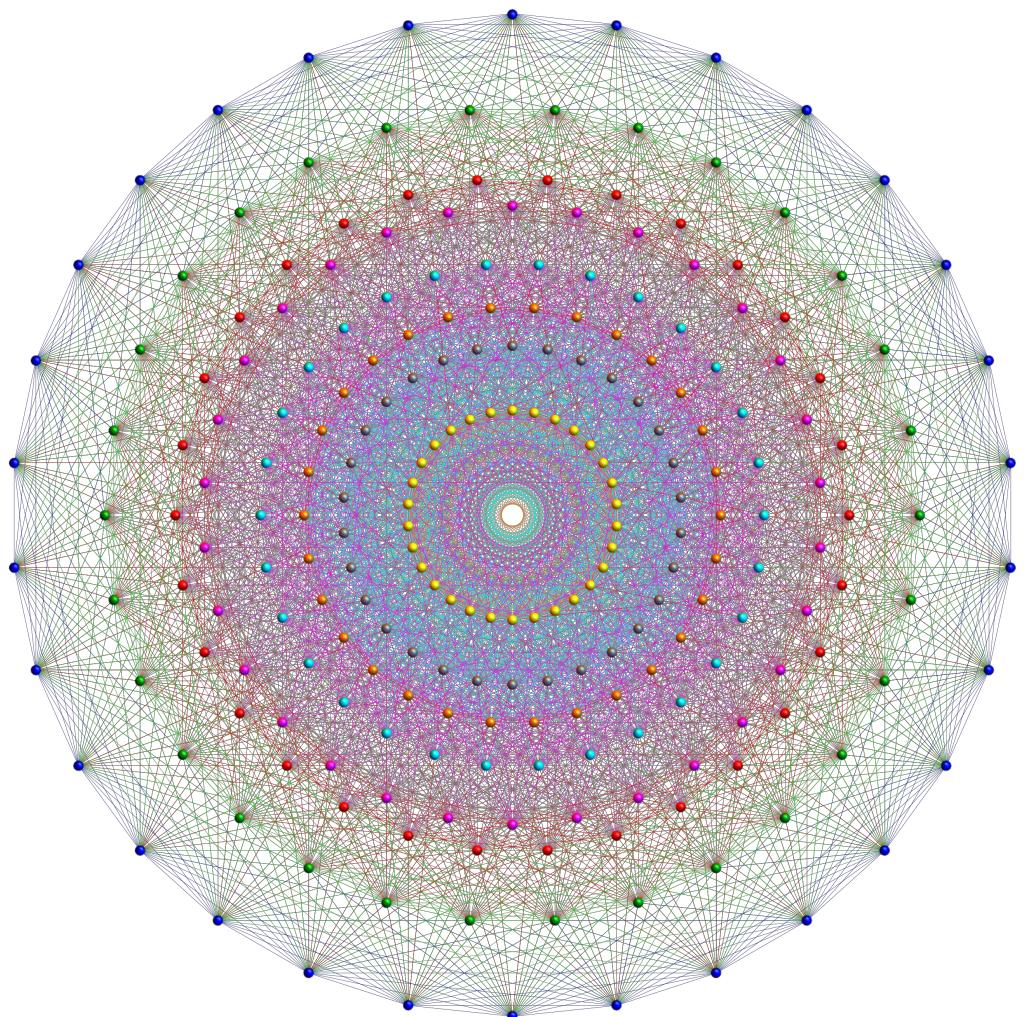


# APPUNTI DI ALGEBRA

MANUEL DEODATO



## INDICE

<b>1 Gli interi</b>	<b>3</b>
1.1 Proprietà di base	3
1.2 Massimo comune divisore	4
1.3 Fattorizzazione unica	5
1.4 Relazioni di equivalenza e congruenza	6

# 1 GLI INTERI

## 1.1 Proprietà di base

Una proprietà dei numeri interi, che si prenderà come assiomatica, è quella del *buon ordinamento*:

*Ogni insieme non-vuoto di interi maggiori o uguali a 0, ha un elemento minimo.*

Da questa deriva la seguente.

### Teorema 1.1 (Principio di induzione (prima forma))

Sia  $A(n)$  un'affermazione valida per ogni intero  $n \geq 1$  e si assume la possibilità di dimostrare che:

- (1).  $A(1)$  è vera;
- (2).  $\forall n \geq 1$ , se  $A(n)$  è vera  $\implies A(n+1)$  è vera.

Allora,  $\forall n \geq 1$ ,  $A(n)$  è vera.

*Dimostrazione.* Sia  $S$  l'insieme di interi per cui  $A(n)$  è falsa. Si mostra che  $S$  è l'insieme vuoto. Assumendo per assurdo che  $S \neq \emptyset \Rightarrow \exists n_0 \in S$ , con  $n_0$  minimo (esistente per il buon ordinamento), e, per assunzione, deve essere  $n_0 \neq 1 \Rightarrow n_0 > 1$ . Questo vuol dire che  $n_0 - 1$  non è in  $S$  e, quindi,  $A(n_0 - 1)$  è vera.

Per la proprietà (2), però, deve essere vera anche  $A(n_0)$  perché  $n_0 = (n_0 - 1) + 1$ , il che è assurdo e, pertanto,  $S = \emptyset$ .  $\square$

**Osservazione 1.1.** Nella dimostrazione sopra, si sarebbe potuto sostituire 1 con 0 e far partire il principio di induzione da  $n = 0$  piuttosto che da  $n = 1$  e non sarebbe cambiato nulla.

Il principio di induzione può essere espresso in una forma alternativa, come segue.

### Teorema 1.2 (Principio di induzione (seconda forma))

Sia  $A(n)$  affermazione vera  $\forall n \geq 0$  e sia possibile mostrare che:

- (1').  $A(0)$  è vera;
- (2').  $\forall n > 0$ , se  $A(k)$  è vera  $\forall 0 \leq k < n$ , allora  $A(n)$  è vera.

Allora  $A(n)$  è vera  $\forall n \geq 0$ .

*Dimostrazione.* Sia ancora  $S$  l'insieme degli interi che non soddisfano  $A(n)$ . Ancora per assurdo, si prende  $S \neq \emptyset$ , quindi deve esistere, per il buon ordinamento, un  $n_0 \in S$  minimo.

Per punto (1'), deve valere  $n_0 \neq 0$  e, visto che  $n_0$  è minimo,  $\forall k$  intero tale che  $0 \leq k < n_0$ ,  $A(k)$  deve essere vera. Per il punto (2'), però, deve essere vera anche  $A(n_0)$ , arrivando nuovamente all'assurdo.  $\square$

Un altro importante risultato del buon ordinamento è l'*algoritmo di Euclide*.

### Teorema 1.3 (Algoritmo di Euclide)

Siano  $m, n$  interi, con  $m > 0$ ; allora esistono interi  $q, r$ , con  $0 \leq r < m$ , tali che

$$n = qm + r \tag{1.1.1}$$

Inoltre, gli interi  $q, r$  sono univocamente determinati da tali condizioni.

*Dimostrazione.* Visto che l'insieme degli interi  $q$  tali per cui  $qm \leq n$  è limitato superiormente per definizione, si può usare il buon ordinamento per affermare che esiste un

elemento più grande tale che

$$qm \leq n < (q+1)m = qm + m$$

ossia  $0 \leq n - qm < m$ . Sia  $r = n - qm$ , per cui vale  $0 \leq r < m$ . Questo dimostra l'esistenza di  $r, q$  come descritti.

Per l'unicità, si assume che valga contemporaneamente

$$\begin{cases} n = q_1 m + r_1 & , 0 \leq r_1 < m \\ n = q_2 m + r_2 & , 0 \leq r_2 < m \end{cases}$$

con  $r_1 \neq r_2$ . Sia, per esempio,  $r_2 > r_1$ ; allora, sottraendo le due, si ha  $(q_1 - q_2)m = r_2 - r_1$ . Però, si avrebbe  $r_2 - r_1 > 0$ , il che non è possibile perché  $q_1 - q_2$  è un intero per cui  $(q_1 - q_2)m > 0$ , quindi si avrebbe  $(q_1 - q_2)m \geq m$ . Pertanto, deve essere  $r_1 = r_2$ , che fra l'altro implica  $q_1 m = q_2 m$ , per cui  $q_1 = q_2$ .  $\square$

Da questo teorema, si definisce  $r$  come il *resto della divisione di  $n$  per  $m$* .

## 1.2 Massimo comune divisore

Siano  $n, d$  due interi diversi da 0. Si dice che  $d$  divide  $n$  se esiste  $q$  intero tale che  $n = dq$ ; in questo caso, si scrive  $d|n$ . Se  $m, n$  sono interi non nulli, per *divisore comune* di  $m$  e  $n$  si intende un intero  $d \neq 0$  tale che  $d|m$  e  $d|n$ . Allora si ha la seguente definizione.

### Definizione 1.1 (Massimo comune divisore)

Per massimo comune divisore di  $m, n$  interi non nulli, si intende un intero  $d > 0$ , divisore comune di  $m$  e  $n$ , e tale che  $\forall e$  intero positivo che divide  $m$  e  $n$ , si ha anche  $e|d$ .

Chiaramente, il massimo comune divisore è univocamente determinato e si mostrerà che esiste sempre. Per farlo, si dà prima la seguente definizione.

### Definizione 1.2 (Ideale)

Sia  $J$  un sottoinsieme degli interi. Si dice che  $J$  è un *ideale* se:

- $0 \in J$ ;
- $m, n \in J \implies m + n \in J$
- se  $m \in J$  e  $n$  è un intero qualsiasi, allora  $mn \in J$ .

**Esempio 1.1.** Siano  $m_1, \dots, m_r$  interi. Sia  $J$  l'insieme di tutti gli interi che si scrivono come

$$x_1 m_1 + \dots + x_r m_r$$

con  $x_1, \dots, x_r$  interi. Allora è automaticamente verificato che  $J$  è un ideale. Infatti

- se  $y_1, \dots, y_r$  sono interi, allora

$$\sum_{i=1}^r x_i m_i + \sum_{j=1}^r y_j m_j = (x_1 + y_1)m_1 + \dots + (x_r + y_r)m_r$$

che, quindi, appartiene a  $J$ ;

- se  $n$  è un intero, si ha

$$n \sum_{i=1}^r x_i m_i = n x_1 m_1 + \dots + n x_r m_r$$

che, quindi, appartiene a  $J$ ;

- si può scrivere 0 come  $0m_1 + \dots + 0m_r$ , quindi anche  $0 \in J$ .

Dall'esempio precedente, si dice che  $J$  è **generato** dagli interi  $m_1, \dots, m_r$  e che questi sono i suoi **generatori**. Si nota che l'insieme  $\{0\}$  è esso stesso un ideale, chiamato **ideale nullo**. Inoltre,  $\mathbb{Z}$  è detto **ideale unità**. Ora si può dimostrare il seguente.

### Teorema 1.4

Sia  $J$  un ideale di  $\mathbb{Z}$ . Allora esiste un intero  $d$  che è un generatore di  $J$ . Inoltre, se  $J \neq \{0\}$ , allora  $d$  è il più piccolo intero positivo in  $J$ .

*Dimostrazione.* Sia  $J$  l'ideale nullo; allora  $0$  è un suo generatore. Sia, ora,  $J \neq \{0\}$ ; se  $n \in J$ , allora  $-n = (-1)n$  è anche in  $J$ , quindi  $J$  contiene degli interi positivi. Si vuole dimostrare che  $d$ , definito come il più piccolo intero positivo, è un generatore. Per farlo, sia  $n \in J$ , con  $n = dq + r$ ,  $0 \leq r < d$ ; allora  $r = n - dq \in J$  e, visto che vale  $r < d$ , segue che  $r = 0$ , quindi  $n = dq$  e, allora,  $d$  è un generatore.  $\square$

### Teorema 1.5

Siano  $m_1, m_2$  due interi positivi e sia  $d$  un generatore positivo per l'ideale generato da  $m_1, m_2$ . Allora  $d$  è il massimo comune divisore di  $m_1, m_2$ .

*Dimostrazione.* Per definizione,  $m_1, m_2 \in J^a$ , quindi esiste un intero  $q_1$  tale che  $m_1 = q_1d$ , per cui  $d|m_1$ . Analogamente  $d|m_2$ . Sia, poi,  $e$  un intero non-nullo che divide sia  $m_1$  che  $m_2$  come  $m_1 = h_1e$  e  $m_2 = h_2e$ , con interi  $h_1, h_2$ . Visto che  $d$  è nell'ideale generato da  $m_1, m_2$ , esistono degli interi  $s_1, s_2$  tali che  $d = s_1m_1 + s_2m_2$ , quindi

$$d = s_1h_1e + s_2h_2e = (s_1h_1 + s_2h_2)e$$

Quindi  $e$  divide  $d$  e il teorema è dimostrato.  $\square$

<sup>a</sup>Questo è ovvio perché  $m_1 = 1m_1 + 0m_2$  e  $m_2 = 0m_1 + 1m_2$ .

**Osservazione 1.2.** La stessa esatta dimostrazione funziona per più di due interi, quindi se si considerassero  $m_1, \dots, m_r$  degli interi, con  $d$  generatore positivo dell'ideale generato,  $d$  sarebbe anche il massimo comune divisore.

### Definizione 1.3 (Interi relativamente primi)

Siano  $m_1, \dots, m_r$  degli interi il cui massimo comune divisore è 1. Allora  $m_1, \dots, m_r$  si dicono *relativamente primi* e, per questi, esistono interi  $x_1, \dots, x_r$  tali che

$$x_1m_1 + \dots + x_r m_r = 1$$

perché 1 appartiene all'ideale generato dagli  $m_i$ .

## 1.3 Fattorizzazione unica

### Definizione 1.4 (Numero primo)

Si dice che  $p$  è un numero primo se è un intero e  $p \geq 2$  tale che, data una fattorizzazione  $p = mn$ , con interi positivi  $m, n$ , allora  $m = 1$  o  $n = 1$ .

Ora si mostra che ogni numero intero ammette un'unica scomposizione in numeri primi. Per dimostrare l'unicità di tale scomposizione, si introduce il seguente lemma.

### Lemma 1.1

Sia  $p$  un numero primo e siano  $m, n$  interi non-nulli e tali che  $p$  divide  $mn$ . Allora o  $p|m$  o  $p|n$ .

*Dimostrazione.* Senza perdita di generalità, si assume che  $p$  non divida  $m$ . Allora, il massimo comune divisore di  $p$  e  $m$  deve essere 1, pertanto esistono interi  $a, b$  tali per cui  $1 = ap + bm$ .

Ora, moltiplicando ambo i membri per  $n$ , si ha  $n = nap + bmn$ , ma  $mn = pc$  per qualche intero  $c$  (essendo in assunzione  $mn$  divisibile per  $p$ ), quindi

$$n = nap + bpc = (na + bc)p$$

il che implica che  $p$  divide  $n$ . □

Per evidenziare l'utilità del lemma nel seguente teorema, si nota che se  $p$  divide un prodotto di numeri primi  $q_1 \dots q_s$ , si hanno due possibilità: o  $p$  divide  $q_1$ , o divide  $q_2 \dots q_s$ ; se divide  $q_1$ , allora  $p \equiv q_1$ , altrimenti si trova  $p \equiv q_i$  procedendo induttivamente. Il caso interessante è quando si ha un uguaglianza tra prodotti di numeri primi

$$p_1 \dots p_r = q_1 \dots q_s$$

Rinumerandoli, si può assumere senza perdita di generalità che  $p_1 = q_1$  e, induttivamente, che  $p_i = q_i$  e  $r = s$ , essendo due scomposizioni in un numeri primi.

### Teorema 1.6

Ogni intero positivo  $n \geq 2$  ammette una fattorizzazione come prodotto di numeri primi (non necessariamente distinti)  $n = p_1 \dots p_r$  e tale fattorizzazione è unica.

*Dimostrazione.* Si assume per assurdo che esista almeno un intero  $\geq 2$  che non possa essere espresso come prodotto di numeri primi. Sia  $m$  il più piccolo di questi.

Per costruzione,  $m$  non può essere primo, quindi  $m = de$ , con  $d, e > 1$ . Visto che  $d$  ed  $e$  sono minori di  $m$  e visto che  $m$  è scelto per essere il più piccolo fra gli interi non fattorizzabili come numeri primi, allora sia  $d$  che  $e$  ammettono scomposizione in prodotto di numeri primi:

$$\begin{aligned} d &= p_1 \dots p_r \\ e &= p'_1 \dots p'_s \end{aligned} \implies m = p_1 \dots p_r p'_1 \dots p'_s$$

da cui l'assurdo.

Per mostrare l'unicità, si usa il lemma 1.1. Come conseguenza, diretta del lemma, se esistessero due scomposizioni in primi  $p_1 \dots p_r$  e  $p'_1 \dots p'_s$ , varrebbe  $p_1 \dots p_r = p'_1 \dots p'_s \Rightarrow p_i = p'_i$  e  $r = s$ , da cui l'unicità □

## 1.4 Relazioni di equivalenza e congruenza

### Definizione 1.5 (Relazione di equivalenza)

Sia  $S$  un insieme. Una relazione di equivalenza su  $S$  è una relazione indicata con  $x \sim y$ ,  $x, y \in S$ , tale che:

ER 1.  $\forall x \in S$ ,  $x \sim x$ ;

ER 2. se  $x \sim y$  e  $y \sim z$ , allora  $x \sim z$ ;

ER 3. se  $x \sim y$ , allora  $y \sim x$ .

Se su  $S$  è definita una relazione di equivalenza  $\sim$ , le classi di equivalenza sono insiemi  $C_x := \{y \in S : y \sim x\}$  partizionano  $S$  in insiemi disgiunti. Inoltre, dati due elementi  $r, s \in S$ , si ha  $C_r \equiv C_s$ , oppure  $C_r, C_s$  non hanno elementi in comune. Si sceglie un elemento che identifica la classe di equivalenza, ad esempio  $x$  per  $C_x$ , e tale elemento si chiama rappresentante della classe di equivalenza. Un esempio di relazione di equivalenza è la congruenza.

### Definizione 1.6 (Congruenza)

Sia  $n$  un intero positivo e siano  $x, y$  due interi. Si dice che  $x$  è *congruente*  $y$  modulo  $n$  se  $\exists m : x - y = mn$ . In tal caso, si scriverà  $x \equiv y \pmod{n}$ .

La congruenza di  $x, y$  come  $x - y = mn$  implica automaticamente che  $x - y$  appartiene all'ideale generato da  $n$ ; inoltre, se  $n \neq 0$ , allora  $x - y$  è divisibile per  $n$ .

Oltre alle proprietà delle relazioni di equivalenza, la congruenza ne soddisfa anche altre due:

- se  $x \equiv y \pmod{n}$  e  $z$  è un intero, allora  $xz \equiv yz \pmod{n}$ ;
- se  $x \equiv y \pmod{n}$  e  $x' \equiv y' \pmod{n}$ , allora  $xx' \equiv yy' \pmod{n}$  e  $x + x' \equiv y + y' \pmod{n}$ .

Dalla definizione di congruenza, si definiscono gli interi **pari** come quelli che sono congruenti a 0  $\pmod{2}$  (quindi  $n = 2m$ ) e quelli **dispari** come gli interi che non sono pari, quindi della forma  $2m + 1$ , per qualche intero  $m$ .