_1, \ldots, \alpha_t$? Se esistesse in L una radice β_1 di $f(x)$ diversa dalle precedenti, potremmo ripetere il procedimento e scrivere un'altra fattorizzazione:

$$f(x) = (x - \beta_1) \cdots (x - \beta_s)\gamma(x)$$

dove anche $\beta_2, .., \beta_s \in L$ sono radici e $\gamma(x) \in L[x]$ è un polinomio che non ha radici in L. Le due fattorizzazioni che abbiamo trovato ci danno un assurdo. Un modo per vederlo è calcolare $f(\beta_1)$. In base alla prima fattorizzazione è un elemento di L diverso da 0, in base alla seconda è uguale a 0. Un altro modo è osservare che le due fattorizzazioni contraddicono l'unicità della fattorizzazione in irriducibili nell'anello euclideo $L[x]$: infatti la seconda fattorizzazione ci dice che $x - \beta_1$ è un fattore irriducibile di $f(x)$ mentre nella prima fattorizzazione, di cui conosciamo tutti i fattori irriducibili di primo grado, non appare alcun fattore associato a $x - \beta_1$.

□

Osservazione 13.8. Attenzione, invece in $\mathbb{Z}_8[x]$ il polinomio $x^2 - 2x$ ha quattro radici distinte: $[0], [2], [4], [6]$.

Osserviamo adesso che, iterando il procedimento che 'aggiunge' una radice di un polinomio, è possibile, dato un campo K e un polinomio $f(x) \in K[x]$, costruire un campo E che estende K e tale che in $E[x]$ il polinomio $f(x)$ si fattorizza nel prodotto di polinomi di grado 1.

Teorema 13.9. *Sia K un campo e sia $f(x) \in K[x]$ un polinomio di grado $n \geq 0$. Allora esistono un campo E tale che $K \subseteq E$ ed elementi $e_1, e_2, ..., e_n$ (eventualmente con ripetizioni) appartenenti ad E tali che $f(x)$ si fattorizza nel seguente modo in $E[x]$:*

$$f(x) = \lambda(x - e_1)(x - e_2) \cdots (x - e_n)$$

dove $\lambda \in E$ è una costante.

Dimostrazione. Per induzione su $n = deg\ f(x)$. Il passo base ($deg\ f(x) = 0$) è una immediata verifica. Supponiamo ora che $n = deg\ f(x) \geq 1$ e sia $f_1(x)$ un fattore irriducibile di $f(x)$. Costruiamo il campo $F = K[x]/(f_1(x))$: come sappiamo dal paragrafo precedente, in tale campo esiste una radice $\overline{x}$ di $f_1(x)$, e poniamo $e_1 = \overline{x}$. A questo punto in $F[x]$ abbiamo la seguente fattorizzazione:

$$f(x) = (x - e_1)g(x)$$

dove $g(x)$ è un polinomio di grado $n - 1$. Per ipotesi induttiva sappiamo che esiste un campo E che estende F ed elementi $e_2, ..., e_n$ in E tali che $g(x)$ si fattorizza nel seguente modo in $E[x]$:

$$g(x) = \lambda(x - e_2) \cdots (x - e_n)$$

con $\lambda \in E$. Per concludere osserviamo che E estende K in quanto $K \subseteq F \subseteq E$ e in $E[x]$ il polinomio $f(x)$ si fattorizza come

$$f(x) = \lambda(x - e_1)(x - e_2) \cdots (x - e_n)$$

□

3. Esercizi

Esercizio 13.10. Consideriamo $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\imath$, radice cubica di 1, e l'estensione semplice $\mathbb{Q}(\omega)$. Qual è la dimensione di $\mathbb{Q}(\omega)$ come spazio vettoriale su $\mathbb{Q}$? Qual è il polinomio minimo di $\sqrt[3]{2}$ sul campo $\mathbb{Q}(\omega)$?

Esercizio 13.11. Trovare il polinomio minimo di $\imath + \sqrt{2}$ su $\mathbb{Q}$.

Esercizio 13.12. Calcolare la dimensione su $\mathbb{Q}$ di $\mathbb{Q}(\sqrt{5})(\imath) = \mathbb{Q}(\sqrt{5}, \imath)$.[5]

Esercizio 13.13. Sia $\alpha \in \mathbb{C}$ una radice di $x^4 + 1$. Qual è la dimensione di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$? È vero o falso che $x^4 + 1$ si fattorizza come prodotto di fattori di grado 1 in $\mathbb{Q}(\alpha)$?

[5]In seguito, dato un campo K incluso in un campo L, e dati degli elementi $\alpha, \beta, \gamma ... \in L$, useremo spesso la notazione $K(\alpha, \beta, \gamma, ...)$ per indicare il campo $K(\alpha)(\beta)(\gamma)$ costruito per estensioni successive. È facile mostrare che tale campo è il più piccolo sottocampo di L che contiene K e $\alpha, \beta, \gamma, ...$, dunque la notazione scelta è una naturale generalizzazione di quella per le estensioni semplici.

CAPITOLO 14

Estensioni di campi

1. Alcune considerazioni sul grado delle estensioni di campi

Dati due campi $F \subseteq K$ diremo che K è una estensione di F. Come abbiamo già osservato nei casi di estensioni studiati nelle lezioni precedenti, K si può vedere anche come uno spazio vettoriale su F. La struttura di spazio vettoriale è quella indotta dal fatto che K è un campo: è già definita la somma fra due elementi di K e anche anche la moltiplicazione per 'scalare' γk, per ogni $\gamma \in F$ e per ogni $k \in K$.

In questa lezione vogliamo discutere alcune informazioni che possiamo ricavare da questa struttura di spazio vettoriale.

DEFINIZIONE 14.1. Dati due campi $F \subseteq K$, il *grado* di K su F è la dimensione di K come spazio vettoriale su F e si indica con il simbolo $[K : F]$. Se la dimensione è infinita si scrive $[K : F] = \infty$. Se il grado è finito, si dice che K è una estensione finita di F, altrimenti si dice che è una estensione infinita.

TEOREMA 14.2. *Se L è una estensione finita di K e K è una estensione finita di F, allora L è una estensione finita di F e*

$$[L : F] = [L : K][K : F]$$

DIMOSTRAZIONE. Un modo per calcolare $dim_F L$ è quello di esibire una base di L su F e contarne gli elementi.

Sia $v_1, ..., v_m$ una base di L su K, e sia inoltre $w_1, ..., w_n$ una base di K su F. Allora l'enunciato del teorema segue dall'osservazione che l'insieme $\{v_i w_j\}$ (dove l'indice i varia fra 1 e m e l'indice j varia fra 1 e n) è una base di L su F costituita da mn elementi.

Infatti, per ogni vettore $v \in L$ possiamo scrivere

$$v = a_1 v_1 + \cdots + a_m v_m$$

con i coefficienti $a_i \in K$. Ma ciascuno degli a_i si può scrivere come

$$a_i = b_{i1} w_1 + \cdots + b_{in} w_n$$

con i coefficienti $b_{ij} \in F$. In conclusione possiamo scrivere

$$v = \sum_{\substack{i = 1, ..., m \\ j = 1, ..., n}} b_{ij} v_i w_j$$

Questo dimostra che gli elementi $v_i w_j$ generano L su F.

D'altra parte se abbiamo l'uguaglianza

$$\sum_{\substack{i = 1, ..., m \\ j = 1, ..., n}} b_{ij} v_i w_j = 0$$

con i coefficienti $b_{ij} \in F$, allora raggruppando i termini possiamo scrivere

$$\sum_{\substack{i = 1, ..., m \\ j = 1, ..., n}} b_{ij} v_i w_j = \sum_{i=1,...,m} (b_{i1} w_1 + \cdots + b_{in} w_n) v_i = 0$$

dove le somme fra parentesi $(b_{i1}w_1+\cdots+b_{in}w_n)$ appartengono a K, e dal fatto che $v_1,...,v_m$ è una base di L su K si deduce che sono tutte uguali a 0, ovvero

$$b_{i1}w_1 + \cdots + b_{in}w_n = 0$$

per ogni $i = 1,...,m$. Visto che $w_1,...,w_m$ è una base di K su F si deduce che i coefficienti b_{ij} che compaiono in queste uguaglianze sono tutti uguali a 0. Questo prova la lineare indipendenza dell'insieme $\{v_iw_j\}$. □

COROLLARIO 14.3. *Se L è una estensione finita di F e $F \subseteq K \subseteq L$ allora K è una estensione finita di F e L è una estensione finita di K. Inoltre $[L:F] = [L:K][K:F]$.*

DIMOSTRAZIONE. Consideriamo L come spazio vettoriale su F. Visto che questo spazio vettoriale ha dimensione finita e che K è un suo sottospazio vettoriale, allora anche K ha dimensione finita su F.

L'altra cosa da dimostrare è che L ha dimensione finita su K, ma questo segue immediatamente dal fatto che una base di L su F è anche un insieme (finito) di generatori di L su K.

Una volta stabilito che le due estensioni $F \subseteq K$ e $K \subseteq L$ sono finite si conclude applicando il Teorema 14.2. □

TEOREMA 14.4. *Dati due campi $F \subseteq K$, un elemento $a \in K$ è algebrico su F se e solo se $F(a)$ è una estensione finita di F.*

DIMOSTRAZIONE. Se $[F(a) : F] = m \in \mathbb{N}$ allora l'insieme $\{1, a, a^2, ..., a^m\}$, visto che contiene $m+1$ elementi, è un insieme di elementi linearmente dipendenti sul campo F, dunque esistono $\gamma_0, \gamma_1, ..., \gamma_m \in F$ non tutti nulli tali che

$$\gamma_m a^m + \cdots + \gamma_1 a + \gamma_0 = 0$$

e allora a è algebrico su F perché è radice del polinomio $\gamma_m x^m + \cdots + \gamma_1 x + \gamma_0 \in F[x]$.

Viceversa se a è algebrico su F sappiamo, per quanto visto nel Paragrafo 1 del Capitolo 13, che $F(a) = F[a] \cong F[x]/(f(x))$ dove $f(x)$ è il polinomio minimo di a su F. Per il Teorema **??** allora il grado $[F(a) : F]$ è finito ed è uguale a *deg* f. □

DEFINIZIONE 14.5. Dati due campi $F \subseteq K$, un elemento $a \in K$ si dice algebrico di grado n su F se $[F(a) : F] = n$, ovvero se il suo polinomio minimo su F ha grado n.

TEOREMA 14.6. *Dati due campi $F \subseteq K$, se $a \in K$ e $b \in K$ sono algebrici su F rispettivamente di grado m e n, allora $a \pm b$, ab e $\frac{a}{b}$ (se $b \neq 0$) sono algebrici su F di grado $\leq mn$.*

DIMOSTRAZIONE. Per prima cosa osserviamo che $[F(a) : F] = m$. Ora b, essendo algebrico su F, a maggior ragione è algebrico su $F(a)$. Sia f il polinomio minimo di b su F: dalle ipotesi sappiamo che *deg* $f = n$.

Il polinomio f potrebbe non essere irriducibile in $F(a)[x]$: in tal caso il polinomio minimo di b su $F(a)$ sarà uno dei fattori irriducibili di f in $F(a)[x]$. Dunque possiamo concludere che il grado di b su $F(a)$ è $\leq n$, ovvero che $[F(a)(b) : F(a)] \leq n$. Per il Teorema 14.2 concludiamo che

$$[F(a)(b) : F] = [F(a)(b) : F(a)][F(a) : F] \leq nm$$

Osserviamo a questo punto che il campo $F(a)(b)$ (possiamo indicarlo anche come $F(a, b)$) è il più piccolo sottocampo di K che contiene F, a e b, dunque in particolare contiene anche $a \pm b$, ab e $\frac{a}{b}$ (se $b \neq 0$).

Tali elementi sono allora algebrici su F, in base al seguente ragionamento: per esempio $F(a+b) \subseteq F(a,b)$, dunque per il Corollario 14.3 sappiamo che $F(a+b)$ ha grado finito $\leq mn$ su F; allora, per il Teorema 14.4, $a+b$ è algebrico su F di grado $\leq mn$.

□

COROLLARIO 14.7. *Dati due campi $F \subseteq K$, gli elementi di K algebrici su F formano un sottocampo di K.*

ESEMPIO 14.8. Per illustrare come si possono utilizzare i teoremi sul grado visti in questa lezione, consideriamo l'elemento $c = \sqrt{2} + \sqrt[3]{2} \in \mathbb{R}$, dimostriamo che è algebrico su $\mathbb{Q}$ di grado 6 e troviamo il suo polinomio minimo.

Osserviamo innanzitutto che il polinomio x^2-2 è irriducibile in $\mathbb{Q}[x]$ (se fosse riducibile, essendo di grado 2, dovrebbe avere una radice in $\mathbb{Q}$; ma allora, visto che conosciamo già due radici, $\sqrt{2}$ e $-\sqrt{2}$, che appartengono a $\mathbb{R}-\mathbb{Q}$, il polinomio avrebbe almeno tre radici reali, assurdo). Dunque per quanto visto nella lezione precedente $\mathbb{Q}[\sqrt{2}] \cong Q[x]/(x^2-2)$ e $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Analogamente si osserva che x^3-2 è irriducibile in $\mathbb{Q}[x]$, dunque $\mathbb{Q}[\sqrt[3]{2}] \cong Q[x]/(x^3-2)$ e $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

Per quanto osservato nella dimostrazione del Teorema 14.6 sappiamo che

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$$

D'altra parte, pensando alla catena di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ deduciamo per il Teorema 14.2 che $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$, cioè 2, divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$.

Analogamente, pensando alla catena di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ deduciamo che 3 divide $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. Dunque deve essere $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Consideriamo ora $c = \sqrt{2} + \sqrt[3]{2}$. Possiamo scrivere:

$$(c - \sqrt{2})^3 = 2$$

e sviluppando i calcoli

$$c^3 + 6c - 2 = \sqrt{2}(3c^2 + 2)$$

Da questa uguaglianza ricaviamo intanto che $\sqrt{2} \in \mathbb{Q}(c)$. Elevando al quadrato entrambi i membri otteniamo poi

$$(c^3 + 6c - 2)^2 = 2(3c^2 + 2)^2$$

Abbiamo dunque trovato che c è radice del polinomio $x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$. Per decidere se questo polinomio è irriducibile, e dunque per decidere se è il polinomio minimo di c su $\mathbb{Q}$, possiamo adesso ricorrere ad una osservazione sui gradi delle estensioni coinvolte. Infatti per il Teorema 14.2 vale

$$[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = [\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}]$$

Ora $\mathbb{Q}(c, \sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ (la dimostrazione delle due inclusioni è immediata), dunque sappiamo che

$$[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = 6$$

Inoltre, visto che abbiamo già osservato che che $\sqrt{2} \in \mathbb{Q}(c)$, vale $[\mathbb{Q}(c, \sqrt{2}) : \mathbb{Q}(c)] = 1$. In conclusione $[\mathbb{Q}(c) : \mathbb{Q}] = 6$, dunque il polinomio minimo di c su $\mathbb{Q}$ ha grado 6, e allora $x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$ è proprio il polinomio minimo.[1]

[1] Come vedete scriviamo 'il polinomio minimo' ma non dimenticate che questo va sempre inteso 'a meno di associati'.

2. Estensioni algebriche

Consideriamo estensioni di campi in cui tutti gli elementi sono algebrici sul campo base.

DEFINIZIONE 14.9. Dati due campi $F \subseteq K$, si dice che K è una estensione algebrica di F se ogni elemento di K è algebrico su F.

OSSERVAZIONE 14.10. Una estensione finita $F \subseteq K$ è algebrica. Infatti dato $a \in K$, possiamo considerare la catena di estensioni $F \subseteq F(a) \subseteq K$ e per il Corollario 14.3 vale che $F(a)$ è una estensione finita di F. Dunque a è algebrico su F per il Teorema 14.4.

Esistono però, come vedremo, estensioni algebriche che non sono finite.

TEOREMA 14.11. *Se L è una estensione algebrica di K e K è una estensione algebrica di F, allora L è una estensione algebrica di F.*

DIMOSTRAZIONE. Sia $u \in L$, vogliamo dimostrare che è algebrico su F. Visto che L è una estensione algebrica di K, sappiamo che u è radice di un polinomio

$$x^n + \gamma_{n-1}x^{n-1} + \cdots + \gamma_1 x + \gamma_0$$

con i coefficienti $\gamma_j \in K$.

Ora, K è algebrico su F e dunque $[F(\gamma_0) : F]$ è finito. Inoltre anche $[F(\gamma_0, \gamma_1) : F]$ è finito: infatti vale che $[F(\gamma_0, \gamma_1) : F(\gamma_0)]$ è finito visto che γ_1 è algebrico su F, e dunque lo è anche su $F(\gamma_0)$. Allora $[F(\gamma_0, \gamma_1) : F]$ è finito per il Teorema 14.2 sulle catene di estensioni.

Procedendo in questo modo in al più n passi si dimostra che $[F(\gamma_0, \gamma_1, ..., \gamma_{n-1}) : F]$ è finito.

Ora il grado $[F(u, \gamma_0, \gamma_1, ..., \gamma_{n-1}) : F(\gamma_0, \gamma_1, ..., \gamma_{n-1})]$ è finito perché u è algebrico su $F(\gamma_0, \gamma_1, ..., \gamma_{n-1})$ (infatti u è radice del polinomio $x^n + \gamma_{n-1}x^{n-1} + \cdots + \gamma_1 x + \gamma_0$ che appartiene a $F(\gamma_0, \gamma_1, ..., \gamma_{n-1})[x]$). Quindi per il Teorema 14.2 sulle catene di estensioni si deduce che $[F(u, \gamma_0, \gamma_1, ..., \gamma_{n-1}) : F]$ è finito. Visto che $F(u) \subseteq F(u, \gamma_0, \gamma_1, ..., \gamma_{n-1})$, per il Corollario 14.3 risulta che $F(u)$ è una estensione finita di F e dunque u è algebrico su F per il Teorema 14.4.

□

Facciamo infine una osservazione nel caso in cui $F = \mathbb{Q}$.

DEFINIZIONE 14.12. Si dice che un numero complesso z è un *numero algebrico* se z è algebrico su $\mathbb{Q}$.

I numeri algebrici formano un sottocampo $\mathcal{A}$ di $\mathbb{C}$, come sappiamo per il Corollario 14.7, e per come è stato definito $\mathcal{A}$ è algebrico su $\mathbb{Q}$. L'Esercizio 14.19 vi chiederà di verificare che $[\mathcal{A} : \mathbb{Q}] = \infty$. Le radici di un polinomio in $\mathcal{A}[x]$ sono ancora numeri algebrici, per una immediata applicazione del Teorema 14.11. Quindi, come conseguenza del Teorema Fondamentale dell'Algebra, osserviamo che ogni polinomio in $\mathcal{A}[x]$ ha una radice in $\mathcal{A}$ e dunque si fattorizza come prodotto di polinomi di grado 1 in $\mathcal{A}[x]$.

3. Esercizi del 02/12/2022

ESERCIZIO 14.13. Determinare $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$, e una base di $\mathbb{Q}(\sqrt[3]{2})$ su $\mathbb{Q}$.

ESERCIZIO 14.14. Determinare in che relazione sono i sottocampi $\mathbb{Q}(\sqrt{6}, \sqrt{7})$ e $\mathbb{Q}(\sqrt{6} - \sqrt{7})$ di $\mathbb{C}$.

Esercizio 14.15. Determinare $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}]$, il polinomio minimo di $\sqrt[3]{2} + i$ su $\mathbb{Q}$, e in che relazione sono $\mathbb{Q}(\sqrt[3]{2}, i)$ e $\mathbb{Q}(\sqrt[3]{2} + i)$.

Esercizio 14.16. Determinare tutti gli omomorfismi di anelli $\varphi : \mathbb{Z} \to F$ dove F è un campo, le possibili immagini e i possibili nuclei.

Esercizio 14.17. Per ogni n in $\{4, 6, 8\}$ determinare se esiste un campo F con n elementi, e se sì costruirne uno e determinare se ne esistono due non isomorfi.

4. Esercizi

Esercizio 14.18. Trovare il polinomio minimo su $\mathbb{Q}$ di $1 + \imath$.

Esercizio 14.19. Dimostrare che $[\mathcal{A} : \mathbb{Q}] = \infty$, dove $\mathcal{A}$ è il campo dei numeri algebrici. [Suggerimento: usare le informazioni che avete sui polinomi irriducibili in $\mathbb{Q}[x]$.]

Esercizio 14.20. Sia $\theta : K \to L$ un omomorfismo fra due campi K e L. Dimostrare che θ è iniettivo. [Suggerimento: ricontrollare tutte le definizioni degli oggetti in gioco.]

Esercizio 14.21. Calcolare il grado di $\mathbb{Q}(\imath, \sqrt{2})$ su $\mathbb{Q}$ e scrivere una base. Trovare il polinomio minimo di $\sqrt{2} + \imath$ su $\mathbb{Q}$, su $\mathbb{Q}(\imath)$, su $\mathbb{Q}(\sqrt{2})$ e su $\mathbb{Q}(\imath\sqrt{2})$.

Esercizio 14.22. Calcolare il grado di $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ su $\mathbb{Q}$ e scrivere una base. Trovare il polinomio minimo di $\sqrt{3} - \sqrt{2}$ su $\mathbb{Q}$ e su $\mathbb{Q}(\sqrt{3})$.

Esercizio 14.23. Calcolare il grado su $\mathbb{Q}$ di $2 + \sqrt{2}$.

Esercizio 14.24. È vero o falso che i polinomi $x^3 - 2$ e $x^3 - 3$ sono irriducibili su $\mathbb{Q}(\imath)$?

Esercizio 14.25. Calcolare $[\mathbb{Q}(\sqrt{3 + 2\sqrt{2}}) : \mathbb{Q}]$.

Esercizio 14.26. Sia $K \subseteq L$ una estensione di campi. Sia $\alpha \in L$ un elemento algebrico su K di grado dispari. Dimostrare che $K(\alpha^2) = K(\alpha)$.

CAPITOLO 15

Approfondimenti sui campi

1. Campi di spezzamento

DEFINIZIONE 15.1. Sia F un campo e sia $f(x) \in F[x]$ un polinomio non nullo. Una estensione finita E di F si dice un campo di spezzamento su F per $f(x)$ se valgono entrambe le seguenti condizioni:

- $f(x)$ si fattorizza in $E[x]$ come prodotto di polinomi di grado 1;
- per ogni campo K tale che $F \subseteq K \subsetneq E$ il polinomio $f(x)$ non si fattorizza come prodotto di polinomi di grado 1 in $K[x]$.

OSSERVAZIONE 15.2. Dunque, con le notazioni della definizione, si può dire che in E si trovano tutte le radici di $f(x)$ e non esiste nessun sottocampo proprio K di E che contiene F e tutte le radici di $f(x)$.

OSSERVAZIONE 15.3. Sia L una estensione di F che contiene tutte le radici di $f(x)$ (in generale esistono molte estensioni con queste caratteristiche, che ne esista almeno una è garantito dal Teorema 13.9), e siano $\alpha_1, ..., \alpha_t$ tali radici. Allora $F(\alpha_1, ..., \alpha_t)$ è un sottocampo di L che è un campo di spezzamento di $f(x)$ su F. Possiamo da questo ricavare che, dato un campo F e un polinomio non nullo $f(x) \in F[x]$, esiste sempre un campo di spezzamento di $f(x)$ su F.

L'osservazione precedente ci permette, dato un campo di spezzamento E, di stimare il grado $[E : F]$.

PROPOSIZIONE 15.4. *Sia F un campo e sia $f(x) \in F[x]$ un polinomio non nullo di grado n. Sia E un campo di spezzamento di $f(x)$ su F. Allora $[E : F] \leq n!$.*

DIMOSTRAZIONE. Siano $\beta_1, ..., \beta_t$ le radici distinte di $f(x)$ in E e dunque $E = F(\beta_1, ..., \beta_t)$. Osserviamo che $[F(\beta_1) : F] \leq n$, visto che il polinomio minimo di β_1 in $F[x]$ è uno dei fattori irriducibili di $f(x)$ e pertanto ha grado $\leq n$. Ora

$$[F(\beta_1, \beta_2) : F] = [F(\beta_1, \beta_2) : F(\beta_1)][F(\beta_1) : F]$$

per il Teorema 14.2. Visto che in $F(\beta_1)[x]$ possiamo scrivere la decomposizione $f(x) = (x - \beta_1)g(x)$, dove $g(x)$ ha grado $n-1$, vale $[F(\beta_1, \beta_2) : F(\beta_1)] \leq n-1$; infatti il polinomio minimo di β_2 su $F(\beta_1)$ è uno dei fattori irriducibili di $g(x)$ in $F(\beta_1)[x]$.

Procedendo in questo modo in n passi si ottiene $[E : F] \leq n!$.

□

Facciamo due esempi, studiando i sottocampi di $\mathbb{C}$ che sono campi di spezzamento dei polinomi $x^3 - 2$ e $x^4 - 2$ su $\mathbb{Q}$.

ESEMPIO 15.5. Il sottocampo di $\mathbb{C}$ che è campo di spezzamento di $x^3 - 2$ su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ dove $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\imath$ è una radice cubica di 1.

Si tratta del più piccolo sottocampo di $\mathbb{C}$ che contiene $\mathbb{Q}$, e le tre radici $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$. Allora tale campo contiene anche ω, e dunque contiene $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Si verifica immediatamente anche l'inclusione opposta, dunque $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ è il campo di spezzamento cercato.

Il grado di $\mathbb{Q}(\sqrt[3]{2}, \omega)$ su $\mathbb{Q}$ è uguale a 6 (cioè 3!, dove 3 è il grado del polinomio $x^3 - 2$). Infatti per calcolare il grado si considera la catena di estensioni

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$$

L'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ha grado 3, come sappiamo visto che $x^3 - 2$ è irriducibile in $\mathbb{Q}[x]$ (e comunque avevamo già considerato questo esempio nel Paragrafo 1 del Capitolo 13). L'estensione $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ ha grado 2, visto che il polinomio minimo di ω su $\mathbb{Q}(\sqrt[3]{2})[x]$ è x^2+x+1. Quest'ultima affermazione si motiva nel seguente modo: osserviamo innanzitutto che $x^3-1 = (x-1)(x^2+x+1)$, dunque ω è radice di x^2+x+1; questo polinomio è irriducibile in $\mathbb{Q}(\sqrt[3]{2})[x]$, perché se fosse riducibile avrebbe delle radici in $\mathbb{Q}(\sqrt[3]{2})$, mentre sappiamo che le sue radici sono ω e ω^2, ovvero dei numeri complessi non reali.

Esempio 15.6. Il sottocampo di $\mathbb{C}$ che è campo di spezzamento di $x^4 - 2$ su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \imath\sqrt[4]{2}, -\imath\sqrt[4]{2})$, ossia il più piccolo sottocampo che contiene $\mathbb{Q}$ e le quattro radici del polinomio.

Si osserva subito che tale campo coincide con $\mathbb{Q}(\sqrt[4]{2}, \imath)$. Il grado di $\mathbb{Q}(\sqrt[4]{2}, \imath)$ su $\mathbb{Q}$ è uguale a 8 (è dunque strettamente minore di 4!, dove 4 è il grado del polinomio $x^4 - 2$). Infatti considerando la catena di estensioni

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, \imath)$$

si osserva che $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ ha grado 4, visto che $x^4 - 2$ è irriducibile in $\mathbb{Q}[x]$, e che $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, \imath)$ ha grado 2, dato che il polinomio minimo di $\imath$ su $\mathbb{Q}(\sqrt[4]{2})$ è $x^2 + 1$.

In generale, dato un campo F ed un polinomio non nullo $f(x) \in F[x]$, si possono costruire vari campi di spezzamento per $f(x)$ su F, ma questi campi di spezzamento sono tutti isomorfi fra loro. Concludiamo il paragrafo riportando, per vostra informazione, l'enunciato preciso del teorema in questione, che dimostreremo l'anno prossimo nel corso di Algebra 1.

Teorema 15.7. *Sia F un campo e siano E ed E' due campi di spezzamento di un polinomio non nullo $f(x) \in F[x]$. Allora esiste un isomorfismo $\phi' : E \to E'$ tale che ϕ' ristretto a F è l'identità.*

Osservazione 15.8. Dal teorema precedente segue che, dato un campo F, il grado su F di un campo di spezzamento di un polinomio non nullo $f(x) \in F[x]$ è unicamente determinato da F e $f(x)$, e non dipende dal particolare campo di spezzamento che stiamo considerando.

2. La caratteristica di un campo

Studiamo adesso i campi da un altro punto di vista, ossia studiando se contengono un sottoanello isomorfo a $\mathbb{Z}$ o no.

Osserviamo innanzitutto che, dato un campo F, c'è un solo omomorfismo di anelli $\phi : \mathbb{Z} \to F$, determinato dalla condizione $\phi(1) = 1$.[1]

Visto che $\mathbb{Z}$ è un anello a ideali principali, vale che $Ker\ \phi = (d)$, per un intero $d \geq 0$. Abbiamo due casi:

[1]Come già specificato in precedenza, in questo corso stiamo considerando esclusivamente anelli con unità, dunque utilizziamo la definizione di omomorfismo fra anelli con unità.

(1) $d = 0$ dunque $Ker\ \phi = (0)$; allora $\mathrm{Imm}\,\phi \cong \mathbb{Z}$ ossia in F abbiamo un sottoanello isomorfo a $\mathbb{Z}$, che chiameremo ancora $\mathbb{Z}$ per non appesantire la notazione. Inoltre, visto che F è un campo, e deve dunque contenere gli inversi di tutti gli elementi diversi da 0, possiamo concludere che in F c'è un sottocampo isomorfo a $\mathbb{Q}$, che chiameremo ancora $\mathbb{Q}$. Si dice in questo caso che F è un *campo di caratteristica 0*.

(2) d è un numero primo. Infatti se d non fosse primo, potremmo scrivere $d = rs$ con r, s interi e $1 < s < d$, $1 < r < d$. Allora $\phi(r)$ e $\phi(s)$ sarebbero elementi diversi da 0 in K ma $\phi(r)\phi(s) = \phi(rs) = \phi(d) = 0$ e questo è assurdo perché nel campo K non ci sono divisori di 0 non banali. Dunque $d = p$ primo, per cui $Ker\ \phi = (p)$ e per il primo teorema di omomorfismo di anelli $\mathrm{Imm}\,\phi \cong \mathbb{Z}/(p) \cong \mathbb{Z}_p$, dunque F contiene un sottocampo isomorfo a $\mathbb{Z}_p$, che chiameremo ancora $\mathbb{Z}_p$. Si dice in questo caso che F è un *campo di caratteristica p*.

Allora in F vale che $1 + \cdots + 1$ (p addendi) è uguale a 0. Infatti

$$1 + \cdots + 1 = \phi(1) + \cdots + \phi(1) = \phi(1 + \cdots + 1) = \phi(p) = 0$$

Consideriamo adesso F come spazio vettoriale su $\mathbb{Z}_p$ e osserviamo che per ogni $v \in F$ la somma $v + \cdots + v$ (p addendi) è uguale a 0. Infatti, per le proprietà della moltiplicazione per scalare, $v + \cdots + v = (1 + \cdots + 1)v = 0v = 0$.

3. Esistono infiniti campi finiti....

3.1. L'omomorfismo di Frobenius per i campi a caratteristica p. Cominciamo presentando un importante omomorfismo.

TEOREMA 15.9 (L'omomorfismo di Frobenius[2]). *Sia p un numero primo, e sia K un campo di caratteristica p. La funzione $\mathcal{F} : K \to K$, definita da $\mathcal{F}(a) = a^p$ per ogni $a \in K$, è un omomorfismo iniettivo.*

DIMOSTRAZIONE. Stabiliamo innanzitutto che $\mathcal{F}$ è un omomorfismo. La verifica che $\mathcal{F}(1) = 1$ e che per ogni $a, b \in K$ vale $\mathcal{F}(ab) = \mathcal{F}(a)\,\mathcal{F}(b)$ è immediata.

La verifica più interessante è quella relativa alla somma: bisogna dimostrare che per ogni $a, b \in K$ vale $\mathcal{F}(a + b) = \mathcal{F}(a) + \mathcal{F}(b)$, ossia $(a + b)^p = a^p + b^p$.

Ci rendiamo conto di aver in sostanza già affrontato questo problema, nella seconda dimostrazione del piccolo teorema di Fermat (Capitolo 3, Paragrafo 3). L'uguaglianza $(a + b)^p = a^p + b^p$ segue dal fatto che si può sviluppare il membro di sinistra utilizzando il teorema del binomio di Newton, e poi si utilizza il fatto che tutti i coefficienti $\binom{p}{i}$, con $1 \le i \le p - 1$, sono multipli di p e dunque sono uguali a 0 in un campo di caratteristica p.

Per quel che riguarda l'iniettività di $\mathcal{F}$, osserviamo che Ker $\mathcal{F}$ è un ideale proprio di K (non può essere Ker $\mathcal{F} = K$ perché $\mathcal{F}(1) = 1$). Visto che K è un campo, l'unico ideale proprio è (0).

□

OSSERVAZIONE 15.10. Come immediata conseguenza del teorema precedente, anche le potenze $\mathcal{F}^j$ (con j intero positivo) dell'omomorfismo di Frobenius sono omomorfismi iniettivi.

Nel prossimo paragrafo (e nel corso di Algebra 1 !) tornerà molto utile la seguente osservazione.

[2]Ferdinand Georg Frobenius, matematico tedesco, 1849-1917.

TEOREMA 15.11. *Sia K un campo, e sia $\psi : K \to K$ un omomorfismo. Allora l'insieme*

$$Fix_\psi = \{k \in K \mid \psi(k) = k\}$$

degli elementi di K lasciati fissi da ψ è un sottocampo di K.

DIMOSTRAZIONE. Dimostriamo innanzitutto che Fix_ψ è un sottoanello di K. Per prima cosa osserviamo che $0 \in Fix_\psi$. Inoltre, se $r \in Fix_\psi$ allora

$$\psi(-r) = -\psi(r) = -r$$

dunque anche l'opposto di r appartiene a Fix_ψ.

Consideriamo ora $r, s \in Fix_\psi$. Vale che

$$\psi(r+s) = \psi(r) + \psi(s) = r + s$$

dunque $r+s \in Fix_\psi$. Abbiamo fin qui dimostrato che Fix_ψ è un sottogruppo rispetto alla somma.

Analogamente si dimostra che se $r, s \in Fix_\psi$ allora il prodotto rs appartiene a Fix_ψ. Inoltre $1 \in Fix_\psi$. Dunque Fix_ψ è un sottoanello di K. L'ultima cosa che resta da dimostrare è l'esistenza in Fix_ψ dell'inverso moltiplicativo di un elemento non zero. Sia $r \in Fix_\psi$ diverso da 0; allora

$$\psi(r^{-1}) = \psi(r)^{-1} = r^{-1}$$

e dunque $r^{-1} \in Fix_\psi$.

□

3.2. Cardinalità dei campi finiti, ed un enunciato di esistenza. Consideriamo un campo finito L (ossia un campo con un numero finito di elementi).

La prima osservazione che possiamo fare è che L non può avere caratteristica 0: in tal caso infatti conterrebbe un sottocampo isomorfo a $\mathbb{Q}$ e non sarebbe finito. Dunque la caratteristica di L è un numero primo p, e L contiene un sottocampo isomorfo a $\mathbb{Z}_p$ (vedi il Paragrafo 2).

Inoltre il grado di L su $\mathbb{Z}_p$ deve essere finito, diciamo $n \in \mathbb{N} - \{0\}$, altrimenti L sarebbe uno spazio vettoriale di dimensione infinita e dunque avrebbe infiniti elementi.

Ora, la cardinalità di uno spazio vettoriale di dimensione n sul campo $\mathbb{Z}_p$ è p^n (considerate una base $v_1, ..., v_n$: un vettore dello spazio è una combinazione lineare $a_1v_1 + \cdots + a_nv_n$ dove i coefficienti a_i appartengono a $\mathbb{Z}_p$, dunque abbiamo p scelte per ogni coefficiente).

Abbiamo ottenuto una prima interessante osservazione, che riassumiamo nella seguente proposizione.

PROPOSIZIONE 15.12. *La cardinalità di un campo finito è un intero della forma p^n per un certo numero primo p ed un certo intero positivo n.*

Ora consideriamo il gruppo moltiplicativo $L^* = L - \{0\}$. Visto che ha cardinalità $p^n - 1$, per il Corollario 4.26 del Teorema di Lagrange vale che, per ogni $g \in L^*$,

$$g^{p^n-1} = 1$$

Considerando anche lo 0, possiamo scrivere che per ogni $g \in L$ vale

$$g^{p^n} = g$$

Dunque il polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ ha esattamente p^n soluzioni in L: più precisamente tutti gli elementi di L sono radici di $x^{p^n} - x$ e $x^{p^n} - x$ si fattorizza come prodotto di fattori di grado 1 in $L[x]$. Pertanto L è un campo di spezzamento di $x^{p^n} - x$ su $\mathbb{Z}_p$.

Mostriamo adesso che avere cardinalità p^n non è solo una condizione necessaria, ma anche sufficiente per l'esistenza di un campo finito:

TEOREMA 15.13. *Ogni campo finito ha cardinalità p^n, dove p è un numero primo e n un intero positivo. Inoltre, per ogni numero primo p e per ogni intero positivo n esiste un campo finito di cardinalità p^n.*

DIMOSTRAZIONE. L'unica cosa che resta da dimostrare è l'esistenza di un campo con p^n elementi. Consideriamo un campo di spezzamento R di $x^{p^n} - x$ su $\mathbb{Z}_p$ (un tale campo esiste, vedi Osservazione 15.3). Il campo R è un campo di caratteristica p ed ha dimensione finita su $\mathbb{Z}_p$ (vedi Proposizione 15.4), dunque è un campo finito.

Sia $L = \{r \in R \mid \mathcal{F}^n r = r\}$ dove $\mathcal{F}$ è l'omomorfismo di Frobenius. Come sappiamo dal Teorema 15.11, l'insieme L, ovvero l'insieme dei punti fissi dell'omomorfismo $\mathcal{F}^n$, è un sottocampo di R; ricordando la definizione dell'omomorfismo di Frobenius, si osserva anche che gli elementi di L sono le radici di $x^{p^n} - x$. Tali radici sono p^n, perché sono tutte distinte fra loro (la derivata[3] di $x^{p^n} - x$ è -1, dato che R ha caratteristica p, e non ha dunque radici in comune con $x^{p^n} - x$).

Allora L è un campo con p^n elementi (e alla fine di questo ragionamento possiamo fra l'altro anche concludere che coincide con R).

□

OSSERVAZIONE 15.14. Alla luce del Teorema 15.7, dato che tutti i campi finiti con p^n elementi sono isomorfi fra loro, è molto diffusa la seguente notazione: quando ci si riferisce ad un campo con p^n elementi, e lo si considera a meno di isomorfismo, tale campo viene indicato con $\mathbb{F}_{p^n}$. In questo corso la utilizzeremo solo marginalmente perché non abbiamo dimostrato il Teorema 15.7.

OSSERVAZIONE 15.15. Abbiamo visto che se un campo L è finito allora ha caratteristica p. È bene ricordare che il viceversa non è vero: esistono campi a caratteristica p con infiniti elementi. Per esempio per ogni primo p si può considerare il campo delle funzioni razionali:

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0 \right\}$$

4. Esercizi

ESERCIZIO 15.16. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^4 + 1$.

ESERCIZIO 15.17. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^5 - 1$.

ESERCIZIO 15.18. Dimostrare che il sottocampo di $\mathbb{C}$ che è campo di spezzamento su $\mathbb{Q}$ di $x^2 - 3$ è campo di spezzamento su $\mathbb{Q}$ anche di $x^2 - 2x - 2$.

ESERCIZIO 15.19. Dimostrare che il sottocampo K di $\mathbb{C}$ che è campo di spezzamento su $\mathbb{Q}$ di $(x^2 - 2x - 2)(x^2 + 1)$ è campo di spezzamento su $\mathbb{Q}$ anche di $x^5 - 3x^3 + x^2 - 3$. Trovare il grado $[K : \mathbb{Q}]$.

ESERCIZIO 15.20. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^4 + 2x^3 - 8x^2 - 6x - 1$.

ESERCIZIO 15.21. Trovare il grado su $\mathbb{Q}$ del campo di spezzamento su $\mathbb{Q}$ di $x^4 - x^2 - 2$.

ESERCIZIO 15.22. Trovare un campo di spezzamento su $\mathbb{Z}_2$ di per il polinomio $x^3 + x + 1$.

[3]Stiamo usando il *criterio della derivata*, che abbiamo enunciato in classe: studiatelo nell'estratto dal libro di Herstein a disposizione su e-learning.

ESERCIZIO 15.23. Trovare un polinomio $f(x) \in \mathbb{Z}_2[x]$ tale che un suo campo di spezzamento su $\mathbb{Z}_2$ abbia 16 elementi.

[Traccia: trovate un polinomio irriducibile $f(x)$ di grado 4 in $\mathbb{Z}_2[x]$. Allora $K = \mathbb{Z}_2[x]/(f(x))$ è un campo di 16 elementi. In particolare in K i polinomi $f(x)$ e $x^{2^4} - x$ hanno una radice in comune, allora non possono essere primi fra loro in $\mathbb{Z}_2[x]$. Visto che $f(x)$ è irriducibile in $\mathbb{Z}_2[x]$, deve essere $f(x)|x^{2^4} - x$. Dunque in K, che contiene tutte le radici di $x^{2^4} - x$, ci sono tutte le radici di $f(x)$...]

ESERCIZIO 15.24. Fattorizzare $x^{16} - x$ come prodotto di polinomi irriducibili in $\mathbb{Z}_2[x]$.

CAPITOLO 16

Un teorema sui sottogruppi moltiplicativi dei campi

1. Un sottogruppo moltiplicativo finito di un campo è ciclico

TEOREMA 16.1. *Sia K un campo e sia G un sottogruppo (moltiplicativo) di K^* con un numero finito di elementi. Allora G è un gruppo ciclico.*

DIMOSTRAZIONE. Sia $|G| = n$. Se $n = 1$ l'enunciato è banale. Sia dunque $n > 1$. Come sappiamo dall'Esercizio 4.38 (che abbiamo poi riletto sotto nuova luce quando abbiamo studiato i gruppi ciclici), per ogni intero positivo n vale:

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

dove i d sono interi positivi. Poniamo ora, per ogni intero positivo d che divide n,

$$X_d = \{a \in G \mid o(a) = d\}$$

e osserviamo che vale

$$\sum_{d|n} |X_d| = n$$

dove i d sono come sopra interi positivi. Se G non fosse ciclico, allora $|X_n| = 0$, dunque confrontando le due formule si nota che dovrebbe esistere un intero positivo d che divide n (ed è $< n$) tale che $|X_d| > \phi(d) \geq 1$.

Sia ora $g \in X_d$. Vale che $o(g) = d$ e in particolare tutti gli elementi di (g) (il sottogruppo ciclico di G generato da g) sono radici di $x^d - 1$. Come sappiamo, in (g) ci sono esattamente $\phi(d)$ elementi di ordine d. Quindi poiché $|X_d| > \phi(d)$, esiste in X_d un elemento h che non appartiene a (g). Allora anche h è una radice di $x^d - 1$, che dunque avrebbe $d + 1$ radici in K. Questo è assurdo perché contraddice il Teorema 13.7.

□

COROLLARIO 16.2. *Dato un campo finito K con p^n elementi (dove p è primo e n è un intero positivo), sia α un generatore del gruppo ciclico K^*. Se chiamiamo $f(x)$ il polinomio minimo di α su $\mathbb{Z}_p[x]$ vale che deg $f = n$. Dunque per ogni numero primo p e per ogni intero positivo n esiste in $\mathbb{Z}_p[x]$ un polinomio irriducibile di grado n.*

DIMOSTRAZIONE. Si tratta di una immediata conseguenza del teorema precedente: il campo $\mathbb{Z}_p(\alpha)$ coincide con K perché $\mathbb{Z}_p(\alpha)$ è un sottoinsieme di K che contiene 0 e le potenze di α, ossia contiene tutti gli elementi di K. Dunque $\mathbb{Z}_p(\alpha)$ è una estensione di grado n su $\mathbb{Z}_p$. Poiché $\mathbb{Z}_p(\alpha)$ è isomorfo a $\mathbb{Z}_p[x]/(f(x))$, segue che *deg* $f = n$. □

CAPITOLO 17

Approfondimenti sui campi finiti

1. Campi di spezzamento finiti

TEOREMA 17.1. *Dato un polinomio irriducibile $f(x) \in \mathbb{Z}_p[x]$ di grado n, il campo $K = \mathbb{Z}_p[x]/(f(x))$ è un campo di spezzamento per $f(x)$ su $\mathbb{Z}_p$.*

DIMOSTRAZIONE. Consideriamo il campo $K = \mathbb{Z}_p[x]/(f(x))$. Come sappiamo si tratta di un campo con p^n elementi. In tale campo il polinomio $f(x)$ ha una radice α, ma tale radice è anche radice di $x^{p^n} - x$, dato che ogni elemento di $\mathbb{F}_{p^n}$ è radice di tale polinomio, per quanto visto nel Paragrafo 3.2 del Capitolo 15. Visto che $f(x)$ è irriducibile, è il polinomio minimo di α, e dunque $f(x)|x^{p^n} - x$. Allora le radici di $f(x)$ sono in particolare radici di $x^{p^n} - x$: dunque si trovano tutte in K perché $K \cong \mathbb{F}_{p^n}$ contiene tutte le radici di $x^{p^n} - x$. La dimostrazione si conclude osservando che nessun sottocampo proprio di K può contenere tutte le radici di $f(x)$, per ragioni di grado (se un sottocampo contiene α, contiene $\mathbb{Z}_p(\alpha)$ che ha grado n su $\mathbb{Z}_p$, dunque coincide con K, che ha anch'esso grado n su $\mathbb{Z}_p$).

□

TEOREMA 17.2. *Dato un numero primo p ed un intero positivo n, dimostrare che $x^{p^n} - x$ è il prodotto di tutti i polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado d divisore di n.*

DIMOSTRAZIONE. Consideriamo un polinomio $q(x)$ irriducibile in $\mathbb{Z}_p[x]$ e di grado d con d divisore di n. Dobbiamo dimostrare che $q(x)$ divide $x^{p^n} - x$. Consideriamo il campo $L = \mathbb{Z}_p[x]/(q(x))$: si tratta di un campo con p^d elementi. Come abbiamo visto nel Paragrafo 3.2 del Capitolo 15, ogni elemento y di L soddisfa $y^{p^d} = y$; inoltre in L c'è una radice α di $q(x)$. Allora per tale α vale

$$\alpha^{p^d} = \alpha$$

Visto che $d|n$ esiste un intero s tale che $ds = n$. Osserviamo allora che

$$\alpha^{p^n} = (\alpha^{p^d})^{p^{(s-1)d}} = \alpha^{p^{(s-1)d}}$$

A partire da questa osservazione si dimostra facilmente per induzione su s che $\alpha^{p^n} = \alpha$. Allora α è una radice del polinomio $x^{p^n} - x$. Dunque $q(x)$ e $x^{p^n} - x$ hanno in comune la radice α in L.

Dato che $q(x)$ è irriducibile, è il polinomio minimo di α su $\mathbb{Z}_p[x]$, dunque deve valere $q(x)|x^{p^n} - x$, come volevamo dimostrare.

Dimostriamo adesso il viceversa, ossia che se $f(x)$ è un polinomio irriducibile che divide $x^{p^n} - x$ allora il grado d di $f(x)$ divide n. Consideriamo un campo L con p^n elementi. Come sappiamo L è un campo di spezzamento per il polinomio $x^{p^n} - x$. Dato che $f(x)$ divide $x^{p^n} - x$, fra gli elementi di L ci sono in particolare tutte le radici di $f(x)$. Sia β una tale radice. Il polinomio minimo di β su $\mathbb{Z}_p$ è proprio $f(x)$ visto che $f(x)$ è irriducibile. Allora il campo $K' = \mathbb{Z}_p(\beta)$ è isomorfo a $K = \mathbb{Z}_p[x]/(f(x))$, pertanto K' è

un sottocampo di L con p^d elementi. Dunque K' ha grado d su $\mathbb{Z}_p$ ed è sottocampo di L che ha grado n su $\mathbb{Z}_p$. Per il Teorema 14.2 segue che $d|n$ come volevamo dimostrare.

Dunque nella fattorizzazione in irriducibili di $x^{p^n} - x$ in $\mathbb{Z}_p[x]$ i fattori irriducibili che compaiono sono, a meno di associati, tutti e soli i polinomi irriducibili monici di grado d che divide n. Poiché $x^{p^n} - x$ non ha radici multiple, ciascun fattore irriducibile compare con esponente 1. A questo punto, considerando il coefficiente del termine di grado massimo, si osserva che il prodotto di tutti i polinomi irriducibili monici di grado d che divide n è esattamente uguale a $x^{p^n} - x$ (non "a meno di associati").

□

2. Esercizi del 14/12/2022 e del 15/12/2022

Esercizio 17.3. Elencare tutti i polinomi monici irriducibili fino al grado 4 in $\mathbb{Z}_2[x]$ e in $\mathbb{Z}_3[x]$.

Esercizio 17.4. Dato p primo, utilizzare il criterio di Eisenstein per dimostrare che $x^{p-1} + x^{p-2} + \cdots + x + 1$ è irriducibile in $\mathbb{Q}[x]$. [Utilizzare il seguente criterio di cambio di variabile: dati K campo e $f(x) \in K[x]$, allora $f(x)$ è irriducibile in $K[x]$ se e solo se lo è $f(ax + b)$, con $a, b \in K$, $a \neq 0$.]

Esercizio 17.5. Dato $n \in \mathbb{N}$, $n \geq 1$, una *radice primitiva n-esima dell'unità* è un numero complesso ζ tale che $\zeta^n = 1$ ma $\zeta^k \neq 1$ per ogni $1 \leq k < n$. Sia $\Phi_n(x) := \prod_{i=1}^{d}(x - \zeta^{(i)})$ dove $\zeta^{(1)}, \zeta^{(2)}, \ldots, \zeta^{(d)}$ sono le radici primitive n-esime dell'unità.

(1) Mostrare che $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
(2) Mostrare che $\Phi_n(x) \in \mathbb{Z}[x]$.
(3) Calcolare esplicitamente $\Phi_n(x)$ per $1 \leq n \leq 6$.

Esercizio 17.6. Sia $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$. Determinare il polinomio minimo di α su $\mathbb{Q}$ e quello di α su $\mathbb{Q}(\sqrt{2})$.

Esercizio 17.7. Sia $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Determinare il campo di spezzamento K di $f(x)$ su $\mathbb{Q}$, e calcolare $[K : \mathbb{Q}]$.

Esercizio 17.8. Calcolare $\Phi_8(x)$ (vedi Esercizio 17.5 per la definizione) e fattorizzarlo in $\mathbb{Q}[x]$ e in $\mathbb{Z}_{41}[x]$.

Esercizio 17.9. Sia F un campo con 8 elementi. Determinare la fattorizzazione in irriducibili in $F[x]$ dei polinomi $\Phi_3(x)$ e $\Phi_7(x)$. Dedurre che $\Phi_7(x)$ non è irriducibile in $\mathbb{Z}_2[x]$.

Esercizio 17.10. Dato un campo finito F, mostrare che esiste un polinomio in $F[x]$ che non ha radici in F.

3. Esercizi

Esercizio 17.11. Sia p un numero primo e siano $f(x)$ e $g(x)$ due polinomi irriducibili di grado n intero positivo in $\mathbb{Z}_p[x]$. Sia $K = \mathbb{Z}_p[x]/(f(x))$. Come sappiamo, K è un campo di spezzamento di $f(x)$ su $\mathbb{Z}_p$. Dimostrare che K è anche un campo di spezzamento di $g(x)$ su $\mathbb{Z}_p$.

Esercizio 17.12. Dato un numero primo p e un polinomio irriducibile $g(x) \in \mathbb{Z}_p[x]$ di grado n intero positivo, dimostrare che in ogni campo L di cardinalità p^m, con m multiplo di n, il polinomio $g(x)$ ha esattamente n radici distinte.

Esercizio 17.13. Dato un numero primo p e due interi positivi m, n, sia L un campo di cardinalità p^n e sia E un campo con cardinalità p^m. Dimostrare che E contiene un sottocampo isomorfo a L se e solo se $n|m$.

Esercizio 17.14. Dato un numero primo p, consideriamo il polinomio $f(x) \in \mathbb{Z}_p[x]$ che si fattorizza in $\mathbb{Z}_p[x]$ nel seguente modo:

$$f(x) = f_1(x)^{\alpha_1} f_2(x)^{\alpha_2} \cdots f_m(x)^{\alpha_m}$$

dove i polinomi $f_i(x)$ sono irriducibili e gli α_i sono interi positivi. Dimostrare che un campo L con p^n elementi è un campo di spezzamento di $f(x)$ su $\mathbb{Z}_p$ se e solo se n è il minimo comune multiplo dei gradi dei polinomi $f_i(x)$.

Esercizio 17.15. Sia $f(x) \in \mathbb{Z}_p[x]$ un polinomio irriducibile di grado d. Sia K una estensione di $\mathbb{Z}_p$ in cui $f(x)$ ha una radice α. Dimostrare, utilizzando l'omomorfismo di Frobenius, che le radici di $f(x)$ in K sono $\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{d-1}}$ (e sono d radici distinte).

Esercizio 17.16. Dimostrare che nel campo $\mathbb{Z}_2[x]/(x^3+x^2+1)$ le radici di x^3+x^2+1 sono $\alpha = x + (x^3+x^2+1)$, α^2 e $\alpha^2+\alpha+1$.

Esercizio 17.17. Dimostrare che nel campo $\mathbb{Z}_5[x]/(x^3+x^2+1)$ le radici di x^3+x^2+1 sono $\alpha = x + (x^3+x^2+1)$, $2\alpha^2+3\alpha$ e $3\alpha^2+\alpha+4$.

Esercizio 17.18. Si consideri nel campo $\mathbb{Z}_7[x]/(x^3-2)$ l'elemento $\alpha = x + (x^3-2)$. Si descrivano, in funzione di α, le tre radici di x^3-2 presenti nel campo.

Esercizio 17.19. Dimostrare che per ogni primo p e per ogni intero positivo n, se L ed E sono due estensioni di Z_p con p^n elementi, allora esiste un isomorfismo fra L ed E che lascia fissi gli elementi di $\mathbb{Z}_p$. [Si tratta dunque di dimostrare il Teorema 15.7, che in questo corso non abbiamo dimostrato, in questo contesto particolare di campi finiti.]

Esercizio 17.20. (difficile) Dimostrare che il polinomio x^4+1 è riducibile in $\mathbb{Z}_p[x]$ per ogni numero primo p.

Esercizio 17.21. (difficile) Dato un numero primo p, un intero positivo n, e un campo L con p^n elementi, dimostrare che esistono $\frac{\phi(p^n-1)}{n}$ polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado n tali che, se chiamiamo $\mathcal{R}$ l'insieme dato dall'unione delle loro radici in L, vale che $\mathcal{R}$ coincide con l'insieme dei generatori del gruppo moltiplicativo L^*.

[La ϕ che compare è la funzione di Eulero. Possiamo notare che questo esercizio ci offre un regalo: ci permette di concludere che il numero $\frac{\phi(p^n-1)}{n}$ è intero, per ogni primo p e per ogni intero positivo n.]

Esercizio 17.22 (difficile). Dato un campo finito K, dimostrare che se un polinomio $f(x) \in K[x]$ è irriducibile in $K[x]$ allora non ha radici multiple in una estensione di K.

Trovare un campo L di caratteristica p e un polinomio $f(x) \in L[x]$ che è irriducibile in $L[x]$ e ha radici multiple in una estensione di L.

CAPITOLO 18

Due teoremi fondamentali - capitolo facoltativo

Questa sarebbe stata l'ultima lezione del corso, ma non si è potuta tenere per una circostanza sfortunata. La abbiamo lasciata comunque nelle dispense, come approfondimento facoltativo.

1. Polinomi simmetrici

Fissiamo un intero positivo $n \in \mathbb{N}$. Sia F un campo, e consideriamo l'anello $F[x_1, x_2, \dots, x_n]$ dei polinomi nelle variabili $x_1, x_2, \dots, x_n$. Dati $\sigma \in S_n$ e $f = f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ poniamo

$$\sigma \cdot f = \sigma \cdot f(x_1, x_2, \dots, x_n) := f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

Ad esempio se $n = 3$, $f(x_1, x_2, x_3) = (x_1 - x_2)^3 \in F[x_1, x_2, x_3]$ e $\sigma = (1, 3) \in S_3$, allora $\sigma \cdot f = (x_3 - x_2)^3$.

Poniamo

$$\mathrm{Sym}[X_n] = \mathrm{Sym}_F[X_n] := \{f \in F[x_1, x_2, \dots, x_n] \mid \sigma \cdot f = f \text{ per ogni } \sigma \in S_n\}$$

Gli elementi di $\mathrm{Sym}[X_n]$ sono detti *polinomi simmetrici*: sono semplicemente i polinomi invarianti per permutazioni delle variabili.

Ad esempio $x_1 + x_2 + \cdots + x_n$ è un polinomio simmetrico, mentre $x_1 - x_2$ non lo è.

Esercizio 18.1. Verificare che $\mathrm{Sym}[X_n]$ è un sottoanello di $F[x_1, x_2, \dots, x_n]$.

Introduciamo una famiglia fondamentale di polinomi simmetrici.

Definizione 18.2. Il *polinomio elementare simmetrico* di grado $d \in \mathbb{N}$ nelle n variabili $x_1, x_2, \dots, x_n$ è definito come

$$e_0(x_1, x_2, \dots, x_n) := 1 \quad \text{se } d = 0,$$
$$e_d(x_1, x_2, \dots, x_n) := \sum_{1 \le i_1 < i_2 < \cdots < i_d \le n} x_{i_1} x_{i_2} \cdots x_{i_d} \quad \text{se } 1 \le d \le n.$$

Ad esempio

$$e_3(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4,$$
$$e_3(x_1, x_2, x_3) = x_1x_2x_3,$$
$$e_3(x_1, x_2) = 0.$$

I polinomi simmetrici elementari mettono in relazione le radici di un polinomio con i suoi coefficienti.

Esercizio 18.3. Sia A un anello commutativo, e sia

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x].$$

Supponiamo che

$$f(x) = \prod_{i=1}^{n} (x - r_i)$$

con $r_i \in A$ per ogni $i = 1, 2, \ldots, n$. Mostrare che per ogni $i = 1, 2, \ldots, n$

$$a_{n-i} = (-1)^i e_i(r_1, r_2, \ldots, r_n).$$

Il seguente teorema è anche noto come *teorema fondamentale dei polinomi simmetrici*.

TEOREMA 18.4. *C'è un isomorfismo di anelli*

$$\mathrm{Sym}[X_n] \cong F[e_1, e_2, \ldots, e_n]$$

dove $e_i := e_i(x_1, \ldots, x_n)$ *per* $i = 1, 2, \ldots n$.

OSSERVAZIONE 18.5. In altre parole il teorema dice che ogni polinomio simmetrico si scrive in modo unico come polinomio negli e_i a coefficienti in F.

DIMOSTRAZIONE. Dato $f \in \mathrm{Sym}[X_n]$, l'idea è di trovare algoritmicamente il polinomio g tale che $f = g(e_1, e_2, \ldots, e_n)$, cancellando il "leading term" di f sottraendo un opportuno monomio nelle e_i, il cui "leading term" coincida con quello di f. E poi procedere iterativamente. Abbiamo bisogno di un po' di notazione.

Dato un monomio $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, scriviamo $\alpha := (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$ e poniamo

$$x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Inoltre poniamo $|\alpha| := \sum_{i=1}^n \alpha_i$. Ora ordiniamo i monomi (monici!) di $F[x_1, x_2, \ldots, x_n]$ con il *degree lexicographic order* dato da $x_1 > x_2 > \cdots > x_n$, ossia dati $\alpha, \beta \in \mathbb{N}^n$ poniamo $x^\alpha < x^\beta$ se $|\alpha| < |\beta|$ oppure se $|\alpha| = |\beta|$ e $\alpha < \beta$ nell'ordine lessicografico di $\mathbb{N}^n$.

Ad esempio $x_1^4 < x_1^3 x_3^2 < x_1^3 x_2 x_3 < x_1^4 x_3$. Il *leading term* di un polinomio sarà semplicemente il suo termine (ossia monomio non necessariamente monico) non nullo con il monomio (monico) più grande. Ad esempio il leading term di e_i è $x_1 x_2 \cdots x_i$.

Osserviamo alcune importanti proprietà di questo ordine sui monomi.

ESERCIZIO 18.6. Il degree lexicographic order sui monomi di $F[x_1, x_2, \ldots, x_n]$ soddisfa le seguenti proprietà:

(1) per ogni x^α, x^β o $x^\alpha \leq x^\beta$ oppure $x^\alpha \geq x^\beta$ (ossia l'ordine sui mononi è totale);
(2) $x^\alpha < x^\beta$ se e solo se $x^\alpha x^\gamma < x^\beta x^\gamma$ per ogni $\alpha, \beta, \gamma \in \mathbb{N}^n$;
(3) per ogni x^α c'è un numero finito di x^β con $x^\beta < x^\alpha$.

Dalle proprietà dell'esercizio precedente è facile dedurre che il leading term del prodotto di due polinomi è il prodotto dei rispettivi leading terms: **esercizio**.

La prima osservazione è che siccome f è simmetrico, il suo leading term cx^α, con $0 \neq c \in F$ e $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, deve essere tale che $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. Infatti, se $\alpha_i < \alpha_{i+1}$, permutando x_i and x_{i+1} fissiamo f, ma questo significa che f ha un termine uguale a $cx^{\alpha'}$ dove α' è ottenuto da α scambiando α_i e α_{i+1}. Ma $\alpha' > \alpha$, che contraddice la massimalità di α.

Ora dato il leading term cx^α di f, consideriamo il prodotto $e_1^{\beta_1} e_2^{\beta_2} \cdots e_n^{\beta_n}$, dove $\beta_i := \alpha_i - \alpha_{i+1}$ per $i = 1, 2, \ldots, n-1$, e $\beta_n := \alpha_n$. Il leading term di questo prodotto è (**esercizio**)

$$x_1^{\beta_1+\beta_2+\cdots+\beta_n} x_2^{\beta_2+\cdots+\beta_n} \cdots x_n^{\beta_n} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \tag{1.1}$$

dunque $f - ce_1^{\beta_1} e_2^{\beta_2} \cdots e_n^{\beta_n}$ è un polinomio simmetrico con monomio del leading term strettamente più piccolo di quello del leading term di f. Iterando questa procedura, per induzione sulla grandezza del monomio del leading term, arriviamo in un numero finito di passi a zero (vedi proprietà (3) dell'Esercizio 18.6). Questo mostra che ogni polinomio simmetrico è un polinomio negli e_i a coefficienti in F. L'unicità segue (**esercizio**) dal fatto che i monomi negli e_i, ossia i $e_1^{\beta_1} e_2^{\beta_2} \cdots e_n^{\beta_n}$, sono linearmente indipendenti, poichè i loro leading terms sono tutti distinti: questo viene dalla formula (1.1). □

2. Teorema fondamentale dell'algebra

In questa sezione dimostriamo il teorema fondamentale dell'algebra.

TEOREMA 18.7 (Teorema fondamentale dell'algebra). *Ogni polinomio di grado positivo a coefficienti complessi ha una radice complessa.*

Mostriamo innanzitutto che basta dimostrare il teorema per i polinomi a coefficienti reali.

LEMMA 18.8. *Se ogni polinomio di grado positivo a coefficienti reali ha una radice complessa, allora ogni polinomio di grado positivo a coefficienti complessi ha una radice complessa.*

DIMOSTRAZIONE. Sia $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, e definiamo

$$\overline{f}(x) := \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0} \in \mathbb{C}[x]$$

dove denotiamo con $\overline{a_i}$ il coniugato complesso di a_i.

Ora il polinomio $g(x) := f(x)\overline{f}(x)$ è un polinomio a coefficienti reali: infatti è facile verificare (**esercizio**) che $\overline{g}(x) = g(x)$. Dunque se $g(x)$ ha una radice complessa $z \in \mathbb{C}$, allora $g(z) = f(z)\overline{f}(z) = 0$, e ora o $f(z) = 0$, oppure $\overline{f}(z) = 0$, ma in quest'ultimo caso si verifica facilmente (**esercizio**) che $f(\overline{z}) = 0$. Dunque in entrambi i casi abbiamo dedotto che $f(x)$ ha una radice complessa. □

Dunque il teorema fondamentale dell'algebra seguirà immediatamente dal prossimo teorema.

TEOREMA 18.9. *Ogni polinomio di grado positivo a coefficienti reali ha una radice complessa.*

La dimostrazione che daremo è dovuta a Laplace.

DIMOSTRAZIONE (LAPLACE). Sia $f(x) \in \mathbb{R}[x]$ un polinomio a coefficienti reali di grado positivo $n = m2^k$, con $m, k \in \mathbb{N}$ e m dispari. Senza perdere di generalità possiamo supporre che $f(x)$ sia monico. Dimostriamo dunque l'affermazione per induzione su k.

Per $k = 0$, $f(x)$ ha grado dispari. In questo caso $f(x)$ ha una radice reale: osserviamo che i limiti $\lim_{y\to+\infty} f(y) = +\infty$ e $\lim_{y\to-\infty} f(y) = -\infty$ hanno segno opposto, dunque il grafico di $f(x)$ deve passare per l'asse delle ascisse (stiamo usando la continuità di $\mathbb{R}$).

Supponiamo ora che $k \geq 1$. Sia K un'estensione del campo $\mathbb{C}$ in cui $f(x)$ fattorizza come prodotto di fattori lineari: abbiamo visto in questo corso che tale estensione esiste sempre. Sia dunque

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \prod_{i=1}^{n}(x - r_i)$$

con $r_1, r_2, \ldots, r_n \in K$ non necessariamente distinti. Vogliamo mostrare che almeno uno degli r_i è in $\mathbb{C}$.

Per ogni numero reale $t \in \mathbb{R}$ consideriamo il polinomio

$$f_t(x) := \prod_{1\leq i<j\leq n} (x - r_i - r_j - t r_i r_j).$$

Osserviamo che i coefficienti di $f_t(x)$ sono polinomi negli r_i a coefficienti reali (poichè $t \in \mathbb{R}$). Dunque a priori i coefficienti di $f_t(x)$ sono in K. Ma osserviamo che questo polinomio è simmetrico nelle r_i, ossia permutando le r_i il polinomio $f_t(x)$ non cambia. Dunque i coefficienti di $f_t(x)$ sono polinomi simmetrici nelle r_i a coefficienti reali. Per

il teorema fondamentale dei polinomi simmetrici, ossia il Teorema 18.4, sappiamo che questi coefficienti si esprimono come polinomi nelle $e_i(r_1, r_2, \dots, r_n)$ a coefficienti reali, e questi $e_i(r_1, r_2, \dots, r_n)$, per l'Esercizio 18.3, sono a meno del segno proprio gli a_{n-i}, che sono numeri reali per ipotesi. Questo mostra che anche il polinomio $f_t(x)$ ha coefficienti reali.

Ora il grado di $f_t(x)$ è $\binom{n}{2} = n(n-1)/2 = m(n-1)2^{k-1}$ (**esercizio**), e chiaramente $n-1$ è dispari (visto che $n = m2^k$ è pari). Allora per ipotesi induttiva $f_t(x)$ ha una radice complessa. Dunque per una certa coppia (i, j) con $1 \le i < j \le n$, $r_i + r_j + t r_i r_j$ è un numero complesso. Questo è vero per ogni $t \in \mathbb{R}$, ma la coppia (i, j) dipende da t. Ma i reali sono infiniti, dunque deve esistere una coppia (i, j) per cui esistono due reali distinti $t_1, t_2 \in \mathbb{R}$ tali che $r_i + r_j + t_1 r_i r_j$ e $r_i + r_j + t_2 r_i r_j$ sono entrambi complessi. Ma allora la loro differenza $(t_1 - t_2) r_i r_j$ è un complesso, dunque $r_i r_j \in \mathbb{C}$, e quindi anche $r_i + r_j \in \mathbb{C}$. Ma allora il polinomio $x^2 - (r_i + r_j)x + r_i r_j = (x - r_i)(x - r_j)$ ha coefficienti complessi. In questo caso sappiamo che le radici sono complesse: infatti abbiamo una formula esplicita in termini dei coefficienti che sono complessi! Questo mostra che r_i e r_j sono loro stessi complessi, e conclude la dimostrazione. □

3. Esercizi

Esercizio 18.10. Dato $n \in \mathbb{N}$, $n \ge 2$, e un polinomio monico di grado n

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \prod_{i=1}^{n} (x - r_i)$$

denotiamo con

$$\Delta_n = \Delta(f) := \prod_{1 \le i < j \le n} (r_i - r_j)^2$$

il *discriminante* di f.

(1) Mostrare che $f(x)$ ha una radice multipla se e solo se $\Delta_n = 0$.
(2) Mostrare che Δ_n è un polinomio simmetrico nelle $r_1, r_2, \dots, r_n$. Dedurre che Δ_n è un polinomio a coefficienti razionali negli $a_0, a_1, \dots, a_{n-1}$.
(3) Usare l'algoritmo della dimostrazione del Teorema 18.4 per calcolare una formula esplicita del discriminante Δ_n in termini dei coefficienti $a_0, a_1, \dots, a_{n-1}$ per $n = 2$ e $n = 3$.
(4) Implementare l'algoritmo della dimostrazione del Teorema 18.4 in un qualsiasi computer algebra system (ad esempio in Sagemath).
(5) Usare il punto precedente per calcolare una formula esplicita del discriminante Δ_n in termini dei coefficienti $a_0, a_1, \dots, a_{n-1}$ per $n = 4$ e $n = 5$.

Bibliografia

[DM] P. Di Martino, *Algebra*, Pisa University Press 2013.
[CDD1] R. Chirivì, I. Del Corso, R. Dvornicich, *Esercizi scelti d i Algebra, Volume 1*, Springer 2017.
[CDD2] R. Chirivì, I. Del Corso, R. Dvornicich, *Esercizi scelti di Algebra, Volume 2*, Springer 2018.