Corso di Laurea in Matematica

ALGEBRA I

dispense anno 2018

La parola “algebra” proviene da un libro scritto nel 830 dall’astronomo Mohammed ibn Musa al-Kouwârizmi e intitolato *Al-jabr w’al muqâbala*. La parola *al-jabr* significa “ristabilire” e in questo comtesto significa ristabilire l’equilibrio di un’equazione scrivendo in un suo membro un termine che era stato eliminato nell’altro membro [...]. *Al-jabr* venne anche a significare “conciaossa” e quando i Mori trasportarono il termine in Spagna esso divenne *algebrista*, continuando a conservare quest’ultimo significato. In quel periodo era molto comune in Spagna vedere un’insegna con la scritta “Algebrista y Sangrador” (conciaossa e salassatore) sopra l’ingresso delle botteghe dei barbieri.

[M. Kline, *Storia del pensiero matematico*]

I matematici si devono applicare ai problemi più astrusi e remoti dall’esistenza materiale, ed a questo scopo la loro mente deve ignorare i sensi e dev’essere addestrata ad avere a malapena un minimo rapporto con il corpo; perciò i matematici sono tutti tardi, distratti, letargici e mai a loro agio negli affari di tutti i giorni. Di conseguenza, ogni loro organo e di fatto il loro intero corpo si sforma e diviene torpido e debole; quasi condannato ad una perpetua oscurità. Infatti mentre la mente è intenta a questi studi, la luce degli istinti animali viene compressa nel suo centro e non può espandersi a illuminare nient’altro che non sia il cervello.

[B. Ramazzini, *De Morbis Artificum Diatriba*[1]]

[1]Bernardino Ramazzini (1633–1714) non era un bischero qualsiasi, ma anzi uno studioso di notevole libertà intellettuale, considerato, oggi, il fondatore della medicina del lavoro. Né è possibile liquidarlo come un “perito di parte” dalle dubbie intenzioni, dato che fu tra l’altro ottimo amico di Leibniz, che ospitò a casa sua a Modena nel 1690, e grazie alle referenze del quale divenne, nel 1706, il primo italiano ammesso all’Accademia delle Scienze di Berlino. In Firenze, Via B. Ramazzini è la prima traversa di Via G. D’Annunzio (all’altezza del cinema).

Indice

Parte prima: INSIEMI E NUMERI

1

Insiemi

1.1. Insiemi e sottoinsiemi.

In queste note, il concetto di insieme verrà assunto in una forma 'ingenua', e la teoria relativa sarà trattata in modo pragmatico, prescindendo da una formulazione assiomatica della stessa. Per quanto attiene ai fini di questo corso, si tratta principalmente di fissare un linguaggio, che è poi quello di base di buona parte della matematica. I fondamenti della teoria degli insiemi sono in genere oggetto di studio nei corsi superiori di logica. Dunque, assumeremo come primitivi i concetti di *oggetto* (o *ente*), *insieme, elemento, appartenenza*.

In genere si utilizzano lettere maiuscole, come $A, X, S, ...$ per indicare gli insiemi, e lettere minuscole, come $a, a', x, y, \alpha, \dots$ per gli elementi di un insieme.

Alcuni insiemi particolarmente importanti hanno un simbolo in esclusiva:

– $\mathbb{N}$ indicherà sempre e solo l'insieme di tutti i numeri **naturali**, cioè dei numeri $0, 1, 2, 3, 4 \dots$.

– $\mathbb{Z}$ è l'insieme dei numeri **interi**; cioè l'insieme dei numeri $0, 1, -1, 2, -2, 3, -3, \dots$

– $\mathbb{Q}$ è l'insieme dei numeri **razionali**; cioè dei numeri $\frac{m}{n}$, dove $m, n \in \mathbb{Z}$ e $n \neq 0$;

– $\mathbb{R}$ è l'insieme dei numeri **reali**;

– $\mathbb{C}$ è l'insieme dei numeri **complessi**.

La definizione rigorosa di questi insiemi a partire dall'insieme $\mathbb{N}$ è argomento che - se mai - tratteremo più avanti; per il momento dovrebbe essere sufficiente la nozione che si ha di essi dalle scuole superiori (e chi ancora non conosce i numeri complessi, non si allarmi: li definiremo rigorosamente nella sezione 2.6).

Il simbolo $\in$ indica l'appartenenza di un elemento ad un certo insieme; $a \in X$ (che si legge "a appartiene a X") significa cioè che a è un elemento dell'insieme X. Con il simbolo $\notin$ si intende la non appartenenza: $a \notin X$ significa che a *non è un elemento* dell'insieme X. Ad esempio, $2 \in \mathbb{N}$ mentre $\pi \notin \mathbb{N}$ (ricordo che π è il numero reale che esprime il rapporto tra la lunghezza di una circonferenza e quella del suo diametro). Uno specifico insieme verrà di solito descritto mediante informazioni delimitate da parentesi graffe: {....}. L'informazione può essere costituita dall'indicazione diretta degli elementi dell'insieme, oppure dalle proprietà che ne individuano univocamente gli elementi. Ad esempio, l'insieme i cui elementi sono i numeri naturali $2, 3, 4$ può essere descritto nelle seguenti maniere (e, naturalmente, in molte altre):

$$\{2, 3, 4\}, \quad \{x \mid x \in \mathbb{N} \text{ e } 2 \leq x \leq 4\}.$$

Nella seconda modalità (che spesso e volentieri si accorcia in $\{x \in \mathbb{N} \mid 2 \leq x \leq 4\}$), la barra verticale $\mid$ segnala che ciò che segue è sono le proprietà (predicati) che servono ad individuare gli elementi dell'insieme. A volte, invece della barra, si usano i 'due punti'. Ad esempio $\{2x : x \in \mathbb{N}\}$ è l'insieme dei numeri interi pari.
È opportuno osservare che né l'ordine con cui sono descritti gli elementi di un insieme, né eventuali ripetizioni, modificano l'insieme. Ad esempio, le scritture:

$$\{1, 2\}, \quad \{1, 2, 1\}, \quad \{2, 1\}$$

descrivono tutte il medesimo insieme.
Inoltre, è bene sapere che gli elementi di un insieme possono anche essere di 'natura' diversa; ad esempio, gli *elementi* dell'insieme $X = \{1, \{1\}\}$, sono il *numero intero* 1 e *l'insieme* $\{1\}$ (X contiene quindi due elementi distinti).

È conveniente contemplare anche la possibilità che un insieme sia privo di elementi. In matematica è infatti frequente la possibilità di considerare proprietà che non sono soddisfatte da alcun oggetto (in un certo insieme universo). Tali proprietà definiscono quindi insiemi privi di elementi. Ad esempio, l'insieme dei numeri interi pari che sono potenza di tre non contiene alcun elemento.
L'insieme privo di elementi si denota con $\emptyset$ e si chiama **insieme vuoto**. Ad esempio, è vuoto l'insieme delle soluzioni reali del sistema di equazioni

$$\begin{cases} 2x + 3y = 3 \\ xy = 1 \end{cases}$$

Questo si può scrivere così: $\{(x, y) \mid x, y \in \mathbb{R},\ 2x + 3y = 3 \text{ e } xy = 1\} = \emptyset$.

Assumeremo, almeno per il momento, come primitivo anche il concetto di numero di elementi di un insieme. Sia X un insieme; diremo che X è un insieme **finito** se X contiene un numero finito di elementi; in tal caso, se il numero di elementi di X è n, scriviamo $|X| = n$. Ad esempio, $|\{1, 2, 6, 8\}| = 4$, e $|\emptyset| = 0$. Se invece X contiene un numero infinito di elementi, diremo che X è un insieme **infinito** e scriveremo $|X| = \infty$. Ad esempio $|\mathbb{N}| = \infty$. Il simbolo $|X|$ (che quindi, per quanto riguarda un approccio introduttivo, sarà ∞ oppure un numero naturale), lo chiameremo **ordine** (o *cardinalità*) dell'insieme X.

Paradosso di Russell. Anche se si tratta di una insidia che non si presenterà nell'ambito della nostra utilizzazione del linguaggio della teoria degli insiemi, è opportuno avvertire che non tutto ciò che ci si presenta intuitivamente come una "*proprietà*" può essere utilizzato per definire un insieme. L'esempio più famoso ed importante per la nascita di quella che sarà poi la teoria assiomatica degli insiemi è il cosiddetto Paradosso di Russell.
Per illustrare il paradosso, diciamo che un insieme è *normale* se non contiene se stesso come elemento (si può pensare ad esempio all'insieme di tutti i concetti astratti: questo è, direi, un concetto astratto esso stesso, quindi contiene se stesso come elemento, non è dunque un insieme normale). Intuitivamente, l'essere normale ci appare senz'altro come una proprietà 'sensata'; ma cosa accade quando la utilizziamo per definire un insieme ?
Definiamo cioè l'insieme N i cui elementi sono tutti gli insiemi normali. Quindi

$$N = \{X \mid X \text{ è un insieme e } X \notin X\}.$$

A questo punto, se N è un insieme, esso è o non è normale. Analizzate le due possibilità: entrambe conducono ad una contraddizione. Quindi N non è un insieme; non ogni proprietà costituisce una definizione.

Il paradosso di Russel mostra che "qualche cosa non si può fare". Il concetto di insieme va quindi specificato in modo più accurato. Il punto del paradosso non è tanto l'immaginarsi come possa avvenire che un insieme contenga se stesso (generando un processo all'infinito), quanto il fatto che una certa relazione tra enti (quella di appartenenza) venga usata in modo "autoreferenziale". Questo è alla base di molti altri 'paradossi logici', come quello del mentitore, del barbiere, etc. che alcuni già conosceranno e nei quali non si fa riferimento a processi all'infinito. Per essere assolutamente moderni vediamo un esempio riferito alla rete Internet.
Come si sa, le varie pagine Internet accessibili in rete contengono diverse connessioni (links) ad altre pagine; tali connessioni sono di norma segnalate da una o più parole sottolineate. Ora, vi sono pagine che contengono un link a se stesse (tipicamente le cosiddette "home pages"), altre (la maggioranza) che non contengono un link a se stesse. Il numero totale di pagine (nel mondo, o possiamo limitarci ad ambiti più ristretti - non cambia nulla) è comunque finito. Supponiamo che io (il Grande Fratello) chieda al mio capo tecnico di allestire una pagina Internet che contenga un link a tutte e sole le pagine che non hanno link a se stesse... Se ci pensate un attimo, vedete che una tale pagina non si può fare, e che tale "paradosso" è molto simile al paradosso di Russell (ma non è esattamente la stessa cosa: per un'introduzione un poco più approfondita al paradosso di Russell ed ad altri paradossi ad esso collegati si può intanto vedere QUI).

Sottoinsiemi. Siano S e A insiemi: S si dice *sottoinsieme* di A, e si scrive

$$S \subseteq A,$$

se ogni elemento di S appartiene ad A.

Se $S \subseteq A$ si dice anche che S è *incluso* in A. Ad esempio $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$, $\{1,6\} \subseteq \{6,3,2,1\}$, mentre $\{1,6\} \not\subseteq \{x | x \in \mathbb{N} \text{ e } 2 \text{ divide } x\}$, dove naturalmente $S \not\subseteq A$ significa che S non è sottoinsieme di A, ovvero che esiste almeno un elemento x tale che $x \in S$ ma $x \notin A$.

Dalla definizione è immediato che ogni insieme è un sottoinsieme di se stesso, così come che l'insieme vuoto è un sottoinsieme di qualunque insieme. Quindi:

$$\textit{per ogni insieme } A: \quad \emptyset \subseteq A \quad e \quad A \subseteq A.$$

È anche chiaro che l'inclusione tra insiemi è una proprietà *transitiva*; ovvero, se A, B, C sono insiemi con $A \subseteq B$ e $B \subseteq C$, allora $A \subseteq C$.

Uguaglianza di insiemi. Due insiemi A e B sono *uguali* (si scrive $A = B$) se ogni elemento di A è elemento di B e viceversa. Quindi $A = B$ se è soddisfatta la *doppia inclusione* : $A \subseteq B$ e $B \subseteq A$. Spesso, per provare l'uguaglianza di due insiemi si dimostra appunto la doppia inclusione; esempi di questo metodo si trovano nelle dimostrazioni delle Proposizioni delle pagine seguenti. Chiaramente, per provare invece che due insiemi *non* sono uguali è sufficiente trovare un elemento di uno dei due insiemi che non appartiene all'altro.

ESEMPI. - $\{1,2,3\} = \{x \mid x \in \mathbb{Z}, \frac{1}{2} \leq x \leq \sqrt{10}\}$;

- $\{1, \{1\}\} \neq \{1\}$;

- $\{1\} \not\subseteq \{\{1\}, \{2\}\}$;

- $\{\emptyset, \{\emptyset\}, \emptyset\} = \{\emptyset, \{\emptyset\}\}$.

Un sottoinsieme S dell'insieme A si dice *proprio* se non coincide con A, ovvero $S \subseteq A$ e $S \neq A$. Per indicare che S è un sottoinsieme proprio di S scriveremo $S \subset A$.

Insieme delle parti. Dato un insieme A, allora la collezione di tutti i sottoinsiemi di A costituisce un insieme, detto *insieme della parti* (o insieme potenza) dell'insieme A, che si denota con $\mathcal{P}(A)$. Quindi

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

ESEMPI. Se $X = \{1, 2\}$, allora $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$;

$\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$;

$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

Osserviamo che, per ogni insieme X si ha $\emptyset \in \mathcal{P}(X)$ e $X \in \mathcal{P}(X)$.

Più avanti in questi appunti dimostreremo il seguente importante fatto: *se A è un insieme finito e $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$.*.

1.2. Operazioni tra insiemi.

Siano A e B insiemi.

Unione. Si chiama *unione* di A e B e si denota con $A \cup B$, l'insieme i cui elementi sono gli oggetti che appartengono ad almeno uno tra A e B. Quindi

$$A \cup B = \{x \mid x \in A \text{ o } x \in B\}.$$

Intersezione. Si chiama *intersezione* di A e B e si denota con $A \cap B$, l'insieme i cui elementi sono gli oggetti che appartengono sia ad A che a B. Quindi

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}.$$

ESEMPI. 1) Siano $A = \{-1, 0, 1\}$ e $B = \{2x \mid x \in \mathbb{N},\ 0 \leq x \leq 3\}$, allora

$$A \cup B = \{-1, 0, 1, 2, 4, 6\} \quad \text{e} \quad A \cap B = \{0\}.$$

2) Siano $P = \{x \mid x \in \mathbb{N},\ 2 \text{ divide } x\}$ e $D = \{x \mid x \in \mathbb{N},\ 2 \text{ non divide } x\}$, rispettivamente, l'insieme dei numeri naturali pari e quello dei numeri naturali dispari, allora

$$P \cup D = \mathbb{N} \quad \text{e} \quad P \cap D = \emptyset.$$

La verifica delle seguenti osservazioni, che è comunque utile formulare esplicitamente, è immediata: *Siano A, B insiemi; allora*

- $A = A \cup \emptyset$ e $\emptyset \cap A = \emptyset$;
- $A \subseteq A \cup B$ e $A \cap B \subseteq A$;
- $A = A \cup B$ se e solo se $B \subseteq A$;

- $A = A \cap B$ se e solo se $A \subseteq B$.

Due insiemi A e B si dicono *disgiunti* se non hanno elementi in comune, cioè se

$$A \cap B = \emptyset.$$

Le operazioni di unione e intersezione soddisfano ad alcune importanti proprietà che sono di facile verifica.

Proposizione 1.1. *Siano A, B e C insiemi. Allora*

1) $A \cup A = A$;

2) $A \cup B = B \cup A$;

3) $A \cup (B \cup C) = (A \cup B) \cup C$.

Dimostrazione. Le proprietà (1) e (2) si verificano immediatamente.
Vediamo la dimostrazione della proprietà (3); proveremo l'uguaglianza degli insiemi $A \cup (B \cup C)$ e $(A \cup B) \cup C$ mediante la verifica della doppia inclusione.
Sia x un elemento di $A \cup (B \cup C)$; allora x appartiene ad A o x appartiene a $B \cup C$. Ora, se $x \in A$, allora $x \in A \cup B$ e quindi $x \in (A \cup B) \cup C$; se $x \in B \cup C$, allora $x \in B$ e dunque $x \in A \cup B$, oppure $x \in C$; comunque si ha $x \in (A \cup B) \cup C$. Abbiamo quindi provato che ogni elemento di $A \cup (B \cup C)$ appartiene a $(A \cup B) \cup C$; cioè che

$$A \cup (B \cup C) \subseteq (A \cup B) \cup C.$$

Allo stesso modo si dimostra l'inclusione inversa: $(A \cup B) \cup C \subseteq A \cup (B \cup C)$; e quindi vale l'uguaglianza. ∎

La proprietà 2) è la proprietá **commutativa** dell'unione; mentre la 3) è la proprietà **associativa** dell'unione.

Proposizione 1.2. *Siano A, B e C insiemi. Allora*

1) $A \cap A = A$;

2) $A \cap B = B \cap A$;

3) $A \cap (B \cap C) = (A \cap B) \cap C$.

Dimostrazione. Per esercizio. ∎

Quindi, anche l'operazione di intersezione di insiemi gode delle proprietà commutativa (2), e associativa (3).

La prossima proposizione descrive le importanti proprietà **distributive** tra l'unione e l'intersezione di insiemi

Proposizione 1.3. *Siano A, B e C insiemi. Allora*

1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Dimostrazione. (1). Sia $x \in A \cap (B \cup C)$. Allora $x \in A$ e $x \in B \cup C$; possiamo scrivere (la parentesi graffa indica, come avviene per i sistemi di equazioni, che entrambe le condizioni devono essere verificate):

$$\begin{cases} x \in A \\ x \in B \ \text{ o } \ x \in C \end{cases}$$

Abbiamo quindi due possibilità:

$$\begin{cases} x \in A \\ x \in B \end{cases}; \quad \text{oppure} \quad \begin{cases} x \in A \\ x \in C \end{cases}$$

Dunque $x \in A \cap B$ o $x \in A \cap C$; cioè $x \in (A \cap B) \cup (A \cap C)$. Abbiamo provato che

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$

Viceversa, sia $x \in (A \cap B) \cup (A \cap C)$. Allora

$$\begin{cases} x \in A \\ x \in B \end{cases} \quad \text{oppure} \quad \begin{cases} x \in A \\ x \in C \end{cases}$$

Nel primo caso $x \in A$ e $x \in B$, allora $x \in A$ e $x \in B \cup C$, e quindi $x \in A \cap (B \cup C)$; allo stesso modo, se $x \in A$ e $x \in C$, allora $x \in A \cap (B \cup C)$. Dunque

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$$

La doppia inclusione è verificata e l'uguaglianza 1) è provata.

La dimostrazione di 2) è simile ed è lasciata per esercizio. ∎

Differenza. Siano A e B due insiemi. Si chiama *differenza* di A e B, e si denota con $A \setminus B$, l'insieme i cui elementi sono gli oggetti che appartengono ad A ma non appartengono a B. Quindi

$$A \setminus B = \{x \mid x \in A \ \text{ e } \ x \notin B \ \}.$$

Ad esempio, se $A = \{1, 2, 3\}$ e $B = \{2x \mid x \in \mathbb{N}\}$, allora

$$A \setminus B = \{1, 3\} \text{ e } B \setminus A = \{2x \mid x \in \mathbb{N} \ \text{ e } \ x \neq 1\}.$$

Questo esempio mostra che la differenza tra insiemi non è commutativa. Le seguenti proprietà sono immediate: siano A, B insiemi, allora

$$A \setminus B \subseteq A; \quad A \setminus A = \emptyset; \quad A \setminus \emptyset = A.$$

Proposizione 1.4 (leggi di De Morgan)**.** *Siano A, B e C insiemi. Allora*

1) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$*;*

2) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$*.*

Dimostrazione. 1). Sia $x \in A \setminus (B \cup C)$, allora $x \in A$ e $x \notin B \cup C$. Quindi

$$x \in A \quad , \quad x \notin B \quad \text{e} \quad x \notin C.$$

In particolare perciò:

$$\begin{cases} x \in A \\ x \notin B \end{cases} \qquad \text{e} \qquad \begin{cases} x \in A \\ x \notin C \end{cases}$$

da cui segue, rispettivamente, $x \in A \setminus B$, e $x \in A \setminus C$.
Dunque: $x \in (A \setminus B) \cap (A \setminus C)$. Abbiamo così provato l'inclusione:

$$A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C).$$

Viceversa, sia $x \in (A \setminus B) \cap (A \setminus C)$; allora $x \in A \setminus B \quad \text{e} \quad x \in A \setminus C$. Cioé:

$$x \in A \quad , \quad x \notin B \quad \text{e} \quad x \notin C.$$

Ora, da $\begin{cases} x \notin B \\ x \notin C \end{cases}$, segue $x \notin B \cup C$, e pertanto $x \in A \setminus (B \cup C)$; dimostrando così l'inclusione inversa

$$(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$$

e dunque l'uguaglianza $\quad (A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C).$

La dimostrazione del punto 2) è lasciata per esercizio. ∎

Differenza simmetrica. Siano A e B due insiemi. Si chiama *differenza simmetrica* di A e B, e si denota con $A\Delta B$, l'insieme i cui elementi che appartengono ad uno e un solo degli insiemi A e B. Quindi

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

Ad esempio, se $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$, allora $A\Delta B = \{1, 2, 4, 5\}$.

La dimostrazione delle principali proprietà della differenza simmetrica è lasciata per esercizio. Si osservino in particolare le proprietà 3), 4), e 5) che, rispettivamente, assicurano che la differenza simmetrica è commutativa, che è associativa, e che l'intersezione è distributiva rispetto alla differenza simmetrica.

Proposizione 1.5. *Siano A, B e C insiemi. Allora*

1) $A\Delta A = \emptyset$ *e* $A\Delta\emptyset = A$;

2) $A\Delta B = (A \cup B) \setminus (A \cap B)$;

3) $A\Delta B = B\Delta A$;

4) $(A\Delta B)\Delta C = A\Delta(B\Delta C)$;

5) $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.

Esercizio 1.1. Siano A, B, C insiemi. Si dimostri che:

(a) $A\triangle(B \cup C) \subseteq (A\triangle B) \cup C$.

(b) $A\triangle(B \cup C) = (A\triangle B) \cup C$ se e solo se $A \cap C = \emptyset$.

SOLUZIONE. (a) $(B \cup C) \setminus A \subseteq (B \setminus A) \cup (C \setminus A) \subseteq (B \setminus A) \cup C \subseteq (A \triangle B) \cup C$. Inoltre, poiché $B \subseteq B \cup C$ si ha $A \setminus (B \cup C) \subseteq A \setminus B \subseteq (A \triangle B)$.
Dunque: $A \triangle (B \cup C) = (A \setminus (B \cup C)) \cup (B \cup C) \setminus A) \subseteq (A \triangle B) \cup C$.
(b) Sia $A \cap C = \emptyset$; per il punto (a) è sufficiente provare l'inclusione $(A \triangle B) \cup C \subseteq A \triangle (B \cup C)$. Sia quindi $x \in (A \triangle B) \cup C = (A \setminus B) \cup (B \setminus A) \cup C$; se $x \in A$, allora $x \notin B$ e (per ipotesi) $x \notin C$, quindi $x \in A \setminus (B \cup C) \subseteq A \triangle (B \cup C)$; se invece $x \in (B \setminus A) \cup C$ allora $x \notin A$ (sempre perchè $A \cap C = \emptyset$), e quindi $x \in (B \cup C) \setminus A \subseteq A \triangle (B \cup C)$.
Dunque $(A \triangle B) \cup C \subseteq A \triangle (B \cup C)$.
Viceversa, sia $A \cap C \neq \emptyset$, e sia $x \in A \cap C$. Allora, poichè $x \in C$, si ha $x \in (A \triangle B) \cup C$; ma $x \notin A \setminus (B \cup C)$ (perchè $x \in C$) e $x \notin (B \cup C) \setminus A$ (perchè $x \in A$); quindi $x \notin (A \setminus (B \cup C)) \cup ((B \cup C) \setminus A) = A \triangle (B \cup C)$.
Dunque $(A \triangle B) \cup C \not\subseteq A \triangle (B \cup C)$. ∎

Unioni e intersezioni generalizzate. Prima di entrare nel merito, diciamo qualcosa a proposito dell'uso degli *indici* nella notazione matematica. Il lettore sarà già familiare con il loro impiego nelle definizioni di successioni: i termini di una successione si denotano in generale con a_n dove n (l'indice) è un numero intero positivo (che per lo più parte da 0 o da 1). Lo stessa convenzione, ovvero quello di assegnare ad ogni ente appartenente ad una famiglia - finita o infinita - un'etichetta che consenta di richiamarlo con una notazione più compatta, viene utilizzato anche in molti altri contesti. Ad esempio, se n è un certo intero positivo, e A è un insieme con n elementi (che è possibile non siano noti con precisione), si possono designare gli elementi di A come

$$A = \{a_1, a_2, a_3, \ldots, a_n\}.$$

Più in generale, data una famiglia - anche infinita - di oggetti (i quali possono a loro volta essere insiemi), può essere spesso opportuno indicizzarli. In generale gli indici sono presi in un altro insieme noto, come $\mathbb{N}$ o $\mathbb{Z}$, ma a volte si può essere generici fino in fondo e assegnare gli indici in un non specificato insieme (che allora viene in genere chiamato I - l'insieme degli indici). Spesso poi, l'indice ha strettamente a che fare con la definizione del particolare ente che esso etichetta; questo normalmente accade nelle successioni. Come altro esempio, l'insieme dei numeri naturali maggiori di un certo numero n può essere indicizzato proprio da tale n

$$A_n = \{a \in \mathbb{N} \mid a \geq n\},$$

che è una notazione conveniente se abbiamo intenzione di considerare tutta la famiglia di insiemi di questo tipo; si dice allora

$$\text{la famiglia degli insiemi } A_n \text{ al variare di } n \in \mathbb{N}.$$

Se A, B e C sono insiemi; allora la proprietà associativa della intersezione consente di poter scrivere senza ambiguità $A \cap B \cap C$, intendendo, indifferentemente $(A \cap B) \cap C$ ovvero $A \cap (B \cap C)$. Chiaramente si ha l'uguaglianza:

$$A \cap B \cap C = \{\, x \mid x \in A,\ x \in B,\ x \in C \,\}.$$

Similmente, per quanto concerne l'unione; avremo:

$$A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C) = \{\, x \mid x \in A \ \text{ o } \ x \in B \ \text{ o } \ x \in C \,\}.$$

Questo si estende ad un numero qualunque di insiemi; se $A_1, A_2, \ldots, A_n$ sono insiemi; allora

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{\, x \mid x \in A_i \ \text{ per qualche } \ i = 1, 2, \ldots, n \,\}.$$

e

$$A_1 \cap A_2 \cap \cdots \cap A_n = \{\ x \mid x \in A_i \ \text{ per ogni } \ i = 1, 2, \ldots, n\ \}.$$

Ora, il passo naturale è passare ad una famiglia infinita di insiemi. Sia F una famiglia di insiemi. Si definisce, rispettivamente, l'unione e l'intersezione degli insiemi della famiglia F nel modo seguente:

$$\bigcup_{A \in F} A = \{x \mid x \in A \ \text{ per qualche } \ A \in F\ \}.$$

$$\bigcap_{A \in F} A = \{x \mid x \in A \ \text{ per ogni } \ A \in F\ \}.$$

Nella pratica, gli insiemi di una famiglia sono in genere *indicizzati*; cioè, come abbiamo detto, viene dato un insieme I, chiamato degli *indici*, ed una corrispondenza tra gli insiemi della famiglia F e gli elementi di I, per cui all'elemento $i \in I$ corrisponde l'insieme $A_i \in F$. Si scrive che F è la famiglia degli insiemi $(A_i)_{i \in I}$ e quindi per unione e intersezione si usa la notazione:

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \ \text{ per qualche } \ i \in I\ \}.$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \ \text{ per ogni } \ i \in I\ \}.$$

Esempi. 1) Per ogni $i \in \mathbb{N}$ sia $M_i = \{x \mid x \in \mathbb{N}\ ,\ x \leq i\}$. In questo caso, l'insieme degli indici è l'insieme dei numeri naturali e, ad esempio, $M_4 = \{0, 1, 2, 3, 4\}$. Allora:

$$\bigcup_{i \in \mathbb{N}} M_i = \mathbb{N} \qquad \text{e} \qquad \bigcap_{i \in \mathbb{N}} M_i = \{0\}.$$

Infatti, sia $X = \bigcup_{i \in \mathbb{N}} M_i$; allora chiaramente $X \subseteq \mathbb{N}$ (dato che, per ogni $i \in \mathbb{N}$: $M_i \subseteq \mathbb{N}$); viceversa, se $n \in \mathbb{N}$ allora $n \in M_n$ e quindi $n \in X$, dunque $\mathbb{N} \subseteq X$.
L'intersezione è chiara, dato che, per ogni $i \in \mathbb{N} : \{0\} \subseteq M_i$ e $\bigcap_{i \in \mathbb{N}} M_i \subseteq M_0 = \{0\}$.

2) Per ogni $i \in \mathbb{N}$ sia $N_i = \{x \mid x \in \mathbb{N}\ ,\ x \geq i\ \}$. Allora:

$$\bigcup_{i \in \mathbb{N}} N_i = \mathbb{N} \qquad \text{e} \qquad \bigcap_{i \in \mathbb{N}} N_i = \emptyset.$$

Infatti, l'unione è chiara dato che $N_0 = \mathbb{N}$; per quanto riguarda l'intersezione, essa è chiaramente contenuta nell'insieme $\mathbb{N}$, ma, per ogni $x \in \mathbb{N}$ abbiamo che $x \notin N_{x+1}$, quindi, a maggior ragione, $x \notin \bigcap_{i \in \mathbb{N}} N_i$.

3) Sia $I = \mathbb{Q}_{>0} = \{a \mid a \in \mathbb{Q}\ , a > 0\ \}$ l'insieme dei numeri razionali strettamente positivi. Per ogni $a \in I$ sia $X_a = \{x \mid x \in \mathbb{R}\ ,\ x^2 \geq a\ \}$. Allora:

$$\bigcup_{a \in I} X_a = \mathbb{R} \setminus \{0\} \qquad \text{e} \qquad \bigcap_{a \in I} X_a = \emptyset.$$

Infatti, per ogni $a \in I$: $X_a \subseteq \mathbb{R} \setminus \{0\}$; viceversa, sia $y \in \mathbb{R} \setminus \{0\}$, allora $y^2 > 0$ ed è noto che quindi esiste un numero *razionale* b tale che $0 < b \leq y^2$, quindi $y \in X_b \subseteq \bigcup_{a \in I} X_a$; ciò prova che

$$\mathbb{R} \setminus \{0\} \subseteq \bigcup_{a \in I} X_a$$

e quindi l'uguaglianza.

Per provare l'affermazione riguardo all'intersezione, dopo aver osservato che ovviamente essa è un sottoinsime di $\mathbb{R}$, notiamo che, se y è un numero reale, certamente esiste un numero razionale positiv a tale che $y^2 < a$; ma allora $y \notin X_a$ e quindi $y \notin \bigcap_{a\in I} X_a$. Dunque $\bigcap_{a\in I} X_a = \emptyset$.

1.3. Prodotto cartesiano

Coppie ordinate. Siano A e B insiemi; siano $a \in A$ e $b \in B$; il simbolo (a, b) è la **coppia ordinata** la cui prima coordinata (o componente) è l'elemento a e la seconda è l'elemento b. Per definizione, due coppie ordinate (a, b) e (a', b') (con $a, a' \in A$, $b, b' \in B$) sono uguali *se e solo se* $a = a'$ e $b = b'$. Questa, come qualcuno avrà sospettato, non è una definizione rigorosa di coppia ordinata. Rimediamo dicendo che, con le notazioni di sopra, se $a \in A$ e $b \in B$, allora (a, b) è, per definizione, $\{\{a\}, \{a, b\}\}$. Il lettore cerchi di capire perché proprio questa definizione (e non altre "più semplici") è quella che esprime correttamente quanto abbiamo in mente quando pensiamo ad una "coppia ordinata", e solo tanto.

La collezione di tutte le coppie ordinate la cui prima componente appartiene all'insieme A e la seconda componente appartiene all'insieme B è un insieme, che si denota con $A \times B$, e si chiama **prodotto cartesiano** di A per B. Quindi:

$$A \times B = \{\ (a, b) \mid a \in A\ , b \in B\ \}.$$

Ad esempio, se $A = \{1, 2\}$ e $B = \{0, 1, \pi\}$; allora

$$A \times B = \{(1, 0), (1, 1), (1, \pi), (2, 0), (2, 1), (2, \pi)\}.$$

$\mathbb{R} \times \mathbb{R}$, che si denota anche con $\mathbb{R}^2$ è l'insieme di tutte le coppie ordinate di numeri reali.

Osservazioni. Siano A , B insiemi.

- $A \times \emptyset = \emptyset = \emptyset \times A$;
- se $A \neq \emptyset \neq B$, allora $A \times B = B \times A$ se e solo se $A = B$;
- se $A' \subseteq A$ e $B' \subseteq B$, allora $A' \times B' \subseteq A \times B$;

Facciamo anche una semplice ma basilare osservazione riguardo al numero di elementi di un prodotto cartesiano, nel caso di insiemi finiti. Supponiamo quindi che A e B siano insiemi finiti, con $|A| = n$ e $|B| = m$ (ricordo che ciò significa che A contiene n elementi e B ne contiene m). Possiamo elencare gli elementi di A e quelli di B, ovvero scrivere

$$A = \{a_1, a_2, \ldots, a_n\} \qquad \text{e} \qquad B = \{b_1, b_2, \ldots, b_n\}.$$

Allora il prodotto cartesiano $A \times B$ avrà come elementi tutte le coppie del tipo (a_i, b_j), con l'indice i che va da 1 a n, e l'indice j che va da 1 a m. Possiamo quindi mentalmente "costruire" gli elementi del prodotto $A \times B$ figurandoci di fissare di volta in volta la prima componente a_i della coppia (per la quale quindi abbiamo n scelte diverse), e quindi sistemare come seconda componente tutte le possibili scelte per b_j (che sono n). È chiaro dunque che in totale otterremo $n \times m = nm$ coppie distinte,

le quali costituiscono la totalità degli elementi di $A \times B$ Pertanto $|A \times B| = nm$, ed abbiamo dunque provato che

$$\textit{se } A \textit{ e } B \textit{ sono insiemi finiti, allora } \ |A \times B| = |A||B|.$$

La definizione di prodotto cartesiano puó essere estesa da due ad un numero finito arbitrario n di insiemi. Siano $A_1, A_2, \ldots, A_n$ insiemi. L'insieme

$$A_1 \times A_2 \times \cdots \times A_n = \{\ (a_1, a_2, \ldots, a_n) \mid a_i \in A_i \ \text{ per ogni } \ i = 1, 2, \ldots, n\ \}$$

è l'insieme delle n-uple ordinate la cui i-esima componente (per ogni $i = 1, \ldots, n$) appartiene all'insieme A_i.
Se tutti gli insiemi A_i coincidono con l'insieme A, allora si parla di insieme delle n-uple ordinate di A, e si denota tale insieme con A^n. Ad esempio, $\mathbb{R}^n$ è l'insieme di tutte le n-uple ordinate di numeri reali. Chiaramente due n-uple sono uguali se e solo se tutte le componenti sono corrispondentemente uguali; inoltre valgono osservazioni simili a quelle fatte sopra per le coppie, la cui esplicita formulazione lasciamo per esercizio[1].

1.4. Applicazioni

Molti dei concetti che abbiamo trattato fino a qui sono di fatto intimamente legati agli assiomi della teoria degli insiemi rigorosa; per esempio, la definizione di uguaglianza tra insiemi, l'esistenza di un insieme vuoto, l'unione di insiemi, l'insieme delle parti, la definizione di coppia ordinata. In questa sezione ne vediamo un altro, fondamentale, che è il concetto di applicazione tra insiemi. Anche in questo caso dovrebbe trattarsi di qualcosa di familiare; per cui - penso - si apprezzerà la nitidezza che un approccio rigoroso conferisce anche alle idee per le quali non ritenevamo ci fosse nulla da chiarire.

Anche in questo caso, diamo prima una definizione non completamente rigorosa. Siano A e B insiemi. Una **applicazione** (o funzione) è costituita da una coppia ordinata A, B, di insieme e da una una legge che ad **ogni** elemento di A associa, o fa corrispondere, **uno ed un solo** elemento dell'insieme B. Si scrive

$$f \ : \ A \longrightarrow B.$$

e, se all'elemento $a \in A$, f fa corrispondere l'elemento $b \in B$, si scrive $\ b = f(a)$; l'elemento b si chiama *immagine* di a tramite f.

Questa notazione si riferisce ad una generica applicazione di A in B. Volendo descrivere invece una specifica applicazione occorre anche enunciare la legge che agli elementi di A associa elementi di B. È conveniente illustrare questa modalità mediante un esempio. Supponiamo di volere introdurre l'applicazione (che vogliamo chiamare f) dall'insieme dei numeri interi nell'insieme dei numeri naturali che ad ogni numero intero associa il suo quadrato. Si usa allora uno dei due schemi seguenti:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & z & \mapsto & z^2 \end{array}$$

[1] Notiamo che, da un punto di vista strettamente formale, se A, B e C sono insiemi, allora $(A \times B) \times C \neq A \times (B \times C)$.

oppure

$$f:\ \mathbb{Z}\ \longrightarrow\ \mathbb{N}\ \text{ definita da, per ogni } z\in\mathbb{Z}:\ f(z)=z^2.$$

Se $f : A \longrightarrow B$ è un'applicazione, si dice che A è il **dominio** di f e che B è il **codominio** di f.

Due applicazioni, $f : A \longrightarrow B$ e $g : A' \longrightarrow B'$, sono **uguali** se

$$A = A'\ ,\ B = B'\ \text{ e per ogni }\ a\in A\ \text{ si ha }\ f(a)=g(a).$$

Il **grafico** $\Gamma(f)$ di un'applicazione $f : A \longrightarrow B$ è il sottoinsieme del prodotto $A \times B$:

$$\Gamma(f)=\{\ (a,b)\mid a\in A\ , b\in B\ \text{ e }\ b=f(a)\ \}.$$

È immediato verificare che due applicazioni con lo stesso dominio e lo stesso codominio sono uguali se e solo se hanno lo stesso grafico. In effetti possiamo identificare concettualmente un'applicazione con il suo grafico; cosa che consente di dare una definizione rigorosa di applicazione (che eviti, cioè, la vaghezza dei termini "legge, associa" che abbiamo usato sopra); precisamente

Definizione. Siano A e B due insiemi. Una *applicazione* (o *funzione*) di A in B è un sottoinsieme f del prodotto cartesiano $A \times B$ che soddisfa alla seguente proprietá:

$$\text{per ogni }\ a\in A\ \text{ esiste uno ed un unico }\ b\in B\ \text{ tale che }\ (a,b)\in f.$$

Quindi, se $f \subseteq A \times B$ è una applicazione si scriverà $f : A \longrightarrow B$, e per una coppia (a, b), invece di $(a, b) \in f$, si scriverà $b = f(a)$.

Se A e B sono insiemi, allora, la famiglia di tutte le applicazioni da A in B è un insieme, che si denota con B^A (dalla definizione, risulta chiaro che B^A è un sottoinsieme du $\mathcal{P}(A \times B)$).

Definizione. Sia A un insieme. L'applicazione che ad ogni elemento di A associa se stesso si chiama **identità** (o applicazione identica) di A, e si denota con ι_A o con 1_A. Quindi:

$$\begin{array}{rccc}\iota_A: & A & \longrightarrow & A\\ & a & \mapsto & a\end{array}$$

Detto altrimenti, $\Gamma(\iota_A) = \{(a, a) \mid a \in A\}$.

Più in generale, se $S \subseteq A$ l'applicazione

$$\begin{array}{rccc}f: & S & \longrightarrow & A\\ & s & \mapsto & s\end{array}$$

si chiama **immersione** di S in A.

Definizione. Sia $f : A \longrightarrow B$ un'applicazione, e sia $S \subseteq A$. Si chiama **immagine di S** tramite f, e si denota con $f(S)$, il sottoinsime di B i cui elementi sono le immagini degli elementi di S; quindi

$$f(S) = \{f(a) \mid a \in S\}.$$

L'immagine $f(A)$ dell'intero dominio di f, si chiama semplicemente **immagine di** f, e si denota anche con $Im(f)$.

Si tenga sempre ben presente che, per ogni sottoinsime non vuoto S di A, $f(S)$ è un **sottoinsime non vuoto** di B; così, se $a \in A$ e $S = \{a\}$, allora $f(S) = \{f(a)\}$.

Esempio. Sia $f : \mathbb{Z} \longrightarrow \mathbb{N}$ l'applicazione definita da, per ogni $x \in \mathbb{Z}$: $f(x) = x^2 + 1$; e sia $S = \{0, 1, -1\}$. Allora

$$f(S) = \{f(0), f(1), f(-1)\} = \{1, 2, 2\} = \{1, 2\} ,$$

$$Im(f) = \{\ x^2 + 1 \mid x \in Z\ \} = \{1, 2, 5, 10, 17, 26, 37, 50, \dots\}.$$

Definizione. Sia $f : A \longrightarrow B$ un'applicazione, e sia $Y \subseteq B$. Si chiama **immagine inversa** di Y (o controimmagine, o retroimmagine di Y) tramite f, e si denota con $f^{-1}(Y)$, il sottoinsime di A costituito dagli elementi di A la cui immagine tramite f appartiene a Y; quindi

$$f^{-1}(Y) = \{\ a \mid a \in A\ , f(a) \in Y\ \}.$$

Chiaramente: $f^{-1}(B) = A$; o meglio, se $Im(f) \subseteq Y \subseteq B$, allora $f^{-1}(Y) = A$.

Esempio. Sia $f : \mathbb{Z} \longrightarrow \mathbb{N}$ l'applicazione definita da, per ogni $x \in \mathbb{Z}$: $f(x) = x^2$;

- sia $Y = \{4\}$; allora $f^{-1}(Y) = \{2, -2\}$;

- sia $Y = \{3, 5, 8\}$; allora $f^{-1}(Y) = \emptyset$;

- sia $Y = \{0, 1, 2, 3\}$; allora $f^{-1}(Y) = \{0, 1, -1\}$;

- sia Y l'insieme dei numeri primi; allora $f^{-1}(Y) = \emptyset$.

Si tenga ben presente che, per ogni sottoinsime Y di B, $f^{-1}(Y)$ è sempre un **sottoinsime** di A che, come si vede anche da alcuni degli esempi forniti, può essere vuoto. Osserviamo anche, lasciandone la facile verifica come esercizio, che data una applicazione $f : A \longrightarrow B$ e $S \subseteq A$, $Y \subseteq B$, allora:

$$S \subseteq f^{-1}(f(S)) \qquad \text{e} \qquad f(f^{-1}(Y)) \subseteq Y.$$

Definizione. Un'applicazione $f : A \longrightarrow B$ si dice **suriettiva** se

$$\text{per ogni } b \in B \text{ esiste un } a \in A \text{ tale che } f(a) = b.$$

Quindi, $f : A \longrightarrow B$ è suriettiva se e solo se $Im(f) = B$ (ovvero se e solo se $f^{-1}(\{b\}) \neq \emptyset$ per ogni $b \in B$).

Esempi. 1) L'applicazione dell'esempio di sopra non è suriettiva: infatti $2 \notin Im(f)$ (naturalmente, in questo caso, molti altri elementi del codominio $\mathbb{N}$ non sono immagine di alcun elemento del dominio tramite f $(3, 5, 6,$ etc.); per provare che f non è suriettiva basta evidenziarne uno).

2) L'applicazione $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definita da, per ogni $x \in \mathbb{Z}$: $f(x) = |x|$, è suriettiva.

3) Sia X un insieme non vuoto e sia Y un sottoinsime fissato di X. Definiamo un'applicazione $\delta : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$, ponendo, per ogni $A \in \mathcal{P}(X)$: $\delta(A) = A \Delta Y$. Allora δ è suriettiva (lo si dimostri per esercizio).

Osserviamo che, data un'applicazione $f : A \longrightarrow B$, è sempre possibile definire in modo naturale, a partire da f, un'applicazione suriettiva $\overline{f} : A \longrightarrow f(A)$, ponendo, per ogni $x \in A$, $\overline{f}(x) = f(x)$.

Definizione. Un'applicazione $f : A \longrightarrow B$ si dice **iniettiva** se soddisfa:

$$\text{per ogni } x, y \in A: \quad \text{se } x \neq y \text{ allora } f(x) \neq f(y).$$

Equivalentemente (ed è questo ciò che usualmente si adotta in pratica), un'applicazione $f : A \longrightarrow B$ è iniettiva se e solo se

$$\text{per ogni } x, y \in A: \quad \text{se } f(x) = f(y) \text{ allora } x = y.$$

Esempi. 1) L'applicazione $f : \mathbb{Z} \longrightarrow \mathbb{N}$, definita da, per ogni $x \in \mathbb{Z}$, $f(x) = x^2$, non è iniettiva: infatti, ad esempio, $f(-1) = 1 = f(1)$.

2) L'applicazione $g : \mathbb{N} \longrightarrow \mathbb{Z}$, definita da, per ogni $x \in \mathbb{Z}$: $f(x) = x^2$, è iniettiva: infatti, se x, y sono numeri naturali tali che $x^2 = y^2$, allora $x = y$.

3) L'applicazione $\delta : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ definita di sopra è iniettiva.

Definizione. Un'applicazione $f : A \longrightarrow B$ si dice **biettiva** se è *iniettiva e suriettiva.*

Ad esempio, è biettiva l'applicazione $g : \mathbb{Z} \longrightarrow \mathbb{Z}$, definita da, per ogni $x \in \mathbb{Z}$, $f(x) = x+2$; ed è biettiva l'applicazione $\delta : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ considerata in precedenti esempi.

Esercizio 1.2. Siano X, Y insiemi (non vuoti), e $f : X \longrightarrow Y$ un'applicazione. Si dimostri che f è iniettiva se e solo se per ogni $T \subseteq X$, $f(X \setminus T) \subseteq Y \setminus f(T)$.

Soluzione. Supponiamo che f soddisfi le ipotesi dell'esercizio, e siano $a, b \in X$ con $a \neq b$. Posto $T = \{b\}$ si ha allora $a \in X \setminus T$ e quindi, per ipotesi, $f(a) \in f(X \setminus T) \subseteq Y \setminus f(T)$. Dunque $f(a) \notin f(T) = f(\{b\}) = \{f(b)\}$ e quindi $f(a) \neq f(b)$ provando che f è iniettiva. Viceversa, sia f iniettiva. Sia $T \subseteq X$; e, ragionando per assurdo, supponiamo $f(X \setminus T) \not\subseteq Y \setminus f(T)$. Allora. $f(X \setminus T) \cap f(T) \neq \emptyset$; quindi esiste $b \in f(X \setminus T) \cap f(T)$. Ma allora esistono $x \in X \setminus T$, e $t \in T$, tali che $f(x) = b = f(t)$, il che contraddice l'initettività di f, dato che, certamente, $x \neq t$.

Il concetto di applicazione biettiva è fondamentale; le applicazioni biettive sono quelle che, nel senso che specificheremo più avanti, si possono 'invertire'.

1.5. Composizione di applicazioni.

La composizione di applicazioni è un altra di quelle tecniche di base, che si usano regolarmente e sono già familiari dalla pratica nelle scuole superiori. Costituisce poi uno dei riferimenti esemplari per l'idea di operazione.

Definizione. Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$, due applicazioni (si osservi che si assume che il domino di g coincida col codominio di f). L'**applicazione composta** $g \circ f$ (si legge "g composta a f") è l'applicazione

$$g \circ f : A \longrightarrow C$$

definita da, per ogni $a \in A$:

$$(g \circ f)(a) = g(f(a)).$$

Siano, ad esempio,

$f : \mathbb{Z} \longrightarrow \mathbb{N}$ definita da $f(z) = |z|$

$g : \mathbb{N} \longrightarrow \mathbb{Z}$ definita da $g(x) = -x$;

allora

$g \circ f : \mathbb{Z} \longrightarrow \mathbb{Z}$ è tale che, per ogni $z \in \mathbb{Z}$: $g \circ f(z) = g(f(z)) = g(|z|) = -|z|$;

$f \circ g : \mathbb{N} \longrightarrow \mathbb{N}$ è tale che, per ogni $x \in \mathbb{N}$: $f \circ g(x) = f(g(x)) = f(-x) = |-x| = x$; (l'ultima uguaglianza deriva dal fatto che, poichè $x \in \mathbb{N}$, x è positivo. Si osservi che $f \circ g = \iota_{\mathbb{N}}$).

L'esempio precedente mostra anche che, in generale, $g \circ f \neq f \circ g$. Questo è il caso anche quando, ed è la situazione più interessante, $A = B = C$. Ad esempio, sia $A = \{1, 2, 3\}$, e consideriamo le due applicazioni $\gamma, \tau : A \longrightarrow A$, definite da:

$$\gamma(1) = 2 \ ; \ \gamma(2) = 3 \ ; \ \gamma(3) = 1 \ ; \quad \text{e} \quad \tau(1) = 1 \ ; \ \tau(2) = 3 \ ; \ \tau(3) = 2$$

(si osservi che si tratta di biezioni di A in se stesso). Allora $\gamma \circ \tau \neq \tau \circ \gamma$; infatti:

$$\gamma \circ \tau(1) = \gamma(\tau(1)) = \gamma(1) = 2 \quad \text{mentre} \quad \tau \circ \gamma(1) = \tau(\gamma(1)) = \tau(2) = 3.$$

Proposizione 1.6. *Siano A, B insiemi; $f : A \longrightarrow B$ un'applicazione; ι_A, ι_B le applicazioni identiche su A e su B rispettivamente. Allora*

1) $\iota_B \circ f = f$;

2) $f \circ \iota_A = f$.

Dimostrazione. È ovvia. ∎

Proposizione 1.7. *(Associatività della composizione) Siano A, B, C e D insiemi; $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \longrightarrow D$ applicazioni. Allora*

$$h \circ (g \circ f) = (h \circ g) \circ f \ .$$

Dimostrazione. Innanzitutto osserviamo che sia $h \circ (g \circ f)$ che $(h \circ g) \circ f$ sono applicazioni con dominio A e codominio D. Ora, per ogni $a \in A$:

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a) \ ;$$

Quindi $h \circ (g \circ f) = (h \circ g) \circ f$. ∎

Proposizione 1.8. *Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$ due applicazioni.*

1) *Se f e g sono iniettive, allora $g \circ f$ è iniettiva;*

2) *se f e g sono suriettive, allora $g \circ f$ è suriettiva;*

3) *se f e g sono biettive, allora $g \circ f$ è biettiva.*

Dimostrazione. (1) Siano f e g iniettive, e siano $a, a' \in A$ tali che

$$(g \circ f)(a) = (g \circ f)(a') \ ,$$

ciò significa : $g(f(a)) = g(f(a'))$. Quindi, poichè g è iniettiva:

$$f(a) = f(a')$$

da cui, poichè f è iniettiva :

$$a = a'$$

provando pertanto che $g \circ f$ è iniettiva.

(2) Siano f e g suriettive, e sia $c \in C$. Poichè g è suriettiva, esiste $b \in B$ tale che $c = g(b)$, e, poichè f è suriettiva, esiste $a \in A$ tale che $b = f(a)$. Ma allora:

$$g \circ f(a) = g(f(a)) = g(b) = c$$

provando pertanto che $g \circ f$ è suriettiva.

(3) Segue immediatamente dai punti (1) e (2). ∎

La Proposizione 1.8 può solo parzialmente essere invertita. Si veda l'esercizio 1.43 al termine del capitolo.

* * *

Dal punto di vista della composizione, il concetto di applicazione biettiva è fondamentale; le applicazioni biettive sono quelle che, nel senso che specificheremo tra poco, si possono 'invertire'.

Proposizione 1.9. *Sia $f : A \longrightarrow B$ un'applicazione; supponiamo che esistano applicazioni $g,\ h : B \longrightarrow A$ tali che $g \circ f = \iota_A$ e $f \circ h = \iota_B$. Allora $g = h$.*

Dimostrazione. Siano f, g e h come nelle ipotesi. Allora,

$$h = \iota_A \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \iota_B = g.$$

∎

Definizione Un'applicazione $f : A \longrightarrow B$ si dice **invertibile** se esiste una applicazione $g : B \longrightarrow A$ tale che

$$g \circ f = \iota_A \quad \text{e} \quad f \circ g = \iota_B.$$

Dalla Proposizione 1.9 segue subito l'importante osservazione che

> se f è invertibile allora esiste una **unica** applicazione $g : B \longrightarrow A$ tale che $g \circ f = \iota_A$ e $f \circ g = \iota_B$. Tale applicazione g si chiama l'applicazione **inversa** di f, e si denota con f^{-1}.

Veniamo ora al risultato fondamentale.

Teorema 1.10. *Una applicazione è invertibile se e soltanto se è biettiva.*

Dimostrazione. Sia $f : A \longrightarrow B$ un'applicazione.

1) Supponiamo che f sia invertibile, e sia $f^{-1} : B \longrightarrow A$ la sua inversa. Allora, se $b \in B$, posto $a = f^{-1}(b)$, si ha

$$f(a) = f(f^{-1}(b)) = (f \circ f^{-1})(b) = \iota_B(b) = b.$$

Quindi f è suriettiva. Siano ora $a, a' \in A$ tali che $f(a) = f(a')$. Allora

$$a = \iota_A(a) = (f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(f(a')) = (f^{-1} \circ f)(a') = \iota_A(a') = a'$$

che dimostra che f è iniettiva. Dunque f è biettiva.

2) Supponiamo ora che f sia biettiva e proviamo che allora ha una inversa. Sia b un qualunque elemento di B; allora, poiché f è suriettiva, esiste un elemento $a \in A$ tale che $f(a) = b$. D'altra parte, poiché f è iniettiva, tale elemento è unico (per ciascun b), e lo denotiamo quindi con $g(b)$. Per costruzione, l'applicazione

$$\begin{array}{ccc} B & \longrightarrow & A \\ b & \mapsto & g(b) \end{array}$$

è l'inversa di f. ∎

Il Teorema precedente può essere reso più preciso mediante l'introduzione (con l'ovvio significato) dei concetti di "inversa destra" e "inversa sinistra", e la seguente proposizione, che lasciamo ai lettori più interessati (si osservi anche il punto (2) dell'esercizio 1.28).

Proposizione 1.11. *Sia $f : A \longrightarrow B$ un'applicazione. Allora*

1) *f è iniettiva se e solo se esiste $g : B \longrightarrow A$ tale che $g \circ f = \iota_A$;*

2) *f è suriettiva se e solo se esiste $h : B \longrightarrow A$ tale che $f \circ h = \iota_B$.*

Dimostrazione. (1) Supponiamo che f sia iniettiva. Fissiamo un elemento $a \in A$, e definiamo una applicazione $g : B \longrightarrow A$, ponendo, per ogni $y \in B$,

$$g(y) = \begin{cases} a \quad \text{se} \quad y \in B \setminus f(A) \\ \\ \text{l'unico} \ \ x \in A \text{ tale che } f(x) = y \text{ se } \ y \in f(A) \end{cases}$$

Allora, per ogni $x \in A$: $g \circ f(x) = g(f(x)) = x$; e quindi $g \circ f = \iota_A$.

Viceversa, si provi per esercizio che se esiste $g : B \longrightarrow A$ tale che $g \circ f = \iota_A$, allora f è iniettiva.

(2) Supponiamo che f sia suriettiva. Allora per ogni $y \in B$ esiste almeno un elemento $a_y \in A$ tale che $f(a_y) = y$. Definiamo quindi $h : B \longrightarrow A$, ponendo, per ogni $y \in B$, $h(y) = a_y$. Abbiamo allora che $f \circ h(y) = f(h(y)) = f(a_y) = y$ per ogni $y \in B$, e quindi $f \circ h = \iota_B$.

Viceversa, si provi per esercizio che se esiste $h : B \longrightarrow A$ tale che $f \circ h = \iota_B$ allora f è suriettiva. ∎

Corollario 1.12. *Siano A e B insiemi. Allora esiste una applicazione iniettiva da A in B se e solo se esiste una applicazione suriettiva da B in A.*

Vediamo ora alcuni esempi.

1. Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ definita da, per ogni $x \in \mathbb{Q}$, $f(x) = 2x - 1$. Si verifica senza difficoltà che f è biettiva. Determiniamo la sua inversa $f^{-1} : \mathbb{Q} \longrightarrow \mathbb{Q}$. Poiché $f \circ f^{-1}$ deve essere la applicazione identica su $\mathbb{Q}$, si dovrà avere, per ogni $y \in \mathbb{Q}$:

$$y = f(f^{-1}(y)) = 2 \cdot f^{-1}(y) - 1$$

da cui, risolvendo una elementare equazione, si ricava:

$$f^{-1}(y) = \frac{y+1}{2} \ , \ \text{per ogni } y \in \mathbb{Q}$$

che è la regola che definisce l'applicazione inversa $f^{-1} : \mathbb{Q} \longrightarrow \mathbb{Q}$.

2. Sia $A = \mathbb{Q} \setminus \{1\}$ e sia $f : A \longrightarrow A$ definita da, per ogni $x \in A,:\ f(x) = \frac{x+1}{x-1}$. Allora f è invertibile e coincide con la propria inversa. Infatti, per ogni $x \in A$ si ha :

$$(f \circ f)(x) = f(f(x)) = f(\frac{x+1}{x-1}) = \frac{\frac{x+1}{x-1} + 1}{\frac{x+1}{x-1} - 1} = \frac{x+1+x-1}{x+1-x+1} = \frac{2x}{2} = x$$

quindi $f \circ f = \iota_A$ e dunque $f^{-1} = f$.

Concludiamo questa sezione con alcune proprietà fondamentali (e facili) dell'inversa.

Proposizione 1.13. *Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$ applicazioni invertibili. Allora:*

(1) *f^{-1} è invertibile e $(f^{-1})^{-1} = f$;*

(2) *$g \circ f$ è invertibile e $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Dimostrazione. (1) è ovvia. Dimostriamo (2).
Poichè f e g sono invertibili, esse sono biettive per il Teorema 1.10, quindi, per la Proposizione 1.8, $g \circ f : A \longrightarrow C$ è biettiva e dunque, ancora per il Teorema 1.10, è invertibile. Ora, osserviamo che:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = (g \circ (f \circ f^{-1})) \circ g^{-1} = (g \circ \iota_B) \circ g^{-1} = g \circ g^{-1} = \iota_C$$

ed allo stesso modo :

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (\iota_B \circ f) = f^{-1} \circ f = \iota_A$$

Dunque, per la unicità della applicazione inversa:

$$f^{-1} \circ g^{-1} = (g \circ f)^{-1},$$

che dimostra il punto (2) ■

Esercizio 1.3. Siano A, B e C insiemi non vuoti, e $f : A \longrightarrow B$ una applicazione fissata. Sia C^B l'insieme di tutte le applicazioni da B in C, e C^A quello di tutte le applicazioni da A in C. Sia $\phi : C^B \longrightarrow C^A$ l'applicazione definita da $\phi(g) = g \circ f$ per ogni $g \in C^B$. Si provi che se f è suriettiva, allora ϕ è iniettiva.

Soluzione. Supponiamo che f sia suriettiva, e proviamo che ϕ è iniettiva. Siano quindi $g_1, g_2 \in C^B$ tali che $\phi(g_1) = \phi(g_2)$ (cioè $g_1 \circ f = g_2 \circ f$). Proviamo che $g_1 = g_2$.
1^o metodo). Sia $b \in B$. Poichè f è suriettiva, esiste $a \in A$ tale che $f(a) = b$. Da ciò segue $g_1(b) = g_1(f(a)) = g_1 \circ f(a) = g_2 \circ f(a) = g_2(f(a)) = g_2(b)$.
Poichè ciò vale per ogni $b \in B$ si ricava $g_1 = g_2$.
2^o metodo). Poichè f è suriettiva, esiste una applicazione $h : B \longrightarrow A$ tale che $f \circ h = \iota_B$. Allora
$g_1 = g_1 \circ \iota_B = g_1 \circ (f \circ h) = (g_1 \circ f) \circ h = (g_2 \circ f) \circ h = g_2 \circ (f \circ h) = g_2 \circ \iota_B = g_2$
provando che ϕ è iniettiva.

Esercizio 1.4. Nelle stesse ipotesi dell'esercizio precedente, provare che se f è iniettiva allora ϕ è suriettiva.

1.6. Cardinalità di insiemi.

Si dice che due insiemi A e B hanno la stessa cardinalità (oppure che sono **equipotenti**) se esiste una applicazione *biettiva* $f : A \longrightarrow B$. In tal caso si scrive $|A| = |B|$.

Dalle proprietà delle applicazioni biettive segue che la relazione di equipotenza gode delle proprietà delle equivalenze (anche se non è una equivalenza in senso rigoroso dato che non è definita su un insieme); cioè per ogni A, B, C insiemi :
- A è equipotente a se stesso (tramite l'applicazione identica ι_A);
- se A è equipotente a B , allora B è equipotente a A (tramite la applicazione inversa);
- se A è equipotente a B , e B è equipotente a C , allora A è equipotente a C (tramite la applicazione composta).

Definizione Un insieme A è finito di **ordine** (o **cardinalità**) n, se esiste $n \in \mathbb{N}$, ed una biezione tra A e l'insieme $\{1, 2, \ldots, n\}$; in questo caso si scrive $|A| = n$.

Definizione Un insieme A si dice **numerabile** se esiste una biezione tra A e l'insieme $\mathbb{N}$ dei numeri naturali.

Esempi. (1) Sia $X = \mathbb{N} \setminus \{0\}$. L'applicazione $f : \mathbb{N} \longrightarrow X$ definita da $f(n) = n + 1$ è biettiva. Quindi l'insieme dei numeri naturali $\mathbb{N}$ è equipotente ad un suo sottoinsieme proprio. Questa eventualità non si può verificare negli insiemi finiti; si può facilmente provare che un insieme è infinito se e solo se è equipotente ad un suo sottoinsieme proprio (anzi, questa proprietà può essere assunta come definizione di un insieme infinito).

(2) L'applicazione definita nell'esercizio 1.15 è una biezione da $\mathbb{N}$ in $\mathbb{Z}$, quindi l'insieme $\mathbb{Z}$ dei numeri interi è numerabile.

Proposizione 1.14. *Sia A un insieme numerabile. Allora anche $A \times A$ è numerabile.*

Dimostrazione. Sia A un insieme numerabile, e sia $f : \mathbb{N} \to A$ una biezione. Allora, si verifica facilmente che l'applicazione

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & A \times A \\ (a, b) & \mapsto & (f(a), f(b)) \end{array}$$

è una biezione. Quindi $|A \times A| = |\mathbb{N} \times \mathbb{N}|$. Pertanto è sufficiente provare che $\mathbb{N} \times \mathbb{N}$ è numerabile.
Ora, ogni numero naturale $n \geq 1$ può essere scritto in uno ed un sol modo nella forma $n = 2^a m$ con m dispari. Da ciò segue che l'applicazione

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \setminus \{0\} \\ (a, b) & \mapsto & 2^a(2b + 1) \end{array}$$

è una biezione. Poiché $\mathbb{N} \setminus \{0\}$ è numerabile, si conclude che $\mathbb{N} \times \mathbb{N}$ è numerabile. ∎

La proprietà seguente non è difficile da provare (tuttavia ne ometto la dimostrazione).

Proposizione 1.15. *(1) Ogni sottoinsieme di un insieme numerabile è finito o numerabile.*

(2) Siano A, B insiemi e $f : A \longrightarrow B$ una applicazione suriettiva. Se A è numerabile allora B è finito o numerabile.

Vale anche la seguente:

Proposizione 1.16. *L'unione di una famiglia finita o numerabile di insiemi finiti o numerabili è finita o numerabile.*

Dimostrazione. Discutiamo il caso di una unione di una famiglia numerabile di insiemi finiti o numerabili (il caso di una famiglia finita è chiaramente più semplice). Sia quindi I un insieme numerabile, $\lambda : \mathbb{N} \longrightarrow I$ una biezione e, per ogni $i \in I$, sia A_i un insieme finito o numerabile. Per ogni $i \in I$ c'è quindi una applicazione suriettiva $\phi_i : \mathbb{N} \longrightarrow A_i$. Consideriamo

$$A = \bigcup_{i \in I} A_i$$

Definiamo ora l'applicazione

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & A \\ (n, m) & \mapsto & \phi_{\lambda(n)}(m) \end{array}$$

Si vede facilmente che tale applicazione è suriettiva, quindi A è numerabile per la seconda parte della Proposizione 1.15. ∎

Vediamo ora cosa si può dire a proposito della cardinalità dell'insieme dei numeri razionali, e di quello dei numeri reali.

Proposizione 1.17. *L'insieme $\mathbb{Q}$ dei numeri razionali è numerabile.*

Dimostrazione. Osserviamo che ogni numero razionale $a \neq 0$ si scrive in modo unico nella forma $a = \frac{m(a)}{n(a)}$ con $m(a) \in \mathbb{Z}$, $n(a) \in \mathbb{N}$ e $MCD(m(a), n(a)) = 1$. Quindi la applicazione

$$f : \mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{Z}$$

definita da

$$f(0) = (0, 0) \text{ e, per ogni } 0 \neq a \in \mathbb{Q},\ f(a) = (m(a), n(a))$$

è iniettiva; dunque, posto $Y = f(\mathbb{Q})$, abbiamo $|Y| = |\mathbb{Q}|$. Ora $Y \subseteq \mathbb{Z} \times \mathbb{Z}$. Ma $\mathbb{Z}$ è numerabile per l'esempio (2), quindi $\mathbb{Z} \times \mathbb{Z}$ è numerabile per la Proposizione 1.14, e dunque Y è numerabile per la Proposizione 1.15.

Proposizione 1.18. *L'insieme $\mathbb{R}$ dei numeri reali non è numerabile.*

Dimostrazione. Per la proposizione 1.15, è sufficiente dimostrare che un sottoinsieme di $\mathbb{R}$ non è numerabile. Vediamo che non è numerabile l'intervallo

$$A = (0, 1] = \{\ x \mid x \in \mathbb{R}\ , 0 < x \leq 1\ \}\ .$$

Osserviamo che ogni $x \in A$ ha una rappresentazione decimale del tipo $0, x_0 x_1 x_2 \ldots$, con $x_i \in \{0, 1, 2, \ldots, 9\}$ (si tenga presente che $1 = 0,999999\ldots$). Tale rappresentazione è unica se si conviene che non debba avere un numero finito di cifre diverse

da zero (cioè conveniamo, ad esempio, di scrivere $0,24457 = 0,244569999\ldots$) Supponiamo per assurdo che esita una applicazione biettiva $f : \mathbb{N} \longrightarrow A$, allora per ogni $n \in \mathbb{N}$ si può scrivere

$$f(n) = 0, x_{n,0}x_{n,1}x_{n,2}\ldots$$

con $x_{n,i} \in \{0, 1, 2, \ldots, 9\}$.
Ora, per ogni $i \in \mathbb{N}$ si scelga un numero naturale

$$a_i \in \{0, 1, 2, \ldots, 9\} \quad \text{con} \quad a_i \neq 0, x_{i,i}$$

e si consideri il numero reale, appartenente ad A :

$$y = 0, a_0a_1a_2a_3\ldots$$

Poichè f è una biezione, esiste $k \in \mathbb{N}$ tale che $y = f(k) = 0, x_{k,0}x_{k,1}x_{k,2}\ldots$; ma allora $x_{k,k} = a_k$ che è una contraddizione.
Quindi una tale f non esiste e dunque $A = [0, 1]$ non è numerabile.

Quest'ultima tecnica dimostrativa è chiamata a volte 'procedimento diagonale', e in sostanza è ciò che si utilizza per provare il famoso Teorema di Cantor.

Teorema (di Cantor). *Sia A un insieme e sia $\mathcal{P}(A)$ l'insieme delle parti di A. Allora $|\mathcal{P}(A)| \neq |A|$.*

Dimostrazione. Sia A un insieme e supponiamo, per assurdo, che esista una biezione

$$f : A \longrightarrow \mathcal{P}(A).$$

Si consideri $U = \{a \in A \mid a \notin f(a)\}$. U è un sottoinsieme di A, quindi, poiché f è suriettiva, esiste $x \in A$ tale che $U = f(x)$. Ora, deve verificarsi una delle seguenti possibilità: $x \in U$, oppure $x \notin U$. Supponiamo che $x \in U$, in tal caso, per definizione di U, $x \notin f(x) = U$, il che è assurdo. Sia quindi $x \notin U = f(x)$, allora, ancora per la definizione di U si ha l'assurdo $x \in U$. Queste contraddizioni provano che una tale f non esiste, e dunque che $|\mathcal{P}(A)| \neq |A|$. ∎

In particolare quindi, $\mathcal{P}(\mathbb{N})$ non è numerabile. Si dice che un insieme X ha la **cardinalità del continuo** se $|X| = |\mathcal{P}(\mathbb{N})|$. Non sarebbe difficile dimostrare che $\mathbb{R}$ ha la cardinalità del continuo.

1.7. Esercizi.

Esercizio 1.5. Si dica quali fra le seguenti affermazioni sono vere.

- $\emptyset \in \{\emptyset, 2\}$;
- $\emptyset \subseteq \{\emptyset, \{\emptyset\}\}$;
- $\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$;
- $\{1\} \in \{1, 2\}$;
- $\{\{1\}\} \subseteq \{1, 2\}$;
- $\emptyset = \{\ x \mid x \in \mathbb{Z}, x^2 < 1\ \}$;
- $\emptyset = \{\ x \mid \{1, x\} = \{1, 2, 3\}\ \}$;

Esercizio 1.6. Si descrivano gli insiemi $\mathcal{P}(\{1,2,3,4\})$, e $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

Esercizio 1.7. Siano A, B insiemi. Si provi che $A \subseteq B$ se e solo se $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Esercizio 1.8. Siano A, B e C insiemi. Si provi che $(A \cup B) \cap C = A \cup (B \cap C)$ se e solo se $A \subseteq C$.

Esercizio 1.9. Siano A e B insiemi. Si provi che $A \setminus B = B \setminus A$ se e solo se $A = B$.

Esercizio 1.10. Siano A e B insiemi. Si provi che $A \setminus (A \setminus B) = A \cap B$.

Esercizio 1.11. Siano A e B insiemi. Si provi che

$$P(A) \cap P(B) = P(A \cap B)$$

$$P(A) \cup P(B) \subseteq P(A \cup B);$$

e si mostri che, nel caso della unione, in genere non vale l'uguaglianza.

Esercizio 1.12. Siano A, B e C insiemi. Si provi che $A \setminus B = A \setminus C$ se e solo se $A \cap B = A \cap C$.

Esercizio 1.13. Siano A, B e C insiemi. Si provi che $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

Esercizio 1.14. Siano A e B insiemi. Si dimostri che $(A \setminus B) \cup (A \cap B) = A$.

Esercizio 1.15. Siano X, Y insiemi. Si dimostri che le seguenti condizioni sono equivalenti:

1) $X \setminus Y = X$

2) $Y \setminus X = Y$

3) $X \cap Y = \emptyset$

Esercizio 1.16. Siano A, B e C insiemi. Si provi che le seguenti condizioni sono equivalenti:

1. $(A \setminus B) \setminus C = A \setminus (B \setminus C)$;
2. $(A \triangle B) \setminus C = A \triangle (B \setminus C)$;
3. $A \cap C = \emptyset$.

Esercizio 1.17. Siano A, B e C insiemi. Si dimostri che:

a) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$

b) $(A \cap B) \Delta (A \cap C) = A \cap C$ se e solo se $A \cap B = \emptyset$.

Esercizio 1.18. Siano A, B e C insiemi. Si provi che $\mathcal{P}(A \setminus (B \cup C)) = \mathcal{P}(A \setminus B) \cap \mathcal{P}(A \setminus C)$.

Esercizio 1.19. Per ogni intero n, sia $D_n = \{d \mid d \in \mathbb{Z} \text{ e } d \text{ divide } n\}$. Si provi che

$$\bigcup_{n \in \mathbb{Z}} (\mathbb{Z} \setminus D_n) = \mathbb{Z} \setminus \{1, -1\}.$$

Esercizio 1.20. Per ogni $n \in \mathbb{N}$ sia $T_n = \{ (x,y) \in \mathbb{R}^2 \mid y \leq nx \}$. Determinare

$$\bigcup_{n\in\mathbb{N}} T_n \quad \text{e} \quad \bigcap_{n\in\mathbb{N}} T_n.$$

Esercizio 1.21. Sia $\mathbb{N}_o$ l'insieme dei numeri naturali diversi da zero.
Per ogni $n \in \mathbb{N}_o$, sia $A_n = \{x \mid x \in \mathbb{Q} \text{ e } nx \in \mathbb{Z}\}$. Si determinino:

$$\bigcup_{n\in\mathbb{N}_o} A_n \qquad \text{e} \qquad \bigcap_{n\in\mathbb{N}_o} A_n.$$

Esercizio 1.22. Sia $\mathbb{N}_o$ l'insieme dei numeri naturali diversi da zero.
Per ogni $n \in \mathbb{N}_o$, sia $B_n = \{ x | x \in \mathbb{R} \text{ e } \frac{1}{n} \leq |x| \leq n \}$. Si determinino:

$$\bigcup_{n\in\mathbb{N}_o} B_n \qquad \text{e} \qquad \bigcap_{n\in\mathbb{N}_o} B_n.$$

Esercizio 1.23. Siano A, B e C insiemi. Si provi che

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

Esercizio 1.24. Siano X, Y insiemi non vuoti, e $f : X \longrightarrow Y$ un'applicazione. Si dimostri che f è suriettiva se e solo se, per ogni $T \subseteq X$. $Y \setminus f(T) \subseteq f(X \setminus T)$.

Esercizio 1.25. Si dica quali fra le seguenti applicazioni sono suriettive.

(*a*) $f : \mathbb{N} \longrightarrow \mathbb{N}$, definita da $f(x) = 3x$, per ogni $x \in \mathbb{N}$.

(*b*) $g : \mathbb{Q} \longrightarrow \mathbb{Q}$, definita da $g(x) = \frac{x-2}{2}$, per ogni $x \in \mathbb{Q}$.

(*c*) $h : \mathbb{N} \longrightarrow \mathbb{Q}^+$, definita da $h(x) = \frac{x}{x+1}$, per ogni $x \in \mathbb{N}$
(dove $\mathbb{Q}^+ = \{x \mid x \in \mathbb{Q},\ 0 < x\}$).

(*d*) $\eta : \mathbb{N} \longrightarrow \mathbb{N}$, definita da, per ogni $n \in \mathbb{N}$,

$$\eta(n) = \begin{cases} 2n & \text{se } n \text{ è pari} \\ 3n & \text{se } n \text{ è dispari} \end{cases}$$

Esercizio 1.26. Si dica quali fra le applicazioni dell'esercizio precedente sono iniettive.

Esercizio 1.27. Si dimostri che l'applicazione $f : \mathbb{N} \longrightarrow \mathbb{Z}$, definita da:

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari} \end{cases}$$

è biettiva.

Esercizio 1.28. Siano $f, g : \mathbb{N} \to \mathbb{N}$ definite da, per ogni $n \in \mathbb{N}$:

$$f(n) = \begin{cases} n+10 & \text{se } n \leq 9 \\ n-10 & \text{se } n \geq 10 \end{cases}$$

$$g(n) = n + 10\ .$$

(1) Si calcoli $f \circ g$ e $g \circ f$.

(2) Si dica se esiste $h : \mathbb{N} \to \mathbb{N}$ tale che $h \circ f = \iota_{\mathbb{N}}$.

Esercizio 1.29. Si determini l'applicazione inversa dell'applicazione f definita nell'esercizio 1.42.

Esercizio 1.30. Siano $f : \mathbb{Q}\setminus\{0\} \longrightarrow \mathbb{Q}\setminus\{0\}$ e $g : \mathbb{Q}\setminus\{0\} \longrightarrow \mathbb{Q}\setminus\{1\}$ le applicazioni definite da, per ogni $x \in \mathbb{Q} \setminus \{0\}$,

$$f(x) = \frac{1}{x} \quad \text{e} \quad g(x) = x + 1.$$

Si provi che l'applicazione composta $g \circ f$ è biettiva e si determini la sua inversa.

Esercizio 1.31. Sia $f : A \longrightarrow B$ un'applicazione, e siano $S, T \subseteq A$. Si provi che

$$\begin{array}{ll} (1) & f(S \cup T) = f(S) \cup f(T); \\ (2) & f(S \cap T) \subseteq f(S) \cap f(T); \\ (3) & f(S) \setminus f(T) \subseteq f(S \setminus T); \end{array}$$

e si mostri, mediante opportuni esempi che le inclusioni ai punti $(2), (3)$ possono essere proprie.

Esercizio 1.32. Sia $f : A \longrightarrow B$ un'applicazione. Si provi che f è iniettiva se e soltanto se $f(X) \cap f(Y) = f(X \cap Y)$ per ogni $X, Y \subseteq A$.

Esercizio 1.33. Sia $f : A \longrightarrow B$ un'applicazione, e siano $X, Y \subseteq B$. Si provi che

$$\begin{array}{ll} (1) & f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y); \\ (2) & f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y); \\ (3) & f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y). \end{array}$$

Esercizio 1.34. Sia $f : A \longrightarrow B$ un'applicazione. Si dimostri che:

(i) f è iniettiva se e solo se $f^{-1}(f(S)) = S$ per ogni $S \subseteq A$;

(i) f è suriettiva se e solo se $f(f^{-1}(Y)) = Y$ per ogni $Y \subseteq B$.

Esercizio 1.35. Sia $f : X \longrightarrow Y$ un';applicazione, e siano $A \subseteq X$ e $B \subseteq Y$. Si dica, motivando opportunamente le risposte quali fra le seguenti affermazioni sono vere:

(a) se $f(A) \subseteq B$ allora $A \subseteq f^{-1}(B)$;

(b) se $f^{-1}(B) \subseteq A$ allora $f(A) \subseteq B$;

(c) se A è infinito allora $f(A)$ è infinito;

(d) se $f^{-1}(B)$ è infinito allora B è infinito;

(e) se B è infinito allora $f^{-1}(B)$ è infinito.

Esercizio 1.36. Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ l'applicazione definita da, per ogni $x \in \mathbb{Q}$,

$$f(z) = \frac{2x}{|x| + 1}.$$

Si dica se f è iniettiva e/o suriettiva.

Esercizio 1.37. Sia X un insieme non vuoto e siano f, g due applicazioni di X in X. Si provi che se $f^{-1}(\{y\}) \subseteq g^{-1}(\{y\})$ per ogni $y \in X$, allora $f = g$.

Esercizio 1.38. Sia X un insieme infinito e siano f, g due applicazioni di X in X. Si provi che se $f^{-1}(A) \subseteq g^{-1}(A)$ per ogni sottinsieme infinito A di X, allora $f = g$.

Esercizio 1.39. Sia $I_{12} = \{x \mid x \in \mathbb{N} \ ; \ 0 \leq x \leq 12\}$, e sia $A = \mathcal{P}(I_{12})$ l'insieme delle parti di I_{12}. Sia $\phi : A \longrightarrow A$ l'applicazione definita da $\phi(X) = X \cup \{0, 1, 2\}$, per ogni $X \in A$. Posto $I_4 = \{x \mid x \in \mathbb{N} \ ; \ 0 \leq x \leq 4\}$ e $B = \mathcal{P}(I_4)$ (come sottoinsieme di A), si determini $\phi^{-1}(B)$.

Esercizio 1.40. Siano $f, g : \mathbb{Z} \to \mathbb{Z}$ due applicazioni. Si definisca $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ ponendo, per ogni $(a, b) \in \mathbb{Z} \times \mathbb{Z}$:

$$\phi(a, b) = (f(a) + g(b), f(a) - g(b)) \ .$$

(a) Si provi che ϕ è iniettiva se e solo se f, g sono entrambe iniettive.

(b) Si trovino due applicazioni suriettive f, g tali che ϕ non è suriettiva.

Esercizio 1.41. Si dimostri che l'applicazione

$$\begin{array}{rccc} f: & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \times \mathbb{Z} \\ & (x, y) & \mapsto & (3x + 4y, x + 2y) \end{array}$$

è iniettiva ma non suriettiva.

Esercizio 1.42. Si dimostri che l'applicazione

$$\begin{array}{rccc} f \ : & \mathbb{Q} \times \mathbb{Q} & \longrightarrow & \mathbb{Q} \times \mathbb{Q} \\ & (x, y) & \mapsto & (3x + 4y, x + 2y) \end{array}$$

è biettiva.

Esercizio 1.43. Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$ applicazioni. Si dimostri che:

(i) se $g \circ f$ è iniettiva allora f è iniettiva;

(ii) se $g \circ f$ è suriettiva allora g è suriettiva.

Si completi poi l'analisi, trovando degli esempi in cui g non è iniettiva ma $g \circ f$ è iniettiva, e in cui f non è suriettiva ma $g \circ f$ è suriettiva.

Esercizio 1.44. Sia $A = \mathbb{R} \times \mathbb{R}$; si provi che l'applicazione $f : A \longrightarrow \mathbb{R}$ definita da $f(x, y) = x^2 - y$, per ogni $(x, y) \in A$ è suriettiva ma non iniettiva; per ogni $b \in \mathbb{R}$ si descriva $f^{-1}(\{b\})$. Si definisca quindi una applicazione $g : \mathbb{R} \longrightarrow A$ tale che $f \circ g = \iota_{\mathbb{R}}$, e si provi che tale g non è unica.

Esercizio 1.45. Si dimostri che l'applicazione $h : \mathbb{Q} \longrightarrow \mathbb{Q}$, definita da $h(x) = 3x - |x|$, per ogni $x \in \mathbb{Q}$, è biettiva, e si determini la sua inversa.

Esercizio 1.46. Sia X un insieme non vuoto, ed Y un sottoinsieme fissato di X. Si provi che l'applicazione $f : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ definita da $f(A) = A \triangle Y$ per ogni $A \in \mathcal{P}(X)$ è una biezione e si determini la sua inversa.

Esercizio 1.47. Sia $f : \mathbb{N} \longrightarrow \mathbb{N}$ l'applicazione definita da $f(n) = 2n + 1$, per ogni $n \in \mathbb{N}$. Si definisca una applicazione $g : \mathbb{N} \longrightarrow \mathbb{N}$ che soddisfi alle seguenti condizioni:

1. g è suriettiva;

2. $g \circ f = i_{\mathbb{N}}$;

3. l'insieme $\{ x \in \mathbb{N} \mid g(x) = x \}$ è infinito.

Esercizio 1.48. Posto $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, sia $f : \mathbb{N}^* \longrightarrow \mathbb{N}$ l'applicazione definita da, per ogni $x \in \mathbb{N}^*$, $f(x) = m$, dove m è l'unico numero naturale tale che $x = 2^m a$ con a dispari.

(a) Si definisca una applicazione $g : \mathbb{N} \longrightarrow \mathbb{N}^*$ tale che $f \circ g = \iota_N$.

(b) Determinare $f^{-1}(\{0\})$.

(c) Provare che, per ogni $n \in \mathbb{N}$, $f^{-1}(\{n\})$ è infinito.

Esercizio 1.49. Sia $f : \mathbb{N} \longrightarrow \mathbb{N}$, definita da, per ogni $n \in \mathbb{N}$:

$$f(n) = \begin{cases} \frac{n}{3} & \text{se} \quad 3|n \\ 3n-1 & \text{se} \quad 3 \not| n \end{cases} .$$

(a) Si provi che f è suriettiva ma non iniettiva.

(b) Si definisca una applicazione $g : N \longrightarrow \mathbb{N}$ tale che $f \circ g = \iota_{\mathbb{N}}$.

Esercizio 1.50. Sia A un insieme e $f, g : A \longrightarrow A$ applicazioni. Si dimostri che:

a) Se f è suriettiva e $g \circ f = f$ allora $g = \iota_A$.

b) Se f è iniettiva e $f \circ g = f$ allora $g = \iota_A$.

Esercizio 1.51. . Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ l'applicazione definita da, per ogni $x \in \mathbb{Q}$, $f(x) = x - |\frac{x}{2}|$. Provare che f è biettiva e determinare f^{-1}.

Esercizio 1.52. Sia $D = \{ z \in \mathbb{Z} \mid 2 \nmid z \}$ l'insieme dei numeri interi dispari, e sia $f : \mathbb{Z} \longrightarrow D$ l'applicazione definita da, per ogni $z \in \mathbb{Z}$:

$$f(z) = \begin{cases} 2z-1 & \text{se} \quad z \text{ è dispari} \\ 2z+3 & \text{se} \quad z \text{ è pari} \end{cases}$$

(a) Provare che f è una biezione.

(b) Determinare f^{-1}.

Esercizio 1.53. Siano A un insieme numerabile, e B un insieme finito (ma non vuoto) o numerabile. Si dimostri che $A \times B$ è numerabile. Si provi quindi che se $A_1, A_2, \ldots, A_n$ sono insiemi numerabili, allora $A_1 \times A_2 \times \cdots \times A_n$ è numerabile.

Esercizio 1.54. Si dimostri la Proposizione 1.15.

1.8. Complementi: Cenni di calcolo proposizionale.

La *logica proposizionale* descrive come trattare le connessioni logiche elementari tra oggetti base di un ragionamento, detti *proposizioni*. Una **proposizione** è una affermazione (una 'frase', un "espressione" nel linguaggio) a cui è possibile associare in modo univoco un valore di verità: Vero [V] o Falso [F]. Ad esempio sono proposizioni le seguenti:

- 24 è un numero pari;
- 24 è un numero primo;
- 24 è somma di due numeri primi;
- ogni numero intero pari è somma di due numeri primi;

delle quali, la prima è vera, la seconda falsa, la terza vera $[24 = 13 + 11 = 17 + 7]$, la quarta è vera o falsa, si presume che sia vera (si tratta della famosa *Congettura di Goldbach*), ma ancora nessuno ne ha stabilito la correttezza. Non sono invece proposizioni le seguenti:

- qual è il massimo comun divisore tra 24 e 30 ?
- sia p un numero primo;
- ogni proposizione che appare in questa riga di testo è falsa.

Vero e Falso si dicono *valori di verità*; ad ogni proposizione viene quindi associato uno ed un solo valore di verità, e corrispondentemente diremo che una certa proposizione "è vera" o "è falsa". I **connettivi logici**, che tra breve descriveremo, traducono in modo formale le principali connessioni tra proposizioni, che usualmente (magari in maniera "ingenua") utilizziamo nello sviluppo di un argomentazione, e consentono di formare nuove proposizioni a partire da altre proposizioni date.

Il primo dei connettivi logici che descriviamo è la *congiunzione* $\wedge$. Esso traduce il concetto espresso nel discorso dalla congiunzione "e": se P e Q sono due proposizioni, allora $P \wedge Q$ (da leggersi, appunto, "P e Q") è quella proposizione che è vera *se e soltanto se entrambe P e Q sono vere*. Questo può essere convenientemente esplicato mediante la sua *tavola di verità*:

P	Q	P $\wedge$ Q
V	V	V
V	F	F
F	V	F
F	F	F

dove, ovviamente, V significa che la proposizione è vera, F che è falsa. La tavola fornisce il valore di verita di $P \wedge Q$ in funzione di tutte le possibili e separate attribuzioni di valori di verità a P ed a Q.

Gli altri connettivi logici che ci interessano sono:

- la *disgiunzione*: $\vee$
- la *negazione*: $\neg$
- l'*implicazione*: $\rightarrow$

La disgiunzione $\vee$ traduce la "o" e, nonostante il nome, indica una opzione non disgiuntiva (ovvero, come nel latino *vel*): $P \vee Q$ (letto "P o Q") significa che *almeno una* tra P e Q è vera. La sua tavola di verità è:

P	Q	P $\vee$ Q
V	V	V
V	F	V
F	V	V
F	F	F

La negazione $\neg$ traduce il "non": $\neg P$ è la proposizione che assume il valore di verità opposto a quello di P. La tavola di verità è cioè la seguente:

P	$\neg$ P
V	F
F	V

L'implicazione $\rightarrow$ esprime l'implicazione *logica*, ovvero il fatto che dalla verità di una proposizione (premessa) segue la verità di un'altra (conseguenza): $P \rightarrow Q$ (letta "P implica Q") significa che Q è vera quando P è vera. La tavola di verità è dunque la seguente:

P	Q	P $\rightarrow$ Q
V	V	V
V	F	F
F	V	V
F	F	V

Si osservi che, secondo la nostra definizione (ma anche secondo l'uso che, almeno nelle forme di pensiero che tendono a qualche rigore, ne è stato fatto), la verità di una implicazione *non* richiede la verità della premessa, anzi quando P è falsa, allora $P \rightarrow Q$ è vera qualsiasi sia la proposizione Q; questo fatto era stato osservato anche in antichità ed espresso nella formula: *ex falso sequitur quodlibet*.

Le tavole di verità per i singoli connettivi possono essere utilizzate in successione per ricavare le tavole di verità di proposizioni più articolate. Ad esempio, ricaviamo la tavola di verità della proposizione

$$\neg Q \rightarrow \neg P$$

(dove conveniamo che la negazione $\neg$ venga letta con diritto di precedenza, ovvero con $\neg Q \rightarrow \neg P$ intendiamo $(\neg Q) \rightarrow (\neg P)$):

P	Q	$\neg P$	$\neg Q$	$\neg Q \rightarrow \neg P$
V	V	F	F	V
V	F	F	V	F
F	V	V	F	V
F	F	V	V	V

Vediamo un altro esempio:

$$(P \vee Q) \rightarrow (\neg Q \rightarrow P)$$

la cui tavola di verità è:

P	Q	$P \vee Q$	$\neg Q$	$\neg Q \rightarrow P$	$(P \vee Q) \rightarrow (\neg Q \rightarrow P)$
V	V	V	F	V	V
V	F	V	V	F	V
F	V	V	F	V	V
F	F	F	V	V	V

Osserviamo l'utlimo esempio; l'esame della tavola di veirtà mostra che la proposizione $(P \vee Q) \rightarrow (\neg Q \rightarrow P)$ è *vera qualsiasi siano* i valori di verità delle proposizioni P e Q che la compongono. Una tale proposizione si dice **tautologia**. Il più tipico esempio di tautologia è la proposizione che esprime il cosiddetto "principio del terzo escluso": $P \vee \neg P$.
Viceversa, una proposizione che è sempre *falsa*, qualsiasi siano i valori di verità delle proposizioni elementari che la compongono si dice una **contraddizione**. L'esempio base di contraddizione è la proposizione che esprime la "reductio ab absurdum": $P \wedge \neg P$.

Osserviamo ora la tavola di verità della proposizione $\neg Q \to \neg P$, che abbiamo ricavato sopra: ci accorgiamo che, in corrispondenza ad ogni possibile assegnazione dei valori di verità di P e di Q, li valore di verità di tale proposizione coincide con quello della proposizione $P \to Q$. Si dice allora che le proposizioni $\neg Q \to \neg P$ e $P \to Q$ sono *logicamente equivalenti*. Da un punto di vista operativo, ciò significa che dimostrare la verità dell'una equivale a dimostrare la verità dell'altra.

NOTA. L'esempio che abbiamo fornito di equivalenza logica esprime in effetti un metodo argomentativo utilizzato di frequente: per provare che da una certa affermazione P segue un'altra affermazione Q, si dimostra che la negazione di Q comporta necessariamente la negazione di P. Altri casi di equivalenze logiche che esprimono comuni, e legittime, tecniche di ragionamento sono descritte nell'esercizio che segue e nell'esercizio 1.57.

Esercizio 1.55. [Prima Legge di De Morgan] Siano P e Q proposizioni. Si provi che $\neg(P \wedge Q)$ è logicamente equivalente a $\neg P \vee \neg Q$.

SOLUZIONE. Basta confrontare le due tavole di verità:

P	Q	$P \wedge Q$	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
V	V	V	F	F	F	F
V	F	F	F	V	V	V
F	V	F	V	F	V	V
F	F	F	V	V	V	V

Poiché, per qualsiasi assegnazione dei valori di verità a P ed a Q, il val;ore di verità assunto da $\neg(P \wedge Q)$ coincide con quello assunto da $\neg P \vee \neg Q$, si conclude che le due proposizioni sono logicamente equivalenti. ■

Introduciamo ora un connettivo logico $\leftrightarrow$ (che leggeremo "*se e solo se*"), che esprima *l'equivalenza logica* tra due proposizioni. Precisamente, definiamo $P \leftrightarrow Q$ come $(P \to Q) \wedge (Q \to P)$. La tavola di verità del connettivo $\leftrightarrow$ (che si ricava da quelle di $\wedge$ e di $\to$) è:

P	Q	P $\leftrightarrow$ Q
V	V	V
V	F	F
F	V	F
F	F	V

Fatto questo, è facile osservare che *due proposizioni (composte) A e B sono logicamente equivalenti se e soltanto se $A \leftrightarrow B$ è una tautologia.*

Esercizio 1.56. Siano P e Q proposizioni. Si scriva la tavola di verità della proposizione $(P \wedge \neg Q) \to (Q \vee \neg P)$. Si sostituiscano quindi P e Q con affermazioni di carattere matematico, scelte in modo che la proposizione risultante sia effettivamente falsa.

Esercizio 1.57. (*Seconda Legge di De Morgan*) Siano P e Q proposizioni. Si provi che $\neg(P \vee Q)$ è logicamente equivalente a $\neg P \wedge \neg Q$.

Esercizio 1.58. Siano P, Q ed R proposizioni. Si provi che $(P \vee Q) \to R$ e $(P \to R) \wedge (Q \to R)$ sono logicamente equivalenti.

Esercizio 1.59. Siano P, Q ed R proposizioni. Si scriva la tavola di verità della proposizione $((\neg P \wedge Q) \to R) \leftrightarrow (R \to ((\neg Q \vee P))$.

Intervallo letterario

PARADOSSI[2]. Come abbiamo osservato, i problemi sollevati dal paradosso di Russell non hanno a che vedere con l'infinito, ma piuttosto con l'autoreferenza negativa. In questo senso, esso è parente di altri paradossi noti fin dall'antichità: come il paradosso del mentitore, o quello del barbiere (vedi qui).

Poiché possono essere espressi mediante racconti di situazioni curiose, paradossi del genere sono stati talvolta utilizzati in narrativa. In tali occasioni assumono in genere l'aspetto di quelli che, nei testi divulgativi, sono chiamati *paradossi della decisione* (ma si tratta, di fatto, di una forma mascherata del paradosso del mentitore). Lo schema è questo: un qualche personaggio X si trova di fronte ad un'autorità, o una legge, o potere, che stabilisce che se costui X mentirà (o non indovinerà una certa cosa) allora accadrà un certo evento A (in genere non favorevole ad X), mentre se dirà il vero (o indovinerà) accadrà non-A. X si trova quindi ad affrontare una normativa che dice $M \leftrightarrow A$ dove M significa "X mente (o non indovina, etc.)", e la scappatoia per X è allora quella di dichiarare "avverrà A"; che corrisponde al fatto che X dichiari "io sto mentendo" (o mentirò, o non indovinerò, etc.),[3]

• Un esempio classico è la storia del coccodrillo, raccontata da Diogene Laerzio e probabilmente nata in ambiente stoico. Un coccodrillo ghermisce un bambino sulle rive del Nilo. La madre accorre e prega il coccodrillo di lasciare andare il piccolo e quello, astuto, le risponde: "Lo lascerò andare se tu indovinerai cosa sto per fare". La madre gli disse: "Tu stai per mangiare mio figlio". Vediamo la prosecuzione nel commento di Lewis Carroll[4] (il quale dà l'impressione di poter immedesimarsi piuttosto facilmente nel predatore),

> Qualunque cosa faccia, il coccodrillo non mantiene la parola data. Se divora il bambino, fa sì che la madre dica la verità, e quindi non mantiene la parola; se lo restituisce, fa sì che la madre dica il falso, e anche in questo caso non mantiene la promessa. Non avendo speranza di salvare il suo onore, non si può dubitare che si comporterà seguendo la sua seconda passione predominante: l'amore per i bambini![5]

• Ecco la versione che ne dà M. de Cervantes nel *Don Chisciotte*; precisamente nella seconda parte del romanzo, quando Don Chisciotte e Sancho Panza sono oggetto di numerose burle. In una di queste vien fatto credere a Sancho di essere governatore dell'isola di Barataria (nella realtà un piccolo villaggio aragonese); gli vengono così sottoposte alcune bizzarre questioni giuridiche[6].

> Il primo ch'ebbe a lui ricorso fu un forestiere che gli disse:
> – Signore, un rapido fiume divideva due confini di un dominio medesimo [...] e sopra questo fiume eravi un ponte, e al capo del ponte un paio di forche, ed una tal casa di audienza o di giustizia in cui stavano di ordinario quattro giudici, che

[2] *Il filosofo vive di problemi come l'uomo di cibi. Un problema insolubile è un cibo indigesto. Quello che nei cibi è il condimento piccante, nei problemi è il paradosso.* [Novalis]

[3] È il caso, ad esempio, della storiella del logico il quale, dopo aver inserito la mano nella Bocca della verità in Santa Maria in Cosmedin, dice "questa mano mi sarà morsa".

[4] L. Carroll, *Symbolic Logic, Part II.*

[5] Con tipico senso dello humor, Carroll propone quindi ai lettori di analizzare il problema nel caso che la prima frase della madre fosse stata: "Tu mi ridarai il bambino". In questo caso, se il coccodrillo lo restituisce, allora mantiene la sua parola; se lo divora, allora la madre ha detto il falso e, di nuovo, il coccodrillo rispetta l'accordo. Conclude Carroll: "In qualunque modo si comporti, il coccodrillo mantiene la parola. Il suo senso dell'onore è dunque pienamente soddisfatto qualunque cosa faccia, così che, di nuovo, sua sola guida rimane la sua seconda passione dominante, il risultato per il bambino sarebbe, temo, esattamente identico a prima".

[6] La traduzione italiana è quella di B. Gamba del 1818.

> giudicavano sul fondamento della legge imposta dal padrone del fiume, del ponte e del dominio: e la legge era questa: "Se alcuno vuole passare per questo ponte dall'una all'altra parte, deve prima dire e giurare dove e per quale oggetto egli passa; giurando il vero, sia lasciato passare, mentendo, sia impiccato sulle forche che stanno alzate, e ciò senza alcuna remissione". Resa pubblica questa legge e la rigorosa condizione, molti passavano, e dal tenore del loro giuramento conoscevasi la verità, ed i giudici li lasciavano liberamente andare. Accadde una volta che ricevendo il giuramento dato da un uomo, egli giurò che passava e andava a morire su quelle forche ch'erano ivi alzate, e nulla pi 'u aggiunse. Ponderarono i giudici questa cosa e dissero: se noi lasciamo passare liberamente questo uomo, egli avrà mentito nel suo giuramento, e noi conformemente alla legge dovremmo farlo impiccare: ma se noi lo impicchiamo, egli ha giurato che andava a morire su quelle forche, ed avendo giurato il vero, a senso della medesima legge dee restarsene libero. Ora io domando alla signoria vostra, signor governatore, che debbano fare i giudici di questo uomo, standosene eglino tuttavia dubbiosi e sospesi?

Dopo essersi fatto rispiegare il fatto, Sancho commenta,

> – A giudizio mio questo negozio è deciso in due parole, e dico così: il tal uomo giura che va a morire sulle forche, e se muore su quelle giura il vero, e in tal caso merita, in forza della legge, di andare libero e di passare il ponte; e se non lo impiccano ha giurato il falso, ed in vigore della stessa legge merita di essere impiccato?

Ed infine la sua decisione (e la sua maniera di rompere il paradosso) è la seguente:

> – Sentite qua, signor buon uomo mio – rispose Sancio; – questo passeggiere di cui parlate, o io sono un animale o egli tiene la stessa ragione per morire come per vivere e per passare il ponte: ora se la verità lo salva, la bugia lo condanna egualmente; ed essendo così la cosa, siccome è infatti, io sono di opinione che andiate a dire ai signori dai quali siete mandato, che trovandosi in eguale bilancia e le ragioni di condannarlo a quelle di assolverlo, lo lascino passare liberamente: perché sempre meglio è fare del bene che del male.

• *Ancora in tribunale.* Così come una proposizione è vera o falsa, una causa (un procedimento giudiziario) si vince o si perde; dunque, intentar causa contro se stessi è una specie di paradosso, simile a quello perpetrato quando si afferma "Io sto mentendo", ed è quello che combina un personaggio minore nel romanzo *Jacques il fatalista* di Denis Diderot:

> – Ma chi vi ci ha fatto mettere? [in carcere]
> – Io stesso.
> – Come, voi?
> – Sì, io, signore.
> – E come avete fatto?
> – Come avrei fatto per un altro. Ho intentato un processo a me stesso; l'ho vinto, e in seguito alla sentenza che ho ottenuto contro me stesso, e al decreto che ne è seguito, sono stato arrestato e portato qui.
> – Siete pazzo?
> – No, signore, vi dico come stanno le cose.
> – Non potreste farvi un altro processo, vincerlo e, in seguito a un'altra sentenza e a un altro decreto, farvi liberare?

La situazione è volutamente assurda; mentre è dato come un aneddoto autentico il racconto che Aulo Gellio, nelle *Noctes Atticae* fa a proposito del filosofo sofista Protagora e di un suo allievo[7]. Il giovane Euatlo vuol diventare oratore forense e prende lezioni da Protagora, corrisponedendogli metà dell'onorario pattuito prima di iniziare le lezioni, con l'accordo di saldare il resto non appena vinta la prima causa. Ma, terminato il corso, per molto tempo

[7] Lo stesso episodio è solo accennato in Diogene Laerzio

Euatlo non perorò alcuna causa, tanto da far sospettare in Protagora l'intenzione di non voler pagare il resto del compenso (che doveva essere piuttosto salato). Il filosofo citò allora Euatlo in tribunale, affinché il giudice costringesse quest'ultimo al pagamento. Di fronte alla corte, così disse

> Sappi, giovane stolto, che mi dovrai pagare, in qualsiasi modo il tribunale si pronunci, sia contro di te che a tuo favore. Infatti, se il giudice ti darà torto, e quindi io vincerò la causa, mi dovrai la somma in base alla sentenza; e se ti verrà data ragione, mi dovrai pagare in base ai patti, perché avrai vinto una causa".

Ribattè Euatlo,

> Potrei facilmente eludere la tua trappola non pronunciando parola e facendomi patrocinare da un altro avvocato. Ma maggior piacere ricaverò dal vincerti non soltanto giuridicamente, ma sul tuo stesso argomento. Apprendi dunque anche tu, dottissimo maestro, che non otterrai da me ciò che chiedi, in qualsiasi modo si pronunci la cote, sia contro di me che a mio favore. Infatti, se i giudici si pronunceranno in mio favore, nulla ti sarà dovuto per loro sentenza; se contro di me, nulla ti dovrò per il patto che si fece, giacché non avrò ancora vinto una causa.

Riferisce quindi Gellio che i giudici, non riuscendo a togliersi dai dubbi, rinviarono la causa a data lontanissima[8].

• Nel racconto *Caro vecchio neon* di David F. Wallace[9] il paradosso del mentitore diventa, nelle parole del narratore-protagonista, il *Paradosso dell'Impostore*[10].

> . . . non potevo essere un impostore assoluto se avevo appena dichiarato [all'analista] la mia impostura riconoscendola davanti a lui un istante prima.

Anche se poi il narratore elabora a lungo l'idea e il paradosso da logico - o linguistico - diventa esistenziale:

> Era che più tempo e più impegno mettevi nel cercare di far colpo sugli altri o di affascinarli, meno sorprendente e affascinante ti sentivi dentro: eri un impostore. E più ti sentivi un impostore, più ti sforzavi di offrire un'immagine sorprendete e piacevole di te stesso per evitare che gli altri capissero che eri un impostore...

[e così via]. Di fatto, l'intero racconto è alimentato da numerosi riferimenti alla logica ed ai paradossi (a partire dall'impianto narrativo: un suicida parla in prima persona degli ultimi mesi della propria vita): oltre a quello del mentitore, Wallace – o il narratore – cita il paradosso di Russell e descrive compiutamente quello di Berry[11]. Ad un certo punto si trova la trascrizione formale della proposizione: *O si ama, o si ha paura, e se si ama non si ha paura*; posto $F(x) = x$ *ha paura*, e $L(x) = x$ *ama*, Wallace scrive:

$$\forall x((F(x) \to \neg L(x)) \wedge (L(x) \to \neg F(x))) \wedge \neg(\exists x(\neg F(x) \wedge \neg L(x))$$

Una proposizione che correttamente riproduce le intenzioni, ma che la lettrice attenta riconoscerà logicamente ridondante: se ne trovi per esercizio una espressione più breve.

---

[8] Sul sito chiamto "Base 5 (appunti di matematica ricreativa)" ho trovato un commento (di un esperto, a giudicare dalla terminologia) che spiega come una corte italiana (in base - pare - all'articolo 1355 del codice civile) avrebbe sanzionato la nullità del contratto tra Protagora e Euatlo e imposto a quest'ultimo, pur perdendo la causa, il pagamento della prestazione.

[9] David Foster Wallace (1962 – 2008), uno dei più notevoli narratori americani contemporanei, applicò spesso, e con varie intenzioni, termini e concetti matematici nelle sue storie. Il racconto in questione si trova nella raccolta *Oblio*; traduzione di G. Granato (Einaudi, Stile Libero, 2004).

[10] Il protagonista è un pubblicitaro; uno di quelli che si autodefiniscono "creativi", il che è già una bella impostura e - diciamolo pure - un paradosso.

[11] vedi: http://web.math.unifi.it/users/casolo/dispense/Algebra1paradossi.pdf

2

Numeri

2.1. Numeri interi e Principio di Induzione.

L'insieme $\mathbb{N}$ dei numeri naturali gode della seguente proprietà (che ci appare ovvia, ma che di fatto è uno degli assiomi di $\mathbb{N}$):

ogni sottoinsieme **non vuoto** *di* $\mathbb{N}$ *ha un elemento* **minimo**.

Questa proprietà si esprime dicendo che l'insieme $\mathbb{N}$ è **bene ordinato** (infatti è chiamata *assioma del buon ordinamento*). Ad esempio, rispetto all'ordine naturale, l'insieme dei numeri interi $\mathbb{Z}$, cosi come ogni intervallo $[a, b] \subset \mathbb{R}$ con $a < b$, *non sono* bene ordinati[1], giacché in entrambi i casi è possibile trovare dei sottoinsiemi non vuoti che non hanno minimo (ad esempio $\mathbb{Z}$ stesso nel primo caso, e il sottoinsieme $(a, b] = \{x | x \in \mathbb{R},\ a < x \leq b\}$ nel secondo caso.

Vediamo in azione questo assioma nella dimostrazione di una proprietà ben nota, ma fondamentale, dei numeri interi: la divisione con resto (*divisone euclidea*).

Teorema 2.1. *Siano a, b numeri interi, con $b \neq 0$. Allora esistono, e sono unici, numeri interi q, r tali che*

$$a = bq + r \quad \text{e} \quad 0 \leq r \leq |b| - 1.$$

Dimostrazione. Dati $a, b \in \mathbb{Z}$ con $b \neq 0$, sia S l'insieme di tutti i numeri naturali della forma $a - bt$, con $t \in \mathbb{Z}$:

$$S = \{s \in \mathbb{N} | s = a - bt \ \text{ per qualche } \ t \in \mathbb{Z}\}.$$

S non è vuoto; infatti, se $a \geq 0$ allora $a = a - b0 \in S$; se $a < 0$, allora, poiché $b^2 \geq 1$, $a - b(ba) = a(1 - b^2) \in S$. Dunque, per il principio del buon ordinamento, S ha un elemento minimo r. Per definizione, esiste un $q \in \mathbb{Z}$ tale che $r = a - bq$, cioè

$$a = bq + r.$$

Dobbiamo ora provare che $r < |b|$. Supponiamo, per assurdo $r \geq |b|$, allora esiste $y \in \mathbb{N}$ tale che $r = |b| + y$; ma allora

$$y = r - |b| = a - bq - |b| = a - b(q \pm 1) \in S$$

[1] ricordo che $[a, b] = \{x | x \in \mathbb{R},\ a \leq x \leq b\}$.

e quindi, poichè $r = \min(S)$, deve essere $r \leq y$, che è assurdo. Dunque $r < |b|$.
La semplice verifica dell'unicità degli interi q, r soddisfacenti alla condizione

$$a = qb + r \quad e \quad 0 \leq r < |b|,$$

è lasciata per esercizio. ■

Induzione. Il principio di induzione è un fondamentale metodo deduttivo in teoria dei numeri interi (ma anche in tutti quei casi in cui determinate situazioni possono essere parametrizzate mediante numeri naturali). Esso è logicamente equivalente all'assioma del buon ordinamento dei numeri naturali.

Principio di induzione (1^a forma).
Sia $n_0 \in \mathbb{N}$, e supponiamo che per ogni $n \geq n_0$ sia assegnata una proposizione $P(n)$ e che siano soddisfatte le seguenti condizioni:

(1) $P(n_0)$ è vera;

(2) per ogni $n \geq n_0$, se $P(n)$ è vera allora anche $P(n+1)$ è vera.

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

Esempio 1. Dimostriamo che, *per ogni numero naturale* $n \geq 1$ si ha:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \ ;$$

in questo caso, $n_0 = 1$ e, per ogni $n \geq 1$ la proposizione $P(n)$ è l'uguaglianza descritta, che, in forma compatta, si scrive

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

Per provare questa affermazione, utilizziamo il principio di induzione nella 1^a forma. Dobbiamo dunque verificare che l'insieme delle proposizioni $P(n)$ soddisfa alle due condizioni richieste per la applicazione del principio:

(1) $P(1)$ è vera; infatti essa si riduce a $1 = \frac{1(1+1)}{2}$ che è una uguaglianza vera.

(2) Sia $n \geq 1$ e supponiamo che $P(n)$ sia vera (questa si chiama *ipotesi induttiva*), cioè che

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

e dimostriamo che *allora* anche $P(n+1)$ è vera. Infatti :

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

quindi $P(n+1)$ è vera.
Per il principio di induzione, si ha che $P(n)$ è vera per ogni $n \geq 1$.

Ricordo la definizione di $n!$ (n *fattoriale*): $0! = 0$ e, se $n \geq 1$

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

Esempio 2. Provare che per ogni numero naturale $n \geq 1$ si ha $2^{2n}(n!)^2 > (2n)!$.

(1) Si inizia con il provare che l'affermazione vale per $n = 1$; come spesso accade, si tratta di una banale verifica; si ha $2^{2\cdot 1}(1!)^2 = 2^2 = 4$, mentre $(2 \cdot 1)!. = 2! = 1 \cdot 2 = 2$, e dunque $2^{2\cdot 1}(1!)^2 > (2 \cdot 1)!.$ (che è la proposizione per $n = 1$).

(2) Supponiamo ora l'affermazione sia vera per $n \geq 1$; per $n + 1$ si ha

$$2^{2(n+1)}((n+1)!)^2 = 2^{2n+2}(n! \cdot (n+1))^2 = 2^2 \cdot 2^{2n} \cdot (n!)^2 \cdot (n+1)^2 = 4(n+1)^2 \cdot \left[2^{2n}(n!)^2\right],$$

e quindi, applicando l'ipotesi induttiva:

$$2^{2(n+1)}((n+1)!)^2 > 4(n+1)^2 \cdot (2n)! > (2n+1)(2n+2) \cdot (2n)! = (2(n+1)!).$$

Per il principio di induzione, si conclude che la disuguaglianza è vera per ogni $n \geq 1$.

Il principio di induzione può anche essere utilizzato per provare proposizioni sull'insieme dei numeri interi, distinguendo il caso dei numeri positivi da quello dei numeri negativi.

Esempio 3. Dimostriamo che, per ogni $z \in \mathbb{Z}$ $z^3 - z$ è divisibile per 6.

Come primo caso, supponiamo $z \geq 0$, utilizzando il principio di induzione.
(1) La affermazione è vera per $n = 0$, infatti

$$0^3 - 0 = 0 = 0 \cdot 6 \text{ , cioè } \quad 6 \text{ divide } 0^3 - 0 \text{ .}$$

(2) Supponiamo la affermazione sia vera per n, cioè che (ipotesi induttiva) 6 divide $n^3 - n$. Allora:

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = (n^3 - n) + 3n(n+1)$$

è divisibile per 6 dato che 6 divide $n^3 - n$ e divide $3n(n + 1)$ (quest'ultima affermazione segue dal fatto che $n(n + 1)$ è certemente un numero pari).
Quindi per il principio di induzione la nostra affermazione è vera per ogni numero intero $z \geq 0$.
Supponiamo ora $z \in \mathbb{Z}$ e $z \leq 0$; allora $-z \geq 0$ e quindi, per il caso precedente, 6 divide

$$(-z)^3 - (-z) = -z^3 + z = -(z^3 - z)$$

e dunque 6 divide $z^3 - z$, completando la dimostrazione.

Esercizio 2.1. Si dimostri il Teorema 2.1 procedendo per induzione su a (si assuma prima che a sia positivo).

Principio di induzione (2^a forma).

Sia $n_0 \in \mathbb{N}$, e supponiamo che per ogni $n \geq n_0$ sia assegnata una proposizione $P(n)$ e che siano soddisfatte le seguenti condizioni:

(1) $P(n_0)$ è vera;

(2) per ogni $n \geq n_0$, se $P(t)$ è vera per ogni numero naturale t con $n_0 \leq t \leq n-1$, segue che anche $P(n)$ è vera.

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

Anche se apparentemente più forte, questa seconda forma è equivalente alla prima, come si potrebbe facilmente provare. Un caso di applicazione dell'induzione in questa forma è nella dimostrazione del teorema fondamentale dell'aritmetica che vedremo più avanti.

2.2. Combinatoria.

In questa sezione stabiliremo alcune quantità numeriche riguardanti insiemi finiti, che fanno parte del bagaglio di base della combinatoria. Cominciamo col provare, mediante il principio di induzione, un'importante formula già enunciata in un capitolo precedente.

Proposizione 2.2. *Sia A un insieme finito; allora $|\mathcal{P}(A)| = 2^{|A|}$.*

Dimostrazione. Sia $n = |A|$, e procediamo per induzione su n.
L'affermazione è vera per $n = 0$, in questo caso infatti $A = \emptyset$ e $|\mathcal{P}(\emptyset)| = 1$.
Supponiamo ora che l'affermazione sia vera per insiemi di ordine n (con $n \geq 0$) e proviamo che allora vale per quelli di ordine $n+1$. Sia A insieme con $|A| = n+1$, allora $A \neq \emptyset$; sia a un fissato elemento di A e sia $B = A \setminus \{a\}$. Ora, ogni sottoinsieme di A è un sottoinsieme di B oppure è del tipo $X \cup \{a\}$ con $X \subseteq B$. Quindi i sottoinsiemi di A sono esattamente il doppio dei sottoinsiemi di B. Ma $|B| = n$ e quindi, per ipotesi induttiva, B ha esattamente 2^n sottoinsiemi. Dunque:

$$|\mathcal{P}(A)| = |\mathcal{P}(B| + |\mathcal{P}(B)| = 2^n + 2^n = 2^{n+1}$$

provando che la affermazione è vera per insiemi di ordine $n+1$.
Per il principio di induzione la Proposizione è dimostrata. ∎

Un'altra importante proprietà degli insiemi finiti è la seguente osservazione (nota anche come *principio della cassetta delle lettere*).

Proposizione 2.3. *Siano A, B un insiemi finiti con $|A| = |B|$; sia $f : A \to B$ un'applicazione. Allora sono equivalenti*

(i) f è iniettiva;
(ii) f è suriettiva;
(iii) f è biettiva.

Fissiamo ora due insiemi finiti A e B, con $|A| = n$ e $|B| = m$.

Con queste notazioni, le seguenti affermazioni sono facilmente verificabili:

(1) $|A \times B| = |A||B| = mn$;

(2) se A e B sono disgiunti allora $|A \cup B| = |A| + |B| = m + n$; in generale

$$|A \cup B| + |A \cap B| = |A| + |B|$$

La prima delle due uguaglianze si può facilmente generalizzare ad un prodotto di un numero k di insiemi finiti: se $A_1, \ldots, A_k$ sono insiemi finiti, allora

$$|A_1 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_k|;$$

in particolare, se $|A| = n$, allora $|A^k| = n^k$.

Anche la uguaglianza (2) si generalizza; la prima parte in modo ovvio:

- se $A_1, \ldots, A_k$ sono insiemi finiti a due a due disgiunti, allora

$$|A_1 \cup \ A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k| \ ;$$

il caso generale non è altrettanto banale; posto $X = \{1, 2, \ldots, k\}$, si ha

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = \sum_{\emptyset \neq I \subseteq X} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|.$$

Ad esempio, nel caso di tre insiemi:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Vogliamo ora determinare il numero di applicazioni da A in B; sia quindi

$$B^A = \{f \mid f : A \longrightarrow B \text{ applicazione}\}.$$

Osserviamo che, se $A = \{a_1, a_2, \ldots, a_n\}$, allora un'applicazione $f : A \longrightarrow B$ è univocamente individuata dalla n-upla delle immagini $(f(a_1), f(a_2), \ldots, f(a_n)) \in B^n$; detto in modo più preciso, l'applicazione $\Gamma : B^A \longrightarrow B^n$ definita da, per ogni $f \in B^A$,

$$\Gamma(f) = (f(a_1), f(a_2), \ldots, f(a_n))$$

è una biezione. Quindi $|B^A| = |B^n| = m^n$. Abbiamo quindi dimostrato

Proposizione 2.4. *Se A e B sono insiemi finiti, allora il numero di applicazioni da A in B è uguale a $|B|^{|A|}$.*

Nota. Utilizziamo quanto appena provato per dare un'altra dimostrazione della Proposizione 2.2. Sia A insieme con $|A| = n \in \mathbb{N}$. Per ogni $B \subseteq A$ definiamo la *funzione caratteristica* $\chi_B : A \to \{0, 1\}$, ponendo, per ogni $a \in A$

$$\chi_B(a) = \begin{cases} 1 & \text{se a} \in \text{B} \\ 0 & \text{se a} \notin \text{B} \end{cases}$$

L'assegnazione $B \mapsto \chi_B$ definisce una *biezione* $\mathcal{P}(A) \to \{0, 1\}^A$ (lo si dimostri per esercizio). Quindi, $|\mathcal{P}(A)|$ coincide con il numero di applicazioni da A in $\{0, 1\}$, che per la Proposizione 2.4, è uguale a 2^n.

Sia $n \in \mathbb{N}$; si definisce $n!$ (n **fattoriale**) nel modo seguente:

$$0! = 1 \text{ e, se } n \geq 1, \ n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n \ .$$

Ora, ci chiediamo quale sia il numero di applicazioni *iniettive* da A in B. Riferendoci all'applicazione $\Gamma : B^A \longrightarrow B^n$ utilizzata in precedenza, vediamo che le applicazioni iniettive corrispondono alle n-uple di elementi *distinti* di B.
Ora per costruire tutte le n-uple $(b_1, b_2, \ldots, b_n) \in B^n$ ad elementi distinti, possiamo pensare di poter scegliere

- b_1 in m modi possibili (ogni elemento di B);
- b_2 in $m-1$ modi possibili (ogni elemento di B con l'esclusione di b_1);
- b_3 in $m-2$ modi possibili (ogni elemento di B con l'esclusione di b_1, b_2);

e così via. Questo processo finisce con b_n per cui abbiamo $m - n + 1$ scelte fra gli elementi di B. In totale il numero di n-uple ad elementi distinti è quindi $m(m-1)(m-2)\cdots(m-n+1)$.
Abbiamo dunque dimostrato

Proposizione 2.5. *Se A e B sono insiemi finiti con $|A| = n \leq m = |B|$, allora il numero di applicazioni iniettive da A in B è uguale a*

$$m(m-1) \ \dots \ (m-n+1) = \frac{m!}{(m-n)!} \ .$$

In particolare, ricordando che per un insieme finito A, una applicazione $f : A \longrightarrow A$ è biettiva se e solo se è iniettiva, abbiamo

Proposizione 2.6. *Sia A un insieme finito con $|A| = n$, allora il numero di applicazioni biettive da A in se stesso è uguale a $n!$.*

È possibile anche trovare una formula per il numero di funzioni *suriettive* da un insieme finito A ad un insieme finito B, in funzione dell'ordine dei due insiemi (chiaramente esistono funzioni suriettive se e solo se $|A| \geq |B|$). Questa formula è però più complicata di quella della Proposizione 2.5 e non la facciamo; chi è interessato la trova dimostrata QUI (ma prima occorre conoscere i coefficienti binomiali, di cui si parla qui di seguito).

Coefficienti binomiali. Siano $k, n \in \mathbb{N}$, con $k \leq n$. Il *coefficiente binomiale* "n su k", è definito come

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

per ogni $n \geq k \geq 1$, mentre per $k = 0$ si pone, per ogni $n \in \mathbb{N}$,

$$\binom{n}{0} = 1.$$

In partenza non è ovvio che il coefficiente binomiale sia un numero naturale. Questa è una conseguenza di quanto proveremo tra poco: ovvero che il coefficiente binomiale $\binom{n}{k}$ rappresenta il numero di sottoinsiemi di ordine k di un insieme di ordine n. Iniziamo però con alcune semplici ma fondamentali relazioni tra coefficienti binomiali.

Lemma 2.7. *Siano $k, n \in \mathbb{N}$ con $k \leq n$. Allora*

(1) $$\binom{n}{k} = \binom{n}{n-k} \ ;$$

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

Dimostrazione. Calcolando direttamente:

$$\binom{n}{n-k} = \frac{n!}{(n-(n-k))!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k} \ .$$

(2) Abbiamo

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} =$$

$$= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{(n-1)!(n-k)+(n-1)!k}{k!(n-k)!} =$$

$$= \frac{(n-1)!(n-k+k)}{k!(n-k)!} = \frac{(n-1)!n}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

che è ciò che si voleva. ∎

Veniamo al risultato annunciato poco sopra.

Teorema 2.8. *Sia A un insieme finito con $|A| = n$, e sia $k \in \mathbb{N}, k \leq n$; allora il numero di sottoinsiemi di A che contengono esattamente k elementi è $\binom{n}{k}$.*

Dimostrazione. Procediamo per induzione su n. Se $n = 0, 1$, l'affermazione è ovvia. Così come è chiaramente vera per $k = 0, n$ ed ogni n (infatti un insieme con n elementi ha un solo sottoinsieme con 0 elementi, che è l'insieme vuoto, ed un solo sottoinsieme con n elementi che è se stesso). Sia quindi $n \geq 2$. $1 \leq k \leq n-1$, e sia $A = \{a_1, a_2, \ldots, a_n\}$ un insieme con n elementi. Poniamo $B = \{a_1, \ldots, a_{n-1}\}$. Per ipotesi induttiva, il numero di sottoinsiemi di ordine k e il numero di quelli di ordine $k-1$ di B, è, rispettivamente:

$$\binom{n-1}{k} \quad \text{e} \quad \binom{n-1}{k-1}.$$

Ora, possiamo ripartire l'insieme dei sottoinsiemi di ordine k di A in due classi: quelli contenuti in B, e quelli non contenuti in B; il numero di sottoinsiemi della prima classe è $\binom{n-1}{k}$, mentre quello dei sottoinsiemi della seconda classe è $\binom{n-1}{k-1}$: infatti tali sottoinsiemi sono del tipo $\{a_n\} \cup X$, dove X è un sottoinsieme di ordine $k-1$ di B, e sono univocamente individuati da tale X. In conclusione, il numero di sottoinsiemi di ordine k di A è

$$\binom{n-1}{k} + \binom{n-1}{k-1},$$

che, per il Lemma 2.7 è uguale a $\binom{n}{k}$. ∎

Osserviamo che questa interpretazione del coefficiente binomiale rende, ad esempio, ovvio il punto (1) del Lemma 2.7; infatti se A è un insieme con n elementi, la regola $X \longrightarrow A \setminus X$, definisce una biezione tra l'insieme dei sottoinsiemi di ordine k di A e l'insieme dei sottoinsiemi di ordine $n-k$; quindi il numero dei sottoinsiemi di ordine k coincide con quello dei sottoinsiemi di ordine $n-k$.

Il nostro prossimo obiettivo è la dimostrazione della formula di Newton per il calcolo delle potenze di un binomio. Il primo passo consiste nel provare le seguenti utili proprietà dei coefficienti binomiali.

Teorema 2.9. (del binomio di Newton). *Siano $a, b \in \mathbb{Z}$ numeri interi, e $0 \neq n \in \mathbb{N}$. Allora*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Dimostrazione. Per induzione su n.

Se $n = 1$ allora la formula è valida; infatti:

$$(a+b)^1 = b + a = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0.$$

Sia ora $n \geq 2$, e per ipotesi induttiva supponiamo:

$$(a+b)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k} \ .$$

Allora, utilizzando la formula (2) del Lemma 2.7:

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \ = a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^k b^{n-k} \ + b^n =$$

$$= a^n + \sum_{k=1}^{n-1} \binom{n-1}{k-1} a^k b^{n-k} \ + \sum_{k=1}^{n-1} \binom{n-1}{k} a^k b^{n-k} \ + b^n =$$

$$= a \cdot \left(a^{n-1} + \sum_{j=0}^{n-2} \binom{n-1}{j} a^j b^{n-1-j} \right) + \left(\sum_{k=1}^{n-1} \binom{n-1}{k} a^k b^{n-1-k} \ + b^{n-1} \right) \cdot b =$$

$$= a \cdot \sum_{j=0}^{n-1} \binom{n-1}{j} a^j b^{n-1-j} \ + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k} \ \cdot b =$$

$$= a(a+b)^{n-1} + (a+b)^{n-1} b = (a+b)(a+b)^{n-1} = (a+b)^n \ .$$

Per il principio di induzione, la formula è vera per ogni $n \geq 1$. ∎

Come applicazione, ridimostriamo una formula già vista.

Sia A insieme finito con $|A| = n$. Allora $|\mathcal{P}(A)| = 2^n$.

Infatti :

$$|\mathcal{P}(A)| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = (1+1)^n = 2^n \ .$$

2.3. Rappresentazioni b-adiche.

La nostra usuale rappresentazione decimale dei numeri interi positivi è basata sulla convenzione che la posizione delle diverse cifre "corrisponde" (da destra a sinistra) a potenze crescenti del numero 10; ad esempio, scrivere $n = 3215$ significa

$$n = 5 \cdot 10^0 + 1 \cdot 10^1 + 2 \cdot 10^2 + 3 \cdot 10^3.$$

Si tratta cioè di una notazione in base 10. La scelta di 10 è (dal punto di vista matematico) del tutto arbitraria: la stessa cosa può essere fatta scegliendo come base qualunque numero naturale $b \geq 2$. In questo caso c'è bisogno di b simboli distinti per i numeri da 0 a $b-1$, e le cifre (da destra a sinistra) corrispondono alle potenze crescenti di b.

Teorema 2.10. *Sia b un numero intero $b \geq 2$. Allora ogni intero positivo n si può scrivere in modo unico nella forma*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

dove gli $a_0, a_1, a_2, \ldots, a_k$ *sono interi tali che*

$$\begin{cases} 0 \le a_i \le b-1 \quad \textit{per} \quad i = 0, 1, \ldots, k-1 \\ \\ 1 \le a_k \le b-1 \end{cases}$$

(Si osservi che, nell'enunciato, k è il minimo intero positivo tale che $b^k \le n < b^{k+1}$)

Tale rappresentazione di n si chiama rappresentazione in base b, o rappresentazione b-adica, di n. Ad esempio, la rappresentazione 2-adica di $n = 1958$ è

$$1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0;$$

si dice anche che

$$11110100110$$

(ovvero, la sequenza delle "cifre" $a_k a_{k-1} \ldots a_2 a_1 a_0$) è la scrittura in base 2 di 1958. La rappresentazione in base 7 dello stesso intero è invece

$$5 \cdot 7^3 + 4 \cdot 7^2 + 6 \cdot 7 + 5$$

e quindi la scrittura 7-adica di 1958 è 5465.

Dimostrazione. Fissata la base $b \ge 2$, sia $n \in \mathbb{N}$. Dimostriamo, per induzione su n, l'esistenza di una rappresentazione b-adica di n e la sua unicità.

Cominciamo con l'esistenza. Se $0 \le n \le b-1$, la cosa è ovvia. Sia quindi $n \ge b$. Dividiamo n per b,

$$n = qb + r \qquad \text{con} \qquad 0 \le r \le b-1.$$

Poiché $n \ge b$, e $b \ge 2$, si ha $1 \le q < n$. Per ipotesi induttiva

$$q = a'_k b^k + \cdots + a'_2 b^2 + a'_1 b + a'_0$$

con $0 \le a'_i \le b-1$ per $i = 0, 1, \ldots, k$ e $a'_k \ne 0$. Allora, ponendo $a_0 = r$,

$$n = (a'_k b^k + \cdots + a'_2 b^2 + a'_1 b + a'_0)b + a_0 = a'_k b^{k+1} + \cdots + a'_2 b^3 + a'_1 b^2 + a'_0 b + a_0,$$

che è una rappresentazione b-adica di n.

Proviamo ora l'unicità. Il caso $n < b$ è banale; supponiamo quindi $n \ge b$, e di avere due rappresentazioni b-adiche di n,

$$a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0 = n = a'_k b^k + \cdots + a'_2 b^2 + a'_1 b + a'_0.$$

Siccome $n \ge b$ si ha $k \ge 1$. Allora, poiché $0 \le a_0 \le b-1$ e $n = (a_k b^{k-1} + \cdots + a_2 b + a_1)b + a_0$, si ha che $q = a_k b^{k-1} + \cdots + a_2 b + a_1$ e a_0 sono, rispettivamente il quoziente ed il resto della divisione di n per b. La stessa cosa vale per la seconda rappresentazione. Per l'unicità di quoziente e resto si ha dunque $a_0 = a'_0$ e

$$a_k b^{k-1} + \cdots + a_2 b + a_1 = a'_k b^{k-1} + \cdots + a'_2 b + a'_1.$$

Per ipotesi induttiva si conclude che $a_i = a'_i$ per ogni $i = 0, 1, 2, \ldots, k$. ∎

La dimostrazione del Teorema 2.10 suggerisce anche un metodo per calcolare le cifre di una rappresentazione b-adica, che lasciamo a chi legge di rendere esplicito (si comincia dividendo n per b, $n = qb + r$, e si prende $a_0 = r$, dopo di che ...).

Esercizio 2.2. Scrivere il numero 2007, rispettivamente, in base 2, 3, 6 e 7.

Soluzione. Vediamo la scrittura del numero (decimale) $n = 2007$ in base 7. Si divide il numero per 7, ottenendo $n = 286 \cdot 7 + 5$; quindi, **5** è la prima cifra (a destra) della rappresentazione in base 7. Si procede dividendo il quoziente ottenuto di sopra: $286 = 40 \cdot 7 + 6$ (la seconda cifra è quindi **6**. Si procede dividendo l'ultimo quoziente: $40 = 5 \cdot 7 + 5$, che fornisce la terza cifra (da destra), **5**, ed anche la quarta, che è ancora **5**. In conclusione la scrittura di $n = 2007$ in base 7 è **5565**. L'eventuale verifica della correttezza si esegue "sviluppando" in base 7:

$$5 \cdot 7^3 + 5 \cdot 7^2 + 6 \cdot 7 + 5 = 5 \cdot 343 + 5 \cdot 49 + 6 \cdot 7 + 5 = 1715 + 245 + 42 = 2007.$$

Procedendo in modo simile, si trova che la scrittura di 2007 in base 2 è 11111010111; quella in base 3 è 2202100, e quella in base 6 è 13143.

Problema 1 (Italia[2], 2013)**.** *In quali basi $b > 6$ la scrittura* 5654 *rappresenta una potenza di un numero primo?*

Soluzione. Il numero rappresentato dalla scrittura 5654 nella base b è

$$5b^3 + 6b^2 + 5b + 4 = 5b^3 + 5b^2 + b^2 + b + 4b + 4 = (5b^2 + b + 4)(b + 1).$$

Poiché sicuramente uno tra i due fattori $b+1$ e $5b^2+b+4$ è un numero pari, se tale numero è la potenza di un primo deve necessariamente essere una potenza di 2. In particolare $b+1 = 2^m$ per qualche $m \geq 3$ (dato che $b \geq 7$). Dunque $b = 2^m - 1$ che, sostituito nell'altro fattore dà, per qualche $k \geq 0$

$$2^k = 5b^2 + b + 4 = 5(2^{2m} - 2^{m+1} + 1) + (2^m - 1) + 4 = 5 \cdot 2^{2m} - 9 \cdot 2^m + 8.$$

Questo forza $m = 3$ e, di conseguenza, $b = 7$. Infatti, facendo una verifica

$$5 \cdot 7^3 + 6 \cdot 7^2 + 5 \cdot 7 + 4 = 5 \cdot 343 + 6 \cdot 49 + 35 + 4 = 2048 = 2^{11}.$$

Dunque la sola base $b > 6$ in cui la scrittura 5654 rappresenta una potenza di un numero primo è $b = 7$. ∎

2.4. Divisibilità e MCD.

Dati due numeri interi $a, b \in \mathbb{Z}$, si dice che a *divide* b (e si scrive $a|b$) se esiste $c \in \mathbb{Z}$ tale che $ac = b$. In tal caso, si dice che a è un *divisore* di b, oppure che b è un *multiplo* di a. Chiaramente, se $b \in \mathbb{Z}$, dalla definizione discende che $1, -1, b$ e $-b$ sono divisori di b. Un divisore a di b si dice *proprio* se a è diverso da $1, -1, b, -b$. Osserviamo che, seconda la definizione appena data, ogni intero z divide 0: infatti $z \cdot 0 = 0$.

Veniamo ora alla definizione esatta di Massimo Comun Divisore. Siano $a, b \in \mathbb{Z}$. Si chiama **massimo comun divisore** (MCD) di a, b ogni numero intero d che soddisfa alle seguenti condizioni

- $d|a$ e $d|b$;
- per ogni $x \in \mathbb{Z}$, se $x|a$ e $x|b$ allora $x|d$.

Se a è un qualsivoglia numero intero, segue subito dalla definizione, e dall'osservazione di sopra, che a mè un MCD di a e 0. In particolare, se $a = 0 = b$, $MCD(a, b) = 0$; in tutti gli altri casi un massimo comun divisore esiste ed è diverso da zero. Più precisamente,

[2]Gli esercizi denominati "problema" sono tratti da varie competizioni matematiche; questo proviene dalla Olimpiade Matematica Italiana del 2013.

Teorema 2.11 (Formula di Bezout[3]). *Siano $a, b \in \mathbb{Z}$ due numeri interi non entrambi nulli. Allora*

1) *il minimo intero $d > 0$ che si può scrivere nella forma $d = \alpha a + \beta b$, con $\alpha, \beta \in \mathbb{Z}$ è un MCD di a e b;*

2) *esistono due MCD di a e b, che sono d e $-d$.*

Dimostrazione. Siano a e b numeri interi non siano entrambi nulli; allora si ha $a^2 + b^2 > 0$ e dunque l'insieme di numeri naturali

$$S = \{\ s |\ s \in \mathbb{N} \ \text{ e } \ 0 \neq s = ax + by \ \text{ con } \ x, y \in \mathbb{Z}\ \}$$

non è vuoto e quindi, per il buon ordinamento di $\mathbb{N}$, ammette un minimo.
Sia $d = \min(S)$. Proviamo che d è un MCD di a, b. Poichè $d \in S$, esistono $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$. Mostriamo ora che $d|a$. Dividendo a per d, troviamo interi $q, r \in \mathbb{Z}$ tali che

$$a = qd + r \quad \text{ e } \quad 0 \leq r < d$$

(dato che $d > 0$). Allora

$$r = a - dq = a - (\alpha a + \beta b)q = a(1 - \alpha q) + b(-\beta q)$$

se fosse $r > 0$, allora $r \in S$ e quindi $r \geq d = \min(S)$ contraddicendo la condizione sul resto $r < d$. Quindi deve essere $r = 0$, cioè $a = qd$ che significa $d|a$.
Allo stesso modo si prova che $d|b$.

Sia ora $c \in \mathbb{Z}$ tale che $c|a$ e $c|b$; allora $c|\alpha a$ e $c|\beta b$, e quindi $c|\alpha a + \beta b = d$.
Questo completa la dimostrazione del punto 1). .

Per dimostrare il punto (3), supponiamo che d_1 sia un altro MCD di a, b. Allora, in particolare, $d|d_1$ e $d_1|d$; cioè esistono $x, y \in \mathbb{Z}$ tali che $d = xd_1$ e $d_1 = yd$. Da ciò segue

$$d = xd_1 = x(yd) = (xy)d$$

e, poichè $d \neq 0$, questo implica $xy = 1$, e siccome $x, y \in \mathbb{Z}$, deve essere $x = y = 1$ oppure $x = y = -1$ che dà $d_1 = d$ oppure $d_1 = -d$. ∎

Dunque, dati due interi a, b non entrambi nulli, esiste un unico MCD d di a, b con $d \geq 1$; tale MCD lo denotiamo con $MCD(a, b)$ (o spesso, quando non ci sia pericolo di confusione, semplicemente con (a, b)). Per il punto 1) del Teorema, esso è il più piccolo numero positivo che si può scrivere nelle forma $\alpha a + \beta b$, con $\alpha, \beta \in \mathbb{Z}$. Ad esempio, poiché $6 \cdot 26 + (-5) \cdot 31 = 1$, si ha che $(26, 31) = 1$.

Due interi a, b non entrambi nulli si dicono **coprimi** se $(a, b) = 1$. Dal Teorema precedente e dalla sua dimostrazione, si ricava il seguente importante

Criterio. *Due interi a, b non entrambi nulli sono coprimi se e solo se esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$.*

Osservazione. La definizione di m.c.d. si estende in modo naturale (lo si faccia per esercizio) dal caso di una coppia ad un numero arbitrario $n \geq 2$ di interi e procedendo per induzione su n si dimostra che il m.c.d. esiste sempre. Similmente si estende anche la formula di Bezout (la dimostrazione è lasciata per esercizio).

[3] Étienne Bézout (1730–1783), matematico francese.

Proposizione 2.12. *Siano $a_1, a_2, \ldots, a_n$ numeri interi non tutti nulli e sia d il minimo intero positivo tale che si rappresenta nella forma*

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = d,$$

con $x_1, x_2, \ldots, x_s \in \mathbb{Z}$. Allora $d = mcd(a_1, a_2, \ldots, a_s)$.

Problema 2 (IMO[4] 1959)**.** *Provare che per ogni intero positivo n la frazione*

$$\frac{21n+4}{14n+3}$$

è in forma ridotta.

Soluzione. Si tratta di provare che, per ogni intero positivo n,

$$mcd(21n+4, 14n+3) = 1.$$

Ma si trova subito che

$$3(14n+3) + (-2)(21n+4) = 1,$$

quindi, per il Criterio sopra enunciato, $21n+4$ e $14n+3$ sono coprimi.

Problema 3 (Putnam[5], 2000)**.** *Si provi, che per ogni coppia di interi $n \geq m \geq 1$, l'espressione*

$$\frac{mcd(m,n)}{n}\binom{n}{m}$$

è un numero intero.

Soluzione. Sia $d = \mathrm{m}cd(m,n)$. Per la Formula di Bezout esistono due numeri interi a, b tali che $d = an + bm$. Dunque

$$\frac{d}{n}\binom{n}{m} = \frac{an+bm}{n}\binom{n}{m} = a \cdot \binom{n}{m} + b \cdot \frac{m}{n}\binom{n}{m} = a \cdot \binom{n}{m} + b \cdot \binom{n-1}{m-1},$$

che è un numero intero.

Problema 4 (Germania 1996)**.** *Una pietra si muove sui punti a coordinate intere del piano secondo le regole seguenti:*

(i) *Da ogni punto (a,b) la pietra può spostarsi in $(2a,b)$ oppure $(a,2b)$.*

(ii) *Da ogni punto (a,b) la pietra può muovere in $(a-b,b)$ se $a > b$, oppure in $(a,b-a)$ se $a < b$.*

Si dica quali punti (x,y) può raggiungere la pietra partendo dal punto $(1,1)$.

Soluzione. Siano a, b interi positivi e $d = mcd(a,b)$; allora $mcd(a-b,b) = mcd(a,b-a) = d$, mentre $mcd(2a,b) = 2^\epsilon d$ e $mcd(2a,b) = 2^\mu d$, dove $\epsilon, \mu \in \{0,1\}$.
Quindi, nel gioco descritto dal Problema, ogni mossa lecita della pietra sposta questa da un punto (a,b) a coordinate intere in un punto il cui massimo comun divisore delle coordinate è uguale oppure il doppio di $mcd(a,b)$. Da ciò segue immediatamente che se il punto (x,y) si può raggiungere da $(1,1)$ allora $mcd(x,y) = 2^t$ per qualche $t \geq 0$.

[4]Questo problema fu proposto nella prima Olimpiade Matematica Internazionale, tenutasi a Bucarest nel 1959; oggi, problemi così facili non se ne vedono.

[5]La *William Lowell Putnam mathematical competition* è un gara matematica per studenti dei primi anni dell'Università che si disputa annualmente tra Canada e Stati Uniti dal 1938 (con l'interruzione negli anni della seconda guerra mondiale).

Viceversa, proviamo che ogni punto (x, y), con $x, y \in \mathbb{N}^*$ e tale che $mcd(x, y) = 2^t$ per qualche $t \in \mathbb{N}$, è raggiungibile da $(1, 1)$ in un numero finito di mosse. Per induzione su $x+y$. Se $x + y = 2$, $(x, y) = (1, 1)$ e non c'è altro da aggiungere. Sia $x + y > 2$. Se $x = 2a$ è pari allora $mcd(a, y)$ è una potenza di due, (a, y) è raggiungibile da $(1, 1)$ per ipotesi induttiva e quindi (x, y) è raggiungibile dato che ci si arriva da (a, y) con una mossa di tipo (i); lo stesso argomento si applica se y è pari. Rimane il caso in cui sia x che y sono dispari, quindi $mcd(x, y) = 1$ e in particolare $x \neq y$; sia $x > y$, allora

$$mcd\Big(\frac{x+y}{2}, y\Big) = 1 \quad \text{e} \quad \frac{x+y}{2} + y < x + y,$$

dunque $(\frac{x+y}{2}, y)$ è raggiungibile da $(1, 1)$ per ipotesi induttiva, e quindi (x, y) è raggiungibile:

$$(1, 1) \to \Big(\frac{x+y}{2}, y\Big) \xrightarrow{\text{(i)}} (x + y, y) \xrightarrow{\text{(ii)}} (x, y).$$

La stessa cosa, nella seconda componente, si fa se $y > x$. In conclusione: (x, y) è raggiungibile da $(1, 1)$ se e soltanto se $mcd(x, y)$ è una potenza di 2.

Problema 5 (San Pietroburgo 2008)**.** *Siano a, b e c interi positivi distinti; si provi che*

$$mcd(ab + 1, ac + 1, bc + 1) < \frac{a + b + c}{3}.$$

Soluzione. Siano a, b, c interi positivi con $a < b < c$ e sia $d = mcd(ab + 1, ac + 1, bc + 1)$. Allora,

$$d \mid (ab + 1)c - a(bc + 1) = c - a,$$

e similmente si prova $d|b-a$. Quindi esistono due numeri interi m, n con $1 \leq m < n$ (perché $a < b < c$, si osservi anche $m + n \geq 3$) tali che

$$\begin{aligned} b &= a + md \\ c &= a + nd. \end{aligned}$$

Dunque

$$\frac{a + b + c}{3} = \frac{a + (a + md) + (a + nd)}{3} = \frac{3a + (m + n)d}{3} \geq \frac{3a + 3d}{3} = a + d > d,$$

come si voleva. ∎

L'Algoritmo di Euclide. L'algoritmo di Euclide (che, come suggerisce il nome, è uno degli algoritmi più antichi) è un metodo meccanico per determinare il MCD di due numeri interi (ma si applica anche in altri contesti - come ad esempio quello dei polinomi). Come vedremo, il passo fondamentale è assicurato dalla seguente semplice proprietà.

Lemma 2.13. *Siano a, b numeri interi non nulli, e sia r il resto della divisione di a per b. Si provi che $(a, b) = (b, r)$.*

Dimostrazione. Per esercizio. ∎

Veniamo all'algoritmo vero e proprio. Siano a, b numeri interi non nulli, che possiamo supporre positivi (infatti, per come è definito, è chiaro che $(a, b) = (|a|, |b|)$.
Poniamo $a_1 = a$ e $a_2 = b$. Iniziamo con dividere a_1 per a_2:

$$a_1 = q_1 a_2 + a_3 \quad \text{con} \quad 0 \leq a_3 < |a_2|$$

quindi si divide a_2 per a_3, ottendo un resto a_4 con $0 \leq a_4 < a_3$. Si prosegue con tale catena di divisioni; ovvero arrivati ad a_i si definisce a_{i+1} come il resto della divisione di a_{i-1} per a_i:

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 \\ a_2 &= q_2 a_3 + a_4 \\ a_3 &= q_3 a_4 + a_5 \\ &\cdots\cdots \\ a_{i-1} &= q_{i-1} a_i + a_{i+1} \\ &\cdots\cdots \end{aligned}$$

in questo modo si ottiene una sequenza di resti

$$|a_2| > a_3 > a_4 > \cdots > a_{i-1} > a_i > \cdots > a_n = 0$$

Poichè tali resti sono numeri interi, tale sequenza arriva a zero dopo un numero finito di passi (che abbiamo indicato con n). Sia quindi a_{n-1} l'ultimo resto non nullo. Utilizzando il Lemma precedente si provi che $a_{n-1} = (a_1, a_2) = (a, b)$.

Esempio. Calcolare il MCD di 6468 e 2275. Si ha

$$\begin{aligned} 6468 &= 2 \cdot 2275 + 1918 \\ 2275 &= 1 \cdot 1918 + 357 \\ 1918 &= 5 \cdot 357 + 133 \\ 357 &= 2 \cdot 133 + 91 \\ 133 &= 1 \cdot 91 + 42 \\ 91 &= 2 \cdot 42 + 7 \\ 42 &= 6 \cdot 7 + 0 \end{aligned}$$

quindi $(6468, 2275) = 7$.

Osserviamo come l'algoritmo di Euclide, dati due interi positivi a e b, oltre a fornire il loro MCD, $d = (a, b)$, consente di trovare coefficienti interi α e β tali che $d = a\alpha + b\beta$. Vediamo come, mediante l'esempio di sopra. Quindi $a = 6468$, $b = 2275$, e $d = 7$. Riutilizzando all'indietro le uguaglianze determinate dalle divisioni successive si ha

$$\begin{aligned} 7 &= 91 + (-2)42 = 91 + (-2)(133 - 91) = 3 \cdot 91 + (-2)133 = \\ &= 3(357 - 2 \cdot 133) + (-2)133 = 3 \cdot 357 + (-8)133 = \\ &= 3 \cdot 357 + (-8)(1918 - 5 \cdot 357) = (-8)1918 + 43 \cdot 357 = \\ &= (-8)1918 + 43(2275 - 1918) = 43 \cdot 2275 + (-51)1918 = \\ &= 43 \cdot 2275 + (-51)(6468 - 2 \cdot 2275) = (-51)6468 + 145 \cdot 2275. \end{aligned}$$

2.5. Numeri primi

Un concetto di fondamentale importanza nella storia e nella pratica della matematica è quello di numero primo. Un numero intero p si dice *primo* se

- $p \neq 0, 1, -1$;
- per ogni $a \in \mathbb{Z}$ se a divide p allora $a \in \{1, -1, p, -p\}$.

In altre parole, un intero è un primo se è diverso da $0, 1, -1$, e non ha divisori propri.

Il Lemma seguente[6] enuclea una proprietà fondamentale dei numeri interi, che non è scontata quanto sembra (come vedremo nella seconda parte del corso).

Lemma 2.14 (Lemma di Euclide)**.** *Siano a, b, n numeri interi tali che $n|ab$. Se $MCD(a, n) = 1$ allora $n|b$.*

Dimostrazione. Siano a, b, n come nell'ipotesi, e supponiamo che n ed a siano coprimi. Allora esistono $x, y \in \mathbb{Z}$ tali che $xa + yn = 1$, da cui si ottiene

$$b = 1 \cdot b = xab + ynb.$$

Poichè $n|ab$, da ciò segue che n divide b. ∎

Corollario 2.15. *Siano $a, b, p \in \mathbb{Z}$ con p primo:*

$$\text{se } p|ab \quad \text{allora} \quad p|a \text{ o } p|b.$$

Dimostrazione. Infatti, se $p \not| a$ allora, poiché p è primo, $MCD(a, p) = 1$. ∎

Osservazione. Procedendo per induzione su n si prova facilmente che se $a_1, \ldots, a_n \in \mathbb{Z}$ e p è un primo tale che $p|a_1 a_2 \cdots a_n$, allora $p|a_i$ per almeno un $i = 1, 2, \ldots, n$.

Esercizio 2.3. Sia $p \in \mathbb{Z}$, $p \neq 0, 1, -1$. Supponiamo che per ogni $a, b \in \mathbb{Z}$ sia verificata

$$p|ab \quad \Rightarrow \quad p|a \text{ o } p|b.$$

Si provi che p è un numero primo.

Soluzione. $p \neq 0, 1, -1$ per ipotesi. Sia $b \in \mathbb{Z}$ un divisore di p; allora esiste $c \in \mathbb{Z}$ tale che $p = cb$. Ora, da ciò segue in particolare che $p|cb$; quindi, per ipotesi, $p|b$ oppure $p|c$. Se $p|b$ si ha $b = \pm p$; mentre da $p|c$ segue $b = \pm 1$. Dunque, in ogni caso $b \in \{1, -1, p, -p\}$ e pertanto p è un primo.

Problema 6 (Iberoamericana[7], 2006)**.** *Determinare tutte le coppie (a, b) di numeri interi positivi tali che $2a - 1$ e $2b + 1$ sono coprimi e $a + b$ divide $4ab + 1$.*

Soluzione. Sia (a, b) una delle coppie cercate. Allora

$$a + b \mid 4a(a + b) - (4ab + 1) = 4a^2 - 1 = (2a + 1)(2a - 1), \qquad (*)$$

e similmente

$$a + b \mid 4b(a + b) - (4ab + 1) = 4b^2 - 1 = (2b + 1)(2b - 1). \qquad (**)$$

Sia $d = mcd(a + b, 2b + 1)$. Poiché d e $2a - 1$ sono coprimi per ipotesi, da $(*)$ e il Lemma di Euclide segue che d divide $2a + 1$, quindi d divide $(2b + 1) + (2a + 1) - 2(a + b) = 2$, e pertanto, poiché $2b + 1$ è dispari, $d = 1$. Dunque, $a + b$ e $2b + 1$ sono coprimi e da $(**)$ (e ancora iol Lemma di Euclide) si deduce che $a+b$ divide $2b-1$. In particolare, $a+b \leq 2b-1$ e pertanto $a+1 \leq b$. Similmente si dimostra che $a+b$ divide $2a+1$, quindi $a+b \leq 2a+1$ e dunque $b \leq a+1$. In conclusione $b = a+1$. La verifica che tutte le coppie del tipo $(a, a+1)$ con $a \geq 1$ soddisfano la condizione assegnata è immediata.

Di fatto, il Lemma di Euclide ed il suo Corollario 2.15 sono alla base di molte interessanti proprietà aritmetiche dell'insieme dei numeri intero. A partire dal cosiddetto "*Teorema fondamentale dell'Aritmetica*".

[6] Lo chiamiamo Lemma di Euclide per semplificarne il richiamo; quello che, nella sostanza, è il contenuto della proposizione 30 del Libro VII degli *Elementi* di Euclide è il caso in cui n è un numero primo, ovvero il Corollario che segue.

[7] *Olimpiada Iberoamericana de Matematicas*, si disputa dal 1985.

Teorema 2.16. *Sia $z \in \mathbb{Z}$ un intero diverso da $0, 1, -1$. Allora esistono numeri primi $p_1, p_2, \ldots, p_n$ tali che*

$$z = p_1 \cdot p_2 \cdot p_3 \cdots p_n.$$

Inoltre tale fattorizzazione è unica a meno del segno dei numeri primi e del loro ordine nel prodotto.

Dimostrazione. (esistenza) Supponiamo prima $z > 0$ (quindi $z \geq 2$) e applichiamo il principio di induzione nella seconda forma.
Se $z = 2$ allora la cosa è banale. Supponiamo ora che $z \geq 3$ e che, per ipotesi induttiva, una fattorizzazione in prodotto di primi esista per ogni $2 \leq k \leq z - 1$.
Se z è primo, allora è gia fattorizzato (con un solo fattore). Supponiamo quindi che z non sia primo. Allora z ha almeno un divisore proprio k ; quindi $z = kb$ con $2 \leq k, b \leq z - 1$. Ma, per ipotesi induttiva, k e b sono un prodotto di numeri primi, e quindi anche z è tale.
Sia ora $z < 0$; allora $-z > 0$ e quindi, per quanto appena visto, $-z = p_1 \cdot p_2 \cdots p_n$, con $p_1, p_2, \ldots, p_n$ numeri primi; quindi $z = (-p_1) \cdot p_2 \cdot p_3 \cdots p_n$. La prova di esistenza è completata.

(unicità) Supponiamo che $p_1, p_2, \ldots, p_n$ e $q_1, q_2, \ldots, q_s$ siano primi tali che

$$p_1 \cdot p_2 \cdots p_n = z = q_1 \cdot q_2 \cdots q_s \ .$$

Allora $p_1 | z = q_1 \cdot q_2 \cdots q_s$, quindi per l'osservazione che segue il Lemma precedente, p_1 divide almeno uno dei q_i. A meno di riordinare $q_1, q_2, \ldots, q_s$ possiamo supporre che $p_1 | q_1$, ma allora, essendo primi, $p_1 = q_1$ oppure $p_1 = -q_1$.
Dividendo ora z per p_1 si ottiene dunque

$$p_2 \cdot p_3 \cdots p_n = \frac{z}{p_1} = \pm q_2 \cdot q_3 \cdots q_s \ .$$

Procedendo in questo modo alla fine si ricava $n = s$, ed anche l'unicità dei primi nelle due fattorizzazioni, a meno dell'ordine e dei segni. ∎

Una delle applicazioni più famose del teorema di fattorizzazione in primi è la dimostrazione dell'esistenza di infiniti numeri primi; un risultato dovuto a Euclide (sostanzialmente con la stessa dimostrazione) e che ammette diverse altre dimostrazioni (anche molto diverse).

Teorema 2.17. (Teorema di Euclide) *Esistono infiniti numeri primi positivi.*

Dimostrazione. Supponiamo per assurdo che l'insieme dei numeri primi positivi sia finito, e siano allora $p_1, p_2, \ldots, p_t$ tutti i numeri primi positivi distinti. Consideriamo il numero intero

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_t + 1 \ .$$

Allora $N \geq 2$ e c'è un fattore primo q di N. Essendo primo, q deve essere uno dei p_i; ma allora $q | p_1 \cdot p_2 \cdots p_t$ e quindi q divide $N - p_1 \cdot p_2 \cdots p_t = 1$, assurdo. ∎

Radici di numeri interi. Un'altra semplice ma fondamentale applicazione del Lemma 2.14 riguarda le radici di numeri interi. Se x è un numero reale positivo e m un numero naturale positivo, denotiamo con $\sqrt[m]{x}$ l'unica radice m-esima reale e positiva di x.

Teorema 2.18. *Siano a, m numeri interi positivi, allora $\sqrt[m]{a} \in \mathbb{Q}$ se e solo se $\sqrt[m]{a} \in \mathbb{N}$ (cioè a è la potenza m-esima di un numero intero positivo).*

Dimostrazione. Sia $\sqrt[m]{a}$ un numero razionale, cioè $\sqrt[m]{a} = \frac{r}{s}$ con r, s interi positivi e coprimi. Allora, elevando alla m-esima potenza,

$$s^m a = r^m.$$

In particolare, $a | r^m$. D'altra parte, poiché $(s^m, r^m) = 1$, il Lemma 2.14 assicura che r^m divide a. Dunque $a = r^m$ e $\sqrt[m]{a} = r \in \mathbb{N}$. □

In particolare, si deduce che *se p un numero primo positivo allora $\sqrt{p}$ è un numero irrazionale* (ad esempio, $\sqrt{2}$, così come $\sqrt{17}$, è un numero irrazionale).

Esercizio 2.4. Siano $a, b \in \mathbb{N}^*$ tali che $\sqrt{a} + \sqrt{b} \in \mathbb{Q}$; provare che a e b sono quadrati in $\mathbb{N}$.

Soluzione. Sia $\sqrt{a} + \sqrt{b} = x$, con $x \in \mathbb{Q}$; allora

$$2\sqrt{ab} = (\sqrt{a} + \sqrt{b})^2 - (\sqrt{a}^2 + \sqrt{b}^2) = x^2 - a - b$$

è un numero razionale. Dunque, per il Teorema 2.18, $ab = t^2$ per qualche $t \in \mathbb{N}$. Allora

$$x = \sqrt{a} + \sqrt{b} = \sqrt{a} + \frac{t}{\sqrt{a}},$$

da cui

$$\sqrt{a} = \frac{a + t}{x} \in \mathbb{Q}.$$

Dunque, a è un quadrato in $\mathbb{N}$ per il Teorema 2.18; di conseguenza anche $\sqrt{b} \in \mathbb{Q}$ e b è un quadrato in $\mathbb{N}$. ■

Problema 7 (Czech-Polish-Slovak[8], 2002)**.** *Siano $n, p \in \mathbb{N}^*$ con $n \geq 2$ e p un primo. Si provi che se $n | p - 1$ e $p | n^3 - 1$ allora $4p - 3$ è un quadrato perfetto.*

Soluzione. Per ipotesi esiste $k \geq 1$ tale che $p = kn + 1$. Ora $n^3 - 1 = (n - 1)(n^2 + n + 1)$, e siccome p è primo ed è maggiore di n,

$$p = kn + 1 \big| n^2 + n + 1.$$

Ciò implica in particolare $k \leq n + 1$. D'altra parte, p divide

$$-np + k(n^2 + n + 1) = k(n^2 + n + 1) - n(nk + 1) = kn - n + k,$$

dunque $p = kn + 1 \leq kn - n + k$, da cui $k \geq n + 1$. Quindi $k = n + 1$ e $p = kn + 1 = n^2 + n + 1$, e pertanto

$$4p - 3 = 4n^2 + 4n + 1 = (2n + 1)^2.$$

Minimo Comune Multiplo. Siano $a, b \in \mathbb{Z}$. Si chiama *minimo comune multiplo* (m.c.m.) di a, b ogni numero intero m che soddisfa alle seguenti condizioni

- $a | m$ e $b | m$;
- per ogni $x \in \mathbb{Z}$, se $a | x$ e $b | x$ allora $m | x$.

Lasciamo per esercizio (vedi Esercizio 2.5) la dimostrazione dell'analogo del Teorema 2.11, ovvero che ogni coppia di interi entrambi non nulli a e b esiste un m.c.m.; anzi,

[8] Il *Czech–Polish–Slovak Match* si disputa dal 1995 (tra Cechia e Slovacchia prima, dal 2001 si è aggiunta la Polonia).

più precisamente ce ne sono due, uno l'opposto dell'altro; quello positivo si denota con $\text{m.c.m.}(a,b)$, o a volte, anche con $[a,b]$.

Avendo a disposizione la fattorizzazione in potenze di numeri primi dei due interi (non nulli) a e b, è facile determinare il loro MCD ed il loro m.c.m. Nella pratica però, fattorizzare un numero in potenze di numeri primi richiede molto più lavoro (e tempo) che effettuare divisioni con resto con termini dati in precedenza (in sostanza, perché per trovare un fattore non sappiamo prima per cosa dividere); l'algoritmo di Euclide è quindi il metodo più efficiente (e quello tuttora implementato) per determinare il MCD di numeri di cui non si conoscono i fattori primi.

Ricordiamo tuttavia la descrizione del MCD, date la fattorizzazioni dei termini. Siano a e c numeri interi non nulli, che per semplicità supponiamo entrambi positivi, e siano

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \quad \text{e} \quad c = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$$

le loro fattorizzati mediante potenze di numeri primi distinti $p_1, p_2, \dots, p_k$, e dove abbiamo eventualmente aggiunto potenze di esponente zero per quei primi che sono divisori di uno solo dei due numeri. Supponiamo che c divida a; allora esiste un intero $r = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ tale che $a = cr$ quindi

$$a = p_1^{s_1+r_1} p_2^{s_2+r_2} \dots p_k^{s_k+r_k}$$

da cui segue in particolare $r_i \le n_i$ per ogni $i = 1, 2 \dots, k$.

Siano ora a, b interi (positivi) non entrambi nulli. Se uno dei due è zero, allora il secondo è un MCD di a e b. Supponiamo quindi che siano entrambi non nulli e fattorizziamoli come potenze di primi:

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \qquad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$$

con il solito accorgimento sugli esponenti. Consideriamo ora l'elemento

$$d = p_1^{\min\{n_1,m_1\}} p_2^{\min\{n_2,m_2\}} \dots p_k^{\min\{n_k,m_k\}} ;$$

chiaramente d divide sia a che b e, dalla osservazione fatta sopra, segue facilmente che d è un MCD di a e b.
Se invece prendiamo

$$m = p_1^{\max\{n_1,m_1\}} p_2^{\max\{n_2,m_2\}} \dots p_k^{\max\{n_k,m_k\}},$$

allora $m = \text{m.c.m}(a,b)$.

Esercizio 2.5. Siano a, b numeri interi positivi. Si provi che

$$[a,b] = \frac{ab}{(a,b)}.$$

Soluzione. Sia $m = \frac{ab}{(a,b)}$. Allora $m = a \cdot \frac{b}{(a,b)} = b \cdot \frac{a}{(a,b)}$, è un multiplo comune di a e di b. Sia ora t un multiplo comune di a e di b (sia $t = ac = bc'$, con $c, c' \in \mathbb{Z}$, e siano $\alpha, \beta \in \mathbb{Z}$ tali che $(a,b) = \alpha a + \beta b$. Allora $(a,b)t = \alpha at + \beta bt = ab(\alpha c' + \beta c)$; quindi $t = m(\alpha c' + \beta c)$, che è un multiplo di m. In questo modo abbiamo anche provato l'esistenza del m.c.m.

LETTURA. Ora alcune pratiche identità, facili da provare ma utili. Intanto, ricordiamo l'espressione delle somme di una serie geometrica: siano $1 \neq a \in \mathbb{R}$, e $1 \le n \in \mathbb{N}$, allora:

$$1 + a + a^2 + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}.$$

Lemma. *Siano $a, n, m \in \mathbb{N}^*$, con $a \neq 1$. Allora*

$$(a^n - 1, a^m - 1) = a^{(n,m)} - 1 \ .$$

Dimostrazione. Dall'identità di sopra, si ricava in particolare che se $c \in \mathbb{N}$ divide n, allora $a^c - 1$ divide $a^n - 1$. Quindi, se $d = (a^n - 1, a^m - 1)$ e $c = (n, m)$, allora, $a^c - 1$ divide d. Viceversa, siano $u, -v \in \mathbb{Z}$, tali che $c = un + (-v)m = un - vm$. Allora, scambiando eventualmente n e m, u, v sono positivi. Ancora per le proprietà delle serie geometriche, abbiamo che d divide $a^{nu} - 1$ e $a^{mv} - 1$. Quindi d divide la differenza,

$$a^{nu} - a^{mv} = a^{mv}(a^{nu-mv} - 1) = a^{mv}(a^c - 1).$$

Poiché d ed a sono chiaramente coprimi, si conclude che d divide $a^c - 1$. ∎

Lemma. *Siano $n \in \mathbb{N}^*$, $n > 1$.*

(1) *Sia $a \in \mathbb{N}^*$; se $a^n - 1$ è un primo, allora $a = 2$ e n è un primo.*

(2) *Sia p un primo; se $p^n + 1$ è un primo, allora $p = 2$ e $n = 2^m$ per qualche $m \in \mathbb{N}^*$.*

Dimostrazione. (1) Poichè $a^n - 1 = (a - 1)(a^{n-1} + \cdots + a + 1)$, se $a^n - 1$ è primo allora $a = 2$ e, per la stessa considerazione, n è primo.
(1) Se $p^n + 1$ è primo allora deve essere dispari e quindi $p = 2$. Supponiamo che n abbia un divisore primo dispari q, e scriviamo $n = mq$. Allora $2^n + 1 = (2^m + 1)(2^{m(q-1)} - (2^{m(q-1)} + \cdots - 2^m + 1)$ non è primo. Dunque, se $2^n + 1$ è primo, n deve essere una potenza di 2. ∎

I numeri primi del tipo (2) sono detti *primi di Fermat*. In generale, per $m \in \mathbb{N}$, l'intero $F_m = 2^{2^m} + 1$ è detto m-esimo numero di Fermat. I primi cinque numeri di Fermat

$$F_0 = 3, \ F_1 = 5, \ F_2 = 17, \ F_3 = 257, \ F_4 = 65537$$

sono numeri primi. Sulla base di questa osservazione, P. Fermat affermò che ogni intero di questo tipo è primo. Fu L. Eulero a scoprire come il termine successivo $F_5 = 2^{32} + 1$ non sia primo: infatti $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$, dunque

$$2^{32} = 2^4 \cdot 2^{28} = (641 - 5^4) \cdot 2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 = 641 \cdot 2^{28} - (641 - 1)^4$$

e quindi esiste un intero positivo t tale che $2^{32} = 641t - 1$, cioè 641 divide $2^{32} + 1 = F_5$ (si verifica che $F_5 = 641 \cdot 6700417$, dove 641 e 6700417 sono numeri primi). Di fatto, oltre ai cinque detti, nessun altro primo di Fermat è stato a tutt'oggi trovato; e neppure è noto se ne esistano un numero infinito o finito, né se esistano infiniti numeri non-primi nella serie F_n (è stato verificato che, per $5 \leq m \leq 21$, F_m non è un primo). Eppure, i primi di Fermat intervengono in diverse situazioni; ad esempio, un celeberrimo teorema di Gauss stabilisce che l'n-agono regolare si può disegnare con "riga e compasso" se e solo se $n = 2^t p_1 \cdots p_s$, con $t \in \mathbb{N}$ e $p_1, \ldots, p_s$ primi di Fermat distinti.

Analogamente a quanto accade per i primi di Fermat, non tutti i numeri del tipo $M_p = 2^p - 1$ (con p primo) sono primi. Quelli che lo sono, sono detti *primi di Mersenne*; il più piccolo numero di Mersenne a non essere primo è $M_{11} = 23 \cdot 89$. Anche in questo caso non è tuttora noto se esistano infiniti primi di Mersenne: ad oggi[9], risultano noti 50 primi di Mersenne, il maggiore dei quali è M_p con $p = 77232917$; che, al momento, è anche il più grande numero primo conosciuto: la sua espansione decimale impiega più di ventitre milioni di cifre (chi fosse interessato può consultare il sito internet: www.mersenne.org).

Oltre a quelle a cui abbiamo accennato, esistono molte altre suggestive congetture aperte riguardanti i numeri primi. Due fra le più famose sono:

Twin prime conjecture: esistono infinite coppie di numeri primi p e q 'consecutivi' (ovvero tali che $p - q = 2$).

[9]Luglio 2018.

Congettura di Goldbach: Ogni numero intero pari si può scrivere come somma di due numeri primi.

Importanti progressi verso queste due congetture sono stati fatti anche in tempi recenti, nella loro generalità, esse sono tuttavia ancora entrambe aperte. **FINE LETTURA**

2.6. I Numeri Complessi.

In questo capitolo abbiamo iniziato lo studio dei numeri interi, riproponendo da un punto di vista rigoroso cose in parte già note. In questo processo, abbiamo assunto per primitiva l'idea di numero intero e di insieme dei numeri interi $\mathbb{Z}$ (il che è molto ragionevole, ed è quello che i matematici hanno sempre fatto: un approfondimento sui fondamenti, e quindi anche sul modello dei numeri interi, è parte dei corsi - più avanzati - di logica). Accanto a $\mathbb{Z}$, siamo certamente già avezzi a trattare con altri insiemi numerici, quali quello dei numeri razionali $\mathbb{Q}$, e quello dei numeri reali $\mathbb{R}$. Di essi daremo una costruzione formale (a partire da $\mathbb{Z}$) più avanti nel corso; per il momento, la nozione che se ne ha dalle scuole superiori ci basta. Analogo discorso dovrebbe valere per l'insieme dei numeri complessi $\mathbb{C}$; poiché tuttavia non sempre questi vengono introdotti in modo adeguato, mentre sono uno strumento con cui è bene familiarizzarsi sin da principio, ne diamo una breve introduzione.

Si parte dall'insieme $\mathbb{R}$ dei numeri reali (che è conveniente pensare rappresentati come punti su una retta orientata in cui sia stata fissata un'origine ed un'unità di misura). Sul prodotto $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ si definiscono un'operazione di somma (addizione) ed un'operazione di prodotto (moltiplicazione), ponendo, per ogni $(a, b), (c, d) \in \mathbb{R}^2$,

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (ac - bd, ad + bc).$$

L'insieme $\mathbb{R}^2$ dotato di tali operazioni si denota con $\mathbb{C}$ e si chiama *campo dei numeri complessi*. Si verifica facilmente che sono soddisfatte le seguenti proprietà:

- La somma è associativa e commutativa. Inoltre per ogni $(a, b) \in \mathbb{C}$,

$$(a, b) + (0, 0) = (a, b) = (0, 0) + (a, b)$$
$$(a, b) + (-a, -b) = (0, 0).$$

- La moltiplicazione è associativa e commutativa. Inoltre per ogni $(a, b) \in \mathbb{C}$,

$$(a, b)(1, 0) = (a, b) = (1, 0)(a, b),$$

e se $(a, b) \neq (0, 0)$, allora

$$(a, b)(a/(a^2 + b^2), -b/(a^2 + b^2)) = (1, 0).$$

- Vale la proprietà distributiva della moltiplicazione rispetto alla somma; ovvero, per ogni $z_1, z_2, z_3 \in \mathbb{C}$, si ha

$$z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3.$$

Come vedremo più avanti, un insieme dotato di due operazioni che godono delle proprietà segnalate per $\mathbb{C}$ (è il caso, ad esempio, di $\mathbb{Q}$ e di $\mathbb{R}$) si dice un *campo* (da qui il nome "campo complesso").

La definizione dei numeri complessi mediante coppie ordinate di numeri reali, consente di accettare subito la rappresentazione dei numeri complessi come punti di un piano cartesiano. Questa rappresentazione è detta di Argand–Gauss (figura 2.1).

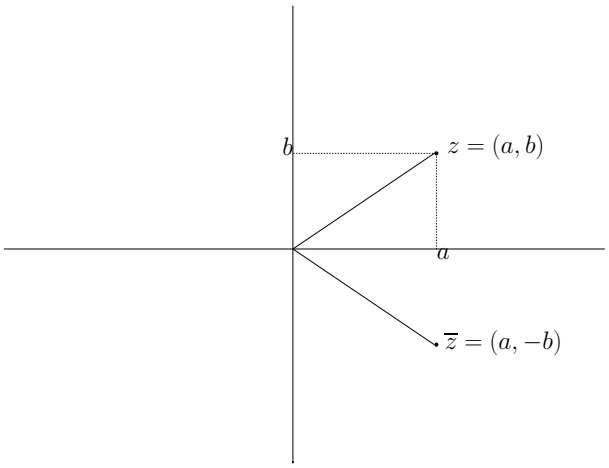

Figura 2.1: il piano di Argand–Gauss

L'applicazione

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ a & \mapsto & (a,0). \end{array}$$

è chiaramente iniettiva. Ciò consente di identificare ciascun numero reale a con la sua immagine $(a,0) \in \mathbb{C}$, e quindi di vedere $\mathbb{R}$ come un sottoinsieme di $\mathbb{C}$ (nel piano di Argand–Gauss i numeri reali sono i punti sull'asse orizzontale, che infatti sarà detto *asse reale*), e l'applicazione descritta sopra si chiama *immersione* di $\mathbb{R}$ in $\mathbb{C}$. Si osservi che questo è coerente con la notazione che avevamo già fissato per gli elementi neutri:

$$0 = (0,0) \qquad \text{e} \qquad 1 = (1,0).$$

A questo punto si pone $i = (0,1)$. Allora

$$i^2 = i \cdot i = (0,1)(0,1) = (-1,0) = -1. \tag{2.1}$$

L'elemento i appena definito si chiama *unità immaginaria* (così come l'asse verticale nel piano di Argand–Gauss si dice *asse immaginario*). Si osserva poi che per ogni $b \in \mathbb{R}$ si ha $b \cdot i = (b,0)(0,1) = (0,b) = i \cdot b$. Quindi, il generico elemento $z = (a,b) \in \mathbb{C}$ si scrive

$$z = (a,0) + (0,b) = (a,0) + (b,0)(0,1) = a + ib$$

che è la scrittura usuale per i numeri complessi; a e b si dicono e denotano, rispettivamente, la *parte reale* $Re(z)$ e la *parte immaginaria* $Im(z)$, del numero complesso $z = a + ib$. Il calcolo è molto più comodo usando questa notazione e la regola (2.1), piuttosto che le definizioni date inizialmente con le coppie ordinate di numeri reali.

Il **coniugato** $\overline{z}$ di un numero complesso $z = a + ib$ è il suo simmetrico rispetto all'asse reale, ovvero il numero corrispondente alla coppia $(a,-b)$,

$$\overline{z} = \overline{a + ib} = a - ib.$$

Il *coniugio* (complesso) è l'applicazione da $\mathbb{C}$ in se stesso che ad ogni $z \in \mathbb{C}$ associa il coniugato $\overline{z}$ (nel piano di Argand–Gauss è quindi la simmetria con asse l'asse reale). Le seguenti proprietà del coniugio si verificano facilmente.

Proposizione 2.19. *Siano $z, z_1 \in \mathbb{C}$. Allora*

1) $z + \overline{z} = 2Re(z)$, *e* $i(\overline{z} - z) = 2Im(z)$;

2) $\overline{z} = z$ *se e solo se* $z \in \mathbb{R}$;

3) $\overline{z + z_1} = \overline{z} + \overline{z}_1$;

4) $\overline{z \cdot z_1} = \overline{z} \cdot \overline{z_1}$.

La *norma* di $z = a + ib$ è definita da

$$N(z) = z\overline{z} = a^2 + b^2.$$

Quindi, per ogni $z \in \mathbb{C}$, $N(z)$ è un numero reale maggiore o uguale a zero. Il **modulo** di z è la radice quadrata della norma di z. Ovvero, se $z = a + ib$,

$$|z| = \sqrt{a^2 + b^2}.$$

Il modulo di $a + ib \in \mathbb{C}$ è quindi la lunghezza del segmento che, nel piano di Argand–Gauss, congiunge il punto (a, b) all'origine. Valgono (e si verificano facilmente) le seguenti e fondamentali proprietà,

Proposizione 2.20. *Siano $z, z_1 \in \mathbb{C}$. Allora*

1) $N(z) = 0$ *se e solo se* $z = 0$;

2) $N(zz_1) = N(z)N(z_1)$ *e* $|zz_1| = |z||z_1|$;

3) $z \neq 0$, *allora* $z^{-1} = \frac{\overline{z}}{N(z)}$.

La forma cartesiana $a+ib$ è molto semplice da manipolare quando si tratti di sommare, dato che basta sommare separatamente parti reali e parti immaginarie. Nel piano di Argand–Gauss ciò si traduce nel fatto che la somma di due numeri complessi si effettua geometricamente mediante la 'regola del parallelogramma" (figura 2.2).

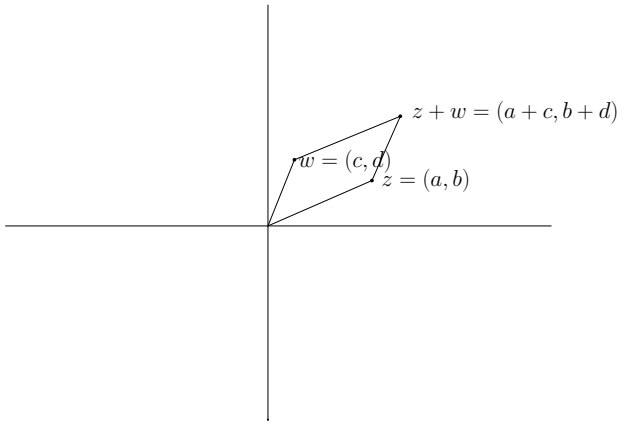

Figura 2.2: somma di numeri complessi

La **forma trigonometrica** di un numero complesso $z = a + ib$ è la sua individuazione nel piano di Argand–Gauss mediante coordinate polari. Dato $z = a + ib$, si pone $\rho = |z|$ (quindi $\rho \in \mathbb{R}_{\geq 0}$) che è la lunghezza del segmento che congiunge z all'origine e definiamo l'*argomento* (o anomalia) α di z come l'angolo (calcolato in senso antiorario) formato dalla semiretta dei reali positivi e tale segmento; questo è illustrato nella figura 2.3.

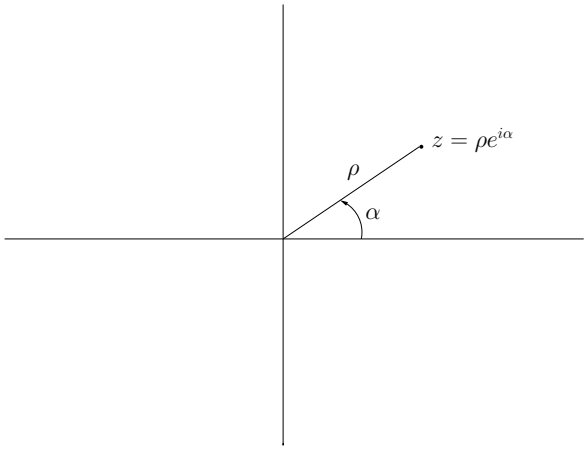

Figura 2.3: forma esponenziale di un numero complesso

Dalle definizioni delle funzioni trigonometriche segue che $a = \rho \cos\alpha$ e $b = \rho \sin\alpha$; quindi

$$z = \rho(\cos\alpha + i\sin\alpha) = |z|(\cos\alpha + i\sin\alpha) \tag{2.2}$$

che è, appunto, la forma trigonometrica di z.

La forma trigonometrica è particolarmente adatta a trattare la moltiplicazione di numeri complessi. Infatti, posto $z = \rho(\cos\alpha + i\sin\alpha)$ e $z' = \rho'(\cos\alpha' + i\sin\alpha')$, ed applicando le note formule di addizione in trigonometria si ha

$$\begin{aligned} zz' &= \rho\rho'((\cos\alpha\cos\alpha' - \sin\alpha\sin\alpha') + i(\cos\alpha\sin\alpha' + \sin\alpha\cos\alpha')) = \\ &= \rho\rho'(\cos(\alpha+\alpha') + i\sin(\alpha+\alpha')) \end{aligned}$$

Possiamo allora formulare la seguente

Regola di moltiplicazione: *il modulo di un prodotto di numeri complessi è il prodotto dei moduli dei singoli fattori, mentre l'argomento del prodotto è la somma degli argomenti dei fattori (eventualmente ridotta modulo 2π).*

Questo è illustrato nella figura 2.4.

Esercizio 2.6. Nel campo $\mathbb{C}$ si trovino le soluzioni dell'equazione $z^2 = -2i$.

Soluzione: Cominciamo con l'esprimere $-2i$ in forma trigonometrica, l'argomento è $3\pi/2$ radianti ed il modulo è 2; quindi

$$-2i = 2(0 - i) = 2\big(\cos\frac{3}{2}\pi + i\sin\frac{3}{2}\pi\big).$$

Posto $z = \rho(\cos\alpha + i\sin\alpha)$, la regola per il prodotto ci da $z^2 = \rho^2(\cos 2\alpha + i\sin 2\alpha)$. Se quindi $z^2 = -2i$ allora dovrà essere $\rho = \sqrt{2}$ e $2\alpha = \frac{3\pi}{2}$; dove la seconda condizione è una

uguaglianza fra angoli espressi in radianti, e quindi va considerata a meno di multipli interi di 2π; come tale ammette dunque due soluzioni distinte, $\frac{3}{4}\pi$ e $\frac{7}{4}\pi$. In conclusione le soluzioni cercate sono date da

$$z_1 = \sqrt{2}\big(\cos\frac{3}{4}\pi + i\sin\frac{3}{4}\pi\big) = \sqrt{2}\big(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\big) = -1 + i$$

$$z_2 = \sqrt{2}\big(\cos\frac{7}{4}\pi + i\sin\frac{7}{4}\pi\big) = \sqrt{2}\big(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\big) = 1 - i = -z_1.$$

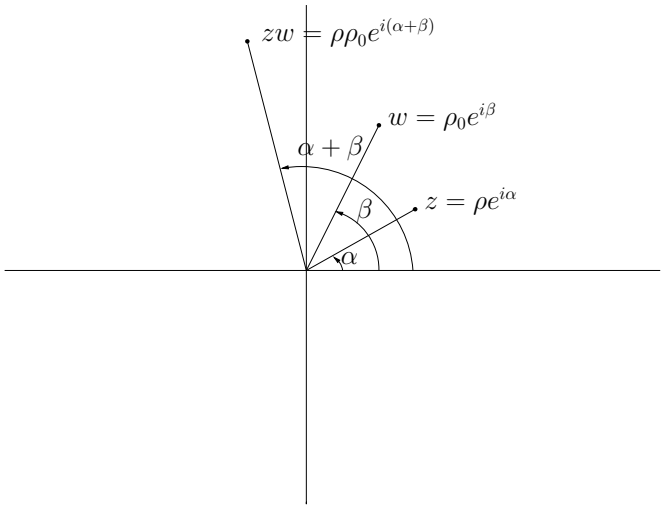

Figura 2.4: prodotto di numeri complessi

Funzione esponenziale. Sia $z = a + ib \in \mathbb{C}$. Si definisce l'esponenziale

$$e^z = e^a(\cos b + i\sin b). \tag{2.3}$$

(dove, chiaramente, il numero reale b esprime una misura in radianti).
Si osservi che $|e^z| = e^a$; e che se $\theta \in \mathbb{R}$, allora $e^{i\theta}$ è, nel piano di Argand–Gauss, il punto staccato sulla circonferenza unitaria da un raggio che forma un angolo della misura di θ radianti con l'asse orizzontale. La forma trigonometrica di un numero complesso di modulo ρ e argomento α si scrive dunque in modo compatto come $\rho e^{i\alpha}$. In particolare, si ha la celebre *Formula di Eulero*[10]:

$$e^{i\pi} = -1. \tag{2.4}$$

È chiaro che quando applicata ai reali la (2.3) coincide con l'usuale esponenziazione. Si verifica poi facilmente (lo si faccia per esercizio) che sono soddisfatte le usuali regole per le potenze, vale a dire: $e^{z+z'} = e^z e^{z'}$, ed $(e^z)^{z'} = e^{zz'}$ (in effetti la (2.3) è la sola maniera per estendere la funzione esponenziale reale, in modo che tali proprietà rimangano soddisfatte). La regola di moltiplicazione in forma trigonometrica diventa

[10]Questa famosa identità discende, per noi, in modo immediato dalla definizione (2.3); la ragione profonda per cui questa è la "corretta" definizione di esponenziale per numeri complessi si vedrà in corsi più avanzati.

allora un'istanza di tale proprietà delle potenze (anche se, di fatto, ne costituisce la dimostrazione):

$$\rho e^{i\alpha}\rho' e^{i\alpha'} = \rho\rho' e^{i(\alpha+\alpha')}.$$

Un caso particolare e importante di utilizzo della regola del prodotto (che abbiamo usato nella soluzione dell'esercizio 2.6) è la formula per le potenze, chiamata anche **formula di de Moivre**:

Siano $z = \rho(\cos\alpha + i\sin\alpha) \in \mathbb{C}$ *e* $n \in \mathbb{N}$. *Allora* $z^n = \rho^n(\cos n\alpha + i\sin n\alpha)$.

In notazione esponenziale:

$$(\rho e^{i\alpha})^n = \rho^n e^{in\alpha}.$$

Da questa formula si ottiene la descrizione delle **radici n-esime dell'unità**. Dato un intero $n \geq 1$, si dicono radice n-esime dell'unità tutti i numeri complessi ζ tali che

$$\zeta^n = 1.$$

Teorema 2.21. *Sia* $1 \leq n \in \mathbb{N}$. *Allora esistono in* $\mathbb{C}$ n *radici* n*-esime dell'unità distinte, date da*

$$\zeta_k = e^{i\frac{2\pi k}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$$

con $k = 0, 1, \ldots, n-1$.

Si osservi che, nelle notazioni del Teorema precedente, $\zeta_0 = 1$, e che, posto $\zeta = \zeta_1$, si ha che, per ogni $k = 1, \ldots, n-1$, $\zeta_k = \zeta^k$. Nel piano di Argand–Gauss, le radici n-esime dell'unità costituiscono l'insieme dei vertici del n-agono regolare, inscritto nella circonferenza unitaria, in cui uno dei vertici coincide con il punto 1 (figura 2.5).

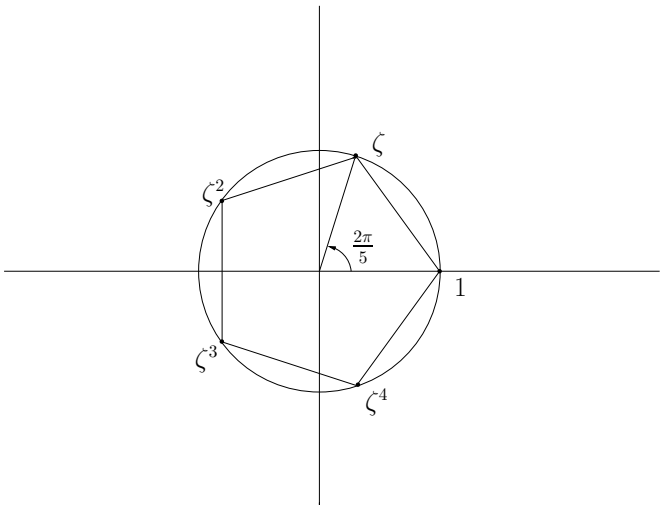

Figura 2.5: le radici 5-te dell'unità

In modo simile, mediante la formula di De Moivre, non è difficile ricondurre la determinazione delle radici (n-esime) di un qualsiasi numero complesso, alla radice reale del suo modulo, ed alle radici dell'unità.

Corollario 2.22. *Sia $1 \leq n \in \mathbb{N}$ e sia $0 \neq u = \rho e^{i\alpha} \in \mathbb{C}$. Sia $w = re^{i\frac{\alpha}{n}}$, dove $r = \sqrt[n]{\rho}$ è la radice n-esima reale positiva del modulo $|u| = \rho$ (esiste ed è unica), e siano $\zeta_0 = 1, \ldots, \zeta_{n-1}$ le radici n-esime distinte dell'unità (notazione del Teorema precedente). Allora i numeri complessi $w, w\zeta_1, \ldots, w\zeta_{n-1}$ sono n radici n-esime di u in $\mathbb{C}$ (cioè le soluzioni, in $\mathbb{C}$, dell'equazione $x^n = u$).*

Infatti, $z = w\zeta_i$, con $0 \leq i \leq n-1$, allora $z^n = w^n\zeta_i^n = r^n e^{i\alpha} \cdot 1 = \rho e^{i\alpha} = u$, quindi z è radice di $x^n = u$. Il viceversa discende altrettanto facilmente dalla Formula di De Moivre.

ESEMPIO. *Calcolare le soluzioni in $\mathbb{C}$ dell'equazione $x^3 = -2i$.*

In forma esponenziale, $-2i = 2e^{i\frac{3\pi}{2}}$ (nelle notazioni del Corollario, $\rho = 2$, $\alpha = \frac{3\pi}{2}$); inoltre, le radici terze dell'unità sono $\zeta_0 = 1, \zeta_1 = e^{i\frac{2\pi}{3}}, \zeta_2 = e^{i\frac{4\pi}{3}}$; quindi le soluzioni cercate sono

$$\begin{aligned} x_0 &= w = \sqrt[3]{2} \cdot e^{i\frac{\pi}{2}} = i\sqrt[3]{2} \\ x_1 &= w \cdot e^{i\frac{2\pi}{3}} = -\frac{\sqrt{3}}{\sqrt[3]{4}} - i\frac{1}{\sqrt[3]{4}} \\ x_2 &= w \cdot e^{i\frac{4\pi}{3}} = \frac{\sqrt{3}}{\sqrt[3]{4}} - i\frac{1}{\sqrt[3]{4}}. \end{aligned}$$

2.7. Esercizi.

• *principio di induzione*

Esercizio 2.7. Applicando il principio di induzione si dimostrino le seguenti affermazioni.

- Per ogni $n \geq 1$: $1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2$.
- Per ogni $n \geq 1$: $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.

Esercizio 2.8. Si provi che per ogni $n \geq 1$, $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots n \cdot n! = (n+1)! - 1$.

Esercizio 2.9. Si determinino tre numeri razionali a, b, c tali che, per ogni $n \geq 1$ si abbia

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = an^3 + bn^2 + cn.$$

Esercizio 2.10. Sia $a \in \mathbb{R}, a > 0$; si provi che, per ogni numero intero $n \geq 2$ si ha

$$(1 + a)^n > 1 + na.$$

Esercizio 2.11. Si dimostri che per ogni numero naturale $n \geq 1$ vale la formula

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n+1)(2n-1)}{3}.$$

Esercizio 2.12. Si provi che per ogni $n \geq 2$,

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

Esercizio 2.13. Applicando il principio d'induzione, si provi che per ogni $n \geq 1$

$$7^n + 3n - 1$$

è un multiplo di 9.

Esercizio 2.14. Si consideri la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix},$$

e, per induzione su n , si dimostri che per ogni $n \geq 1$:

$$A^n = \begin{pmatrix} 1 & 2^n - 1 \\ 0 & 2^n \end{pmatrix}.$$

Esercizio 2.15. Si dimostri, per induzione su n, che per ogni $n \geq 1$:

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

Esercizio 2.16. Procedendo per induzione su n si dimostri che, per ogni $n \geq 2$,

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n}.$$

Esercizio 2.17. Siano a, b numeri interi, con $b \geq 1$. Si provi che esistono unici interi t, s tali che $a = bt + s$ e $-\frac{b}{2} < s \leq \frac{b}{2}$.

Esercizio 2.18. Si provi che per ogni numero intero $n \geq 1$, il numero

$$\frac{(2n)!}{n! 2^n}$$

è dispari.

Esercizio 2.19. Sia $f : \mathbb{N} \longrightarrow \mathbb{N}$. Diciamo che f è strettamente crescente se f è iniettiva e per ogni $i \in \mathbb{N}$ si ha $f(i) \leq f(i+1)$.

(a) Procedendo per induzione su $k = n - m$, si dimostri che se f è strettamente crescente allora per ogni $n, m \in \mathbb{N}$ con $n \geq m$ si ha $f(n) \geq f(m) + k$.

(b) Siano $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ strettamente crescenti. Si dimostri che $f = g$ se e solo se $f(\mathbb{N}) = g(\mathbb{N})$.

Esercizio 2.20. Procedendo per induzione su n, si dimostri che, per ogni $n \geq 3$,

$$\binom{3n}{2n} \geq 4^n \ .$$

Esercizio 2.21. [*Media aritmetica vs Media geometrica*] Siano $a_1, \ldots, a_n$ numeri reali con $a_i > 0$ per ogni $i = 1, \ldots, n$. Procedendo per induzione su n si provi che

$$\sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \cdots + a_n}{n}$$

(la media geometrica è minore o uguale alla media aritmetica). [sugg. Si tratta di provare che $((a_1 + \cdots + a_n)/n)^n \geq a_1 \cdots a_n$. Si dimostra direttamente la cosa per

$n = 2$ (usare il fatto che $a_1^2 + a_2^2 \geq 2a_1a_2$); dopo di che si prova che se è vera per t allora è vera anche per $n = 2t$:

$$a_1 \cdots a_n \leq \Big(\frac{a_1 + \cdots + a_t}{t}\Big)^t \Big(\frac{a_{t+1} + \cdots + a_n}{t}\Big)^t \leq$$

$$\leq \frac{1}{4}\Big(\Big(\frac{a_1 + \cdots + a_t}{t}\Big)^t + \Big(\frac{a_{t+1} + \cdots + a_n}{t}\Big)^t\Big)^2 \leq \cdots$$

adattare poi al caso generale; vedi QUI]

• *combinatoria e rappresentazioni b-adiche*

Esercizio 2.22. Sia $X = \{1, 2, 3, 4, 5\}$.

(a) Quanti sono i sottoinsiemi di X che contengono 1 ?

(b) Quanti sono i sottoinsiemi A di X tali che $A \cap \{2, 3\} \neq \emptyset$ che contengono 1 ?

(c) Quante sono le applicazioni iniettive di X in $\{1, 2, 3\}$?

(d) Quante sono le applicazioni iniettive di $\{1, 2, 3\}$ in X ?

(e) Quante sono le applicazioni suriettive di X in $\{1, 2, 3\}$?

Esercizio 2.23. Calcolare il numero di applicazioni suriettive f dell'insieme $A = \{1, 2, 3, 4, 5, 6\}$ nell'insieme $B = \{1, 2, 3\}$ tali che per ogni $b \in B$ sia $|f^{-1}(b)| \leq 2$.

Esercizio 2.24. Si scrivano le rappresentazioni in base 2, 3, 7, 11 del numero 2002 (si faccia attenzione che per la base 11 c'è bisogno di un simbolo per le cifre in più, che rappresenti il numero 10).

Esercizio 2.25. Il numero 2002 è detto "palindromo" perché la sua rappresentazione decimale è palindroma, ovvero è uguale se letta in entrambi i versi. Naturalmente la palindromia non è una proprietà intrinseca di un numero ma dipende dal numero e dalla base per la rappresentazione. Si determinino tutte le basi $2 \leq b \leq 10$ tale che la rappresentazione b-adica del numero 1785 è palindroma.

Esercizio 2.26. Si provi che per ogni intero $n \geq 3$ esiste una base $b < n$ tale che la rappresentazione b-adica di n è palindroma. Si provi che non esiste alcuna base b tale che la rappresentazione b-adica del numero 39 è composta da almeno tre cifre ed è palindroma.

Esercizio 2.27. Per ogni $2 \leq n \in \mathbb{N}$, sia

$$\Delta_n = \left[\frac{n}{2}\right] + \left[\frac{n-1}{2}\right] + \cdots + \left[\frac{1}{2}\right]$$

(dove, per $a \in \mathbb{Q}$, $[a]$ denota la parte intera di a). Si provi che

$$\Delta_n = \begin{cases} [n/2]^2 & \text{se n è pari} \\ [n/2]^2 + [n/2] & \text{se n è dispari} \end{cases}$$

Esercizio 2.28. Siano b e k interi maggiori o uguali a due. Si dica quanti numeri naturali hanno una scrittura b-adica palindroma composta esattamente da k cifre.

Esercizio 2.29. Dati n, b interi positivi, $b \geq 2$, sia $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_0$ la rappresentazione b-adica di n. Si provi che $b + 1$ divide

$$n - \sum_{i=0}^{k} (-1)^i a_i.$$

Esercizio 2.30. Sia A un insieme con n elementi, che consideriamo ripartito nell'unione disgiunta di 3 sottoinsiemi $A = A_1 \cup A_2 \cup A_3$, con $|A_i| = n_i$ (per cui, $n_1 + n_2 + n_3 = n$). Si dica quanti elementi contiene l'insieme di tutti i sottoinsiemi $\{x, y\}$ di A tali che x e y appartengono a termini diversi della partizione.

Esercizio 2.31. Sia A un insieme con n elementi; sia $d \geq 1$ un divisore di n, e $c = n/d$. Si dica in quanti modi è possibile ripartire A come unione disgiunta $A = A_1 \cup \cdots \cup A_c$ con $|A_i| = d$, per ogni $i = 1, \ldots, c$.

Esercizio 2.32. Siano A, B insiemi con $|A| = 5$, $|B| = 9$. Determinare il numero di applicazioni $\{f : A \to B \mid |f(A)| \leq 3\}$.

Esercizio 2.33. Sia $n \geq 2$, e siano $A_1, A_2, \ldots, A_n$ insiemi (non necessariamente finiti). Si provi che la differenza simmetrica

$$A_1 \Delta A_2 \Delta \ldots \Delta A_n$$

è costituita da tutti gli elementi dell'unione $A_1 \cup \cdots \cup A_n$ che appartengono esattamente ad un numero dispari di insiemi A_i. [sugg. induzione su n]

• *MCD e dintorni*

Esercizio 2.34. Trovare due numeri interi a e b tali che $19a + 21b = 1$.

Esercizio 2.35. Calcolare il MCD di 4415 e 1554.

Esercizio 2.36. Siano a, b, c numeri interi non nulli. Si dimostri che $(a, (b, c)) = ((a, b), c)$.

Esercizio 2.37. Siano a, b, c numeri interi non nulli. Si dimostri che se a divide bc allora $a/(a, b)$ divide c.

Esercizio 2.38. Calcolare $(1001, 4485)$, e quindi scriverlo come combinazione a coefficienti interi dei due numeri dati.

Esercizio 2.39. Siano a, b numeri interi positivi non nulli, e sia $d = (a, b)$. Si provi che

$$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{[a, b]}{d}.$$

Esercizio 2.40. Siano a, b e c interi non nulli tali che $c|a$ e $c|b$. Si provi che

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a, b)}{c}.$$

In particolare, se $d = (a, b)$, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Esercizio 2.41. Siano a, b e c interi non nulli. Si provi che

1) $(ca, cb) = c(a, b)$;
2) $[ca, cb] = c[a, b]$.

Esercizio 2.42. Siano a, b e c interi non nulli. Si provi che

$$(a, [b, c]) = [(a, b), (a, c)].$$

Esercizio 2.43. Sia n un numero intero. Si provi che $(2n+1, 1-n)$ è uguale a 1 o a 3.

Esercizio 2.44. Siano a e b due interi dispari tali che $(a,b) = 1$. Si determini il massimo comun divisore $((a+b)^3, (a-b)^3)$.

Esercizio 2.45. Siano n e m interi positivi tali che

$$\begin{cases} n+m = 63 \\ [n,m] = 962 \end{cases}$$

Si determinino n e m.

Esercizio 2.46. Si determini una soluzione intera dell'equazione:

$$910x + 1406y = 8.$$

Esercizio 2.47. Siano a, b due numeri interi non entrambi nulli e sia d un MCD positivo di a e b. Siano $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$. Si provi che $(\alpha, \beta) = 1$.

Esercizio 2.48. Sia $1 < n \in \mathbb{N}$. Si provi che

$$u = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

non è un numero intero.

Esercizio 2.49. La successione di *Fibonacci* è definita da:

$$u_0 = 0,\ u_1 = 1, \quad \text{e} \quad u_{n+2} = u_{n+1} + u_n$$

(i primi termini di essa sono $0, 1, 1, 2, 3, 5, 8, 13, 21, 34 \dots$). Provare i seguenti fatti

1) se $x = (1+\sqrt{5})/2$ e $y = (1-\sqrt{5})/2$, allora $u_n\sqrt{5} = x^n - y^n$ (x, y sono le radici reali dell'equazione $t^2 - t - 1$)
2) $(u_n, u_{n+1}) = 1$
3) $u_{m+n} = u_{n-1}u_m + u_n u_{m+1}$
4) se $r \in \mathbb{N}^*$, u_n divide u_{nr}
5) se $(m,n) = d$, allora $(u_m, u_n) = u_d$.

Esercizio 2.50. Si dimostri che ogni numero naturale n è somma di numeri di Fibonacci a due a due distinti [sugg. induzione nella seconda forma]

Esercizio 2.51. Sia u_n l'n-esimo numero di Fibonacci. Si provi che, per $n \geq 3$, $u_n \geq n^2$.

Esercizio 2.52. Sia $n \in \mathbb{N}$. Si provi che n, $n+2$ e $n+4$ sono numeri primi se e solo se $n = 3$.

Esercizio 2.53. Siano $n, k \in \mathbb{N}$, con $k \geq 3$. Si provi che se $n,\ n+k,\ n+2k, \dots, n+(k-2)k$ sono tutti numeri primi allora $n = k-1$.

• *Numeri complessi*

Esercizio 2.54. Si provi che, per ogni $z, z' \in \mathbb{C}$, $|z + z'| \leq |z| + |z'|$.

Esercizio 2.55. Si esprimano nella forma $a + ib$ i numeri complessi

$$\frac{(5-4i)^2}{1+i}\ ; \qquad \frac{3i(1-6i)}{(-1-i)^2}.$$

Esercizio 2.56. Si determinino, nel campo complesso, le radici cubiche di 1 e di $1+i$ e se ne individui la posizione nel piano di Argand-Gauss.

Esercizio 2.57. Si determinino le radici quarte del numero complesso $\alpha = -3+\sqrt{3}i$.

Esercizio 2.58. Si determinino le radici complesse dell'equazione $z^2 + z + 1 = 0$.

Esercizio 2.59. Si risolva in $\mathbb{C}$ l'equazione di secondo grado $z^2+2iz-3+2i\sqrt{3} = 0$.

Esercizio 2.60. Si calcoli $(1 + i)^{2000}$.

Esercizio 2.61. Sia $1 \leq n \in \mathbb{N}$, e siano $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ le radici complesse n-esime distinte dell'unità. Si provi che

$$\sum_{k=0}^{n-1} \zeta_k = 0 \qquad \text{e} \qquad \prod_{k=0}^{n-1} \zeta_k = \pm 1$$

(nel caso del prodotto, il segno dipende dall'essere n dispari o pari)

Esercizio 2.62. Siano u e w numeri complessi. Si provi che l'area del triangolo i cui vertici, nel piano di Argand–Gauss, sono u, w e 0, è data da $\frac{1}{4}|u\overline{w} - \overline{u}w|$.

Esercizio 2.63. Per $n \in \mathbb{N}$, sia $F_n = 2^{2^n} + 1$. Si provi che se $n \neq m$ allora $(F_n, F_m) = 1$ (si osservi che, se $n < m$, allora F_n divide $F_m - 2$).

3

Operazioni e relazioni

In questo capitolo introduciamo alcuni concetti fondamentali che, assieme a quello di applicazione, informano il linguaggio di tutta la matematica (e non solo dell'algebra): relazioni, equivalenze, ordinamenti ed operazioni.

3.1. Operazioni binarie.

Assieme con le applicazioni e le relazioni, le operazioni occupano una posizione di preminenza nell'Algebra astratta. In questa sezione introdurremo solo i concetti fondamentali riguardanti le operazioni binarie. Lo studio di alcune importanti classi di strutture algebriche definite a partire da una o più operazioni sarà approfondito nel seguito.

Sia A un insieme non vuoto. Una **operazione binaria**, o legge di composizione, su A è un'applicazione

$$* : A \times A \longrightarrow A.$$

Se $*$ è una operazione su A, per ogni $(a, b) \in A \times A$, scriveremo $a * b$ invece di $*((a, b))$.

Nota. La definizione che abbiamo dato è quella di un'operazione binaria *interna* - ovvero tale che il risultato della composizione di due elementi di A è ancora un elemento di A. In matematica sono talvolta chiamate operazioni esterne quelle per cui il risultato delle composizioni appartiene ad un altro insieme: il tipico esempio è, per chi lo conosce, il cosiddetto "prodotto scalare" di vettori. Un altro tipo di estensione del concetto di operazione è quello di *operazione n-aria*: dato $n \geq 1$, un'operazione n-aria dell'insieme A è una applicazione dall'insieme delle n-uple ordinate di A in A (quindi un'operazione 1-aria è una qualsiasi applicazione $A \longrightarrow A$).

Dalla definizione, risulta che su un insieme non vuoto A è possibile definire un gran numero di operazioni. La maggior parte di esse è tuttavia scarsamente importante (secondo il punto di vista delle strutture algebriche). La proprietà fondamentale che, in genere, esclude operazioni poco interessanti, o di difficile studio, è la cosiddetta *associatività*.
Un'operazione $*$ sull'insieme A si dice **associativa** se, per ogni $a, b, c \in A$ risulta:

$$(a * b) * c = a * (b * c).$$

ESEMPI. Sono operazioni "interessanti" (oltre che naturali) quelle usuali di "somma" e di "prodotto" sugli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. La sottrazione, nel significato usuale, è una operazione su $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, ma non è una operazione su $\mathbb{N}$, dato che la differenza di due numeri naturali non è, in genere, un numero naturale. Tranne il caso della sottrazione (dove essa è definita), tutte queste operazioni sono associative.

Per **semigruppo** si intende una coppia $(A, \cdot)$ dove A è un insieme non vuoto, e $\cdot$ è un'operazione associativa su A.

Osservazione importante. Se $(A, \cdot)$ è un semigruppo, allora, per ogni $a, b, c \in A$ possiamo scrivere senza ambiguità

$$a \cdot b \cdot c$$

intendendo con ciò l'elemento $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Questa osservazione si estende ad una stringa finita qualunque di elementi di A. Ad esempio se $a_1, a_2, a_3, a_4 \in A$, allora:

$$a_1 \cdot ((a_2 \cdot (a_3 \cdot a_4)) = a_1 \cdot ((a_2 \cdot a_3) \cdot a_4)) = a_1 \cdot (a_2 \cdot a_3 \cdot a_4) = (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = (a_1 \cdot a_2 \cdot a_3) \cdot a_4 = \text{ etc.}$$

elemento che scriviamo semplicemente: $a_1 \cdot a_2 \cdot a_3 \cdot a_4$.
Più in generale, per ogni $n \geq 1$ e $a_1, a_2, \ldots, a_n \in A$ possiamo individuare senza ambiguità l'elemento

$$a_1 \cdot a_2 \cdot \cdots \cdot a_n.$$

Una operazione $*$ sull'insieme A si dice **commutativa** se per ogni $a, b \in A$ risulta:

$$a * b = b * a.$$

Non si dà un nome particolare ad un insieme dotato di operazione commutativa. Se $(A, \cdot)$ è un semigruppo e l'operazione è commutativa, si dice che $(A, \cdot)$ è un semigruppo commutativo.

ESEMPI. Sono commutative le operazioni di somma e moltiplicazione in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, mentre (dove è definita) non è commutativa la sottrazione. La composizione di applicazioni o il prodotto righe×colonne tra matrici (vedi §1.3.6) sono gli esempi fondamentali di operazioni associative ma non commutative.

Esercizio 3.1. Su $\mathbb{Z} \times \mathbb{Z}$ si definisca l'operazione $*$ ponendo, per ogni $(x, y), (x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) * (x_1, y_1) = (x, y_1)$. Si dica se $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigruppo. Si dica se è commutativo.

SOLUZIONE. Siano $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$. Allora

$$\begin{aligned}(x, y) * ((x_1, y_1) * (x_2, y_2)) &= (x, y) * (x_1, y_2) = (x, y_2) = \\ &= (x, y_1) * (x_2, y_2) = ((x, y) * (x_1, y_1)) * (x_2, y_2)\end{aligned}$$

dunque l'operazione $*$ è associativa e $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigruppo. Non è commutativo perché, ad esempio, $(1, 2) * (2, 1) = (1, 1) \neq (2, 2) = (2, 1) * (1, 2)$. ∎

Caso importante. Se X è un insieme non vuoto, allora la *composizione* $\circ$ è una operazione sull'insieme X^X di tutte le applicazioni di X in se stesso. La composizione è anche una operazione sull'insieme $Sym(X)$ di tutte le applicazioni biettive di X in se stesso; infatti la composizione di due applicazioni biettive è biettiva.

Nota. Se $|X| \geq 2$ la composizione in X^X non è commutativa. Infatti siano a, b elementi distinti di X e si considerino le applicazioni $f, g : X \to X$ definite da

$$f(x) = a \text{ per ogni } x \in X \quad \text{e} \quad g(x) = b \text{ per ogni } x \in X \ ;$$

allora $(f \circ g)(a) = f(g(a)) = f(b) = a$, mentre $(g \circ f)(a) = g(f(a)) = g(a) = b$. Quindi $f \circ g \neq g \circ f$.
Se $|X| \geq 3$, la composizione in $Sym(X)$ non è commutativa. Infatti siano a, b, c elementi distinti di X; si considerino le permutazioni $\sigma, \tau : X \to X$ definite da

$$\sigma(a) = b \ , \ \sigma(b) = a \ , \ \sigma(x) = x \ \text{ per ogni altro } x \in X$$

$$\tau(a) = c \ , \ \tau(c) = a \ , \ \tau(x) = x \ \text{ per ogni altro } x \in X$$

e si provi che $\sigma \circ \tau \neq \tau \circ \sigma$.

Sia $\cdot$ una operazione sull'insieme A. Un sottoinsieme B di A si dice **chiuso** (rispetto a $\cdot$) se, per ogni $b, b' \in B$ risulta $b \cdot b' \in B$.

Se B è un sottoinsieme chiuso, allora si può definire su B l'operazione $\cdot$ *indotta* da A (cioè quella definita dalla restrizione della operazione $A \times A \longrightarrow A$ ad una operazione $B \times B \longrightarrow B$, dove la regola che determina il prodotto rimane la stessa). Ovviamente se l'operazione su A è associativa (commutativa), anche l'operazione indotta su un sottoinsieme chiuso è tale. Una proprietà elementare ma importante dei sottoinsiemi chiusi è che l'intersezione di due o più di essi è ancora un sottoinsieme chiuso.

Esempi L'insieme $2\mathbb{Z}$ dei numeri interi pari è un sottoinsieme chiuso di $(\mathbb{Z}, +)$ e di $(\mathbb{Z}, \cdot)$, mentre l'insieme dei numeri dispari è chiuso in $(\mathbb{Z}, \cdot)$ ma non in $(\mathbb{Z}, +)$.

Sia $(A, \cdot)$ un semigruppo. Un elemento $e \in A$ si dice **elemento identico** (o identità, o elemento neutro) se per ogni $a \in A : \ a \cdot e = a = e \cdot a$.

Proposizione 3.1. *Sia $(A, \cdot)$ un semigruppo, e siano e, e' elementi identici in A. Allora $e = e'$.*

Dimostrazione. Se e, e' sono elementi identici, si ha:

$$e = e \cdot e' = e'$$

dove la prima uguaglianza sussiste perché e' è un elemento identico, e la seconda perché lo è e. ∎

Dunque, se un semigruppo $(A, \cdot)$ ha un elemento identico, esso è unico. Lo si denota, in generale, con 1_A. Un semigruppo dotato di elemento identico si dice **monoide**. Un monoide $(M, \cdot)$ si dice *commutativo* se l'operazione $\cdot$ è commutativa.

Esempi. 1) Sono monoidi i semigruppi $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ (l'elemento identico è 0); sono monoidi i semigruppi $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ (l'elemento identico è 1).

2) Se X è un insieme non vuoto, allora $(X^X, \circ)$ è un monoide, con identità l'applicazione identica ι_X.

Inversi. Passiamo ora all'importante questione dell'esistenza di "inversi" rispetto ad una data operazione. Il caso che ci può guidare (ma con un po' di attenzione, perché le operazioni interessanti non sempre sono commutative) è quello familiare delle operazioni di somma e prodotto: se a è un numero (diciamo razionale) allora $-a$ è "l'inverso" di a rispetto all'operazione $+$ di somma, infatti $a + (-a) = 0$, e 0 è l'elemento neutro per la somma. Se invece consideriamo il prodotto (ovvero lavoriamo nel monoide moltiplicativo $(\mathbb{Q}^*, \cdot)$, dove $\mathbb{Q}^*$ è l'insieme dei numeri razionali non nulli), allora l'inverso di $a \in \mathbb{Q}^*$ è l'usuale inverso razionale $1/a$: infatti $a \cdot (1/a) = 1$, e 1 è l'elemento neutro di $(\mathbb{Q}^*, \cdot)$.

Proposizione 3.2. *Sia $(M, \cdot)$ un monoide con elemento identico 1_M, e sia $a \in M$. Se b, c sono elementi di M tali che $ba = 1_M = ac$, allora $b = c$.*

Dimostrazione. Siano $a, b, c \in M$ come nelle ipotesi. Allora:

$$b = b \cdot 1_M = b(ac) = (ba)c = 1_M \cdot c = c.$$

■

Sia $(M, \cdot)$ un monoide con elemento identico 1_M. Un elemento $a \in M$ si dice **invertibile** se esiste $b \in M$ tale che

$$a \cdot b = 1_M = b \cdot a.$$

Per la proposizione 3.2, un tale b è unico; si denota con a^{-1}, e si chiama l'**elemento inverso** di a in M.

Osserviamo che l'elemento identico 1_M di un monoide M è sempre invertibile, e coincide con il proprio inverso. L'insieme degli elementi invertibili di un monoide M lo denoteremo con $U(M)$.

Nota. Più in generale, se $(M, \cdot)$ è un monoide e $a \in M$, un elemento b tale che $ba = 1_M$ si dice *inverso sinistro* di a; un elemento c tale che $ac = 1_M$ si dice *inverso destro* di a. Mentre è possibile che un elemento di un monoide abbia diversi inversi sinistri o diversi inversi destri, la proposizione precedente implica che se un elemento a di un monoide ha un inverso sinistro e un inverso destro allora questi coincidono (in tal caso l'elemento a ha, quindi, un unico inverso sinistro (che è anche l'unico inverso destro).

Esempi. 1) Gli elementi invertibili del monoide $(\mathbb{Z}, \cdot)$ sono 1 e -1, quindi $U(\mathbb{Z}, \cdot) = \{1, -1\}$. Gli elementi invertibili del monoide $(\mathbb{Q}, \cdot)$ sono tutti i numeri razionali diversi da 0, quindi $U(\mathbb{Q}, \cdot) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0, \}$ (e similmente per $\mathbb{R}$ e $\mathbb{C}$).

2) Se X è un insieme non vuoto, gli elementi invertibili di $(X^X, \circ)$ sono precisamente le applicazioni invertibili (ovvero biettive) $f : X \to X$. Quindi l'insieme degli elementi invertibili di $(X^X, \circ)$ è $Sym(X)$.

L'osservazione seguente mostra, in particolare, che l'insieme degli elementi invertibili di un monoide costituisce un sottoinsieme chiuso. Si noterà come la dimostrazione sia essenzialmente la stessa già data nel caso delle applicazioni biettive.

Proposizione 3.3. *Sia $(M, \cdot)$ un monoide con elemento identico 1_M, e siano a, b elementi invertibili di M. Allora*

1) *a^{-1} è invertibile e $(a^{-1})^{-1} = a$;*

2) *ab è invertibile e $(ab)^{-1} = b^{-1}a^{-1}$.*

Dimostrazione. 1) Poichè $(a^{-1})a = 1_M = a(a^{-1})$, si ha che a^{-1} è invertibile e, per l'unicità dell'inverso, $(a^{-1})^{-1} = a$.

2) Se a e b sono invertibili:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1_M b = b^{-1}b = 1_M \ ;$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1_M a^{-1} = aa^{-1} = 1_M$$

dunque ab è invertibile e, per l'unicità dell'inverso, $(ab)^{-1} = b^{-1}a^{-1}$. ■

Esercizio 3.2. Sull'insieme $\mathbb{Z}$ dei numeri interi si definisca l'operazione $*$ ponendo, per ogni $n, m \in \mathbb{Z}$: $n * m = n + m - nm$. Si dimostri che $(\mathbb{Z}, *)$ è un monoide e si determinino gli elementi invertibili.

SOLUZIONE. Verifichiamo che l'operazione $*$ è associativa: siano $n, m, t \in \mathbb{Z}$, allora

$$n * (m * t) = n + (m * t) - n(m * t) = n + (m + t - mt) - n(m + t - mt) = \\ = (n + m - nm) + t - (n + m - nm)t = (n * m) * t.$$

Proviamo ora che 0 è l'elemento identico di $(\mathbb{Z}, *)$. Infatti, per ogni $n \in \mathbb{Z}$

$$n * 0 = n + 0 - n \cdot 0 = n = 0 * n.$$

Quindi $(\mathbb{Z}, *)$ è un monoide (commutativo). Supponiamo ora che $n \in \mathbb{Z}$ sia invertibile in $(\mathbb{Z}, *)$, allora esiste $n' \in \mathbb{Z}$ tale che

$$0 = n * n' = n + n' - nn'.$$

Quindi, deve essere che $n' = \frac{n}{n-1}$ appartiene a $\mathbb{Z}$; ciò si verifica solo per $n = 0, 2$. Pertanto, gli invertibili di $(\mathbb{Z}, *)$ sono 0 e 2, e (come si verifica immediatamente), coincidono con i loro inversi. ■

Gruppi. I gruppi costituiranno uno degli argomenti principali del secondo corso di Algebra. Per il momento, ne vediamo quasi solo la definizione.

DEFINIZIONE. Un **gruppo** è un *monoide in cui ogni elemento è invertibile*.

Quindi un insieme con operazione $(G, \cdot)$ è un gruppo se e solo se sono soddisfatte le seguenti condizioni:

1. *Per ogni* $a, b, c \in G$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. *Esiste* $1_G \in G$ *tale che, per ogni* $a \in G$: $a \cdot 1_G = a = 1_G \cdot a$.
3. *Per ogni* $a \in G$ *esiste* $b \in G$ *tale che* $a \cdot b = 1_G = b \cdot a$ (tale b è unico e si denota con a^{-1}).

ESEMPI (TUTTI FONDAMENTALI). 1) Sono gruppi i monoidi additivi

$$(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +),\ (\mathbb{C}, +),$$

e quelli moltiplicativi

$$(\mathbb{Q}^*, \cdot),\ (\mathbb{R}^*, \cdot),\ (\mathbb{C}^*, \cdot),$$

dove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

2) Se X è un insieme non vuoto, allora

$$(Sym(X), \circ)$$

è un gruppo, detto il *Gruppo Simmetrico* su X.

3) Se $(M, \cdot)$ è un monoide, allora, per la Proposizione 3.3, l'insieme $U(M)$ degli elementi invertibili di M è un gruppo rispetto alla operazione indotta da M.

Notazione additiva. Un gruppo si dice *commutativo* (o *abeliano*) se l'operazione è commutativa. Per i gruppi (o monoidi) commutativi, a volte è conveniente utilizzare la cosiddetta *notazione additiva* in cui l'operazione si denota con il simbolo $+$ (mentre

la notazione che usiamo in generale, in cui il simbolo dell'operazione è un puntino oppure viene omesso, si dice moltiplicativa). In notazione additiva il simbolo per l'elemento neutro è 0_M (o, semplicemente, 0); se $(A,+)$ è un monoide commutativo, un elemento $a \in A$ è invertibile se esiste $b \in A$ tale che $a+b=0$, in tal caso si scrive $b=-a$ (invece di $b=a^{-1}$) e $-a$ si chiama *l'opposto* di a. L'enunciato della Proposizione 4 diventa : se a,b sono invertibli, $-(-a)=a$ e $-(a+b)=-b+(-a)=-a+(-b)$ (perchè M è commutativo). Infine, se $(A,+)$ è un gruppo, e $x,y \in A$, si adotta la convenzione di scrivere $x+(-y)=x-y$.

3.2. Equivalenze.

DEFINIZIONE. Sia A un insieme. Una **relazione** (binaria) su A è un sottoinsieme del prodotto cartesiano $A \times A$.
Se $\rho \subseteq A \times A$ è una relazione su A, e la coppia ordinata (a,b) appartiene a ρ, si scrive

$$a \rho b$$

invece di $(a,b) \in \rho$, e si legge 'a è in relazione ρ con b'.

Ad esempio, dati due numeri interi a,b, si dice che a *divide* b se esiste $c \in \mathbb{Z}$ tale che $ac=b$. La relazione di "divisibilità" nell'insieme dei numeri interi $\mathbb{Z}$ è quindi descritta dal seguente sottoinsieme di $\mathbb{Z} \times \mathbb{Z}$:

$$\{\ (a,b) \mid a,b \in \mathbb{Z} \text{ ed esiste } c \in \mathbb{Z} \text{ tale che } ac=b\}.$$

In pratica, raramente si definisce una relazione descrivendo per esteso il sottoinsieme del prodotto. Ad esempio, la relazione di divisibilità si descrive più naturalmente così:

è la relazione $|$ sull'insieme $\mathbb{Z}$, definita da, per ogni $a,b \in \mathbb{Z}$, $a|b$ se a divide b.

Sia ρ una relazione sull'insieme A.

1) ρ si dice **riflessiva** se, per ogni $a \in A$: $a \rho a$

2) ρ si dice **simmetrica** se, per ogni $a\ , b \in A$: da $a \rho b$ segue $b \rho a$

3) ρ si dice **transitiva** se, per ogni $a\ , b\ , c \in A$: da $a \rho b$ e $b \rho c$ segue $a \rho c$

Ad esempio, la relazione di divisibilità nei numeri interi è riflessiva e transitiva, ma non è simmetrica.

DEFINIZIONE. Una relazione si dice **relazione di equivalenza** se è riflessiva, simmetrica e transitiva.

ESEMPI. 1) La relazione ρ sull'insieme $\mathbb{R}$ dei numeri reali definita da, per ogni $x,y \in \mathbb{R}$, $x \rho y$ se $|x|=|y|$, è una relazione di equivalenza.

2) Sia Σ l'insieme di tutte le circonferenze del piano. La relazione

$$\{\ (C,C') \in \Sigma \times \Sigma \mid C \text{ e } C' \text{ hanno lo stesso centro}\}$$

è una equivalenza su Σ.

3) Sia $A = \mathbb{N} \times (\mathbb{N} \setminus \{0\})$ l'insieme delle coppie ordinate di numeri naturali la cui seconda componente è diversa da zero. La relazione ω su A definita da

$$\text{per ogni } (a,b),(c,d) \in A : \ (a,b)\omega(c,d) \ \text{ se } \ ad = bc$$

è una relazione di equivalenza. Riflessività e simmetria sono di immediata verifica; dimostriamo la transitività. Siano $(a,b),(c,d),(r,s) \in A$ tali che $(a,b)\omega(c,d)$ e $(c,d)\omega(r,s)$; allora, per definizione di ω: $ad = bc$ e $cs = dr$, Se $c = 0$ allora $a = 0 = r$ e dunque $as = 0 = br$, se invece $c \neq 0$:

$$as(cd) = ad \cdot cs = bc \cdot dr = br(cd)$$

da cui segue, essendo $cd \neq 0$, $as = br$; dunque, in ogni caso $(a,b)\omega(r,s)$.
(Si dica se la relazione definita allo stesso modo sull'insieme $\mathbb{N} \times \mathbb{N}$ è ancora una equivalenza.)

Per relazioni che sono di equivalenza si utilizzano solitamente simboli che suggeriscono la simmetria della relazione stessa, come $\sim$, $\equiv$, ω , $\simeq$, etc.

Osservazione importante. Ogni insieme non vuoto A ammette sempre almeno due relazioni di equivalenza:

• *l'uguaglianza*: $x \sim y$ se e solo se $x = y$. In $A \times A$ corrisponde all'insieme (detto *diagonale*) $\{(x,y) \mid x,y \in A, \ x = y\}$.

• *la relazione banale*: $x \sim y$ per ogni $x,y \in A$: corrispondente all'intero prodotto $A \times A$.

Tali equivalenze sono distinte se e solo se $|A| \geq 2$. Osserviamo inoltre che la proprietà riflessiva per una relazione ρ sull'insieme A equivale alla condizione che, come sottoinsiemi di $A \times A$, $\{(x,x) \mid x \in A\} \subseteq \rho$. Quindi possiamo dire che l'uguaglianza e la relazione banale sono, rispettivamente e rispetto alla relazione di inclusione nell'insieme della parti di $A \times A$, la minima e la massima tra le equivalenze di A.

DEFINIZIONE. Sia $\sim$ una relazione di equivalenza sull'insieme A, e sia $a \in A$. L'insieme di tutti gli elementi x di A tali che $a \sim x$ si chiama **classe di equivalenza di** a (modulo $\sim$) e si denota con $[a]_\sim$; quindi:

$$[a]_\sim = \{ \ b \mid b \in A \ , a \sim b \ \}.$$

Osservazione. La proprietà riflessiva dell'equivalenza ci dice che, per ogni $a \in A$, $a \sim a$, quindi $a \in [a]_\sim$. In particolare $[a]_\sim \neq \emptyset$ per ogni $a \in A$, ed inoltre

$$\bigcup_{a \in A} [a]_\sim = A.$$

È importante sottolineare che $[a]_\sim$ è un sottoinsieme di A e che, anche se (come elementi) $a \neq b$, $[a]_\sim$ e $[b]_\sim$ possono avere elementi in comune (Proposizione 3.4); vedremo poi (Proposizione 3.5) che se $[a]_\sim$ e $[b]_\sim$ hanno elementi in comune, allora coincidono come sottoinsiemi di A.

Ad esempio, se ρ è l'equivalenza sull'insieme $\mathbb{R}$ dell'esempio 1), allora, per ogni $x \in \mathbb{R}$ la classe di equivalenza di x è $[x]_\rho = \{x, -x\}$.
Riferendosi all'esempio 2) di sopra, la classe di equivalenza di una circonferenza C è l'insieme di tutte le circonferenze concentriche a C.

Vediamo subito il fondamentale criterio di uguaglianza tra classi di equivalenza

Proposizione 3.4. *Sia $\sim$ una relazione di equivalenza sull'insieme A, e siano $a, b \in A$. Allora*

$$[a]_\sim = [b]_\sim \quad \textit{se e solo se} \quad a \sim b.$$

Dimostrazione. Sia $[a]_\sim = [b]_\sim$. Allora, per la proprietà riflessiva, $b \in [b]_\sim = [a]_\sim$ e quindi, per definizione di $[a]_\sim$, $a \sim b$.

Viceversa, sia $a \sim b$. Allora $b \sim a$ per simmetria. Sia $x \in [a]_\sim$; allora $a \sim x$ e quindi, per transitività, $b \sim x$, cioè $x \in [b]_\sim$, provando che $[a]_\sim \subseteq [b]_\sim$. Allo stesso modo si dimostra l'inclusione inversa, e dunque l'uguaglianza $[a]_\sim = [b]_\sim$. ∎

Quindi se $b \in [a]_\sim$ allora $[a]_\sim = [b]_\sim$. In tal caso a e b si dicono *rappresentanti* della stessa classe di equivalenza $[a]_\sim$.

Proposizione 3.5. *Sia $\sim$ una relazione di equivalenza sull'insieme A, e siano $a, b \in A$. Se $[a]_\sim \cap [b]_\sim \neq \emptyset$ allora $[a]_\sim = [b]_\sim$.*

Dimostrazione. Supponiamo che $[a]_\sim \cap [b]_\sim \neq \emptyset$, e sia $x \in [a]_\sim \cap [b]_\sim$. Per definizione di classi di equivalenza, si ha allora $a \sim x$ e $b \sim x$, da cui, per la proprietà simmetrica (che ci dà $x \sim b$) e la proprietà transitiva, si ottiene $a \sim b$. Ciò implica, per la Proposizione 3.4, $[a]_\sim = [b]_\sim$. ∎

DEFINIZIONE. Sia $\sim$ una relazione di equivalenza sull'insieme A. L'insieme di tutte le classi di equivalenza di elementi di A si chiame **insieme quoziente** (di A modulo $\sim$) e si denota con $A/\sim$. Quindi

$$A/\sim = \{\ [a]_\sim \mid a \in A\}.$$

Un concetto utile è quello dell'applicazione che ad ogni elemento di un insieme A su cui è data una equivalenza $\sim$, associa la corrispondente classe di equivalenza. Sia $\sim$ una relazione di equivalenza sull'insieme A. La **proiezione canonica** di A su $A/\sim$ è l'applicazione $\pi : A \longrightarrow A/\sim$ definita da, per ogni $x \in A, \pi(x) = [x]_\sim$.

Data una equivalenza $\sim$ sull'insieme non-vuoto A, gli elementi dell'insieme quoziente $A/\sim$ sono quindi sottoinsiemi di A, *non vuoti, disgiunti* (per la Proposizione 3.5), e *la cui unione è l'intero* insieme A.

Una famiglia di sottoinsiemi di un dato insieme A che soddisfa alle tre proprietà enunciate in corsivo di sopra, si dice partizione di A. Precisamente:

DEFINIZIONE. Sia A un insieme non vuoto. Una famiglia $\mathcal{F}$ di sottoinsiemi di A si dice **partizione** di A se :

i) $X \neq \emptyset$ per ogni $X \in \mathcal{F}$;

ii) $\bigcup_{X \in \mathcal{F}} X = A$;

iii) per ogni $X, Y \in \mathcal{F}$: se $X \neq Y$ allora $X \cap Y = \emptyset$.

Quindi, se $A \neq \emptyset$, l'insieme quoziente di A modulo una relazione di equivalenza è una partizione di A. Viceversa, si vede facilmente che se $\mathcal{F}$ è una partizione di A, allora la relazione $\sim_\mathcal{F}$ su A definita da

$$a \sim_\mathcal{F} b \quad \text{se esiste} \quad X \in \mathcal{F} \quad \text{tale che} \quad \{a, b\} \subseteq X$$

è una relazione di equivalenza. Inoltre, se $\sim$ è un'equivalenza su A e $\mathcal{F}$ è l'insieme quoziente $A/\sim$, allora $\sim_\mathcal{F}$ coincide con $\sim$.

Fissato un insieme A, il concetto di relazione di equivalenza e quello di partizione su A sono quindi equivalenti.

Equivalenza definita da una applicazione. Sia $f : A \longrightarrow B$ un'applicazione. L' equivalenza definita da f è la relazione $\sim_f$ sull'insieme A definita da, per ogni $x, y \in A$: $x \sim_f y$ se $f(x) = f(y)$.

Si verifica facilmente che la relazione $\sim_f$, così definita, è una equivalenza su A; infatti:

riflessività: per ogni $a \in A$ si ha $f(a) = f(a)$ e dunque $a \sim_f a$.

simmetria: se $a, b \in A$ e $a \sim_f b$, allora $f(a) = f(b)$, dunque $f(b) = f(a)$ e $b \sim_f a$.

transitività: siano $a, b, c \in A$ con $a \sim_f b$, $b \sim_f c$; allora $f(a) = f(b) = f(c)$ e dunque $f(a) = f(c)$ e $a \sim_f c$.

Esempi. 1) L'equivalenza ρ dell'esempio 1) di pagina 76 è l'equivalenza definita dall'applicazione:

$$\begin{array}{rcl} f: & \mathbb{R} & \longrightarrow \mathbb{R} \\ & x & \mapsto |x| \end{array}$$

2) L'equivalenza dell'esempio 2) è l'equivalenza definita dall'applicazione dall'insieme Σ di tutte le circonferenze nell'insieme dei punti del piano, che ad ogni circonferenza $C \in \Sigma$ associa il centro di C.

3) L'equivalenza ω dell'esempio 3) è l'equivalenza definita dall'applicazione:

$$\begin{array}{rcl} f: & \mathbb{N} \times \mathbb{N} \setminus \{0\} & \longrightarrow \mathbb{Q} \\ & (a, b) & \mapsto \frac{a}{b} \end{array}$$

Un'applicazione f è iniettiva se e solo se l'equivalenza definita da f è l'uguaglianza (e in tal caso l'insieme quoziente $A/\sim_f$ si può identificare con A). In generale, l'equivalenza definita da un'applicazione f è lo strumento che consente di definire in modo naturale, a partire da f, un'applicazione iniettiva. Questa procedura è descritta dal seguente Teorema, che chiameremo *di fattorizzazione delle funzioni*, perché mostra come ogni applicazione sia la composizione di una applicazione suriettiva per unaapplicazione iniettiva.

Teorema 3.6. *Sia $f : A \longrightarrow B$ un'applicazione, sia $\sim_f$ l'equivalenza definita da f, e sia $\pi : A \longrightarrow A/\sim_f$ la proiezione canonica di A su $A/\sim_f$. Allora esiste una ed un'unica applicazione $\overline{f} : A/\sim_f \longrightarrow B$ tale che $f = \overline{f} \circ \pi$. Inoltre $\overline{f}$ è iniettiva e $Im(\overline{f}) = Im(f)$ (quindi se f è suriettiva, $\overline{f}$ è biettiva).*

Dimostrazione. Dimostriamo innanzi tutto l'esistenza di una applicazione $\overline{f}$ con la proprietà che $f = \overline{f} \circ \pi$. Per comodità denotiamo semplicemente con $\sim$ l'equivalenza definita dall'applicazione f; per ogni $a \in A$, abbiamo la classe di equivalenza

$$[a]_\sim = \{\ x \mid x \in A, a \sim x\ \} = \{\ x \mid x \in A, f(x) = f(a)\ \}.$$

Osserviamo che, per ogni $a, b \in A$, se $[a]_\sim = [b]_\sim$ allora $a \sim b$, cioè $f(a) = f(b)$. Quindi è **ben definita** (vedi commento che segue la dimostrazione) l'applicazione

$$\begin{array}{rcl} \overline{f} : A/\sim & \longrightarrow & B \\ [x]_\sim & \mapsto & f(x) \end{array}.$$

Si verifica quindi immediatamente che $f = \overline{f} \circ \pi$; infatti, per ogni $x \in A$ si ha

$$\overline{f} \circ \pi(x) = \overline{f}(\pi(x)) = \overline{f}([x]_\sim) = f(x).$$

Proviamo ora che tale applicazione $\overline{f}$ è unica.
Sia infatti $g : A/\sim_f \longrightarrow B$ tale che $f = g \circ \pi$. Allora, per ogni $[x]_\sim \in A/\sim$,:

$$g([x]_\sim) = g(\pi(x)) = (g \circ \pi)(x) = f(x) = \overline{f}([x]_\sim)$$

quindi $g = \overline{f}$.

Infine, è chiaro che, per come è stata definita $\overline{f}$, si ha $Im(f) = Im(\overline{f})$. Rimane da verificare che $\overline{f}$ è iniettiva: siano $[a]_\sim, [b]_\sim \in A/\sim$ tali che $\overline{f}([a]_\sim) = \overline{f}([b]_\sim)$; allora, per definizione di $\overline{f}$, $f(a) = f(b)$ quindi $a \sim b$ e perciò $[a]_\sim = [b]_\sim$, dimostrando così che $\overline{f}$ è iniettiva. ∎

Importante. Quando si definisce qualche cosa (applicazioni, relazioni, etc.) su un insieme quoziente, occorre tenere ben presente che gli *elementi del quoziente sono sottoinsiemi* (di un qualche insieme A) *e non i loro rappresentanti.* Bisogna cioè essere certi che le definizioni che diamo dipendano dalle classi in sé (come, ripeto, elementi del quoziente) e non da un particolare rappresentante. Questo si dice dare una **buona definizione**.

Ad esempio, l'applicazione $\overline{f}$ nella dimostrazione del Teorema di sopra, è ben definita perchè, data una classe di equivalenza $K \in A/\sim$, se $a \in K$ e poniamo $y = f(a)$, allora $f(b) = y$ per ogni $b \in K$ e quindi $\overline{f}(K) = y = f(a)$ non dipende dal rappresentante a della classe $K = [a]_\sim$ ma solo dalla classe K.

Come altro esempio, si consideri la relazione d'equivalenza ρ sull'insieme $\mathbb{Z}$ dei numeri interi, definita da, per ogni $x, y \in \mathbb{Z}$: $x\rho y$ se $|x| = |y|$. Supponiamo di pretendere di definire una applicazione g dall'insieme quoziente $\mathbb{Z}/\rho$ in $\mathbb{Z}$ mediante la regola:

$$\text{per ogni } [x]_\rho \in \mathbb{Z}/\rho \text{ poniamo } g([x]_\rho) = x + 1,$$

questa **non è** una buona definizione, dato che, ad esempio, $[-2]_\rho = [2]_\rho$, mentre la nostra definizione darebbe: $-1 = -2 + 1 = g([-2]_\rho) = g([2]_\rho) = 2 + 1 = 3$, che non sta in piedi.
Invece l'applicazione $g : \mathbb{Z}/\rho \longrightarrow \mathbb{Z}$ definita da, per ogni $[x]_\rho \in \mathbb{Z}/\rho$, $f([x]_\rho) = (-1)^x$ è ben definita. Infatti, per ogni $x, y \in \mathbb{Z}$, se $[x]_\rho = [y]_\rho$ allora $|x| = |y|$ e quindi $(-1)^x = (-1)^{|x|} = (-1)^y$.

3.3. Relazioni d'ordine.

Un relazione ρ sull'insieme A si dice **antisimmetrica** se, per ogni $a, b \in A$:

$$a\rho b \text{ e } b\rho a \Rightarrow a = b.$$

DEFINIZIONE. Una relazione ρ sull'insieme A si dice **relazione d'ordine** (o *ordinamento parziale*) se ρ è *riflessiva, antisimmetrica e transitiva.* Ovvero se, per ogni $a, b, c \in A$:

$$\begin{array}{rl} i) & a\rho a \\ ii) & a\rho b \text{ e } b\rho a \Rightarrow a = b \\ iii) & a\rho b \text{ e } b\rho c \Rightarrow a\rho c. \end{array}$$

Un **insieme parzialmente ordinato** (p.o.) è una coppia (A, ρ) dove A è un insieme e ρ una data relazione di ordine su A.

Esempi. 1) Sono insiemi parzialmente ordinati

$$(\mathbb{R}, \leq) \quad (\mathbb{Q}, \leq) \quad (\mathbb{Z}, \leq) \quad (\mathbb{N}, \leq)$$

dove $\leq$ è l'ordine naturale (ad esempio definito su $\mathbb{R}$ da $x \leq y$ se $y - x \geq 0$, ovvero se esiste $a \in \mathbb{R}$ tale che $y - x = a^2$).

2) Se X è un insieme, allora $(\mathcal{P}(X), \subseteq)$ dove $\subseteq$ è l'inclusione tra insiemi, è un insieme parzialmente ordinato.

3) Sia $|$ la relazione di divisibilità su $\mathbb{N}$, definita da, per ogni $a, b \in \mathbb{N}$:

$$a|b \text{ se esiste } c \in \mathbb{N} \text{ tale che } ac = b.$$

Allora $|$ è una relazione di ordine su $\mathbb{N}$. Infatti
- per ogni $n \in \mathbb{N}$, $n1 = n$, quindi $n|n$ e la relazione è riflessiva.
- se $n|m$ e $m|n$, allora esistono $c, d \in \mathbb{N}$ tali che $m = cn$ e $n = dm$; da cui segue $m = cn = cdm$. Se $m = 0$, allora $n = dm = 0$; altrimenti si ha $cd = 1$ e poichè $c, d \in \mathbb{N}$ deve essere $c = 1 = d$ e quindi $n = m$ e la relazione è antisimmetrica.
- Siano $n, m, s \in \mathbb{N}$ con $n|m$, $m|s$. Allora esistono $c, d \in \mathbb{N}$ tali che $m = cn$ e $s = dm$; quindi $s = dm = (dc)n$. Dunque $n|s$ e la relazione è transitiva.

Per indicare una generica relazione d'ordine su un insieme (generico o no) useremo di solito il simbolo $\leq$.

Un insieme parzialmente ordinato $(A, \leq)$ si dice **totalmente ordinato** se ogni coppia di elementi di A è "confrontabile"; ovvero se

$$\text{per ogni } a, b \in A, \ a \leq b \text{ o } b \leq a \ .$$

Gli esempi del tipo 1) di sopra sono insiemi totalmente ordinati. Quelli del tipo 2) non sono totalmente ordinati se $|X| \geq 2$; infatti se a_1, a_2 sono elementi distinti di X, allora $\{a_1\}, \{a_2\} \in \mathcal{P}(X)$ e $\{a_1\} \not\subseteq \{a_2\}$, $\{a_2\} \not\subseteq \{a_1\}$.
Infine, $(\mathbb{N}, |)$ nell' esempio 3) non è totalmente ordinato: ad esempio $2 \not| 3$ e $3 \not| 2$.

Definizioni. Sia $(A, \leq)$ un insieme parzialmente ordinato e sia $a \in A$:

1. a si dice elemento **massimo** di A se per ogni $b \in A$, $b \leq a$.
2. a si dice elemento **minimo** di A se per ogni $b \in A$, $a \leq b$.
3. a si dice elemento **massimale** di A se per ogni $b \in A$, $a \leq b \ \Rightarrow \ a = b$.
4. a si dice elemento **minimale** di A se per ogni $b \in A$, $b \leq a \ \Rightarrow \ a = b$.

Ad esempio, gli insiemi p.o. $(\mathbb{R}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{Z}, \leq)$ non hanno nè massimo nè minimo, nè elementi massimali o minimali. L'insieme $(\mathbb{N}, \leq)$ non ha massimo (nè elementi massimali) ed ha minimo 0 che è anche il solo elemento minimale
Se X è un insieme, l'insieme p.o. $(\mathcal{P}(X), \subseteq)$ ha minimo $\emptyset$ e massimo X.
L'insieme p.o. $(\mathbb{N}, |)$ ha minimo 1 (infatti $1|n$ per ogni $n \in \mathbb{N}$) e massimo 0 (infatti $n|0$ per ogni $n \in \mathbb{N}$). Se però togliamo 0 e consideriamo $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, l'insieme p.o. $(\mathbb{N}^*, |)$ non ha massimo nè elementi massimali: infatti, se $n \in \mathbb{N}^*$ allora $n|2n$ e $n \neq 2n$.

Dalle definizioni segue, in particolare, che ogni elemento massimo (minimo) è anche un elemento massimale (minimale). Osserviamo anche che un insieme p.o. può avere diversi elementi minimali (o massimali). Ad esempio nell'insieme p.o. $(\mathbb{N} \setminus \{1\}, |)$ dei numeri naturali diversi da 1 ordinato per divisibilità, gli elementi minimali sono tutti i numeri primi (positivi).
Questo non avviene per massimo e minimo: essi, se esistono, sono unici.

Proposizione 3.7. *Sia $(A, \leq)$ un insieme parzialmente ordinato. Se $(A, \leq)$ ha un elemento massimo (minimo), allora esso è l'unico elemento massimale (minimale) di $(A, \leq)$.*

Dimostrazione. Sia $a \in A$ un elemento massimo di $(A, \leq)$ e sia b un massimale. Allora $b \leq a$ perchè a è massimo, e quindi, poichè b è massimale, $a = b$.
(la dimostrazione per il minimo ed i minimali è simile.) ∎

Da questa proposizione segue in particolare che il massimo (minimo) di $(A, \leq)$, se esiste, è unico; esso si denota con $\max(A)$ (rispettivamente, $\min(A)$). Più in generale, se $(A, \leq)$ è un insieme p.o. e B è un sottoinsieme non vuoto di A, un elemento $x \in B$ si dice massimo (minimo) di B se, per ogni $b \in B$ si ha $b \leq x$ ($x \leq b$). Si dimostra allo stesso modo che se B ha un massimo (minimo) esso è unico, e si denota con $\max(B)$ (rispettivamente, $\min(B)$).

Ad esempio in $(\mathbb{N}, |\ )$ consideriamo il sottoinsieme $B = \{3n \mid 0 \neq n \in \mathbb{N}\}$. Allora B non ha massimo, e $\min(B) = 3$. (Si veda l'esercizio 3.43 per un esempio di insieme p.o. con un unico elemento minimale e nessun minimo.)

DEFINIZIONE. Sia $(A, \leq)$ un insieme parzialmente ordinato, sia $B \subseteq A$ e sia $a \in A$:

1. a si dice **maggiorante** di B se per ogni $b \in B,\ b \leq a$.
2. a si dice **minorante** di B se per ogni $b \in B,\ a \leq b$.

Esempi. 1) Nell'insieme p.o. $(\mathbb{Z}, \leq)$ il sottoinsieme $\mathbb{N}$ non ha maggioranti, mentre i suoi minoranti sono tutti gli interi $z \leq 0$.
In $(\mathbb{Q}, \leq)$ gli insiemi $B = \{x \in \mathbb{Q} \mid x \leq \frac{1}{3}\}$ e $C = \{x \in \mathbb{Q} \mid x < \frac{1}{3}\}$ hanno lo stesso insieme di maggioranti che è $\{x \in \mathbb{Q} \mid x \geq \frac{1}{3}\}$.
In $(\mathbb{R}, \leq)$ l'insieme dei maggioranti di $\{x \in \mathbb{Q} \mid x^2 \leq 2\}$ è $\{x \in \mathbb{R} \mid x \geq \sqrt{2}\}$.
2) Se X è un insieme non vuoto e $Y, Z \subseteq X$, l'insieme dei minoranti di $B = \{Y, Z\}$ nell'insieme p.o. $(\mathcal{P}(X), \subseteq)$ è $\{T \subseteq X \mid T \subseteq Y \cap Z\}$.
3) In $(\mathbb{N}, |)$ consideriamo il sottoinsieme $B = \{6,\ 9,\ 15\}$; allora i minoranti di B sono $1, 3$ e i maggioranti di B sono tutti i multipli di 90.

Dalla Proposizione 3.7, risulta che se l'insieme dei maggioranti (minoranti) di un sottoinsieme B ha minimo (massimo), esso è unico. Da qui la seguente definizione.

DEFINIZIONE. Sia $(A, \leq)$ un insieme parzialmente ordinato e sia $B \subseteq A$:

1. l'**estremo superiore** $\sup_A(B)$ di B in A è, se esiste, il minimo dei maggioranti di B.
2. l'**estremo inferiore** $\inf_A(B)$ di B in A è, se esiste, il massimo dei minoranti di B.

Dalla definizione segue immediatamente che se B ha massimo (minimo) allora $\max(B) = \sup_A(B)$ $(\min(B) = \inf_A(B))$.

Esempi. Con riferimento agli esempi di sopra, abbiamo

- $\inf_{\mathbb{Z}} \mathbb{N} = 0$; mentre $\mathbb{N}$ non ha estremo superiore in $(\mathbb{Z}, \leq)$.
- Se $B = \{x \in \mathbb{Q} \mid x < \frac{1}{3}\}$, $\sup_{\mathbb{Q}}(B) = \frac{1}{3}$.

- Se $C = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$, allora $\inf_{\mathbb{R}}(C) = -\sqrt{2}$, $\sup_{\mathbb{R}}(C) = \sqrt{2}$, mentre C non ha estremi inferiore e superiore in $(\mathbb{Q}, \leq)$.
- Se $Y, Z \subseteq X$, allora $\inf_{\mathcal{P}(X)}(\{Y, Z\}) = Y \cap Z$ e $\sup_{\mathcal{P}(X)}(\{Y, Z\}) = Y \cup Z$.
- $B = \{6,\ 9,\ 15\}$ ha estremo inferiore in $(\mathbb{N}, |)$ l'elemento 3, mentre il suo estremo superiore è 90.

Osserviamo che se X è un insieme e $\mathcal{S}$ un sottoinsieme non vuoto di $\mathcal{P}(X)$, allora

$$U = \bigcup_{X \in \mathcal{S}} X = \sup_{\mathcal{P}(X)}(\mathcal{S}) \qquad \text{e} \qquad W = \bigcap_{X \in \mathcal{S}} X = \inf_{\mathcal{P}(X)}(\mathcal{S})$$

infatti, U è un maggiorante di $\mathcal{S}$ in $(\mathcal{P}(X), \subseteq)$, e se Y è un maggiorante di $\mathcal{S}$ allora $X \subseteq Y$ per ogni $X \in \mathcal{S}$, e quindi $U \subseteq Y$. Dunque U è il minimo dei maggioranti di $\mathcal{S}$ e quindi $U = \sup_{\mathcal{P}(X)}(\mathcal{S})$. Similmente si osserva che W è il massimo dei minoranti di $\mathcal{S}$.

Reticoli. Un *reticolo* è un insieme parzialmente ordinato $(A, \leq)$ in cui, per ogni $a, b \in A$ esiste $\sup(\{a, b\})$ e $\inf(\{a, b\})$.

Se $(A, \leq)$ è un reticolo, e $a, b \in A$ si scrive

$$a \wedge b = \inf(\{a, b\}) \quad \text{e} \quad a \vee b = \sup(\{a, b\}).$$

L'esempio di riferimento per i reticoli è quello dell'insieme delle parti di un insieme. Infatti, se X è un insieme non vuoto allora $(\mathcal{P}(X), \subseteq)$ è un reticolo; dove, per ogni $Y, Z \in \mathcal{P}(X)$:

$$Y \wedge Z = Y \cap Z \quad \text{e} \quad Y \vee Z = Y \cup Z.$$

Altri esempi. 1) Sia $(A, \leq)$ un insieme parzialmente ordinaro, e $a, b \in A$ con $a \leq b$, allora $a = \inf(\{a, b\})$ e $b = \sup(\{a, b\})$. Da ciò segue che ogni insieme totalmente ordinato è un reticolo (relativamente banale).

2) $(\mathbb{N}, |)$ è un reticolo. Se $a, b \in \mathbb{N}$, allora $a \wedge b = MCD(a, b)$ e $a \vee b = m.c.m.(a, b)$.

3) Sia X un insieme, con $|X| \geq 4$ e sia $\mathcal{D} = \{\ Y \subseteq X \mid |Y|$ è dispari $\}$. Allora $(\mathcal{D}, \subseteq)$ è un un insieme p.o. ma non è un reticolo. Infatti, siano $a, b \in X$ con $a \neq b$ e poniamo $A = \{a\}$, $B = \{b\}$; allora $A, B \in \mathcal{D}$ e, per ogni $x \in X$ con $a \neq x \neq b$ il sottoinsieme $\{a, b, x\}$ è un elemento minimale nell'insieme dei maggioranti in $\mathcal{D}$ di $\{A, B\}$. Poichè $|X| \geq 4$ l'insieme dei maggioranti di $\{A, B\}$ ha almeno due elementi minimali e dunque non ha minimo, cioè non esiste l'estremo superiore in $\mathcal{D}$ di $\{A, B\}$.

Lemma di Zorn. Il Lemma di Zorn, che non dimostreremo, è uno strumento che trova applicazioni in diverse parti della matematica. Esso è equivalente al cosiddetto *Assioma della Scelta*, che è enunciato più avanti.

Sia $(A, \leq)$ un insieme parzialmente ordinato. Un sottoinsieme non vuoto C di A si dice una **catena** se è totalmente ordinato dall'ordine indotto da A, ovvero se, per ogni $x, y \in C$ si ha $x \leq y$ o $y \leq x$.

Ad esempio l'insieme $\{\ 2^n \mid n \in \mathbb{N}\ \}$ è una catena dell'insieme p.o. $(\mathbb{N}\ , |)$.
(altro esempio) Posto, per ogni $0 \leq r \in \mathbb{R}$, $I_r = \{\ x \in \mathbb{R} \mid |x| \leq r\ \}$, l'insieme $\mathcal{C} = \{\ I_r \mid 0 \leq r \in \mathbb{R}\ \}$ è una catena dell'insieme p.o. $(\mathcal{P}(\mathbb{R}), \subseteq)$. (osserviamo che tale catena $\mathcal{C}$ non è numerabile).

DEFINIZIONE. Un insieme parzialmente ordinato $(A, \leq)$ si dice **induttivo** se per ogni sua catena C esiste almeno un maggiorante di C in A.

Esempi. 1) L'insieme p.o. $(\mathbb{Z}, \leq)$ non è induttivo: infatti è esso stesso una catena e non ha estremo superiore (massimo).

2) Posto $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, l'insieme p.o. $(\mathbb{N}^*, |)$ non è induttivo; ad esempio la catena $\{ 2^n \mid n \in \mathbb{N} \}$ non ha estremo superiore.

3) Sia X un insieme. Allora l'insieme p.o. $(\mathcal{P}(X), \subseteq)$ è induttivo; infatti se $\mathcal{C}$ è una catena di $\mathcal{P}(X)$ allora $\bigcup_{A \in \mathcal{C}} A = \sup(\mathcal{C})$.

Lemma di Zorn. *Ogni insieme parzialmente ordinato induttivo ha almeno un elemento massimale.*

Nel corso del primo anno di studi una applicazione importante del Lemma di Zorn riguarda lo studio degli spazi vettoriali, ed è la dimostrazione che ogni spazio vettoriale ha almeno una *base*. Vediamo rapidamente questo fatto.

Sia $\mathbf{V}$ uno spazio vettoriale. Un insieme X di vettori di $\mathbf{V}$ è detto linearmente indipendente, se tale è ogni sottoinsieme finito non vuoto di X. Consideriamo ora l'insieme $\mathcal{I}$ di tutti i sottoinsiemi linearmente indipendenti di $\mathbf{V}$ ordinato per inclusione. Allora $\mathcal{I} \neq \emptyset$ (per ogni $\mathbf{0} \neq \mathbf{v} \in \mathbf{V}, \{\mathbf{v}\} \in \mathcal{I}$) e $(\mathcal{I}, \subseteq)$ è un insieme p.o. **induttivo**. Infatti sia $\mathcal{C}$ una catena in $\mathcal{I}$ e sia $U = \bigcup_{X \in \mathcal{C}} X$; proviamo che $U \in \mathcal{I}$. Sia $\{v_1, v_2, \ldots, v_n\}$ un sottoinsieme finito non vuoto di U, allora per ogni $i = 1, 2, \ldots, n$ esiste $X_i \in \mathcal{C}$ tale che $v_i \in X_i$; ma poichè $\mathcal{C}$ è una catena l'insieme $\{X_1, X_2, \ldots, X_n\}$ ha massimo (vedi l'esercizio 5) che possiamo supporre sia X_1; cioè, per $i = 1, 2, \ldots, n$, $X_i \subseteq X_1$, e dunque $\{v_1, v_2, \ldots, v_n\} \subseteq X_1$, quindi $\{v_1, v_2, \ldots, v_n\}$ è linearmente indipendente, e questo dimostra, per definizione, che U è linearmente indipendente, cioè che $U \in \mathcal{I}$. Ma allora $U = sup_{\mathcal{I}}(\mathcal{C})$.

Quindi $(\mathcal{I}, \subseteq)$ è induttivo e dunque, per il Lemma di Zorn, ha almeno un elemento massimale B. La dimostrazione si completa provando che B è una base di $\mathbf{V}$, e ciò si fa osservando che se $\mathbf{v} \in \mathbf{V} \setminus B$ allora $B \cup \{\mathbf{v}\}$ non è linearmente indipendente.

Assioma della Scelta. *Sia S un insieme, e F un insieme non vuoto di sottoinsiemi non vuoti di S. Allora esiste una applicazione $f : F \to S$ tale che per ogni $X \in F$, $f(X)$ è un elemento di X.*

In sostanza l'Assioma della Scelta dice che se abbiamo un insieme non vuoto di sottoinsiemi non vuoti di S allora esiste un insieme (l'immagine della funzione f) che contiene un elemento "scelto" in ciascuno dei sottoinsiemi che stiamo considerando.

Per quanto appaia naturale, l'Assioma della Scelta è, nelle principali assiomatizzazioni della Teoria degli Insiemi, indipendente dagli altri assiomi (che non possiamo discutere qui). Si può provare che esso è equivalente al Lemma di Zorn. Accettando l'Assioma della Scelta si ha il Lemma di Zorn; mentre se non si accetta l'Assioma della Scelta, come nelle impostazioni più rigorosamente costruttiviste, si deve anche rinunciare al Lemma di Zorn.

Esercizio 3.3. Sia A un insieme e ρ una relazione di equivalenza su A. Si consideri l'insieme delle parti $P(A)$ ordinato per inclusione. Diciamo che un sottoinsieme X di A è *libero* se per ogni coppia $a, b \in X$, $a \neq b$ si ha $(a, b) \notin \rho$. Utilizzando il Lemma di Zorn si dimostri che esistono sottoinsiemi liberi massimali, e che essi hanno tutti lo stesso numero di elementi.

3.4. Esercizi.

• *esercizi sulle operazioni e i semigruppi*

Esercizio 3.4. Sia S un insieme non vuoto. Si provi che l'operazione definita su S da $(a,b) \mapsto a$ è associativa.

Esercizio 3.5. Sia X un insieme non vuoto, e $P = \mathcal{P}(X)$ il suo insieme delle parti. Si provi che $(P, \cup)$ e $(P, \cap)$ sono monoidi commutativi.

Esercizio 3.6. Sia G un gruppo, e sia $g^{-1} = g$ per ogni $g \in G$. Si dimostri che G è commutativo.

Esercizio 3.7. Si dica se i monoidi dell'esercizio 3.5 sono gruppi. Si provi che $(\mathcal{P}(X), \Delta)$ è un gruppo.

Esercizio 3.8. Siano $(A, \cdot)$, $(B, *)$ semigruppi. Sul prodotto diretto $A \times B$ si definisca una operazione ponendo, per ogni $(a,b), (a_1, b_1) \in A \times B$:

$$(a,b)(a_1,b_1) = (a \cdot a_1, b * b_1) \ .$$

Si dimostri che, con tale operazione, $A \times B$ è un semigruppo. Si provi che se A e B sono monoidi (gruppi), allora $A \times B$ è un monoide (gruppo).

Esercizio 3.9. Sull'insieme $\mathbb{N}^*$ dei numeri naturali diversi da zero si definisca l'operazione τ ponendo, per ogni $n, m \in \mathbb{N}^*$: $n \tau m = MCD(n,m)$. Si dica se tale operazione è associativa e se esiste un elemento identico.

Esercizio 3.10. Sia $(S, \cdot)$ un semigruppo e siano T, V sottoinsiemi chiusi di S. Sia $TV = \{\, x \cdot y \mid x \in T \ \text{ e } \ y \in V \,\}$. Si dimostri che se $x \cdot y = y \cdot x$ per ogni $x \in T$ e $y \in V$, allora TV è un sottoinsieme chiuso di S.

Esercizio 3.11. Sia M un monoide che soddisfa la *legge di cancellazione*; per ogni $a, b, c \in M$ se $ab = ac$ allora $b = c$. Si provi che se M è finito allora è un gruppo. [sugg.: per ogni $a \in M$ si consideri la applicazione da M in se stesso definita da $x \mapsto ax$; usando la proprietà di cancellazione si provi che è iniettiva e quindi ...] Si dica se la stessa affermazione vale se M è infinito.

Esercizio 3.12. Sia $(G, \cdot)$ un gruppo e sia $a \in G$ tale che $ag = ga$ per ogni $g \in G$. Su G si definisca una nuova operazione $*$, ponendo, per ogni $x, y \in G$: $x * y = x \cdot a \cdot y$. Si provi che $(G, *)$ è un gruppo,

Esercizio 3.13. Sia $U = \{z \in \mathbb{C} \mid |z| = 1\}$ (nel piano di Argand–Gauss è l'insieme dei punti della circonferenza di centro l'origine e raggio 1). Si provi che U è un gruppo rispetto alla moltiplicazione.

Esercizio 3.14. Si provi che l'insieme di numeri razionali

$$\mathbb{Q}_2 = \left\{ \ \frac{m}{2^i} \mid m \in \mathbb{Z}, \ i \in \mathbb{N} \ \right\}$$

è un gruppo rispetto all'addizione.

Esercizio 3.15. Si dimostri che un gruppo non può essere unione insiemistica di due sottoinsiemi chiusi propri. Cosa si può dire in proposito per un monoide ?

• *esercizi sulle relazioni d'equivalenza*

Esercizio 3.16. Si provi che la relazione $\sim$ definita sull'insieme $\mathbb{R}$ dei numeri reali da, per ogni $x, y \in \mathbb{R}$,

$$x \sim y \text{ se } x - y \in \mathbb{Z}$$

è una relazione di equivalenza.

Esercizio 3.17. Sia ω un'equivalenza sull'insieme A. Su $A \times A$ sia definita una relazione ρ ponendo, per ogni $(a,b),(c,d) \in A \times A$, $(a,b)\rho(c,d)$ se $a\omega c$ o $b\omega d$. Si dica se ρ è una relazione di equivalenza.

Esercizio 3.18. Siano ρ, ρ' relazioni su un insieme A. Si definisce la *relazione composta* $\rho \circ \rho'$ ponendo, per ogni $x, y \in A$, $x(\rho \circ \rho')y$ se esiste $z \in A$ tale che $x\rho z$ e $z\rho' y$. Si provi che

(a) se ρ e ρ' sono riflessive, allora $\rho \circ \rho'$ è riflessiva;

(b) ρ è transitiva se e solo se $\rho \circ \rho \subseteq \rho$;

(c) si trovi un esempio in cui ρ e ρ' sono equivalenze ma $\rho \circ \rho'$ non è una equivalenza.

Esercizio 3.19. Sia ρ la relazione sull'insieme $\mathbb{Z}$ dei numeri interi definita da:

per ogni $a, b \in \mathbb{Z}$, $a\rho b$ se $a^2 - b^2$ è divisibile per 4.

Si provi che ρ è un'equivalenza su $\mathbb{Z}$, quindi si determini la classe di equivalenza di 3 (modulo ρ).

Esercizio 3.20. Determinare tutte le relazioni di equivalenza dell'insieme $\{1, 2, 3\}$.

Esercizio 3.21. Si descrivano le classi di equivalenza nel caso dell'esempio 3) a pagina 73.

Esercizio 3.22. Sia $A = \mathbb{N}^{\mathbb{N}} = \{\ f |\ f : \mathbb{N} \longrightarrow \mathbb{N}\ \}$ l'insieme di tutte le applicazioni di $\mathbb{N}$ in se stesso; sia ω la relazione su A definita da, per ogni $f, g \in A$:

$$f\omega g \quad \text{se l'insieme } \{n \mid n \in \mathbb{N}\ , f(n) \neq g(n)\} \text{ è finito.}$$

(1) Si provi che ω è una relazione di equivalenza su A.

(2) Si dimostri che l'insieme quoziente A/ω è infinito [sugg.: si rifletta intorno alle applicazioni costanti].

Esercizio 3.23. Sia X un insieme non vuoto e siano $\mathcal{F}$ e $\mathcal{G}$ partizioni di X. Si provi che $\mathcal{F} \cup \mathcal{G}$ è una partizione di X se e solo se $\mathcal{F} = \mathcal{G}$.

Esercizio 3.24. Nell'insieme $A = \mathbb{N} \times \mathbb{N}$ sia definita la relazione ω ponendo , per ogni $(a,b),(c,d) \in A$: $(a,b)\omega(c,d)$ se e solo se $b = d$.
Si provi che ω è una equivalenza, si descriva l'insieme quoziente A/ω, e si trovi un'applicazione $f : A \longrightarrow \mathbb{N}$ tale che ω sia l'equivalenza definita da f.

Esercizio 3.25. Sia X un insieme non vuoto e sia $A = X^{\mathbb{N}}$ l'insieme di tutte le applicazioni dall'insieme $\mathbb{N}$ dei numeri naturali nell'insieme X. In A si consideri la relazione ω , definita ponendo, per ogni $f\ , g \in A$, $f\omega g$ se e solo se esiste $n \in \mathbb{N}$ tale che $f(i) = g(i)$ per ogni $i \geq n$. Si dimostri che ω è una relazione di equivalenza.

Esercizio 3.26. Sia A un insieme non vuoto e siano ρ_1 e ρ_2 relazioni di equivalenza su A. Si provi che se $\rho_1 \cup \rho_2 = A \times A$ allora una delle due relazioni è banale (la relazione banale su A è $A \times A$).

Esercizio 3.27. Sia $A = \mathcal{P}(\mathbb{N})$ l'insieme delle parti dell'insieme dei numeri naturali. Si dica quali fra le seguenti relazioni ω_1, ω_2 definite su A sono equivalenze.

1) per ogni $X, Y \in A$, $X\omega_1 Y$ se $X \cap Y$ è finito.

2) per ogni $X, Y \in A$, $X\omega_2 Y$ se $X \triangle Y$ è finito.

Esercizio 3.28. Sia $f : A \longrightarrow B$ un'applicazione tra insiemi non vuoti. Sia $\Omega = \mathcal{P}(B) \setminus \{\emptyset\}$, e sia ρ la relazione su Ω definita da:

$$\text{per ogni} \quad X, Y \in \Omega \ , \ X\rho Y \ \text{ se } \ f^{-1}(X) \cap f^{-1}(Y) \neq \emptyset \ .$$

Si dica quali delle seguenti affermazioni sono vere.
(a) ρ è riflessiva se e solo se f è suriettiva.
(b) ρ è simmetrica.
(c) ρ è transitiva se e solo se f è iniettiva.
(d) ρ è transitiva se e solo se $|f(A)| = 1$.

Esercizio 3.29. Sia A un insieme con $|A| \geq 2$ e $\Omega = \mathcal{P}(A) \setminus \{A\}$. Sia ρ la relazione su Ω definita da:

$$\text{per ogni } X, Y \in \Omega, \ X\rho Y \ \text{ se } \ X \cup Y \neq A.$$

(a) Si dica se ρ è una relazione di equivalenza su A.

(b) Sia ω una relazione di equivalenza su Ω tale che $\rho \subseteq \omega$ (cioè $X\rho Y \Rightarrow X\omega Y$ per ogni $X, Y \in \Omega$). Si provi che ω è la relazione banale (cioè $X\omega Y$ per ogni $X, Y \in \Omega$).

Esercizio 3.30. Siano A, B insiemi non vuoti, con $|B| \geq 2$, e sia $f : A \longrightarrow B$ una applicazione. Sia $\Omega = \mathcal{P}(B) \setminus \{\emptyset, B\}$ e sia ρ la relazione su Ω definita da, per ogni $X, Y \in \Omega$, $X\rho Y$ se solo se $f^{-1}(X) \cup f^{-1}(Y) \neq A$. Provare che :

(a) ρ è riflessiva se e solo se f è suriettiva;

(b) se $|f(A)| \geq 3$, ρ non è transitiva.

Esercizio 3.31. Sia X un insieme finito e Y un fissato sottoinsieme di X. Sull'insieme $\mathcal{P}(X)$ si definisca la relazione ρ ponendo, per ogni $S, T \in \mathcal{P}(X)$:

$$S \,\rho\, T \quad \Leftrightarrow \quad S \setminus Y = T \setminus Y \ .$$

(1) Si provi che ρ è una relazione d'equivalenza.

(2) Per ogni $S \in \mathcal{P}(X)$, si descriva la classe di equivalenza $[S]_\rho$, e si determini $|[S]_\rho|$.

(3) Si calcoli $\left|\frac{\mathcal{P}(X)}{\rho}\right|$.

Esercizio 3.32. Sull'insieme $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$ si definisca la relazione ω ponendo, per ogni $x, y \in \mathbb{Z}_0$, $x\omega y$ se e solo se xy è un quadrato in $\mathbb{Z}$ (ovvero se esiste $a \in \mathbb{Z}$ tale che $xy = a^2$).

(a) Si provi che ω è una equivalenza in $\mathbb{Z}_0$.

(b) Si provi che l'insieme quoziente $\mathbb{Z}_0/\omega$ è infinito.

Esercizio 3.33. Sull'insieme $A = \mathbb{C} \setminus \{0\}$ si considerino le relazioni ρ_1, ρ_2 definite da, per ogni $z = a + ib$, $z_1 = a_1 + ib_1 \in A$:

$$z\rho_1 z_1 \quad \text{se e solo se} \quad |z| = |z_1| \ ;$$

$$z\rho_2 z_1 \quad \text{se e solo se} \quad ab_1 = a_1 b.$$

(a) Si provi che $z\rho_2 z_1$ se e solo se esiste $a \in R$ tale che $z_1 = az$; si provi quindi che ρ_2 è una equivalenza.

(b) Sia ρ la relazione su A definita da, per ogni $z, z_1 \in A$, $z\rho z_1$ se e soltanto se esiste $x \in A$ tale che $z\rho_1 x$ e $x\rho_2 z_1$. Si dimostri che ρ è la relazione banale su A.

Esercizio 3.34. Sia $\sim$ la relazione sull'insieme dei numeri reali $\mathbb{R}$ definita da, per ogni $x, y \in \mathbb{R}$:

$$x \sim y \quad \text{se} \quad (x + y + 1)(x - y) = 0.$$

(a) Si provi che $\sim$ è una relazione di equivalenza.

(b) Si provi che $\sim$ è la equivalenza associata alla applicazione

$$f : \mathbb{R} \longrightarrow \mathbb{R}, \text{ definita da, per ogni } x \in \mathbb{R} : \ f(x) = x^2 + x + 1.$$

(c) Si dica se la seguente equaglianza è vera:

$$\mathbb{R}/\sim = \{ \ [x]_\sim \mid x \in \mathbb{R} \ , x \geq 0 \ \}$$

dove $[x]_\sim$ è la classe di equivalenza di x.

Esercizio 3.35. Sia $\mathbb{N}$ l'insieme dei numeri naturali, e sia $A = \mathbb{N} \times \mathbb{N}$. Sia ρ la relazione su A definita da, per ogni $(n, m), (n_1, m_1) \in A$:

$$(n, m)\rho(n_1, m_1) \ \text{ se e solo se } \ max\{n, m\} = max\{n_1, m_1\}.$$

(a) Si dimostri che ρ è una relazione di equivalenza;

(b) Si dica se il quoziente A/ρ è finito o infinito;

(c) Al variare di $(n, m) \in A$ si dica se la classe di equivalenza $[(n, m)]_\rho$ è finita o infinita.

Esercizio 3.36. Fissato un intero $n \geq 1$, su $\mathbb{Z}$ si definisca la relazione $\sim$ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a \sim b \quad \text{se} \quad \begin{cases} n \mid a - b & \text{per} \quad a, b \geq 3 \\ 2n \mid a - b & \text{per} \quad a, b < 3 \end{cases}$$

(a) Si provi che $\sim$ è una relazione d'equivalenza su $\mathbb{Z}$.

(b) Si determini la cardinalità dell'insieme quoziente $\mathbb{Z}/\sim$.

Esercizio 3.37. Sia $\sim$ la relazione sull'insieme $\mathbb{R}$ dei numeri reali definita da, per ogni $x, y \in \mathbb{R}$:

$$x \sim y \quad \text{se} \quad x - y \in \mathbb{Z} \ .$$

a) si provi che $\sim$ è una equivalenza;

b) si provi che la seguente applicazione è ben definita:

$$f : \ \mathbb{R}/\sim \longrightarrow \ \mathbb{R}/\sim \quad \text{definita da, per ogni } [x] \in \mathbb{R}/\sim : \ f([x]) = [2x],$$

e si dica quindi se f è suriettiva e/o iniettiva;

c) si provi che, per ogni $x \in \mathbb{R}$

$$f^{-1}([x]) = \ \left\{ \left[\frac{x}{2}\right] \ , \ \left[\frac{x+1}{2}\right] \right\}.$$

• *esercizi sulle relazioni d'ordine* (altri problemi, con soluzione, si trovano QUI)

Esercizio 3.38. Descrivere tutte le relazioni d'ordine sull'insieme $\{1, 2, 3\}$.

Esercizio 3.39. Sull'insieme $\mathbb{N}^*$ dei numeri naturali non nulli si definiamo la relazione ρ ponendo, per ogni $x, y \in \mathbb{N}^*$, $x\rho y$ se $\frac{1}{x} \leq \frac{1}{y}$. Si dimostri che ρ è una relazione d'ordine su $\mathbb{N}^*$.

Esercizio 3.40. (Ordine lessicografico) Siano (A, ρ), (B, σ) due insiemi parzialment ordinati. Sul prodotto $A \times B$ definiamo la relazione $\leq$ ponendo, per ogni $(a, b), (a_1, b_1) \in A \times B$,

$$(a, b) \leq (a_1, b_1) \text{ se } a\rho a_1 \text{ e } a \neq a_1 \text{ oppure } a = a_1 \text{ e } b\sigma b_1.$$

Si dimostri che $\leq$ è una relazione d'ordine su $A \times B$. Si dimostri che $(A \times B, \leq)$ è totalmente ordinato se e solo se tali sono (A, ρ) e (B, σ).

Esercizio 3.41. Sia $(A, \leq)$ un insieme parzialmente ordinato. Sull'insieme A^A di tutte le applicazioni di A in sè definiamo la relazione ρ ponendo, per ogni $f, g \in A^A$, $f\rho g$ se $f(a) \leq g(a)$ per ogni $a \in A$. Si dimostri che ρ è una relazione d'ordine parziale. Si provi che ρ è una relazione d'ordine totale se e solo se $|A| = 1$.

Esercizio 3.42. Sia $(A, \leq)$ un insieme totalmente ordinato. Si dimostri che ogni sottoinsieme **finito** e non vuoto di A ha massimo e minimo.

Esercizio 3.43. Sia $A = P(\mathbb{N})$ l'insieme delle parti dell'insieme dei numeri naturali. Su A si definisca una relazione ρ ponendo, per ogni $X, Y \in A$, $X\rho Y$ se $X \subseteq Y$ e $Y \setminus X$ è finito. Si provi che ρ è una relazione d'ordine e si dica se è una relazione d'ordine totale. Si dica se è vero che per ogni $X, Y \in A$, $\{X, Y\}$ ammette un estremo inferiore in (A, ρ).

(a) Si determinino, se esistono, massimo, minimo, massimali e minimali di A.

(b) Sia $B = \{\mathbb{N} \setminus \{n\} | n \in \mathbb{N}\}$; si determinino, se esistono, l'estremo inferiore e superiore di B in A.

Esercizio 3.44. Sull'insieme $\mathbb{N}^*$ dei numeri naturali non nulli definiamo la relazione ρ ponendo, per ogni $n, m \in \mathbb{N}^*, n\rho m$ se esiste $b \in \mathbb{N}^*$ tale che $m = n^b$. Si dimostri che ρ è una relazione d'ordine. Si determinino, se esistono, gli elementi massimali e minimali di $(\mathbb{N}^*, \rho)$. Si dica per quali coppie $n, m \in \mathbb{N}^*$ esiste l'estremo superiore di $\{n, m\}$.

Esercizio 3.45. Sia X un insieme non vuoto e sia ρ una relazione su X che è riflessiva e transitiva. Su X si definisca quindi una relazione $\#$ ponendo, per ogni $a, b \in X : a\#b$ se avviene $a\rho b$ e $b\rho a$. Si dimostri che $\#$ é una equivalenza. Quindi, sull'insieme quoziente $X/\#$ si definisca (si provi che si tratta di una buona definizione !) una relazione $\leq$ ponendo per ogni $a, b \in X : [a]_\# \leq [b]_\#$ se $a\rho b$. Si provi che la $\leq$ così è una relazione d' ordine su $X/\#$.

Esercizio 3.46. Sia $(A, \leq)$ un insieme parzialmente ordinato. Sia $a \in A$ tale che per ogni $x \in A$ il sottoinsieme $\{a, x\}$ ha estremo superiore. Si dimostri che $a \leq b$ per ogni elemento massimale b di A.

Esercizio 3.47. Sia $(A, \leq)$ un insieme parzialmente ordinato, e siano $a, b \in A$. Si dimostri che le seguenti affermazioni sono equivalenti

1. $a = \inf(\{a, b\})$;
2. $a \leq b$;
3. $b = \sup(\{a, b\})$.

Esercizio 3.48. Sia $P = \{p^n | p$ è un numero primo e $n \geq 1\}$ l'insieme dei numeri naturali che sono potenze di un primo. Su P si definisca la relazione $\lhd$ ponendo, per ogni $p^n, q^m \in P$,

$$p^n \lhd q^m \text{ se } p \leq q \text{ e } n \text{ divide } m.$$

Si dimostri che $(P, \lhd)$ é un insieme parzialmente ordinato, se ne determinino gli eventuali elementi minimali e si dica se $(P, \lhd)$ é totalmente ordinato.

Esercizio 3.49. Sia $(A, \leq)$ un insieme totalmente ordinato con almeno due elementi e sia $X = A^{\mathbb{N}}$ l'insieme delle applicazioni da $\mathbb{N}$ in A.
Sia $\lhd$ la relazione su X definita da, per ogni $f, g \in X$, $f \lhd g$ se $f = g$ oppure

$$\text{esiste } m \in \mathbb{N} \text{ tale che } f(x) = g(x) \text{ per ogni } x < m \text{ e } f(m) < g(m)$$

(a) Si dimostri che $\lhd$ é una relazione d'ordine su X.

(b) Si determini in $(X, \lhd)$ una catena discendente $f_1 \rhd f_2 \rhd f_3 \rhd \ldots$ con $f_i \neq f_{i+1}$ per ogni $i \in \mathbb{N}$.

Esercizio 3.50. Su $\mathbb{Q}$ definiamo la relazione ρ ponendo, per ogni $x, y \in \mathbb{Q}$, $x \rho y$ se esiste $n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$ tale che $y = nx$. Si dimostri che $(\mathbb{Q}, \rho)$ è un insieme parzialmente ordinato. Si dica se è totalmente ordinato. Si determinino, se esistono, gli estremi inferiore e superiore dei sottoinsiemi $\{\frac{1}{2^m} \mid 0 \neq m \in \mathbb{N}\}$ e $\{\frac{1}{3}, \frac{3}{2}\}$. Si dica se $(\mathbb{Q}, \rho)$ è un reticolo.

Esercizio 3.51. Sia $A = P(\mathbb{N})$ l'insieme delle parti dell'insieme dei numeri naturali. Su A si definisca una relazione ρ ponendo, per ogni $X, Y \in A$, $X \rho Y$ se $X \subseteq Y$ e $Y \setminus X$ é finito.
Si provi che ρ é una relazione d'ordine e si dica se é una relazione d'ordine totale. Si dica se é vero che per ogni $X, Y \in A$, $\{X, Y\}$ ammette un estremo inferiore in (A, ρ).

(a) Si determinino, se esistono, massimo, minimo, elementi massimali e minimali di A.

(b) Sia $B = \{\mathbb{N} \setminus \{n\} | n \in \mathbb{N}\}$; si determinino, se esistono, l'estremo inferiore e superiore di B in A.

Esercizio 3.52. Sia $\mathbb{N}$ l'insieme dei numeri naturali. Si consideri il seguente sottoinsieme di $P(\mathbb{N})$:

$$\mathbf{A} = \{X \subseteq \mathbb{N} \mid |\mathbb{N} \setminus X| \text{ è finito }\} \cup \{\emptyset\}.$$

Si dica se $\mathbf{A}$ ha un estremo inferiore e se ha un estremo superiore nell'insieme parzialmente ordinato $(P(\mathbb{N}), \subseteq)$ e in caso affermativo, li si determini.

Esercizio 3.53. Sull'insieme Γ di tutte le applicazioni da $\mathbb{N}$ in $\mathbb{N}$ si definisca la relazione $\angle$ ponendo, per ogni $f, g \in \Gamma$, $f \angle g$ se per ogni sottoinsieme <u>infinito</u> X di N si ha $f(X) \subseteq g(X)$.
Si dimostri che $\angle$ é una relazione d'ordine. Si dica quindi se si tratta di una relazione d'ordine totale su Γ.

Esercizio 3.54. Siano $\mathbb{Q}$ l'insieme dei numeri razionali, $\mathbb{N}_o$ l'insieme dei numeri naturali diversi da zero, e $A = \mathbb{Q} \times \mathbb{N}_o$. Sia ω la relazione su A definita da, per ogni $(x, n), (y, k) \in A$,

$$(x, n)\omega(y, k) \text{ se } x < y \text{ oppure } x = y \text{ e } n|k.$$

(a) Si dimostri che ω è una relazione d'ordine su A.

(b) Si dica se l'ordine indotto da ω è totale.

(c) Sia $B = \{(x, n) \in A \mid x \leq 0 \text{ e } n \leq 3\}$. Si determini, se esiste, $\sup(B)$. Stessa domanda per $C = \{(x, n) \in A \mid x < 0 \text{ e } n \leq 3\}$.

Esercizio 3.55. Sia $(A, \leq)$ un reticolo e $a \in A$ un elemento massimale. Si dimostri che a è il massimo di A.

3.5. Complementi: Reticoli e algebre di Boole

In questa sezione approfondiremo la teoria dei reticoli, che riveste una certa importanza nelle applicazioni informatiche. Abbiamo già dato la definizione: un *reticolo* è un insieme parzialmente ordinato $(A, \leq)$ in cui per ogni $a, b \in A$ esistono $\sup(\{a, b\})$ e $\inf(\{a, b\})$. In tal caso di scrive

$$a \wedge b = \inf(\{a, b\}) \quad \text{e} \quad a \vee b = \sup(\{a, b\}).$$

Un reticolo L dotato di massimo e di minimo si dice **limitato**; in tal caso è uso denotare il massimo di L con 1, ed il minimo con 0. Abbiamo indicato alcuni tra i più importanti esempi di reticoli nella sezione 3.3. Ricoprdiamo solo come l'esempio fondamentale di reticolo limitato è quello costituito dell'insieme delle parti $\mathcal{P}(X)$ di un insieme non vuoto X con la relazione di inclusione.

Facciamo ora l'ovvia ma importante osservazione che in un reticolo L i simboli $\vee$ e $\wedge$ possono essere intesi come quelli di due operazioni binarie su L; ed è chiaro dalle definizioni che per ogni coppia di elementi a, b di L si ha $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$, ovvero che le due operazioni sono commutative. La seguente facile proposizione riguarda altre proprietà elementari delle operazioni $\vee$ e $\wedge$ in un reticolo.

Proposizione 3.8. *Sia $(A, \leq)$ un reticolo. Allora, per ogni $x, y, z \in A$ si ha:*

1. (associatività di $\wedge$) $x \wedge (y \wedge z) = (x \wedge y) \wedge z)$
2. (associatività di $\vee$) $x \vee (y \vee z) = (x \vee y) \vee z)$
3. (proprietà di assorbimento) $x \wedge (x \vee y) = x = x \vee (x \wedge y)$.

Dimostrazione. Poiché le proprietà 1. e 2. sono di facile verifica, proviamo solo la 3. Siano x, y elementi di un reticolo $(A, \leq)$. Allora, $a = x \vee y = \sup(\{x, y\}) \leq x$, e quindi $x \wedge (x \vee y) = \sup(\{x, a\}) = x$. La dimostrazione che $x = x \vee (x \wedge y)$ è analoga. ∎

Quindi, ogni reticolo $(L, \leq)$, che inizialmente è un insieme parzialmente ordinato, è naturalmente dotato di una struttura algebrica affine a quelle di strutture come i semigruppi o i gruppi: su $(L \leq)$ sono definite le due operazioni binarie $(a, b) \mapsto$

$a \vee b$, $(a, b) \mapsto a \wedge b$, che per la Proposizione 3.8 e l'osservazione che la precede, sono *commutative*, *associative* e soddisfano la cosiddetta *proprietà di assorbimento* (punto 3. della proposizione). Se inoltre il reticolo L è limitato, e si denotano, rispettivamente con 0 e con 1 il minimo e il massimo di L, allora, per ogni $a \in L$

$$a \vee 0 = a = 0 \vee a \qquad \text{e} \qquad a \wedge 1 = a = 1 \wedge a.$$

Quindi 0 e 1 sono, rispettivamente l'elemento neutro per $\vee$ e per $\wedge$ (siccome le due operazioni sono associativi gli elementi neutri, se esistono, sono unici).

Viceversa è possibile partire da un insieme dotato di due operazioni che si comportano, da un punto di vista algebrico, "come" $\vee$ e $\wedge$, e definire a partire da esse una relazione d'ordine che rende R un reticolo nel senso iniziale della definizione.

Proposizione 3.9. *Sia $(R, \vee, \wedge)$ un insieme dotato di due operazioni binarie $\vee$ e $\wedge$ che siano commutative e che soddisfino le proprietà della Proposizione 3.8. Definiamo su R una relazione $\leq$ ponendo, per ogni $a, b \in R$, $a \leq b$ se $a \wedge b = a$. Allora $(R, \leq)$ è un reticolo. Se inoltre $\vee$ e $\wedge$ ammettono elementi neutri, questi sono, rispettivamente, il minimo ed il massimo di $(R, \leq)$.*

Dimostrazione. Verifichiamo innanzi tutto che $(R, \leq)$ è un insieme parzialmente ordinato. Sia $a \in R$. Per la proprietà di assorbimento $a = a \vee (a \wedge a)$ e quindi $a = a \wedge [a \vee (a \wedge a)] = a \wedge a$, da cui $a \leq a$, e dunque $\leq$ è riflessiva.
Siano $a, b \in R$ con $a \leq b$ e $b \leq a$. Allora, per la commutatività, $a = a \wedge b = b \wedge a = b$, e quindi $a = b$, e $\leq$ è antisimmetrica. Siano $a, b, c \in R$ con $a \leq b$ e $b \leq c$. Allora $a = a \wedge b$, $b = b \wedge c$, e per l'associatività, $a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$; dunque $a \leq c$ e $\leq$ è transitiva, e pertanto una relazione d'ordine su R.
Proviamo ora che, per ogni $a, b \in R$, $a \wedge b = \inf\{a, b\}$. Ora, $(a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b$ e dunque $a \wedge b \leq b$. Similmente (usando la commutatività) si trova che $a \wedge b \leq a$. Quindi $a \wedge b$ è un minorante di $\{a, b\}$. Mostriamo che è il massimo dei minoranti. Sia $d \in R$ con $d \leq a$ e $d \leq b$; allora $d = d \wedge a$ e $d = d \wedge b$, da cui $d \wedge (a \wedge b) = (d \wedge a) \wedge b = d \wedge b = d$, e quindi $d \leq a \wedge b$. Dunque $a \wedge b = \inf\{a, b\}$. In modo simile si prova che $a \vee b = \sup\{a, b\}$, ed in conclusione che $(R, \leq)$ è un reticolo. L'ultima parte della dimostrazione è lasciata per esercizio. ∎

Sia $(R, \vee, \wedge)$ un reticolo definito mediante le operazioni $\vee$ e $\wedge$; osserviamo che se $\leq$ è la relazione d'ordine associata come nella proposizione 3.9, allora per ogni $a, b \in R$ sono equivalenti: $a \wedge b = a$ e $a \vee b = b$.

Ricapitolando, ad ogni reticolo (come insieme parzialmente ordinato) può essere canonicamente associata una struttura algebrica di insieme dotato di due operazioni con certe proprietà (Proposizione 3.8), e viceversa ad ogni insieme dotato di due operazioni con tali proprietà si può canonicamente assegnare una relazione d'ordine che lo rende un reticolo (Proposizione 3.9). Si vede facilmente (lo si faccia per esercizio) che questi due processi sono l'uno l'inverso dell'altro. Ovvero, se si parte da un reticolo $(R, \leq)$, si definiscono le operazioni $x \vee y = \inf(\{x, y\})$, $x \wedge y = \sup(\{x, y\})$, e quindi a partire da queste si definisce una relazione d'ordine come nella Proposizione 3.9, si ottiene esattamennte la relazione d'ordine di partenza su R. A seconda delle esigenze, si può quindi vedere un reticolo come insieme parzialmente ordinato con cerrte proprietà, oppure come struttura algebrica dotata di due operazioni con le proprietà della Proposizione 3.8. Il più delle volte è conveniente lavorare sfruttando entrambe le strutture; così quando faremo rifferimento ad una relazione d'ordine in

un reticolo dato come insieme con due operazioni intenderemo ovviamente trattarsi della relazione deffinita canonicamente dalla Proposizione 3.9.

Esercizio 3.56. Sia $(A, \leq)$ un reticolo e $a \in A$ un elemento massimale. Si dimostri che a è il massimo di A.

Esercizio 3.57. Si provi che ogni reticolo finito è limitato.

Esercizio 3.58. Si provi che se L è un reticolo, allora per ogni $a, b, c \in L$ si ha

$$a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c).$$

Reticoli distributivi. Una proprietà che, se soddisfatta, rende un reticolo particolarmente interessante è la reciproca distributività tra le operazioni $\vee$ e $\wedge$. La prima osservazione che facciamo è che la distributività di una delle due rispetto all'altra implica la distributività della seconda rispetto alla prima.

Proposizione 3.10. *Sia L un reticolo. Allora le seguenti proprietà sono equivalenti.*

(i) per ogni $a, b, c \in L$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$;

(ii) per ogni $a, b, c \in L$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Dimostrazione. Proviamo che la proprietà (i) implica la (ii) (il viceversa è del tutto analogo). Siano $a, b, c \in L$. Per la proprietà di assorbimento si ha: $a = a \wedge (a \vee c)$ e $a = (a \wedge b) \vee a$. Assumendo che valga (i) (così come scritta: cioè per ogni terna di elementi di L); tenendo conto di commutatività e associatività si ricava:

$$\begin{aligned} a \wedge (b \vee c) &= (a \wedge (a \vee c)) \wedge (b \vee c) = a \wedge ((a \vee c) \wedge (b \vee c)) = \\ &= a \wedge ((a \wedge b) \vee c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = \\ &= (a \wedge b) \vee (a \wedge c) \end{aligned}$$

come si voleva. ■

Un reticolo che soddisfa una delle (e quindi entrambe le) condizioni della Proposizione precedente si dice *reticolo distributivo*. Ad esempio, se X è un insieme, il reticolo $(\mathcal{P}(X), \cap, \cup)$ è un reticolo distributivo. Chiaramente, anche, ogni insieme totalmente ordinato è un reticolo distributivo.
Ma, ad esempio, il reticolo dei sottospazi di uno spazio vettoriale V di dimensione almeno 2 non è distributivo. Infatti, siano $u, w \in V$ vettori linermente indipendenti (esistono perché V ha dimensione almeno 2) e consideriamo i tre sottospazi $U =< u >$, $W =< w >$ e $T =< u + w >$, generati, rispettivamente da u, w e $u + w$. Poiché questi tre vettori sono a due a due indipendenti, si ha $U \cap W = W \cap T = T \cap U = \{0\}$; e inoltre $U + W =< u, w >= U + T = T + W$. Quindi, nel reticolo $\mathcal{L}(V)$ dei sottospazio di V si ha: $U \wedge (W \vee T) = U \cap (W + T) = U$, mentre $(U \wedge W) \vee (U \wedge T) = (U \cap W) + (U \cap T) = \{0\}$. Dunque $\mathcal{L}(V)$ non è distributivo.

Esercizio 3.59. Sia $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Si dica se il reticolo $(\mathbb{N}^*, |)$ è distributivo.

Esercizio 3.60. Sia X un insieme infinito, e sia $\mathcal{P}_c(X)$ l'insieme dei sottoinsiemi *cofiniti* di X, cioè l'insieme dei sottoinsiemi Y di X tali che $X \setminus Y$ è finito. Si provi che $(\mathcal{P}_c(X), \subseteq)$ è un reticolo distributivo ma non limitato.

Esercizio 3.61. Sia $A = \mathbb{R}^{\mathbb{R}}$ l'insieme di tutte le applicazioni di $\mathbb{R}$ in $\mathbb{R}$, dotato della relazione d'ordine $\leq$ definita da, per ogni $f, g \in A$, $f \leq g$ se $f(a) \leq g(a)$ per ogni $a \in \mathbb{R}$. Si provi che $(A, \leq)$ è un reticolo, e si dica se è distributivo.

Reticoli complementati. Sia L un reticolo limitato, ed $a \in L$. L'elemento a si dice *complementato* se esiste $b \in L$ tale che $a \wedge b = 0$ e $a \vee b = 1$. In tal caso b si chiama un complemento di a. Chiaramente 1 e 0 sono complementati, e 0 è il solo complemento di 1 (e viceversa). Un reticolo limitato in cui ogni elemento è complementato si dice appunto *reticolo complementato*.

Proposizione 3.11. *Sia L un reticolo limitato e distributivo, e sia $a \in L$ complementato. Allora il complemento di a è unico (e si denota con a').*

Dimostrazione. Siano b e b' complementi di a in L. Poiché L è distributivo si ha

$$b' = b' \vee 0 = b' \vee (a \wedge b) = (b' \vee a) \wedge (b' \vee b) = 1 \wedge (b' \vee b) = b' \vee b$$

da cui segue $b \leq b'$. Allo stesso modo si prova che $b' \leq b$, e dunque $b' = b$. ∎

Ancora una volta, l'esempio principale di reticolo complementato è $\mathcal{P}(X)$, dove X è un insieme. In tal caso, per ogni $Y \in \mathcal{P}(X)$, il complemento di Y è $Y' = X \setminus Y$.

Osservazione: Anche il reticolo $\mathcal{L}(V)$ dei sottospazi di uno spazio vettoriale V (che assumiamo per semplicità, ma la cosa non è necessaria, di dimensione finita), è complementato ($\mathcal{L}(V)$ è limitato: il minimo è $\{0\}$ ed il massimo è V). Sia infatti U un sottospazio di V. Se $U = V$, allora $\{0\}$ è il suo complemento; dualmente, se $U = \{0\}$ allora V è il complemento. Sia quindi U un sottospazio proprio e non banale, e sia $\{u_1, \ldots, u_t\}$ una sua base. Per un fondamentale teorema di algebra lineare, è possibile estendere la base di U ad una base $\{u_1, \ldots, u_t, u_{t+1}, \ldots, u_n\}$ di V. Consideriamo ora il sottospazio $W\langle u_{t+1}, \ldots, u_n\rangle$. Allora $U \cap W = \{0\}$ e $U + W = V$; quindi W è un complemento di U in $\mathcal{L}(V)$ (ma non è l'unico).

In un reticolo limitato L nel quale ogni elemento ha un unico complemento, si denota, per ogni $a \in L$, con a' l'unico complemento di a. Il seguente Lemma è un'osservazione importante la cui dimostrazione è ovvia.

Lemma 3.12. *Sia L un reticolo limitato nel quale ogni elemento ha un unico complemento. Allora per ogni $a \in L$, $(a')' = a$.*

Esercizio 3.62. Sia $(A, \leq)$ un insieme totalmente ordinato e limitato. Si provi che A è complementato se e solo se $|A| \leq 2$.

Esercizio 3.63. Siano a, b e c elementi di un reticolo distributivo L. Si provi che se $a \vee b = a \vee c$ e $a \wedge b = a \wedge c$ allora $b = c$.

Esercizio 3.64. Sia $A = \{X \subseteq \mathbb{N} \mid |X| \text{ è finito }\}$, e sia $L = A \cup \{\mathbb{N}\}$. Si provi che $(L, \subseteq)$ è un reticolo limitato e distributivo, ma che non è complementato.

Esercizio 3.65. Sia $D(210)$ l'insieme dei numeri naturali diversi da 0, che sono divisori di 210. Si provi che $(D(210), |)$ è un reticolo booleano. Sia $D(420)$ l'insieme dei divisori positivi di 420 diversi da 0. Si provi che $(D(420), |)$ è un reticolo in cui non tutti gli elementi sono complementati; si provi tuttavia che se un suo elemento è complementato, allora il complemento è unico.

Algebre di Boole. Un reticolo limitato, distributivo e complementato si chiama *reticolo booleano* (da George Boole, $1815-1864$). In un reticolo booleano, per la Proposizione 3.11, ogni elemento a ha quindi uno ed un unico complemento a'. Vediamo subito una utile proprietà dei complementi in un reticolo booleano.

Proposizione 3.13. (Formule di De Morgan) *Sia L un reticolo booleano. Allora per ogni $a, b \in L$ si ha*

$$(a \vee b)' = a' \wedge b' \qquad e \qquad (a \wedge b)' = a' \vee b'.$$

Dimostrazione. Siano a, b elementi del reticolo booleano L. Allora $a \wedge b = b \wedge a$, ed applicando l'associatività e la distributività:

$$\begin{aligned}(a' \wedge b') \wedge (a \vee b) &= ((a' \wedge b') \wedge a) \vee ((a' \wedge b') \wedge b) = (b' \wedge (a' \wedge a)) \vee (a' \wedge (b' \wedge b)) = \\ &= (b' \wedge 0) \vee (a' \wedge 0) = 0 \vee 0 = 0,\end{aligned}$$

$$\begin{aligned}(a' \wedge b') \vee (a \vee b) &= ((a' \wedge b') \vee b) \vee a = ((a' \vee b) \wedge (b' \vee b)) \vee a = ((a' \vee b) \wedge 1) \vee a = \\ &= (a' \vee b) \vee a = b \vee (a' \vee a) = b \vee 1 = 1.\end{aligned}$$

Quindi $a' \wedge b'$ è l'unico complemento di $a \vee b$, e dunque $(a \vee b)' = a' \wedge b'$. Analogamente si prova che $(a \wedge b)' = a' \vee b'$. ∎

Un'algebra di Boole non è che un reticolo booleano, quando sia inteso come una struttura algebrica con operazioni. Ovvero

DEFINIZIONE. Un'**algebra di Boole** $(L, \vee, \wedge, \ ')$ è un insieme non vuoto L dotato di due operazioni binarie $\vee$ e $\wedge$ e di una biezione $\ ' : L \to L$, tali che

1) $\vee$ e $\wedge$ sono commutative e associative;
2) esistono $0, 1 \in L$ tali che: $\forall a \in L,\ 0 \vee a = a = 1 \wedge a$;
3) valgono le proprietà di assorbimento: $\forall x, y \in L, x \vee (x \wedge y) = x = x \wedge (x \vee y)$;
4) valgono le proprietà distributive di $\vee$ rispetto a $\wedge$ e di $\wedge$ rispetto a $\vee$;
5) per ogni $a \in L$ si ha: $a \wedge a' = 0$ e $a \vee a' = 1$.

Lasciamo per esercizio il compito di verificare in tutti i dettagli che le algebre di Boole così definite sono le strutture che si ottengono dai reticoli booleani mediante la definizione di $\vee$ e $\wedge$ rispettivamente come sup e inf e di a' com il complementare nel senso di un reticolo booleano; e che viceversa, applicando ad un'algebra di Boole la procedura della Proposizione 3.9 si ottiene un reticolo booleano.

Come c'era da aspettarsi, gli esempi principali di reticoli booleani sono i reticoli $\mathcal{P}(X)$, con X un insieme. In questo caso siamo però in grado di giustificare questa predilezione: ogni reticolo booleano finito è essenzialmente di questo tipo. Concludiamo infatti enunciando un risultato fondamentale (la dimostrazione non è terribilmente difficile, ma tuttavia la omettiamo). Per farlo in modo proprio dobbiamo introdurre il concetto - naturale - di isomorfismo di reticoli.
Siano $(L, \vee, \wedge)$ e $(R, \vee, \wedge)$ reticoli. Un'applicazione $\phi : L \to R$ si dice *omomorfismo* di reticoli se, per ogni $a, b \in L$, si ha

$$\phi(a \vee b) = \phi(a) \vee \phi(b) \quad \text{e} \quad \phi(a \wedge b) = \phi(a) \wedge \phi(b).$$

Se inoltre è una biezione, ϕ si dice un **isomorfismo** (di reticoli).

Possiamo ora enunciare il fondamentale:

Teorema 3.14. *Sia L un reticolo booleano finito, allora esiste un insieme finito X tale che L è isomorfo a $\mathcal{P}(X)$.*

Corollario 3.15. *Sia L un reticolo booleano finito. Allora $|L| = 2^n$ per qualche intero $n \geq 0$.*

Segnaliamo però che il teorema 3.14 non si può estendere al caso dei reticoli infiniti.

Esercizio 3.66. Siano $(A, \leq)$ e $(B, \lesssim)$ due reticoli. Si dica se l'ordine lessicografico (vedi esercizio 3.40) definisce in generale una struttura di reticolo su $A \times B$.

Esercizio 3.67. Sia B un reticolo booleano, e siano $a, b, c \in B$ tali che $a \wedge b = a \wedge c$. Si provi che $a' \vee b = a' \vee c$.

Esercizio 3.68. Sia $(L, \vee, \wedge)$ un reticolo booleano, e sia $a \in L$. Si provi che

$$a' = \max\{b \in L \mid a \wedge b = 0\}.$$

Esercizio 3.69. Siano L, M reticoli booleani, e sia $\phi : L \to M$ un omomorfismo di reticoli tale che $\phi(0_L) = 0_M$ e $\phi(1_L) = 1_M$. Sia $K = K(\phi) = \{a \in L \mid \phi(a) = o_M\}$. Si provi che, per ogni $x, y \in L$, $\phi(x) = \phi(y)$ se e soltanto se $x \wedge y'$, $x' \wedge y \in K$. Si deduca che ϕ è iniettivo se e solo se $K = \{0_L\}$.

Esercizio 3.70. Assumendo, con le stesse altre ipotesi e notazioni dell'esercizio precedente, che l'omomorfismo $\phi : L \to M$ sia suriettivo, si cerchi di definire un "reticolo quoziente" L/K e si cerchi di provare che è isomorfo a M.

Esercizio 3.71. Siano $(L, \vee, \wedge)$ un reticolo distributivo, e $a \in L$ un elemento fissato. Si provi che l'applicazione $\phi : L \to L$, definita da $\phi(x) = a \vee x$, per ogni $x \in L$, è un omomorfismo di reticoli. Si provi che è un isomorfismo se e soltanto se a è il minimo di L (ed in tal caso ϕ è l'applicazione identica).

Esercizio 3.72. Siano A e B reticoli limitati, e sia $\phi : A \to B$ un omomorfismo di reticoli tale che $\phi(0_A) = 0_B$ e $\phi(1_A) = 1_B$. Si provi che se $x, y \in A$ e y è un complemento di x allora $\phi(y)$ è un complemento di $\phi(x)$ in B. Si provi con un esempio che non vale il viceversa.

4

Primi passi nella teoria dei numeri

Wonder – is not precisely Knowing
And not precisely Knowing not–
A beautiful but bleak condition
He has not lived who has not felt–
[E. Dickinson, 1331]

4.1. Equazioni diofantee.

Con *equazione diofantea* (dal matematico alessandrino Diofanto) si intende genericamente un'equazione algebrica le cui eventuali soluzioni sono cercate nell'insieme numeri interi. Allo studio della risolubilità (e delle soluzioni) di particolari equazioni diofantee è riconducibile una considerevole parte della teoria dei numeri, così come sono molteplici gli strumenti sviluppati nel corso dei secoli per affrontare simili questioni.

Un primo semplice caso di equazione diofantea è collegato al Teorema 2.11

Proposizione 4.1. *Siano a, b ed n numeri interi (con a e b non entrambi nulli); allora l'equazione*

$$ax + by = n$$

ammette soluzioni in $\mathbb{Z}$ se e solo se $(a, b)|n$.

Dimostrazione. Siano a, b, n numeri interi, con a e b non entrambi nulli, e sia $d = (a, b)$.

Supponiamo che esistano $x, y \in \mathbb{Z}$, tali che $ax + by = n$. Poiché d divide sia a che b, a/d e b/d sono numeri interi, e quindi

$$\frac{n}{d} = \frac{a}{d} \cdot x + \frac{b}{d} \cdot y$$

è un numero intero. Dunque d divide n.

Viceversa, supponiamo che d divida n, e sia $c = n/d$ (che è un numero intero). Per il Teorema 2.11 esistono interi α e β tali che $\alpha a + \beta b = d$. Ponendo $u = c\alpha$ e $w = c\beta$, si ha $u, w \in \mathbb{Z}$ e

$$au + bw = c\alpha a + c\beta b = c(\alpha a + \beta b) = cd = n$$

e dunque la coppia ordinata (u, w) è una soluzione dell'equazione $ax + by = n$. ∎

In generale, se $a_1, a_2, \ldots, a_k$ sono interi non nulli, allora esiste il loro MCD positivo, che è denotato con $(a_1, a_2, \ldots, a_k)$, ed è definito nel modo ovvio. Si provi, ragionando per induzione su k che $(a_1, a_2, \ldots, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k)$, e dunque che esistono interi $\alpha_1, \alpha_2, \ldots \alpha_k$ tali che

$$(a_1, a_2, \ldots, a_k) = \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k a_k.$$

Si provi quindi che l'equazione $a_1x_1 + a_2x_2 + \cdots + a_kx_k = n$ ammette soluzioni intere se e solo se $(a_1, a_2, \ldots, a_k)$ divide n.

Nota. Sia a un intero. Con $a\mathbb{Z}$ si denota l'insieme di tutti i multipli interi di a, ovvero

$$a\mathbb{Z} = \{az \mid z \in \mathbb{Z}\}.$$

Sia $b \in \mathbb{N}$ un altro numero intero, e poniamo, per definizione

$$a\mathbb{Z} + b\mathbb{Z} = \{x + y \mid x \in a\mathbb{Z},\ y \in b\mathbb{Z}\} = \{az_1 + bz_2 \mid z_1, z_2 \in \mathbb{Z}\}.$$

Allora, la Proposizione 4.1 dice precisamente che, se a e b sono non entrambi nulli

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}.$$

Esercizio 4.1. Sia $n \in \mathbb{N}^*$ e siano a, b interi non nulli tali che $(a, b)|n$. Sia (x_0, y_0) una soluzione dell'equazione diofantea $ax + by = n$. Si provi che l'insieme delle soluzioni di tale equazione è

$$\left\{ \left(x_0 + t\frac{b}{(a,b)},\ y_0 - t\frac{a}{(a,b)} \right) \;\middle|\; t \in \mathbb{Z} \right\}.$$

SOLUZIONE. ∎

Complemento: il problema delle monete. La situazione si complica quando, dati a, b ed n interi positivi, con $(a, b) = 1$, si cercano soluzioni *non negative* dell'equazione diofantea $ax + by = n$. Ad esempio, l'equazione $4x + 7y = 17$ non ha soluzioni con $x \geq 0$ e $y \geq 0$. In generale, se a, b sono interi positivi e coprimi, l'equazione $ax + by = ab - a - b$ non ha soluzioni non negative (lo si dimostri per conto proprio); tuttavia

Lemma 4.2. *Siano $a, b, n \in \mathbb{N}^*$, con $(a, b) = 1$. L'equazione $ax + by = n$ ha soluzioni $(x, y) \in \mathbb{N} \times \mathbb{N}$ per ogni $n \geq ab - a - b + 1$.*

Dimostrazione. Sia $n \geq ab-a-b+1 = (a-1)(b-1)$. Possiamo ovviamente assumere $a < b$; per la Proposizione 4.1, $ax + by = n$ ammette soluzioni intere e, per l'esercizio 4.1, esistono soluzioni con $x \geq 0$. Sia quindi (x_0, y_0) una soluzione con $0 \leq x_0$ minimo possibile. Allora $(x_0 - b, y_0 + a)$ è ancora una soluzione, e quindi, per la scelta di (x_0, y_0), si ha $x_0 - b < 0$, ovvero $0 \leq x_0 < b$. Pertanto

$$(a - 1)(b - 1) \leq n = ax_0 + by_0 < ab + y_0b,$$

da cui $-2b + 1 < y_0b$. Poiché $b \geq 1$, segue $y_0 \geq -1$. Se fosse $y_0 = -1$, si avrebbe $ax_0 = n + b > ab - a = a(b - 1)$, e quindi $x_0 > b - 1$, cioè $x_0 \geq b$, il che non è. Dunque $y_0 \geq 0$, e (x_0, y_0) è la soluzione cercata. ∎

I problemi aumentano molto quando ci siano tre o più coefficienti ($a_1x_1 + \ldots + a_kx_k = n$ con $k \geq 3$); in generale il problema di stabilire per quali interi positivi n esistano soluzioni non negative è ancora ampiamente aperto (quelche ulteriore informazione su questo problema si trova QUI)

Un esempio molto famoso di equazione diofantea è il cosiddetto *ultimo teorema di Fermat*, che fu enunciato da P. Fermat nel 1637. Fermat scrisse di averne trovato una dimostrazione 'mirabile', ma di non avere lo spazio per riportarla (egli stava appunto annotando un testo di Diofanto). Dopo secoli di sforzi (inefficaci a dimostrare l'asserzione di Fermat, ma importantissimi per lo sviluppo di molte idee matematiche), l'ultimo teorema di Fermat è stato finalmente dimostrato da Andrew Wyles verso la fine del secolo scorso, utilizzando metodi assai profondi di geometria algebrica.

Teorema 4.3. (Fermat - Wyles). *Sia n un numero naturale. Se $n \geq 3$, non esistono soluzioni intere dell'equazione*

$$x^n + y^n = z^n$$

tali che $xyz \neq 0$.

Il caso in cui l'esponente n è uguale a 2, le cui soluzioni sono dette - per ovvie ragioni - *terne pitagoriche*, è elementare.

Proposizione 4.4. *Ogni soluzione intera non-banale (cioè $(x, y, z) \neq (0, 0, 0)$) dell'equazione*

$$x^2 + y^2 = z^2$$

si scrive nella forma $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$, dove $k \in \mathbb{N}^*$ e $(m, n) = 1$.

Dimostrazione. Si verifica facilmente che per ogni $k, n, m \in \mathbb{N}^*$, con $(n, m) = 1$, la terna $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$ è una soluzione dell'equazione data (ed è detta, per ovvî motivi, *terna pitagorica*).
Viceversa, siano $x, y, z \in \mathbb{N}^*$ tali che $x^2 + y^2 = z^2$, e sia $k = (x, y)$. Osserviamo che allora $k = (x, z) = (y, z)$. Siano $a, b, c \in \mathbb{N}^*$, con

$$x = ka, \quad y = kb, \quad z = kc \ .$$

Allora $(a, b) = (a, c) = (b, c) = 1$ e $a^2 + b^2 = c^2$. Dunque

$$c^2 = a^2 + b^2 = (a + b)^2 - 2ab \ .$$

a e b non sono entrambi pari. Se fossero entrambi dispari, allora $a + b$ e c sarebbero pari, e quindi $4|c^2$ e $4|(a+b)^2$, da cui segue la contraddizione $4|2ab$. Possiamo quindi assumere che a sia dispari e b sia pari (e quindi c è dispari). Sia $d = (c + a, c - a)$; allora $2|d$, ed inoltre $d|(c + a) + (c - a) = 2c$ (analogamente $d|2a$), e dunque, poiché a e c sono coprimi, $d = 2$. Siano ora $u, v \in \mathbb{N}^*$ tali che

$$c + a = 2u \qquad c - a = 2v \ .$$

Per quanto appena osservato $(u, v) = 1$. Inoltre

$$b^2 = c^2 - a^2 = (c + a)(c - a) = 4uv \ ;$$

e dunque u e v sono quadrati: sia $u = m^2$ e $v = n^2$. Allora,

- $b^2 = 4m^2n^2$, e quindi $b = 2mn$, e $y = 2kmn$.
- $2c = 2(u + v) = 2(m^2 + n^2)$, e quindi $c = m^2 + n^2$, e $z = k(m^2 + n^2)$.
- $2a = 2(u - v) = 2(m^2 - n^2)$, e quindi $a = m^2 - n^2$, e $x = k(m^2 - n^2)$. ∎

L'importanza delle equazione diofantee non risiede tanto nella loro applicabilità 'pratica' (anche all'interno della matematica stessa), quanto nel profluvio di idee - a volte molto sofisticate - a cui il loro studio ha dato e dà luogo (ad esempio la teoria degli anelli e degli ideali, che studieremo più avanti, è nata da un tentativo di attaccare la congettura di Fermat), e nella suggestione esercitata da problemi i cui enunciati sono comprensibili anche ad un livello assolutamente elementare.
Un esempio rilevante è la congettura di Catalan, risalente all'800 e dimostrata nel 2002 dal matematico romeno Preda Mihailescu.

Congettura di Catalan: *Siano* $2 \leq n, m \in \mathbb{N}$. *L'unica soluzione dell'equazione diofantea*

$$x^n = y^m - 1$$

si ha per $n = 2$, $m = 3$, ed è $x = 3$, $y = 2$.

(I soli numeri consecutivi che sono potenze non banali di numeri interi sono 8 e 9.)

4.2. Congruenze.

Le congruenze sono fondamentali relazioni d'equivalenza definite sull'insieme $\mathbb{Z}$ dei numeri interi (nella forma usata ancor oggi sono state introdotte da C.F. Gauss). Le ritroveremo in molte situazioni durante l'intero corso. Devono quindi diventare quanto prima un oggetto familiare.

Definizione. Sia $n \geq 1$ un fissato numero naturale. Due interi a, b si dicono *congrui modulo* n se n divide $a - b$. In tal caso si scrive

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

In altri termini, due interi a, b sono congrui modulo n se e solo se esiste $z \in \mathbb{Z}$ tale che $a - b = zn$; ovvero se e solo se $b = a + nz$ per qualche $z \in \mathbb{Z}$.

Verifichiamo subito che, per ogni fissato $n \geq 1$, la relazione di congruenza modulo n è una equivalenza su $\mathbb{Z}$.

- vale la *riflessività*. Infatti, per ogni $a \in \mathbb{Z}$ si ha $0n = a - a$ e quindi $a \equiv a \pmod{n}$.

- vale la *simmetria*. Infatti, siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$. Allora $a - b = nz$ per qualche $z \in \mathbb{Z}$. Da ciò segue subito $b - a = n(-z)$ e quindi $b \equiv a \pmod{n}$.

- vale la *transitività*. Infatti, siano $a, b, c \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$. Allora esistono $z, z' \in \mathbb{Z}$ tali che $a - b = nz$ e $b - c = nz'$. Da ciò segue

$$a - c = (a - b) + (b - c) = nz + nz' = n(z + z')$$

e quindi $a \equiv c \pmod{n}$.

Dato un $n \geq 1$, per ogni $a \in \mathbb{Z}$ la classe di equivalenza di a modulo la congruenza modulo n si chiama **classe di congruenza** di a modulo n. Quando il modulo n sia fissato e non vi siano possibilità di confusione, per comodità indicheremo la classe di congruenza di a semplicemente con $\overline{a}$ (o anche con $[a]$). Per quanto osservato sopra si ha quindi

$$\overline{a} = \{\ b \in \mathbb{Z} \mid a \equiv b \pmod{n}\ \} = \{\ b \in \mathbb{Z} \mid b = a + nz \ \text{ con } z \in \mathbb{Z}\ \}\ .$$

Un'altra maniera per denotare la classe di congruenza di a modulo n è quella di scrivere

$$a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\}.$$

Ad esempio, se $n = 5$,
$\overline{0} = \{\ b \in \mathbb{Z} \mid b = 5z \ \text{ con } z \in \mathbb{Z}\ \} = \{\ 5z \mid z \in \mathbb{Z}\ \} = \{0, 5, -5, 10, -10, 15, -15, \dots\}$,
$\overline{1} = 1 + 5\mathbb{Z} = \{\ 1 + 5z \mid z \in \mathbb{Z}\ \} = \{1, 6, -4, 11, -9, 16, -14, \dots\}$, e così via.

Dato $n \geq 1$, l'insieme di tutte la classi di congruenza modulo n (cioè l'insieme quoziente di $\mathbb{Z}$ modulo la congruenza modulo n) lo denoteremo con $\mathbb{Z}/n\mathbb{Z}$.

Osserviamo che la congruenza modulo 1 non è altro che la relazione banale su $\mathbb{Z}$; infatti per ogni $a, b \in \mathbb{Z}$, 1 divide $a-b$. Rispetto alla congruenza modulo 1 esiste quindi una sola classe di equivalenza che è $\mathbb{Z}$ stesso. Se invece consideriamo la congruenza modulo 2, osserviamo che due interi a, b sono congrui modulo 2 se e solo se sono entrambi pari o entrambi dispari. Dunque rispetto alla congruenza modulo 2 esistono due classi di equivalenza: una costituita da tutti i numeri pari e la seconda da tutti i numeri dispari (cioè $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$). Tutto ciò si può generalizzare; proveremo ora che, fissato $n \geq 1$, il numero di classi di congruenza modulo n è esattamente n.

Preliminarmente, facciamo la seguente semplice ma importante osservazione. Dato il modulo $n \geq 1$, possiamo dividere ogni intero a per n

$$a = nq + r \qquad \text{con} \quad 0 \leq r \leq n - 1;$$

pertanto n divide la differenza $a - r$, e dunque,

$$a \equiv r \pmod{n}.$$

Abbiamo cioè che, fissato il modulo $n \geq 1$, *un intero a è congruo modulo n al resto della divisione di a per n.* Enunciamo ora il risultato generale.

Teorema 4.5. *Sia $n \geq 1$ e, per ogni $a \in \mathbb{Z}$ indichiamo con $\overline{a}$ la classe di congruenza di a modulo n, e con $\mathbb{Z}/n\mathbb{Z}$ l'insieme quoziente. Allora*

$$\mathbb{Z}/n\mathbb{Z} = \{\ \overline{0},\ \overline{1},\ \overline{2}, \dots, \overline{n-1}\ \}.$$

Quindi $|\mathbb{Z}/n\mathbb{Z}| = n$. Inoltre per ogni $a \in \mathbb{Z}$, $\overline{a} = \overline{r}$ dove r è il resto della divisione di a per n.

Dimostrazione. Sia $a \in \mathbb{Z}$. Per quanto abbiamo osservato sopra,

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

dove r è il resto della divisione di a per n. Quindi $\overline{a} = \overline{r}$. Poiché $0 \leq r \leq n - 1$, concludiamo che ogni classe di congruenza modulo n coincide con una delle

$$\overline{0},\ \overline{1},\ \overline{2}, \dots, \overline{n-1}\ .$$

Rimane da provare che queste sono a due a due distinte. Siano quindi j, k tali che $0 \leq j \leq k \leq n - 1$ e supponiamo che, modulo n, $\overline{j} = \overline{k}$. Allora $k \equiv j \pmod{n}$ cioè n divide $k - j$. Ma $0 \leq k - j \leq n - 1$, dunque la sola possibilità che n divida $k - j$ è che $k = j$. Abbiamo così completato la dimostrazione. ∎

L'aspetto veramente importante delle congruenze è che con esse (o più precisamente con le classi di congruenza) è possibile eseguire le operazioni di somma e prodotto.

Teorema 4.6. *Sia $n \geq 1$, e siano $a, b, c, d \in \mathbb{Z}$ tali che*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases}$$

Allora $a + c \equiv b + d \pmod{n}$ *e* $ac \equiv bd \pmod{n}$.

Dimostrazione. Siano $a, b, c, d \in \mathbb{Z}$ con $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Allora, n divide sia $a - b$ che $c - d$. Quindi

$$n \text{ divide } (a - b) + (c - d) = (a + c) - (b + d),$$

e dunque

$$a + c \equiv b + d \pmod{n}.$$

Similmente, n divide

$$(a - b)c + b(c - d) = ac - bc + bc - bd = ac - bd,$$

e dunque $ac \equiv bd \pmod{n}$. ∎

Esempio. Come esempio di applicazione del risultato precedente dimostriamo il seguente *criterio di divisibilità per* 11: un intero positivo n è divisibile per 11 se e solo se la somma delle cifre decimali di posto pari di n è congrua modulo 11 alla somma delle cifre decimali di posto dispari. Ad esempio, 13570645 è divisibile per 11 (il più noto criterio di divisibilità per 3 sarà trattato negli esercizi). Iniziamo con il provare, per induzione su $k \geq 1$, che

$$10^k \equiv (-1)^k \pmod{11}.$$

La cosa è immediata per $k = 1$. Sia $k \geq 2$. Allora, per ipotesi induttiva $10^{k-1} \equiv (-1)^{k-1} \pmod{11}$., ed inoltre $10 \equiv (-1) \pmod{11}$. Applicando la parte relativa al prodotto del Teorema 4.6 si ottiene allora

$$10^k = 10^{k-1} \cdot 10 \equiv (-1)^{k-1}(-1) \pmod{11},$$

completando così l'induzione. A questo punto, sia

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

la rappresentazione decimale del numero n e supponiamo, per semplicità, che k sia pari. Allora, per quanto osservato sopra, e ancora per la parte additiva del Teorema 4.6 si ha

$$\begin{aligned} n_0 &= a_k 10^k + a_{k-2} 10^{k-2} + \cdots + a_2 10^2 + a_0 \equiv \\ &\equiv a_k (-1)^k + a_{k-2} (-1)^{k-2} + \ldots a_2 (-1)^2 + a_0 \equiv \\ &\equiv a_k + a_{k-2} + \ldots a_2 + a_0 \pmod{11}, \end{aligned}$$

ed inoltre

$$\begin{aligned} n_1 &= a_{k-1} 10^{k-1} + a_{k-3} 10^{k-3} + \cdots + a_3 10^3 + a_1 10 \equiv \\ &\equiv a_{k-1} (-1)^{k-1} + a_{k-3} (-1)^{k-3} + \ldots a_3 (-1)^3 + a_1 (-1) \equiv \\ &\equiv -(a_{k-1} + a_{k-3} + \ldots a_3 + a_1) \pmod{11}. \end{aligned}$$

Ora $11 | n$ se e solo se $n_0 + n_1 = n \equiv 0 \pmod{11}$, e questo, per quanto provato sopra, è a sua volta equivalente a

$$(a_k + a_{k-2} + \ldots a_2 + a_0) - (a_{k-1} + a_{k-3} + \ldots a_3 + a_1) \equiv 0 \pmod{11}$$

ovvero a

$$(a_k + a_{k-2} + \dots a_2 + a_0) \equiv (a_{k-1} + a_{k-3} + \dots a_3 + a_1) \pmod{11}$$

provando così il criterio annunciato.

Il Teorema 4.6 consente di valutare anche la congruenza di potenze. Infatti, siano $n \geq 1$ il modulo, $a \in \mathbb{Z}$ e $1 \leq k \in \mathbb{N}$. Allora, se $a \equiv r \pmod{n}$, si ha $a^k \equiv r^k \pmod{n}$. Ad esempio, poiché $2^5 \equiv 1 \pmod{31}$, si deduce che

$$2^{62} = 2^{5\cdot 12+2} = (2^5)^{12}2^2 \equiv 4 \pmod{31}.$$

Teorema 4.7. (Fermat). *Sia p un numero primo positivo, e sia $a \in \mathbb{Z}$ un intero non divisibile per p. Allora*

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

Dimostrazione. Sia p un numero primo positivo, e sia $S = \{1, 2, \dots, p-1\}$. Sia a un intero non divisibile per p, e per ogni $k \in S$ denotiamo con a_k il resto della divisione di $a \cdot k$ per p. Osserviamo che, poiché p è un primo e non divide né a né k, p non divide $a \cdot k$, e dunque $a_k \in S$; inoltre $a_k \equiv a \cdot k \pmod{p}$. Consideriamo l'applicazione $\Phi : S \longrightarrow S$ che ad ogni $k \in S$ associa a_k. Tale applicazione è iniettiva: infatti se, per $k, t \in S$, si ha $a_k = a_t$ allora $a \cdot k \equiv a \cdot t \pmod{p}$, ovvero p divide $a \cdot k - a \cdot t = a(k-t)$ e, siccome p non divide a, segue che p divide $k - t$ che, per la definizione di S, implica $k = t$. Dunque Φ è iniettiva; essendo S un insieme finito, ne segue che Φ è una biezione. Quindi

$$a_1 \cdot a_2 \cdot a_3 \dots a_{p-1} = 1 \cdot 2 \cdot 3 \dots (p-1) = (p-1)!$$

Pertanto

$$a^{p-1}(p-1)! = (a \cdot 1)(a \cdot 2) \dots (a \cdot (p-1)) \equiv a_1 \cdot a_2 \cdot a_3 \dots a_{p-1} \equiv (p-1)! \pmod{p},$$

cioè, p divide

$$a^{p-1}(p-1)! - (p-1)! = (a^{p-1} - 1)(p-1)!$$

Poiché p è primo, esso non divide $(p-1)!$ e dunque deve dividere $a^{p-1} - 1$, il che prova l'asserto del Teorema. ∎

Del Teorema di Fermat esistono diverse dimostrazioni; una seconda è basata sul seguente risultato di interesse indipendente.

Proposizione 4.8. *Sia p un primo positivo, e siano $a, b \in \mathbb{Z}$. Allora*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Dimostrazione. Sia p un primo positivo, e sia $1 \leq k \leq p-1$; allora p non divide $1 \cdot 2 \cdot 3 \cdot (k-1) \cdot k = k!$, e quindi

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

è un multiplo di p. Pertanto, applicando lo sviluppo del binomio di Newton (Teorema 2.9) ed il Teorema 4.6, si ha

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p \equiv a^p + b^p \pmod{p}$$

completando la dimostrazione. ∎

A questo punto si provi per esercizio che, fissato un primo positivo p, per ogni intero a si ha $a^p \equiv a \pmod{p}$ (si osservi che si può assumere $a \in \mathbb{N}$, quindi si ragioni per induzione, usando la Proposizione 4.8). Da ciò segue che $a(a^{p-1} - 1) \equiv 0 \pmod{p}$. Se p non divide a si conclude allora che p divide $a^{p-1} - 1$, provando così il Teorema di Fermat.

Equazioni alle congruenze. Vediamo ora alcuni aspetti elementari della teoria delle equazioni con congruenze. La lettera x va quindi intesa come una indeterminata, n un fissato numero naturale diverso da 0. Sia $f(x)$ un polinomio a coefficienti interi; siamo interessati a stabilire la risolubilità (ed a eventualmente determinare le "soluzioni") di congruenze del tipo

$$f(x) \equiv 0 \pmod{n} \tag{4.1}$$

Con "soluzione" di una tale congruenza si intende ovviamente un intero $a \in \mathbb{Z}$ tale che $f(a) \equiv 0 \pmod{n}$.
Cominciamo osservando un fatto quasi ovvio, ma basilare, la cui dimostrazione, che deriva in sostanza dal Teorema 4.6, lasciamo per esercizio.

Lemma 4.9. *Sia $c \in \mathbb{Z}$ una soluzione della congruenza (4.1). Allora ogni elemento della classe di congruenza di c modulo n è una soluzione della stessa congruenza.*

Dunque, se esistono, le soluzioni di (4.1) sono infinite, ma corrispondono tuttavia ad un numero finito di classi di congruenza. Quindi potremo riferirci al *numero di soluzioni* di una congruenza del tipo (4.1), intendendo il numero di classi di congruenza distinte i cui elementi sono soluzioni vere e proprie (in altri termini, il numero di interi $0 \leq a \leq n-1$ tali che $f(a) \equiv 0 \pmod{n}$).

Rimanendo ad un livello introduttivo, ci occuperemo qui di risolvere equazioni alle congruenze di primo grado, ovvero del tipo,

$$ax \equiv b \pmod{n} \tag{4.2}$$

con $a, b \in \mathbb{Z}$.

Notiamo ora che dire che $c \in \mathbb{Z}$ è una soluzione di (4.2), equivale a dire che esiste $d \in \mathbb{Z}$ tale che $ac + nd = b$. Quindi, risolvere una congruenza di primo grado come la (4.2) equivale a risolvere l'equazione diofantea $ax + ny = b$. La Proposizione 4.1 ci fornisce allora un'immediata risposta.

Proposizione 4.10. *Siano $a, b \in \mathbb{Z}$. Allora la congruenza $ax \equiv b \pmod{n}$ ammette soluzioni se e solo se (a, n) divide b.*

Ad esempio, la congruenza $15x \equiv 7 \pmod{6}$ non ha soluzioni.

Corollario 4.11. *Sia p un numero primo e $a, b \in \mathbb{Z}$. Allora la congruenza $ax \equiv b \pmod{p}$ ammette soluzioni se e solo se $p|b$ oppure $p \not| a$, e nel secondo caso la soluzione è una sola.*

Per risolvere congruenze di questo tipo (come, del resto, le corrispondenti equazioni diofantee) si può quindi adoperare l'algoritmo di Euclide. Supponiamo, ad esempio, di voler risolvere la congruenza

$$57x \equiv 21 \pmod{12}.$$

Si trova, $57 = 4 \cdot 12 + 9$, e $12 = 1 \cdot 9 + 3$; dunque, andando a ritroso,

$$(57, 12) = 3 = (-1) \cdot 57 + 5 \cdot 12.$$

Ora $21 = 3 \cdot 7$ e pertanto si ha

$$21 = 7 \cdot 3 = 7 \cdot ((-1) \cdot 57 + 5 \cdot 12) = 57 \cdot (-7) + 12 \cdot 35.$$

Dunque -7 è una soluzione cercata, ed ogni intero ad essa congruo modulo 12 è tale. Ad esempio, 5 è una soluzione. Le altre eventuali soluzioni (si intende, come abbiamo spiegato sopra, modulo 12) si possono determinare mediante una applicazione dell'esercizio 4.1: esse sono date da

$$5 + t\frac{12}{(57, 12)} = 5 + t \cdot 4$$

con $0 \leq t < 3$, ovvero sono 5, $5 + 4 = 9$ e $5 + 8 = 13$. In conclusione, le soluzioni della congruenza di partenza sono tutti e soli i numeri interi a tali che $a \equiv 1, 5, 9 \pmod{12}$.

Il teorema cinese dei resti. Questo metodo (così chiamato perché nella sostanza appare noto ad antichi matematici cinesi - come Sun Tze, vissuto nel 1^o secolo D.C.) consente di ridurre le equazioni alle congruenze al caso in cui il modulo sia una potenza di un numero primo. Iniziamo vedendone una formulazione "astratta".

Teorema 4.12. *Siano $m_1, m_2, \ldots, m_s$ elementi di $\mathbb{N}^*$ a due a due coprimi, e sia $n = m_1 m_2 \cdots m_s$. Allora l'applicazione*

$$\begin{array}{rcl} \dfrac{\mathbb{Z}}{n\mathbb{Z}} & \to & \dfrac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m_2\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{m_s\mathbb{Z}} \\ a + n\mathbb{Z} & \mapsto & (a + m_1\mathbb{Z},\ a + m_2\mathbb{Z},\ \ldots,\ a + m_s\mathbb{Z}) \end{array}$$

è una biezione.

Dimostrazione. Verifichiamo innanzi tutto che Γ è ben definita. Siano $a, b \in \mathbb{Z}$ tali che $a + n\mathbb{Z} = b + n\mathbb{Z}$. Allora $n|a - b$, e quindi per ogni $i = 1, 2, \ldots, s$, $m_i|a - b$, e di consguenza $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$, provando che secondo la definizione $\Gamma(a + n\mathbb{Z}) = \Gamma(b + n\mathbb{Z})$.

Proviamo che Γ è iniettiva. Siano $a + n\mathbb{Z}, b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, tali che $\Gamma(a + n\mathbb{Z}) = \Gamma(b + n\mathbb{Z})$. Allora, per ogni $i = 1, 2, \ldots, s$, $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$; e quindi m_i divide $a - b$. Poiché gli interi m_i sono a due a due coprimi, da ciò segue che $n = m_1 m_2 \cdots m_s$ divide $a - b$, e dunque che $a + n\mathbb{Z} = b + n\mathbb{Z}$, provando l'iniettività di Γ.

Per la suriettività, si osservi che

$$\left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = n = \left|\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right| \times \cdots \times \left|\frac{\mathbb{Z}}{m_s\mathbb{Z}}\right| = \left|\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_s\mathbb{Z}}\right|.$$

Dunque Γ è una applicazione iniettiva tra insiemi finiti dello stesso ordine, e pertanto è anche suriettiva. ∎

Quello che, nel contesto di cui ci occupiamo, risulta più utile è proprio la *suriettività* della funzione Γ. Vediamo il caso più semplice di applicazione.

Teorema 4.13. *(*Teorema Cinese dei resti*) Siano $m_1, m_2 \geq 1$ tali che $(m_1, m_2) = 1$. Allora per ogni coppia a, b di numeri interi il sistema di congruenze*

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

ammette soluzioni.

Dimostrazione. Per la suriettività dell'applicazione Γ del Teorema 4.12, esiste $x_0 \in \mathbb{Z}$ tale che $x_0 + m_1\mathbb{Z} = a + m_1\mathbb{Z}$ e $x_0 + m_2\mathbb{Z} = b + m_2\mathbb{Z}$. Tale x_0 è quindi una soluzione del sistema. ∎

Abbiamo enunciato il Teorema Cinese dei Resti nel caso di due moduli coprimi, ma è chiaro che il Teorema 4.12 consente di concludere similmente anche con un numero arbitrario di moduli, purché siano a due a due coprimi. Inoltre, la dimostrazione che abbiamo dato è elegante ma astratta. In particolare non sembra suggerire un metodo pratico per trovere le soluzioni. Tale metodo non è però difficile da trovare. Ecco come si fa.
Con le notazioni del Teorema 4.13, abbiamo che, per il Teorema 2.11, esistono $\alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha m_1 + \beta m_2$. Allora

$$a\beta m_2 = a - a\alpha m_1 \equiv a \pmod{m_1}$$

e

$$b\alpha m_1 = b - b\beta m_2 \equiv b \pmod{m_2}.$$

Quindi $c = a\beta m_2 + b\alpha m_1$ è una soluzione del sistema.

Si osserva poi che, in questo caso, la coprimità di m_1 e m_2 non è sempre necessaria per l'esistenza di soluzioni del sistema.

Proposizione 4.14. *Siano $1 \leq m_1, m_2 \in \mathbb{N}$. Il sistema di congruenze*

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

è risolubile se e solo se $(m_1, m_2) | a - b$.

Dimostrazione. Supponiamo che (m_1, m_2) divida $a - b$. Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che $a - b = \alpha m_1 + \beta m_2$. Quindi $c = a - \alpha m_1 = b + \beta m_2$ è una soluzione del sistema. Viceversa, se il sistema è risolubile e c è una sua soluzione, allora esistono $r, s \in \mathbb{Z}$ tali che $a + rm_1 = c = b + sm_2$. Da ciò si ricava $a - b = (-r)m_1 + sm_2$, e quindi (m_1, m_2) divide $a - b$. ∎

4.3. Funzioni moltiplicative

Questa sezione, per quanto ancora di natura piuttosto elementare, si avvia con maggior decisione verso la Teoria dei Numeri; di solito non viene trattata durante il corso, tuttavia la includiamo per quante/i si sentano già irrimediabilmente malate/i.

Definizione. Una funzione aritmetica (cioè con dominio un sottoinsieme di $\mathbb{Z}$)

$$f : \mathbb{N}^* \longrightarrow \mathbb{Z}$$

(dove $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$) si dice **moltiplicativa** se $f(1) \neq 0$ e, per ogni $n, m \in \mathbb{N}^*$

$$(n, m) = 1 \quad \Rightarrow \quad f(nm) = f(n)f(m). \tag{4.3}$$

Osservazioni. 1) Se f è una funzione moltiplicativa allora $f(1) = 1$. Infatti si ha $f(1) = f(1)f(1)$ e ciò implica (poiché $f(1) \neq 0$) $f(1) = 1$.

2) Sono moltiplicative la funzione costante $f(n) = 1_A$, e la funzione identica $f(n) = n$ (quest'ultima definita con dominio in $\mathbb{Z}$).

Le funzioni moltiplicative sono uno strumento fondamentale in teoria dei numeri. Vedremo tra poco esempi importanti anche per il corso di Algebra (segnatamente, la funzione di Möbius e la funzione di Eulero); incominciamo però con il provare un risultato utilissimo per costruire funzioni moltiplicative a partire da altre (e più semplici) funzioni moltiplicative. Nel seguito adottiamo la convenzione che, se $n \in \mathbb{N}^*$, allora con il simbolo

$$\sum_{d|n}$$

indichiamo la sommatoria su tutti gli indici d divisori interi e positivi di n.

Teorema 4.15. *Sia $f : \mathbb{N}^* \longrightarrow \mathbb{Z}$ una funzione moltiplicativa, e sia $F : \mathbb{N}^* \longrightarrow \mathbb{Z}$, definita ponendo, per ogni $n \in \mathbb{N}^*$*

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

Allora F è moltiplicativa.

Dimostrazione. Siano $n, m \in \mathbb{N}^*$ tali che $(n, m) = 1$. Osserviamo allora che i divisori di nm sono in corrispondenza biunivoca con le coppie (d_1, d_2), dove d_1 e d_2 sono, rispettivamente divisori di n e di m: ogni divisore d di nm si scrive infatti *in modo unico* come prodotto $d = d_1 d_2$ con dove $d_1|n$ e $d_2|m$. Quindi, tenendo presente che ogni divisore di n è coprimo con ogni divisore di m,

$$F(nm) = \sum_{d|nm} f(d) = \sum_{d_1|n\ d_2|m} f(d_1 d_2) = \sum_{d_1|n\ d_2|m} f(d_1) f(d_2) =$$

$$= \sum_{d_1|n} f(d_1) \left(\sum_{d_2|m} f(d_2) \right) = \sum_{d_1|n} f(d_1) \cdot \sum_{d_2|m} f(d_2) = F(n)F(m) \ .$$

Poiché $F(1) = f(1) \neq 0$, si conclude che F è moltiplicativa. ∎

Applichiamo subito questo risultato per individuare alcune prime interessanti funzioni moltiplicative. Sia $n \in \mathbb{N}^*$; si pone

$$\tau(n) = \text{ numero di divisori positivi di } n$$

$$\sigma(n) = \text{ somma dei divisori positivi di } n$$

Ovvero, per ogni $n \in \mathbb{N}^*$,

$$\tau(n) = \sum_{d|n} 1 \qquad \sigma(n) = \sum_{d|n} d;$$

e quindi, τ e σ sono moltiplicative per il Teorema 4.15.

La moltiplicatività di una funzione consente di determinarne i valori a partire da quelli che assume sulle potenze dei numeri primi. Infatti, se f è una funzione moltiplicativa, e $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ dove i p_i sono primi distinti e gli α_i interi maggiori o uguali a 1, allora chiaramente

$$f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_k}) \ .$$

Ad esempio, se p è un primo e $\alpha \in \mathbb{N}^*$, allora si osserva che

$$\tau(p^\alpha) = 1 + \alpha \quad \text{e} \quad \sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1} \ .$$

Possiamo dunque concludere con la seguente

Proposizione 4.16. *Sia $n \in \mathbb{N}^*$, e sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la fattorizzazione in primi di n; allora*

$$\tau(n) = \prod_{i=1}^{k} (1 + \alpha_i) \quad e \quad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \ .$$

Vediamo alcune applicazioni nell'ambito di quella che talvolta è chiamata "Matematica ricreativa".

1. Un problema classico. *Le celle di una prigione sono numerate da* 1 *a* 100 *e le loro porte sono controllate da un pulsante centrale. Quando viene premuto, il pulsante attiva alcune delle porte, aprendole se sono chiuse, chiudendole se aperte. Partendo dallo stato in cui tutte le porte sono chiuse il pulsante viene premuto* 100 *volte, attivando alla k-esima pressione tutte e sole le porte che sono numerate con un multiplo di k. Quali porte saranno aperte alla fine?*

Soluzione. La porta numerata con n (per $1 \leq n \leq 100$) si attiva un numero di volte pari al numero di divisori positivi di n, cioè $\tau(n)$; poiché la porta è inizialmente chiusa, sarà alla fine aperta se e solo se $\tau(n)$ è dispari. Ora, dalla Proposizione 4.16 segue il seguente

Corollario 4.17. *Un intero positivo ha un numero dispari di divisori positivi se e solo se è un quadrato intero.*

Infatti, se $n > 1$ è un intero positivo (il caso $n = 1$ è ovvio), dalla prima formula in 4.16, si ha che $\tau(n)$ è dispari se e solo se α_i è pari per ogni primo p_i che divide n, e questo è equivalente all'essere n un quadrato intero.

Dunque, l'insieme dei numeri $1 \leq n \leq 100$ che hanno un numero dispari di divisori positivi è $\{1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}$. Le porte numerate con uno di tali numeri saranno al termine aperte, tutte le altre chiuse. ∎

2. Numeri perfetti. Un numero $1 \leq n \in \mathbb{N}$ si dice *perfetto* se è uguale alla somma dei suoi divisori diversi da sé. In altri termini, n è perfetto se e solo se $2n = \sigma(n)$. I primi due numeri perfetii sono $6 = 1 + 2 + 3$ e $28 = 1 + 2 + 4 + 7 + 14$.

Teorema 4.18. *Un numero pari n è perfetto se e solo se $n = 2^{p-1}(2^p - 1)$, dove p e $2^p - 1$ sono primi.*

Dimostrazione. Supponiamo prima che $n = 2^{p-1}(2^p - 1)$, con p e $2^p - 1$ numeri primi. Allora, poiché σ è una funzione moltiplicativa,

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = 2n$$

e dunque n è perfetto.
Viceversa, sia n un numero perfetto pari. Allora $n = 2^{k-1}m$ con $k \geq 2$ e m dispari. Inoltre

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m) \ .$$

Quindi, $2^k - 1$ divide m. Sia $m = (2^k - 1)m'$; allora

$$\sigma(m) = \frac{2^k m}{2^k - 1} = 2^k m' \ .$$

Poichè m e m' sono distinti e dividono entrambi m si ha

$$\sigma(m) \geq m + m' = (2^k - 1)m' + m' = 2^k m' = \sigma(m)$$

da cui $m' = 1$. Quindi m è primo e $m = 2^p - 1$ per qualche primo p. ∎

Il Teorema precedente (parzialmente già noto ai matematici greci e provato definitivamente da Eulero) riconduce quindi la descrizione dei numeri perfetti pari alla determinazione dei primi di Mersenne. In particolare se il numero di primi di Mersenne è finito, allora i numeri perfetti pari sono finiti. Il problema dell'esistenza di numeri perfetti dispari è invece tuttora aperto, anche se la congettura prevalente è che non ve ne siano (una cosa nota è che se esiste un numero perfetto dispari, esso deve avere almeno sette divisori primi distinti).

La funzione di Möbius. La *funzione di Möbius* classica è l'applicazione

$$\mu : \mathbb{N} \longrightarrow \{0, 1, -1\} \subset \mathbb{Z},$$

definita nel modo seguente

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se esiste un primo } p \text{ tale che } p^2 | n \\ (-1)^s & \text{se } n = p_1 p_2 \dots p_s \text{ con i } p_i \text{ primi distinti} \end{cases}$$

La funzione di Möbius può essere generalizzata in modo da venire definita per insiemi parzialmente ordinati; quella che abbiamo esposto è la versione classica (in cui l'insieme parzialmente ordinato è $\mathbb{N}^*$ con la relazione di divisibilità).
Chiaramente μ è una funzione moltiplicativa. Inoltre si ha

Lemma 4.19.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & se \quad n = 1 \\ 0 & se \quad n > 1 \end{cases}$$

Dimostrazione. Poniamo $\Delta(n) = \sum_{d|n} \mu(d)$. Allora Δ è moltiplicativa per il Teorema 4.15, e $\Delta(1) = 1$. Sia p un numero primo, e $a \geq 1$; allora

$$\Delta(p^a) = \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^a) = \mu(1) + \mu(p) = 1 - 1 = 0 \ ;$$

poichè Δ è moltiplicativa, si conclude che, se $n > 1$, $\Delta(n) = 0$. ∎

L'importanza della funzione di Möbius risiede principalmente nella *Formula di Inversione di Möbius* che è il contenuto del prossimo Teorema.

Teorema 4.20. *Sia $f : \mathbb{N}^* \to A$ una funzione aritmetica, e per ogni $n \in \mathbb{N}$ definiamo $F(n) = \sum_{d|n} f(d)$. Allora, per ogni $n \in \mathbb{N}^*$*

$$f(n) = \sum_{d|n} \mu(n/d) F(d) = \sum_{d|n} \mu(d) F(n/d) \ .$$

Dimostrazione. Sia $n \in \mathbb{N}^*$. Allora

$$\sum_{d|n} \mu(d)F(n/d) = \sum_{du=n} \mu(d)F(u) = \sum_{du=n} \left(\mu(d) \sum_{t|u} f(t) \right) = \sum_{dt|n} \mu(d)f(t)$$

e, applicando quindi il Lemma 4.19

$$\sum_{d|n} \mu(d)F(n/d) = \sum_{t|n} f(t) \cdot \sum_{d|n/t} \mu(d) = f(n) \ .$$

L'altra uguaglianza nell'enunciato è ovvia. ∎

Come primo esempio di applicazione di questa formula, vediamo come si possa invertire il Teorema 4.15.

Teorema 4.21. *Sia f una funzione aritmetica tale che la funzione F definita da $F(n) = \sum_{d|n} f(d)$ è moltiplicativa. Allora f è moltiplicativa.*

Dimostrazione. Siano $n, m \in \mathbb{N}^*$ con $(n, m) = 1$. Tendendo conto che F e μ sono moltiplicative, ed applicando la formula di inversione di Möbius, si ha

$$f(mn) = \sum_{d|m,\, t|n} \mu\left(\frac{mn}{dt}\right) F(dt) = \sum_{d|m,\, t|n} F(d)\mu(m/d)F(t)\mu(n/t) =$$

$$= \sum_{d|m} F(d)\mu(m/d) \cdot \sum_{t|n} F(t)\mu(n/t) = f(m)f(n)$$

e dunque f è moltiplicativa. ∎

La funzione di Eulero. Dato $n \in \mathbb{N}^*$, si indica con $\phi(n)$ il numero di interi compresi tra 1 e n che sono coprimi con n. La funzione ϕ così definita si chiama *funzione di Eulero.* Riscrivendo la definizione

$$\phi(n) = |\{a \in \mathbb{N} \ ; \ 1 \le a \le n \ \text{ e } \ (a, n) = 1\}| \ .$$

Lemma 4.22. *Per ogni $n \in \mathbb{N}^*$*

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

Dimostrazione. Poniamo $A = \{1, 2, \ldots, n\}$ e $\Delta_n = \{1 \le d \le n \ ; \ d|n\}$. Definiamo una applicazione $c : A \to \Delta_n$ ponendo, per ogni $a \in A$, $c(a) = (a, n)$. Allora, chiaramente

$$n = \sum_{d|n} |c^{-1}(d)| \ .$$

D'altra parte, per ogni $d \in \Delta_n$,

$$|c^{-1}(d)| = |\{a \in A \ ; \ (a, n) = d\}| = |\{1 \le a \le n/d \ ; \ (a, n/d) = 1\}| = \phi(n/d) \ .$$

Dunque

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(d/n) = \sum_{d|n} |c^{-1}(d)| = n \ .$$

■

Teorema 4.23. *La funzione ϕ di Eulero è moltiplicativa. Inoltre, per ogni $n \in \mathbb{N}^*$ si ha*

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

Dimostrazione. La prima affermazione discende immediatamente dal Teorema 4.21, poichè la funzione $n = \sum_{d|n} \phi(d)$ è ovviamente moltiplicativa.
La seconda affermazione è un'altra facile applicazione della formula di inversione di Möbius all'uguaglianza del Lemma 4.22; infatti da queste si ha, per ogni $n \in \mathbb{N}^*$

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

■

La moltiplicatività della funzione di Eulero consente di determinarne i valori. Innanzi tutto supponiamo che $n = p^\alpha$ sia la potenza di un numero primo. Allora, per ogni $a \in \mathbb{N}^*$, $(a, n) = 1$ se e solo se $(a, p) = 1$; ora i multipli di p compresi tra 1 e p^α sono in numero di $p^{\alpha-1}$, e quindi

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) \ = p^\alpha \left(1 - \frac{1}{p}\right) \ .$$

Ne segue che se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ è la fattorizzazione in potenze di primi distinti di n, allora

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \ .$$

Osserviamo che, se p è un primo, il valore di ϕ in p^α si può anche ricavare immediatamente dall'uguaglianza del Teorema 4.23; infatti da questa si ha

$$\phi(p^\alpha) = p^\alpha \sum_{i=0}^{\alpha} \frac{\mu(p^i)}{p^i} = p^\alpha \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p}\right) = p^\alpha \left(1 - \frac{1}{p}\right) \ .$$

4.4. Esercizi.

• *Equazioni diofantee*

Esercizio 4.2. Si trovino le soluzioni intere dell'equazione $3xy + 7x = 15$.

Esercizio 4.3. Si risolva l'equazione diofantea

$$6x + 10y + 15z = 3.$$

Esercizio 4.4. Sia $2 \leq n \in \mathbb{N}$. Si provi che l'equazione $x^n = 2y^n$ non ha soluzioni nell'insieme dei numeri interi non nulli.

Esercizio 4.5. Si risolva l'equazione diofantea $x^2 - y^2 = 17$.

Esercizio 4.6. Provare che l'equazione $x^4 + y^4 = z^2$ non ha soluzioni intere non banali (cioè tali che $xyz \neq 0$). In particolare, quindi, il Teorema di Fermat è vero per l'esponente $n = 4$.

Esercizio 4.7. Si provi che l'equazione diofantea $x^2 - xy + y^2 = 0$ non ha soluzioni intere non banali.

Esercizio 4.8. Sia $n \in \mathbb{N}^*$. Si provi che l'equazione diofantea $x + 2xy + y = n$ ha soluzioni non banali (cioè $x \neq 0 \neq y$) se e solo se $2n + 1$ non è un numero primo.

Esercizio 4.9. Si dimostri che se $x, y, z \in \mathbb{N}$ sono tali che $x^2 + y^2 = z^2$, allora $xyz \equiv 0 \pmod{60}$.

• *Congruenze*

Esercizio 4.10. Si determini la classe di congruenza modulo 7 del numero

$$19 + 24(11 - 12^7) - 1984(3^9 + 5151) + 344.$$

Esercizio 4.11. Si dimostri che, per ogni numero naturale n si ha $10^n \equiv 1 \pmod{9}$.

Esercizio 4.12. Utilizzando l'esercizio precedente si provi che ogni numero intero è congruo modulo 9 alla somma delle cifre della sua rappresentazione decimale. Dedurre il noto criterio di divisibilità per 3: un numero intero è divisibile per 3 se e solo se la somma delle sue cifre decimali è divisibile per 3.

Esercizio 4.13. Siano $a, b \in \mathbb{Z}$, e $1 \leq n, m \in \mathbb{N}$. Si provi che

1) Se $a \equiv b \pmod{n}$, allora $(a, n) = (b, n)$.
2) Se $a \equiv b \pmod{n}$, e $a \equiv b \pmod{m}$, allora $a \equiv b \pmod{[n, m]}$.

Esercizio 4.14. Sia $4 < n \in \mathbb{N}$. Si provi che se n non è primo allora $(n - 1)! \equiv 0 \pmod{n}$.

Esercizio 4.15. Determinare l'ultima cifra decimale di 9^{139}, e quella di 7^{2001}.

Esercizio 4.16. Siano a, b, k, n interi tali che $n \geq 1$ e $ka \equiv kb \pmod{n}$. Si provi che

$$a \equiv b \pmod{\frac{n}{(n, k)}}.$$

Esercizio 4.17. Sia $a679b$ un numero di cinque cifre (in base 10) divisibile per 72. Determinare a e b.

Esercizio 4.18. Dire per quali $a \in \mathbb{Z}$ il numero

$$2^{1346} + 12 \cdot 48^{121} + 21003 \cdot 5^{30} + a$$

è divisibile per 7.

Esercizio 4.19. Si determinino le soluzioni della congruenza $39x \equiv 5 \pmod{14}$.

Esercizio 4.20. Sia a_o una soluzione della congruenza (4.2). Si provi che un sistema completo di rappresentanti modulo n di tutte le soluzioni è dato dagli interi

$$a_o + t\frac{n}{(a,n)} \qquad \text{con} \quad 0 \leq t \ < (a,n).$$

In particolare, il numero di soluzioni è (a,n).

Esercizio 4.21. Si determinino tutti i numeri primi (positivi) p tali che

$$5^{p-1} \equiv 5^{p+2} \ (mod\ p).$$

Esercizio 4.22. Si provi che, per ogni $a, b \in \mathbb{Z}$,

$$5^a \equiv 5^b \ (\mathrm{mod}\, 7) \quad \text{se e solo se} \quad a \equiv b \ (\mathrm{mod}\, 6).$$

Esercizio 4.23. Si risolvano le seguenti congruenze,

$$2x \equiv 5 \ (\mathrm{mod}\ 9), \qquad 15x \equiv 3 \ (\mathrm{mod}\ 6), \qquad x^2 \equiv 5 \ (\mathrm{mod}\ 6).$$

Esercizio 4.24. Si risolva il seguenti sistema di congruenze:

$$\begin{cases} x \equiv 3\,(\mathrm{mod}\ 6) \\ x \equiv 5\,(\mathrm{mod}\ 7) \\ x \equiv 7\,(\mathrm{mod}\ 11) \end{cases}$$

Esercizio 4.25. Siano $1 \leq m_1, m_2 \in \mathbb{N}$ interi coprimi, e sia $m = m_1 m_2$. Sia $f(x)$ un polinomio a coefficienti interi. Si provi che l'equazione $f(x) \equiv 0 \ (mod\, m)$ è risolubile in $\mathbb{Z}$ se e soltanto se $f(x) \equiv 0 \ (mod\, m_1)$ e $f(x) \equiv 0 \ (mod\, m_2)$ sono risolubili.

Esercizio 4.26. Si risolva il seguente sistema di congruenze:

$$\begin{cases} 4x - y \equiv 3\,(\mathrm{mod}\ 13) \\ \\ 7x + 2y \equiv 5\,(\mathrm{mod}\ 13) \end{cases}$$

Esercizio 4.27. Si risolva il seguente sistema di congruenze:

$$\begin{cases} 3x + 2y \equiv 1 \pmod 7 \\ 2x - y \equiv 2 \pmod 7 \end{cases}$$

Esercizio 4.28. Si determini il sottoinsieme S dei numeri naturali x tali che:

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 3 \pmod 5 \end{cases}$$

Esercizio 4.29. Si dica per quali interi x si ha $x^{35} \equiv 1\,(\mathrm{mod}\ 37)$.

Esercizio 4.30. Sia $A = \mathbb{Z} \times \mathbb{Z}$ e su A definiamo la relazione $\sim$ ponendo, per ogni $(a,b),(c,d) \in A$,

$$(a,b) \sim (c,d) \qquad \text{se} \qquad 2^{a^2+d^2} \equiv 2^{b^2+c^2} \ (\mathrm{mod}\, 5)$$

(a) Si provi che $\sim$ è una relazione d'equivalenza su A.

(b) Si provi che se $f : A \to \mathbb{Z}/4\mathbb{Z}$ è definita da $f((a,b)) = (a^2 - b^2) + 4\mathbb{Z}$ (per ogni $(a,b) \in A$), si ha $\sim = \sim_f$.

(c) Si determini $Im(f)$ [sugg.: se x è dispari allora $x^2 \equiv 1 \ (\mathrm{mod}\, 4)$].

(d) Si determini $|A/\sim|$.

Esercizio 4.31. Sia $2 \leq n \in \mathbb{N}$. Sull'insieme $A = \mathbb{Z}/n\mathbb{Z}$ si definisca la relazione $\sim$ ponendo, per $a, b \in A$,

$$a \sim b \text{ se } (a-b)(a+b-1) = n\mathbb{Z}.$$

(a) Si provi che $\sim$ è una relazione d'equivalenza su A.

(b) Assumendo che n sia un primo dispari, si determini il numero di classi di equivalenza di A modulo $\sim$.

Esercizio 4.32. Si determinino i numeri interi x tali che

$$2^{x^2} \equiv 2^x \pmod{15}.$$

Esercizio 4.33. Si provi che esistono infiniti numeri primi p tali che $p \equiv 3 \pmod 4$

Esercizio 4.34. Per $n \in \mathbb{N}$, sia $F_n = 2^{2^n} + 1$ l'n-esimo numero di Fermat. Si provi che ogni divisore primo di F_n è del tipo $2^{n+1}k + 1$. Si deduca che, per ogni $n \geq 1$, esistono infiniti numeri primi congrui a 1 modulo 2^n.

Esercizio 4.35. Determinare gli $x \in \mathbb{Z}$ tali che

$$4^{36001} \cdot x \equiv 6^{34568172} \pmod{19}.$$

Esercizio 4.36. Sia determinino le soluzioni intere della congruenza

$$x^{201} \equiv x^{21} \pmod{209}.$$

Esercizio 4.37. Si determinino i numeri interi x tali che

$$2^{x^2} \equiv 2^x \pmod{15}.$$

Esercizio 4.38. Sia p un numero primo positivo. Si determinino gli interi x soluzione della congruenza

$$x^{p-2} \equiv 1 \pmod{p}\ .$$

Esercizio 4.39. Sia ω la relazione su $\mathbb{Z}$ definita ponendo, per $a, b \in \mathbb{Z}$,

$$a \omega b \text{ se } a^3 \equiv b^3 \pmod 7.$$

a) Si provi che ω è una relazione di equivalenza su $\mathbb{Z}$.

b) Si determini l'insieme quoziente $\mathbb{Z}/\omega$.

Esercizio 4.40. Si determinino gli interi k per cui il numero

$$2^{1198765432104} + k$$

sia divisibile per 13.

Esercizio 4.41. Sia $n \geq 1$ un fissato intero. Dato $a \in \mathbb{Z}$, siano $h, k \in \mathbb{Z}$ tali che $ah + nk = (a, n)$.

1) Si provi che porre

$$f(a) = (a, n)h + n\mathbb{Z}$$

definisce un'applicazione $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

2) Si provi che se $f(a) = 1 + n\mathbb{Z}$ allora $(a, n) = 1$, e quindi si determini la retroimmagine $f^{-1}(1 + n\mathbb{Z})$.

• *Funzioni moltiplicative*

Esercizio 4.42. Si provi che per ogni $n \geq 1$

$$\sum_{d|n} \tau^3(d) = \left(\sum_{d|n} \tau(d) \right)^2$$

Esercizio 4.43. Siano f e g funzioni moltiplicative. Si provi che la funzione $f * h$ definita da

$$(f * h)(n) = \sum_{d|n} f(d) g(n/d)$$

è moltiplicativa. Si dimostri quindi che l'operazione $*$ (detta prodotto di convoluzione) è un'operazione associativa e commutativa nell'insieme delle funzioni moltiplicative.

Esercizio 4.44. Si provi che per ogni $n \geq 1$

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

Esercizio 4.45. Si dimostri la seguente proprietà della funzione di Möbius. Per ogni $n \in \mathbb{N}^*$,

$$\sum_{d^2|n} \mu(d) = |\mu(n).|$$

Esercizio 4.46. Si provi che, per ogni $n \geq 2$,

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p} \right)$$

dove p varia nell'insieme dei numeri primi che dividono n.

Esercizio 4.47. Si provi che, per ogni $n \geq 2$,

$$\sum_{i \leq n,\, (i,n)=1} i = \frac{1}{2} n \phi(n) \ .$$

Esercizio 4.48. Si provi che l'ultima cifra dello sviluppo decimale di un numero perfetto pari è 6 o 8.

Esercizio 4.49. Si provi che se n è un numero perfetto dispari, allora n è diviso da almeno 3 primi distinti.

Esercizio 4.50. Fissato un intero $k \geq 2$, si dice che $n \in \mathbb{N}$ è k-perfetto se $\sigma(n) = kn$. Si determinino tutti i numeri naturali n che sono 3-perfetti, con $1 \leq n \leq 150$.

Esercizio 4.51. Provare che se $\sigma(n)$ è dispari, allora $n = a^2$ oppure $n = 2a^2$, per qualche $a \in \mathbb{N}$.

Esercizio 4.52. (Olimpiadi Matematiche 1998) Sia $k \in \mathbb{N}^*$. Provare che esiste $n \in \mathbb{N}$ tale che

$$\frac{\tau(n^2)}{\tau(n)} = k$$

se e solo se k è dispari.

Esercizio 4.53. (La funzione λ di Liouville). Dato $n \in \mathbb{N}^*$, poniamo $\nu(1) = 0$, e per $n > 1$, $\nu(n)$ uguale al numero di fattori primi (non necessariamente distinti) di n (ad esempio, $\nu(24) = 4$). La funzione λ di Liouville è definita da

$$\lambda(n) = (-1)^{\nu(n)} .$$

Si provi che λ è moltiplicativa, e che per ogni $n \in \mathbb{N}^*$,

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ è un quadrato} \\ 0 & \text{altrimenti} \end{cases}$$

Esercizio 4.54. Si provi che la disuguaglianza $\phi(x) \geq x - \sqrt{x}$ ha come sole soluzioni intere i numeri p e p^2, con p primo.

4.5. Complementi: Il sistema crittografico RSA.

L'idea di *sistema crittografico* può essere resa mediante uno schema del tipo:

$$M \xrightarrow{f} C \xrightarrow{g} M$$

dove M è l'insieme dei messaggi, C quello dei messaggi cifrati, ed f e g sono applicazioni tali che

$$g \circ f = \iota_M$$

(quindi è necessario che f, che è detta la *chiave* di cifratura, sia iniettiva). f è la procedura di cifratura, e g quella di decifratura.

Nei sistemi crittografici classici (o romanzeschi, come ad esempio nel racconto *Lo scarabeo d'oro* di E. A. Poe), la chiave è *segreta*, ovvero consiste in una procedura per lo più complicata, che è nota solo a chi invia e a chi riceve il messaggio, mentre è difficilmente individuabile da altri. In questi casi, la procedura di decifratura è facilmente ricavabile qualora si conosca quella di cifratura, e in genere è della stessa natura (si può dire, senza voler essere precisi, che la procedura di decifratura è "simmetrica" a quella di cifratura).

Per fare un esempio abbastanza banale, la chiave di cifratura potrebbe consistere nel rimpiazzare ciascuna consonante del messaggio con la consonante immediatamente seguente nell'ordine alfabetico, e la lettera Z con la lettera B: così ad esempio, il messaggio SONO INFELICE viene cifrato, e inviato al destinatario–complice, come TOPO IPGEMIDE. È chiaro che in un sistema di questo tipo, la segretezza della chiave di cifratura è fondamentale, e che conoscendo questa si ricava subito la procedura di decifratura: chi sa cifrare sa anche decifrare, e viceversa[1].

Uno degli svantaggi di un sistema crittografico a chiave segreta è che coloro che lo utilizzano devono essersi preventivamente accordati sulla chiave, e quindi dev'essere già avvenuta tra loro una trasmissione d'informazioni non protetta (o protetta in altro modo). Al di là delle difficoltà logistiche, ciò pone oggi diversi problemi, dato che le necessità di trasmissione d'informazioni protette tra entità che per lo più non

[1] Sistemi basati su permutazioni delle lettere erano tipici tra i cabalisti, i quali infatti ritenevano la Bibbia come un enorme messaggio cifrato, e loro compito quello di cercare la chiave.

si conoscono, diventano sempre più diffuse. Si pensi, ad esempio, alla trasmissione per via elettronica di dati personali.
In tempi recenti, grazie anche allo sviluppo degli strumenti di calcolo, hanno quindi acquisito notevole importanza i sistemi crittografici a *chiave pubblica*. Questi sono basati su procedure di cifratura f per le quali sia estremamente complicato trovare la procedura inversa g (funzioni one–way). In tali sistemi, la procedura g è nota *solo al destinatario*, mentre la f può da questi essere *resa pubblica* (dato che a partire da essa è praticamente impossibile trovare la g). Ciò ha il vantaggio di non richiedere alcuno scambio preventivo di informazioni tra chi invia e chi riceve il messaggio

Il sistema RSA (dai nomi dei suoi inventori ufficiali: Rivest, Shamin e Adleman (1978)) è uno dei primi ed il più noto sistema crittografico a chiave pubblica. RSA è basato sul fatto che mentre è algoritmicamente semplice moltiplicare due numeri primi, il risalire ai fattori conoscendone il prodotto (cioè il problema di fattorizzare un numero intero) è estremamente difficile.

Ecco come funziona il sistema RSA.

Zerlina, destinataria dei messaggi, sceglie due numeri primi distinti p e q piuttosto grandi (per le attuali potenzialità di calcolo 100 cifre vanno già bene), e ne calcola il prodotto $n = pq$. Sceglie quindi un intero e che sia coprimo con $\phi = (p-1)(q-1)$ (questo non è difficile), e determina un altro intero d tale che

$$ed \equiv 1 \pmod{\phi}$$

(anche questo non è difficile per Zerlina, che conosce ϕ, e che può ad esempio usare l'algoritmo di Euclide).
Zerlina rende quindi pubblica la chiave di crittatura, che è la coppia

$$(n, e).$$

Masetto[2], intendendo inviarle quanto prima un messaggio che Don Giovanni non possa interpretare, procede nel modo seguente:

- codifica le singole unità del messaggio mediante un numero intero compreso tra 0 e $n-1$ (questo si fa con procedure standard), che denotiamo con x.

- calcola $f(x)$ come l'intero compreso tra 0 e $n-1$ tale che $f(x) \equiv x^e \pmod{n}$ (una procedura computazionalmente semplice).

- invia $f(x)$.

Per decifrare il messaggio, a Zerlina basta calcolare $f(x)^d$ modulo n. Questo restituisce il valore x, come assicura la seguente facile conseguenza del Teorema di Fermat (per applicarla al caso di sopra si osservi che $f(x)^d \equiv x^{ed} \pmod{n}$).

Proposizione 4.24. *Siano p, q primi distinti e sia $h \equiv 1 \pmod{(p-1)(q-1)}$. Allora per ogni $x \in \mathbb{Z}$,*

$$x^h \equiv x \pmod{pq}.$$

Dimostrazione. Poiché p e q sono primi distinti, sarà sufficente provare separatamente che $x^h \equiv x \pmod{p}$ e $x^h \equiv x \pmod{q}$. Naturalmente, i due casi sono del tutto analoghi, e quindi dimostriamo il primo. Per ipotesi, esiste un $t \in \mathbb{Z}$ tale che

$$h = 1 + t(p-1)(q-1).$$

[2]Ma anche chiunque altro Zerlina abbia informato della chiave

Se p divide x, allora $p \equiv 0 \pmod{p}$ e quindi banalmente $p^h \equiv 0 \pmod{p}$. Supponiamo quindi che p non divida x. Applicando allora il Teorema di Fermat 4.7 si ha

$$x^h = x^{t(p-1)(q-1)+1} = (x^{(p-1)})^{t(q-1)} x \equiv 1 \cdot x \pmod{p},$$

e questo completa la dimostrazione. ■

Il problema per Don Giovanni è che, pur conoscendo il modulo n, ed avendo intercettato il messaggio $f(x) = x^e$, egli non è capace di decifrarlo, dato che non conosce il valore d (si osservi che neppure Masetto lo sa). Infatti, la sola maniera per determinarlo, è conoscere i primi p e q. Don Giovanni dovrebbe quindi essere in grado di fattorizzare n, e questo, se p e q sono sufficintemente grandi, è impraticabile anche con i moderni strumenti di calcolo.

Esercizio 4.55. Con le notazioni di sopra, siano $p = 5$, $q = 11$ ed $e = 27$. Si decifri il messaggio $f(x) = 18$.

Seconda parte:
ANELLI E POLINOMI

5

Anelli

5.1. Prime proprietà.

Il termine **anello** è usato per indicare una particolare *struttura algebrica*, ovvero, parlando in modo generico, un insieme in cui sono fissate alcune operazioni che godono di specifiche proprietà. Nel caso degli anelli, le operazioni sono due ,ed il cui modello iniziale è costituito dall'insieme $\mathbb{Z}$ dei numeri interi con le operazioni usuali di somma e moltiplicazione. Infatti, il concetto di anello ha la sua origine dalla teoria di numeri, ed è sorto dall'idea di astrarre le proprietà fondamentali che caratterizzano (per quanto riguarda le due operazioni fondamentali) gli insiemi di numeri (interi, reali o complessi).

Definizione. Un **anello** è un insieme A dotato di due operazioni $+$, $\cdot$ (che saranno sempre chiamate "somma" e "prodotto"), che soddisfano le seguenti proprietà:

(S1) $a + (b + c) = (a + b) + c \quad \forall a, b, c, \in A$ (associatività della somma)

(S2) $a + b = b + a$ per ogni $a, b \in A$ (commutatività della somma)

(S3) esiste $0_A \in A$ tale che, per ogni $a \in A$, $a + 0_A = a$ (elemento neutro per la somma)

(S4) per ogni $a \in A$ esiste $a' \in A$ tale che $a + a' = 0_A$ (esistenza dell'opposto)

(P1) $a(bc) = (ab)c$ per ogni $a, b, c, \in A$ (associatività del prodotto)

(P2) esiste $1_A \in A$ tale che, per ogni $a \in A$, $a1_A = a = 1_A a$ (elemento neutro per il prodotto), ed inoltre $1_A \neq 0_A$

(D) Valgono le **proprietà distributive** del prodotto rispetto alla somma, ovvero, per ogni $a, b, c \in A$:

$$a(b + c) = ab + ac$$

$$(b + c)a = ba + ca \ .$$

Riferendoci alle definizioni di monoide e di gruppo (sezione 3.1), si riconosce che gli assiomi (S1) – (S4) esprimono la richiesta che $(A, +)$ sia un gruppo commutativo, e gli assiomi (P1) – (P2) quella che $(A, \cdot)$ sia un monoide.

Sono anelli, con le usuali operazioni di somma e prodotto, gli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e C. Altri esempi importanti (per i quali facciamo riferimento ai corsi di algebra

lineare) sono gli anelli di matrici quadrate $M_n(\mathbb{R})$, in questo caso le operazioni sono quella di somma (per componenti) e di prodotto righe $\times$ colonne, di matrici quadrate. Altri esempi ancora si trovano sparsi tra gli esercizi.

Dagli assiomi che definiscono la struttura di anello, seguono di fatto molte di quelle proprietà delle operazioni che utilizziamo familiarmente nel caso di anelli numerici. Le elenchiamo nelle seguenti proposizioni: la prima riguarda la somma, le non è altro che la legge di cancellazione, valida in qualsiasi gruppo; a seconda riguarda il prodotto (si osservi come sia fondamentale la proprietà distributiva)..

Proposizione 5.1. *Sia A un anello. Allora, per ogni $a, b, c \in A$,*

$$a + b = a + c \quad \Rightarrow \quad b = c.$$

In particolare, esiste un unico elemento neutro per l'addizione, che si denota sempre con 0_A e si chiama zero di A, e per ogni $a \in A$ esiste un unico elemento opposto di a, che si denota con $-a$.

Dimostrazione. Siano per ogni $a, b, c \in A$, tali che $a + b = a + c$, e sia $a' \in A$ tale che $a' + a = 0_A$. Allora

$$b = 0_A + b = (a' + a) + b = a' + (a + b) = a' + (a + c) = (a' + a) + c = 0_A + c = c.$$

Supponiamo ora che $0'_A$ sia un elemento neutro per la somma; allora

$$0'_A = 0'_A + 0_A = 0_A.$$

Infine se a' e a'' sono opposti dell'elemento a, allora $a + a' = 0_A = a + a''$, e quindi, per quanto provato sopra, $a' = a''$. ∎

Se a e b sono elementi dell'anello A, si adotta la seguente notazione: $a - b = a + (-b)$.

Proposizione 5.2. *Sia A un anello, e siano $a, b \in A$. Allora*

1. *esiste un unico elemento neutro per il prodotto.*
2. $a0_A = 0_A a = 0_A$.
3. $a(-b) = -(ab) = (-a)b$.
4. $(-a)(-b) = ab$.

Dimostrazione. 1) Siano 1_A e $1'_A$ elementi neutri per il prodotto; allora, analogamente a quanto visto per l'addizione

$$1'_A = 1'_A \cdot 1_A = 1_A.$$

2) Sia $c = a0_A$. Allora, applicando la proprietà distributiva:

$$c = a0_A = a(0_A + 0_A) = a0_A + a0_A = c + c$$

e quindi $c = c + c - c = c - c = 0_A$. Analogamente si dimostra che $0_A a = 0_A$.

3) Proviamo che $a(-b) = -(ab)$. Applicando la proprietà distributiva ed il punto 2):

$$a(-b) + ab = a(-b + b) = a0_A = 0_A$$

e quindi, $a(-b) = -(ab)$. Analogamente si dimostra che $(-a)b = -(ab)$.

4) Per il punto 3) si ha $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. ∎

Attenzione. In alcuni testi, la definizione di anello viene data senza richiedere l'esistenza dell'elemento neutro per la moltiplicazione (cioè senza includere l'assioma (P2)). Da questo punto di vista, un anello nel senso che invece adottiamo noi viene chiamato **anello con unità**. Ribadisco quindi che, secondo la definizione da noi adottata, un anello A ha **sempre** l'unità 1_A. Un anello R si dice *degenere* se $0_R = 1_R$; in tal caso (lo si dimostri), R è costituito dal solo elemento 0_R. Con il termine *anello* noi intenderemo **sempre** un *anello non degenere*, quindi tale che $0_R \neq 1_R$.

Esercizio 5.1. Sia A un insieme dotato di due operazioni $+$, $\cdot$ che soddisfano le condizioni (S1),(S3),(S4), (P1),(P2),(D). Provare che A è un anello.

Definizione. Un anello A si dice **commutativo** se il prodotto è commutativo, ovvero se, per ogni $a, b \in A$ si ha $ab = ba$.

Sono commutativi gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, mentre non sono commutativi gli anelli di matrici $M_n(\mathbb{R})$, con $n \geq 2$.

Potenze. Anche per un generico anello è possibile definire l'elevazione a potenza per un intero positivo, nella stessa maniera in cui si fa per gli interi. Sia quindi A un anello. Allora, per ogni $a \in A$ e per ogni $n \in \mathbb{N}$, la potenza n-esima a^n di a si definisce induttivamente nella maniera seguente:

$$a^0 = 1_A \qquad \text{e} \qquad a^{n+1} = a^n a.$$

In pratica, se $n \in \mathbb{N}$,

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{\text{n volte}}$$

Come nel caso degli interi è facile verificare le proprietà delle potenze.

Proposizione 5.3. *Sia A un anello, $a \in A$, e siano $n, m \in \mathbb{N}$. Allora*

(i) $a^{n+m} = a^n a^m$

(ii) $a^{nm} = (a^n)^m$

Dimostrazione. (i) Procediamo per induzione su $m \in \mathbb{N}$. Se $m = 0$, si ha $a^{n+0} = a^n = a^n \cdot 1_A = a^n a^0$.
Sia ora $m \geq 0$, e per ipotesi induttiva, sia $a^{n+m} = a^n a^m$. Allora,

$$\begin{aligned} a^{n+(m+1)} &= a^{(n+m)+1} = a^{n+m}a \qquad \text{(per definizione)} \\ &= (a^n a^m)a \qquad\qquad\quad \text{(per ipotesi induttiva)} \\ &= a^n(a^m a) = a^n a^{m+1} \qquad \text{(per definizione).} \end{aligned}$$

(ii) La dimostrazione di questo punto è lasciata per esercizio: si proceda ancora per induzione su m, utilizzando anche il punto (i). ∎

Osservazione. In generale, in un anello (non commutativo) A, non è detto che, dati $a, b \in A$ e $n \in \mathbb{N}$, valga $(ab)^n = a^n b^n$ (vedi l'esercizio 6.9). Tuttavia, non è difficile provare che se $ab = ba$ allora si ha, per ogni $n \in \mathbb{N}$, $(ab)^n = a^n b^n$.
In particolare, questa ulteriore proprietà delle potenze sussiste negli anelli commutativi, ai quali non è difficile estendere quindi il Teorema del binomio di Newton. Precisamente

Proposizione 5.4. *Sia A un anello commutativo, e siano $a, b \in A$. Allora per ogni $n \in \mathbb{N}$,*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \ .$$

Un'altra semplice identità, riguardante le potenze, che vale in qualsiasi anello, è quella riguardante le somme di serie geometriche: *sia A anello, $a \in A$, e $1 \leq n \in \mathbb{N}$; allora*

$$a^n - 1 = (a-1)(a^{n-1} + \cdots + a + 1).$$

Multipli interi. Si sarà osservato come, nell'enunciato della proposizione 5.4, sia stato dato un senso anche ad una scrittura del tipo na per $a \in A$, e $n \in \mathbb{N}$ (infatti i coefficienti binomiali che compaiono nella formula sono numeri interi). Questo va definito, ed è il corrispondente per la somma di quello che le potenze sono rispetto al prodotto (e si può fare con interi anche negativi).
Se A è un anello, $a \in A$ e $n \in \mathbb{N}$, si scrive

$$\begin{aligned} &0a = 0_A; \\ &na = a + a + \ \ldots \ + a \qquad \text{(n volte)}; \\ &(-n)a = n(-a) = -(na). \end{aligned}$$

L'elemento na si chiama il *multiplo n-esimo* di a.

In modo del tutto analogo a quanto visto per il prodotto, si prova facilmente che, per ogni $a, b \in A$ ed ogni $m, n \in \mathbb{Z}$,

$$(n+m)a = na + ma \qquad (nm)a = n(ma) \qquad m(a+b) = ma + mb.$$

Il concetto di *sottoanello* S di un anello A si presenta in modo naturale.

Definizione. Un sottoinsieme (non vuoto) S di un anello A si dice **sottoanello** di A se soddisfa alle seguenti condizioni

(1) $a - b \in S$, per ogni $a, b \in S$;

(2) $ab \in S$, per ogni $a, b \in S$ e $1_A \in S$.

Se S è un sottoanello di A, allora è chiaro che in S sono soddisfatte le proprietà distributive (in quanto casi particolari delle proprietà analoghe di A). Quindi S risulta, con le operazioni indotte da A, un anello esso stesso, con la stessa unità di A ($1_S = 1_A$). Similmente, un sottoanello di un anello commutativo è un anello commutativo.

Esempi. 1) Conviene subito mostrare che anche negli anelli che ci sono maggiormente usuali, si trovano numerosi sottoanelli. Ad esempio, consideriamo il seguente sottoinsieme di $\mathbb{R}$

$$\mathbb{Q}[\sqrt{2}] = \{\ a + b\sqrt{2} \mid a, b \in \mathbb{Q}\ \}\ ,$$

e verifichiamo che è un sottoanello dell'anello $\mathbb{R}$. Infatti, se $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ sono due elementi di $\mathbb{Q}[\sqrt{2}]$ (quindi $a, b, c, d \in \mathbb{Q}$), allora $x - y = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, e $xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$; infine $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Come vedremo più avanti, sottoanelli di questo tipo sono piuttosto importanti e si possono individuare a partire da un qualunque altro numero reale o complesso al posto di $\sqrt{2}$.

2) Introduciamo ora un anello che useremo spesso per illustrare diversi aspetti della teoria. Consideriamo l'insieme $\mathbb{R}^{\mathbb{R}}$ di tutte le applicazioni dall'insieme dei numeri reali in se stesso,

con le abituali operazioni di somma e moltiplicazione di funzioni reali. Quindi, se $f, g \in \mathbb{R}^{\mathbb{R}}$ allora $f+g$ e fg sono definite da

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (fg)(x) &= f(x)g(x)\end{aligned}$$

per ogni $x \in \mathbb{R}$ (attenzione: qui il prodotto non è la composizione di applicazioni). Si verifica facilmente che, con tali operazioni, $\mathbb{R}^{\mathbb{R}}$ è un anello commutativo, il cui zero ed uno sono, rispettivamente, le funzioni costanti c_0 e c_1 definite da, per ogni $x \in \mathbb{R}$, $c_0(x) = 0$, $c_1(x) = 1$. Se denotiamo con $\mathcal{C}(\mathbb{R})$ il sottoinsieme di $\mathbb{R}^{\mathbb{R}}$ costituito dalle applicazioni *continue*, allora noti teoremi di Analisi assicurano che $\mathcal{C}(\mathbb{R})$ è un sottoanello di $\mathbb{R}^{\mathbb{R}}$.

3) Anelli che godono di proprietà piuttosto singolari sono gli anelli delle parti. Sia X un insieme non vuoto. Allora l'insieme delle parti $\mathcal{P}(X)$ con le operazioni di differenza simmetrica Δ (come somma) e intersezione $\cap$ (come prodotto) è un anello (lo si provi per esercizio, usando le proprietà di queste operazioni descritte nella sezione 1.2), con $0_{\mathcal{P}(X)} = \emptyset$ e $1_{\mathcal{P}(X)} = X$.

Concludiamo questa sezione osservando che, se A è un anello, e U, V sono sottoinsiemi non vuoti di A, è possibile definire la "somma" di U e V, nel modo seguente

$$U + V = \{\ x + y \mid x \in U,\ y \in V\ \}.$$

$U + V$ è quindi ancora un sottoinsieme non vuoto di A.

Esercizio 5.2. Si completi la dimostrazione della proposizione 5.3, e quella dell'osservazione seguente.

Esercizio 5.3. Sia $S = \{\ (x, y) \mid x, y \in \mathbb{R}\ \}$. Su S definiamo addizione e moltiplicazione ponendo, per ogni $(a, b), (c, d) \in S$:

$$(a, b) + (c, d) = (a + c, b + d) \qquad (a, b)(c, d) = (ac, ad + bc)\ ,$$

Si provi che, con tali operazioni, S è un anello commutativo, determinando esplicitamente 0_S e 1_S.

Esercizio 5.4. Sia p un numero primo fissato e sia

$$\mathbb{Q}_p = \left\{ \frac{m}{p^i} \;\middle|\; m \in \mathbb{Z}\ , i \in \mathbb{N} \right\}.$$

Si provi che $\mathbb{Q}_p$ è un sottoanello dell'anello $\mathbb{Q}$ dei numeri razionali.

Esercizio 5.5. Sia R un anello. Si provi che $Z(R) = \{a \in R \mid ab = ba\ \forall b \in R\}$ è un sottoanello di R. ($Z(R)$ è detto il centro di R).

5.2. Tipi di anello.

Nella Proposizione 5.2 abbiamo provato alcune proprietà degli anelli, che per $\mathbb{Z}$ siamo abituati a considerare "naturali". Ora, $\mathbb{Z}$ soddisfa anche altre proprietà, quali il fatto che il prodotto di due elementi diversi da zero è diverso da zero. Il motivo per cui questa proprietà non compare nella proposizione 5.2, è che essa non discende dagli assiomi di anello; anzi, esistono anelli in cui essa non vale.

Un elemento a di un anello A si dice **divisore dello zero** se $a \neq 0_A$ ed esiste $b \neq 0_A$ tale che $ab = 0_A$.

Un primo esempio di di divisori dello zero si può trovare negli anelli di matrici; ad esempio, in $M_2(\mathbb{R})$:

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

Definizione. Un anello commutativo privo di divisori dello zero si dice un **Dominio d'integrità**.

Quindi, gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono domini d'integrità, mentre l'anello delle matrici $M_2(\mathbb{R})$ non lo è. Un esempio di anello commutativo che non è un dominio d'integrità è l'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ (vedi pagina seguente).

Proposizione 5.5. (Legge di cancellazione). *Sia A un dominio d'integrità. Allora, per ogni $a, b \in A, 0_A \neq c \in A$:*

$$ac = bc \qquad \Rightarrow \qquad a = b \ .$$

Dimostrazione. Siano $a, b \in A,\ 0_A \neq c \in A$ con $ac = bc$. Allora $0_A = ac - bc = (a-b)c$. Poichè A è privo di divisori dello zero e $c \neq 0_A$, deve essere $a - b = 0_A$, cioè $a = b$. ∎

Un elemento a di un anello A si dice un **invertibile** di A se esiste un elemento $b \in A$ tale che $ab = 1_A = ba$.

Come abbiamo dimostrato nel caso delle applicazioni, ed in generale per i monoidi (Proposizione 3.2) si prova immediatamente che un elemento invertibile a di un anello A ha un unico inverso.

Proposizione 5.6. *Sia A un anello, e sia a un elemento invertibile di A. Allora esiste un unico $b \in A$ tale che $ab = 1_A = ba$ (che si denota con $b = a^{-1}$).*

L'insieme di tutti gli elementi invertibili di un anello A lo denoteremo con $U(A)$. Chiaramente, $U(A) \neq \emptyset$ dato che $1_A \in U(A)$. Ad esempio, gli elementi invertibili dell'anello $\mathbb{Z}$ sono 1 e -1, quindi $U(\mathbb{Z}) = \{1, -1\}$; gli elementi invertibili dell'anello delle matrici $M_n(\mathbb{R})$ sono le matrici con determinante diverso da 0; gli elementi invertibili dell'anello $\mathbb{Q}$ sono tutti i numeri razionali diversi da 0, quindi $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$.

Esempio. L'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ non è un dominio d'integrità, e neppure il sottoanello delle funzioni continue $\mathcal{C}(\mathbb{R})$; ad esempio, se f, g sono le funzioni definite da

$$f(x) = \begin{cases} 0 & \text{se} \quad x \leq 0 \\ x & \text{se} \quad x \geq 0 \end{cases} \qquad g(x) = \begin{cases} x & \text{se} \quad x \leq 0 \\ 0 & \text{se} \quad x \geq 0 \end{cases}$$

allora f, g sono funzioni continue, diverse dalla funzione zero, il cui prodotto è la funzione zero (che, ricordo, è l'elemento 0 dell'anello $\mathbb{R}^{\mathbb{R}}$.
Ricordando poi che l'identità dell'anello $\mathbb{R}^{\mathbb{R}}$ è la costante 1, si ottiene immediatamente che gli elementi invertibili sono tutte e sole le funzioni $f \in \mathbb{R}^{\mathbb{R}}$ tali che $f(x) \neq 0$ per ogni $x \in \mathbb{R}$.

Esercizio 5.6. Si provi che nell'anello $\mathbb{R}^{\mathbb{R}}$ ogni elemento diverso da 0 è invertibile oppure un è un divisore dello zero. Si rifletta se la stessa affermazione vale per l'anello $\mathcal{C}(\mathbb{R})$ delle funzioni continue.

Definizione. Un anello commutativo A si dice un **campo** se ogni suo elemento non nullo è un invertibile.

Ad esempio sono campi gli anelli $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
Si vede facilmente che la famiglia dei campi è una sottofamiglia di quella dei domini d'integrità (propria: ad esempio $\mathbb{Z}$ è un dominio d'integrità ma non un campo).

Proposizione 5.7. *Ogni campo è un dominio d'integrità.*

Dimostrazione. Sia F un campo e $0_F \neq a \in F$. Supponiamo che $b \in F$ sia tale che $ab = 0_F$. Allora $b = 1_F b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0_F = 0_F$, quindi a non è un divisore dello zero. ∎

Esercizio 5.7. Provare che ogni dominio d'integrità finito è un campo.

Soluzione. Sia R un dominio d'integrità finito, e sia $0_R \neq a \in R$. Consideriamo l'applicazione $\lambda_a : R \to R$, definita da $\lambda_a(x) = ax$ per ogni $x \in R$. Siano ora $x, y \in R$ tali che $\lambda(x) = \lambda(y)$, allora $ax = ay$ che, per la legge di cancellazione, implica $x = y$. Dunque λ_a è iniettiva; poichè R è un insieme finito, λ_a è anche suriettiva. In particolare esiste $b \in R$ tale che $1_R = \lambda(b) = ab$. Essendo R commutativo, $ab = 1_R = ba$, quindi a è invertibile. Dunque R è un campo.

Prodotto diretto. Siano A e B anelli. Sull'insieme $A \times B$ si definiscono operazioni di somma e prodotto ponendo, per ogni $(a, b), (a', b') \in A \times B$,

$$(a, b) + (a', b') = (a + a', b + b') \qquad \text{e} \qquad (a, b) \cdot (a', b') = (aa', bb').$$

Si verifica facilmente (lo si svolga come esercizio) che, con le operazioni così definite, $A \times B$ è un anello, che si chiama anello *prodotto diretto* degli anelli A e B. Chiaramente, $0_{A\times B} = (0_A, 0_B)$ e $1_{A\times B} = (1_A, 1_B)$.
Inoltre, $A \times B$ è commutativo se e solo se A e B sono commutativi; mentre si provi per esercizio che $A \times B$ non è mai un dominio d'integrità.

Un elemento e di un anello A si dice **idempotente** se $e^2 = e$. In ogni anello A, 1_A e 0_A sono idempotenti. Se A è un dominio d'integrità questi sono i suoi soli elementi idempotenti, infatti se $e \in A$ è idempotene, allora $e^2 = e$ e quindi $e(e - 1) = 0$ (se A è un dominio d'integrità, ciò forza $e \in \{0_A, 1_A\}$). Per trovare elementi idempotenti non-banali, possiamo ad esempio considerare il prodotto diretto $\mathbb{Z} \times \mathbb{Z}$; in tale anello (che è commutaivo) gli elementi idempotenti sono $(0, 0), (1, 1), (0, 1)$ e $(1, 0)$.

Proposizione 5.8. *Sia R anello in cui ogni elemento è idempotente; allora $-1_R = 1_R$ e R è commutativo.*

Dimostrazione. Sia R come nelle ipotesi, e sia $a \in R$. Allora

$$-a = (-a)^2 = (-a)(-a) = a^2 = a;$$

in particolare $-1_R = 1_R$. Inoltre, per ogni $a, b \in R$ si ha

$$a + b = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + b + ab + ba$$

da cui segue $ab + ba = 0$ e dunque, per quanto visto sopra $ba = -(ab) = ab$. Quindi R è commutativo. ∎

Un anello in cui ogni elemento è idempotente si chiama **anello di Boole**. I casi fondamentali di anelli di Boole sono gli anelli delle parti, ovvero gli anelli del tipo $(\mathcal{P}(X), \Delta, \cap)$ (con X insieme non vuoto): infatti, per ogni elemento Y di un tale anello (quindi $Y \subseteq X$) si ha $Y^2 = Y \cap Y = Y$.
Diversamente dai domini d'integrità e dai campi, gli anelli di Boole non saranno oggetto di ulteriore approfondimento in questo corso; li abbiamo citati per la loro rilevanza nelle applicazioni alla logica e all'informatica.

Un elemento a di un anello R si dice **nilpotente** se esiste un intero $n \geq 1$ (che dipende in genere da a) tale che $a^n = 0_R$. Un esempio di elemento nilpotente non nullo lo troviamo, ad esempio, nell'anello di matrici $M = M_2(\mathbb{R})$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_M.$$

Esempi di elementi nilpotenti $\neq 0$ in anelli commutativi li incontreremo più avanti (vedi Esercizio 6.7). Per il momento, osserviamo i due fatti seguenti:

1) In un dominio di integrità R il solo elemento nilpotente è 0_R.

2) Sia a un elemento nilpotente dell'anello R. Allora $1 - a$ è un elemento invertibile. Infati, se per $a \in R$ e $1 \leq n \in \mathbb{N}$ si ha $a^n = 0$, allora

$$1 = 1 - a^n = (1 - a)(1 + a + a^2 + \cdots + a^{n-1}).$$

Esercizio 5.8. Sia S l'anello dell'esercizio 5.3. Si determinino gli elementi invertibili di S e si dica se S è un dominio di integrità.

Esercizio 5.9. Sia A un dominio d'integrità, e $0 \neq a \in A$. Si provi che se esistono interi $1 \leq m < n$, tali che $a^n = a^m$, allora esiste anche $1 \leq k \in \mathbb{N}$ tale che $a^k = 1_A$.

Esercizio 5.10. Si provi che l'anello $\mathbb{Q}[\sqrt{2}]$ è un campo.

Esercizio 5.11. Si determinino gli elementi invertibili e i divisori dello zero nell'anello $\mathbb{Z} \times \mathbb{Z}$.

Esercizio 5.12. Sia A un anello commutativo, e $a, b \in A$. Si provi che

(1) Se a è invertibile e b è nilpotente, allora $a + b$ è invertibile.

(2) Se a è divisore dello zero, b è nilpotente e $a + b \neq 0_A$, allora $a + b$ è divisore dello zero.

5.3. Ideali.

Gli ideali costituiscono il tipo più importante di sottoinsieme di un anello, e uno dei singoli argomenti più importanti di questo corso. Ecco la definizione.

Sia A un anello. Un **ideale** di A è un sottoinsieme non vuoto I di A che gode delle seguenti proprietà:

(i) $a - b \in I$ per ogni $a, b \in I$;

(ii) $ax \in I,\ xa \in I$ per ogni $a \in I,\ x \in A$.

Osserviamo subito che la proprietà (i), assieme alla richiesta che I non sia vuoto, comporta che *ogni ideale di A contiene* 0_A. Notiamo anche che ogni anello A ammette almeno due ideali; l'ideale *improprio* A e l'ideale *nullo o banale* $\{0_A\}$.

Esempio. Sia $\mathbb{R}^{\mathbb{R}}$ l'anello delle applicazioni dall'insieme dei numeri reali in se stesso definito nella sezione 5.1. Sia $a \in \mathbb{R}$ un numero reale fissato. Allora $Z_a = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\}$ è un ideale di $\mathbb{R}^{\mathbb{R}}$. Infattti

1) $Z_a \neq \emptyset$ (la finzione costante c_0 appartiene a Z_a);

2) se $f_1, f_2 \in Z_a$ allora $(f_1 - f_2)(a) = f_1(a) - f_2(a) = 0 - 0 = 0$ e dunque $f_1 - f_2 \in Z_a$,

3) se $f \in Z_a$ e $g \in \mathbb{R}^{\mathbb{R}}$, allora $fg(a) = f(a)g(a) = 0 \cdot g(a) = 0$ e dunque $fg \in Z_a$, similmente si ha $gf \in Z_a$.

Ideali di $\mathbb{Z}$. Un caso molo importante riguarda l'anello degli interi $\mathbb{Z}$, i cui ideali si descrivono facilmente. Infatti, sia fissato un intero $n \geq 0$; allora l'insieme di tutti i multipli interi di n, ovvero

$$n\mathbb{Z} = \{\ nz \mid z \in \mathbb{Z}\ \}$$

è un ideale di $\mathbb{Z}$ (un facile esercizio). La cosa rilevante è che vale il viceversa.

Teorema 5.9. *Gli ideali dell'anello $\mathbb{Z}$ dei numeri interi, sono tutti e soli i sottoinsiemi del tipo $n\mathbb{Z}$ con $n \geq 0$.*

Dimostrazione. Per quanto osservato prima, è sufficiente provare che ogni ideale di $\mathbb{Z}$ è del tipo $n\mathbb{Z}$. Sia dunque I un ideale di $\mathbb{Z}$. Se $I = \{0\}$ allora $I = 0\mathbb{Z}$.
Supponiamo quindi che $I \neq \{0\}$. Allora esiste $0 \neq a \in I$; poichè I è un ideale, si ha anche $-a \in I$. Ora, uno di questi due elementi di I è un numero positivo non nullo, quindi l'insieme

$$\mathcal{S} = \{\ m \in I \mid m > 0\ \}$$

è un sottoinsieme non vuoto dei numeri naturali. Sia $n = min(\mathcal{S})$. Proviamo che $I = n\mathbb{Z}$.
Poichè $n \in I$ ed I è un ideale, I contiene tutti i multipli di n, cioè $n\mathbb{Z} \subseteq I$. Viceversa, sia $b \in I$; poichè $n \neq 0$ possiamo dividere b per n; esistono cioè $q, r \in \mathbb{Z}$ tali che

$$b = nq + r \qquad \text{e} \qquad 0 \leq r < n\ .$$

Ora, $nq \in I$ per quanto osservato sopra, e quindi

$$r = b - nq \in I\ ;$$

se fosse $r > 0$ allora $r \in \mathcal{S}$ e quindi, per la scelta di $n = min(\mathcal{S})$, sarebbe $n \leq r$ che contraddice la proprietà del resto. Dunque $r = 0$, cioè $b = nq \in n\mathbb{Z}$. Quindi $I \subseteq n\mathbb{Z}$ e pertanto $I = n\mathbb{Z}$. ∎

Ideali Principali. Sia A un anello *commutativo* e sia $a \in A$; allora l'insieme

$$(a) = \{ax \mid x \in A\}$$

è un ideale di A.
Infatti, $0_A = a0_A \in (a)$ e quindi $(a) \neq \emptyset$; se $u = ax, w = ay \in (a)$ (con $x, y \in A$) allora $u - w = ax - ay = a(x - y) \in (a)$; infine se $u = ax \in (a)$ e $y \in A$, allora

$y(ax) = (ax)y = a(xy) \in (a)$ (osservate come la commutatività di A sia essenziale in questo punto).

Un ideale del tipo (a) di un anello commutativo A si dice **ideale principale** generato da (a), ed è il minimo ideale di A che contiene l'elemento a (nel senso generale che vedremo tra breve). In particolare, l'ideale nullo e quello improprio di qualsiasi anello commutativo A sono principali, infatti si ha $(0_a) = \{0_a\}$ e $(1_A) = A$.

Osserviamo quindi che tutti gli ideali dell'anello $\mathbb{Z}$ sono principali (infatti, per ogni $n \geq 0$, $n\mathbb{Z}$ è l'ideale principale generato da n, cioè $n\mathbb{Z} = (n)$). Non tutti gli anelli commutativi godono di questa proprietà.

Esempio. Nell'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ consideriamo il sottoinsieme

$$I = \{f \in \mathbb{R}^{\mathbb{R}} \mid \exists r_f \in \mathbb{R} \text{ tale che } f(x) = 0 \text{ per ogni } x \geq r_f\}.$$

I è un ideale di $\mathbb{R}^{\mathbb{R}}$ (lo si verifichi per esercizio), ma non è principale. Infatti, sia $f \in I$ e poniamo $r = r_f$, allora per ogni $g \in \mathbb{R}^{\mathbb{R}}$ si ha, per ogni $x \geq r$. $fg(x) = f(x)g(x) = 0 \cdot g(x) = 0$. Consideriamo ora $h \in \mathbb{R}^{\mathbb{R}}$ definita da, per ogni $x \in \mathbb{R}$,

$$h(x) = \begin{cases} 1 & \text{se} \quad x < r + 1 \\ 0 & \text{se} \quad x \geq r + 1. \end{cases}$$

Allora $h \in I$, ma, per quanto osservato prima, $h \notin (f)$. Questo prova che I non è un ideale principale.

Esercizio 5.13. Sia $a \in \mathbb{R}$; si provi che l'ideale $Z_a = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\}$ è un ideale principale di $\mathbb{R}^{\mathbb{R}}$.

Soluzione. Sia $g \in \mathbb{R}^{\mathbb{R}}$ definita da, per ogni $x \in \mathbb{R}$,

$$g(x) = \begin{cases} 1 & \text{se} \quad x \neq a \\ 0 & \text{se} \quad x = a. \end{cases}$$

Allora $Z_a = (g)$. Infatti $g \in Z_a$, e se $f \in Z_a$, si ha $f = gf$ (come si vede subito tenendo conto che $f(a) = 0$).

Per altre proprietà degli ideali di $\mathbb{R}^{\mathbb{R}}$ si veda l'esercizio 5.38.

Un dominio d'integrità in cui ogni ideale è principale si chiama **dominio a ideali principali** (abbreviato: P.I.D.). Dunque $\mathbb{Z}$ è un dominio ad ideali principali. Esempi di domini d'integrità che non sono a ideali principali li vedremo più avanti nel corso.

Il concetto di generazione di ideali si estende agli anelli non necessariamente commutativi, ed a più di un generatore.
Infatti, si vede immediatamente che, se I, J sono ideali di un anello A, allora anche $I \cap J$ è un ideale di A. Più in generale, se $\mathcal{F}$ è una famiglia di ideali di A, allora

$$\bigcap_{I \in \mathcal{F}} I$$

è un ideale di A.
Dunque, dato un sottoinsieme X di un anello A, l'intersezione di tutti gli ideali che contengono X è un ideale, che è detto *ideale generato da* X e che si denota con (X). Se $X = \{a_1, \ldots, a_n\}$ è un sottoinsieme finito di A, si scrive di solito $(X) = (a_1, \ldots, a_n)$ (trascurando, cioè, le graffe) e si dice che (X) è un ideale *finitamente generato*. Nel

caso in cui A è commutativo e $X = \{a\}$, l'ideale generato da X è proprio l'ideale principale generato da a. Sempre nel caso commutativo non è difficile descrivere gli elementi di un ideale finitamente generato:

Esercizio 5.14. Sia A un anello commutativo e $a, b \in A$. Sia (a, b) l'ideale di A generato da $\{a, b\}$; si provi che

$$(a, b) = \{ax + by \mid x, y \in A\}.$$

In generale, se A è un anello commutativo e $\mathfrak{a} = \{a_1, \ldots, a_n\} \subseteq A$, allora l'ideale generato da $\mathfrak{a}$ è $(a_1, \ldots, a_n) = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in A\}$.

Se A non è commutativo, la descrizione dell'ideale generato anche da un singolo elemento è più complicata. Infatti, se $a \in A$, allora l'ideale generato da a deve contenere tutti gli elementi del tipo $x_1ay_1 + \ldots x_nay_n$, al variare di $1 \leq n \in \mathbb{N}$, e $x_1, y_1, \ldots, x_n, y_n \in A$.

Somma di ideali. L'unione insiemistica di due ideali non è in genere un ideale (vedi esercizio 5.15). Per ottenere un ideale che contenga due ideali dati I e J di un anello A, occorre sommare i due ideali secondo la definizione alla fine della sezione 5.1.

Proposizione 5.10. *Siano I e J sono ideali di un anello A, Allora*

$$I + J = \{x + y \mid x \in I,\ y \in J\}$$

è un ideale di A, ed è il più piccolo ideale che contiene $I \cup J$.

Dimostrazione. Intanto $I+J$ non è vuoto dato che tali sono I e J. Siano ora $a, a' \in I$ e $b, b' \in J$, allora

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I + J,$$

dato che $a - a' \in I$ e $b - b' \in J$. Similmente se $a \in I$, $b \in J$ e $x \in A$, allora $ax, xa \in I$ e $bx, xb \in J$, e quindi

$$(a + b)x = ax + bx \in I + J \quad \text{e} \quad x(a + b) = xa + xb \in I + J.$$

Dunque $I + J$ è un ideale di A. Infine, per definizione di ideale, ogni ideale che contiene I e J deve necessariamente contenere $I + J$; quindi $I + J$ è il più piccolo ideale di A che contiene sia I che J. ∎

A questo punto, ci poniamo la questione di descrivere gli ideali degli anelli $\mathbb{Q}, \mathbb{R}$ e C. Tali anelli sono campi, e per i campi la descrizione degli ideali è molto semplice e assolutamente generale: come vediamo subito, gli ideali di un campo sono soltanto l'ideale nullo e quello improprio (in particolare, quindi, i campi sono domini a ideali principali). Inoltre, nell'ambito degli anelli commutativi, questa proprietà è caratteristica dei campi.

Lemma 5.11. *Sia I un ideale dell'anello R. Se I contiene un elemento invertibile allora $I = R$.*

Dimostrazione. Sia I un ideale di R e supponiamo che esista un elemento invertibile a di R contenuto in I. Sia $x \in R$; allora, per la proprietà (ii) degli ideali, $x = x1_R = x(a^{-1}a) = (xa^{-1})a \in I$. Dunque $R \subseteq I$, e quindi $R = I$. ∎

Teorema 5.12. *Sia R un anello commutativo. Allora R è un campo se e solo se i soli ideali di R sono $\{0_R\}$ e R.*

Dimostrazione. ($\Rightarrow$) Sia R un campo, e sia I ideale di R con $I \neq \{0_R\}$. Allora I contiene un elemento $a \neq 0_R$. Poichè R è un campo, a è invertibile e quindi, per il Lemma precedente, $I = R$.

($\Leftarrow$) Viceversa, supponiamo che R sia un anello commutativo i cui soli ideali sono $\{0_R\}$ e R. Sia $0_R \neq a \in R$ e consideriamo l'ideale principale $(a) = \{\ ax \mid x \in R\ \}$ generato da a. Poichè $(a) \neq \{0_R\}$, deve essere $(a) = R$. In particolare, $1_R \in (a)$, cioè esiste $b \in R$ tale che $1_R = ab$; poichè R è commutativo, concludiamo che a è invertibile. Ciò vale per qualunque $0_R \neq a \in R$ e dunque R è un campo. ∎

Questo Teorema non vale per anelli non commutativi; vedremo nella sezione 6.2 che l'anello di matrici $M_2(\mathbb{R})$, che è ben lontano dall'essere un campo, ha due soli ideali (quello banale e quello improprio).

Esercizio 5.15. Siano I e J ideali dell'anello A. Si provi che se $I \cup J$ è un ideale allora $I \subseteq J$ oppure $J \subseteq I$.

Esercizio 5.16. Siano n e m interi positivi. Si provi che $n\mathbb{Z} \subseteq m\mathbb{Z}$ se e solo se m divide n. Si deduca che

$$n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z} \quad \text{e} \quad n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}.$$

Esercizio 5.17. Sia u un elemento invertibile dell'anello commutativo R. Si provi che $(ua) = (a)$ per ogni $a \in R$.

Esercizio 5.18. Siano a, b elementi di una anello A (non necessariamente commutativo). Si provi che $(a, b) = (a) + (b)$.

Esercizio 5.19. Sia R un anello commutativo; si provi che l'insieme degli elementi nilpotenti di R è un ideale.

Esercizio 5.20. Siano R, S anelli. Si provi che i sottoinsiemi $\{(a, 0_S) \mid a \in R\}$ e $\{(0_R, x) \mid x \in S\}$ sono ideali di $R \times S$. Si determinino quindi tutti gli ideali dell'anello $\mathbb{R} \times \mathbb{R}$.

5.4. Omomorfismi e isomorfismi.

Definizione. 1) Siano R ed S anelli. Un **omomorfismo** (di anelli) di R in S è una applicazione $\phi : R \to S$ tale che:

(i) $\phi(a + b) = \phi(a) + \phi(b)$ per ogni $a, b \in R$;

(ii) $\phi(ab) = \phi(a)\phi(b)$ per ogni $a, b \in R$;

(iii) $\phi(1_R) = 1_S$.

2) Un **isomorfismo** tra anelli è un **omomorfismo biettivo**.

Due anelli R ed S si dicono **isomorfi** se esiste un isomorfismo da R in S. In tal caso scriveremo $R \simeq S$. Da un punto di vista algebrico astratto, due anelli isomorfi sono

considerai come "lo stesso" anello: l'isomorfismo trasferisce infatti tutte le proprietà algebriche (cioè derivanti dalle sole operazioni che lo definiscono come anello) da uno dei due anelli all'altro (come ad esempio è illustrato dal Lemma 5.13).
Un endomorfismo di un anello R è un omomorfismo da R in se stesso; mentre un isomorfismo di R in se stesso si dice **automorfismo** di R.

Esempi. 1) Il coniugio $\mathbb{C} \to \mathbb{C}$ che ad ogni $z = x + iy \in \mathbb{C}$ $(x, y \in \mathbb{R})$ associa $\overline{z} = x - iy$ è un automorfismo del campo $\mathbb{C}$.

3) Consideriamo le applicazioni $\phi_1, \phi_2 : \mathbb{R} \to M_2(\mathbb{R})$ definite da, per ogni $a \in \mathbb{R}$

$$\phi_1(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \qquad \phi_2(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

Per $i = 1, 2$, ed ogni $a, b \in \mathbb{R}$ si ha $\phi_i(a+b) = \phi_i(a) + \phi_i(b)$ e $\phi_i(ab) = \phi_i(a)\phi_i(b)$; ma ϕ_1 è un omomorfismo dato che $\phi_1(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{M_2(\mathbb{R})}$, mentre ϕ_2 non è un omomorfismo dato che $\phi_2(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_{M_2(\mathbb{R})}$.

Lemma 5.13. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

(i) $\phi(0_R) = 0_S$ e, per ogni $a \in R$, $\phi(-a) = -\phi(a)$; in generale, per ogni $a \in R$ ed ogni $z \in \mathbb{Z}$, si ha $\phi(za) = z\phi(a)$;

(ii) se $a \in R$ è invertibile, $\phi(a)$ è invertibile in S e $\phi(a)^{-1} = \phi(a^{-1})$.

(iii) $\phi(a^n) = (\phi(a))^n$, per ogni $a \in R$ e ogni $n \in \mathbb{N}$.

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo di anelli.
(i) Denotiamo con $e = \phi(0_R)$. Allora

$$e + e = \phi(0_R + 0_R) = \phi(0_R) = e = e + 0_S$$

e quindi $e = 0_S$. Sia ora $a \in R$; allora

$$\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0_R) = 0_S$$

e pertanto $\phi(-a) = -\phi(a)$.
L'ultima affermazione con una semplice induzione su $|z|$.
(ii) Sia a un elemento invertibile di R. Allora

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_R) = 1_S$$

e, similmente, $\phi(a^{-1})\phi(a) = 1_S$. Quindi $\phi(a)$ è un invertibile di S, e $\phi(a^{-1})$ è il suo inverso.
(iii) Induzione su n. ∎

Gli omomorfismi (e gli isomorfismi) di anelli si comportano bene rispetto alla composizione di applicazioni, come suggerisce la seguente proposizione.

Proposizione 5.14. *Siano $\phi : R \to S$ e $\psi : S \to T$ omomorfismi di anelli. Allora*

1) $\psi \circ \phi : R \longrightarrow T$ è un omomorfismo di anelli.

2) Se ϕ è un isomorfismo, allora anche ϕ^{-1} è un isomorfismo.

Dimostrazione. 1) Per esercizio.
2) Se ϕ è un isomorfismo, allora è per definizione una applicazione biettiva, e quindi esiste l'applicazione inversa $\phi^{-1} : S \longrightarrow R$, che è pure biettiva. Mostramo che ϕ^{-1} è un isomorfismo.
Siano $x, y \in S$. Allora, siccome ϕ è un omomorfismo

$$\phi(\phi^{-1}(x) + \phi^{-1}(y)) = \phi(\phi^{-1}(x)) + \phi(\phi^{-1}(y)) = x + y = \phi(\phi^{-1}(x + y)).$$

Poichè ϕ è iniettiva, si ha $\phi^{-1}(x + y) = \phi^{-1}(x) + \phi^{-1}(y)$. In modo analogo si prova che $\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$. Infine,

$$\phi^{-1}(1_S) = \phi^{-1}(\phi(1_R)) = 1_R.$$

Dunque ϕ^{-1} è un isomorfismo. ∎

Sia $\phi : R \to S$ un omomorfismo di anelli. Com'è usuale, denotiamo con $Im(\phi)$ l'immagine dell'applicazione ϕ, cioè

$$Im(\phi) = \phi(R) = \{\phi(x) \mid x \in R\}.$$

La dimostrazione della seguente proposizione è molto facile, e si lascia per esercizio.

Proposizione 5.15. *Sia $\phi : R \to S$ un omomorfismo di anelli; allora $Im(\phi)$ è un sottoanello di S.*

Definizione. Sia $\phi : R \to S$ un omomorfismo di anelli. Il **nucleo** $Ker(\phi)$ di ϕ è l'insieme degli elementi di R la cui immagine tramite ϕ è 0_S; cioè

$$Ker(\phi) = \{x \in R \mid \phi(x) = 0_S\}.$$

Esempio. Sia a un fissato numero reale. Allora la *sostiuzione* $\sigma_a : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$, definita da, per ogni $f \in \mathbb{R}^{\mathbb{R}}$, $\sigma_a(f) = f(a)$, è un omomorfismo di anelli. Infatti, per ogni $f, g \in \mathbb{R}^{\mathbb{R}}$,

$$\sigma_a(f + g) = (f + g)(a) = f(a) + g(a) = \sigma_a(f) + \sigma_a(g)$$

$$\sigma_a(fg) = (fg)(a) = f(a)g(a) = \sigma_a(f)\sigma_a(g),$$

inoltre, se $\underline{1}$ è la funzione costante 1 (che è l'identità di $\mathbb{R}^{\mathbb{R}}$), $\sigma_a(\underline{1}) = \underline{1}(a) = 1$. Il nucleo di un tale omomorfismo è

$$Ker(\sigma_a) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\},$$

che, per quano visto in un esempio precedente, è un ideale di $\mathbb{R}^{\mathbb{R}}$.

Il fatto che, in queso esempio, il nucleo sia un ideale di $\mathbb{R}^{\mathbb{R}}$ (ovvero del dominio dell'omomorfismo) non è accidentale. Infatti vale il seguente fondamentale risultato.

Teorema 5.16. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

(1) *$Ker(\phi)$ è un ideale di R.*

(2) *ϕ è iniettivo se e solo se $Ker(\phi) = \{0_R\}$.*

Dimostrazione. (1) Poichè $\phi(0_R) = 0_S$, $Ker(\phi)$ non è vuoto. Siano $a, b \in Ker(\phi)$ e $r \in R$; allora

$$\phi(a - b) = \phi(a) - \phi(b) = 0_S - 0_S = 0_S$$

quindi $a - b \in Ker(\phi)$; inoltre

$$\phi(ar) = \phi(a)\phi(r) = 0_S\phi(r) = 0_S \qquad \text{e} \qquad \phi(ra) = \phi(r)\phi(a) = \phi(r)0_S = 0_S$$

quindi $ar, ra \in Ker(\phi)$. Dunque $Ker(\phi)$ è un ideale di R.

(2) Poichè $\phi(0_R) = 0_S$, $Ker(\phi) = \{0_R\}$ se ϕ è iniettivo. Viceversa, sia $Ker(\phi) = \{0_R\}$ e siano $a, b \in R$ tali che $\phi(a) = \phi(b)$; allora $\phi(a - b) = \phi(a) - \phi(b) = 0_S$, quindi $a - b \in Ker(\phi)$ che implica $a - b = 0_R$, cioè $a = b$. Dunque ϕ è iniettivo. ■

L'iniettività di un certo omomorfismo è una proprietà molto importante (e ricercata): infatti, se $\phi : R \to S$ è un omomorfismo iniettivo di anelli, allora, restringendo il codominio S all'immagine di ϕ (che è ancora un anello), si ricava un *isomorfismo* da R in $Im(\phi)$ (quindi, se ϕ è iniettivo, $R \simeq Im(\phi)$). In particolare abbiamo,

Corollario 5.17. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora, ϕ è un isomorfismo se e soltanto se $Im(\phi) = S$ e $\ker(\phi) = \{0_R\}$.*

Esercizio 5.21. Sia $\phi : R \to S$ un omomorfismo di anelli. Provare che se R è un campo allora ϕ è iniettivo.

Soluzione. $Ker(\phi)$ è un ideale di R. Se R è un campo, per il Teorema 5.12, $Ker(\phi) = R$ oppure $Ker(\phi) = \{0_R\}$. Ma $Ker(\phi) \neq R$ perchè $\phi(1_R) = 1_S \neq 0_S$; quindi $Ker(\phi) = \{0_R\}$ e dunque ϕ è iniettivo per il Teorema precedente.

Esercizio 5.22. Sia $\phi : R \to S$ un omomorfismo di anelli.

1) Sia T un ideale di S. Si provi che $\phi^{-1}(T)$ è un ideale di R.
2) Sia I un ideale di R. Si provi che, se ϕ è suriettivo allora $\phi(I)$ è un ideale di S.
3) Sia $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita da $\phi(z) = (z, z)$, per ogni $z \in \mathbb{Z}$. Si provi che ϕ è un omomorfismo di anelli; si dimostri che se I è un ideale di $\mathbb{Z}$ tale che $\phi(I)$ è un ideale di $\mathbb{Z} \times \mathbb{Z}$, allora $I = \{0\}$.

Esercizio 5.23. Siano ϕ e ψ due endomorfismi di uno stesso anello A (cioè omomorfismi di A in se stesso). Si provi che $B = \{a \in A \mid \phi(a) = \psi(a)\}$ è un sottoanello di A, e che se A è un campo allora anche B è un campo.

Esercizio 5.24. Sull'insieme $\mathbb{Q}$ dei numeri razionali si considerino l'usuale addizione $+$ e la moltiplicazione $*$ definita ponendo, per ogni $x, y \in \mathbb{Q}$, $x * y = 3/4\ xy$. Si dimostri che $(\mathbb{Q}, +, *)$ è un campo isomorfo al campo dei numeri razionali $(\mathbb{Q}, +, \cdot)$.

Esercizio 5.25. Determinare tutti gli automorfismi dell'anello $\mathbb{Q}[\sqrt{2}]$ definito nella sezione 5.1.

5.5. Esercizi.

Esercizio 5.26. (Interi di Gauss). (a) Si provi che

$$\mathbb{Z}[i] = \{\mathrm{a} + i\mathrm{b} \mid \mathrm{a}, \mathrm{b} \in \mathbb{Z}\}$$

è un sottoanello di $\mathbb{C}$.

$\mathbb{Z}[i]$ è detto *l'anello degli interi di Gauss*. Si consideri la restrizione della norma complessa a $\mathbb{Z}[i]$ (cioè l'applicazione $N : \mathbb{Z}[i] \to \mathbb{Z}$ definita da $N(\mathrm{a} + i\mathrm{b}) = \mathrm{a}^2 + \mathrm{b}^2$, per ogni $\mathrm{a} + i\mathrm{b} \in \mathbb{Z}[i]$), e si osservi che $N(z_1 z_2) = N(z_1)N(z_2)$ per ogni $z_1, z_2 \in \mathbb{Z}[i]$.

(b) Si dimostri che se z è un elemento invertibile dell'anello $\mathbb{Z}[i]$ allora $N(z) = 1$.

(c) Si dimostri che gli elementi invertibili di $\mathbb{Z}[i]$ sono $1, -1, i, -i$.

Esercizio 5.27. Sia R un anello, X un insieme non vuoto, e sia $A = R^X$ l'insieme di tutte le applicazioni da X in R. Su A si definiscano una addizione e una moltiplicazione ponendo, per ogni $f, g \in A$:

$$(f + g)(x) = f(x) + g(x), \quad fg(x) = f(x)g(x) \quad \textit{per ogni} \quad x \in X.$$

Allora $(A, +, \cdot)$ è un anello commutativo.

(a) Si determini l'identità dell'anello A.

(b) Si determinino i divisori dello zero di A e si dica se il loro insieme costituisce un ideale di A.

(c) Si determinino gli elementi invertibili di A (assumendo di conoscere quelli di R).

(d) Posto $X = \{0, 1\}$, si provi che l'anello R^X è isomorfo a $R \times R$.

Esercizio 5.28. Sia R l'anello $\mathbb{Z} \times \mathbb{Z}$, e sia $S = \{(x, y) \in R \mid 3 \text{ divide } x - y\}$. Si provi che S è sottoanello ma non è ideale di R. Si determinino quindi gli elementi invertibili di S.

Esercizio 5.29. Sia R un anello commutativo. Si provi che R è un dominio d'integrità se e solo se soddisfa la legge di cancellazione.

Esercizio 5.30. Sia R un anello commutativo e sia $a \in R$. Si provi che l'insieme $N(a) = \{x | x \in R, xa = 0_R\}$ è un ideale di R. Più in generale, si provi che, se I un ideale di R, allora

$$N_I(a) = \{x \in R \mid xa \in I\}.$$

è un ideale di R .

Esercizio 5.31. Siano I, L, K ideali dell'anello A tali che

$$I + L = A \qquad \text{e} \qquad L \cap K \subseteq I \ ;$$

si provi che $K \subseteq I$.

Esercizio 5.32. Sia $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$ una catena ascendente di ideali *propri* di un anello R. Si provi che $\bigcup_{n \in \mathbb{N}} I_n$ è un ideale proprio di R.

Esercizio 5.33. Sia p un primo fissato e sia $R = \{ \frac{m}{n} \in \mathbb{Q} \mid p \text{ non divide } n \}$.

(a) Si dimostri che R Ŕ un anello. (basta provare che Ŕ un sottoanello di $(\mathbb{Q}, +, \cdot)$).

Sia $U(R)$ l'insieme degli elementi invertibili di R, e sia $I = R \setminus U(R)$.

(b) Si determinino gli elementi di $U(R)$.

(c) Si provi che I è un ideale di R.

(d) Si dimostri che ogni ideale proprio di R è contenuto in I.

Esercizio 5.34. Sia R un anello e sia e un elemento idempotente (cioè tale che $e^2 = e$) con $e \neq 0_R, 1_R$..

(a) Sia $I = \{a \in R \mid ea = a\}$. Si provi che se R è commutativo allora I è un ideale di R, e contiene (e).

(b) Considerando l'elemento $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ nell'anello delle matrici $M_2(\mathbb{R})$, si provi che l'affermazione del punto (b) non vale se R non è commutativo.

Esercizio 5.35. Sia I un ideale dell'anello commutativo R.

(a) Siano $x, y \in R$, si provi che se x^2, $x + y \in I$ allora $y^2 \in I$.

(b) Sia $x \in R$ tale che $x^2 \in I$; si provi che $K = \{\ y \in R \mid x(x+y) \in I\ \}$ è un ideale di R.

Esercizio 5.36. Sia R un sottoanello dell'anello $\mathbb{Q}$ dei numeri razionali.

(a) Si provi che se $\frac{a}{b} \in R$ con $(a, b) = 1$ allora $\frac{1}{b} \in R$.

(b) Si provi che se I è un ideale di R esiste $n \in \mathbb{Z}$ tale che $I = (n) = nR$.

Esercizio 5.37. Sia p un numero primo; si provi che

$$\mathbb{Q}_p = \left\{ \frac{n}{p^i} \mid n \in \mathbb{Z},\ i \in \mathbb{N} \right\}$$

è un dominio a ideali principali.

Esercizio 5.38. Siano $f, g \in \mathbb{R}^{\mathbb{R}}$; si provi che l'ideale generato (f, g) di $\mathbb{R}^{\mathbb{R}}$ è principale. Si provi poi che ogni ideale finitamente generato dell'anello $\mathbb{R}^{\mathbb{R}}$ è principale.

Esercizio 5.39. Dato $f \in \mathbb{R}^{\mathbb{R}}$, poniamo $Z(f) = \{x \in \mathbb{R} \mid f(x) = 0\}$. Si provi che l'insieme

$$\{f \in \mathbb{R}^{\mathbb{R}} \mid \mathbb{R} \setminus Z(f) \text{ è finito } \}$$

è un ideale dell'anello $\mathbb{R}^{\mathbb{R}}$ che non è principale.

Esercizio 5.40. Sia R un anello commutativo. Si provi che se esistono ideali non banali I e J di R tali che $I \cap J = \{0\}$ allora R non è un dominio d'integrità.

Esercizio 5.41. Sia $f : R \longrightarrow S$ un omomorfismo di anelli e sia H un ideale di R. Si dimostri che

$$f^{-1}(f(H)) = H + Ker(f).$$

Esercizio 5.42. Si provi che non esistono omomorfismi dell'anello $\mathbb{Q}$ nell'anello $\mathbb{Z}$. Si provi che l'applicazione identica è l'unico automorfismo di $\mathbb{Z}$ ed è l'unico automorfismo di $\mathbb{Q}$.

Esercizio 5.43. Sia $\mathbb{R}^{\mathbb{R}}$ l'anello delle funzioni reali. Si provi che non esiste alcun omomorfismo di anelli da $\mathbb{C}$ in $\mathbb{R}^{\mathbb{R}}$.

Esercizio 5.44. Sia R un dominio d'integrità e sia $f : R \to R$ l'applicazione definita da $f(a) = a^2$ per ogni $a \in R$. Si provi che f è iniettiva se e solo se è un omomorfismo. [sugg.: si provi che se f è iniettiva allora per ogni $a \in R$ si ha $a + a = 0_R$].

Esercizio 5.45. Sia R un anello commutativo. Si assuma che $x^2 \neq 0$ per ogni $0 \neq x \in R$, e che esista un ideale non banale minimo I di R (cioè $I \subseteq J$ per ogni ideale non banale J di R). Si provi che R è un dominio d'integrità. Si concluda infine che R è un campo (ovvero che $I = R$). [sugg.: si osservi che I è principale, quindi si assuma per assurdo che esistano $x, y \in R$ tali che $xy = 0$ ...]

Esercizio 5.46. Sia R un dominio di integrità (anello commutativo privo di divisori dello zero), e sia $a \in R$, $a \neq 0$ ed a non invertibile. Si provi che l'ideale (a^2) é contenuto propriamente nell'ideale (a). Si dimostri quindi che un dominio di integritá con un numero finito di ideali è un campo.

Esercizio 5.47. Sia A un anello commutativo, e sia $I = \{a \in A \mid a \text{ non è invertibile}\}$. Si provi che le seguenti condizioni sono equivalenti:

(i) I è un ideale di A;

(ii) esiste un ideale proprio di A che contiene tutti gli ideali propri di A.

Esercizio 5.48. (Ideali di un anello di parti). Sia X un insieme non vuoto, e consideriamo l'anello delle parti $(\mathcal{P}(X), \Delta, \cap)$.

(a) Si provi che per ogni $Y \in \mathcal{P}(X)$, l'ideale principale generato da Y è $\mathcal{P}(Y)$.

(b) Si provi che se $\mathcal{I}$ è un ideale di $\mathcal{P}(X)$ e $Y, Z \in \mathcal{I}$, allora $Y \cup Z \in \mathcal{I}$. Si deduca che se X è finito, ogni ideale di $\mathcal{P}(X)$ è principale.

(c) Sia X un insieme *infinito*; si provi che $\mathcal{F} = \{Y \in \mathcal{P}(X) \mid |Y| < \infty\}$ è un ideale di $\mathcal{P}(X)$, e che non è principale.

Esercizio 5.49. (Sugli anelli di Boole) Sia A un anello di Boole (vedi Proposizione 5.8). Su A si definisca la relazione $\leq$ ponendo, per ogni $a, b \in A$, $a \leq b$ se $ab = a$.

(a) Si provi che $\leq$ è una relazione d'ordine su A.

(b) Si provi che $(A, \leq)$ è un reticolo, con $\max A = 1$ e $\min A = 0$.

(c) Si provi che il reticolo $(A, \leq)$ è *complementato*: per ogni $a \in A$ esiste $a' \in A$ tale che $a \vee a' = 1$ e $a \wedge a' = 0$.

6

Anelli notevoli

6.1. Anelli di classi di congruenza. Caratteristica di un anello

Sia $n \geq 2$. L'insieme $\mathbb{Z}/n\mathbb{Z}$ di tutte le classi di congruenza modulo n, fornisce un importante caso di anello commutativo.
Ovviamente, dobbiamo iniziare con il definire opportune operazioni di somma e di prodotto sull'insieme $\mathbb{Z}/n\mathbb{Z}$.

Sia quindi fissato il modulo $n \geq 2$. Denotando con $\overline{a}$ la classi di congruenza modulo n di $a \in \mathbb{Z}$, si ha $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}]|$. Siano $a, b \in \mathbb{Z}$; allora

$$\overline{a} = a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\} \qquad \overline{b} = b + n\mathbb{Z} = \{b + nz \mid z \in \mathbb{Z}\}.$$

sono sottoinsiemi non vuoti dell'anello $\mathbb{Z}$, che possiamo quindi sommare secondo la regola descritta nella sezione 4.2:

$$\begin{aligned} \overline{a} + \overline{b} &= \{\ x + y \mid x \in \overline{a},\ y \in \overline{b}\ \} = \{\ (a + nz_1) + (b + nz_2) \mid z_1, z_2 \in \mathbb{Z}\ \} = \\ &= \{\ (a + b) + n(z_1 + z_2) \mid z_1, z_2 \in \mathbb{Z}\ \} = \{\ (a + b) + nz \mid z \in \mathbb{Z}\ \} = \\ &= \overline{a + b}. \end{aligned}$$

In pratica, *la somma di classi di congruenza modulo n è ancora una classe di congruenza modulo n*, che è descritta dalla regola

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Questo definisce un'operazione di somma sull'insieme $\mathbb{Z}/n\mathbb{Z}$ di tutte le classi di congruenza modulo n. In modo simile è possibile definire un prodotto per classi di congruenza. Con gli stessi n, a e b di sopra, si pone

$$\overline{a} \cdot \overline{b} = \{\ xy \mid x \in \overline{a},\ y \in \overline{b}\ \}.$$

Quindi,

$$\begin{aligned} \overline{a} \cdot \overline{b} &= \{(a + nz_1)(b + nz_2) \mid z_1, z_2 \in \mathbb{Z}\} = \\ &= \{ab + n(az_2 + bz_1 + nz_1z_2) \mid z_1, z_2 \in \mathbb{Z}\} = \\ &= \{ab + nz \mid z \in \mathbb{Z}\ \} = \overline{ab}. \end{aligned}$$

Dunque, anche in questo caso, *il prodotto di due classi di congruenza modulo n è una classe di congruenza modulo n*, ed è descritto da

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Ciò definisce pertanto un'operazione di prodotto su $\mathbb{Z}/n\mathbb{Z}$.

A questo punto, risulta laborioso ma non difficile provare che l'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$, con le operazioni di somma e prodotto definite sopra, è un anello commutativo, che si chiama **anello delle classi resto modulo n**. Inoltre si ha

$$0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0} = n\mathbb{Z} \qquad \text{e} \qquad 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1} = 1 + n\mathbb{Z}.$$

(Si tratta di verificare proprietà che discendono naturalmente da quelle analoghe in $\mathbb{Z}$, e dalle definizioni delle operazioni. Per esempio verifichiamo la proprietà distributiva.
Siano $\overline{a}, \overline{b}, \overline{c}$, generici elementi di $\mathbb{Z}/n\mathbb{Z}$. Allora

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$$

Le altre verifiche si conducono in modo simile. È altresì immediato verificare che, per ogni $k \in \mathbb{N}$, ed ogni $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, si ha $\overline{a}^k = \overline{a^k}$.)

Per comodità, se $2 \leq n \in \mathbb{N}$, denoteremo talvolta con $\mathbb{Z}_n$ l'anello $\mathbb{Z}/n\mathbb{Z}$.

Esempi. 1) Nell'anello $\mathbb{Z}/6\mathbb{Z}$ eseguiamo il calcolo seguente

$$\begin{aligned} \overline{5} - \overline{2}^3 \cdot (\overline{3} + \overline{4} \cdot \overline{5}) + (\overline{2} + \overline{3})^3 (\overline{3} - \overline{5}) &= \overline{5} - \overline{8} \cdot (\overline{3} + \overline{20}) + (\overline{2+3})^3 (\overline{3-5}) = \\ &= \overline{5} - \overline{2} \cdot \overline{23} + \overline{5}^3 \cdot (\overline{-2}) = \\ &= \overline{5} - \overline{2} \cdot \overline{5} + \overline{(-1)^3} \cdot \overline{4} = \\ &= \overline{5} - \overline{2} \cdot \overline{5} + \overline{(-1)} \cdot \overline{4} = \overline{5 - 10 - 4} = \overline{-9} = \overline{3}. \end{aligned}$$

2) Sia p un numero primo. Il Teorema di Fermat (Teorema 4.7) può essere interpretato come una eguaglianza nell'anello $\mathbb{Z}/p\mathbb{Z}$; esso afferma che

$$\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z} \quad \Rightarrow \quad \overline{a}^{p-1} = \overline{1}.$$

Facciamo subito un'importante osservazione. Sia $n \geq 1$, e sia $\mathbb{Z}/n\mathbb{Z}$ l'anello delle classi di congruenza modulo n. Allora l'applicazione

$$\begin{array}{rccc} \rho_n : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & a & \mapsto & a + n\mathbb{Z} \end{array}$$

è un omomorfismo suriettivo di anelli, che si chiama *riduzione modulo n.* Come avremo anche modo di vedere più avanti, sii tratta di uno strumento semplice ma basilare in molti campi della teoria (elementare e no) dei numeri. Osserviamo anche che, se ρ_n è la riduzione modulo n, allora $ker(\rho_n) = n\mathbb{Z}$.

Abbiamo già osservato che, per $n \geq 2$, l'anello $\mathbb{Z}/n\mathbb{Z}$ è commutativo. In generale però non è un dominio d'integrità: ad esempio, nell'anello $\mathbb{Z}/12\mathbb{Z}$ delle classi resto modulo 12, $\overline{4} \neq \overline{0}$, $\overline{3} \neq \overline{0}$, ma $\overline{4} \cdot \overline{3} = \overline{12} = \overline{0} = 0_{\mathbb{Z}/12\mathbb{Z}}$, e quindi $\overline{4}$ e $\overline{3}$ sono divisori dello zero. D'altra parte è possibile che $\mathbb{Z}/n\mathbb{Z}$ contenga elementi invertibili che non provengono da invertibili di $\mathbb{Z}$. Ad esempio, sempre in $\mathbb{Z}/12\mathbb{Z}$, l'elemento $\overline{5}$ è diverso sia da $\overline{1}$ che da $\overline{-1}$, e purtuttavia è invertibile. Infatti, in $\mathbb{Z}/12\mathbb{Z}$,

$$\overline{5} \cdot \overline{5} = \overline{25} = \overline{1} = 1_{\mathbb{Z}/12\mathbb{Z}},$$

quindi $\overline{5}$ è un elemento invertibile di $\mathbb{Z}/12\mathbb{Z}$ (e coincide con il proprio inverso). Queste osservazioni sono estese e chiarite dal Teorema seguente.

Teorema 6.1. *Sia $n \geq 2$. Allora*

1. *Un elemento $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $(a,n) = 1$. Quindi $U(\mathbb{Z}/n\mathbb{Z}) = \{\ \overline{a} \mid 1 \leq a \leq n-1,\ (a,n) = 1\ \}$.*
2. *$\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo. Se n non è primo, allora $\mathbb{Z}/n\mathbb{Z}$ non è un dominio d'integrità.*

Dimostrazione. 1) Sia $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Possiamo prendere $1 \leq a \leq n-1$ (escludiamo $\overline{a} = \overline{0}$ perchè chiaramente lo zero di un anello non è mai un invertibile - e d'altra parte, $(0,n) = n$). Per definizione, $\overline{a}$ è invertibile se e solo se esiste $1 \leq b \leq n-1$ tale che

$$\overline{ab} = \overline{a} \cdot \overline{b} = 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1}$$

ovvero, $ab \equiv 1 \pmod{n}$. Quindi, $\overline{a}$ è invertibile se e solo se esiste $1 \leq b \leq n-1$ ed un $z \in \mathbb{Z}$ tali che

$$ab + zn = 1$$

cioè se e solo se $(a,n) = 1$.

2) $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se ogni elemento non nullo è invertibile. Quindi, per il punto 1), $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo $(a,n) = 1$ per ogni $1 \leq a \leq n-1$, e questo avviene se e solo se n è un numero primo.
Supponiamo, infine, che n non sia un numero primo. Dunque n si fattorizza propriamente, e quindi esistono interi $2 \leq a,\ b \leq n-1$, tali che $ab = n$. Ma allora, nell'anello $\mathbb{Z}/n\mathbb{Z}$, $\overline{a}$ e $\overline{b}$ sono diversi da $0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0}$, mentre $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{n} = \overline{0}$. Dunque $\overline{a}$ e $\overline{b}$ sono divisori dello zero, e quindi $\mathbb{Z}/n\mathbb{Z}$ non è un dominio d'integrità. ∎

Un aspetto della massima importanza del risultato precedente, e che merita di essere ribadito, è che se p è un numero primo positivo, allora $\mathbb{Z}/p\mathbb{Z}$ è un campo.

Corollario 6.2. *Per ogni numero primo positivo p esiste un campo di ordine p.*

Esercizio 6.1. Determinare le soluzioni dell'equazione $\overline{3}x^2 - \overline{2} = \overline{0}$, nel campo $\mathbb{Z}/7\mathbb{Z}$.

Soluzione. Poichè tutti gli elementi non nulli di $F = \mathbb{Z}/7\mathbb{Z}$ sono invertibili, possiamo moltiplicare per l'inverso di $\overline{3}$, che è $\overline{5}$ (infatti $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$), ottenendo l'equazione equivalente

$$\overline{0} = x^2 - \overline{2} \cdot \overline{5} = x^2 - \overline{3}.$$

A questo punto, possiamo testare più facilmente gli elementi di F, trovando che $\overline{1}^2 = \overline{6}^2 = \overline{1}$, $\overline{2}^2 = \overline{5}^2 = \overline{4}$, $\overline{3}^2 = \overline{4}^2 = \overline{2}$; concludendo così che l'equazione data non ha soluzioni in F.

Esercizio 6.2. Si determinino tutti gli elementi invertibili ed i divisori dello zero negli anelli $\mathbb{Z}/24\mathbb{Z}$ e $\mathbb{Z}/16\mathbb{Z}$.

Esercizio 6.3. Trovare le soluzioni di $x^2 = \overline{1}$, e di $x^3 = \overline{1}$, negli anelli $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ e $\mathbb{Z}/11\mathbb{Z}$.

Caratteristica di un anello. Sia a un elemento di un anello R. Allora, per ogni numero intero n è definito il multiplo n-esimo na di a nel modo che conosciamo

$$na = \underbrace{a + a + \cdots + a}_{n} \qquad \text{se } n \geq 1$$

e $na = (-n)(-a)$ se $n \leq -1$, $0a = 0_R$. Valgono le regole descritte nella sezione 5.1.

Proposizione 6.3. *Sia R un anello. Esiste un solo omomorfismo da $\mathbb{Z}$ in R, ed è definito da, per ogni $z \in \mathbb{Z}$, $z \mapsto z1_R$.*

Dimostrazione. Sia ϕ un omomorfismo da $\mathbb{Z}$ in R. Allora $\phi(1) = 1_R$ e $\phi(0) = 0_R$, da cui segue $\phi(-1) = -1_R$ e, per ogni $n \geq 0$

$$\phi(n) = \phi(1 + 1 + \cdots + 1) = \phi(1) + \phi(1) + \cdots + \phi(1) = n1_R$$

e $\phi(-n) = -\phi(n) = -(n1_R) = (-n)1_R$.
Viceversa, si verifica usando le regole sopra ricordate, che l'applicazione

$$\begin{array}{rcl} \mathbb{Z} & \to & R \\ z & \mapsto & z1_R \end{array}$$

è un omomorfismo di anelli. ∎

Ora, dato un anello R, sia ϕ l'unico omomorfismo da $\mathbb{Z}$ in R. Il suo nucleo è un ideale di $\mathbb{Z}$, quindi $\ker(\phi) = n\mathbb{Z}$ per un numero naturale n univocamente determinato. Tale naturale n si dice la **caratteristica** dell'anello R. Osserviamo che se la caratteristica è diversa da 0 allora deve essere almeno 2.
Quindi la caratteristica di R è 0 se e solo se l'omomorfismo ϕ è iniettivo; se invece la caratteristica è $n \geq 2$, allora (ricordando come si trova il generatore positivo di un ideale di $\mathbb{Z}$ - Teorema 5.9) n è il minimo intero > 0 che appartiene al nucleo di ϕ. Possiamo dunque dedurre la seguente definizione alternativa di caratteristica:

La caratteristica di un anello R è

0 *se* $n1_R \neq m1_R$ *per ogni* $n, m \in \mathbb{Z}$, $n \neq m$;

$n > 0$ *se* n *è il minimo numero naturale non nullo tale che* $n1_R = 0_R$.

Ad esempio, gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ hanno caratteristica 0, mentre, per $n \geq 2$, l'anello $\mathbb{Z}/n\mathbb{Z}$ ha caratteristica n. La Proposizione 5.8 afferma, in particolare, che un anello di Boole ha caratteristica 2.

Esercizio 6.4. Determinare la caratteristica dell'anello $A = \mathbb{Z}_6 \times Z_4$.

Soluzione. Poiché $1_A = (\overline{1}, \overline{1})$ (dove, ovviamente, la barra denota classi di congruenza modulo 6 e modulo 4 rispettivamente nelle due coordinate), si ha $12 \cdot 1_A = (\overline{12}, \overline{12}) = (\overline{0}, \overline{0}) = 0_A$. Ciò significa che, posto n la caratteristica di A, si ha $12 \in n\mathbb{Z}$. In altre parole, $n \geq 2$ è un divisore di 12. Ma $6 \cdot 1_A = (\overline{6}, \overline{6}) = (\overline{0}, \overline{2}) \neq 0_A$, e similmente $4 \cdot 1_A = (\overline{4}, \overline{4}) = (\overline{4}, \overline{2}) \neq 0_A$. Si conclude quindi che $n = 12$.

Esaminiamo ora più a fondo l'immagine dell'unico omomorfismo ϕ da $\mathbb{Z}$ in R definito nella Proposizione 6.3

$$Im(\phi) = \{z1_R \mid z \in \mathbb{Z}\},$$

che si denota con P_R. Si tratta di un sottoanello di R, che è contenuto in ogni altro sottoanello di R (perché ?). Per questo motivo P_R è detto *sottoanello fondamentale* o sottoanello *primo* di R.
Sia n è la caratteristica di R. Se $n = 0$, l'omomorfismo ϕ è iniettivo e dunque $P_R \simeq \mathbb{Z}$. Sia $n \geq 2$; allora è ben definita l'applicazione

$$\begin{array}{rcl} \overline{\phi} : \mathbb{Z}/n\mathbb{Z} & \to & P_R \\ \overline{z} & \mapsto & z1_R \end{array}$$

Siano infatti $z, z_1 \in \mathbb{Z}$ tali che $\overline{z} = \overline{z_1}$; allora n divide $z_1 - z$, e conseguentemente $0_R = (z_1 - z)1_R = z_1 1_R - z1_R$, da cui $z_1 1_R = z1_R$. Ora, $\overline{\phi}$ è suriettiva (per definizione di P_R), e si verifica facilmente che è un omomorfismo di anelli; è inoltre iniettiva, perché $0_R = \overline{\phi}(\overline{z}) = z1_R \ \Rightarrow \ n|z \ \Rightarrow \overline{z} = \overline{0}$. Dunque $\overline{\phi}$ è un isomorfismo. Abbiamo così una completa descrizione dei sottoanelli fondamentali, che ricapitoliamo nella seguente proposizione.

Proposizione 6.4. *Sia R una anello, e sia P_R il suo sottoanello fondamentale. Allora*

(1) la caratteristica di R è zero se e solo se $P_R \simeq \mathbb{Z}$;

(2) la caratteristica di R è $n > 0$ se e solo se $P_R \simeq \mathbb{Z}/n\mathbb{Z}$.

Osserviamo che se n è la caratteristica di un anello R, allora $na = 0_R$ per ogni $a \in R$. Ciò è per definizione se $n = 0$; mentre se $n > 0$ per ogni $a \in R$ si ha

$$na = a + \cdots + a = 1_R a + \cdots + 1_R a = (1_R + \cdots 1_R)a = (n1_R)a = 0_R a = 0_R \ .$$

Concludiamo con la seguente importante osservazione:

Proposizione 6.5. *La caratteristica di un dominio d'integrità è 0 oppure un numero primo.*

Dimostrazione. Sia R un dominio d'integrità di caratteristica $n > 0$. Allora il sottoanello fondamentale P_R è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Poiché P_R è anch'esso un dominio d'integrità, n deve essere un numero primo (Teorema 6.1). ∎

Esercizio 6.5. Provare che gli anelli $\mathbb{Z}_5 \times \mathbb{Z}_5$ e $\mathbb{Z}_{25}$ non sono isomorfi.

Esercizio 6.6. Si determini la caratteristica dell'anello $R = (\mathbb{Z}/12\mathbb{Z}) \times \mathbb{Z}$.

Esercizio 6.7. Ricordiamo che un elemento a di un anello A è detto *nilpotente* se esiste un intero $n \geq 1$ tale che $a^n = 0_A$. Si determinino gli elementi nilpotenti dell'anello $\mathbb{Z}/18\mathbb{Z}$, e quelli di $\mathbb{Z}/12\mathbb{Z}$.

Esercizio 6.8. Si provi che l'insieme $\{3x + 12\mathbb{Z} \mid x \in \mathbb{Z}\}$ è un ideale dell'anello $\mathbb{Z}/12\mathbb{Z}$.

6.2. Anelli di matrici.

Esempi principali di anelli non commutativi sono gli anelli di matrici, il cui studio approfondito fa parte del programma di altri corsi. Richiamiamo qui, per comodità del lettore e senza dimostrazioni, solo alcuni fatti significativi dal nostro punto di vista, fatti che chi legge probabilmente già conosce almeno nel caso di coefficienti reali. Come diremo subito, è possibile considerare matrici a coefficienti in un qualsiasi anello commutativo. Per molte delle proprietà più importanti, le dimostrazioni nel caso generale non differiscono formalmente da quelle per matrici reali (o complesse).

Sia R un anello commutativo e sia $1 \leq n \in \mathbb{N}$. Una **matrice quadrata di ordine n** a coefficienti in R è una tabella

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

dove i coefficienti a_{ij} sono elementi di R. L'insieme di tutte le matrici quadrate di ordine n a coefficienti nell'anello R si denota con $M_n(R)$.

La **somma** $A + B$ di due matrici (di ordine n) $A = (a_{ij})$ e $B = (b_{ij})$ a coefficienti in R, è la matrice (di ordine n) i cui coefficienti si ottengono sommando tra loro i coefficienti corrispondenti di A e B. Ovvero, posto $(s_{ij}) = S = A + B$, si pone $s_{ij} = a_{ij} + b_{ij}$ (per ogni $i, j = 1, \ldots, n$). Un esempio è forse superfluo, ma eccone uno con $A = \mathbb{Z}$ e $n = 2$:

$$\begin{pmatrix} 1 & -2 \\ 6 & 3 \end{pmatrix} + \begin{pmatrix} -3 & 0 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} -2 & -2 \\ 7 & -1 \end{pmatrix}.$$

Si verifica facilemente che tale somma soddisfa gli assiomi (S1) – (S4) di anello. È cioè un'operazione transitiva, commutativa, con un elemento neutro che è la matrice nulla 0_M (ovvero quella con tuti i coefficienti uguali a 0_R), e tale che ogni matrice ha una matrice 'opposta' (definita prendendo gli opposti dei coefficienti). Ad esempio, per $n = 2$,

$$0_{M_2(R)} = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix} \qquad - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}.$$

Se $A = (a_{ij}) \in M_n(R)$, allora, per ogni $i = 1, 2, \ldots, n$, la n-upla

$$(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

è detta **i-esima riga** della matrice A. Mentre la **i-esima colonna** di A è

$$(a_{1i}\ a_{2i}\ \cdots\ a_{ni}).$$

Il **prodotto** di due matrici quadrate di ordine n, $A = (a_{ij})$, $B = (b_{ij})$ è definito nella maniera seguente: $(a_{ij})(b_{ij}) = (c_{ij})$ dove, per ogni $i, j = 1, 2, \ldots, n$

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}. \tag{6.1}$$

Cioè il coefficiente di posto ij nella matrice prodotto è

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{in}b_{nj}$$

ovvero il prodotto (scalare) della i-esima riga di A per la j-esima colonna di B.

Esempi (in $M_2(\mathbb{Q})$):

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + (-\frac{1}{2} \cdot \frac{1}{2}) & 1 \cdot (-1) + (-\frac{1}{2}) \cdot (-2) \\ -2 \cdot 0 + 3 \cdot \frac{1}{2} & -2 \cdot (-1) + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{3}{2} & -4 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 1 \\ 3 & 0 & 1 \\ -2 & \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 5 & \frac{1}{4} & 2 \\ 3 & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Si verifica che, per ogni $n \geq 1$ il prodotto di matrici quadrate di ordine n è una operazione associativa. Inoltre la **matrice identica**

$$I_n = \begin{pmatrix} 1_R & 0 & \cdots & 0 \\ 0 & 1_R & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1_R \end{pmatrix}$$

è l'elemento identico. Sono quindi soddisfatti anche gli assiomi (P1) (P2) (ovvero $(M_n(R), \cdot)$ è un monoide). Si verifica poi che sussistono anche le proprietà distributive. Abbiamo quindi

Proposizione 6.6. *Sia R un anello commutativo. Allora, per ogni $n \geq 1$ e con le operazioni sopra definite, $M_n(R)$ è un anello.*

Se $n \geq 2$ il prodotto di matrici *non è commutativo*, ad esempio:

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

(si osservi che per $M_1(R)$ coincide con R).

Sempre per $n \geq 2$, $M_2(R)$ contiene elementi unipotenti non nulli (quindi divisori dello zero): si provi ad esempio che se

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

allora $A^3 = 0$.

Esercizio 6.9. Nell'anello $M_2(\mathbb{R})$ si trovino due elementi a e b tali che $(ab)^2 \neq a^2b^2$.

Ad ogni matrice quadrata $A \in M_n(R)$ è associato un elemento di R $|A| = Det(A)$ detto **determinante** di A. La definizione generale di determinante di una matrice e le sue proprietà sono parte del corso di Geometria. Qui ricordo solo il caso di matrici di ordine $n = 2, 3$. (Una matrice di ordine 1 è un elemento di R e coincide con il suo determinante)

$$Det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$$Det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} Det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + (-1) a_{12} Det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} Det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Ad esempio

$$Det \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} = 1 \cdot Det \begin{pmatrix} 2 & \frac{1}{2} \\ 1 & 0 \end{pmatrix} + (-1)0 \cdot Det \begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} + (-1) \cdot Det \begin{pmatrix} 0 & 2 \\ -\frac{1}{2} & 1 \end{pmatrix} =$$

$$= 1(2 \cdot 0 - 1\frac{1}{2}) - 0 - 1(0 \cdot 1 - 2(-\frac{1}{2})) = -\frac{1}{2} - 0 - 1 = -\frac{3}{2}.$$

Una proprietà molto importante del determinante è che per ogni $A, B \in M_n(R)$:

$$Det(A \cdot B) = Det(A)Det(B). \tag{6.2}$$

Inoltre, per ogni $n \geq 1, Det(I_n) = 1_R$.

Un altro fatto fondamentale è che

$$A \in M_n(R) \text{ è invertibile se e solo se } Det(A) \text{ è un elemento invertibile di } R. \tag{6.3}$$

Quindi, ad esempio gli elementi invertibili di $M_n(\mathbb{Z})$ sono tutte e sole le matrici a coefficienti interi (di ordine n) il cui determinante è 1 o -1. Mentre, più in generale, *se K è un campo*, $U(M_n(K)) = \{A \in M_n(K) \mid Det(A) \neq 0_K\}$. L'insieme degli elementi invertibili dell'anello di matrici $M_n(R)$ è (come in ogni anello) un gruppo rispetto alla moltiplicazione - cioè il prodotto righe per colonne - che si denota con $GL(n, R)$.

Rimandiamo ancora al corso di Geometria per le regole generali per determinare l'inversa di una matrice invertibile. Qui riporto, al fine di comprendere esempi ed esercizi, il caso $n = 2$.

Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ con $\Delta = Det(A) \in U(R)$. Allora

$$A^{-1} = \begin{pmatrix} d\Delta^{-1} & -b\Delta^{-1} \\ -c\Delta^{-1} & a\Delta^{-1} \end{pmatrix}. \tag{6.4}$$

Concludiamo questa sezione con un esercizio: proviamo che i soli ideali di $M_2(\mathbb{R})$ sono $\{0\}$ e $M_2(\mathbb{R})$ (cosa che si generalizza a qualsiasi anello di matrici a coefficienti su un campo). Poiché $M_2(\mathbb{R})$ contiene elementi non nulli e non invertibili, questo mostra che il Teorema 5.12 non si estende al caso non–commutativo (che, d'altra parte, esistano anelli non–commutativi in cui ogni elemento non nullo è invertibile sarà dimostrato nella sezione 6.4).
Sia dunque I un ideale di $M_2(\mathbb{R})$, e supponiamo che I contenga un elemento non nullo

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Se $Det(A) \neq 0$, A è invertibile e dunque $I = M_2(\mathbb{R})$. Assumiamo quindi $Det(A) = 0$. Poiché I contiene gli elementi

$$A\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} c & d \\ a & b \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$$

possiamo anche assumere $a \neq 0$. Ora, I contiene la matrice

$$B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d+a \end{pmatrix}.$$

Si ha $Det(B) = ad + a^2 - bc = a^2 + Det(A) = a^2 \neq 0$; quindi B è invertibile, e pertanto $I = M_2(\mathbb{R})$, il che completa la dimostrazione.

Di fatto, nella teoria generale degli anelli non commutativi, il concetto di ideale è affiancato da quelli di *ideale destro* e di *ideale sinistro*. Un sottoinsieme non–vuoto I

di un anello R è un ideale destro se, per ogni $a, b \in I$, $x \in R$, $a - b \in I$ e $ax \in I$ (non si richiede, cioè, $xa \in I$). L'ideale sinistro è definito richiedendo invece $a - b \in I$ e $xa \in I$, per ogni $a, b \in I$, $x \in R$. Se R è commutativo, è chiaro che ogni ideale destro (o sinistro) è un ideale; ma per anelli non–commutativi questi due concetti assumono significato (si veda l'esercizio 6.14). Se $a \in R$, allora l'insieme $\{ax \mid x \in \mathbb{R}\}$ è un ideale destro, che si denota con aR ed è il minimo ideale destro di R che contiene a (similmente si definisce l'ideale sinistro $Ra = \{xa \mid x \in R\}$).

Esercizio 6.10. Si provi che ogni elemento non nullo di $M_2(\mathbb{R})$ è invertibile, oppure un divisore dello zero. Si dica se la stessa cosa vale in $M_2(\mathbb{Z})$.

Esercizio 6.11. Sia A un anello commutativo, e sia I un ideale di A. Sia $1 \leq n \in \mathbb{N}$; si provi che

$$M_n(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in I \right\}$$

è un ideale di $M_n(A)$.

Esercizio 6.12. Sia $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.

a) Si provi che A è un sottoanello dell'anello $M_2(\mathbb{R})$.

b) Si provi che l'applicazione $\phi : A \to \mathbb{C}$, definita da

$$\phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + ib$$

è un isomorfismo di anelli.

c) Si trovi un automorfismo $A \to A$ che sia diverso dall'applicazione identitica.

Esercizio 6.13. Sia $n \geq 2$; si provi che l'insieme degli elementi nilpotenti di $M_n(\mathbb{R})$ non è un ideale di $M_n(\mathbb{R})$.

Esercizio 6.14. Sia A un anello commutativo. Si provi che l'insieme

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A \right\}$$

è un ideale destro ma non è un ideale sinistro di $M_2(A)$. Si dica poi se esiste un elemento $X \in M_2(A)$ tale che $J = XM_2(A)$.

6.3. Campo delle frazioni.

Sia $\phi : R \to S$ un omomorfismo *iniettivo* di anelli. Allora R è isomorfo a $\phi(R)$ che è un sottoanello di S; in tal caso si identificano gli elementi di R con le loro immagini tramite ϕ, e si dice che l'anello S è una **estensione** dell'anello R. L'istanza più semplice è quando R è già un sottoanello di S e ϕ associa ogni elemento di R con se stesso.

In questa sezione, per ogni dominio di integrità D costruiremo una estensione F di D che è un campo. Inoltre tale campo F ha la proprietà che ogni campo che sia estensione di D è anche estensione di F. Quindi, in questo senso, F è la *minima*

estensione di D che è un campo. Tale F si chiamerà il **campo delle frazioni** di D. Applicata al caso $D = \mathbb{Z}$ questa costruzione fornisce il campo $\mathbb{Q}$ dei numeri razionali.

Sia D un dominio di integrità. Assumiamo perciò che D sia commutatativo e privo di divisori dello zero: entrambe queste condizioni sono necessarie per la costruzione del campo F. Iniziamo considerando l'insieme

$$D \times D^* = \{(a, b) \mid a, b \in D,\ b \neq 0_D\}$$

di tutte le coppie ordinate di elementi di D la cui seconda componente non è zero. Su tale insieme definiamo una relazione $\sim$ ponendo, per ogni $(a, b), (c, d) \in D \times D^*$,

$$(a, b) \sim (c, d) \quad \text{se} \quad ad = bc\ .$$

Si verifica facilmente che $\sim$ è una relazione di equivalenza. Infatti:

1) $(a, b) \sim (a, b)$ per ogni $(a, b) \in D \times D^*$ perchè $ab = ba$ essendo D commutativo.

2) Se $(a, b) \sim (c, d)$ allora $ad = bc$, quindi $cb = da$, cioè $(c, d) \sim (a, b)$.

3) Siano $(a, b), (c, d), (r, s) \in D \times D^*$ tali che $(a, b) \sim (c, d)$, $(c, d) \sim (r, s)$, allora $ad = bc$ e $cs = dr$; quindi $(as)d = (ad)s = (bc)s = b(cs) = b(dr) = (br)d$; poichè $d \neq 0_D$ e D è un dominio d'integrità, per la legge di cancellazione, si ha $as = br$ e dunque $(a, b) \sim (r, s)$.

Per ogni $(a, b) \in D \times D^*$ indichiamo con $\frac{a}{b}$ la classe di equivalenza di (a, b) modulo $\sim$, e chiamiamo F l'insieme quoziente modulo $\sim$, cioè

$$F = \frac{D \times D^*}{\sim} = \left\{ \frac{a}{b} \mid (a, b) \in D \times D^* \right\}\ .$$

Definiamo quindi su F le operazioni di somma e prodotto nel modo seguente. Per ogni $\frac{a}{b}, \frac{c}{d} \in F$,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}\ , \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}\ .$$

Occorre verificare che si tratta di buone definizioni. Siano dunque $\frac{a}{b}, \frac{c}{d}, \frac{a'}{b'}, \frac{c'}{d'} \in F$ con $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$; allora $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$, cioè $ab' = ba'$ e $cd' = dc'$. Dunque:

$$\begin{aligned} (ad + bc)b'd' &= adb'd' + bcb'd' = ab'dd' + cd'bb' = \\ &= ba'dd' + dc'bb' = a'd'bd + b'c'bd = (a'd' + b'c')bd \end{aligned}$$

e quindi

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'}\ .$$

Similmente

$$(ac)(b'd') = ab'cd' = ba'dc' = (a'c')(bd)$$

e quindi

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'c'}{b'd'} = \frac{a'}{b'} \cdot \frac{c'}{d'}\ .$$

Ora, è facile provare che, con tali operazioni, F è un anello commutativo con $0_F = \frac{0}{1}$, $1_F = \frac{1}{1}$. Vediamo ad esempio la distributività; osserviamo preliminarmente che per

ogni $\frac{a}{b} \in F$, e $0 \neq c \in D$ si ha $\frac{a}{b} = \frac{ac}{bc}$; siano quindi $\frac{a}{b}, \frac{c}{d}, \frac{r}{s} \in F$, allora

$$\begin{aligned} \frac{a}{b}(\frac{c}{d} + \frac{r}{s}) &= \frac{a}{b}\frac{cs+dr}{ds} = \frac{a(cs+dr)}{b(ds)} = \frac{acs+adr}{bds} = \\ &= \frac{acsb+adrb}{bdsb} = \frac{ac}{bd} + \frac{ar}{sb} = \\ &= \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{r}{s}. \end{aligned}$$

Lasciamo le altre verifiche per esercizio.
Per dimostrare che F è un campo, resta da provare che ogni elemento non nullo di F è invertibile. Sia $\frac{a}{b} \neq 0_F = \frac{0}{1}$, allora $(a,b) \not\sim (0,1)$, cioè $a = a1 \neq b0 = 0$ e quindi $\frac{b}{a} \in F$ e si ha

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1_F$$

dunque $\frac{b}{a} = (\frac{a}{b})^{-1}$. Quindi F è un campo.

Proviamo che F è una estensione di D mediante l'applicazione

$$\begin{array}{rccc} \phi: & D & \to & F \\ & a & \mapsto & \frac{a}{1} \end{array}$$

ϕ è un omomorfismo, infatti $\phi(1) = \frac{1}{1} = 1_F$, e per ogni $a, a' \in D$

$$\phi(a+a') = \frac{a+a'}{1} = \frac{a1+a'1}{1 \cdot 1} = \frac{a}{1} + \frac{a'}{1} = \phi(a) + \phi(a')$$

$$\phi(aa') = \frac{aa'}{1} = \frac{aa'}{1 \cdot 1} = \frac{a}{1} \cdot \frac{a'}{1} = \phi(a)\phi(a') \ ,$$

ed è iniettivo, infatti

$$\phi(a) = 0_F \quad \Leftrightarrow \quad \frac{a}{1} = \frac{0}{1} \quad \Leftrightarrow \quad (a,1) \sim (0,1) \quad \Leftrightarrow \quad a = a1 = 1 \cdot 0 = 0$$

dunque $Ker(\phi) = \{0\}$.

Il campo F così costruito si chiama **campo delle frazioni** del dominio D, ed identificando D con la sua immagine $\phi(D)$, possiamo dire che F "contiene" D. Abbiamo quindi provato la prima parte del seguente

Teorema 6.7. *Sia D un dominio d'integrità. Allora esiste un campo F che è una estensione di D. Inoltre, se K è un campo che è una estensione di D, allora K è una estensione di F.*

Dimostrazione. Rimane da provare la seconda parte dell'enunciato. Sia quindi F il campo delle frazioni del dominio D, e sia $\phi : D \to K$ una estensione di D ad un campo K. Allora per ogni $b \neq 0_D$, $\phi(b) \neq 0_K$ (perchè ϕ è iniettivo), e quindi $\phi(b)$ è invertibile in K. È possibile dunque definire

$$\begin{array}{rccc} \overline{\phi}: & F & \to & K \\ & \frac{a}{b} & \mapsto & \phi(a)\phi(b)^{-1} \end{array}$$

per ogni $a, b \in D$, $b \neq 0_D$. Tale applicazione è ben definita; infatti se $\frac{a}{b} = \frac{c}{d}$ allora $ad = bc$ e quindi $\phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1}$. Si verifica poi facilmente che $\overline{\phi}$ è un

omomorfismo (esercizio). Infine, $\overline{\phi}$ è iniettiva, infatti (tenendo conto che K è un campo e quindi, in particolare, un dominio d'integrità)

$$0_K = \overline{\phi}(\frac{a}{b}) = \phi(a)\phi(b)^{-1} \quad \Leftrightarrow \quad \phi(a) = 0_K \quad \Leftrightarrow \quad a = 0_D \quad \Leftrightarrow \quad \frac{a}{b} = 0_F \ .$$

Osserviamo infine che per ogni $a = \frac{a}{1} \in D$ si ha $\overline{\phi}(\frac{a}{1}) = \phi(a)$. ∎

Se applicata all'anello $\mathbb{Z}$, questa procedura conduce alla costruzione del campo $\mathbb{Q}$ dei numeri razionali. Anzi, volendo essere rigorosi, il campo $\mathbb{Q}$ è *definito* come il campo delle frazioni di $\mathbb{Z}$.

Esercizio 6.15. Sia F un campo. Qual è il campo delle frazioni di F?

Esercizio 6.16. Sia A un dominio d'integrità, e $a, b \in A$. Si provi che se esistono interi positivi coprimi n, m tali che $a^n = b^n$ e $a^m = b^m$, allora $a = b$.

Esercizio 6.17. Sia A un dominio d'integrità e sia $\emptyset \neq S$ un sottoinsieme *moltiplicativamente chiuso* di A (cioè, per ogni $s_1, s_2 \in S$, $s_1 s_2 \in S$) tale che $0_A \notin S$. Su $A \times S$ si definisca la relazione $\sim$ ponendo $(a, s) \sim (b, t)$ se $at = bs$ (per ogni $a, b \in A$ e $s, t \in S$).

(1) Si provi che $\sim$ è un'equivalenza, e si denoti con A_S l'insieme quoziente. Su A_S si definiscano quindi operazioni di somma e prodotto come nel caso del campo delle frazioni, e si provi che A_S è un dominio d'integrità.

(2) Si definisca un omomorfismo iniettivo $\phi : A \to A_S$.

(3) Si provi che per ogni $s \in S$, $\phi(s)$ è invertibile in A_S.

[Si noti che non si assume $1 \in S$, e quindi si faccia attenzione nel definire correttamente l'identità di A_S e l'omomorfismo ϕ.]

Esercizio 6.18. Sia p un numero primo e sia $S = \{p^n \mid n \in \mathbb{N}\}$. Si provi, con le notazioni dell'esercizio precedente, che $\mathbb{Z}_S$ è isomorfo all'anello $\mathbb{Q}_p$ dell'esercizio 5.4.

Esercizio 6.19. Qual è il campo delle frazioni di $\mathbb{Q}_p$?

6.4. Quaternioni.

Un anello in cui ogni elemento non nullo è invertibile si dice **anello con divisione** o anche *corpo*. Un campo è quindi un anello con divisione commutativo. Il fatto che esistano anelli con divisione non commutativi non è scontato e, come vedremo in questa sezione, la costruzione di esempi del genere non è banale (anche se di anelli con divisione non commutativi ce ne sono in abbondanza). Citiamo, ad esempio, un Teorema di Wedderburn (la cui dimostrazione esula da questo corso), che afferma che ogni anello con divisione finito è commutativo ed è, quindi, un campo.

L'anello dei **Quaternioni** è il più importante e, storicamente, il primo esempio di anello con divisione non commutativo (cioè che non sia un campo). Esso fu scoperto (o, se preferite, costruito) da W.R. Hamilton nel 1843. Dopo numerosi tentativi di costruire strutture algebriche (campi) che contenessero il campo $\mathbb{C}$ dei complessi, ed avessero dimensione 3 sui reali (i complessi hanno dimensione 2), Hamilton si rese conto che ciò non era possibile, e di dover quindi di dover salire a dimensione 4 e al

contempo rinunciare alla commutatività del prodotto. Ma bando alle chiacchere e vediamo la costruzione.

Nell'anello $M_2(\mathbb{C})$ delle matrici quadrate complesse di ordine 2, consideriamo il seguente sottoinsieme:

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} .$$

Dove se $a = x + iy \in \mathbb{C}$ (con $x, y \in \mathbb{R}$), allora $\overline{a} = x - iy$ è il suo **coniugato**. Ricordo le proprietà fondamentali che riguardano i coniugati (vedi sezione 5.2):

- per ogni $a, b \in \mathbb{C}$: $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{ab} = \overline{a}\overline{b}$
- se $a = x+iy \in \mathbb{C}$ allora $a\overline{a} = x^2+y^2$ è un numero reale positivo, e $a\overline{a} = 0 \Leftrightarrow a = 0$
- $\overline{\overline{a}} = a$ per ogni $a \in \mathbb{C}$ e $\overline{a} = a$ se e solo se $a \in \mathbb{R}$.

Utilizzando tali proprietà si dimostra facilmente che $\mathbb{H}$ è un sottoanello dell'anello $M_2(\mathbb{C})$. $\mathbb{H}$ si chiama *anello dei Quaternioni*. $\mathbb{H}$ non è commutativo: ad esempio

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

Osserviamo subito che $\mathbb{H}$ è *un'estensione* di $\mathbb{C}$, e quindi di $\mathbb{R}$; infatti, porre

$$z \mapsto \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$$

definisce un omomorfismo iniettivo $\mathbb{C} \to \mathbb{H}$.

Verifichiamo ora che $\mathbb{H}$ è un anello con divisione. Quello che manca è la seguente

Proposizione 6.8. *In $\mathbb{H}$ ogni elemento non nullo è invertibile.*

Dimostrazione. Sia

$$0_{\mathbb{H}} \neq x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H}$$

(con $a, b \in \mathbb{C}$, $(a, b) \neq (0, 0)$) e sia $d = a\overline{a} - (-\overline{b}b) = Det(x)$. Allora $d = a\overline{a} + \overline{b}b \in \mathbb{R}$ e $d \neq 0$ perchè $(a, b) \neq (0, 0)$, dunque

$$y = \begin{pmatrix} \overline{a}d^{-1} & -bd^{-1} \\ \overline{b}d^{-1} & ad^{-1} \end{pmatrix} = \begin{pmatrix} \overline{a}d^{-1} & -bd^{-1} \\ -\overline{(-bd^{-1})} & \overline{\overline{a}d^{-1}} \end{pmatrix} \in \mathbb{H},$$

e inoltre

$$xy = yx = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{\mathbb{H}} ,$$

quindi x è invertibile in $\mathbb{H}$. ∎

Consideriamo ora i seguenti elementi di $\mathbb{H}$:

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} .$$

Inoltre identifichiamo ogni numero reale α con l'elemento $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ di $\mathbb{H}$. Si verificano facilmente le seguenti uguaglianze:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k} \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i} \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}\ .$$

In particolare, ritroviamo che $\mathbb{H}$ non è commutativo.

Osserviamo infine che se $a = \alpha + i\beta,\ b = \gamma + i\delta \in \mathbb{C}$ (con $\alpha, \beta, \gamma, \delta \in \mathbb{R}$), allora

$$\begin{aligned} \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} &= \begin{pmatrix} \alpha + i\beta & \gamma + i\delta \\ -\gamma + i\delta & \alpha - i\beta \end{pmatrix} = \\ &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} i\beta & 0 \\ 0 & -i\beta \end{pmatrix} + \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix} + \begin{pmatrix} 0 & i\delta \\ i\delta & 0 \end{pmatrix} = \\ &= \alpha \cdot 1 + \beta \cdot \mathbf{i} + \gamma \cdot \mathbf{j} + \delta \cdot \mathbf{k} \end{aligned}$$

e tale scrittura è unica ($\mathbb{H}$ è dunque anche uno spazio vettoriale di dimesione 4 sui reali, con una base costituita da $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$).

Esercizio 6.20. Si determini il centro di $\mathbb{H}$ (vedi esercizio 5.5).

Esercizio 6.21. Il *coniugio* su $\mathbb{H}$ è l'applicazione $\overline{\cdot} : \mathbb{H} \to \mathbb{H}$ definita da, per ogni $u = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H}$,

$$\overline{u} = a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}.$$

La *norma* su $\mathbb{H}$ è l'applicazione $N : \mathbb{H} \to \mathbb{R}$ definita da

$$N(u) = u\overline{u} = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

per ogni $u = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H}$.
Si provi che la norma è moltiplicativa; ovvero $N(uv) = N(u)N(v)$ per ogni $u, v \in \mathbb{H}$, e e che il coniugio è un *antiautomorfismo* moltiplicativo; ovvero che, per ogni $a, b \in \mathbb{H}$, si ha $\overline{ab} = \overline{b}\overline{a}$.

Esercizio 6.22. Sia $v = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$. Si osservi che $N(v) = -v^2$. Si concluda che per ogni $0 < r \in \mathbb{R}$, l'equazione $x^2 + r = 0$ ha infinite soluzioni in $\mathbb{H}$. Quindi, ad esempio, le soluzioni in $\mathbb{H}$ di $x^2 + 1 = 0$ sono tutti e soli i quaternioni del tipo $b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ tali che $b^2 + c^2 + d^2 = 1$.

Esercizio 6.23. Si provi che $\mathbb{H}(\mathbb{Z}) = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H} \mid a, b, c, d \in \mathbb{Z}\}$ è un sottoanello dell'anello dei quaternioni $\mathbb{H}$.

Esercizio 6.24. Sia R un anello tale che i soli ideali destri di R sono $\{0\}$ ed R. Si provi che R è un anello con divisione.

6.5. Esercizi.

Esercizio 6.25. (Omomorfismo di Frobenius) Sia p un primo, e sia R un dominio d'integrità di caratteristica p. Utilizzando la dimostrazione della Proposizione 4.8 si provi che

$$(a+b)^p = a^p + b^p \ .$$

Dedurre da ciò che l'applicazione $\Phi : R \to R$ definita da, per ogni $a \in R$: $\Phi(a) = a^p$ è un omomorfismo di R in se stesso (detto endomorfismo di Frobenius). Provare infine che se R è finito allora Φ è un automorfismo.

Esercizio 6.26. Si definisca un omomorfismo dell'anello $\mathbb{Z}_{20}$ nell'anello $\mathbb{Z}_5$.

Esercizio 6.27. Siano p, q numeri primi.

(a) Provare che l'applicazione

$$\begin{array}{rccc} \theta : & \mathbb{Z} & \to & \mathbb{Z}_p \times \mathbb{Z}_q \\ & z & \mapsto & (z + p\mathbb{Z}, z + q\mathbb{Z}) \end{array}$$

è un omomorfismo di anelli, e determinare $Ker(\theta)$.

(b) Provare che θ è suriettiva se e solo se $p \neq q$.

Esercizio 6.28. Sia $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_6 \right\}$ l'anello delle matrici quadrate di ordine 2 a coefficienti in $\mathbb{Z}_6$. Si determinino la cardinalità di R ed il suo sottoanello fondamentale; si dica se il sottoanello fondamentale di R è un campo.

Esercizio 6.29. Sia R un anello di caratteristica zero e sia $f : \mathbb{Z} \to R$ un omomorfismo suriettivo di anelli; si provi che f è un isomorfismo.

Esercizio 6.30. Sia A un anello commutativo di caratteristica p, dove p è un numero primo, e sia P il sottoanello fondamentale di A. Si provi che se I è un ideale *proprio* di A, allora $I \cap P = \{0_A\}$.

Esercizio 6.31. Trovare le soluzioni di $x^2 = x$ in $\mathbb{Z}/12\mathbb{Z}$, ed in $\mathbb{Z}/11\mathbb{Z}$.

Esercizio 6.32. Determinare elementi invertiibili, elementi nilpotenti e ideali dell'anello $\mathbb{Z}_4 \times \mathbb{Z}_6$.

Esercizio 6.33. Sia R un anello commutativo, e I un suo ideale. Sia

$$D(I) = \{\ x \in R \mid x + x \in I\ \}.$$

a) Si provi che $D(I)$ è un ideale di R.

b) Si consideri l'anello $\mathbb{Z}$ dei numeri interi, e $n \geq 2$. Si provi che $D(n\mathbb{Z}) = n\mathbb{Z}$ se e solo se n è dispari.

Esercizio 6.34. Sia $\varphi : R \longrightarrow S$ un omomorfismo di anelli commutativi, e sia c $\neq 0$ la caratteristica di S. Si dimostri che c divide la caratteristica di R.

Esercizio 6.35. Siano A un anello commutativo, $1 \leq n \in \mathbb{N}$, e $x, y \in M_n(A)$. Si provi che se $xy = 1$ allora $yx = 1$.

Esercizio 6.36. Nell'anello delle matrici quadrate di ordine 2 a coefficienti interi si consideri l'insieme

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}.$$

(a) Si provi che A è un anello (rispetto alle usuali operazioni di somma e di prodotto tra matrici).

(b) Si dimostri che $J = \left\{ \begin{pmatrix} 5x & y \\ 0 & 5z \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\}$ è un ideale di A.

Esercizio 6.37. Sia $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$.

(a) Si provi che R è un anello commutativo (si dimostri infatti che è un sottoanello di $M_2(\mathbb{Q})$).

(b) Si provi che, se D è l'insieme dei divisori dello zero di R, allora $I = D \cup \{0\}$ è un ideale di R.

(c) Si provi che gli ideali di R sono $\{0\}$, I, R.

Esercizio 6.38. Sia $A = \left\{ \begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$. Provare che A è un sottoanello di $M_2(\mathbb{Z})$. Provare quindi che l'applicazione $\phi : A \to \mathbb{Z}$, definita da

$$\phi\left(\begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix} \right) = a$$

è un omomorfismo suriettivo e determinare il suo nucleo.

Esercizio 6.39. Sia α un numero reale e sia

$$A_\alpha = \left\{ \begin{pmatrix} a & b \\ \alpha b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} .$$

a) Si provi che A_α è un sottoanello commutativo dell'anello $M_2(\mathbb{R})$ delle matrici quadrate di ordine due sui reali.

b) Si provi che A_α è un campo se e solo se $\alpha < 0$.

c) Posto quindi $\alpha = 1$ e $A = A_1$, si provi che l'applicazione $\Phi : A \longrightarrow \mathbb{R}$ definita da

$$\Phi \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b$$

è un omomorfismo di anelli.

Esercizio 6.40. Siano R un anello e $\emptyset \neq X \subseteq R$. Si provi che

$$An_r(X) = \{r \in \mathbb{R} \mid xr = 0 \ \forall x \in X\}$$

è un ideale destro di R, e che se X è un ideale destro, allora $An_r(X)$ è un ideale di R.

Esercizio 6.41. Sia R un anello e sia J un ideale destro proprio (cioè $J \neq R$) di R. Si assuma che J contenga tutti gli ideali destri propri di R e si provi che allora J è un ideale.

Esercizio 6.42. Sia $u \in \mathbb{H}(\mathbb{Z})$. Si provi che le seguenti proprietà sono equivalenti:

(i) u è invertibile in $\mathbb{H}(\mathbb{Z})$;

(ii) $N(u) = 1$;

(ii) $u \in \{\pm 1, \pm i, \pm j, \pm k\}$.

Esercizio 6.43. si verifichi che l'insieme $Q = \{1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ è un gruppo non commutativo (rispetto alla moltiplicazione). Esso è detto *gruppo dei Quaternioni*.

Esercizio 6.44. Sia $y \in \mathbb{H} \setminus \mathbb{R}$. Si provi che esistono $a, b \in \mathbb{R}$ tali che $y^2 + ay + b = 0$. [sugg.: Se $y = a_0 + a_1 i + a_2 j + a_3 k$, considerare $v = y - a_0$ e osservare che $\overline{v} = -v$, quindi $v^2 = \dots$]

Esercizio 6.45. Sia K un sottoanello di $\mathbb{H}$, con $\mathbb{R} \subseteq K$ e $\mathbb{R} \neq K$. Si provi che esiste $u \in K$ tale che $u^2 = -1$. Si deduca che K contiene un campo isomorfo a $\mathbb{C}$.

Esercizio 6.46. (Anello degli endomorfismi, I) Sia R un anello; denotiamo con $End(R)$ l'insieme di tutti gli endomorfismi della *struttura additiva* di R, ovvero le applicazioni $f : R \to R$ tali che $f(a + b) = f(a) + f(b)$ per ogni $a, b \in \mathbb{R}$.

(a) Si provi che per ogni $f \in End(R)$, $f(0_R) = 0_R$, e che f è iniettivo se e solo se $Ker f = \{a \in R \mid f(a) = 0_R\} = \{0_R\}$.

(b) Si provi che per ogni $a \in R$, l'applicazione $\lambda_a : R \to R$ definita da $\lambda_a(x) = ax$ (per ogni $x \in R$) appartiene a $End(R)$.

(c) Sia $R = \mathbb{Z}$, si provi che ogni elemento di $End(\mathbb{Z})$ è del tipo λ_a per qualche $a \in \mathbb{Z}$.

Esercizio 6.47. (Anello degli endomorfismi, II) Sia R una anello; su $End(R)$ si definisca l'addizione ponendo $(f + g)(a) = f(a) + g(a)$, per ogni $f, g \in End(R)$ ed ogni $a \in R$,

(a) Si provi che $E = (End(R), +, \circ)$ (dove $\circ$ è la composizione di applicazioni) è un anello, con 0_E l'applicazione costante 0, e 1_E l'applicazione identica ι_E.

(b) Sia $f \in End(R)$; si provi che f è invertibile in $End(R)$ se e solo se è biettiva.

Esercizio 6.48. (Anello degli endomorfismi, III) Sia R un anello. Utilizzando opportunamente il punto (b) dell'esercizio 6.46 si definisca un omomorfismo iniettivo $R \to End(R)$. Si provi quindi che se $R = \mathbb{Z}$ oppure $R = \mathbb{Z}_n$ (per qualche $n \geq 2$), allora $R \simeq End(R)$.

Esercizio 6.49. (Anello degli endomorfismi, IV) Sia $R = \mathbb{Z} \times \mathbb{Z}$. Si provi che $End(R) \simeq M_2(\mathbb{Z})$.

Esercizio 6.50. (Anello degli endomorfismi, V) Sia R un anello. Si provi che se $End(R)$ è un campo, allora R è un campo.

7

Fattorizzazioni

In questo capitolo approfondiremo lo studio degli anelli commutativi, ed in special modo dei domini d'integrità, avendo come riferimento le proprietà dell'anello $\mathbb{Z}$ dei numeri interi. In particolare, cercheremo di generalizzare l'idea di fattorizzazione unica. Come si vedrà. il ruolo svolto dal concetto di ideale (ed in particolare di ideale principale) è fondamentale.

7.1. Divisibilità e fattorizzazioni

In queste prime sezioni estenderemo ai domini d'integrità i concetti di divisibilità, primalità. MCD, etc. già introdotti nel caso dell'anello degli interi; mediante tale processo di astrazione ne chiariremo gli aspetti fondamentali.
Cominciamo col generalizzare certe definizioni.

Definizioni. Sia R un anello commutativo, e siano $a, b \in R$.

(1) Diciamo che a *divide* b (o anche a è un fattore di b) se esiste $c \in R$ tale che $ac = b$. In tal caso si scrive $a|b$.

(2) Diciamo che a, b sono *associati* se $a|b$ e $b|a$, e scriviamo allora $a \sim b$.

Un divisore a di b si dice *proprio* se non è invertibile e non è associato a b.

Osserviamo subito che se u è un elemento invertibile di R allora $u|b$ per ogni $b \in R$: infatti $b = u(u^{-1}b)$.

La situazione che ci interessa è quella in cui R è un *dominio d'integrità*. In questo caso se $a, b \in R$ sono associati, esistono $c, d \in R$ tali che $ac = b$ e $bd = a$; da ciò segue $a = a(cd)$ e, per la legge di cancellazione, $cd = 1$; quindi c, d sono invertibili. Viceversa, se u è invertibile allora $a \sim ua$. Pertanto, due elementi a, b di un dominio d'integrità, *sono associati se e solo se differiscono per un fattore invertibile.*

Questi concetti hanno una immediata interpretazione in termini di ideali principali. Ricordo che, se R è un anello commutativo e $a \in R$, l'ideale principale generato da a è

$$(a) = \{\ ax \mid x \in R\ \},$$

ed è il minimo ideale di R contenente a.

Proposizione 7.1. *Sia R un anello commutativo, e siano $a, b \in R$. Allora*

(1) *$a|b$ se e solo se $(b) \subseteq (a)$.*

(2) *$a \sim b$ se e solo se $(a) = (b)$.*

Dimostrazione. (1) Siano $a, b \in R$. Allora

$$(b) \subseteq (a) \;\Leftrightarrow\; b \in (a) \;\Leftrightarrow\; (\text{esiste } c \in R:\; b = ac\;) \;\Leftrightarrow\; a|b\;.$$

(2) Discende immediatamente da (1) e dalla definizione di elementi associati. ∎

Definizione. Un elemento a di un dominio d'integrità R si dice **irriducibile** se

(i) a non è 0_R e non è invertibile;

(ii) i soli divisori di a sono gli invertibili e gli elementi associati (detto altrimenti: a non ha divisori propri).

Quindi, gli elementi irriducibili di $\mathbb{Z}$ sono i numeri primi, mentre un campo non contiene elementi irriducibili.

Fattorizzazione in irriducibili. Si dice che un elemento a di un dominio d'integrità R ammette una *fattorizzazione in irriducibili* se a si può scrivere come prodotto di irriducibili di R, e si dice che la fattorizzazione è *essenzialmente unica* se due diverse decomposizioni di a come prodotto di irriducibili hanno lo stesso numero di fattori e, a meno di scambiare i termini di una delle due fattorizzazioni, i fattori irriducibili delle due decomposizioni sono a due a due tra loro associati. Detto formalmente:

La fattorizzazione $a = s_1 s_2 \dots s_n$ come prodotto di elementi irriducibili è essenzialmente unica se per ogni altra fattorizzazione $a = r_1 r_2 \dots r_k$ con r_i irriducibili, si ha $k = n$ ed esiste una permutazione π (cioè una biezione in se stesso) di $\{1, 2, \dots, n\}$ tale che s_i è associato a $r_{\pi(i)}$ per ogni $i = 1, 2, \dots, n$.

Un dominio d'integrità R si dice **Dominio a Fattorizzazione Unica** (abbreviato: UFD) se ogni elemento non nullo e non invertibile di R ammette una fattorizzazione in irriducibili ed essa è essenzialmente unica.

L'anello $\mathbb{Z}$ è un UFD. Per il momento è il solo che conosciamo; ma nel prossimo capitolo vedremo quanto più ampia, e quanto importante, sia questa classe di anelli. Il risultato principale di questa sezione è una caratterizzazione degli UFD, che utilizzeremo nella prossima sezione per provare il fatto fondamentale che ogni dominio a ideali principali è un dominio a fattorizzazione unica.
Cominciamo osservando che per ogni elemento non nullo e non invertibile a di un dominio a fattorizzazione unica R, il numero di fattori che compaiono in ogni fattorizzazione in irriducibili di a è fisso e dipende solo dall'elemento a; indichiamo questo numero con $\ell(a)$. Si prova immediatamente il Lemma che segue, che sarà poi utile nella dimostrazione del Teorema principale.

Lemma 7.2. *Sia R un UFD e sia $a \in R$ un elemento non nullo e non invertibile. Allora, per ogni divisore proprio b di a, si ha $\ell(b) \leq \ell(a) - 1$.*

Dimostrazione. Esercizio. ∎

Ci occorre ora un'altra definizione.

Definizione. Un elemento a di un dominio d'integrità R si dice **primo** se

(i) a non è 0_R e non è invertibile;

(ii) per ogni $b, c \in R$, se $a|bc$ allora $a|b$ oppure $a|c$.

Chiaramente la terminologia è ereditata da $\mathbb{Z}$. Nell'anello $\mathbb{Z}$ elementi primi ed elementi irriducibili coincidono. Questo non vale in generale, ed una delle cose che ci servono è provare che negli UFD tale coincidenza continua a sussistere. Per una direzione è sufficiente assumere che l'anello sia un dominio d'integrità.

Lemma 7.3. *Sia R un dominio d'integrità. Allora ogni elemento primo di R è irriducibile.*

Dimostrazione. Sia a un elemento primo del dominio d'integrità R. Allora, per definizione, a non è nullo e non è invertibile. Sia quindi b un divisore di a; allora esiste $c \in R$ tale che $a = bc$. Per la definizione di elemento primo si ha allora $a|b$ oppure $a|c$. Nel primo caso b è associato ad a, nel secondo caso c è associato ad a e quindi b è invertibile. Dunque i soli divisori di a sono o associati ad a oppure gli invertibili, e pertanto a è un irriducibile. ∎

Il viceversa vale negli UFD: questo è il punto (1) del seguente risultato.

Lemma 7.4. *Sia R un Dominio a Fattorizzazione Unica. Allora*

(1) *Ogni elemento irriducibile di R è un primo.*

(2) *Non esistono catene infinite $a_0, a_1, a_2, \ldots$ di elementi di R tali che, per ogni i, a_{i+1} è un divisore proprio di a_i.*

Dimostrazione. (1) Sia a un elemento irriducibile del dominio a fattorizzazione unica R. Allora a è non nullo e non invertibile per definizione. Siano $b, c \in R$ tali che $a|bc$, e sia $d \in R$ tale che $ad = bc$. Possiamo assumere $b \neq 0 \neq c$ (infatti $a|0$). Se b è invertibile allora $adb^{-1} = c$, e quindi $a|c$; allo stesso modo, se c è invertibile allora $a|b$. Supponiamo quindi che né b né c siano invertibili. Allora entrambi ammettono una fattorizzazione in irriducibili

$$b = s_1 s_2 \ldots s_n \qquad e \qquad c = r_1 r_2 \ldots r_m$$

Osservo che allora d non è invertibile; perché, se lo fosse, si avrebbe $a = d^{-1}bc$, ed, essendo a irriducibile, uno tra b e c dovrebbe essere invertibile. Quindi d non è invertibile e $d \neq 0$; pertanto d ammette una fattorizzazione $d = q_1 q_2 \ldots q_k$, in fattori irriducibili. Allora

$$a q_1 q_2 \ldots q_k = s_1 s_2 \ldots s_n r_1 r_2 \ldots r_m$$

sono due fattorizzazioni in irriducibili dello stesso elemento $bc = ad$. Per la essenziale unicità della fattorizzazione deve essere, in particolare, a associato ad un s_i o ad un r_j; nel primo caso $a|b$ e nel secondo caso $a|c$.
In ogni caso quindi $a|b$ oppure $a|c$, dunque a è un elemento primo.

(2) Siano $a_0, a_1, a_2, \ldots$ elementi di R tali che, per ogni i, a_{i+1} è un divisore proprio di a_i. Per ogni i, sia n_i il numero di fattori in una decomposizione di a_i in irriducibili. Allora, per il Lemma 7.2, si ha $n_0 > n_1 > n_2 > \ldots$; quindi per qualche $k \leq n_0$ si deve avere $n_k = 1$, che significa che a_k è irriducible. Poichè un elemento irriducible non ha divisori propri, la catena si arresta a a_k. ∎

Il bello è che questo Lemma si può invertire, fornendo così la caratterizzazione degli UFD che cerchiamo.

Teorema 7.5. *Sia R un dominio d'integrità. Allora R è un dominio a fattorizzazione unica se e solo se soddisfa alle proprietà (1) e (2) del Lemma precedente.*

Dimostrazione. Un verso è proprio il Lemma 7.4. Supponiamo quindi che R sia un dominio d'integrità che soddisfa alle proprietà (1) e (2) del Lemma 7.4, e proviamo che R è un UFD.
Sia a un elemento non nullo e non invertibile di R; cominciamo con il provare che

1) *esiste un irriducibile b_1 che divide a.*

Se a è irriducibile, allora $b_1 = a$. Altrimenti, $a = a_0$ ha un divisore proprio a_1; se questo è irriducibile si pone $b_1 = a_1$, altrimenti a_1 ha un divisore proprio a_2; ancora, se a_2 è irriducibile si pone $b_1 = a_2$ (chiaramente $a_2|a_0 = a$); altrimenti si prosegue trovando un divisore proprio a_3 di a_2. Per la proprietà (2) questo processo non può proseguire indefinitamente: si arriverà quindi dopo un numero finito k di passi ad un elemento a_k irriducibile che divide ogni a_i per $0 \leq i \leq k$. In particolare a_k divide $a_0 = a$ e si ha $b_1 = a_k$.

2) *a ha una fattorizzazione in irriducibili.*

Se a è irriducible siamo a posto. Supponiamo che a non sia irriducibile; allora per il punto 1) esiste un divisore irriducibile b_1 di $a = a_0$. Sia $a_1 \in R$ tale che $a = b_1 a_1$; poiché a non è irriducibile, a_1 non è invertibile; se a_1 è irriducibile allora $a = b_1 a_1$ è la fattorizzazione cercata; altrimenti ripetiamo su a_1 le operazioni fatte su a, trovando $a_1 = b_2 a_2$ con b_2 irriducibile. Se a_2 è irriducibile allora $a = b_1 b_2 a_2$ è la fattorizzazione cercata; altrimenti ripetiamo su a_2 le stesse operazioni. In questo modo otteniamo una catena $a = a_0, a_1, a_2, \ldots$ di elementi di R ognuno dei quali è un divisore proprio del precedente, e tale che, per ogni i, $a_i = b_{i+1} a_{i+1}$ con b_{i+1} irriducibile. Per la proprietà (2) tale catena si arresta ad un termine irriducibile $a_n = b_{n+1}$; ma allora

$$a = a_0 = b_1 a_1 = b_1 b_2 a_2 = \ \cdots = b_1 b_2 \ldots b_n b_{n+1}$$

e quindi a ammette una fattorizzazione in irriducibili.

3) *unicità della fattorizzazione in irriducibili.*

Consideriamo due fattorizzazioni in irriducibili dello stesso elemento (non nullo e non invertibile):

$$r_1 r_2 r_3 \ \ldots \ r_n = s_1 s_2 s_3 \ \ldots \ s_k \qquad (*)$$

e, procedendo per induzione su n, mostriamo che sono essenzialmente la stessa decomposizione.
Se $n = 1$ allora $r_1 = s_1 s_2 s_3 \ldots s_k$ è irriducibile, quindi $k = 1$ e $s_1 = r_1$. Sia $n \geq 2$ e supponiamo per ipotesi induttiva che due fattorizzazioni dello stesso elemento siano essenzialmente la stessa se una delle due è costituita da al più $n - 1$ fattori. Ora, r_1 è irriducibile e quindi, per la proprietà (1), r_1 è primo. Poiché $r_1 | s_1 s_2 \ldots s_k$ si ha allora che r_1 divide un s_j; a meno di riordinare i termini $s_1, s_2, \ldots, s_m$ nel prodotto, possiamo assumere che r_1 divida s_1. Poiché r_1, s_1 sono irriducibili si ha quindi $r_1 \sim s_1$, dunque $s_1 = r_1 u$ con u invertibile. Allora

$$r_1 r_2 r_3 \ \ldots \ r_n = r_1 u s_2 s_3 \ \ldots \ s_k = r_1 s_2' s_3' \ \ldots \ s_k'$$

con $s_2' = u s_2 \sim s_2$ e $s_j' = s_j$ per $3 \leq j \leq k$. Per la proprietà di cancellazione possiamo dedurre che

$$r_2 r_3 \ \ldots \ r_n = s_2' s_3' \ \ldots \ s_k'$$

Applicando quindi l'ipotesi induttiva, otteniamo $n = k$ e, a meno di riordinare i fattori s_j', $r_j \sim s_j'$ per ogni $2 \leq j \leq n$. Dunque le fattorizzazioni $(*)$ da cui siamo partiti sono essenzialmente la stessa. Per il principio di induzione l'essenziale unicità delle

fattorizzazioni è provata per ogni numero n di fattori irriducibili, così completando la dimostrazione che R è un UFD. ∎

Esempio. (dove proviamo che esistono domini d'integrità che non sono UFD.) Scriviamo $\sqrt{-5} = i\sqrt{5}$ e consideriamo il sottoinsieme dei numeri complessi

$$\mathbb{Z}[\sqrt{-5}] = \{\ a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\ \}\ .$$

Si provi per esercizio che $\mathbb{Z}[\sqrt{-5}]$ è un sottoanello di $\mathbb{C}$ (e quindi è un dominio d'integrità). Per studiare le fattorizzazioni in $\mathbb{Z}[\sqrt{-5}]$, introduciamo la funzione di *norma* $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$,

$$N(z) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2\ .$$

Le solite proprietà sono di verifica immediata:

i) $N(zz_1) = N(z)N(z_1)$ per ogni $z, z_1 \in \mathbb{Z}[\sqrt{-5}]$;
ii) $z \neq 0 \ \Rightarrow\ N(z) > 0$;
iii) $N(z) = 1 \ \Leftrightarrow\ z = \pm 1$.

Con queste si prova facilmente che $U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$. Inoltre, $1 + \sqrt{-5}$ è un elemento irriducibile di $\mathbb{Z}[\sqrt{-5}]$: infatti se $1 + \sqrt{-5} = zz_1$ con $z, z_1 \in \mathbb{Z}[\sqrt{-5}]$ e $z = a + b\sqrt{-5}$, allora

$$6 = N(1 + \sqrt{-5}) = N(zz_1) = N(z)N(z_1)\ .$$

Se $N(z) = 1$ allora $z = \pm 1$ è invertibile, similmente se $N(z) = 6$ allora $z_1 = \pm 1$; altri casi non se ne possono verificare, poichè $N(z) = a^2 + 5b^2 \neq 2, 3$ per ogni $a, b \in \mathbb{Z}$. In modo analogo si dimostra che $2,\ 3,\ 1 - \sqrt{-5}$ sono irriducibili in $\mathbb{Z}[\sqrt{-5}]$. Quindi

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

sono due fattorizzazioni di 6 in irriducibili che non differiscono per fattori invertibili (gli invertibili di $\mathbb{Z}[\sqrt{-5}]$ sono $1, -1$). Dunque $\mathbb{Z}[\sqrt{-5}]$ non è un dominio a fattorizzazione unica.

Torniamo alla teoria generale, ed estendiamo ai domini d'integrità il concetto di MCD.

Definizione. Siano a, b elementi di un dominio d'integrità R; allora $d \in R$ si dice un **massimo comun divisore** (MCD) di a e b se $d|a$, $d|b$, e per ogni $d' \in R$, tale che $d'|a$ e $d'|b$, si ha $d'|d$.

Il massimo comun divisore, se esiste, è individuato a meno di associati. Infatti, se d, c sono due MCD di a e b, allora, per definizione, $c|d$ e $d|c$, quindi esiste un invertibile $u \in R$ tale che $c = ud$.
Ma non sempre un MCD esiste. Nell'anello $\mathbb{Z}[\sqrt{-5}]$ dell'esempio di sopra, 2 e $1+\sqrt{-5}$ sono divisori comuni di $a = 6$ e di $b = 2(1 + \sqrt{-5})$; se $d = x + y\sqrt{-5}$ fosse un massimo comun divisore di a e b, allora $N(d)|(N(a), N(b)) = (36, 24) = 12$ e, inoltre $4 = N(2)|N(d)$ e $6 = N(1 + \sqrt{-5})|N(d)$ (dato che $2|d$ e $(1 + \sqrt{-5})|d$); quindi deve essere $N(d) = x^2 + 5y^2 = 12$ che è impossibile per $x, y \in \mathbb{Z}$.

Sia R sia un dominio a fattorizzazione unica. Per ogni classe di elementi irriducibili associati fissiamo uno ed un solo elemento, e chiamiamo P l'insieme degli elementi così prescelti. In

ogni classe la scelta dell'elemento è arbitraria, ma in certi casi può essere effettuata in modo uniforme. Ad esempio, nel caso di $\mathbb{Z}$ possiamo prendere come P l'insieme numeri primi positivi.
Allora ogni $a \in R$ non nullo si può scrivere in modo unico (a meno dell'ordine dei fattori) come il prodotto

$$a = up_1^{n_1}p_2^{n_2}p_3^{n_3} \ \dots \ p_k^{n_k}$$

con u un invertibile di R, $p_i \in P$ e $n_i \in \mathbb{N}$ per $i = 1, 2, \dots, k$ (osserviamo che se a è invertibile basta porre $n_i = 0$ per ciascun i).
Ora, siano $a = up_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$ e $c = wp_1^{s_1}p_2^{s_2}\dots p_k^{s_k}$ elementi non nulli di R, fattorizzati mediante gli elementi di P, con u, w invertibili, e dove abbiamo eventualmente aggiunto potenze di esponente zero per quegli irriducibili che sono divisori di uno solo dei due elementi. Supponiamo che c divida a; allora esiste $r = w'p_1^{r_1}p_2^{r_2}\dots p_k^{r_k} \in R$ tale che $a = cr$ quindi

$$a = ww'p_1^{s_1+r_1}p_2^{s_2+r_2}\dots p_k^{s_k+r_k}$$

da cui segue in particolare $r_i \leq n_i$ per ogni $i = 1, 2 \dots, k$.

Siano ora $a, b \in R$. Se uno dei due è zero, allora l'altro è un MCD di a e b. Supponiamo quindi che siano entrambi non nulli e fattorizziamoli mediante gli elementi di P:

$$a = up_1^{n_1}p_2^{n_2}\dots p_k^{n_k} \qquad b = vp_1^{m_1}p_2^{m_2} \ \dots p_k^{m_k}$$

con u, v invertibili ed il solito accorgimento sugli esponenti. Consideriamo ora l'elemento

$$d = p_1^{\min\{n_1,m_1\}}p_2^{\min\{n_2,m_2\}} \ \dots \ p_k^{\min\{n_k,m_k\}} \ ;$$

chiaramente d divide sia a che b, e dall'osservazione fatta sopra segue facilmente che e d è un MCD di a e b. Abbiamo quindi provato:

Proposizione 7.6. *Sia R un UFD. Allora ogni coppia di elementi non nulli di R ammette un massimo comun divisore.*

Esercizio 7.1. Sia R un dominio d'integrità tale che ogni coppia di elementi non nulli di R ammette un MCD. Siano $a, b, c \in R \setminus \{0\}$ e sia d un MCD di a, b. Si provi che dc è un MCD di ac, bc.

Soluzione. Sia d_1 un MCD di ac, bc; poichè dc divide sia ac che bc, si ha $dc|d_1$. Sia $e \in R$ tale che $d_1 = dce$, e siano $r, s \in R$ tali che $ac = d_1r$, $bc = d_1s$. Allora $ac = dcer$ e quindi, per la legge di cancellazione, $a = der$, dunque $de|a$; similmente $b = des$ e dunque $de|b$. Da ciò segue $de|d$, che implica che e è invertibile. Quindi $dc \sim d_1$ e pertanto dc è un MCD di ac, bc.

Esercizio 7.2. Usando l'esercizio 7.1, si provi che se R è un dominio d'integrità in cui ogni coppia di elementi non nulli di R ammette un MCD, allora ogni elemento irriducibile di R è primo.

Esercizio 7.3. 1) Dire quali fra gli elementi 5, 7, 11, 29 sono irriducibili in $\mathbb{Z}[\sqrt{-5}]$.
2) Si dia un esempio di un elemento irriducibile di $\mathbb{Z}[\sqrt{-5}]$ che non è primo.
3) Si provi che $\mathbb{Z}[\sqrt{-5}]$ soddisfa alla proprietà (2) del Lemma 7.4.

Esercizio 7.4. Si provi che $\mathbb{Z}[\sqrt{10}] = \{a+b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ è un dominio d'integrità, ma non è a fattorizzazione unica.

Esercizio 7.5. Si dia una definizione di *minimo comune multiplo* in un dominio d'integrità. Quindi si provi che in UFD ogni coppia di elementi non nulli ammette un minimo comune multiplo.

7.2. Ideali massimali e ideali primi

In questa sezione introduciamo due importanti tipi di ideali di un anello che, come vedremo, sono strettamente legati alle proprietà di fattorizzazione. Nel prossimo capitolo svolgeranno un ruolo ancor più importante nella costruzione di nuovi campi e nello studio delle estensioni algebriche del campo $\mathbb{Q}$ dei razionali..

Definizione. Un ideale I di un anello commutativo R si dice **ideale primo** se

(i) $I \neq R$,

(ii) per ogni $a, b \in R$, se $ab \in I$ allora $a \in I$ o $b \in I$.

Ad esempio, l'ideale nullo $\{0_R\}$ è un ideale primo dell'anello commutativo R se e solo se R è un dominio d'integrità (provarlo per esercizio).

Esempio. Consideriamo l'anello $\mathbb{Z}[\sqrt{-5}]$ descritto nella sezione precedente, e i suoi ideali principali (5) e $(\sqrt{-5})$. Si ha $(5) = \{a + b\sqrt{-5} \mid a, b \in 5\mathbb{Z}\}$, e, osservando che, per ogni $u, v \in \mathbb{Z}$, $5u + v\sqrt{-5} = \sqrt{-5}(v - u\sqrt{-5})$ si deduce che $(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a \in 5\mathbb{Z}\}$. L'ideale (5) non è primo: infatti, ad esempio $\sqrt{-5} \notin (5)$ ma $\sqrt{-5}^2 \in (5)$. Invece l'ideale $(\sqrt{-5})$ è primo: infatti, siano $x = a + b\sqrt{-5}, y = c + d\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ tali che

$$(\sqrt{-5}) \ni xy = (ac - 5bd) + (ad + bc)\sqrt{-5}\,:$$

allora $5 \mid ac - 5bd$, e quindi $5 \mid ac$; da ciò segue $5 \mid a$, oppure $5 \mid b$; dunque $x \in (\sqrt{-5})$, oppure $y \in (\sqrt{-5})$.

Osserviamo subito che in $\mathbb{Z}$ gli ideali primi non nulli sono tutti e soli quelli del tipo $p\mathbb{Z}$, con p un numero primo. Questo non è un caso; infatti gli ideali primi di un dominio d'integrità sono strettamente correlati agli elementi primi dell'anello stesso.

Proposizione 7.7. *Sia R un dominio d'integrità, e sia $0_R \neq a \in R$ Allora a è un elemento primo se e solo se (a) è un ideale primo.*

Dimostrazione. Sia $a \neq 0_R$ un elemento primo del dominio d'integrità R. Allora, per definizione a non è invertibile, e quindi $(a) \neq R$. Siano ora $x, y \in R$ tali che $xy \in (a)$. Allora $a|xy$; poiché a è primo, da ciò segue che $a|x$, oppure $a|y$. Nel primo caso $x \in (a)$, ed altrimenti $y \in (a)$. Dunque (a) è un ideale primo.
Viceversa, sia $0_R \neq a \in R$, e supponiamo che l'ideale (a) sia primo. Allora $(a) \neq R$, e quindi a non è invertibile. Se $x, y \in R$ sono tali che $a|xy$, allora $xy \in (a)$. Poiché (a) è un ideale primo, da ciò segue che $x \in (a)$, oppure $y \in (a)$. Nel primo caso $a|x$, e nel secondo $a|y$. Dunque a è un elemento primo. ∎

Osserviamo che, se R è un dominio d'integrità, allora (0_R) è un ideale primo, che non è compreso tra quelli descritti nella Proposizione 7.7.

Definizione. Un ideale I di un anello R si dice **ideale massimale** se

(i) $I \neq R$,

(ii) per ogni ideale J : $I \subseteq J \subseteq R \quad \Rightarrow \quad J = I$ o $J = R$.

In altri termini, un ideale I di un anello R è massimale se e solo se è proprio ed i soli ideali compresi tra I ed R sono I stesso ed R. Il Teorema 5.12 dice che un anello commutativo R è un campo se e solo se l'ideale nullo $\{0_R\}$ è massimale.

Esempio. Nell'anello $\mathbb{R}^{\mathbb{R}}$, fissato $r \in \mathbb{R}$, consideriamo l'ideale $I_r = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(r) = 0\}$. I_r è un ideale massimale. Infatti è chiaramente proprio. Supponiamo che J sia un ideale di $\mathbb{R}^{\mathbb{R}}$

con $I \subseteq J$ e $I_r \neq J$. Allora esiste $g \in J \setminus I$; quindi $g(r) \neq 0$. Sia e_r l'applicazione data da $e_r(r) = 0$ e $e_r(x) = 1$ se $x \neq r$. Allora $e_r \in I \subseteq J$ e, poiché J è un ideale, si ha che anche $e_r + g^2$ appartiene J. Ma, come si constata subito, $e_r + g^2$ non assume mai valore 0, ed è quindi un elemento invertibile di $\mathbb{R}^{\mathbb{R}}$. Dunque J contiene un elemento invertibile e pertanto $J = \mathbb{R}^{\mathbb{R}}$. Questo prova che J è un ideale massimale.

L'esempio di sopra non è un dominio d'integrità. Vediamo cosa succede in $\mathbb{Z}$:

Proposizione 7.8. *Gli ideali massimali di $\mathbb{Z}$ sono tutti e soli gli insiemi del tipo $p\mathbb{Z}$ con p un numero primo.*

Dimostrazione. Sia p un numero primo. Allora $p\mathbb{Z}$ è un ideale proprio di $\mathbb{Z}$. Sia ora $n\mathbb{Z}$ (con $n \geq 1$) un altro ideale di $\mathbb{Z}$ contenente $p\mathbb{Z}$. Allora, per la Proposizione 7.1, n divide p. Ne consegue che $n = 1$ oppure $n = p$. Nel primo caso $n\mathbb{Z} = \mathbb{Z}$, e nel secondo $n\mathbb{Z} = p\mathbb{Z}$. Dunque i soli ideali di $\mathbb{Z}$ che contengono $p\mathbb{Z}$ sono $\mathbb{Z}$ e lo stesso $p\mathbb{Z}$; quindi $p\mathbb{Z}$ è un ideale massimale.
Viceversa sia $m\mathbb{Z}$ (con $m \geq 1$) un ideale massimale di $\mathbb{Z}$. In particolare $m\mathbb{Z} \neq \mathbb{Z}$ e quindi $m \neq 1$. Supponiamo che q sia un divisore primo di m. Allora, per la Proposizione 7.1, $m\mathbb{Z} \subseteq q\mathbb{Z}$. Siccome $m\mathbb{Z}$ è massimale, e $q\mathbb{Z} \neq \mathbb{Z}$, deve essere $q\mathbb{Z} = m\mathbb{Z}$. Ma allora $m|q$, e dunque $m = q$, che è un numero primo. ∎

Segue dalle proposizioni precedenti che nell'anello $\mathbb{Z}$ l'insieme degli ideali primi diversi da (0) coincide con quello degli ideali massimali. Come vedremo nella prossima sezione, questa è una proprietà che vale in ogni dominio a ideali principali, ma non in generale nei domini d'integrità.
C'è comunque una relazione tra ideali primi e ideali massimale che sussiste in ogni anello commutativo.

Proposizione 7.9. *Sia R un anello commutativo. Allora ogni ideale massimale di R è un ideale primo.*

Dimostrazione. Sia I un ideale massimale dell'anello commutativo R. Allora $I \neq R$ per definizione. Siano $a, b \in R$ tali che $ab \in I$, e supponiamo che $b \notin I$. Allora l'ideale (b) non è contenuto in I, e quindi l'ideale $(b) + I$ contiene propriamente I. Poiché I è massimale, si ha quindi $R = (b) + I$. In particolare, esistono $x \in R$ e $y \in I$ tali che $1 = bx + y$. Quindi $a = a(bx + y) = (ab)x + ay$ appartiene ad I. Dunque, I è un ideale primo. ∎

Questa Proposizione in genere non si inverte. Esempi banali si trovano considerando domini d'integrità che non siano campi (ad esempio, $\mathbb{Z}$): in tali casi l'ideale nullo $\{0\}$ è primo ma non è massimale. Per degli esempi riferiti ad ideali non nulli si vedano gli esercizi 7.6 e 7.21 (in questi esercizi l'anello non è un dominio d'integrità; esempi in domini d'integrità in cui esistono ideali primi che non sono massimali, li vedremo nel prossimo capitolo).

Ricordo che un dominio d'integrità si dice **Dominio a Ideali Principali** (abbreviato PID) se ogni suo ideale è principale; ovvero se per ogni ideale I di R esiste un elemento $a \in I$ tale che $I = (a)$. Con la prossima proposizione vediamo come la Proposizione 7.8 si estenda ad un PID.

Proposizione 7.10. *Sia R un dominio a ideali principali, e sia $0 \neq a \in R$. Allora a è un elemento irriducibile se e solo se (a) è un ideale massimale di R.*

Dimostrazione. Sia a un elemento irriducibile del dominio a ideali principali R. Allora a non è invertibile e quindi (a) è un ideale proprio di R. Sia J ideale di R con $(a) \subseteq J$. Poichè ogni ideale di R è principale, esiste $b \in R$ tale che $J = (b)$. Per la Proposizione 7.1, $b|a$. Poichè a è irriducibile si ha che b è associato ad a oppure è un invertibile. Nel primo caso $(b) = (a)$, nel secondo caso $(b) = R$. Quindi (a) è un ideale massimale.

Viceversa, supponiamo che per un $0 \neq a \in R$ sia (a) ideale massimale di R e proviamo che a è irriducibile. a non è invertibile perchè (a) è un ideale proprio. Sia $b \in R$ un divisore di a. Allora per la Proposizione 7.1, $(a) \subseteq (b)$. Poichè (a) è massimale si ha $(b) = (a)$ oppure $(b) = R$. Nel primo caso $b \sim a$, e nel secondo caso b è invertibile. Quindi a è un irriducibile. ∎

Esercizio 7.6. Sia $A = \mathbb{Z}^{\mathbb{R}}$ l'anello delle applicazioni da $\mathbb{R}$ in $\mathbb{Z}$. Si provi che

$$I = \{f \in \mathbb{Z}^{\mathbb{R}} \mid f(0) = 0\}$$

è un ideale primo, ma non massimale di A.

Esercizio 7.7. Ricordo che un elemento a di un anello R si dice *nilpotente* se esiste un intero $n \geq 1$ (che dipende da a) tale che $a^n = 0_R$. Si provi che se R è un anello commutativo, allora gli elementi nilpotenti di R sono contenuti nell'intersezione di tutti gli ideali primi di R.

Esercizio 7.8. Sia R un anello commutativo e sia

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ I_3 \subseteq \ \cdots$$

una catena (infinita) di ideali primi di R. Si provi che $\bigcup_{i \in \mathbb{N}} I_i$ è un ideale primo di R.

Esercizio 7.9. Sia I un ideale proprio dell'anello commutativo R. Si dimostri che I è massimale se e solo se per ogni a $\in R \setminus I$ esiste $x \in R$ tale che $1 - ax \in I$.

Esercizio 7.10. Sia $\phi : A \to B$ un omomorfismo di anelli commutativi.

(a) Si provi che se J è un ideale primo di B, allora $\phi^{-1}(J)$ è un ideale primo di A.

(b) Si provi che se ϕ è suriettivo e I è un ideale massimale di A, allora $\phi(I) = B$ oppure $\phi(I)$ è un ideale massimale di B.

Esercizio 7.11. Sia $n \geq 2$. Si provi che gli ideali primi di $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ sono massimali.

7.3. Domini a Ideali Principali

Vediamo subito il risultato fondamentale di questa sezione.

Teorema 7.11. *Ogni Dominio a Ideali principali è un dominio a Fattorizzazione Unica.*

Dimostrazione. Sia R un PID. Proviamo che R soddisfa le condizioni (1) e (2) del Lemma 7.4.

(1) Siano $a_0, a_1, a_2, \ldots$ elementi di R tali che, per ogni i, a_{i+1} è un divisore proprio di a_i. Allora, per la Proposizione 7.1, in R c'è la catena di ideali

$$(a_0) \subset (a_1) \subset (a_2) \subset (a_3) \subset \ \ldots$$

in cui ogni inclusione è propria. Sia

$$I = \bigcup_i (a_i) \ .$$

Si verifica facilmente che I è un ideale di R. (Inoltre $I \neq R$; infatti se fosse $I = R$, allora $1_R \in (a_i)$ per qualche i, il che implica $(a_i) = R$, quindi a_i è invertibile, contro l'assunzione che sia un divisore proprio di a_{i-1}).
Poiché R è un PID, esiste un elemento $b \in R$ non invertibile tale che $I = (b)$. Ora, $b \in (b) = \bigcup_i (a_i)$ e quindi $b \in (a_n)$ per qualche n, che comporta $I = (a_n)$, e dunque la catena si arresta con a_n.

(2) Sia a un elemento irriducibile di R. Allora, per la Proposizione 7.10, (a) è un ideale massimale di R, e quindi per la Proposizione 7.9, (a) è un ideale primo. Per la Proposizione 7.7, si conclude che a è un elemento primo.

Per il Teorema 7.5, R è dunque un dominio a fattorizzazione unica. ∎

Domini Euclidei. La nozione di dominio euclideo fornisce un metodo operativo per provare (quando funziona) che certi anelli sono domini a ideali principali;

Un dominio d'integrità R si dice *Dominio Euclideo* se esiste una applicazione

$$\delta : R \setminus \{0\} \ \to \ \mathbb{N}$$

(detta *valutazione euclidea*) con la seguente proprietà:

per ogni $a, b \in R,\ b \neq 0$ esistono $q, r \in R$ tali che

$$\begin{array}{ll} \text{(i)} & a = qb + r \\ \text{(ii)} & r = 0 \quad \text{oppure} \quad \delta(r) < \delta(b) \ . \end{array}$$

(osserviamo che non richiediamo l'unicità di q, r).

È un dominio euclideo l'anello $\mathbb{Z}$, con valutazione $\delta(z) = |z|$ per ogni $z \in \mathbb{Z} \setminus \{0\}$. La dimostrazione che $\mathbb{Z}$ è un dominio a ideali principali è stata possibile proprio utilizzando la divisione "con resto". Un argomento analogo funziona per i domini euclidei in generale (ed è il motivo per cui questo concetto è stato introdotto).

Teorema 7.12. *Ogni Dominio Euclideo è un Dominio a Ideali Principali.*

Dimostrazione. Come detto, la dimostrazione ricalca quella data per $\mathbb{Z}$ (Teorema 5.9), sostituendo al valore assoluto la generale valutazione euclidea.
Sia quindi R un dominio euclideo e δ una sua valutazione. Sia I un ideale di R. Se I è banale, allora $I = (0_R)$. Supponiamo pertanto $\{0_R\} \neq I$. Allora l'insieme $S = \{\delta(a) \mid 0_R \neq a \in I\}$ è un sottoinsieme non vuoto di $\mathbb{N}$, che ha dunque un minimo. Sia $b \in I$ tale che $\delta(b) = \min S$. Proviamo che $I = (b)$. Un'inclusione ($(b) \subseteq I$) è ovvia. Sia quindi $a \in I$. Per la proprietà euclidea, esistono $q, r \in R$ tali che $a = qb + r$, e $\delta(r) < \delta(b)$ oppure $r = 0_R$.
Ma $r = a - qb \in I$, e quindi, per la scelta di b, non può essere $\delta(r) < \delta(b)$. Dunque, $r = 0_R$, e pertanto $a = qb \in (b)$. Ciò prova che $I \subseteq (b)$, e dunque che $I = (b)$

(osserviamo ancora che b è un elemento non nullo di I con *valutazione minima* tra gli elementi di I). ∎

Osservazione. Non tutti i domini a ideali principali sono domini euclidei. Questo è piuttosto difficile da provare: infatti per stabilire che un certo dominio a ideali principali A non è euclideo, occorre provare che non ammette valutazioni euclidee, ovvero che *qualsiasi* applicazione $A \setminus \{0\} \to \mathbb{N}$ non soddisfa la proprietà richesta (il che, si intuisce, non è facile). Un esempio di PID che non è euclideo è l'anello $\mathbb{Z}[(1+\sqrt{-19})/2]$ (mentre $\mathbb{Z}[\sqrt{-19}]$ non è neppure un PID).

Massimo comun divisore. Abbiamo già osservato che in un dominio a fattorizzazione unica A, esiste sempre il massimo comun divisore tra due elementi. Se inoltre A è un dominio a ideali principali, allora le proprietà del M.C.D. assomigliano molto a quelle per i numeri interi. Infatti, siano a, b elementi di un dominio a ideali principali A, e sia d un loro M.C.D. Allora, $d|a$ e $d|b$ e dunque, per la Proposizione 7.1, $(a) \subseteq (d)$ e $(b) \subseteq (d)$; quindi $(a)+(b) \subseteq (d)$. Ora, $(a)+(b)$ è un ideale di A (è l'ideale generato da $\{a, b\}$); poiché A è un P.I.D. esiste $c \in A$ tale che $(a)+(b) = (c)$. Dunque $(c) \subseteq (d)$; sempre per la Proposizione 7.1, $c|a$ e $c|d$, e dunque (per la definizione di massimo comun divisore) $c|d$, ovvero $(d) \subseteq (c)$. Quindi $(c) = (d)$, dunque $(d) = (a) + (b)$, e pertanto concludiamo che *esistono* $\alpha, \beta \in A$ *tali che* $d = a\alpha + b\beta$. In particolare a e b sono coprimi se e soltanto se esistono $\alpha, \beta \in A$ tali che $1_A = a\alpha + b\beta$ (il che equivale a dire $(a) + (b) = A$).

Se inoltre A è un dominio euclideo, allora il calcolo di un MCD di due elementi non nulli può essere effettuato mediante l'algoritmo di Euclide, in modo del tutto analogo a come si opera per calcolare il MCD di due numeri interi (vedremo un'importante istanza di ciò con gli anelli di polinomi nel prossimo capitolo).

Esercizio 7.12. Sia R un PID, e $\{0\} \neq I$ un ideale di R. Si provi che I è ideale primo se e solo se è un ideale massimale.

Esercizio 7.13. Ogni campo è un dominio euclideo. Rispetto a quale valutazione?

Esercizio 7.14. Si provi che $\mathbb{Z}[\sqrt{2}]$ è un dominio euclideo.

Esercizio 7.15. Sia R un dominio a ideali principali, e sia $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$ una catena infinita discendente di ideali di R. Si provi che $\bigcap_{n\in\mathbb{N}} I_n = (0)$.

7.4. Interi di Gauss.

L'anello degli interi di Gauss è un esempio molto interessante di dominio euclideo, che ha diverse applicazioni, cui però noi accenneremo soltanto. Questa sezione, che non è essenziale per la comprensione del resto del corso, può essere considerata una lettura o un'esercitazione svolta. L'abbiamo inserita perché l'argomento è interessante, e perché ci consente di tirare a cinque anche le sezioni di questo capitolo.

L'anello degli interi di Gauss è l'insieme

$$\mathbb{Z}[i] = \{\ u + iv \mid u, v \in \mathbb{Z}\ \}.$$

$\mathbb{Z}[i]$ è un sottoanello dell'anello $\mathbb{C}$ (vedi esercizio 5.26), ed è quindi un dominio d'integrità. Proviamo che è un dominio euclideo, usando come valutazione la restrizione

ad esso del quadrato del modulo sui complessi, ovvero la *norma* definita da, per ogni $z = u + vi \in \mathbb{Z}[i]$

$$\delta(z) = z\overline{z} = (u + iv)(u - iv) = u^2 + v^2 \ .$$

Si verifica facilmente che $\delta(zz_1) = \delta(z)\delta(z_1)$ per ogni $z, z_1 \in \mathbb{Z}[i]$.

Teorema 7.13. *L'anello $\mathbb{Z}[i]$ degli interi di Gauss è un dominio euclideo; quindi è un PID.*

Dimostrazione. Siano $a, b \in \mathbb{Z}[i]$, con $b \neq 0$. Ora $ab^{-1} \in \mathbb{Q}[i]$ dunque $ab^{-1} = \alpha + \beta i$ con $\alpha, \beta \in \mathbb{Q}$. Quindi esistono numeri interi u, v con

$$|\alpha - u| \leq \frac{1}{2} \ , \qquad |\beta - v| \leq \frac{1}{2} \ .$$

Posto $\epsilon = \alpha - u, \ \eta = \beta - v$ si ha

$$a = b((u + \epsilon) + (v + \eta)i = b(u + vi) + b(\epsilon + \eta i) = bq + r$$

con $q = u + vi \in \mathbb{Z}[x]$ e $r = b(\epsilon + \eta i) = a - bq \in \mathbb{Z}[i]$. Inoltre, se $r \neq 0$

$$\delta(r) = \delta(b)(\epsilon^2 + \eta^2) \leq \frac{1}{2}\delta(b)$$

provando quindi che $\mathbb{Z}[i]$ è un dominio euclideo. ∎

L'anello degli interi di Gauss è utile in diverse applicazioni alla teoria dei numeri. Vediamo un esempio.

Proposizione 7.14. *a) Sia p un numero primo tale che $p \equiv 1 \ (mod\, 4)$; allora esiste un intero z tale che $z^2 \equiv -1 \ (mod\, p)$.*

b) Un numero primo positivo p si può scrivere come somma $p = a^2 + b^2$ dei quadrati di due interi a, b se e solo se $p = 2$ o $p \equiv 1 \ (mod\, 4)$.

Dimostrazione. a) Sia p un primo tale che $4|(p-1)$, e sia $s \in \mathbb{N}$ tale che $p - 1 = 4s$. L'affermazione a) equivale a provare che il polinomio $x^2 + \overline{1}$ ammette radici nel campo $\mathbb{Z}/p\mathbb{Z}$. Sia $\overline{a}$ un elemento non nullo di $\mathbb{Z}/p\mathbb{Z}$; allora, per il teorema di Fermat, $\overline{a}^{4s} = \overline{1}$, e quindi $\overline{a}^{2s}$ è radice di $x^2 - \overline{1}$. Siccome $\mathbb{Z}/p\mathbb{Z}$ è un campo (e $p \neq 2$), le radici di quest'ultimo polinomio sono solo due (vedi, più avanti, il Teorema 8.9), e sono $\pm\overline{1}$. Ancora, le radici di $x^{2s} - \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}$ sono al più $2s$. Siccome $2s < p - 1$, ciò implica che esiste $\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$, tale che $\overline{a}^{2s} \neq \overline{1}$. Per quanto osservato sopra, deve essere pertanto $\overline{a}^{2s} = -\overline{1}$, e quindi $\overline{a}^s$ è radice del polinomio $x^2 + \overline{1}$, ovvero $(a^s)^2 \equiv -1$ $(mod\ p)$.

b) Supponiamo $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$ e p dispari. Allora a e b non possono essere entrambi pari o entrambi dispari e quindi possiamo supporre $a = 2h$, $b = 2k + 1$, con $h, k \in \mathbb{Z}$. Segue $a^2 \equiv 0 \ (mod\ 4)$ e $b^2 = 4k^2 + 4k + 1 \equiv 1 \ (mod\ 4)$ e dunque $p \equiv 1$ $(mod\ 4)$.

Proviamo ora l'implicazione inversa. Possiamo supporre, dato che evidentemente $2 = 1^2 + 1^2$, che sia $p \equiv 1 \ (mod\ 4)$. Per il punto a) esiste dunque un intero z tale che $p|(z^2 + 1)$. Dunque, in $\mathbb{Z}[i]$, $p|z^2 + 1 = (z + i)(z - i)$ e quindi p non può essere un elemento primo in $\mathbb{Z}[i]$, poiche' un intero di Gauss e' divisibile per $n \in \mathbb{Z}$ se e solo se ha parte reale ed immaginaria divisibili per n. Dunque p non è irriducibile in $\mathbb{Z}[i]$ ed esistono $\alpha, \beta \in \mathbb{Z}[i]$, α, β non invertibili, tali che $p = \alpha\beta$. Segue $p^2 = \delta(p) = \delta(\alpha)\delta(\beta)$ e, osservando che $\delta(\alpha)$ e $\delta(\beta)$ sono interi > 1 (poiche' α e β non sono invertibili),

abbiamo $\delta(\alpha) = \delta(\beta) = p$. Pertanto, se $\alpha = a + ib$ con $a, b \in \mathbb{Z}$, concludiamo $\delta(\alpha) = a^2 + b^2 = p$. ∎

Con argomenti simili possiamo provare il seguente risultato.

Lemma 7.15. *Sia $\pi \in \mathbb{Z}[i]$. Allora, π è un primo di $\mathbb{Z}[i]$ se e solo se una delle seguenti condizioni è soddisfatta.*

i) *$\pi \sim p$ con p intero primo, $p \equiv 3$ (mod 4);*

ii) *$\delta(\pi) = p$ con p intero primo, $p = 2$ o $p \equiv 1$ (mod 4)*

Dimostrazione. Sia $\pi = a + ib$ un primo di $\mathbb{Z}[i]$. Osserviamo che $\delta(\pi) = \pi\overline{\pi}$ è un intero > 1 e quindi esistono $p_1, p_2, \ldots, p_h \in \mathbb{Z}$, p_i primi in $\mathbb{Z}$, tali che $\pi\overline{\pi} = p_1 p_2 \ldots p_h$. Ma π è primo in $\mathbb{Z}[i]$ e quindi $\pi | p$ per un $p = p_i$, ovvero $p = \pi\alpha$ con $\alpha \in \mathbb{Z}[i]$. Segue $\delta(\pi)|\delta(p) = p^2$. Dato che $1 \neq \delta(\pi) \in \mathbb{N}$, abbiamo due possibillità: i) $\delta(\pi) = a^2 + b^2 = p$; oppure ii) $\delta(\pi) = p^2$. Nel caso ii), da $p = \pi\alpha$, segue $p^2 = \delta(p) = \delta(\pi)\delta(\alpha) = p^2\delta(\alpha)$ e quindi $\delta(\alpha) = 1$ e α e' un'unità, ovvero $\pi \sim p$. In particolare, p è primo e quindi irriducibile in $\mathbb{Z}[i]$ e quindi $p \neq 2 = (1+i)(1-i)$ e $p \not\equiv 1$ (*mod* 4), dato che altrimenti per la Proposizione 7.14 avremmo $p = x^2+y^2 = (x+iy)(x-iy)$ per $x+iy, x-iy \in \mathbb{Z}[i]$ non invertibili. Pertanto se π è un primo di $\mathbb{Z}[i]$ allora

i) $\pi \sim p$ con p intero primo, $p \equiv 3$ (*mod* 4) oppure

ii) $\delta(\pi) = p$ con p intero primo, $p = 2$ o $p \equiv 1$ (*mod* 4).

Sia, viceversa, $\pi \in \mathbb{Z}[i]$ tale che valgano i) o ii). Se $\delta(\pi)$ è un primo allora si verifica subito, per la moltiplicatività della valutazione, che π è irriducibile. Sia quindi $\pi \sim p$ con p intero primo, $p \equiv 3$ (*mod* 4) e supponiamo π riducibile. Allora anche p è riducibile e $p = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[i]$ non invertibili. Segue $p^2 = \delta(p) = \delta(\alpha)\delta(\beta)$ e, poichè $1 < \delta(\alpha), \delta(\beta) \in \mathbb{N}$, concludiamo $\delta(\alpha) = p$. Quindi $p = x^2 + y^2$ per opportuni $x, y \in \mathbb{Z}$ e, ancora per la Proposizione 7.14, abbiamo la contraddizione $p = 2$ oppure $p \equiv 1$ (*mod* 4). Pertanto, $\pi \in \mathbb{Z}[i]$ è primo se e solo se valgono i) o ii).
Osserviamo infine che se vale i) π è un numero reale od un immaginario puro, mentre se vale ii) allora $Re(\pi) \neq 0 \neq Im(\pi)$. ∎

Esercizio 7.16. Si fattorizzi $12 + 22i$ come prodotto di elementi irriducibili di $\mathbb{Z}[i]$.

Esercizio 7.17. Trovare un MCD di $5 + 10i$ e $80 + 70i$ in $\mathbb{Z}[i]$

7.5. Esercizi.

Esercizio 7.18. Sia A un dominio d'integrità in cui per ogni $a, b \in A \setminus \{0_A\}$, a è associato a b. Si provi che A è un campo.

Esercizio 7.19. Sia A un dominio d'integrità in cui ogni elemento non nullo è irriducibile o invertibile. Si provi che A è un campo.

Esercizio 7.20. Si provi che nell'anello $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ non esiste massimo comun divisore di 4 e $2 + 2\sqrt{-3}$.

Esercizio 7.21. Si consideri l'anello $\mathbb{Z} \times \mathbb{Z}$ (le operazioni sulle componenti). Sia $P = \{(\mathrm{a}, 0) \mid \mathrm{a} \in \mathbb{Z}\}$; si dimostri che P è un ideale primo di $\mathbb{Z}$x$\mathbb{Z}$.

Esercizio 7.22. Siano A e B ideali dell'anello R, e sia

$$I = \{\ r \in R \mid ar \in B \ \text{ per ogni } a \in A\ \}\ .$$

Si provi che se B è un ideale massimale e $A \not\subseteq B$, allora $I = B$.

Esercizio 7.23. Determinare gli ideali massimali dell'anello $\mathbb{R} \times \mathbb{R}$.

Esercizio 7.24. Si determini l'intersezione degli ideali massimali dell'anello $\mathbb{Z}_{24}$.

Esercizio 7.25. Sia $n \geq 2$. Si provi che l'intersezione degli ideali massimali di $\mathbb{Z}_n$ è $\{0\}$ se e soltanto se n è un prodotto di primi distinti. In tal caso, quali sono gli elementi nilpotenti di $\mathbb{Z}_n$?

Esercizio 7.26. Siano I e K ideali dell'anello commutativo A, e sia $a \in A$ un elemento fissato. Definiamo

$$I_{(K,a)} = \{\ x \in I \mid xa \in K\ \}\ .$$

(a) Si provi che $I_{(K,\,a)}$ è un ideale di A.

(b) Nell'anello $\mathbb{Z}$ si determini (cioè se ne trovi un generatore), l'ideale $3\mathbb{Z}_{(4\mathbb{Z},\,2)}$.

(c) Sia A un dominio a ideali principali, sia I un ideale di A, e sia $K = (c)$ un ideale massimale. Si provi che $I_{(K,\,a)} = I$ se e solo se $I \subseteq K$ o $a \in K$.

Esercizio 7.27. Sia $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$. Si provi che $\mathbb{Z}[\sqrt{10}]$ è un anello, e si provi che l'ideale $(2, \sqrt{10})$ di $\mathbb{Z}[\sqrt{10}]$ è un ideale primo.

Esercizio 7.28. Sia R un dominio d'integrità a fattorizzazione unica, e sia $0_R \neq a \in R$ un elemento non invertibile di R.

a) Si provi che il numero di ideali principali di R contenenti l'ideale (a) è finito.

b) Si provi che

$$\bigcap_{n \in \mathbb{N}} (a^n) = \{0_r\}.$$

Esercizio 7.29. Si provi che non esiste alcun omomorfismo d'anelli da $\mathbb{Z}[\sqrt{-5}]$ in $\mathbb{Z}$.

Esercizio 7.30. Si provi che l'insieme di matrici

$$A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

è un sottoanello commutativo dell'anello $M_2(\mathbb{R})$ delle matrici quadrate di ordine due sui reali. Si provi che

$$H = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

è un ideale massimale di A.

Esercizio 7.31. Sia R un anello commutativo e siano K, Y ideali primi di R. Si dimostri che $K \cap Y$ é un ideale primo di R se e solo se $K \supseteq Y$ oppure $Y \supseteq K$.

Esercizio 7.32. Sia R un anello commutativo in cui ogni ideale principale diverso da R è un ideale primo. Si provi che R Ŕ un campo.

Esercizio 7.33. Provare che nell'anello $\mathbb{Z}[\sqrt{-7}]$ l'elemento 2 è irriducibile ma non primo.

Esercizio 7.34. Sia $R = \mathbb{Z}[\sqrt{-6}]$. Si provi che 1 è un massimo comun divisore di $a = 5$ e $b = 2 + \sqrt{-6}$, ma non appartiene all'ideale $(a) + (b)$.

Esercizio 7.35. Siano $\alpha = 12+21i$, $\beta = 25+10i$, $\gamma = 3-i$, $\delta = 3+24i$ e $I = (\alpha, \beta)$, $J = (\gamma, \delta)$ gli ideali di $\mathbb{Z}[i]$ generati rispettivamente da α e β, e da γ e δ. Si provi che $I = J$.

Esercizio 7.36. Si provi che i seguenti sottoinsiemi di $\mathbb{Z}[\sqrt{-5}]$ sono ideali

$$A = \{\ z \in \mathbb{Z}[\sqrt{-5}] \mid 2 \text{ divide } N(z)\ \}, \qquad B = \{\ z \in \mathbb{Z}[\sqrt{-5}] \mid 5 \text{ divide } N(z)\ \}$$

e si dica quali fra essi è principale.

Esercizio 7.37. Siano $\mathbb{C}$ il campo dei numeri complessi, e $\mathbb{Z}$ l'anello degli interi. Sia quindi $A = \mathbb{C} \times \mathbb{Z}$ l'anello prodotto diretto. Definiamo,

$$C = \{(x, 0) \in A \mid x \in \mathbb{C}\} \qquad Z = \{(0, y) \in A \mid y \in \mathbb{Z}\}\ .$$

(a) Si provi che C e Z sono ideali di A.

(b) Si dica se Z è un ideale massimale di A.

(c) Sia I un ideale di A. Si provi che $C \subseteq I$ oppure $I \subseteq Z$.

Esercizio 7.38. Sia R un anello commutativo di caratteristica 2, e sia dato un ideale I di R. Si ponga $K(I) = \{x \in R \mid x^2 \in I\}$. Si dimostri che:

(i) $K(I)$ è ideale di R.

(ii) Se I è un ideale primo allora $K(I) = I$.

Esercizio 7.39. (a) Sia $\mathbb{P}$ l'insieme dei numeri primi positivi. Si provi che

$$\bigcap_{p \in \mathbb{P}} p\mathbb{Z} = \{0\}\ .$$

(b) Sia A un P.I.D. e sia $\mathcal{M}$ la famiglia di tutti gli ideali massimali di A. Si provi che, se $\mathcal{M}$ è infinita,

$$\bigcap_{I \in \mathcal{M}} I = \{0_A\}\ .$$

Esercizio 7.40. Sia S un sottoinsieme moltiplicativamente chiuso di un anello commutativo A, e tale che $0 \notin S$, Sia I un ideale di A tale che I è massimale tra gli ideali di A che hanno intersezione vuota con S (ovvero: $I \cap S = \emptyset$ e se J è ideale di A con $I \subseteq J$ e $I \neq J$, allora $J \cap S \neq \emptyset$). Si provi che I è un ideale primo di A.

Esercizio 7.41. Sia p un numero primo, e sia

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \text{ non divide } b \right\}.$$

Si provi che $\mathbb{Q}_p$ è un anello locale, ovvero che esiste un ideale (massimale) J di $\mathbb{Q}_p$ che contiene ogni ideale proprio di $\mathbb{Q}_p$.

Esercizio 7.42. Sia A un anello commutativo, e sia I un suo ideale. Si pone

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ per qualche } n \in \mathbb{N}\}.$$

(a) Si provi che $\sqrt{I}$ è un ideale di A, e che $\sqrt{\sqrt{I}} = \sqrt{I}$.

(b) Si provi che se I è un ideale primo, allora $\sqrt{I} = I$.

Esercizio 7.43. (Ideali primari, I) Un ideale P di un anello commutativo A si dice *primario* se $P \neq A$ e per ogni $a, b \in A$

$$\begin{cases} ab \in P \\ a \notin P \end{cases} \quad \Rightarrow \quad b^n \in P \text{ per qualche } n \geq 1.$$

Si descrivano tutti gli ideali primari dell'anello $\mathbb{Z}$.

Esercizio 7.44. (Ideali primari, II) (1) Sia A un PID e I un ideale di A; si provi che I è un ideale primario se e solo se esiste un elemento irriducibile $a \in A$ ed un intero $n \geq 1$, tali che $I = (a^n)$.

(2) Si provi che in un PID ogni ideale non nullo è l'intersezione di un numero finito di ideali primari.

Esercizio 7.45. (Anelli noetheriani, I) Un anello commutativo A si dice *noetheriano* (da Emmy Noether, 1882–1935) se ogni catena di ideali $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ con $I_i \neq I_j$, è finita. Si provi che ogni PID è un anello noetheriano.

Esercizio 7.46. (Anelli noetheriani, II) Sia A un anello commutativo. Si provi che le seguenti condizioni sono equivalenti.

(1) A è noetheriano;

(2) ogni insieme di ideali di A ammette elementi massimali (rispetto alla relazione d'inclusione):

(3) ogni ideale di A è finitamente generato.

Esercizio 7.47. (Anelli noetheriani, III) Siano A e B anelli noetheriani. Si provi che il prodooto diretto $A \times B$ è un anello noetheriano.

8

Polinomi

8.1. Definizioni.

Sia R un anello commutativo. Un **polinomio** a coefficienti in R nell'*indeterminata* x è una espressione del tipo

$$a_0 + a_1x + a_2x^2 + \ \ldots\ + a_nx^n$$

dove n è un numero naturale, $a_0, a_1, a_2, \ldots, a_n$ sono elementi di R (appunto, i *coefficienti* del,polinomio), ed x è un simbolo (detto indeterminata) "indipendente" dagli elementi di R.
L'insieme di tutti i polinomi a coefficienti in R nell'indeterminata x si denota con $R[x]$.(Questa definizione non è del tutto formale; daremo una costruzione rigorosa di $R[x]$ alla fine della sezione, nella quale anche la misteriosa indeterminata x avrà un significato formalmente preciso).

Due polinomi $a_0 + a_1x + \ \ldots\ + a_nx^n$ e $c_0 + c_1x + \ \ldots\ + c_mx^m$ a coefficienti in R sono **uguali** se $a_i = b_i$ per ogni $i \geq 0$; con la convenzione che i coefficienti non scritti sono uguali a zero (cioè $a_i = 0$ per ogni $i > n$ e $c_i = 0$ per ogni $c_i > m$; in particolare confrontando due polinomi possiamo sempre supporre $n = m$).
Un'altra convenzione familiare è che scrivendo semplicemente x^n si intende 1_Rx^n.
Ogni elemento di R è un polinomio, quindi $R \subseteq R[x]$. Abitualmente, indicheremo i polinomi con lettere $f, g, h, \ldots$

Sull'insieme dei polinomi $R[x]$ si definiscono somma e prodotto nel modo seguente (che è la generalizzazione di quello familiare nel caso di polinomi a coefficienti reali). Quindi, se

$$f = a_0 + a_1x + a_2x^2 + \ \ldots\ + a_nx^n \quad \text{e} \quad g = c_0 + c_1x + c_2x^2 + \ \ldots\ + c_mx^m$$

sono polinomi a coefficienti in R, con $n \geq m$, si pone

$$f + g = (a_0 + c_0) + (a_1 + c_1)x + (a_2 + c_2)x^2 + \ \ldots\ + (a_n + c_n)x^n$$

(dove abbiamo eventualmente aggiunto coefficienti $c_i = 0$ per $i > m$), e

$$fg = d_0 + d_1x + d_2x^2 + \ \ldots\ + d_{n+m}x^{n+m}$$

dove, per ogni $0 \leq i \leq n + m$

$$d_i = \sum_{r=0}^{i} a_r c_{i-r} \ .$$

Potete constatare da soli che queste sono le operazioni sui polinomi che vi sono già familiari dalle scuole superiori. Inoltre si verifica che con tali operazioni l'insieme $R[x]$ è un anello in cui zero e identità sono, rispettivamente, 0_R e 1_R. $R[x]$ si chiama **l'anello dei polinomi** nell'indeterminata x a coefficienti in R, e chiaramente contiene R come sottoanello (in particolare, *la caratteristica di $R[x]$ coincide con la caratteristica di R*).

Se f è un polinomio (a coefficienti in un anello commutativo) e $f \neq 0$, conveniamo di scrivere

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

con $a_n \neq 0$. Il numero naturale n è detto allora **grado** del polinomio f e si denota con $\deg f$; osserviamo in particolare che $\deg f = 0$ se e solo se $f \in R \setminus \{0\}$. Il termine a_n è detto **coefficiente direttivo** di $f \neq 0$ (mentre a_0 e detto "termine noto"); conveniamo che il coefficiente direttivo del polinomio nullo è 0). Ancora, $0 \neq f \in R[x]$. si dice **monico** se il suo coefficiente direttivo è 1_R.
Le seguenti proprietà sono di immediata verifica, che lasciamo per esercizio.

Proposizione 8.1. *Siano $f, g \in R[x] \setminus \{0_R\}$.*

(1) *se $f + g \neq 0$ allora $\deg(f + g) \leq \max\{\deg f, \deg g\}$;*

(2) *se $fg \neq 0$ allora $\deg(fg) \leq \deg f + \deg g$;*

(3) *se R è un dominio d'integrità allora $fg \neq 0$ e $\deg(fg) = \deg f + \deg g$.*

Osserviamo che l'uguaglianza al punto (2) può non sussistere se R non è un dominio d'integrità; ad esempio, in $(\mathbb{Z}/6\mathbb{Z})[x]$: $(\overline{2}x + \overline{1})(\overline{3}x + \overline{1}) = \overline{6}x^2 + \overline{5}x + \overline{1} = \overline{5}x + \overline{1}$.

Esercizio 8.1. Siano $f, g \in R[x] \setminus \{0_R\}$. Si provi che se il coefficiente direttivo di almeno uno tra f e g è invertibile in R, allora $\deg(fg) = \deg f + \deg g$.

Dalla proposizione 8.1 seguono facilmente le prime importanti constatazioni a proposito delle proprietà generali degli anelli di polinomi.

Proposizione 8.2. *Sia R un dominio d'integrità. Allora*

(1) *$R[x]$ è un dominio d'integrità.*

(2) *Gli elementi invertibili di $R[x]$ sono tutti e soli gli elementi invertibili di R; in particolare, se F è un campo l'insieme degli elementi invertibili di $F[x]$ è $F \setminus \{0\}$.*

Dimostrazione. (1) Sia R un dominio d'integrità, e siano $f, g \in R[x]$ polinomi non nulli. Allora $\deg f \geq 0$ e $\deg g \geq 0$; quindi per il punto (2) della Proposizione precedente, $\deg(fg) = \deg f + \deg g \geq 0$, e dunque $fg \neq 0$. Quindi $R[x]$ è un dominio d'integrità.
(2) Sia R un dominio d'integrità, e sia f un elemento invertibile di $R[x]$. Allora esiste $g \in R[x]$ tale che $1 = fg$. Quindi, sempre per il punto (2) della Proposizione precedente

$$\deg f + \deg g = \deg(fg) = \deg(1) = 0$$

che forza $\deg f = \deg g = 0$, cioè $f, g \in R$ e di conseguenza f, g sono elementi invertibili di R. ∎

Sia R un sottoanello dell'anello commutativo S e sia $b \in S$. Sia $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ un polinomio in $R[x]$. Poichè i coefficienti a_i sono in particolare elementi di S, ha senso considerare la "sostituzione di x con b in f":

$$f(b) = a_0 + a_1b + a_2b^2 + \ \ldots \ + a_nb^n$$

che è un elemento di S.
Ora, si verifica facilmente che, fissato $b \in S$, l'applicazione

$$\begin{array}{rccc} \sigma_b : & R[x] & \longrightarrow & S \\ & f & \mapsto & f(b) \end{array}$$

è un omomorfismo di anelli, che si chiama *omomorfismo di sostituzione* per b.
L'immagine di σ_b si denota con $R[b]$; quindi

$$R[b] = \{\ f(b) \mid f \in R[x]\ \} = \{a_0 + a_1b + \cdots + a_nb^n \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in R\}.$$

Il nucleo di σ_b è

$$I_b = \ker(\sigma_b) = \{\ f \in R[x] \mid f(b) = 0\ \}\ .$$

Osservazione. Sia R un sottoanello dell'anello commutativo S, e sia b in S. Allora, $R[b]$ è il più piccolo sottoanello di S che contiene $R \cup \{b\}$ (ovvero ogni sottoanello di S che contiene R e b, contiene $R[b]$). Infatti $R[b]$ è un sottoanello di S poiché è immagine di un omomorfismo. Inoltre, è chiaro che ogni sottoanello di S che contiene b contiene anche tutte le potenze b^n con $n \in \mathbb{N}$. Dunque ogni sottoanello T di S che contiene $R \cup \{b\}$ contiene ogni elemento ab^n con $a \in R,\ n \in \mathbb{N}$, e quindi contiene anche ogni elemento del tipo

$$a_0 + a_1b + a_2b^2 + \ \ldots \ + a_nb^n$$

con $a_0, a_1, \ldots, a_n \in R$ e $n \in \mathbb{N}$. Dunque T contiene $R[b]$.

Gli omomorfismi di sostituzione sono un'applicazione particolare di quella che è chiamata la proprietà fondamentale degli anelli di polinomi, e che è descritta dal risultato che segue.

Teorema 8.3. (Principio di sostituzione). *Sia $\phi : R \to S$ un omomorfismo di anelli commutativi, sia $b \in S$, e sia $R[x]$ l'anello dei polinomi a coefficienti in R. Allora esiste uno ed un solo omomorfismo $\phi_b : R[x] \to S$ tale che*

$$\begin{cases} \phi_b(a) = \phi(a) \ \ \textit{per ogni} \ \ a \in R \\ \phi_b(x) = b. \end{cases}$$

Dimostrazione. Sia $\phi_b : R[x] \to S$ un omomorfismo che soddisfi le proprietà richieste nell'enunciato. Allora se $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, deve essere

$$\phi_b(f) = \phi_b(a_0) + \phi_b(a_1)\phi_b(x) + \cdots + \phi_b(a_n)\phi_b(x^n) = \phi(a_0) + \phi(a_1)b + \cdots + \phi(a_n)b^n.$$

Quindi, se esiste, ϕ_b è univocamente determinato. Vediamo ora che, effettivamente, ponendo per ogni $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$

$$\phi_b(f) = \phi(a_0) + \phi(a_1)b + \cdots + \phi(a_n)b^n$$

si ottiene un omomorfismo. E' chiaro che $\phi_b(1) = \phi(1) = 1_S$. Sia ora $g = c_0 + \cdots + c_mx^m \in R[x]$. La verifica che $\phi_b(f+g) = \phi_b(f) + \phi_b(g)$ è facile. Consideriamo quindi

il prodotto: $fg = \sum_{i=0}^{n+m} d_i x^i$, dove, per ogni $i = 1, 2, \ldots, n+m \ : \ d_i = \sum_{r=0}^{i} a_r c_{i-r}$; allora,

$$\phi_b(fg) = \phi_b\left(\sum_{i=0}^{n+m} d_i x^i\right) = \sum_{i=0}^{n+m} \phi(d_i) b^i$$

ora, per ogni $i = 1, 2, \ldots, n+m$:

$$\phi(d_i) = \phi\left(\sum_{r=0}^{i} a_r c_{i-r}\right) = \sum_{r=0}^{i} \phi(a_r)\phi(c_{i-r})$$

è proprio il coefficiente i-esimo (rispetto alle potenze di b) del prodotto in S

$$(\phi(a_0) + \phi(a_1)b + \cdots + \phi(a_n)b^n)(\phi(c_0) + \phi(c_1)b + \cdots + \phi(c_m)b^m)$$

dunque

$$\phi_b(fg) = \sum_{i=0}^{n+m} \phi(d_i) b^i = \phi_b(f)\phi_b(g) \ .$$

Quindi ϕ_b è un omomorfismo e la dimostrazione è completata. ∎

La situazione da cui siamo partiti (quella di un elemento b contenuto in un anello S che contiene R come sottoanello) è quindi un caso particolare di applicazione del principio di sostituzione. L'omomorfismo (di sostituzione) σ_b definito in quel caso è l'unica estensione a $R[x]$ dell'omomorfismo identico da R in S che manda x in b,

Vediamo un'altra applicazione. Sia $n \geq 2$, e consideriamo l'omomorfismo

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \to & (\mathbb{Z}/n\mathbb{Z})[x] \\ & a & \mapsto & \overline{a} \end{array}$$

dove, come consuetudine, $\overline{a} = a + n\mathbb{Z}$. Scegliendo $b = x \in (\mathbb{Z}/n\mathbb{Z})[x]$, per il principio di sostituzione possiamo concludere che esiste un unico omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}[x]$ che manda ogni $a \in \mathbb{Z}$ in $\overline{a}$ e x in x. Chiaramente tale omomorfismo è definito da, per ogni $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$,

$$f \mapsto \overline{f} = \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n \ .$$

Il polinomio $\overline{f} \in (\mathbb{Z}/n\mathbb{Z})[x]$ definito in questa maniera si chiama la *riduzione modulo* n del polinomio intero f e, come vedremo più avanti, risulta utile in molte circostanze. Ad esempio, la riduzione modulo 3 del polinomio $5 + 12x - 5x^2 + 7x^3 + 6x^4$ è

$$\overline{5} + \overline{12}x + \overline{-5}x^2 + \overline{7}x^3 + \overline{6}x^4 = \overline{2} + x^2 + x^3 \in \mathbb{Z}/3\mathbb{Z}[x] \ .$$

Costruzione formale dell'anello dei polinomi. Sia R un anello commutativo e consideriamo l'insieme di tutte le sequenze infinite

$$(a_0,\ a_1,\ a_2,\ a_3,\ \ldots\ldots) \qquad (*)$$

ad elementi $a_0, a_1, a_2, \ldots$ in R. Osserviamo che tale insieme può essere identificato con l'insieme $R^{\mathbb{N}}$ di tutte le applicazioni da $\mathbb{N}$ in R, facendo corrispondere alla sequenza $(a_0, a_1, a_2, a_3, \ \ldots)$ l'applicazione che ad ogni $n \in \mathbb{N}$ associa l'elemento a_n della sequenza.

Denotiamo con B il sottoinsieme costituito da tutte le sequenze "quasi ovunque nulle", cioè le sequenze che hanno un numero finito di termini a_i diversi da zero (che corrispondono alle

applicazioni f da $\mathbb{N}$ in R per le quali esiste un k tale che $f(i) = 0$ per ogni $i \geq k$). Su B definiamo una somma ponendo

$$(a_0, a_1, a_2, a_3, \dots) + (b_0, b_1, b_2, b_3, \ \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, \ \dots) \ .$$

Si verifica facilmente che rispetto a tale operazione B soddisfa gli assiomi (S1), (S2) e (S3) per gli anelli, con elemento neutro $0_B = (0, 0, 0, \dots)$.
Introduciamo quindi una moltiplicazione ponendo

$$(a_0, a_1, a_2, a_3, \dots)(b_0, b_1, b_2, b_3, \ \dots) = (c_0, c_1, c_2, c_3, \ \dots)$$

dove, per ogni $i \in \mathbb{N}$: $c_i = \sum_{r=0}^{i} a_r b_{i-r}$. (osserviamo che se $a_r = 0$ per $r \geq n$ e $b_s = 0$ per $s \geq m$ allora $c_i = 0$ per $i \geq n + m$ e quindi $(c_0, c_1, c_2, c_3, \ \dots) \in B$). Con un po' di lavoro, ma senza difficoltà, anche in questo caso si dimostra che rispetto a tale prodotto B soddisfa gli assiomi (P1) e (P2) di anello, con identità $1_B = (1, 0, 0, 0, \dots)$, e che è soddisfatta la proprietà distributiva del prodotto rispetto alla somma.
Quindi, con tali operazioni, B è un anello commutativo.
Consideriamo ora la applicazione $R \to B$ che ad ogni $a \in R$ associa $(a, 0, 0, \dots)$. Essa è un omomorfismo iniettivo di anelli; possiamo quindi identificare $(a, 0, 0, \dots)$ con l'elemento $a \in R$ e considerare R come sottoanello di B.
Poniamo ora $x = (0, 1, 0, 0, \dots)$. Allora, applicando la definizione di prodotto in B, e ragionando per induzione, si prova che per ogni $n \in \mathbb{N}$

$$x^n = (0, 0, \dots, 0, 1, 0, \dots)$$

con 1 al posto n. Da ciò segue che per ogni $a \in \mathbb{R}$

$$ax^n = (a, 0, 0, \dots)(0, 0, \dots, 0, 1, 0 \dots) = (0, 0, \dots, 0, a, 0 \dots)$$

con a al posto n. Quindi, ogni $f = (a_0, a_1, \dots, a_n, 0, 0, \dots) \in B$ si scrive

$$f = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + (0, 0, a_2, \dots) + (0, 0, \dots, 0, a_n, 0, \dots) = a_0 + a_1 x + a_2 x^2 + \dots a_n x^n \ .$$

Quindi, ragionando nell'estensione $R \subseteq B$, si ha $B = R[x]$. Questo si dice l'anello dei polinomi a coefficienti in R nell'indeterminata x.

La costruzione dell'anello dei polinomi si estende in modo naturale a più indeterminate. Si tratta di 'aggiungere' successivamente le indeterminate: così, se R è una anello commutativo, e x, y sono due distinte indeterminate si pone $R[x, y] = (R[x])[y]$. Il caso generale è definito induttivamente: se $n \geq 2$ e $x_1, \dots, x_n$ sono distinte indeterminate, si pone

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n].$$

Si ha chiaramente una catena di inclusioni tra sottoanelli;

$$R \subseteq R[x_1] \subseteq R[x_1, x_2] \subseteq \cdots \subseteq R[x_1, \dots, x_n].$$

La Proposizione 8.2 assicura che gli elementi invertibili di $R[x_1, \dots, x_n]$ sono gli invertibili di R, e che se R è un dominio d'integrità allora anche $R[x_1, \dots, x_n]$ è tale.
Limitiamoci, per semplicità di notazioni, al caso di due indeterminate, x e y. Usando le proprietà distributive (e la commutatività) si riconosce allora, con un po' di lavoro, che ogni elemento $f \in R[x, y]$ si scrive in modo unico nella forma

$$f = \sum_{i,j \in \mathbb{N}} a_{ij} x^i y^j \tag{8.1}$$

con a_{ij} elementi di R che sono nulli tranne che per un numero finito di coppie (i,j). Per cui si può pensare all'anello $R[x,y]$ come a quello ottenuto considerando tutte le espressioni del tipo (8.1), ovvero 'aggiungendo' ad R assieme le due indeterminate x e y, che sono assunte commutare tra loro. Che l'ordine con cui si considerano le indeterminate sia ininfluente (cosa piuttosto naturale) si può provare in modo più concettuale utilizzando il Principio di sostituzione. Infatti, l'isomorfismo naturale tra $R[x]$ e $R[y]$ (che è l'identità su R e manda $x \mapsto y$) per il principio di sostituzione si estende ad un unico omomorfismo

$$\Sigma : R[x,y] = R[x][y] \longrightarrow R[y,x]$$

che manda y in x. Ìpoiché Σ è in modo piuttosto ovvio invertibile, se ne conclude che è un isomorfismo, ovvero che $R[x,y] \simeq R[y,x]$.

Esercizio 8.2. Sia A una anello commutativo. Sia R un sottoanello di A; si provi che $R[x]$ è un sottoanello di $A[x]$. Sia I un ideale di A; si provi che l'insieme dei polinomi di $A[x]$ i cui coefficienti appartengono a I è un ideale di $A[x]$.

Esercizio 8.3. Si provi che, per ogni $n \in \mathbb{N}$, il polinomio $\overline{2}x^n + 1$ è un elemento invertibile dell'anello $(\mathbb{Z}/4\mathbb{Z})[x]$. Si concluda che $(\mathbb{Z}/4\mathbb{Z})[x]$ contiene infiniti elementi invertibili (la ragione di questa anomalia va ricercata nel fatto che $(\mathbb{Z}/4\mathbb{Z})[x]$ non è un dominio d'integrità).

Esercizio 8.4. Sia σ l'omomorfismo di sostituzione: $\sigma : \mathbb{Z}[x] \to \mathbb{Q}$ definito da, per ogni $f \in \mathbb{Z}[x]$, $\sigma(f) = f(1/3)$, e sia $\mathbb{Z}[1/3] = Im(\sigma)$.

(a) Si provi che

$$\mathbb{Z}[1/3] = \{ \frac{m}{3^i} \mid m \in \mathbb{Z}\ , i \geq 0 \}.$$

(b) Si dica, motivando la risposta, se $\mathbb{Z}[1/3]$ è un campo.

Esercizio 8.5. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi. Si provi che il sottoinsieme $\{a_0 + a_1x + \cdots + a_nx^n \mid n \in \mathbb{N},\ a_o, a_1, \ldots, a_n \in \mathbb{Z}, \sum_{i=o}^{n} a_i = 0\}$ è un ideale di $\mathbb{Z}[x]$.

8.2. Divisione tra polinomi.

In questa sezione mostriamo, in particolare, il fatto fondamentale che se F è un campo, allora l'anello dei polinomi $F[x]$ è euclideo (pertanto è un dominio a ideali principali e a fattorizzazione unica).

Attenendoci alle definizioni introdotte nel capitolo precedente, se f, g sono polinomi a coefficienti nell'anello commutativo A, allora f *divide* g (e scriviamo $f|g$) se esiste $h \in A[x]$ tale che $g = fh$.

Esempio, Sia A un anello commutativo e siano $1 \leq m, n \in \mathbb{N}$ con $m|n$; allora il polinomio $x^m - 1 \in A[x]$ è un divisore di $x^n - 1$. Infatti, se $d \in \mathbb{N}$ è tale che $n = md$, come si verifica facendo i calcoli,

$$x^n - 1 = (x^m - 1)(x^{(d-1)m} + \cdots + x^{2m} + x^m + 1).$$

Essendo l'anello dei polinomi ben lontano dall'essere un campo, fissati casualmente due polinomi in $A[x]$ è assai improbabile che uno dei due divida l'altro. Tuttavia, se A è un campo è possibile definire una "divisione con resto". Più in generale, è possibile dividere con resto (nel senso che preciseremo subito) se il coefficiente direttivo del polinomio "divisore" è un elemento invertibile di A

Teorema 8.4. *Sia A un anello commutativo, e sia $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ con a_n un elemento* invertibile *di A. Allora per ogni $g \in A[x]$ esistono due polinomi $h, r \in A[x]$ tali che*

$$\begin{array}{ll} (i) & g = hf + r \\ (ii) & r = 0 \quad \textit{oppure} \quad \deg(r) \leq \deg(f) - 1 \end{array}$$

inoltre, h, r sono univocamente determinati da tali condizioni.

Dimostrazione. 1) (esistenza) Sia f come nell'enunciato e e $g = b_0 + b_1x + \cdots + b_mx^m$. Se $g = 0$ allora $g = 0f + 0$. Sia quindi $g \neq 0$ e procediamo per induzione su $m = \deg(g)$.

Sia $m = 0$, allora $g \in A$. Se $n = \deg f \geq 1$ allora possiamo scrivere $g = 0f + g$ e siamo a posto perchè $\deg g = 0 < \deg f$. Se invece $\deg f = 0$, allora $f = a_0$ è invertibile in A e quindi $g = a_0(a_0^{-1}g) = fh + 0$ con $h = a_0^{-1}g$.

Sia ora $m \geq 1$ e supponiamo l'enunciato vero per ogni polinomio dividendo di grado $\leq m - 1$.
Se $m \leq n - 1$ allora $g = 0f + g$ soddisfa le condizioni.
Sia quindi $m \geq n$, e poniamo

$$g_1 = a_ng - b_mx^{m-n}f = a_n(b_0 + b_1x + \cdots + b_mx^m) - b_mx^{m-n}(a_0 + a_1x + \cdots + a_nx^n) =$$

$$= a_nb_0 + \cdots + a_nb_mx^m - a_0b_mx^{m-n} - \cdots - a_{n-1}b_mx^{m-1} - a_nb_mx^m \ .$$

Allora, $g = 0$ oppure $\deg g_1 \leq m - 1$; quindi, per ipotesi induttiva esistono $h_1, r_1 \in A[x]$ tali che $g_1 = h_1f + r_1$ e $r_1 = 0$ o $\deg r_1 \leq n - 1$. Segue che

$$g = a_n^{-1}(g_1 + b_mx^{m-n}f) = a_n^{-1}(h_1f + r_1 + b_mx^{m-n}f) = a_n^{-1}(h_1 + b_mx^{m-n})f + a_n^{-1}r_1$$

e le condizioni dell'enunciato sono soddisfatte con $h = a_n^{-1}(h_1 + b_mx^{m-n})$ ed $r = a_n^{-1}r_1$.

2) (unicità) Supponiamo di poter scrivere $g = hf + r = h'f + r'$ con la condizione (ii) soddisfatta. Allora $(h - h')f = r' - r$, se fosse $h \neq h'$ avremmo l'assurdo $\deg(f) \leq \deg((h - h')f) = \deg(r - r') \leq \deg(f) - 1$ (vedi esercizio 8.1). Quindi $h = h'$ da cui discende immediatamente anche $r = r'$. ∎

La dimostrazione del Teorema fornisce anche il metodo per eseguire una divisione tra polinomi (quando consentito); si tratta di ripetere il passo in cui si "dividono" i monomi di grado massimo, ottenendo un monomio che va moltiplicato per il divisore e quindi sottratto dal polinomio su cui si sta operando, ottenendo così un polinomio di grado inferiore, ed andando avanti. È il solito metodo che si impara nelle scuole.

Esercizio 8.6. Nell'anello $\mathbb{Q}[x]$ dividere $g = 2x^4 - x^2 + 5x$ per $f = x^2 - x + 1$.

Soluzione. La familiare tabella:

$$\begin{array}{rrrrr|l}
2x^4 & & -x^2 & +5x & & x^2-x+1 \\
\cline{6-6}
2x^4 & -2x^3 & +2x^2 & & & 2x^2+2x-1 \\
\cline{1-4}
 & 2x^3 & -3x^2 & +5x & & \\
 & 2x^3 & -2x^2 & +2x & & \\
\cline{2-4}
 & & x^2 & +3x & & \\
 & & x^2 & +x & -1 & \\
\cline{3-5}
 & & & 2x & -1 &
\end{array}$$

Quindi, $g = (2x^2 + 2x - 1)f + (2x - 1)$.

Si osservi come, nella dimostrazione del Teorema 8.4, sia essenziale il fatto che il coefficiente direttivo a_n del polinomio divisore f sia invertibile. In particolare, il Teorema si applica al caso in cui f è monico.

Ma ancora più importante è notare che se F è un campo, allora il Teorema sussiste per qualsiasi $f \in F[x]$ purché sia $f \neq 0$. Questo ci conferma che, assumendo come valutazione euclidea il grado $deg : F[x] \to \mathbb{N}$, l'anello dei polinomi $F[x]$ è un dominio euclideo. Di conseguenza (Teorema 7.12), $F[x]$ è un Dominio a Ideali Principali. Questo ultimo fatto è così importante che lo rienunciamo esplicitamente, e ne forniamo anche una dimostrazione diretta (che non è altro che l'adattamento al caso di quella del Teorema 7.12).

Teorema 8.5. *Sia F un campo. Allora*

(1) $F[x]$ è un dominio euclideo;

(2) $F[x]$ è un dominio a ideali principali. Più precisamente: se $I \neq \{0\}$ è un ideale non-nullo di $F[x]$, e $0 \neq f \in I$ è un polinomio di grado minimo *tra quelli non-nulli appartenenti a I, allora $I = (f)$.*

Dimostrazione. (1) Il Teorema 8.4, applicato al caso in cui $A = F$ è un campo, afferma in particolare che $F[x]$, dotato della valutazione data dal grado, è un dominio euclideo.
(2) Questo discende immediatamente dal punto (1) e dal Teorema 7.12; ma vediamo la dimostrazione diretta. Sia I un ideale di $F[x]$. Se $I = \{0\}$ allora $I = (0)$. Sia quindi $I \neq \{0\}$; allora I contiene almeno un elemento non nullo, sia $n = \min\{\deg f \mid f \in I\ , f \neq 0\}$; e sia $f \in I$ tale che $\deg f = n$. Proviamo che $I = (f)$
In un verso, poichè (f) è il minimo ideale che contiene f, e $f \in I$, si ha $(f) \subseteq I$.
Viceversa, sia $g \in I$. Dividiamo g per f:

$$g = fq + r \qquad \text{con} \quad r = 0 \ \text{ o } \ \deg r < \deg f = n\ .$$

Ora $fq \in I$ e quindi $r = g - fq \in I$. Se fosse $r \neq 0$ allora r sarebbe un elemento non nullo di I di grado strettamente minore del grado di f, e questo contraddice la scelta di f in I. Quindi $r = 0$ e di conseguenza $g = fq \in (f)$. Dunque $I \subseteq (f)$; pertanto $I = (f)$, completando la dimostrazione. ∎

Osservazione. Il Teorema precedente non vale in generale per anelli di polinomi a coefficienti in un dominio d'integrità. Ad esempio, nell'anello $\mathbb{Z}[x]$ consideriamo l'insieme

$$I = \{a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] \mid 2 \ \text{ divide } \ a_0\}\ .$$

Si verifichi per esercizio che I è un ideale di $\mathbb{Z}[x]$ (ad esempio provando che è il nucleo di un opportuno omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$). Di fatto I è l'ideale di $\mathbb{Z}[x]$ generato da x e da 2,

ovvero $I = (2, x)$. Supponiamo per assurdo che I sia principale, cioè che esista $a \in \mathbb{Z}[x]$ tale che $I = (a)$. Allora, poichè $2 \in I$, esiste $g \in \mathbb{Z}[x]$ tale che $2 = ag$, ciò implica $\deg a = 0$, cioè $a \in \mathbb{Z}$. Ma è anche $x \in I$ e quindi esiste $h \in \mathbb{Z}[x]$ tale che $x = ah$; per la formula dei gradi, deve essere $h = c + dx$, con $c, d \in \mathbb{Z}$; quindi $x = a(c + dx) = ac + adx$, da cui segue $c = 0$ e $ad = 1$. Dunque $a = \pm 1$, ma allora $I = (a) = \mathbb{Z}[x]$ il che è assurdo perchè $I \neq \mathbb{Z}[x]$.

Sia F un campo. Richiamando le definizioni fissate nella sezione 7.1, e ricordando che gli invertibili di $F[x]$ sono tutti e soli gli elementi non-nulli di F, si conclude che $f, g \in F[x]$ sono *associati* (e quindi, $(f) = (g)$) se e soltanto se $g = af$, per qualche $0 \neq a \in F$. Detto in modo apparentemente più preciso, si ha il seguente Lemma, che non dovrebbe risultare difficile dimostrare.

Lemma 8.6. *Sia F un campo; e siano $0 \neq f, g \in F[x]$ con g un divisore di f. Allora*

(i) g è un divisore proprio se e solo se $0 < \deg g < \deg f$;

(ii) $f|g$ (e quindi $f \sim g$) se e solo se esiste $0 \neq c \in F$ tale che $g = cf$.

(Si rifletta a come e perché tali affermazioni non valgano se l'anello dei coefficienti non è un campo - ad esempio nel caso di $\mathbb{Z}[x]$).

In particolare, i polinomi generatori di un ideale $\{0\} \neq I$ di $F[x]$ differiscono tra loro per il prodotto di un elemento non nullo di F (in particolare, hanno lo stesso grado, che è il minimo tra i gradi degli elementi non-nulli di I).
Se $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ è un polinomio non nullo a coefficenti in F, con $a_n \neq 0_F$, allora a_n è invertibile in F, e si può scrivere

$$f = a_n(x^n + a_n^{-1} a_{n-1} x^{n-1} + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0.)$$

Ovvero $f = a_n f_0$ è il prodotto del suo coefficiente direttivo a_n per un polinomio monico f_0 (che, è chiaro, sono univocamante individuati da f). Quindi, ogni ideale non nullo di $F[x]$ ha uno ed un solo generatore *monico*.

Queste osservazioni conducono al fatto che i divisori propri di un $f \in F[x] \setminus F$ hanno grado strettamente minore di quello di f. In particolare si ricava una descrizione degli elementi irriducibili di $F[x]$ (F è sempre un campo) che è molto conveniente: *un polinomio $f \in F[x]$ è* **irriducibile** *in $F[x]$ se e solo se $\deg f \geq 1$ e f non ha divisori non invertibili di grado strettamente minore di $\deg f$.*
In altri termini $f \in F[x] \setminus F$ è irriducibile se non è possibile scrivere $f = gh$ con g e h polinomi tali che $\deg g < \deg f$ e $\deg h < \deg f$. In particolare, ogni polinomio di grado 1 in $F[x]$ è irriducibile. Si noti che questo non è più vero se i coefficienti non sono su un campo; ad esempio il polinomio $2x - 6$ è riducibile in $\mathbb{Z}[x]$ come prodotto dei divisori propri $2(x - 3)$ (infatti, 2 non è invertibile in $\mathbb{Z}[x]$).

Esempio. Il polinomio $x^3 + 2x^2 + 2x + 1 \in \mathbb{Q}[x]$ è riducibile in $\mathbb{Q}[x]$; infatti si trova facilmente che $x^3 + 2x^2 + 2x + 1 = (x + 1)(x^2 + x + 1)$. Mentre $x^2 + x + 1$ è un polinomio irriducibile di $\mathbb{Q}[x]$ (lo si dimostri).

Un'ovvia avvertenza è che un polinomio va sempre considerato come un elemento dell'anello dei polinomi a coefficienti in un esplicito anello commutativo, ed è in tale anello dei polinomi che ha senso chiedersi se sia o meno irriducibile (si vedano esempi nella prossima sezione).

Massimo comun divisore tra polinomi. Sia ancora F un campo. La proprietà di fattorizzazione unica di $F[x]$ assicura che ogni coppia di polinomi f e g in $F[x]$ ammette un massimo comun divisore d (come abbiamo visto in generale per gli UFD nella sezione 7.1).

Poiché $F[x]$ è anche un PID, le osservazioni poste alla fine della sezione 7.3 comportano che se $d \in F[x]$ è un massimo comun divisore di f e g, allora d può essere scritto nella forma

$$d = \alpha \cdot f + \beta \cdot g$$

con $\alpha, \beta \in F[x]$; anzi, d è, tra i polinomi che si scrivono in questa forma, uno di grado minimo (diverso da zero). Inoltre, dal Lemma 8.6, segue che, se d e d_1 sono due massimi comun divisori di f e g, esiste un $0 \neq a \in F$ tale che $d_1 = ad$. Ne segue, sempre per il Lemma 8.6, che f e g hanno un *unico* massimo comun divisore *monico*, che si denota quindi con (f, g). Come nel caso degli interi, diremo che due polinomi a coefficienti su un campo f e g sono *coprimi* se $(f, g) = 1$.
Infine, anche con l'anello $F[x]$, per calcolare il massimo comun divisore di due polinomi non nulli, è possibile applicare l'algoritmo di Euclide. La procedura è la stessa del caso dei numeri interi (ed è fondata sulla divisione euclidea, Teorema 8.4), per cui, invece che descriverla nuovamente in generale, ci limitiamo a fornire un esempio della sua applicazione.

Esercizio 8.7. Calcolare un MCD in $\mathbb{Q}[x]$ dei polinomi:

$$f = 12x^7 + 5x^5 + 10x^4 - 7x^3 + 10x^2 \qquad g = 2x^5 - x^4 + 2x^3 + 1.$$

Soluzione. L'algoritmo di Euclide opera mediante divisioni successive. In questo caso si ha:

$$\begin{array}{ll} f = (6x^2 + 3x - 2)g + r_1 & r_1 = 2x^4 - 3x^3 + 4x^2 - 3x + 2 \\ g = (x + 1)r_1 + r_2 & r_2 = x^3 - x^2 + x - 1 \\ r_1 = (2x - 1)r_2 + r_3 & r_3 = x^2 + 1 \\ r_2 = (x - 1)r_3 + 0 & \end{array}$$

quindi $r_3 = x^2 + 1$ è un MCD di f e g.

Esercizio 8.8. Si dica per quali valori di $a \in \mathbb{Q}$, $x^2 + 1$ divide $x^4 + 3x^3 + 3x - a^2$ nell'anello $\mathbb{Q}[x]$.

Esercizio 8.9. In $\mathbb{Q}[x]$ si considerino i polinomi

$$f = x^5 - 2x^4 + x^3 - 9x^2 + 18x - 9 \qquad g = x^5 - x^3 - 9x^2 + 9\ .$$

Determinare un massimo comun divisore di f e g.

Esercizio 8.10. Si dica per quali $a \in \mathbb{Z}$ i seguenti polinomi sono coprimi in $\mathbb{Q}[x]$,

$$3x^4 + 4x^3 + ax^2 + ax + a \qquad x^2 + 2x + 1\ .$$

Esercizio 8.11. Sia $g = \overline{2}x + \overline{2} \in \mathbb{Z}_4[x]$.
Si provi che se $f \in \mathbb{Z}_4[x]$ è un polinomio monico, allora non esiste alcuna coppia $q, r \in \mathbb{Z}_4[x]$ tale che $f = qg + r$ e $\deg r < \deg g$.

Esercizio 8.12. Sia R un dominio di integrità. Provare che se R non è un campo, $R[x]$ non è un dominio a ideali principali.

8.3. Radici e fattorizzazioni.

Un'immediata conseguenza del Teorema 8.5 e del Teorema 7.11 è la seguente.

Corollario 8.7. *Sia F un campo. Allora $F[x]$ è un dominio a fattorizzazione unica.*

Quindi, ogni polinomio non nullo di grado diverso da zero a coefficienti su un campo F (ciò vale a dire: ogni elemento non zero e non invertibile di $F[x]$) si fattorizza in modo essenzialmente unico come prodotto di polinomi irriducibili. Poiché ogni classe di polinomi irriducibili associati contiene uno ed un solo polinomio monico, possiamo concludere che, se F è un campo, allora *ogni polinomio $f \in F[x] \setminus F$ si scrive in modo unico (a meno dell'ordine dei fattori) come $f = a_n f_1 f_2 \dots f_k$ dove a_n è il coefficiente direttivo di f e $f_1, f_2, \dots, f_k$ sono polinomi monici irriducibili in $F[x]$.*

Esempio. Vediamo le fattorizzazioni in irriducibili del polinomio $x^4 + 1$ rispettivamente in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.

$x^4 + 1$ è irriducibile in $\mathbb{Q}[x]$ (lo si provi per esercizio).

$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ in $\mathbb{R}[x]$.

$x^4 + 1 = (x - \omega_1)(x - \omega_2)(x - \omega_3)(x - \omega_4)$ in $\mathbb{C}[x]$,
dove $\omega_1 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $\omega_2 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $\omega_3 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$, $\omega_4 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.

(osserviamo che dalla fattorizzazione in $R[x]$ si deduce che $x^4 + 1$ è irriducibile in $\mathbb{Q}[x]$; infatti $x^4 + 1$ non ha radici in $\mathbb{Q}$ e quindi non ha fattori di grado 1, se si decomponesse in $\mathbb{Q}[x]$ come prodotto di due fattori (monici) di grado 2, allora tali fattori sarebbero anche i fattori nella decomposizione in $R[x]$ e quindi, per l 'unicità della fattorizzazione, dovrebbero coincidere con i fattori scritti sopra che tuttavia non sono a coefficienti razionali).

Osservazione importante. Ribadiamo il fatto che se R è un dominio d'integrità ma non è un campo, allora $R[x]$ non è un PID. Lo abbiamo già verificato nel caso $R = \mathbb{Z}$ nell'esempio che segue il Teorema 8.5: un ideale non principale di $\mathbb{Z}[x]$ è, per esempio l'ideale $(p, x) = \{pf + xg \mid f, g \in \mathbb{Z}[x]\}$, con $p \in \mathbb{Z} \setminus \{0, 1, -1\}$. Si cerchi di adattare questo argomento a qualsiasi dominio R che possiede elementi non-nulli e non–invertibili.
Nella prossima sezione proveremo tuttavia che anche $\mathbb{Z}[x]$ è un UFD, provando così in particolare che esistono domini a fattorizzazione unica che non sono a ideali principali.

Definizione. Sia R un anello e $0 \neq f \in R[x]$. Un elemento $a \in R$ si dice **radice** (o, anche, "zero") di f se $f(a) = 0$.

Un primo criterio di riducibilità (cioè di esistenza di divisori propri) di un polinomio è il noto Teorema di Ruffini. Si tratta, in fin dei conti, di una conseguenza del Teorema 8.4.

Teorema 8.8. (di Ruffini) *Sia A un anello commutativo, $0 \neq f \in A[x]$ ed $a \in A$. Allora a è una radice di f se e solo se $(x - a)$ divide f.*

Dimostrazione. Supponiamo $f(a) = 0$, e dividiamo f per $x - a$. Esistono $h, r \in A[x]$ tali che $f = (x-a)h+r$, con $r = 0$ o $\deg r = 0$. Quindi, in ogni caso, $r \in A$ e dunque $r(a) = r$. Ora

$$0 = f(a) = (a - a)h(a) + r(a) = 0h(a) + r = r$$

quindi $f = (x - a)h$ cioè $(x - a)$ divide f.

Viceversa, supponiamo che $(x-a)$ divida f. Allora $f=(x-a)h$ per qualche $h \in A[x]$ e pertanto

$$f(a) = (a-a)h(a) = 0h(a) = 0$$

quindi a è una radice di f. ∎

Osserviamo che una conseguenza banale del Teorema di Ruffini è che un polinomio $0 \neq f$ a coefficienti in un campo F ha divisori di primo grado se e soltanto se ha radici in F. Infatti se $g = ax+b$ (con $a, b \in F$) è un divisore di f, allora $g = a(x-(-ba^{-1}))$, e quindi anche $x-(-ba^{-1})$ è un divisore di f; pertanto $-ba^{-1}$ è una radice di f.

Esempio. Il polinomio x^2+x-1 è irriducibile in $\mathbb{Q}[x]$ dato che ha grado 2 e non ha radici in $\mathbb{Q}$ (e quindi non ha divisori di grado 1 in $\mathbb{Q}[x]$); d'altra parte x^2+x-1 è riducibile in $\mathbb{R}[x]$, dato che, in $\mathbb{R}[x]$,

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

L'esempio che abbiamo dato tratta un polinomio di secondo grado a coefficienti reali, per i quali esiste una ben nota formula esplicita per il calcolo delle radici. Per polinomi di grado superiore, applicare il teorema di Ruffini ai fini di studiare l'irriducibilità è meno agevole (il famoso teorema di Galois asserisce, in particolare, che non esistono formule risolutive generali per calcolare le radici di un polinomio razionale di grado maggiore o uguale a 5); tuttavia, almeno per polinomi monici in $\mathbb{Q}[x]$ i cui coefficienti sono tutti degli interi, c'è un facile trucco.
Sia $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ un polinomio monico in $\mathbb{Q}[x]$, tale che i coefficienti $a_0, a_1, \ldots, a_{n-1}$ sono numeri interi e $a_0 \neq 0$. Supponiamo che $q \in \mathbb{Q}$ sia una radice di f. Sia $q = a/b$, con $a, b \in \mathbb{Z}$, $(a,b) = 1$ e $b \geq 1$. Allora

$$0 = f(\alpha) = q^n + a_{n-1}q^{n-1} + \cdots + a_1q + a_0 = \frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + a_1\frac{a}{b} + a_0.$$

Moltiplicando per b^n si ha

$$-a^n = a_{n-1}a^{n-1}b + \cdots + a_1ab^{n-1} + a_0b^n.$$

Questa è una relazione tra numeri interi, e siccome a e b sono coprimi, da essa segue che $b = 1$. Dunque $q = a \in \mathbb{Z}$; inoltre $-a_0 = a^n + a_{n-1}a^{n-1} + \cdots + a_1a = (a^{n-1} + a_{n-1}a^{n-2} + \cdots + a_1)a$, e dunque a divide a_0 in $\mathbb{Z}$. Abbiamo cioè provato che le eventuali radici in $\mathbb{Q}$ di un polinomio monico i cui coefficienti sono numeri interi, sono numeri interi che dividono (come numeri interi) il termino noto a_0 del polinomio (questa osservazione è generalizzata nell'esercizio 8.13). Ad esempio, il polinomio $f = x^4 + 2x^3 - 7x + 1$ non ha radici in $\mathbb{Q}$ (e dunque non ha divisori di primo grado in $\mathbb{Q}[x]$), dato che 1 e -1 non sono radici di f.

Torniamo ad occuparci di polinomi su un campo generico. Sia $0 \neq f$ un polinomio a coefficienti sul campo F e sia $a \in F$ una radice di f. Allora $(x-a)$ divide f, e quindi si può scrivere $f = (x-a)g$ con $g \in F[x]$. A sua volta, a potrebbe essere una radice di g; in tal caso $(x-a)$ divide g, e quindi $(x-a)^2$ divide f. Dunque, se a è una radice di f, esiste un massimo intero positivo $m(a)$ tale che $(x-a)^m$ divide f. Tale intero si chiama *molteplicità (algebrica)* della radice a, e chiaramente soddisfa $1 \leq m(a) \leq \deg f$. Possiamo fattorizzare f come $f = (x-a)^{m(a)}h$, dove $h \in F[x]$, e $h(a) \neq 0$. Se $m(a) = 1$, la radice a si dice *semplice*, altrimenti si dice multipla. Un criterio per il calcolo delle eventuali radici multiple di un polinomio $f \in F[x]$ è fornito dall'esercizio 8.34.

Considerazioni di simile natura sono applicate per dimostrare la seguente e importantissima conseguenza del Teorema di Ruffini.

Teorema 8.9. *Sia F un campo e $0 \neq f \in F[x]$, con $n = \deg f$. Allora il numero di radici distinte di f in F è al più n.*

Dimostrazione. Siano $\alpha_1, \alpha_2, \ldots, \alpha_k$ radici distinte di f in F. Procedendo per induzione su k proviamo che $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ divide f. Per $k = 1$ è il teorema di Ruffini. Sia quindi $k \geq 2$ e assumiamo per ipotesi induttiva che $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})$ divida f. Sia $g \in F[x]$ tale che $f = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})\cdot g$. Allora

$$0 = f(\alpha_k) = (\alpha_k-\alpha_1)(\alpha_k-\alpha_2)\cdots(\alpha_k-\alpha_{k-1})g(\alpha_k)$$

in cui il termine di destra è un prodotto di elementi del campo F; quindi, poichè $\alpha_k \neq \alpha_i$ per $i = 1, 2, \ldots, k-1$, deve essere $g(\alpha_k) = 0$. Per il Teorema di Ruffini $(x-\alpha_k)$ divide g, quindi $g = (x-\alpha_k)h$ per un $h \in F[x]$ e dunque

$$f = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})(x-\alpha_k)h$$

Quindi, per il principio di induzione, l'affermazione è provata. Ora se $\alpha_1, \alpha_2, \ldots, \alpha_t$ sono *tutte* le radici distinte di f, per quanto appena visto $d = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)$ divide f e quindi $n = \deg f \geq \deg d = t$. ∎

In effetti, il Teorema precedente può essere reso ulteriormente preciso nel modo seguente (la verifica consiste nel ripercorrere con attenzione la dimostrazione del Teorema 8.9 tenendo conto delle osservazioni che lo precedono, ed è lasciata per esercizio).

Teorema 8.10. *Sia F un campo, e sia $0 \neq f \in F[x]$, un polinomio non nullo di grado n. Siano $a_1, a_2, \ldots, a_k$ le radici distinte di f in F, e per ogni $i = 1, 2, \ldots, k$, sia $m_i = m(a_i)$ la molteplicità della radice a_i. Allora $m_1 + m_2 + \cdots + m_k \leq n$.*

Vediamo un'interessante applicazione alla teoria dei numeri.

Teorema 8.11. (**Teorema di Wilson**) *Sia p un numero primo positivo. Allora*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dimostrazione. Sia p un primo positivo (che chiaramente possiamo supporre dispari), e consideriamo il campo $\mathbb{Z}/p\mathbb{Z}$. Sappiamo, dal teorema di Fermat, che

$$0 \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z} \quad \Rightarrow \quad \overline{a}^{p-1} = \overline{1}.$$

Quindi $\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}$ sono le radici distinte del polinomio $x^{p-1} - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[x]$. Allora, per la dimostrazione del teorema 8.9,

$$x^{p-1} - \overline{1} = (x-\overline{1})(x-\overline{2})(x-\overline{3})\cdots(x-\overline{p-1}).$$

Confrontando i termini noti si trova che

$$-\overline{1} = (-\overline{1})\cdot(-\overline{2})\cdot(-\overline{3})\cdot\cdots\cdot(-\overline{p-1}) = (-1)^{p-1}\overline{1\cdot 2\cdot 3\cdot\cdots\cdot(p-1)} = \overline{(p-1)!}$$

e quindi $(p-1)! \equiv -1 \pmod{p}$. ∎

Esercizio 8.13. Sia $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, con $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, e sia $u = a/b \in \mathbb{Q}$ (con $a, b \in \mathbb{Z}$, $b \geq 1$ e $(a, b) = 1$). Si provi che se u è una radice di f, allora $b|a_n$ e $a|a_0$.

Esercizio 8.14. Si provi che i polinomi a coefficienti razionali

$$x^3 + x^2 + x + 2 \qquad \text{e} \qquad x^4 + 1$$

sono irriducibili in $\mathbb{Q}[x]$.

Esercizio 8.15. Si provi che il polinomio $x^3 - x$ ha sei radici distinte in $\mathbb{Z}_6$.

Esercizio 8.16. Sia F un campo. Provare che in $F[x]$ esistono infiniti polinomi monici irriducibili. [imitare la dim. dell'infinità di numeri primi]

Esercizio 8.17. Si provi che il polinomio $x^2 + x + \overline{1}$ è irriducibile in $(\mathbb{Z}/5\mathbb{Z})[x]$. Si provi che il polinomio $x^2 + x + \overline{1}$ è riducibile in $(\mathbb{Z}/7\mathbb{Z})[x]$. Si studi la riducibilità del polinomio $x^3 + \overline{1}$ in $(\mathbb{Z}/11\mathbb{Z})[x]$.

Serie formali. Questa breve appendice, in cui descriviamo un'estensione dell'idea di anello dei polinomi, è complementare al materiale specifico del corso e può ragionevolmente essere presa come una lettura, come materiale per esercizi, o carta da riciclare. L'abbiamo inserita perché ci consente di accennare ad altri esempi interessanti (anche se concettualmente un po' alieni) di domini a ideali principali, e può suggerire un inquadramento anche algebrico della teoria dello sviluppo in serie (ci vuole però sempre cautela).

Dato un campo F l'insieme delle espressioni (dette *serie formali*)

$$\sum_{i\in\mathbb{N}} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

con $a_i \in F$ per ogni $i \in \mathbb{N}$, costituisce un dominio di integrità (esercizio 8.18) rispetto alle operazioni di somma e prodotto che estendono quelle definite per i polinomi:

$$\sum_{i\in\mathbb{N}} a_i x^i + \sum_{i\in\mathbb{N}} b_i x^i = \sum_{i\in\mathbb{N}} (a_i + b_i) x^i$$

$$\left(\sum_{i\in\mathbb{N}} a_i x^i\right)\left(\sum_{i\in\mathbb{N}} b_i x^i\right) = \sum_{i\in\mathbb{N}} c_i x^i$$

dove, per ogni $i \in \mathbb{N}$,

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} \quad .$$

L'anello così definito si dice *anello delle serie formali (a coefficienti in F)* e si denota con il simbolo $F[[x]]$.
Le serie formali con solo un numero finito di coefficienti non nulli, (ovvero le serie $\sum a_i x^i$ per cui esista un $n \in \mathbb{N}$ tale che $a_i = 0$ per ogni $i \geq n$), cioè i *polinomi* a cofficienti in F, costituiscono un sottoanello di $F[[x]]$. In particolare, identifichiamo gli elementi di F con le serie formali $\sum a_i x^i$ tali che $a_i = 0$ per ogni $i \geq 1$.

Proviamo ora che gli elementi invertibili dell'anello $F[[x]]$ sono tutti e soli quelli del tipo $\sum a_i x^i$ con $a_0 \neq 0$. La serie $\alpha = \sum a_i x^i$ è infatti invertibile in $F[[x]]$ se e solo se esiste $\beta = \sum b_i x^i$ tale che

$$1_{F[[x]]} = 1 + 0x + 0x^2 + \ldots = \alpha\beta = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

ovvero se e solo se esistono $b_0, b_1, b_2 \ldots \in F$ tali che

$$a_0b_0 = 1 \qquad a_0b_1 + a_1b_0 = 0 \qquad a_0b_2 + a_1b_1 + a_2b_0 = 0 \qquad \ldots \ .$$

Si osserva subito, quindi, che la condizione $a_0 \neq 0$ è necessaria per l'invertibilità di $\sum a_i x^i$. D'altra parte, se $a_0 \neq 0$ definiamo $b_0 = a_0^{-1}$ e per induzione, definiti $b_0, b_1, \ldots, b_{i-1}$, poniamo

$$b_i = -a_0^{-1}(\sum_{j=1}^{i} a_j b_{i-j}).$$

La serie $\sum b_i x^i$ è quindi l'inversa della serie $\sum a_i x^i$, ed abbiamo provato che la condizione $a_0 \neq 0$ è anche sufficiente.

Ad esempio, l'inversa della serie geometrica $\sum_{i\in\mathbb{N}} x^i = 1 + x + x^2 + x^3 + \ldots$ è il polinomio $1 - x$ (fare i calcoli).

Osserviamo in particolare che l'insieme degli elementi non invertibili di $F[[x]]$ è pertanto

$$J = \left\{ \sum a_n \in F[[x]] \mid a_0 = 0 \right\}$$

che non è altro che l'ideale principale generato dall'elemento x: cioè $J = (x)$. Questo comporta, in particolare, che ogni ideale proprio di $F[[x]]$ è contenuto in J. Infatti, sia I un ideale di $F[[x]]$ e supponiamo che $I \not\subseteq J$; allora esiste $f \in I \setminus J$; poiché $f \notin J$, f è invertibile per quanto provato in precedenza, dunque $F[[x]] = (f) \subseteq I$, e questo prova che $I = F[[x]]$ non è proprio.
Un anello commutativo A che ammette un ideale proprio J che contiene ogni altro ideale proprio, si dice *anello locale*. La condizione è equivalente (vedi Esercizio 5.47) all'essere $A \setminus J$ l'insieme degli elementi invertibili di A (ogni campo è, in modo banale, un anello locale).

Vediamo ora come $F[[x]]$ sia un dominio a ideali principali.
Cominciamo con l'osservare che, a differenza dell'anello dei polinomi $F[x]$, che possiede (per ogni campo F) un numero infinito di polinomi monici irriducibili (esercizio 7.1), l'anello delle serie formali $F[[x]]$ ha, a meno di associati, *un solo* elemento irriducibile. Il polinomio x è infatti un elemento irriducibile di $F[[x]]$ (verificare) e se $\pi = \sum_{i=0}^{\infty} a_i x^i$ non è invertibile, esiste $n \geq 1$ tale che $a_i = 0$ per ogni $0 \leq i < n$ e $a_n \neq 0$, per cui

$$\pi = x^n \sum_{i=0}^{\infty} a_{n+i} x^i \quad \sim \quad x^n \tag{8.2}$$

dato che $\sum a_{n+i} x^i$ è invertibile, e quindi π è irriducibile se e solo se $n = 1$ e $\pi \sim x$. La (8.2) dice come sono le fattorizzazioni in irriducibili in $F[[x]]$: ogni $f \in F[[x]]$ si scrive in modo unico nella forma $f = x^n g$ con $n \geq 0$ e g invertibile. Infine, gli ideali di $F[[x]]$ sono $\{0\}$ e tutti e soli quelli del tipo (x^n) con $n \geq 0$.

Esercizio 8.18. Si provi che $F[[x]]$ è un dominio d'integrità.

Esercizio 8.19. In $\mathbb{R}[[x]]$ si calcoli l'inversa della serie formale

$$f = \sum_{n\in\mathbb{N}} \frac{x^n}{n!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

Esercizio 8.20. Sia I un ideale proprio di $F[[x]]$. Si provi che esiste $n \in \mathbb{N}$ tale che $I = (x^n)$. Si deduca che $F[[x]]$ è un dominio a ideali principali. Si dica se $F[[x]]$ è un dominio euclideo.

8.4. Fattorizzazioni in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$

In questa sezione dimostreremo, in particolare, che $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica (quindi $\mathbb{Z}[x]$ è un esempio di UFD che non è un PID), e vedremo come il problema della fattorizzazione in $\mathbb{Q}[x]$ si riconduca a quello della fattorizzazione in $\mathbb{Z}[x]$. Le idee, anche se espresse in modo formale, sono del tutto elementari, a partire dal "raccoglimento del fattor comune" per i polinomi interi. Per comodità, denoteremo con $\mathbb{Z}_p$ l'anello delle classi resto $\mathbb{Z}/p\mathbb{Z}$.

Definizione. Sia $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un polinomio non nullo in $\mathbb{Z}[x]$. f si dice **primitivo** se $\mathrm{MCD}(a_0, a_1, a_2, \ldots, a_n) = 1$.

Sia $0 \neq f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ e sia $d = \mathrm{MCD}(a_0, a_1, \ldots, a_n)$. Allora, chiaramente, $f_0 = \frac{a_0}{d} + \frac{a_1}{d}x + \cdots + \frac{a_n}{d}x^n$ è un polinomio primitivo in $\mathbb{Z}[x]$ e $f = df_0$. Inoltre se $f = cf_1$ con $c \in \mathbb{Z}$ e $f_1 \in \mathbb{Z}[x]$ primitivo, allora c divide tutti i coefficienti di f e quindi $c|d$; similmente $\frac{d}{c}$ divide tutti i coefficienti di f_1 che è primitivo, quindi $c = \pm d$ e $f_1 = \pm f_0$. Pertanto abbbiamo il seguente

Lemma 8.12. *Sia $0 \neq f \in \mathbb{Z}[x]$. Allora $f = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo, e tale fattorizzazione è unica a meno del segno.*

Osservazione che ciò si estende facilmente al caso razionale.

Lemma 8.13. *Sia $0 \neq f \in \mathbb{Q}[x]$. Allora $f = \gamma f_0$ con $\gamma \in \mathbb{Q}$ e f_0 un polinomio primitivo in $\mathbb{Z}[x]$. Tale fattorizzazione è unica a meno del segno.*

Dimostrazione. Sia $0 \neq f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$. Per ogni $i = 0, \ldots, n$ sia $a_i = \frac{r_i}{s_i}$ con $r_i, s_i \in \mathbb{Z}$. Allora, posto $s = s_1s_2 \ldots s_n$, si ha $sf \in \mathbb{Z}[x]$ dunque, per il Lemma 8.12, $sf = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo, e quindi $f = \frac{d}{s}f_0$ con $\frac{d}{s} \in \mathbb{Q}$. Supponiamo ora che $f = \frac{a}{b}f_1$ con $\frac{a}{b} \in \mathbb{Q}$ $(a, b \in \mathbb{Z})$ e f_1 primitivo in $\mathbb{Z}[x]$; allora $bdf_0 = asf_1$ e, ancora per il Lemma 8.12, $f_1 = \pm f_0$ e $bd = \pm as$ da cui $\frac{a}{b} = \pm\frac{d}{s}$. ∎

Veniamo ora al Lemma fondamentale per quanto riguarda i polinomi primitivi. Per la sua dimostrazione è conveniente utilizzare la riduzione modulo un primo p dei polinomi interi, cioè l'omomorfismo

$$\begin{array}{ccc} \mathbb{Z}[x] & \to & \mathbb{Z}_p[x] \\ f & \mapsto & \overline{f} \end{array}$$

dove se $f = a_0 + a_1x + \cdots + a_nx^n$, $\overline{f} = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$ (vedi sezione 6.1). Osserviamo che $\overline{f} = 0$ se e soltanto se il primo p divide tutti i coefficienti di f; in particolare, se f è primitivo allora $\overline{f} \neq 0$ nella riduzione per qualsiasi primo p.

Lemma 8.14 (Lemma di Gauss)**.** *Il prodotto di polinomi interi primitivi è primitivo.*

Dimostrazione. Siano $f, g \in \mathbb{Z}[x]$ e supponiamo che il prodotto fg **non** sia primitivo. Allora esiste un primo p che divide tutti i coefficienti di fg. Considerando la riduzione modulo p si ha dunque (ricordando che la riduzione è un omomorfismo):

$$0 = \overline{fg} = \overline{f} \cdot \overline{g}$$

che è una uguaglianza nel dominio d'integrità $\mathbb{Z}_p[x]$. Dunque deve essere $\overline{f} = 0$ oppure $\overline{g} = 0$ e quindi, per quanto osservato, f e g non possono essere entrambi primitivi, dimostrando così il Lemma. ∎

Proposizione 8.15. *Sia $0 \neq f \in \mathbb{Q}[x]$ e scriviamo $f = \gamma f_0$ con $\gamma \in \mathbb{Q}$ e $f_0 \in \mathbb{Z}[x]$ primitivo. Allora f è irriducibile in $\mathbb{Q}[x]$ se e solo se f_0 è irriducibile in $\mathbb{Z}[x]$.*

Dimostrazione. Supponiamo che il polinomio f sia riducibile in $\mathbb{Q}[x]$, cioè che $f = gh$ con $g, h \in \mathbb{Q}[x]$ e $\deg g, \deg h < \deg f$. Scriviamo $g = \alpha g_0$, $h = \beta h_0$ con $\alpha, \beta \in \mathbb{Q}$ e g_0, h_0 polinomi primitivi in $\mathbb{Z}[x]$. Allora $f = \gamma f_0 = \alpha\beta g_0 h_0$. Per il Lemma di Gauss, $g_0 h_0$ è primitivo, e quindi, per il Lemma 8.13, $f_0 = \pm g_0 h_0$ provando che f_0 si riduce in $\mathbb{Z}[x]$.
Viceversa, supponiamo che f_0 si riduca in $\mathbb{Z}[x]$: $f_0 = gh$ con $g, h \in \mathbb{Z}[x]$ e $g \neq \pm 1 \neq h$. Poiché f_0 è primitivo, né g né h appartengono a $\mathbb{Z}$; quindi $\deg g < \deg f_0 = \deg f$ e $\deg h < \deg f$, e dunque $f = (\gamma h)g$ è una decomposizione in fattori propri di f in $\mathbb{Q}[x]$, provando così che f è riducibile in $\mathbb{Q}[x]$. ∎

Questa proposizione mostra, in particolare, che il problema della determinazione della irriducibilità o meno di un polinomio razionale si riconduce al caso di un polinomio intero primitivo. Riterneremo più avanti su questa questione. Prima proviamo il risultato principale di questa sezione.

Teorema 8.16. *$\mathbb{Z}[x]$ è un dominio a fattorizzazione unica;*

Dimostrazione. Sia $f \in \mathbb{Z}[x] \setminus \{0, 1, -1\}$. Proviamo che f ammette un fattorizzazione essenzialmente unica in irriducibili (osserviamo che in questo caso "essenzialmente unica" significa a meno dell'ordine e del segno dei fattori).
Cominciamo con lo scrivere $f = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo, e fattorizziamo f in $\mathbb{Q}[x]$, $f = g_1 g_2 \dots g_k$, con g_i polinomi irriducibili in $\mathbb{Q}[x]$ individuati a meno di moltiplicazione per elementi non nulli di $\mathbb{Q}$. Quindi scriviamo ciascun g_i come $g_i = \gamma_i g_i'$ con $\gamma_i \in \mathbb{Q}$, g_i' polinomio primitivo in $\mathbb{Z}[x]$ individuati a meno del segno. Allora, posto $\gamma = \gamma_1 \gamma_2 \dots \gamma_k$,

$$df_0 = f = \gamma g_1' g_2' g_3' \ \dots \ g_k' \ .$$

Per il Lemma di Gauss $g = g_1' g_2' \dots g_k'$ è primitivo e quindi, per il Lemma 8.13, $\gamma = \pm d$ e $g = \pm f_0$. Inoltre, per la Proposizione 8.15, ogni g_i' è irriducibile in $\mathbb{Z}[x]$.
Quindi, se $d = \pm 1$, allora (a meno del segno)

$$f = g_1' g_2' g_3' \ \dots \ g_k'$$

è una fattorizzazione di f in irriducibili di $\mathbb{Z}[x]$.
Se $d \neq \pm 1$, si fattorizza $d = p_1 p_2 \dots p_s$ come prodotto di primi di $\mathbb{Z}$ (che sono elementi irriducibili in $\mathbb{Z}[x]$) e quindi

$$f = p_1 p_2 \dots p_s g_1' g_2' g_3' \ \dots \ g_k' \qquad (*)$$

è una fattorizzazione di f in irriducibili di $\mathbb{Z}[x]$.
Infine la (essenziale) unicità delle fattorizzazioni $f = df_0$, $d = p_1 p_2 \dots p_s$ e di f_0 come polinomio in $\mathbb{Q}[x]$, assicurano che la fattorizzazione $(*)$ è essenzialmente unica.
∎

Abbiamo dimostrato il Teorema 8.16 per l'anello $\mathbb{Z}$, ma, con un po' di attenzione, non è difficile generalizzare gli argomenti usati ad un qualunque dominio a fattorizzazione unica R. In questo caso, il ruolo svolto da $\mathbb{Q}$ è affidato al campo dell frazioni (sezione 6.3) di R, e la locuzione "a meno del segno" rimpiazzata con "a meno di moltiplicazione per elementi invertibili di R". Si può cosi dimostrare la seguente versione più generale.

Teorema 8.17. *Sia R un dominio a fattorizzazione unica. Allora $R[x]$ è un dominio a fattorizzazione unica.*

Vediamo ora alcuni strumenti pratici che possono essere usati per studiare la riducibilità di un polinomio intero (o razionale). Cominciamo con il richiamare un'osservazione elementare ma utile, la cui dimostrazione si trova nella sezione precedente.

Sia $f = a_0 + a_1 x + \cdots + x^n$ un polinomio monico a coefficienti interi. Allora ogni radice razionale di f è un numero intero e divide a_0.

Esempio 1. Proviamo che il polinomio $x^3 + 2x^2 - x + 2$ è irriducibile in $\mathbb{Q}[x]$. Se f fosse riducibile dovrebbe avere un fattore di grado 1 (attenzione! questa affermazione vale perchè $\deg f \leq 3$) e quindi, per il Teorema di Ruffini, una radice in $\mathbb{Q}$. Ora, per l'osservazione precedente, le eventuali radici razionali di f sono divisori interi di 2. Ma $f(1) = 4,\ f(-1) = 4,\ f(2) = 16$ e $f(-2) = 4$; quindi f non ha radici razionali e pertanto è irriducibile in $\mathbb{Q}[x]$.

Vediamo ora una applicazione della riduzione modulo un primo. Sia p un numero primo. Allora come abbiamo visto, la riduzione modulo p è un omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$; seguendo le notazioni adottate precedentemente, denotiamo con $\overline{f}$ la riduzione modulo p del polinomio $f \in \mathbb{Z}[x]$. Sia f un polinomio primitivo in $\mathbb{Z}[x]$ tale che p non divida il coefficiente direttivo a_n di f. Supponiamo che f sia riducibile in $\mathbb{Z}[x]$; allora $f = gh$ con g, h polinomi in $\mathbb{Z}[x]$ il cui grado (essendo f primitivo) è strettamente minore del grado di f ed il cui coefficiente direttivo non è diviso da p. Applicando la riduzione modulo p si ha $\overline{f} = \overline{g}\overline{h}$ in $\mathbb{Z}_p[x]$, e per la condizione sul coefficiento direttivo, $\deg \overline{g} < \deg \overline{f}$ e $\deg \overline{h} < \deg \overline{f}$. Quindi $\overline{f}$ è riducibile in $\mathbb{Z}_p[x]$. Possiamo enunciare quanto abbiamo così stabilito nel modo seguente:

Criterio 1. *Sia f un polinomio primitivo in $\mathbb{Z}[x]$, sia p un primo che non divide il coefficiente direttivo di f e sia $\overline{f} \in \mathbb{Z}_p[x]$ la riduzione di f modulo p. Se $\overline{f}$ è irriducibile in $\mathbb{Z}_p[x]$ allora f è irriducibile in $\mathbb{Z}[x]$ (e quindi anche in $\mathbb{Q}[x]$).*

Esempio 2. Proviamo che il polinomio

$$\frac{2}{3}x^4 + x^3 + \frac{1}{6}x^2 - \frac{1}{2}x - \frac{2}{3}$$

è irriducibile in $\mathbb{Q}[x]$. Innanzi tutto riportiamoci ad un polinomio intero primitivo: si ha $f = \frac{1}{6}g$ con $g = 4x^4 + 6x^3 + x^2 - 3x - 4$. Ora, 3 non divide il coefficiente direttivo di g e, riducendo modulo 3 si considera

$$\overline{g} = \overline{4}x^4 + \overline{6}x^3 + \overline{1}x^2 - \overline{3}x - \overline{4} = x^4 + x^2 - \overline{1}\ .$$

Proviamo che $\overline{g}$ è irriducibile on $\mathbb{Z}_3[x]$. Innanzi tutto, $\overline{g}(\overline{0}) = -\overline{1},\ \overline{g}(\overline{1}) = \overline{1}$ e $\overline{g}(\overline{2}) = \overline{1}$, quindi $\overline{g}$ non ha radici in $\mathbb{Z}_3[x]$ e dunque (essendo $\mathbb{Z}_3$ un campo) non ha fattori di grado 1 in $\mathbb{Z}_3[x]$. Supponiamo che $\overline{g}$ sia il prodotto di due fattori (monici) di grado 2:

$$x^4 + x^2 - \overline{1} = \overline{g} = (x^2 + ax + b)(x^2 + cx + d)$$

con $a, b, c, d \in \mathbb{Z}_3$. Dal confronto tra i coefficienti di grado 0 risulta $bd = -\overline{1} = \overline{2}$, quindi (a meno di scambiare i due polinomi) possiamo supporre $b = \overline{1}$ e $d = \overline{2}$ ottenendo

$$\overline{g} = (x^2 + ax + \overline{1})(x^2 + cx + \overline{2})$$

il cui confronto dei coefficienti di grado 1,2 e 3 dà: $2a + c = \overline{0},\ ac = \overline{1}\ a + c = \overline{0},$ condizioni che non sono soddisfatte da alcuna coppia $a, c \in \mathbb{Z}_3$.
Quindi $\overline{g}$ è irriducibile in $\mathbb{Z}_3[x]$ e dunque per il Criterio 1, g è irriducibile in $\mathbb{Z}[x]$. Per la Proposizione 8.15, f è irriducibile in $\mathbb{Q}[x]$.

Osserviamo che l'implicazione del Criterio 1 non si inverte; ad esempio $x^2 + 1$ è irriducibile in $\mathbb{Z}[x]$ mentre la sua riduzione modulo 5 è riducibile in $\mathbb{Z}_5[x]$: $x^2 + \overline{1} = (x + \overline{2})(x + \overline{3})$.

Anzi esistono polinomi monici irriducibili in $\mathbb{Z}[x]$ la cui riduzione modulo qualunque primo è riducibile.

Un famoso e utile criterio di irriducibilità, sul quale ci soffermeremo un po' più a lungo è il criterio di Eisenstein.

Criterio di Eisenstein. *Sia $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, con $n \geq 1$, $a_n \neq 0$, e supponiamo che esista un primo p tale che*

(i) p non divide a_n
(ii) p divide $a_0,\ a_1,\ \ldots,\ a_{n-1}$
(iii) p^2 non divide a_0

allora f è irriducibile in $\mathbb{Q}[x]$ e, se è primitivo, f è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Supponiamo che f sia primitivo. Supponiamo per assurdo che $f = gh$ con $g = b_mx^m + \cdots + b_0$ e $h = c_{n-m}x^{n-m} + \cdots + c_0$ polinomi interi di grado positivo. Consideriamo quindi la riduzione modulo p di f; per le condizioni (i) e (ii) si ha

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n}x^n. \tag{8.3}$$

Poiché $\mathbb{Z}_p[x]$ è un dominio a fattorizzazione unica, e x è un suo elemento irriducibile, i divisori propri di $\overline{a_n}x^n$ sono tutti del tipo $\overline{c}x^k$ con $0 \neq \overline{c} \in \mathbb{Z}_p$ e $0 \leq k \leq n$; si deduce quindi da (8.3) che , $\overline{g} = \overline{b_m}x^m$ e $\overline{h} = \overline{c_{n-m}}x^{n-m}$. In particolare si trova $\overline{b_0} = \overline{c_0} = \overline{0}$, il che implica $p|b_0$ e $p|c_0$. Ma allora $p^2|b_0c_0 = a_0$ contro la condizione (iii).
Se f non è primitivo si considera $f = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo e si osserva che, per la condizione (i), p non divide d e dunque si può applicare il criterio al polinomio primitivo f_0. ∎

Prima di vederne delle applicazioni, facciamo un'utile osservazione generale, riguardante quello che è volgarmente chiamato "cambiamento di variabile". Sia R un anello commutativo, e $a, b \in R$ con $a \neq 0$. Il principio di sostituzione assicura che esiste un unico omomorfismo $\nu : R[x] \to R[x]$ che fissa gli elementi di R e manda x in $ax + b$; quello che di solito si intende rappresentare con $f(x) \mapsto f(ax + b)$. Se assumiamo che a sia invertibile in R, l'omomorfismo ν di prima ha un inverso, dato dall'unico omomorfismo di $R[x]$ in sè tale che $x \mapsto a^{-1}x - a^{-1}b$. Dunque, se a è invertibile, l'applicazione ν (che, dal punto di vista pratico, è la sostituzione di x con $ax + b$) è un isomorfismo, e quindi *un automorfismo* di $R[x]$. In particolare ne segue l'utile constatazione che: *se F è un campo, e $a, b \in F$ con $a \neq 0$, allora $f(x) \in F[x]$ è irriducibile se e soltanto se $f(ax + b)$ è irriducibile.*

L'esempio che diamo ora di applicazione del Criterio di Eisenstein è sufficientemente importante da essere enunciato come una Proposizione.

Proposizione 8.18. *Sia p un numero primo. Allora il polinomio*

$$x^{p-1} + x^{p-2} + \ \ldots\ + x^2 + x + 1$$

è irriducibile in $\mathbb{Q}[x]$.

Dimostrazione. Sia $f = x^{p-1} + \ \ldots\ + x + 1$. Poniamo $y = x + 1$ e scriviamo $f(y) = (x + 1)^{p-1} + \ \ldots\ + (x + 1) + 1$. Per quanto osservato prima, f è irriducibile

se e solo se $f(y)$ è irriducibile. Si ha

$$\begin{aligned} xf(y) &= (y-1)(y^{p-1}+\cdots+y+1) = y^p - 1 = (x+1)^p - 1 = \\ &= x^p + \tbinom{p}{1}x^{p-1} + \tbinom{p}{2}x^{p-2} + \ldots + \tbinom{p}{p-1}x + 1 - 1 \\ &= x(x^{p-1} + \tbinom{p}{1}x^{p-2} + \ldots + \tbinom{p}{p-2}x + p) \end{aligned} .$$

Ora, sappiamo che, per ogni $1 \leq i \leq p-1$, p divide $\binom{p}{i}$. Quindi, per il Criterio di Eisenstein,

$$f(y) = x^{p-1} + \binom{p}{1}x^{p-2} + \ \ldots \ + \binom{p}{p-2}x + p$$

è irriducibile, e dunque f è irriduciblile. ∎

Se p è un primo il polinomio $\Phi_p = x^{p-1} + x^{p-2} + \ \ldots \ + x + 1$ si chiama *polinomio ciclotomico p-esimo*, e poichè $(x-1)\Phi_p = x^p - 1$, le sue radici complesse sono le radici p-esime dell'unità diverse da 1.

Fattorizzazioni in $\mathbb{R}[x]$ e $\mathbb{C}[x]$. Completiamo questa sezione illustrando rapidamente la situazione per quanto riguarda i polinomi irriducibili in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$. Una delle proprietà fondamentali dell'anello dei numeri complessi è che esso contiene radici di ogni polinomio non costante. L'enunciato di questo fatto viene tradizionalmente chiamato "**Teorema fondamentale dell'Algebra**" (anche se tale denominazione appare oggi non del tutto giustificata). La sua dimostrazione è in genere fatta usando strumenti del corso di Analisi, e quindi la omettiamo.

Definizione. Un campo F si dice **algebricamente chiuso** se ogni polinomio di grado maggiore o uguale a 1 in $F[x]$ ammette almeno una radice in F.

Teorema 8.19. *Il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso.*

Dalla definizione seguono immediatamente le seguenti proprietà, che valgono in particolare per il campo $\mathbb{C}$. La dimostrazione è lasciata per esercizio.

Proposizione 8.20. *Sia F un campo algebricamente chiuso. Allora*

(1) *I polinomi irriducibili di $F[x]$ sono tutti e soli i polinomi di grado 1.*

(2) *Ogni polinomio $f \in F[x]$ con $\deg f = n \geq 1$ si decompone in $F[x]$ come $f = a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ con $a, \alpha_1, \alpha_2, \ldots, \alpha_n$ elementi di F.*

Vediamo ora cosa si può dire per il campo dei numeri reali $\mathbb{R}$.
Sia $f = a_0 + a_1x + \cdots + a_nx^n$ un polinomio a coefficienti in $\mathbb{R}$ e grado $n \geq 1$. Sia $\alpha \in \mathbb{C}$ una radice (complessa) di f. Ricordando che il coniugio in $\mathbb{C}$ è un isomorfismo che manda ogni numero reale in se stesso, si ha

$$0 = \overline{a_0 + a_1\alpha + \cdots + a_n\alpha^n} = \overline{a_0} + \overline{a_1\alpha} + \cdots + \overline{a_n\alpha}^n == a_0 + a_1\overline{\alpha} + \cdots + a_n\overline{\alpha}^n = f(\overline{\alpha}).$$

Quindi, abbiamo provato il seguente fatto:

Lemma 8.21. *Se α è una radice complessa del polinomio $f \in \mathbb{R}[x]$ allora anche il suo coniugato $\overline{\alpha}$ è una radice di f.*

Proposizione 8.22. *Gli elementi irriducibili di $\mathbb{R}[x]$ sono*

(i) *I polinomi di grado 1.*

(ii) *I polinomi $ax^2 + bx + c$ con $a \neq 0$ e $b^2 - 4ac < 0$.*

Dimostrazione. Chiaramente ogni polinomio di grado 1 è irriducibile (questo vale per coefficienti in qualsiasi campo). Sia quindi $f \in \mathbb{R}[x]$ un polinomio irriducibile di grado almeno 2. Allora f non ha radici in $\mathbb{R}$ (altrimenti, per il Teorema di Ruffini, avrebbe un fattore di grado 1). Sia α una radice in $\mathbb{C}$ di f, allora $\alpha \in \mathbb{C} \setminus \mathbb{R}$ e quindi $\alpha \neq \overline{\alpha}$. Per il Lemma 8.21, $\overline{\alpha}$ è una radice di f e quindi, per il Teorema di Ruffini, $g = (x-\alpha)(x-\overline{\alpha})$ divide f in $\mathbb{C}[x]$, cioè $f = gh$ con $h \in \mathbb{C}[x]$. Ora, se $\alpha = u + iv$ con $u, v \in R$:

$$g = (x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2ux + (u^2+v^2) \in \mathbb{R}[x] \ .$$

Allora, se $f = gq + r$ è la divisione di f per g in $\mathbb{R}[x]$, essa è anche la divisione di f per g in $\mathbb{C}[x]$. Ma, in $\mathbb{C}[x]$, $f = gh$. Per l'unicità della divisione, deve essere $r = 0$ e $h = q \in \mathbb{R}[x]$. Quindi $g|f$ in $\mathbb{R}[x]$. Poichè f è irriducibile, deve essere $f = ag$ per $a \in \mathbb{R}$ (a non è altro che il coefficiente direttivo di f), in particolare $\deg f = 2$.

Infine, sia $f = ax^2 + bx + c$ un polinomio di grado 2 in $\mathbb{R}[x]$. Allora, f è irriducibile se e soltanto se non ha fattori di grado 1, ovvero se e soltanto se non ha radici in $\mathbb{R}$, ed è ben noto che questa condizione equivale all'essere $b^2 - 4ac < 0$. ∎

Da questa proposizione segue che ogni polinomio in $\mathbb{R}[x] \setminus \mathbb{R}$ si fattorizza in $\mathbb{R}[x]$ come il prodotto di polinomi di grado 1 o 2. In particolare, ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha almeno un fattore di grado 1, quindi ha almeno una radice reale. Questo fatto si può dimostrare senza ricorrere alla chiusura algebrica di $\mathbb{C}$. Infatti sia $f \in \mathbb{R}[x]$; denotiamo con $f(x)$ la funzione reale associata ad f, cioè

$$\begin{array}{rccc} f(x): & \mathbb{R} & \to & \mathbb{R} \\ & a & \mapsto & f(a) \end{array}$$

$f(x)$ è una funzione continua. Se f ha grado dispari allora

$$\lim_{x\to+\infty} f(x) = +\infty \qquad \text{e} \qquad \lim_{x\to-\infty} f(x) = -\infty$$

quindi il grafico di $f(x)$ interseca l'asse delle x, e dunque esiste $a \in \mathbb{R}$ tale che $f(a) = 0$.

Esercizio 8.21. Senza usare il Teorema 8.16 si provi che ogni irriducibile di $\mathbb{Z}[x]$ è primo.

Esercizio 8.22. Si fattorizzi il polinomio $2x^4 - x^3 + 6x^2 + 7x - 5$ in $\mathbb{Z}[x]$.

Esercizio 8.23. 1) Si fattorizzi $x^4 + 3x + 2$ in $\mathbb{Q}[x]$.

2) Siano p, q primi positivi. Si provi che, escluso il caso $p = 2$, $q = 3$, il polinomio $x^4 + qx + p$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 8.24. Si provi che per ogni primo p dispari il polinomio $x^p + px + 1$ è irriducibile in $\mathbb{Q}[x]$. [sugg.: si faccia la sostituzione $x = y - 1$.]

8.5. Esercizi.

Esercizio 8.25. Sia A una anello commutativo. Sia I_* un ideale di $A[x]$.

(1) Si provi che l'insieme dei termini noti dei polinomi in I_* costituisce un ideale di A. Viceversa, sia I è un ideale di A; si provi che l'insieme dei polinomi in $A[x]$ il cui termine noto appartiene ad I è un ideale di $A[x]$.

(2) Si provi che l'insieme dei coefficienti direttori dei polinomi in I_* costituisce un ideale di A. Si dice se è vero che, se I è un ideale di A, allora l'insieme dei polinomi in $A[x]$ il cui coefficiente direttore appartiene ad I è un ideale di $A[x]$.

Esercizio 8.26. Sia $Y = \{a_0 + a_1x^2 + a_2x^4 ... + a_nx^{2n} \mid n \in \mathbb{N}, a_i \in \mathbb{Q}\}$. Si provi che Y è un sottoanello ma non è un ideale di $\mathbb{Q}[x]$.

Esercizio 8.27. Sia R un anello commutativo e sia $f \in R[x]$. Si provi che se f è un divisore dello zero in $R[x]$ allora esiste $b \in R$ tale che $b \neq 0_R$ e $bf = 0$. [sugg.: fare induzione su deg f]

Esercizio 8.28. Siano $f = x^4 - x^3 - 4x^2 + 4x$ e $h = x^2 - a$ polinomi a coefficienti in $\mathbb{Q}$. Si determini per quali valori $a \in \mathbb{Q}$ si ha $(h, f) = 1$.

Esercizio 8.29. Si provi che il polinomio $x^3 - 4$ è irriducibile in $\mathbb{Q}[x]$, mentre ammette radici in ciascuno dei campi $\mathbb{Z}_p$ con $p = 3, 5, 7, 11$.

Esercizio 8.30. In $\mathbb{Q}[x]$ si considerino i polinomi

$$f = x^4 + 3x^3 + 2x^2 + x + 6 \qquad g = x^3 + x^2 + 2x + 3 \ .$$

Si determini un massimo comun divisore di f e g in $\mathbb{Q}[x]$.
Sia considerino poi le riduzioni modulo 7, $\overline{f}$, $\overline{g}$, di f e di g; se ne determini un massimo comun divisore in $\mathbb{Z}_7[x]$ (si confronti il risultato con il caso dei razionali).

Esercizio 8.31. Sia A un dominio d'integrità e sia $0 \neq f \in A[x]$. Si provi che il numero di radici distinte di f in A è al più deg f.

Esercizio 8.32. Siano $c = \sqrt{5}$, $d = (\sqrt{5})^{-1}$. Denotiamo con σ_c, σ_d rispettivamente gli automorfismi di sostituzione da $\mathbb{Q}[x]$ in $\mathbb{R}$, definiti da, per ogni $f \in \mathbb{Q}[x]$:

$$\sigma_c(f) = f(c) \qquad \sigma_d(f) = f(d) \ .$$

(a) σ_c è iniettivo ?

(b) $d \in Im(\sigma_c)$?

(c) $Im(\sigma_c) \cap Im(\sigma_d)$ è finito o infinito ?

Esercizio 8.33. Sia p un numero primo, con $p \equiv 2 \pmod 3$. Si provi che il polinomio $x^2 + x + 1$ è irriducibile in $\mathbb{Z}_p[x]$.

Esercizio 8.34. Sia $f = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Q}[x]$. Definiamo il *polinomio derivato* di f, come

$$f' = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1$$

(a) Si dimostri che per ogni $f, g \in \mathbb{Q}[x]$ si ha $(fg)' = f'g + fg'$.

(b) Sia $b \in \mathbb{Q}$; si provi che b è radice comune di f e di f' se e solo se $(x-b)^2$ divide f (in questo caso si dice che b è una radice multipla di f).

Esercizio 8.35. Provare che se f è un polinomio irriducibile in $\mathbb{Q}[x]$ allora f non ha radici multiple in $\mathbb{C}$.

Esercizio 8.36. Sia R un anello commutativo, e x, y due distinte indeterminate. Si enunci e dimostri un principio di sostituzione "in due variabili" per $R[x, y]$, analogo al Teorema 8.3. [Nella dimostrazione potete applicare 8.3]

Esercizio 8.37. Sia R un anello commutativo. Si provi che

$$\{f \in R[x, y] \mid f(a, b) = f(b, a) \text{ per ogni } a, b \in R\}$$

è un sottoanello ma non un ideale di $R[x, y]$.

Esercizio 8.38. Sia $\Sigma = \{f \in \mathbb{Q}[x] \mid f(n) = f(-n) \text{ per ogni } n \in \mathbb{N}\}$.

(a) Si provi che Σ è un sottoanello di $\mathbb{Q}[x]$.

(b) Si provi che Σ è un dominio euclideo.

(c) Sia $f \in \Sigma$; si provi che $f(r) = f(-r)$ per ogni $r \in \mathbb{Q}$.

Esercizio 8.39. Sia F un campo. Nell'anello $F[x, y]$ si consideri l'ideale (x, y). Si provi che $(x, y) = \{f \in F[x, y] \mid f(0, 0) = 0\}$, e che (x, y) non è principale. Si provi quindi che $S = \{f \in F[x, y] \mid f(a, a) = 0 \text{ per ogni } a \in F\}$ è un ideale è principale di $F[x, y]$.

Esercizio 8.40. Si provi che per ogni $f, g \in \mathbb{Q}[x]$ si ha

$$(f, g) = (f + g, f - g).$$

Si dica se la stessa proprietà vale in $\mathbb{Z}$ (invece che in $\mathbb{Q}[x]$).

Esercizio 8.41. In $\mathbb{Q}[x]$ si trovi un generatore del seguente ideale

$$(x^7 + 2x^4 + x^3 + x + 3,\ x^4 + 1)\ .$$

Esercizio 8.42. Siano $f, g \in \mathbb{Q}[x]$ polinomi non nulli. Sia d un MCD di f, g in $\mathbb{Q}[x]$. Si provi che d è un MCD di f, g in $\mathbb{R}[x]$.

Esercizio 8.43. Si fattorizzino i polinomi $x^9 - x$ e $x^5 - 2x^3 - x^2 + 2$ in irriducibili in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$.

Esercizio 8.44. Siano $a, b \in \mathbb{Q}$ (fissati), e si consideri l'applicazione $\Phi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}$ definita da $\Phi(f) = (f(a), f(b))$ per ogni $f \in \mathbb{Q}[x]$.

(a) Si provi che Φ è un omomorfismo d'anelli.

(b) Si determini $Ker(\Phi)$ (trovandone un generatore).

(c) Si provi che $\{a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{Q}[x] \mid a_0 + a_2 + \cdots = 0 = a_1 + a_3 + \dots\}$ è un ideale di $\mathbb{Q}[x]$ e si trovi un suo generatore.

Esercizio 8.45. Si dica quali fra i seguenti polinomi sono irriducibili in $\mathbb{Q}[\sqrt{2}][x]$:

$$x^2 - 2,\quad x^2 + 2,\quad x^2 - 4x + 2,\quad x^3 - 2,\quad x^4 + 1.$$

Esercizio 8.46. Siano $f, g \in \mathbb{Z}[x]$ polinomi monici. Si provi che il massimo comun divisore di f e g in $\mathbb{Q}[x]$ ha coefficienti interi.

Esercizio 8.47. Si provi che le condizioni su un campo F descritte dai punti (1) e (2) della Proposizione 8.20 sono entrambe equivalenti ad affermare che F è algebricamente chiuso.

Esercizio 8.48. Si fattorizzi in prodotto di irriducibili i seguenti polinomi:

1) $x^4 - x^2 - 2 \in K[x]$, con $K = \mathbb{Z}/2\mathbb{Z}$, e $K = \mathbb{Q}$.

2) $x^4 + 1 \in K[x]$, con $K = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z}$.

3) $f = x^5 - 2x^4 + x^3 - 9x^2 + 18x - 9$ in $\mathbb{Q}[x]$.

4) $x^5 - 1$ in $\mathbb{Z}_p[x]$, con $p = 3,\ 5,\ 11$.

Esercizio 8.49. Si determini per quali valori $h \in \mathbb{Z}$ il polinomio $f_h = x^4 - x^2 + hx + 1$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 8.50. (Funzioni polinomiali, I) Sia F un campo. L'anello F^F di tutte le funzioni da F in F è definito analogamente a quanto abbiamo visto per $\mathbb{R}^{\mathbb{R}}$ nella sezione 5.1 (vedi anche l'Esercizio 5.27). Ad ogni polinomio $f \in F[x]$ è associata una *funzione polinomiale* $f^* \in F^F$, definita mediante sostituzione, ovvero si pone $f^*(a) = f(a)$ per ogni $a \in F$ (si osservi che, se $f = a_0 + a_1 x + \cdots + a_n$ allora, denotando con ι l'applicazione identica su F, si ha, nell'anello F^F, $f^* = a_0 + a_1\iota + \cdots + a_n\iota^n$). Definiamo quindi l'applicazione $\Phi : F[x] \to F^F$, ponendo $\Phi(f) = f^*$, per ogni $f \in F$. L'immagine di Φ si chiama insieme delle *funzioni polinomiali* di F.
Si provi che Φ è un omomorfismo d'anelli. Si provi quindi che se F *è infinito*, allora Φ è iniettiva. [applicare la conseguenza del teorema di Ruffini]
Sia quindi p un numero primo e $F = \mathbb{Z}_p$. In questo caso, $\Phi : F[x] \to F^F$ non può essere iniettiva (dato che F^F è finito mentre $F[x]$ è comunque infinito); si provi che

$$\ker \Phi = (x^p - x).$$

[applicare il Teorema di Fermat per una inclusione, Ruffini e il Teorema 8.5 per l'altra]

Esercizio 8.51. (Funzioni polinomiali, II) Siano $F = \mathbb{Z}_p$ e Φ come nell'esercizio precedente, e sia $X = \{f \in F[x] \mid f = 0 \text{ o } \deg f \leq p - 1\}$.

(1) Si provi che la restrizione di Φ a X è iniettiva. [Ruffini]

(2) Si provi che ogni funzione di F in sé è polinomiale. [contare].

(Quanto negli ultimi due esercizi vale in generale per un campo F di ordine finito)

Esercizio 8.52. (Funzioni polinomiali, III) Sia F un campo. Il concetto di funzione polinomiale si estende nel modo naturale a polinomi in più indeterminate. Si consideri, ad esempio, il caso di due indeterminate x, y; si definisca una applicazione $\Phi_2 : F[x, y] \to F^{F \times F}$, analoga alla Φ degli esercizi precedenti; si provi che è un omomorfismo d'anelli e che è iniettiva se e solo se F è infinito.

9

Quozienti

9.1. Anelli quoziente.

In questa sezione, la costruzione degli anelli del tipo $\mathbb{Z}/n\mathbb{Z}$ verrà estesa ad un anello generico R (non necessariamente commutativo) e qualunque suo ideale proprio I.

Sia dunque I un ideale dell'anello R. Per ogni $a \in R$ si definisce la **classe laterale** (modulo l'ideale I) di rappresentante a,

$$a + I = \{\ a + x \mid x \in I\ \}.$$

Si tratta quindi di un sottoinsieme non vuoto di R (dato che $a = a + 0_r \in a + I$). Si pone quindi

$$R/I = \{\ a + I \mid a \in R\ \}$$

l'insieme di tutte la classi laterali distinte modulo I.

Ora, fissato l'ideale I, è sempre possibile definire una equivalenza $\sim_I$ su R, in modo tale che le classi laterali modulo I coincidono con le classi di equivalenza modulo $\sim_I$. Precisamente, per ogni $x, y \in R$, si pone

$$x \sim_I y \quad \Leftrightarrow \quad x - y \in I.$$

Innanzi tutto, verifichiamo che $\sim_I$ è una equivalenza su R. Come si vedrà, quasto fatto dipende essenzialmente dalle proprietà additive degli ideali. Per ogni $a \in R$, $a - a = 0_R \in I$, quindi $a \sim_I a$, e pertanto $\sim_I$ è riflessiva. Siano $a, a \in R$ con $a \sim_I b$; allora $a - b \in I$, dunque $b - a = -(a - b) \in I$, cioè $b \sim_I a$, provando che $\sim_I$ è simmetrica. Infine, se $a, b, c \in R$ sono tali che $a \sim_I b$ e $b \sim_I c$, allora $a - b \in$ e $b - c \in I$, da cui segue $a - c = (a - b) + (b - c) \in I$, e quindi $a \sim_I c$. Pertanto $\sim_I$ è anche transitiva, e dunque è una relazione di equivalenza.
Ora, dato $a \in R$, la classe di equivalenza di a modulo $\sim_I$ è costituita da *tutti gli elementi $b \in R$ tali che la differenza $x = b - a$ appartiene all'ideale I*; si tratta cioè di tutti i $b \in R$ che si possono scrivere nella forma $b = a + x$ con $x \in I$. Dunque, la classe di equivalenza di a modulo $\sim_I$ coincide con la classe laterale $a + I$, come definita all'inizio della sezione.

Dalla teoria generale delle relazioni d'equivalenza, segue che le classi laterali modulo l'ideale I costituiscono una partizione di R, in particolare esse sono a due a due disgiunte, ed il loro insieme R/I è l'insieme quoziente $R/\sim_I$. Ancora, evidenziamo il seguente elementare ma importante fatto.

Lemma 9.1. *Sia I un ideale dell'anello R, e siano $a, b \in R$. Allora*

$$a + I = b + I \quad \Leftrightarrow \quad a - b \in I.$$

Da qui in avanti assumiamo che l'ideale I di R sia proprio (cioè $I \neq R$). In questa situazione, nell'insieme quoziente R/I definiamo un'operazione di somma, ed un'operazione di prodotto, ponendo, per ogni $a + I, b + I \in R/I$,

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

dove le operazioni tra i rappresentanti a e b delle due classi sono quelle nell'anello R.

Prima di fare ogni ulteriore osservazione, è indispensabile stabilire che quelle date sopra sono **buone** definizioni, che effettivamente determinano operazioni sull'insieme quoziente. Occorre cioè provare che il risultato (come classe laterale) non dipende dalla scelta dei due particolari rappresentanti a e b ma solo dalle loro classi $a + I$ e $b + I$. Siano dunque a' e b' elementi di R tali che

$$\begin{cases} a + I = a' + I \\ b + I = b' + I \end{cases}$$

Allora $a - a' \in I$ e $b - b' \in I$. Poiché I è un ideale, si ha allora

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

e dunque $(a + b) + I = (a' + b') + I$, mostrando che la somma è ben definita.
Tenendo anche conto delle proprietà di assorbimento di I, si ha inoltre

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$$

(dato che $(a - a')b \in I$ e $a'(b - b') \in I$). Dunque $ab + I = a'b' + I$, provando che il prodotto su R/I è ben definito.

A questo punto, si verifica facilmente che, rispetto a tali operazioni di somma e prodotto R/I è un anello che si chiama **anello quoziente** di R modulo I. In tale anello

- $0_{R/I} = 0_R + I = I$;
- per ogni $a + I \in R/I$, $-(a + I) = (-a) + I$;
- $1_{R/I} = 1_R + I$ (la condizione che I sia un ideale proprio serve ad evitare che R/I sia degenere);

Ad esempio, per $n \geq 2$, l'anello delle classi resto $\mathbb{Z}/n\mathbb{Z}$ è proprio l'anello quoziente di $\mathbb{Z}$ modulo l'ideale $n\mathbb{Z}$.

Esempio. Consideriamo l'anello $\mathbb{R}^{\mathbb{R}}$ di tutte le applicazioni $f : \mathbb{R} \to \mathbb{R}$. Si verifica facilmente che l'insieme

$$I = \{ f \in \mathbb{R}^{\mathbb{R}} \mid f(0) = 0 \}$$

è un ideale di $\mathbb{R}^{\mathbb{R}}$ (vedi sezione 5.3). È quindi possibile costruire l'anello quoziente $\mathbb{R}^{\mathbb{R}}/I$, i cui elementi sono le classi laterali $f + I$, al variare di $f \in \mathbb{R}^{\mathbb{R}}$. Osserviamo che $f + I = g + I$ se e soltanto se $f - g \in I$, ovvero $0 = (f - g)(0) = f(0) - g(0)$, cioè se e solo se $f(0) = g(0)$.

Per ogni $r \in \mathbb{R}$, denotiamo con C_r la funzione costante definita da $C_r(x) = r$ per ogni $x \in \mathbb{R}$. Da quanto osservato sopra, segue in particolare che, dati $r, s \in \mathbb{R}$

$$C_r + I = C_s + I \quad \Leftrightarrow \quad r = s,$$

e quindi che, al variare di $r \in \mathbb{R}$, le classi laterali $C_r + I$ sono tutte distinte. Ancora, se $f \in \mathbb{R}^{\mathbb{R}}$, allora $C_{f(0)}(0) = f(0)$, e dunque $C_{f(0)} + I = f + I$. In conclusione,

$$\frac{\mathbb{R}^{\mathbb{R}}}{I} = \{\ C_r + I \mid r \in \mathbb{R}\ \},$$

e le classi $C_r + I$ sono tutte distinte (questo si esprime dicendo che l'insieme $\{C_r \mid r \in \mathbb{R}\}$ è un sistema completo di rappresentanti delle classi laterali di $\mathbb{R}^{\mathbb{R}}$ modulo I).
Inoltre, proprio per come sono definite le operazioni nel quoziente $\mathbb{R}^{\mathbb{R}}/I$, si può facilmente verificare che l'applicazione $\Psi : \mathbb{R} \longrightarrow \mathbb{R}^{\mathbb{R}}/I$, definita da $\Psi(r) = C_r + I$ per ogni $r \in \mathbb{R}$, è un isomorfismo d'anelli. Quest'ultimo fatto non è un caso, ed il motivo verrà chiarito nella sezione che segue.

Come c'è da aspettarsi, e come vedremo anche nelle prossime sezioni, vi sono forti legami tra le proprietà di un ideale e quelle del suo corrispondente anello quoziente. Il seguente è un primo rilevante esempio di ciò.

Teorema 9.2. *Sia R un anello commutativo, ed I un ideale di R. Allora I è un ideale primo se e solo se l'anello quoziente R/I è un dominio d'integrità.*

Dimostrazione. ($\Rightarrow$) Sia I un ideale primo dell'anello commutativo R (quindi R/I è non degenere, dato che $I \neq R$). Siano $a + I$ e $b + I$ elementi di R/I tali che

$$ab + I = (a + I)(b + I) = 0_{r/I} = I.$$

Allora $ab \in I$ e, poiché I è un ideale primo, si ha $a \in I$ oppure $b \in I$. Nel primo caso $a + I = I = 0_{R/I}$; altrimenti $b + I = I = 0_{R/I}$. Dunque R/I è un dominio d'integrità.

($\Leftarrow$) Sia R/I un dominio d'integrità, e siano $a, b \in R$ tali che $ab \in I$. Allora,

$$0_{R/I} = I = ab + I = (a + I)(b + I).$$

Poiché R/I è un dominio d'integrità, si ha allora $a + I = 0_{R/I}$, oppure $b + I = 0_{R/I}$. Nel primo caso $a \in I$, e nel secondo, $b \in I$. Dunque I è un ideale primo di R. ∎

Esercizio 9.1. Sia R un anello commutativo, sia a un elemento nilpotente di R e sia $J = (a)$ l'ideale generato da a. Sia $b \in R$ tale che $b + J$ è un elemento nilpotente dell'anello quoziente R/J. Si provi che b è un elemento nilpotente di R.

Esercizio 9.2. Sia A un dominio di integrità e sia I un ideale di A tale che A/I è isomorfo a $\mathbb{Z}/p\mathbb{Z}$, con p un numero primo. Si dimostri che $char(A) \in \{0, p\}$.

Esercizio 9.3. Si provi che l'anello quoziente $\mathbb{Q}[x]/(x^2)$ non è un dominio d'integrità. Si provi che l'anello $\mathbb{Q}[x]/(x + 1)$ è isomorfo a $\mathbb{Q}$.

Esercizio 9.4. Sia F un campo e sia $0 \neq f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in F[x]$. Si provi che la classe laterale $x + (f)$ è un elemento invertibile di $F[x]/(f)$ se e solo se $a_0 \neq 0$.

9.2. Quozienti e omomorfismi.

Sia $\phi : R \to S$ un omomorfismo d'anelli. Abbiamo dimostrato in precedenza (Teorema 5.16) che il nucleo $\ker(\phi) = \{a \in R \mid \phi(a) = 0_S\}$ è un ideale di R.

Viceversa, sia I un ideale dell'anello R. Si verifica facilmente che la *proiezione canonica*

$$\begin{array}{rccc} \pi : & R & \to & R/I \\ & a & \mapsto & a+I \end{array}$$

è un omomorfismo suriettivo di anelli. Inoltre, $\ker(\pi) = I$; infatti, tenendo conto del Lemma 9.1,

$$\ker(\pi) = \{a \in R \mid \pi(a) = 0_{R/I}\} = \{a \in R \mid a + I = I\} = \{a \in R \mid a \in I\} = I.$$

Quindi abbiamo provato la seguente fondamentale fatto.

Proposizione 9.3. *Un sottoinsieme di un anello è un ideale se e solo se è il nucleo di qualche omomorfismo dell'anello.*

Proviamo ora un teorema fondamentale riguardante omomorfismi e quozienti, che ha un corrispettivo in diverse altre strutture algebriche.

Teorema 9.4 (di omomorfismo)**.** *Sia $\phi : R \to S$ un omomorfismo di anelli. Siano $I = \ker(\phi)$ il suo nucleo, e π la proiezione canonica di R su R/I. Allora esiste un unico omomorfismo $\overline{\phi} : R/I \to S$ tale che $\overline{\phi} \circ \pi = \phi$; inoltre $\overline{\phi}$ è iniettivo e $Im(\overline{\phi}) = Im(\phi)$.*

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo di anelli, e $I = \ker(\phi)$. Definiamo un'applicazione $\overline{\phi} : R/I \to S$ ponendo, per ogni $a + I \in R/I$,

$$\overline{\phi}(a + I) = \phi(a).$$

Verifichiamo, innanzi tutto, che questa è una buona definizione. Siano $a, a' \in R$ tali che $a + I = a' + I$; allora $a - a' \in I = \ker(\phi)$, e quindi

$$0_S = \phi(a - a') = \phi(a) - \phi(a'),$$

da cui segue $\phi(a) = \phi(a')$, ovvero (come deve essere) $\overline{\phi}(a + I) = \overline{\phi}(a' + I)$.

Proviamo ora che $\overline{\phi}$ è un omomorfismo di anelli; ciò dipende dal fatto che tale è ϕ. Siano $a + I, b + I \in R/I$; allora

$$\begin{array}{rcl} \overline{\phi}((a+I)+(b+I)) & = & \overline{\phi}(a+b+I) = \phi(a+b) = \phi(a) + \phi(b) = \overline{\phi}(a+I) + \overline{\phi}(b+I) \\ \overline{\phi}((a+I)(b+I)) & = & \overline{\phi}(ab+I) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(a+I)\overline{\phi}(b+I) \end{array}$$

ed inoltre

$$\overline{\phi}(1_{R/I}) = \overline{\phi}(1_R + I) = \phi(1_R) = 1_S.$$

Dunque $\overline{\phi}$ è un omomorfismo. Per dimostrarne l'iniettività è ora sufficiente provare che il suo nucleo è banale.

$$\begin{array}{rcl} \ker(\overline{\phi}) & = & \{a + I \in R/I \mid \overline{\phi}(a + I) = 0_S\} = \{a + I \in R/I \mid \phi(a) = 0_S\} \\ & = & \{a + I \in R/I \mid a \in I\} = \{I\} = \{0_{R/I}\} \end{array}$$

dunque $\overline{\phi}$ è iniettivo. Il fatto che $Im(\overline{\phi}) = Im(\phi)$ è chiaro dalla definizione di $\overline{\phi}$. Infine, per ogni $a \in R$,

$$\overline{\phi} \circ \pi(a) = \overline{\phi}(\pi(a)) = \overline{\phi}(a + I) = \phi(a)$$

e dunque $\overline{\phi} \circ \pi = \phi$.

Infine, l'unicità dell'omomorfismo $\overline{\phi}$ è quasi ovvia: se $\psi : R/I \to S$ è un omomorfismo tale che $\psi \circ \pi = \phi$, allora, per ogni $a + I \in R/I$.

$$\psi(a + I) = \psi(\pi(a)) = \phi(a) = \overline{\phi}(a + I),$$

e dunque $\psi = \overline{\phi}$. ∎

Una conseguenza immediata ma molto importante è il seguente

Corollario 9.5. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

$$R/\ker(\phi) \simeq Im(\phi);$$

in particolare, se ϕ è suriettivo allora $R/\ker(\phi) \simeq S$.

Esempio. Rivediamo alla luce di questo corollario l'ultima osservazione dell'esempio alla fine della sezione precedente. Definiamo $\phi : \mathbb{R}^{\mathbb{R}} \longrightarrow \mathbb{R}$, ponendo, per ogni $f \in \mathbb{R}^{\mathbb{R}}$, $\phi(f) = f(0)$. Allora, come si verifica facilmente, ϕ è un omomorfismo suriettivo di anelli, ed il nucleo di ϕ è proprio l'ideale $I = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(0) = 0\}$ definito nell'esempio. Per il Corollario 9.5, si ha quindi che esiste un isomorfismo $\overline{\phi} : \mathbb{R}^{\mathbb{R}}/I \to \mathbb{R}$ (che è l'inverso dell'isomorfismo Ψ descritto nell'esempio).

Il prossimo Teorema prosegue nell'analisi degli anelli quoziente modulo il nucleo di un omomorfismo. Premettiamo un facile Lemma (vedi Esercizio 5.22).

Lemma 9.6. *Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli. Allora*

i) Se I è un ideale di R, $\phi(I)$ è un ideale di S.

ii) Se T è un ideale di S, la sua immagine inversa $\phi^{-1}(T)$ è un ideale di R che contiene $\ker(\phi)$.

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli.

i) Sia I un ideale di R Allora, $\phi(I) \neq \emptyset$ perchè $0_S = \phi(0_R) \in \phi(I)$; inoltre, se $x, y \in \phi(I)$, esistono $a, b \in I$ tali che $x = \phi(a)$, $y = \phi(b)$ e, poiché I è un ideale, $x - y = \phi(a) - \phi(b) = \phi(a - b) \in \phi(I)$. Infine sia $x = \phi(a) \in \phi(I)$ (con $a \in I$) e $s \in S$; poiché ϕ è suriettivo, esiste $r \in R$ tale che $s = \phi(r)$, quindi $xs = \phi(a)\phi(r) = \phi(ar) \in \phi(I)$ e similmente $sx \in \phi(I)$. Dunque $\phi(I)$ è un ideale di S.

ii) Sia T un ideale di S, e sia $M = \phi^{-1}(T)$ la sua immagine inversa rispetto a ϕ; proviamo che M è un ideale di R che contiene $\ker(\phi)$. Innanzi tutto, per ogni $a \in \ker(\phi)$ si ha $\phi(a) = 0_S \in T$, quindi $a \in \phi^{-1}(T) = M$, e dunque $\ker(\phi) \subseteq M$. Resta da provare che M è un ideale; siano $a, b \in M$ allora $\phi(a), \phi(b) \in T$ ed essendo T un ideale, $\phi(a - b) = \phi(a) - \phi(b) \in T$, e quindi $a - b \in \phi^{-1}(T) = M$; infine, se $a \in M$ e $r \in R$ allora $\phi(ar) = \phi(a)\phi(r) \in T$ perché $\phi(a) \in T$ e T è un ideale di S; quindi $ar \in M$ e similmente si prova che $ra \in M$. Dunque M è un ideale di R che contiene $\ker(\phi)$. ∎

Teorema 9.7 (di Corrispondenza)**.** *Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli e sia $K = \ker(\phi)$. Allora ϕ definisce una biezione Φ tra l'insieme degli ideali di R che contengono K e l'insieme di tutti gli ideali di S. Inoltre, per ogni ideale I contenente K, I è un ideale massimale (primo) in R se e soltanto se $\Phi(I)$ è ideale massimale (rispettivamente, primo) in S.*

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli, e denotando con $\mathcal{A}$, $\mathcal{B}$ rispettivamente l'insieme degli ideali di R che contengono $K = \ker(\phi)$ e l'insieme di tutti gli ideali di S. Per il lemma precedente, possiamo dunque definire le seguenti applicazioni:

$$\begin{array}{rccc} \Phi : & \mathcal{A} & \to & \mathcal{B} \\ & I & \mapsto & \phi(I) \end{array}$$

$$\begin{array}{rccc} \Psi : & \mathcal{B} & \to & \mathcal{A} \\ & T & \mapsto & \phi^{-1}(T) \end{array}$$

Dimostriamo che Φ e Ψ sono una l'inversa dell'altra.
Sia pertanto $I \in \mathcal{A}$. Allora

$$(\Psi \circ \Phi)(I) = \Psi(\Phi(I)) = \Psi(\phi(I)) = \phi^{-1}(\phi(I)).$$

Ora, $I \subseteq \phi^{-1}(\phi(I))$ per definizione di immagine inversa. Viceversa, sia $a \in \phi^{-1}(\phi(I))$; allora $\phi(a) \in \phi(I)$, e dunque esiste $b \in I$ tale che $\phi(a) = \phi(b)$; da ciò segue che $\phi(a - b) = 0_S$, ovvero che $a - b \in \ker(\phi) \subseteq I$. Dunque $a - b = c \in I$, e pertanto $a = b + c \in I$, provando che $\phi^{-1}(\phi(I)) \subseteq I$. Quindi

$$I = \phi^{-1}(\phi(I)) = (\Psi \circ \Phi)(I).$$

Sia ora $T \in \mathcal{B}$. Allora, ancora per definizione di immagine inversa,

$$\phi(\phi^{-1}(T)) \subseteq T.$$

Viceversa, siccome ϕ è suriettivo, per ogni $t \in T$ esiste $a \in R$ tale che $\phi(a) = t$ (dunque $a \in \phi^{-1}(T)$); quindi $T \subseteq \phi(\phi^{-1}(T))$. Pertanto

$$(\Phi \circ \Psi)(T) = \phi(\phi^{-1}(T)) = T.$$

Dunque Φ e Ψ sono una l'inversa dell'altra; quindi, in particolare, sono biezioni.

L'affermazione che, per ogni $I \in \mathcal{A}$, I è massimale (primo) in R se e soltanto se $\Phi(I)$ è massimale (rispettivamente, primo) in S non è difficile ed è lasciata per esercizio.
■

Osserviamo che l'ipotesi che l'omomorfismo ϕ è suriettivo non è limitante; infatti l'immagine $Im(\phi)$ di un omomorfismo di anelli $\phi : A \to B$ è un anello, possiamo quindi applicare il teorema di corrispondenza, rimpiazzando B con $Im(\phi)$ (tenendo conto che, quindi, vanno considerati gli ideali di quest ultimo).

La prima fondamentale applicazione del Teorema di corrispondenza è la descrizione degli ideali di un anello quoziente. Siano I, K ideali dell'anello R tali che $K \subseteq I$. Denotiamo con I/K l'immagine di I tramite la proiezione canonica π di R su R/K, cioè $I/K = \pi(I) = \{\ a + K \mid a \in I\ \}$. Per il Teorema di Corrispondenza applicato a π, I/K è un ideale di R/K. Si dimostra quindi il seguente

Teorema 9.8. *Sia K un ideale dell'anello R. Gli ideali dell'anello quoziente R/K sono tutti e soli quelli del tipo T/K al variare di T nell'insieme degli ideali di R che contengono K.*

Dimostrazione. Sia K un ideale dell'anello R; la proiezione canonica $\pi : R \to R/K$ è un omomorfismo suriettivo il cui nucleo è K. Per il teorema di Corrispondenza, gli ideali di R/K sono quindi le immagini tramite la proiezione degli ideali T di R tali che $K \subseteq T$, ovvero sono tutti e soli quelli del tipo T/K definiti prima dell'enunciato. ■

Caso importante. Dato $n \geq 1$, consideriamo l'anello quoziente $\mathbb{Z}/n\mathbb{Z}$. I suoi ideali sono in corrispondenza con gli ideali $m\mathbb{Z}$ di $\mathbb{Z}$ tali che $n\mathbb{Z} \subseteq m\mathbb{Z}$ (con $n, m \geq 0$). Per la Proposizione 7.1 quest'ultima condizione si verifica se e solo se $m|n$. Quindi, gli ideali di $\mathbb{Z}/n\mathbb{Z}$ sono tutti e soli quelli del tipo

$$m\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} \mid x \in m\mathbb{Z}\} = \{mz + n\mathbb{Z} \mid z \in \mathbb{Z}\} = \{mz + n\mathbb{Z} \mid 0 \leq mz \leq n-1\}$$

con $m|n$.
Ad esempio, gli ideali di $\mathbb{Z}/12\mathbb{Z}$ sono (utilizzando la convenzione di indicare con una barra le classi resto: $a + 12\mathbb{Z} = \overline{a}$):

$$\begin{aligned}
\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{1},\ \overline{2},\ \ldots, \overline{11}\ \}\ , \\
2\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{2},\ \overline{4},\ \overline{6},\ \overline{8},\ \overline{10}\ \}\ , \\
3\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{3},\ \overline{6},\ \overline{9}\ \}\ , \\
4\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{4},\ \overline{8}\ \}\ , \\
6\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{6}\ \}\ , \\
12\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0}\ \}\ .
\end{aligned}$$

Esempio . Sia $R = \mathbb{Z}[\sqrt{2}] = \{\ x + y\sqrt{2} \mid x, y \in \mathbb{Z}\ \}$. Si provi che R è un anello (dimostrando che è un sottoanello di $\mathbb{R}$). Consideriamo il seguente ideale di R:

$$I = \{\ x + y\sqrt{2} \mid x, y \in 2\mathbb{Z}\ \}$$

(I è - lo si verifichi - l'ideale generato da 2 in R). Vogliamo determinare gli ideali dell'anello quoziente R/I. Per il Teorema precedente, ciò si realizza determinando gli ideali J di R che contengono I. Cominciamo con

$$K = (\sqrt{2}) = \{\ \sqrt{2}(y + x\sqrt{2}) \mid x, y \in \mathbb{Z}\ \} = \{\ 2x + y\sqrt{2} \mid x, y \in \mathbb{Z}\ \}$$

chiaramente $I \subseteq K$ (e $I \neq K$).
Sia ora J ideale di R con $I \subseteq J$. Supponiamo che J contenga un elemento $x + y\sqrt{2}$ con $2 \not| x$; allora $x - 1 \in 2\mathbb{Z}$, quindi $x - 1 \in I \subseteq J$, dunque $x + y\sqrt{2} - (x-1) = 1 + y\sqrt{2} \in J$. Poichè J è ideale si ha $2y + \sqrt{2} = (1 + y\sqrt{2})\sqrt{2} \in J$ e dunque $\sqrt{2} \in J$ (dato che $2y \in I \subseteq J$); quindi $1 = (1 + y\sqrt{2}) - y\sqrt{2} \in J$, che implica $J = R$.
Sia dunque $J \neq R$ allora, per quanto dimostrato sopra, $J \subseteq K$. Supponiamo $I \neq J$. Allora esiste un elemento $x + y\sqrt{2} \in J$ con y dispari (e x pari dato che $J \subseteq K$). Poichè $x, (y-1)\sqrt{2} \in J$ si ha $\sqrt{2} = (x + y\sqrt{2}) - x - (y-1)\sqrt{2} \in J$; ma allora $K = (\sqrt{2}) \subseteq J$ e quindi $J = K$.
In conclusione, gli ideali di R che contengono I sono I, K ed R; di conseguenza, gli ideali di R/I sono $I/I = \{0_{R/I}\}$, K/I e R/I.

Esercizio 9.5. Sia $f: R \to S$ un omomorfismo suriettivo di anelli commutativi, e sia K il nucleo di f. Sia I un ideale massimale di R. Si dimostri che si ha una delle seguenti possibilità:

- $f(I)$ Ŕ un ideale massimale di S;
- $K + I = R$.

Esercizio 9.6. (Teorema cinese del Resto generalizzato) Sia R un anello commutativo, e siano I_1, I_2 ideali propri di R tali che $R = I_1 + I_2$. Si provi che

$$\frac{R}{I_1 \cap I_2} \simeq \frac{R}{I_1} \times \frac{R}{I_2}$$

[sugg.: provare che la applicazione $R \to R/I_1 \times R/I_2$ definita da $a \mapsto (a+I_1, a+I_2)$ è un omomorfismo suriettivo il cui nucleo è $I_1 \cap I_2$.]
Dedurre, applicando il punto precedente all'anello $\mathbb{Z}$, il Teorema Cinese dei resti (Teorema 4.13).

Esercizio 9.7. Sia R l'anello $\mathbb{Z}/24\mathbb{Z}$.

(1) Quali sono gli ideali massimali di R? E quelli primi?

(2) Descrivere i campi F tali che esiste un omomorfismo suriettivo $R \to F$.

Esercizio 9.8. Sia p un numero primo fissato e sia $R = \{ \frac{m}{p^i} \mid m \in \mathbb{Z}, i \in \mathbb{N} \}$. Sia q un numero primo con $q \neq p$, e sia

$$J = \left\{ \frac{m}{p^i} \in R \mid q \text{ divide } m \right\}.$$

Si provi che J è un ideale primo di R.

9.3. Quozienti di un PID e di $F[x]$.

In questa sezione applicheremo quanto visto nelle precedenti al caso di Domini a Ideali Principali. Cominciamo però con un'importante caratterizzazione degli ideali massimali, che vale in qualunque anello commutativo, e che ricorda il Teorema 9.2.

Teorema 9.9. *Sia R un anello commutativo, ed I un ideale proprio di R. Allora I è un ideale massimale se e solo se l'anello quoziente R/I è un campo.*

Dimostrazione. ($\Rightarrow$) Sia I un ideale massimale e consideriamo l'anello quoziente R/I (è non degenere, perchè $I \neq R$). Per il Teorema di corrispondenza, gli ideali di R/I sono tutti e soli del tipo J/I con J ideale di R contenente I; per la massimalità di I, un tale J coincide con R o con I. Quindi, gli ideali di R/I sono : R/I e $I/I = \{0_{R/I}\}$. Per il Teorema 5.12, si ha che R/I è un campo.
($\Leftarrow$) Sia R/I un campo. Allora, ancora per il Teorema 5.12, gli ideali di R/I sono R/I e $\{0_{R/I}\}$. Per il Teorema di corrispondenza, essi sono in corrispondenza biunivoca con tutti gli ideali di R che contengono I. Dunque tali ideali sono R (che corrisponde a R/I) e I stesso (che corrisponde a $\{0_{R/I}\} = I/I$). Quindi I è un ideale massimale. ∎

Mediante questo Teorema, e la Proposizione 7.8, si ottiene una nuova dimostrazione che $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo. In modo simile il Teorema è utilizzato nell'esempio seguente. Più avanti, lo utilizzeremo in senso inverso.

Esempio. Consideriamo l'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ definito in precedenza. Fissato $a \in \mathbb{R}$, proviamo che l'insieme

$$I_a = \{\ f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\ \}$$

è un ideale massimale di $\mathbb{R}^{\mathbb{R}}$. Si consideri la applicazione $\Phi : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$ definita da $\Phi(f) = f(a)$. Provate che Φ è un omomorfismo suriettivo di anelli e che I_a è il suo nucleo; dal teorema di omomorfismo segue allora che $\mathbb{R}^{\mathbb{R}}/I_a$ è isomorfo a $\mathbb{R}$ che è un campo. Per il Teorema 9.9, I_a è un ideale massimale.

Veniamo ora a descrivere i quozienti dei domini a ideali principali. Come vedremo si tratta di mettere assieme diversi risultati provati finora.

Teorema 9.10. *Sia A un PID, e sia $0_A \neq a \in A$. Le seguenti condizioni sono equivalenti:*

(1) *(a) è primo;*

(2) *a è irriducibile;*

(3) *(a) è massimale;*

(4) *$A/(a)$ è un campo;*

Dimostrazione. (1) $\Rightarrow$ (2). Segue dal lemma 7.3.

(2) $\Rightarrow$ (3). Segue dalla Proposizione 7.10.

(3) $\Rightarrow$ (4). Segue dal Teorema 9.9

(4) $\Rightarrow$ (1). Se $A/(a)$ è un campo, allora $A/(a)$ è un dominio d'integità, dunque (a) è primo per il Teorema 9.2, e quindi a è un elemento primo per la Proposizione 7.7. ∎

Osservazione. Sia A un PID, sia a un suo elemento irriducibile, e sia $I = (a)$. Allora, A/I è un campo. In particolare, ogni elemento $b+I \neq I = 0_{A/I}$ di A/I ha un inverso. Vediamo come questo fatto possa essere dimostrato anche senza l'ausilio del Teorema di Corrispondenza. Ora $b + I \neq I$ se e solo se $b \notin I$, ovvero se e solo se a non divide b, e dato che a è irriducibile, ciò equivale a dire che $MCD(a, b) = 1$. Poiché A è un PID, per l'osservazione alla fine della sezione 8.3, se $b \notin I$, esistono allora $\alpha, \beta \in A$ tali che $a\alpha + b\beta = 1$. Ma allora, nel quoziente A/I, $(\beta + I)(b + I) = 1 + I = 1_{A/I}$, quindi $b + I$ è invertibile.
Un caso importante è quando A è un dominio euclideo (ad esempio un anello di polinomi a coefficienti su un campo), poiché in tal caso i coefficienti α e β di sopra (e dunque in particolare $\beta + I = (b + I)^{-1}$) possono essere trovati mediante l'algoritmo di Euclide.

Quozienti di $F[x]$. Applicando il Teorema 9.10 agli anelli di polinomi a coefficienti su un campo (che è un dominio a ideali principali), si ha il seguente e fondamentale risultato.

Teorema 9.11. *Sia F un campo, e sia $0 \neq f \in F[x]$. Allora sono equivalenti*

(1) f è irriducibile;

(2) (f) è un ideale massimale di $F[x]$;

(3) $F[x]/(f)$ è un campo.

Questo Teorema verrà usato appieno nella prossima sezione. Concludiamo questa con un risultato di notevole importanza pratica, in quanto descrive in modo conveniente gli elementi di un quoziente di un anello di polinomi (si osservi che qui non si richiede che il generatore dell'ideale sia irriducibile)

Proposizione 9.12. *Sia F un campo, sia $I = (f)$ un ideale non nullo e proprio di $F[x]$ e sia $n = \deg f$. Allora ogni elemento di $F[x]/I$ si scrive in modo unico nella forma*

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + I$$

con $a_0, a_1, \ldots, a_{n-1} \in F$.

Dimostrazione. Poichè $I = (f)$ è proprio e non nullo, si ha $n = \deg f \geq 1$. Sia $g + I$ un generico elemento di $F[x]/I$. Dividendo g per f, otteniamo $g = fq + r$, con $q, r \in F[x]$ e $r = 0$ o $\deg r \leq n - 1$; quindi $r = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ per $a_0, a_1, \ldots, a_{n-1} \in F$. Ora $g - r = fq \in (f) = I$, quindi $g + I = r + I$, cioè

$$g + I = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + I \ .$$

Proviamo ora l'unicità. Siano $b_0, b_1, \ldots, b_{n-1} \in F$ tali che

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + I = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + I$$

allora

$$h = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} \in I = (f)$$

quindi $h = ft$ per qualche $t \in F[x]$. Poichè $\deg h \leq n - 1 < n = \deg f$, ciò forza $h = 0$ e quindi $a_i = b_i$ per ogni $i = 0, 1, \ldots, n - 1$. ∎

Esempio. Sia $f = x^2 + x + 1$. In $\mathbb{Q}[x]/(f)$ troviamo le eventuali radici del polinomio $t^3 - 8$. Per la proposizione 9.12, gli elementi di $\mathbb{Q}[x]/(f)$ si scrivono nella forma $u = ax + b + (f)$, con $a, b \in \mathbb{Q}$. Dunque se u è una radice di $t^3 - 8$ si ha

$$\begin{aligned} 8 + (f) = u^3 &= (ax + b)^3 + (f) = a^3x^3 + 3a^2bx^2 + 3ab^2x + b^3 + (f) \\ &= (3ab^2 - 3a^2b)x + (a^3 + b^3 - 3a^2b) + (f) \end{aligned}$$

(dove $(3ab^2 - 3a^2b)x + (a^3 + b^3 - 3a^2b)$ è il resto della divisone di $a^3x^3 + 3a^2bx^2 + 3ab^2x + b^3$ per f). Per l'unicità della scrittura in $\mathbb{Q}[x]/(f)$ dev'essere:

$$\begin{cases} 3ab^2 - 3a^2b = 0 \\ a^3 + b^3 - 3a^2b = 8 \end{cases}$$

Le soluzioni razionali di questo sistema sono $(a, b) = (2, 0), (0, 2), (-2, -2)$. Quindi se $u \in \mathbb{Q}[x]/(f)$, allora $u^3 = 8 + (f)$ se e solo se $u \in \{2x + (f), 2 + (f), -2x - 2 + (f)\}$.

Oltre che per lo studio delle estensioni, che vedremo nella prossima sezione, il Teorema 9.11 è uno strumento molto efficace per la costruzione di campi con particolari proprietà. Questo aspetto verrà approfondito nel corso di Algebra II; per il momento vediamo come si possano costruire campi finiti diversi dai quozienti $\mathbb{Z}/p\mathbb{Z}$.
Ad esempio, consideriamo il campo $\mathbb{Z}_2$, ed il polinomio $f = x^2 + x + \overline{1} \in \mathbb{Z}_2[x]$. Poichè $f(\overline{1}) = \overline{3} = \overline{1}$ e $f(\overline{0}) = \overline{1}$, f non ha radici in $\mathbb{Z}_2$ e dunque, essendo $\mathbb{Z}_2$ un campo, non ha fattori di grado 1. Quindi f è irriducibile in $\mathbb{Z}_2[x]$ e pertanto

$$E = \frac{\mathbb{Z}_2[x]}{(x^2 + x + \overline{1})}$$

è un campo. Inoltre sappiamo dalla Proposizione 9.12 che $E = \{a + bx + (f) \mid a, b \in \mathbb{Z}_2\}$. Per ciascuno degli elementi a, b sono possibili due scelte ($\overline{0}$ o $\overline{1}$), dunque E contiene esattamente 4 elementi. Abbiamo quindi costruito un campo di ordine 4, che fino a questo punto ci era sconosciuto.
Con un procedimento simile si può costruire per ogni primo p e ogni $n \geq 1$ un campo di ordine p^n. Anzi, ogni campo finito è isomorfo ad un campo costruito in questo modo. Questo risultato, insieme con la teoria di base dei campi finiti, verrà studiato nel corso di Algebra II.

Esercizio 9.9. Si provi che in un PID ogni quoziente modulo un ideale *non nullo* è un campo oppure possiede divisore dello zero.

Esercizio 9.10. Sia $f = x^4 - 6x^2 + 4$. Si provi che $\mathbb{Q}[x]/(f)$ è un campo.

Esercizio 9.11. Si dica se il seguente anello è un campo

$$R = \frac{\mathbb{Z}_5[x]}{(x^3 + \overline{2}x + \overline{1})}$$

e si dica quanti elementi contiene.

Esercizio 9.12. 1) Sia dica se il seguente anello R è un campo e, in caso di risposta negativa, si determinino i suoi ideali massimali

$$R = \frac{\mathbb{Q}[x]}{(x^3 - 3x + 2)} \ .$$

2) Si dica se esistono elementi $0 \neq a \in R$ tali che $a^2 = 0$.

Esercizio 9.13. Si costruisca un campo con 9 elementi.

Esercizio 9.14. Sia J un ideale diverso dall'ideale nullo dell'anello degli interi di Gauss $\mathbb{Z}[i]$. Si provi che l'anello quoziente $\mathbb{Z}[i]/J$ è finito.

9.4. Estensioni semplici

Sia R un sottoanello dell'anello *commutativo* S (il modello principale a cui fare riferimento è $\mathbb{Q} \subseteq \mathbb{C}$). Fissato un elemento $b \in S$ ci proponiamo di studiare il più piccolo sottoanello di S che contiene $R \cup \{b\}$; tale (sotto)anello, che certamente esiste, lo denoteremo con $R[b]$, e diremo che $R[b]$ è ottenuto da R mediande *l'aggiunzione* dell'elemento b. Un'estensione di R ottenibile mediante l'aggiunzione di un singolo elemento si dice *estensione semplice* di R. Osserviamo che dalla definizione segue immediatamente che $R[b] = R$ se e solo se $b \in R$.

Esempi. Abbiamo già incontrato esempi di questo tipo. Come abbiamo visto, l'insieme

$$\{\ a + b\sqrt{2} \mid a, b \in \mathbb{Q}\ \}$$

è un sottoanello dei numeri reali. Esso contiene $\mathbb{Q} \cup \{\sqrt{2}\}$, ed è chiaramente incluso in ogni sottoanello di $\mathbb{R}$ che contiene $\mathbb{Q} \cup \{\sqrt{2}\}$; si tratta quindi proprio del minimo sottoanello di $\mathbb{R}$ che contiene $\mathbb{Q} \cup \{\sqrt{2}\}$, cioè $\mathbb{Q}[\sqrt{2}]$ (come del resto lo avevamo denotato).

Similmente, l'anello $\mathbb{Z}[i]$ degli interi di Gauss è il minimo sottoanello di $\mathbb{C}$ che contiene $\mathbb{Z} \cup \{i\}$.

Un altro esempio è $\mathbb{C} = \{\ a + ib \mid a, b \in \mathbb{R}\ \} = \mathbb{R}[i]$.

Sia R sottoanello di S e $b \in S$. Chiaramente, ogni sottoanello di S che contiene b contiene anche tutte le potenze b^n con $n \in \mathbb{N}$. Dunque ogni sottoanello di S che contiene $R \cup \{b\}$ contiene ogni ab^n con $a \in R,\ n \in \mathbb{N}$ e quindi contiene anche ogni elemento del tipo

$$a_0 + a_1 b + a_2 b^2 + \ \ldots\ + a_n b^n \qquad (*)$$

con $a_0, a_1, \ldots, a_n \in R$ e $n \in \mathbb{N}$ (osserviamo che possiamo intendere $a_0 = a_0 b^0$).
Ora, l'insieme degli elementi di S del tipo $(*)$ costituisce un sottoanello di S. Innanzi tutto possiamo convenientemente scrivere in forma contratta tali elementi:

$$a_0 + a_1 b + a_2 b^2 + \ \ldots\ + a_n b^n = \sum_{i=0}^{n} a_i b^i\ .$$

Siano quindi $u = \sum_{i=0}^{n} a_i b^i,\ v = \sum_{i=0}^{m} c_i b^i$ con $a_i\ (i = 0, \ldots, n),\ c_j\ (j = 0, \ldots, m)$ elementi di R, $n, m \in \mathbb{N}$; se $n \geq m$ (cosa che possiamo senz'altro assumere), riscriviamo: $v = \sum_{i=0}^{n} c_i b^i$ ponendo $c_i = 0$ per ogni $m + 1 \leq i \leq n$. Allora:

$$u - v = \sum_{i=0}^{n} a_i b^i - \sum_{i=0}^{n} c_i b^i = (a_0 - c_0) + (a_1 - c_1)b + \cdots + (a_n - c_n)b^n = \sum_{i=0}^{n} (a_i - c_i) b^i$$

che è del tipo $(*)$. Inoltre, usando le proprietà distributiva e commutativa, si prova che

$$uv = \left(\sum_{i=0}^{n} a_i b^i \right) \left(\sum_{i=0}^{m} c_i b^i \right) = \sum_{i=0}^{n+m} d_i b^i$$

dove $d_0 = a_0 c_0,\ d_1 = a_0 c_1 + a_1 c_0,\ d_2 = a_0 c_2 + a_1 c_1 + a_2 c_0,\ \ldots$, e in generale, per $0 \leq i \leq n + m$:

$$d_i = a_0 c_i + a_1 c_{i-1} + \cdots + a_{i-1} c_1 + a_i c_0 = \sum_{r=0}^{i} a_r c_{i-r}$$

infine $1_S = 1_R$ è del tipo $(*)$.

Dunque l'insieme degli elementi di S del tipo $(*)$ è un sottoanello che, per quanto osservato all'inizio, deve essere contenuto in ogni sottoanello di S che contiene $R \cup \{b\}$. Abbiamo quindi provato

Teorema 9.13. *Sia R sottoanello di S e sia $b \in S$. Allora*

$$R[b] = \left\{ \sum_{i=0}^{n} a_i b^i \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in R \right\}\ .$$

Come risulta dagli esempi visti in precedenza, per ottenere gli elementi di $R[b]$ non è sempre necessario dover considerare tutte le potenze b^n. Ad esempio, poichè $(\sqrt{2})^2 = 2$, $(\sqrt{2})^3 = 2(\sqrt{2})$, etc., ogni potenza di $\sqrt{2}$ con esponente ≥ 2 può essere riscritta nella forma 2^i oppure $2^i\sqrt{2}$ e quindi $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. La ragione generale di questo fenomeno, che si verifica solo per particolari elementi $b \in S$, sarà chiara tra poco.

Esercizio 9.15. Provare che $\mathbb{Q}[\sqrt{2}] \cap \mathbb{Q}[\sqrt{3}] = \mathbb{Q}$.

Soluzione. Si vede facilmente che $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Sia $u = x + y\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$ (con $x, y \in \mathbb{Q}$) e supponiamo per assurdo $y \neq 0$. Poichè $x, y^{-1} \in \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}]$ si ha in particolare $\sqrt{2} = y^{-1}(u - x) \in \mathbb{Q}[\sqrt{3}]$. Quindi esistono $a, b \in \mathbb{Q}$ tali che $\sqrt{2} = a + b\sqrt{3}$, da cui, elevendo al quadrato si ottiene $2ab\sqrt{3} = 2 - (a^2 + 3b^2) \in \mathbb{Q}$. Poichè $\sqrt{3} \notin \mathbb{Q}$, deve essere $ab = 0$. Se $b = 0$ allora $\sqrt{2} = a \in \mathbb{Q}$ che è assurdo. Dunque $a = 0$ e quindi si ha $\sqrt{2} = b\sqrt{3}$. Sia $b = \frac{m}{n}$ con $m, n \in \mathbb{N}$; allora, elevando al quadrato, $2n^2 = 3m^2$ il che è impossibile perchè il primo 2 compare con esponente dispari nella fattorizzazione di $2n^2$ e con esponente pari in quella di $3m^2$. Quindi, se $u = x + y\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$, allora $y = 0$ cioè $u \in \mathbb{Q}$. Dunque $\mathbb{Q}[\sqrt{2}] \cap \mathbb{Q}[\sqrt{3}] = \mathbb{Q}$.

La notazione si estende naturalmente al caso di aggiunzione di 2 o più elementi. Se R è un sottoanello dell'anello commutativo S, e $b_1, b_2 \in S$, si denota con $R[b_1, b_2]$ il più piccolo sottoanello di S che contiene $R \cup \{b_1, b_2\}$. Chiaramente, $R[b_1, b_2] = R[b_1][b_2] = R[b_2][, b_1]$. Similmente, se $b_1, b_2, \ldots, b_n \in S$ allora $R[b_1, b_2, \ldots, b_n]$ è il più piccolo sottoanello di S che contiene $R \cup \{b_1, b_2, \ldots, b_n\}$, e $R[b_1, b_2, \ldots, b_n] = R[b_1, b_2, \ldots, b_{n-1}][b_n]$ etc.

Veniamo ora ad un punto importante. Sia R un sottoanello dell'anello commutativo S e sia $b \in S$. Sia $f = a_0 + a_1x + a_2x^2 + \ \ldots \ + a_nx^n$ un polinomio in $R[x]$. Poichè i coefficienti a_i sono in particolare elementi di S, ha senso considerare la "sostituzione di x con b in f":

$$f(b) = a_0 + a_1b + a_2b^2 + \ \ldots \ + a_nb^n$$

che è un elemento di S. Dalla discussione precedente, risulta immediatamente

$$R[b] = \{f(b) \mid f \in R[x]\},$$

che è l'immagine dell'omomorfismo di sostituzione

$$\begin{array}{rccc} \sigma_b : & R[x] & \to & S \\ & f & \mapsto & f(b) \end{array}$$

Ora, il nucleo di tale omomorfismo è $I_b = \ker(\sigma_b) = \{f \in R[x] \mid f(b) = 0\}$.
Dal Teorema di omomorfismo 9.4 discende allora che

$$R[b] \simeq \frac{R[x]}{I_b}.$$

Questo è un fatto molto importante, perché ci dice che *ogni estensione semplice di un anello R si può realizzare come un opportuno quoziente dell'anello dei polinomi $R[x]$* e merita di essere enunciato come un Teorema.

Teorema 9.14. *Sia R sottoanello dell'anello S e sia $b \in S$. Allora*

$$\{f \in R[x] \mid f(b) = 0\} = I_b$$

è un ideale di $R[x]$ e $R[b] \simeq R[x]/I_b$.

Prima di continuare in questa analisi, passando a vedere cosa succede quando R è un campo, diamo una importante definizione.

Elementi algebrici e trascendenti. Sia R un sottoanello dell'anello S e sia $b \in S$.

(1) b si dice **algebrico** su R se esiste un polinomio $f \neq 0$ in $R[x]$ tale che $f(b) = 0$.

(2) b si dice **trascendente** su R se per ogni polinomio $f \neq 0$ in $R[x]$ si ha $f(b) \neq 0$.

Esempio 1. Per ogni $n, m \in \mathbb{N}$ con $m \geq 1$, $\sqrt[m]{n}$ è un numero reale algebrico su $\mathbb{Q}$ (ed anche su $\mathbb{Z}$), essendo radice del polinomio $x^m - n \in \mathbb{Z}[x]$.

Esempio 2. Similmente, $i \in \mathbb{C}$ è algebrico su $\mathbb{Q}$ essendo radice del polinomio $x^2 + 1$.

Esempio 3. Proviamo che $u = \sqrt{2} - \sqrt{3}$ è algebrico su $\mathbb{Q}$. Occorre trovare un polinomio non nullo in $\mathbb{Q}[x]$ che ammette u come radice. Cominciamo con elevare u al quadrato

$$u^2 = 2 - 2\sqrt{2}\sqrt{3} + 3 = 5 - 2\sqrt{6}$$

da cui $2\sqrt{6} = 5 - u^2$ ed elevando ancora al quadrato

$$24 = u^4 - 10u^2 + 25$$

quindi u è radice del polinomio $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ e dunque è algebrico su $\mathbb{Q}$.

Osserviamo che se R è sottoanello in S e $b \in S$ è trascendente su R, allora l'ideale $I_b = \{f \in R[x] \mid f(b) = 0\}$ del Teorema 9.14 coincide con $\{0\}$; dunque, in questo caso, l'omomorfismo di sostituzione σ_b è iniettivo. Si ha quindi la

Teorema 9.15. *Sia R un sottoanello dell'anello S e sia $b \in S$ trascendente su R. Allora $R[b] \simeq R[x]$.*

Esistono numeri reali che sono trascendenti su $\mathbb{Q}$. Esempi sono i numeri π ed e (e quindi, per il Teorema 9.15, $\mathbb{Q}[\pi]$ è, ad esempio, isomorfo all'anello dei polinomi $\mathbb{Q}[x]$). La dimostrazione di questo fatto è stata ottenuta da F. Lindemann nel 1882, ed è piuttosto complicata. Tuttavia, non è difficile provare che l'insieme dei numeri reali che sono algebrici su $\mathbb{Q}$ è un insieme numerabile; poichè l'insieme dei reali non è numerabile, da ciò segue che devono esistere numeri reali trascendenti su $\mathbb{Q}$.

Estensioni semplici di campi. Supponiamo ora che F sia un campo contenuto come sottoanello di S, e che b sia un elemento di S algebrico su F. Allora, per definizione, esiste almeno un polinomio non nullo a coefficienti in F che ammette b come radice. Essendo F un campo, l'ideale

$$I_b = \{\ g \in F[x] \mid g(b) = 0\ \}$$

è principale e non è l'ideale nullo. Dunque, dalla dimostrazione del Teorema 8.5, sappiamo che un generatore f di I_b è un polinomio di grado *minimo* tra i polinomi non nulli di I_b; quindi

se b è un elemento algebrico sul campo F, allora l'ideale $I_b = \{g \in F[x] \mid g(b) = 0\}$ di $F[x]$ è un ideale principale, generato da un polinomio di grado minimo tra i polinomi non nulli a coefficienti in F che ammettono b come radice.

Supponiamo ora che f e f_1 siano due generatori del medesimo ideale $I \neq \{0\}$ di $F[x]$; dalla Proposizione 7.1 sappiamo che f ed f_1 sono associati in $F[x]$, e quindi che esiste un elemento $0_F \neq c \in F$ (si ricordi che gli elementi invertibili di $F[x]$ sono tutti e soli gli elementi non nulli di F) tale che $f_1 = cf$. Ora, se $f = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$ allora $a_n^{-1}f$ è il solo polinomio associato ad f che abbia coefficiente direttivo uguale a 1. (Ricordo che un polinomio con coefficiente direttivo uguale ad 1 si dice *monico*).
Assemblando le osservazioni fatte sopra, otteniamo che ogni ideale non nullo di $F[x]$ (F è sempre un campo) ha un solo generatore monico. In particolare se b è un

elemento algebrico sul campo F, allora l'ideale $I_b = \{g \in F[x] \mid g(b) = 0\}$ ha un unico generatore monico, che si chiama **il polinomio minimo** di b su F.

Poniamoci ora nella situazione che ci interessa di più, che è quella in cui F è sottocampo di un altro campo K (il caso principale è quello di $\mathbb{Q}$ come sottocampo di $\mathbb{C}$).
Sia $b \in K$ un elemento algebrico su F, e sia $f \in F[x]$ il suo polinomio minimo. Supponiamo che f si fattorizzi in $F[x]$ come il prodotto di due polinomi, cioè che $f = gh$ con $g, h \in F[x]$ (ed, essendo $f \neq 0$, è anche $g \neq 0 \neq h$). Allora, applicando l'omomorfismo di sostituzione:

$$0 = f(b) = g(b)h(b) \ ;$$

poichè K è un campo, si deve avere $g(b) = 0$ oppure $h(b) = 0$. Sia $g(b) = 0$, allora, poichè $g \neq 0$, deve essere $\deg g = \deg f$, quindi $\deg h = 0$, che significa $h \in F^*$; similmente, se $h(b) = 0$ si ha $\deg h = \deg f$ e $g \in F^*$. Abbiamo quindi concluso che il polinomio f è irriducibile; un fatto fondamentale che riportiamo nel seguente enunciato.

Proposizione 9.16. *Sia F un sottocampo del campo K, e sia $b \in K$ un elemento algebrico su F. Allora il polinomio minimo di b su F è irriducibile.*

Osserviamo che, viceversa, se $f \in F[x]$ è un polinomio monico irriducibile che ammette b come radice nel campo K, allora f è il polinomio minimo di b su F; infatti il polinomio minimo g di b divide f e quindi $\deg g = \deg f$ da cui $g = f$ (essendo entrambi monici).

Esempio. Consideriamo il numero reale $u = \sqrt{2} - \sqrt{3}$ dell'esmpio 3 a pagina precedente, e proviamo che $f = x^4 - 10x^2 + 1$ è proprio il polinomio minimo di u su $\mathbb{Q}$. Per quanto osservato sopra, è sufficiente provare che f non è il prodotto di due polinomi razionali di grado minore o uguale a 3. Cominciamo con l'osservare che f non ha divisori di grado 1. Infatti se g fosse un divisore di grado 1 di f, moltiplicando per un invertibile, possiamo assumere $g = x - a$ per qualche $a \in \mathbb{Q}$. Allora, per il Teorema di Ruffini, $f(a) = 0$. Ma ogni radice α di f soddisfa

$$\alpha^2 = 5 \pm \sqrt{24}$$

e quindi non è un numero razionale. Dunque f non ha divisori di grado 1.
Supponiamo per assurdo che f sia il prodotto di due polinomi razionali di grado 2. Allora

$$f = (x^2 + ax + b)(x^2 + cx + d)$$

con $a, b, c, d \in \mathbb{Q}$. Eseguendo il prodotto e confrontando i coefficienti con quelli di f si ottengono le condizioni

$$\begin{cases} a + c = 0 \\ d + ac + b = -10 \\ ad + bc = 0 \\ bd = 1 \end{cases}$$

da cui, con elementari passaggi algebrici, si ricava $a = 0$ oppure $b = b^{-1}$. Nel primo caso segue che $c = 0$ e b, d sono radici del polinomio $x^2 + 10x + 1$ che non sono razionali. Nel secondo caso, $b = \pm 1$ ed $a^2 = 10 \pm 2$ che ancora non è soddisfatta per valori razionali di a. Dunque il sistema non ha soluzioni razionali, e di conseguenza f non è il prodotto di due polinomi razionali di grado 2. In conclusione, f è il polinomio minimo di $\sqrt{2} - \sqrt{3}$ su $\mathbb{Q}$.

Unendo la Proposizione 9.16 con i Teoremi 9.11 e 9.14 si ottiene un'immediata ed importante conseguenza:

Teorema 9.17. *Sia F un sottocampo del campo K, sia $b \in K$ un elemento algebrico su F. Allora $F[b]$ è un campo.*

Dimostrazione. Sia f il polinomio minimo di b su F. Allora, per la Proposizione 9.16, f è un polinomio irriducibile, quindi, per il Teorema 9.11, (f) è un ideale massimale e dunque, per il Teorema 9.14

$$F[b] \simeq \frac{F[x]}{(f)}$$

è un campo. ■

Esempio. x^2+1 è il polinomio minimo su $\mathbb{R}$ dell'elemento $i \in \mathbb{C}$, ed inoltre $\mathbb{C} = \mathbb{R}[i]$. Quindi

$$\mathbb{C} \simeq \frac{\mathbb{R}[x]}{(x^2+1)}$$

che si può anche vedere come una costruzione del campo $\mathbb{C}$ a partire da $\mathbb{R}$; si potrebbe cioè *definire* il campo dei numeri complessi come l'anello $\mathbb{R}[x]/(x^2+1)$.

Infine, se $b \in K$ è un elemento algebrico su F e $f \in F[x]$ è il suo polinomio minimo, utilizzando la Proposizione 9.12, e mediante l'isomorfismo $F[x]/(f) \to F[b]$, otteniamo una descrizione conveniente degli elementi di $F[b]$.

Proposizione 9.18. *Sia F un campo, b un elemento algebrico su F appartenente ad campo K e $f \in F[x]$ il suo polinomio minimo. Allora ogni elemento di $F[b]$ si scrive in modo unico nella forma*

$$a_0 + a_1 b + \cdots + a_{n-1} b^{n-1}$$

dove $n = \deg f$ e $a_0, a_1, \ldots, a_{n-1} \in F$.

Esempio 1. Sia $\zeta = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$ una radice primitiva terza dell'unità. $\zeta^3 = 1$, quindi ζ è radice del polinomio razionale $x^3 - 1$. Si ha $x^3 - 1 = (x-1)(x^2+x+1)$ e poichè ζ non è radice di $x-1$ deve essere radice di $f = x^2 + x + 1$. Ora, f è irriducibile in $\mathbb{Q}[x]$ (dato che non ha radici in $\mathbb{Q}$, non ha divisori di grado 1 in $\mathbb{Q}[x]$), e dunque è il polinomio minimo di ζ su $\mathbb{Q}$. Quindi $\mathbb{Q}[\zeta] \simeq \mathbb{Q}[x]/(x^2+x+1)$ è un campo; inoltre per la Proposizione 9.18

$$\mathbb{Q}[\zeta] = \{\ a + b\zeta \mid a, b \in \mathbb{Q}\ \}\ .$$

Il polinomio minimo fornisce la relazione fondamentale per eseguire i calcoli in $\mathbb{Q}[\zeta]$: $\zeta^2 = -\zeta - 1$. Proviamo, ad esempio che $i \notin \mathbb{Q}[x]$. Supponiamo per assurdo che esistano $a, b \in \mathbb{Q}$ tali che $a + b\zeta = i$; allora

$$-1 = i^2 = a^2 + 2ab\zeta + b^2\zeta^2 = a^2 + 2ab\zeta - b^2\zeta - b^2 = (a^2 - b^2) + (2a - b)b\zeta$$

per l'unicità della scrittura degli elementi di $\mathbb{Q}[\zeta]$ nella forma $x + y\zeta$ si ha

$$\begin{cases} a^2 - b^2 = -1 \\ (2a - b)b = 0 \end{cases}$$

da cui $b = 0$ oppure $b = 2a$; nel primo caso si ha allora $a^2 = -1$ che è assurdo (a è razionale); nel secondo caso si ha $3a^2 = 1$ che anche non è possibile per $a \in \mathbb{Q}$. Quindi $i \notin \mathbb{Q}[\zeta]$.

Esempio 2. Sia $u = \sqrt{2} - \sqrt{3}$. Come abbiamo visto il u è algebrico su $\mathbb{Q}$; quindi $\mathbb{Q}[u]$ è un campo. In particolare $v = \sqrt{2} + \sqrt{3} = -u^{-1} \in \mathbb{Q}[u]$ e conseguentemente

$$\sqrt{2} = \frac{v+u}{2} \in \mathbb{Q}[u] \qquad \text{e} \qquad \sqrt{3} = \frac{v-u}{2} \in \mathbb{Q}[u]$$

Quindi $\mathbb{Q}[\sqrt{2},\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}-\sqrt{3}]$; d'altra parte è chiaro che $\mathbb{Q}[\sqrt{2}-\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3}]$ e dunque $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}-\sqrt{3}]$.
Si provi per esercizio che $\mathbb{Q}[\sqrt{2}-\sqrt{3}] = \{\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\ \}$.

Grado di una estensione. Concludiamo questo capitolo con una utile considerazione, che sarà ripresa ed approfondita in un corso successivo.

Sia F un sottocampo del campo K. Allora è possibile vedere K come spazio vettoriale su F: i vettori sono gli elementi di K, gli scalari quelli di F e il prodotto di un vettore per uno scalare è effettuato mediante la moltiplicazione dei due elementi nel campo K. In questa situazione, la dimensione di K come spazio vettoriale su F si chiama **grado** di K su F, e si denota con $[K:F]$.
Ad esempio, ogni numero complesso si scrive in modo unico nella forma $a+ib = a1+bi$ con $a,b \in \mathbb{R}$, cioè come combinazione lineare (a coefficienti nel campo degli scalari $\mathbb{R}$) di 1 e i (visti come vettori). Quindi $\{1,i\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$ e quindi $[\mathbb{C}:\mathbb{R}] = 2$.
Più in generale, se $b \in K$ è algebrico su F e il polinomio minimo di b su F ha grado n, la Proposizione 9.18 asserisce che l'insieme $\{1,\ b,\ b^2,\ \ldots\ ,\ b^{n-1}\}$ è una base di $F[b]$ come spazio vettoriale su F, la cui dimensione è quindi n. Con le notazioni introdotte sopra, abbiamo provato

Proposizione 9.19. *Sia F sottocampo del campo K, sia $b \in K$ un elemento algebrico su F, e sia $f \in F[x]$ il suo polinomio minimo. Allora $[F[b]:F] = \deg f$.*

Il concetto di grado svolgerà un ruolo essenziale nello studio delle estensioni di campi nel corso di Algebra II.

Esercizio 9.16. Descrivere gli elementi di $\mathbb{Q}[\sqrt{2},\sqrt{3}]$.

Esercizio 9.17. Si provi che l'elemento $u = 1-\sqrt[3]{2}$ è algebrico su $\mathbb{Q}$. Si determini il suo polinomio minimo e, in $\mathbb{Q}[u]$, si calcoli u^{-1}.

Esercizio 9.18. Siano $F \subseteq E$ campi e $b \in E$ un elemento algebrico su F. Provare che, per ogni $a \in F$, $b+a$ è algebrico su F.

Esercizio 9.19. Provare che $\mathbb{Z}[\frac{1}{3}] \simeq \mathbb{Z}[x]/(3x-1)$.

Esercizio 9.20. Sia $S = \mathbb{R}\times\mathbb{R}$ l'anello prodotto diretto. Sia $\overline{\mathbb{R}} = \{\ (a,a) \mid a \in \mathbb{R}\ \}$. Si provi che $\overline{\mathbb{R}}$ è un sottoanello di S e che $\overline{\mathbb{R}} \simeq \mathbb{R}$. Si consideri quindi l'elemento $b = (0,1) \in S$, si provi che è algebrico su $\overline{\mathbb{R}}$ e che il suo polinomio minimo è x^2-x, che **non** è irriducibile in $\mathbb{R}[x]$. Quindi la Proposizione 9.16 non vale se l'elemento algebrico b non viene preso in un campo. Si provi infine che $\overline{\mathbb{R}}[(0,1)] = S$, concludendo che $\mathbb{R}\times\mathbb{R} \simeq \mathbb{R}[x]/(x^2-x)$.

Esercizio 9.21. Si determini il grado $[\mathbb{Q}[\sqrt[4]{2}]:\mathbb{Q}]$.

9.5. Esercizi.

Esercizio 9.22. Sia $\phi:\ \mathbb{Z}[x] \to \mathbb{Q}$ un omomorfismo d'anelli.

(a) Si provi che $\mathrm{Im}(\phi) \neq \mathbb{Q}$.

(b) Si provi che se $\phi(x) = \frac{r}{s}$ con $r,s \in \mathbb{Z}$ e $(r,s) = 1$, allora $\ker(\phi) = (sx-r)$.

(c) Quanti sono gli omomorfismi distinti da $\mathbb{Z}[x]$ in $\mathbb{Q}$?

(d) Quanti sono gli omomorfismi distinti da $\mathbb{Q}$ in $\mathbb{Z}[x]$?

[suggerimento per il punto (b): osservare innanzi tutto che $\phi(z) = z$ per ogni $z \in \mathbb{Z}$. Quindi, posto $f = rx - s$, l'inclusione $(f) \subseteq \ker(\phi)$ è facile; per il viceversa, osservare che è sufficiente provare che ogni polinomio primitivo $g \in \ker(\phi)$ appartiene a (f); quindi dividere g per f in $\mathbb{Q}[x]$, come deve essere il resto ?...quindi applicare le considerazioni che riguardano le fattorizzazioni dei polinomi primitivi...]

Esercizio 9.23. Sia

$$A = \{\ a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N},\ a_0 \in \mathbb{Z},\ a_i \in 12\mathbb{Z} \text{ per } i = 1, \ldots, n\}\ .$$

(a) Si provi che A è un sottoanello dell'anello dei polinomi $\mathbb{Z}[x]$.

(b) Si provi che $J = \{\ f \in A \mid f(0) = 0\ \}$ è un ideale di A, e si dica se è un ideale massimale.

(c) Determinare gli ideali dell'anello A/J.

(d) Dire se A/J è un dominio d'integrità.

Esercizio 9.24. Sia $f = x^2 - 3 \in \mathbb{Q}[x]$. Si determinino gli elementi invertibili dell'anello $\mathbb{Q}[x]/(f)$.

Esercizio 9.25. Al variare di $a \in (\mathbb{Z}/5\mathbb{Z})$ sia $f_a = x^3 + 2ax - 1 \in (\mathbb{Z}/5\mathbb{Z})[x]$. Si dica per quali valori di a l'anello $(\mathbb{Z}/5\mathbb{Z})[x]/(f_a)$ è un campo.

Esercizio 9.26. Siano $f = x^4 + x^3 - 5x^2 + x - 6$ e $g = x^5 + x^4 - 7x^3 - 3x^2 + 4x + 12$, e sia $I = (f, g)$ l'ideale generato da f e g in $\mathbb{Q}[x]$.

(a) Si provi che I non è un ideale massimale di $\mathbb{Q}[x]$.

(b) Si determinino i divisori dello zero dell'anello quoziente $\mathbb{Q}[x]/I$.

Esercizio 9.27. Sia $f = x^4 + 4x^2 - 10 \in \mathbb{Q}[x]$, e sia $\overline{f} \in (\mathbb{Z}/5\mathbb{Z})[x]$ la riduzione modulo 5 di f.

(a) Si dica se $\mathbb{Q}[x]/(f)$ è un campo.

(b) Si dica se $\overline{f}$ è irriducibile in $(\mathbb{Z}/5\mathbb{Z})[x]$.

Esercizio 9.28. (a) Si trovi un generatore dell'ideale

$$I = (x^3 - x^2 - 3x + 2\ ,\ x^4 + x^3 - 3x^2 - 2x + 2)$$

nell'anello $\mathbb{Q}[x]$. Si dica se $\mathbb{Q}[x]/I$ è un campo.

(b) Stesse domande in $\mathbb{R}[x]$.

Esercizio 9.29. Sia

$$F = (\mathbb{Z}/3\mathbb{Z})[x]/(x^3 - x + \overline{1}).$$

(a) Si provi che F è un campo, e si dica quanti elementi ha F.

(b) Posto $\alpha = x + (x^3 - x + \overline{1})$, si scriva l'elemento $(\alpha^3 - 1)^{-1}$ come combinazione a coefficienti in $\mathbb{Z}/3\mathbb{Z}$ di $1\ , \alpha\ , \alpha^2$.

Esercizio 9.30. Dire, motivando le risposte, se le seguenti affermazioni sono vere.

(a) $\mathbb{Q}[i] = \mathbb{Q}[i + 2]$.

(b) $\mathbb{Q}[i] = \mathbb{Q}[2i]$.

(c) $\mathbb{Q}[i] = \mathbb{Q}[i + \sqrt{2}]$.

Esercizio 9.31. Dimostrare o confutare che $\mathbb{Q}[\sqrt{2},\sqrt{7}] = \mathbb{Q}[\sqrt{2}+\sqrt{7}]$.

Esercizio 9.32. Per ogni $h \in \mathbb{Z}$ sia

$$E_h = \frac{\mathbb{Q}[x]}{(x^3 + hx^2 - hx + 2)}$$

(a) Si dica per quali $h \in \mathbb{Z}$, E_h è un campo.

(b) Posto $h = 2$ si dica se esiste un elemento $u \in E_h$ tale che $u^2 = -3$.

(c) Posto $h = 1$ si determini un ideale I di $\mathbb{Q}[x]$ tale che $(x^3 + hx^2 - hx + 2) \subseteq I$ e $\mathbb{Q}[x]/I$ contiene un elemento w tale che $w^2 = -3 + I$.

Esercizio 9.33. Sia $f = x^4 + 5x^2 + 6 \in \mathbb{Q}[x]$.

(a) Si dica, motivando la risposta, se l'anello $E = \mathbb{Q}[x]/(f)$ è un campo.

(b) Si dica se $x + (f)$ è un elemento invertibile di E.

(c) Si determinino tutti gli ideali di $\mathbb{Q}[x]$ che contengono l'ideale (f).

Esercizio 9.34. Determinare in $\mathbb{Q}[x]$ il polinomio minimo di $\sqrt[3]{2} - 2$ e quello di $\sqrt[3]{4} - \sqrt[3]{2}$.

Esercizio 9.35. Sia $\mathbb{R} = \mathbb{Q}[\sqrt{2},\sqrt{3}]$.

(a) Si dica se R è un campo, e in R si determini $(\sqrt{2}-3)^{-1}$.

(b) Si dica quali fra i seguenti numeri reali appartengono a R: $\sqrt{2}$, $\sqrt{5}$, $\sqrt{6}$.

(c) Si dica se esiste un automorfismo ϕ di R tale che $\phi(\sqrt{2}) = \sqrt{3}$.

Esercizio 9.36. Sia $u = \sqrt[3]{5} - 2$.

(a) Si calcoli il polinomio minimo di u su $\mathbb{Q}$.

(b) Si provi che $\mathbb{Q}[u] = \mathbb{Q}[u^2]$.

(c) Si dica se il polinomio $x^3 - 5$ ha soluzioni diverse da 1 in $\mathbb{Q}[u]$.

Esercizio 9.37. Sia $1 \neq a \in \mathbb{C}$ un elemento algebrico su $\mathbb{Q}$, e sia $h \in \mathbb{Q}[x]$ il suo polinomio minimo su $\mathbb{Q}$.

(a) Si provi che esiste $g \in \mathbb{Q}[x]$ tale che $g(a) = \frac{1}{a-1}$.

(b) Sia $I = \{f - g \mid f, g \in \mathbb{Q}[x] \text{ e } f(a) = ag(a)\}$; si provi che I è un ideale di $\mathbb{Q}[x]$ che contiene (h).

Esercizio 9.38. Determinare $\mathbb{Q}[\sqrt[3]{2}] \cap \mathbb{Q}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt[3]{2}] \cap \mathbb{Q}$.

Esercizio 9.39. Sia b una radice complessa del polinomio $x^3 - 3x + 4$.

(a) Si calcoli il grado del polinomio minimo di b su $\mathbb{Q}$;

(b) In $\mathbb{Q}[b]$ si scriva b^{-1} come combinazione di $1, b, b^2$ a coefficienti razionali.

(c) Si dica se $i \in \mathbb{Q}[b]$.

Esercizio 9.40. Si calcoli il polinomio minimo di $\sqrt{2} + \sqrt{3}$ sul campo $\mathbb{Q}(\sqrt{6})$.

Esercizio 9.41. Sia $f = x^5 - 2x^3 - 2x^2 + 4 \in \mathbb{Q}[x]$.

(1) Si dica se $\mathbb{Q}[x]/(f)$ è un campo.

(2) Si dica se il campo $E = \mathbb{Q}(\sqrt[6]{2})$ contiene tutte le radici complesse di f.

Esercizio 9.42. Sia $f = x^4 + 4x^3 - 2 \in \mathbb{Q}[x]$.

(a) Si provi che f è irriducibile in $\mathbb{Q}[x]$, ma che le riduzioni di f rispettivamente modulo 2, 3 e 5 sono riducibili in $(\mathbb{Z}/2\mathbb{Z})[x]$, $(\mathbb{Z}/3\mathbb{Z})[x]$ e $(\mathbb{Z}/5\mathbb{Z})[x]$.

(b) Sia $\alpha \in \mathbb{C}$ una radice di f, e si consideri il suo quadrato α^2. Si provi che il polinomio minimo di α^2 su $\mathbb{Q}$ ha grado 4.

Esercizio 9.43. Sia $f = a_o + a_1x + ... + a_nx^n \in \mathbb{Q}[x]$, con $a_o \neq 0 \neq a_n$. Si definisca quindi il polinomio $Rew(f) = a_n + a_{n-1}x + ... + a_ox^n$, e si provi che $Rew(f)$ è irriducibile in $\mathbb{Q}[x]$ se e solo se f è irriducibile in $\mathbb{Q}[x]$.

Esercizio 9.44. Sia f un polinomio monico irriducibile in $\mathbb{Q}[x]$ e sia $\beta \in \mathbb{C}$ una sua radice. Si provi che per ogni $0 \neq a \in \mathbb{Q}$, $\beta + a$ non è una radice di f. [sugg.: Poichè f è monico e irriducibile, f è il polinomio minimo di β su $\mathbb{Q}$. Supponete, per assurdo, che per un certo $0 \neq a \in \mathbb{Q}$, $\beta + a$ sia una radice di f, allora β è una radice del polinomio $g = f(x + a) \in \mathbb{Q}[x]$; per l'unicità del polinomio minimo, $g = f$. Ma allora $f(\beta + 2a) = f(\beta + a + a) = g(\beta + a) = f(\beta + a) = 0$ ...]

Esercizio 9.45. Si provi che ogni numero complesso è algebrico su $\mathbb{R}$.

Esercizio 9.46. Si dimostri che l'anello $E = \mathbb{Q}[x]/(x^4 + 15x^3 + 7)$ è un campo. Si dica quindi se il polinomio $x^2 - 2$ è irriducibile in $E[x]$.

Esercizio 9.47. Al variare di $h \in \mathbb{Q}$, sia $f_h = x^3 + hx + 1 \in \mathbb{Q}[x]$, e sia E_h il campo ottenuto aggiungendo a $\mathbb{Q}$ tutte le radici complesse di f_h.

(a) Per quali valori razionali di h si ha $[E_h : \mathbb{Q}] = 2$?

(b) Per quali valori razionali di h esistono due radici complesse distinte c_1 e c_2 di f_h tali che $c_1c_2 \in \mathbb{Q}$?

Esercizio 9.48. Si costruisca un campo di ordine 25.

Esercizio 9.49. A partire da $\mathbb{Z}/3\mathbb{Z}$ si costruisca un campo E di ordine 27. Si dica quali sono nel campo E le radici del polinomio $x^5 - 1$.