

252-0025-01L

Prof. Dr. Ueli MAURER

Diskrete Mathematik

Niccolò Cavallini (21-924-147)

ETH Zürich – HS 2021

Diskrete Mathematik

Niccolò Cavallini (21-924-147)
ncavallini@student.ethz.ch

Indice

2 Ragionamento matematico, dimostrazioni e introduzione alla logica	7
2.1 Affermazioni matematiche	7
2.3 Introduzione alla logica proposizionale	7
2.4 Introduzione alla logica predicativa	9
2.5 Formule logiche vs. affermazioni matematiche	11
2.6 Alcune tecniche di dimostrazione	11
2.6.1 Composizione di implicazioni	11
2.6.2 Dimostrazione diretta di un'implicazione	11
2.6.3 Dimostrazione indiretta di un'implicazione	11
2.6.4 <i>Modus Ponens</i>	12
2.6.5 Distinzione dei casi	12
2.6.6 Dimostrazione per assurdo	13
2.6.7 Dimostrazione d'esistenza	13
2.6.8 Dimostrazioni d'esistenza per mezzo del <i>Principio dei cassetti</i>	13
2.6.9 Dimostrazioni con controesempio	13
2.6.10 Dimostrazione per induzione completa	14
3 Insiemi, relazioni e funzioni	15
3.1 Insiemi e operazioni sugli insiemi	15
3.1.1 Il concetto di insieme	15
3.1.2 Descrizione di insiemi	15

3.1.3	Uguaglianza tra insiemi	15
3.1.4	Insiemi come elementi (di altri insiemi)	15
3.1.5	Sottoinsiemi	16
3.1.6	L'insieme vuoto	16
3.1.7	Costruzione di insiemi a partire da \emptyset	16
3.1.8	Una costruzione dei numeri naturali	17
3.1.9	L'insieme potenza	17
3.1.10	Unione e intersezione di insiemi	17
3.1.11	Il prodotto cartesiano	18
3.2	Relazioni	19
3.2.1	Il concetto di relazione	19
3.2.2	La rappresentazione di una relazione	19
3.2.3	Operazioni insiemistiche sulle relazioni	20
3.2.4	La relazione inversa	20
3.2.5	Composizione di relazioni	20
3.2.6	Speciali proprietà delle relazioni	21
3.2.7	La chiusura transitiva	22
3.3	Relazioni d'equivalenza	22
3.3.1	Partizioni formate dalle relazioni di equivalenza	22
3.4	Relazioni d'ordine parziale	23
3.4.1	Definizione	23
3.4.2	Diagrammi di Hasse	24
3.4.3	Combinazione dei posets e dell'ordine lessicografico	25
3.4.4	Elementi speciali nei posets	25
3.4.5	<i>Meet, join</i> e reticolli	26
3.5	Funzioni	26
3.6	Insiemi numerabili e non numerabili	28

3.6.1	Numerabilità	28
3.6.2	Tra finito e infinito numerabile	28
3.6.3	Importanti insiemi numerabili	29
3.6.4	Non-numerabilità di $\{0, 1\}^\infty$	30
3.6.5	Esistenza di funzioni incalcolabili	30
4	Teoria dei Numeri	32
4.2	Divisori e divisione	32
4.2.1	Divisori	32
4.2.2	Divisione con resto	32
4.2.3	Massimi comuni divisori	33
4.2.4	Minimo comune multiplo	34
4.3	Scomposizione in fattori primi	35
4.3.1	Numeri primi e Teorema Fondamentale dell’Aritmetica	35
4.3.3	Espressione di gcd e lcm	35
4.5	Congruenze e aritmetica modulare	35
4.5.1	Congruenze modulari	35
4.5.2	Aritmetica modulare	36
4.5.3	Inversi moltiplicativi	37
4.5.4	Il Teorema Cinese del Resto (CRT)	37
4.6	Applicazione: Lo scambio di chiavi Diffie-Hellman	38
5	Algebra	39
5.1	Introduzione	39
5.1.2	Strutture algebriche	39
5.2	Monoidi e gruppi	39
5.2.1	Elementi neutri	39
5.2.2	Associatività e monoidi	40

5.2.3	Elementi inversi e gruppi	40
5.2.4	(Non)-minimalità degli assiomi dei gruppi	42
5.3	La struttura dei gruppi	42
5.3.1	Il prodotto diretto di gruppi	42
5.3.2	Omomorfismo di gruppi	43
5.3.3	Sottogruppi	43
5.3.4	L'ordine di un gruppo e dei suoi elementi	43
5.3.5	Gruppi ciclici	44
5.3.7	L'ordine dei sottogruppi	44
5.3.8	Il gruppo \mathbb{Z}_m^* e la funzione φ di Eulero	45
5.4	Applicazione: Crittosistema RSA	46
5.4.1	Radici e -esime in un gruppo	46
5.4.2	Descrizione dell'RSA	47
5.5	Anelli e campi	48
5.5.1	Definizione di anello	48
5.5.2	Divisori	49
5.5.3	Unità e gruppo moltiplicativo di un anello	49
5.5.4	Divisori di zero e dominio d'integrità	49
5.5.5	Anelli di polinomi	50
5.5.6	Campi	51
5.6	Polinomi su un campo	51
5.6.1	Fattorizzazione e polinomi irriducibili	51
5.6.2	Divisibilità in $F[x]$	52
5.7	Polinomi come funzioni	52
5.7.2	Radici	52
5.7.3	Interpolazione polinomiale	53
5.8	Campi finiti	54

5.8.1	L'anello $F[x]_{m(x)}$	54
5.8.2	Costruzione dei campi estesi	54
6	Logica	55
6.2	Sistemi di dimostrazione	55
6.2.1	Definizione	55
6.2.2	Esempi	55
6.3	Concetti generali di Logica	59
6.3.1	Obiettivo della Logica	59
6.3.2	Sintassi, semantica, interpretazione e modello	59
6.3.4	Soddisfabilità, tautologia, conseguenza, equivalenza	60
6.3.5	Gli operatori logici \wedge , \vee e \neg	60
6.3.6	Conseguenza logica vs. insoddisfabilità	61
6.4	Calcoli logici	61
6.4.2	Sistema di Hilbert (<i>Hilbert-Style Calculi</i>)	61
6.4.3	Derivazioni dalle assunzioni	62
6.5	Logica proposizionale	62
6.5.1	Sintassi	62
6.5.2	Semantica	63
6.5.4	Forme normali	63
6.5.6	Il calcolo risolutivo	64
6.6	Logica predicativa	66
6.6.1	Sintassi	66
6.6.2	Variabili libere e sostituzione	67
6.6.3	Semantica	67
6.6.4	Logica predicativa con uguaglianza	68
6.6.5	Alcune equivalenze riguardanti i quantificatori	68

6.6.7	Instanziamento universale	69
6.6.8	Forme normali	69
6.6.9	Un teorema e le sue interpretazioni	69

2 Ragionamento matematico, dimostrazioni e introduzione alla logica

2.1 Affermazioni matematiche

Definizione 2.1 (Proposizione). Un'affermazione matematica che è o vera o falsa (ma non entrambi) è detta **proposizione**.

Esempio 1. Si considerino le seguenti affermazioni:

- 13 è un numero primo → proposizione vera
- Dato p primo, anche $2^p - 1$ è primo → proposizione falsa (si scelga ad es. $p = 11$)
- “Domani pioverà” → non è una proposizione



2.3 Introduzione alla logica proposizionale

Definizione 2.4 (Valori di verità). Esistono due valori di verità (o *costanti logiche*): 0 e 1, ossia **FALSO** e **VERO**.

Definizione 2.5 (E, O, e NON logico). Si definiscono i seguenti tre operatori tra proposizioni:

- (i) Il **NON** logico denotato con $\neg A$
- (ii) L'**E** logico (congiunzione), denotato con $A \wedge B$
- (iii) L'**O** logico (disgiunzione), denotato con $A \vee B$.

Vale la seguente **tavola di verità**

A	B	$\neg A$	$A \wedge B$	$A \vee B$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

Definizione 2.6 (Formula). Varie proposizioni possono essere combinate, per mezzo degli operatori logici, in **formule**. Ad es:

$$F = (A \wedge B) \vee C$$

Definizione 2.7 (Equivalenza tra formule). Due formule F, G si dicono **equivalenti**, e si scrive $F \equiv G$ se, per ogni assegnazione dei valori di verità in F e G si ottiene lo stesso risultato.

Osservazione 1. Definiamo l'operatore logico **implicazione** come segue:

$$A \rightarrow B \equiv \neg A \vee B$$

In lingua italiana, tale relazione è traducibile come: A implica B , ossia: “quando A è vero, allora anche B è vero”. Vale la seguente tabella di verità:

A	B	$A \rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Osservazione 2. Allo stesso modo è definibile la **doppia implicazione**, i.e.

$$A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$$

Vale la seguente tabella di verità:

A	B	$A \leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Lemma 2.1 (Regole di calcolo). *Dette A, B, C formule logiche, valgono le seguenti regole di calcolo:*

- (1) **Idempotenza:** $A \wedge A \equiv A$; $A \vee A \equiv A$.
- (2) **Commutatività di \wedge e \vee :** $A \wedge B \equiv B \wedge A$; $A \vee B \equiv B \vee A$
- (3) **Associatività:** $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$; $(A \vee B) \vee C \equiv A \vee (B \vee C)$
- (4) **Assorbimento:** $A \wedge (A \vee B) \equiv A$; $A \vee (A \wedge B) \equiv A$
- (5) **Distributività I:** $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- (6) **Distributività II:** $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
- (7) **Doppia negazione:** $\neg(\neg A) \equiv A$
- (8) **Leggi di De Morgan:** $\neg(A \wedge B) \equiv \neg A \vee \neg B$; $\neg(A \vee B) \equiv \neg A \wedge \neg B$

Definizione 2.8 (Conseguenza logica). Una formula G è una **conseguenza logica** di una formula F , ossia

$$F \models G$$

quando si verifica la seguente condizione:

Se F è valutata 1, allora G è valutata 1

Grazie al Lemma 2.1, è possibile dimostrare equivalenze e conseguenze logiche anche senza dover scrivere le varie tabelle di verità. Si veda per esempio l'esercizio bonus 2.3.

Definizione 2.9 (Tautologia). Una formula F è detta **tautologia** se è valutata 1 per ogni assegnazione dei simboli proposizionali contenuti in F . Si scrive $\models F$ o anche $F \equiv \top$.

Esempio 2. La formula $F = A \vee \neg A$ è una tautologia. Lo dimostra la seguente tabella di verità:

A	$\neg A$	F
0	1	1
1	0	1



Definizione 2.10 (Formula soddisfacibile). Una formula F è detta **soddisfacibile** se è vera per almeno un'assegnazione dei valori di verità nei simboli proposizionali contenuti in F . In caso contrario, F è detta **insoddisfacibile**. Una formula insoddisfacibile è spesso denotata con \perp .

Esempio 3. La formula $F = A \wedge \neg A$ è insoddisfacibile, cioè $F \equiv \perp$.



Lemma 2.2. Una formula F è una tautologia se e solo se $\neg F$ è insoddisfacibile.

Lemma 2.3. Dette F, G due formule, $H = F \rightarrow G$ è tautologia se e solo se $F \models G$.

2.4 Introduzione alla logica predicativa

Definizione 2.11 (Predicato k -ario). Un **predicato k -ario** P su un insieme U , detto universo, è una funzione

$$P : U^k \rightarrow \{0, 1\}$$

Un predicato P assegna a ogni lista di k elementi $(a_1, \dots, a_k) \in U$ il valore $P(a_1, \dots, a_k)$ che è vero (1) oppure falso (0).

Esempio 4. Sia $U = \mathbb{N}$ e P il predicato unario

$$\text{prime}(x) = \begin{cases} 1 & \text{se } x \text{ è primo} \\ 0 & \text{altrimenti} \end{cases}$$

Allo stesso modo, in un universo con una relazione d'ordine \leq (ad es. $U = \mathbb{N}$ o $U = \mathbb{R}$), è definibile il predicato binario

$$\text{less}(x, y) = \begin{cases} 1 & \text{se } x < y \\ 0 & \text{altrimenti} \end{cases}$$



Definizione 2.12 (Quantificatori). Sia $P(x)$ un predicato su un universo U . Allora le seguenti affermazioni logiche sono definite:

- $\forall x P(x)$ $P(x)$ è vero **per ogni** $x \in U$
- $\exists x P(x)$ $P(x)$ è vero **per un qualche** $x \in U$, i.e., **esiste** un $x \in U$ che verifica $P(x)$.

I quantificatori possono essere **annidati**, come mostra il seguente

Esempio 5. L'Ultimo Teorema di Fermat afferma che, dato $n \geq 3$, non esistono $x, y, z \in \mathbb{N} \setminus \{0\}$ tali che:

$$x^n + y^n = z^n$$

Questo Teorema può essere riscritto, in logica predicativa, come:

$$\neg (\exists x \exists y \exists z \exists n (n \geq 3 \wedge x^n + y^n = z^n))$$

considerando l'universo $U = \mathbb{N} \setminus \{0\}$.



Si elencano di seguito alcune regole utili della logica predicativa. Dati $P(x), Q(x)$ predicati si ha:

$$(i) \quad \forall x P(x) \wedge \forall x Q(x) \equiv \forall x(P(x) \wedge Q(x))$$

$$(ii) \quad \exists x(P(x) \wedge Q(x)) \models \exists x(P(x) \wedge Q(x))$$

$$(iii) \quad \exists x P(x) \wedge \exists x Q(x) \not\models \exists x(P(x) \wedge Q(x))$$

$$(iv) \quad \neg \forall x P(x) \equiv \exists x \neg P(x)$$

$$(v) \quad \neg \exists x P(x) \equiv \forall x \neg P(x)$$

$$(vi) \quad \exists y \forall x P(x, y) \models \forall x \exists y P(x, y) \quad \text{MA:}$$

$$(vii) \quad \forall x \exists y, P(x, y) \not\models \exists y \forall x P(x, y)$$

2.5 Formule logiche vs. affermazioni matematiche

Una formula logica generalmente *non* è un'affermazione matematica, perché, a seconda dell'interpretazione data, può essere vera o falsa. Per considerare una formula un'affermazione matematica, è necessario dapprima fissare un'interpretazione.

Lemma 2.4. *Dette F, G due formule, se vale*

$$F \models G$$

allora vale anche:

$$F \text{ è tautologia} \Rightarrow G \text{ è tautologia}$$

Dimostrazione. $F \models G$ significa che per ogni interpretazione delle formule, se F è vera, allora anche G è vera. Pertanto, se F è vera **per ogni** interpretazione, allora anche G è vera **per ogni** interpretazione, che è il significato di tautologia. ■

2.6 Alcune tecniche di dimostrazione

2.6.1 Composizione di implicazioni

Definizione 2.13 (Composizione di implicazioni). Se $S \Rightarrow T$ e $T \Rightarrow U$ sono entrambe vere, allora si può concludere che anche $S \Rightarrow U$ è vera.

La correttezza di tale metodo è data dal

Lemma 2.5. $(A \rightarrow B) \wedge (B \rightarrow C) \models A \rightarrow C$.

Dimostrazione. Tramite le tabelle di verità. ■

2.6.2 Dimostrazione diretta di un'implicazione

Definizione 2.14 (Dimostrazione diretta di un'implicazione). Una dimostrazione diretta di un'implicazione $S \Rightarrow T$ si basa sul seguente principio: si assume S vera e si dimostra la veridicità di T sotto tale assunto.

2.6.3 Dimostrazione indiretta di un'implicazione

Definizione 2.15 (Dimostrazione indiretta di un'implicazione). Una dimostrazione indiretta di un'implicazione $S \Rightarrow T$ procede assumendo T falsa e dimostrando che S è falsa sotto questo assunto.

La correttezza di tale metodo è data dal

Lemma 2.6. $\neg B \rightarrow \neg A \models A \rightarrow B$

Dimostrazione. Tramite le tabelle di verità. ■

2.6.4 Modus Ponens

Definizione 2.16 (Modus Ponens). La dimostrazione di un'affermazione S per mezzo del *Modus Ponens* procede come segue:

1. Trovare un'affermazione matematica adatta R
2. Dimostrare R
3. Dimostrare $R \Rightarrow S$

Lemma 2.7. $A \wedge (A \rightarrow B) \models B$

2.6.5 Distinzione dei casi

Definizione 2.17 (Distinzione dei casi). La dimostrazione di un'affermazione S per distinzione dei casi procede come segue:

1. Trovare una lista finita di affermazioni matematiche R_1, \dots, R_k (*i casi*)
2. Dimostrare la veridicità di un certo R_i
3. Dimostrare $R_i \Rightarrow S$ per ogni $i = 1, \dots, k$

Lemma 2.8. Per ogni k abbiamo

$$(A_1 \vee \dots \vee A_k) \wedge (A_1 \rightarrow B) \wedge \dots \wedge (A_k \rightarrow B) \models B$$

Dimostrazione. Per k fisso (e.g. $k = 2$) è possibile dimostrare il Lemma precedente osservando le tabelle di verità. Per generalizzare, serve una dimostrazione per induzione su k (vedi sezione 2.6.10). ■

Osservazione 3. Per $k = 1$, il metodo della distinzione dei casi corrisponde al *Modus Ponens*.

2.6.6 Dimostrazione per assurdo

Definizione 2.18 (Dimostrazione per assurdo). Una **dimostrazione per assurdo** di un'affermazione S procede nel seguente modo:

1. Trovare un'affermazione matematica adatta T
2. Mostrare che T è falsa
3. Assumere che S sia falsa e provare che T è vera sotto tale assunto, generando così un paradosso.

La correttezza di tale metodo è data dal

Lemma 2.9. $(\neg A \rightarrow B) \wedge \neg B \models A$

2.6.7 Dimostrazione d'esistenza

Definizione 2.19 (Dimostrazioni d'esistenza). Si consideri un insieme X di parametri e un'affermazione S_x per ogni $x \in X$. Una **dimostrazione d'esistenza** è una dimostrazione della veridicità di S_x per almeno una x . Una tale dimostrazione si dice **costruttiva** se indica un a per cui S_a è vera, altrimenti si dice **non costruttiva**.

2.6.8 Dimostrazioni d'esistenza per mezzo del *Principio dei cassetti*

Il seguente fatto è conosciuto come **Principio dei cassetti / Pigeonhole Principle / Schuhbladenprinzip**

Teorema 2.10 (*Principio dei cassetti*). *Se un insieme di n oggetti viene suddiviso in $k < n$ insiemi, allora, almeno uno di questi insiemi conterrà $\lceil \frac{n}{k} \rceil$ oggetti.*

Dimostrazione. La dimostrazione avviene per contraddizione. Si supponga che tutti gli insiemi nelle partizioni abbiano al massimo $\lceil \frac{n}{k} \rceil - 1$ oggetti. Allora, il numero totale di oggetti è al massimo $k(\lceil \frac{n}{k} \rceil - 1)$, che è minore di n siccome

$$k \left(\lceil \frac{n}{k} \rceil - 1 \right) < k \left(\left(\frac{n}{k} + 1 \right) - 1 \right) = k \cdot \frac{n}{k} = n$$

■

2.6.9 Dimostrazioni con controesempio

Le dimostrazioni con controesempio sono un particolare tipo di dimostrazioni d'esistenza costruttive.

Definizione 2.20 (Dimostrazione con controesempio). Sia X un insieme di parametri ed esista un'affermazione S_x per ogni $x \in X$. Una **dimostrazione con controesempio** è una dimostrazione della **falsità** di S_x per ogni $x \in X$ per mezzo della presentazione di un a (il controesempio) per cui S_a è falsa.

2.6.10 Dimostrazione per induzione completa

Una dimostrazione per induzione completa si svolge in due passaggi fondamentali. Formulata l'ipotesi di induzione $P(n)$, si vuol dimostrare che essa valga per ogni n . Si procede nel modo indicato nella

Definizione 2.21 (Dimostrazione per induzione).

1. **Caso base.** Si dimostra $P(0)$, cioè la validità di P per il primo elemento per cui essa si assume valga
2. **Passo d'induzione.** Si dimostra l'implicazione $P(n) \Rightarrow P(n + 1)$ per un n arbitrario.

La correttezza del metodo è data dal

Teorema 2.11. *Per l'universo \mathbb{N} e un qualsiasi predicato unario P si ha:*

$$P(0) \wedge \forall n (P(n) \rightarrow P(n + 1)) \Rightarrow \forall n P(n)$$

3 Insiemi, relazioni e funzioni

3.1 Insiemi e operazioni sugli insiemi

3.1.1 Il concetto di insieme

Sia A un insieme ed x un oggetto qualsiasi. Assumiamo definito il fatto che x sia **elemento** di A (si scrive $x \in A$) o meno (si scrive $x \notin A$).

Definizione 3.1 (Cardinalità). Il numero di elementi di un insieme finito A è detto **cardinalità** di A e si denota con $|A|$. La cardinalità di insiemi infiniti verrà discussa in seguito.

3.1.2 Descrizione di insiemi

Un insieme A è completamente descritto quando è data esplicitamente la lista dei suoi elementi (es. $A = \{1, 2, 3\}$) o quando è definita una proprietà P che gli elementi di A devono soddisfare per essere tali, i.e., $\{x \in A \mid P(x)\}$.

3.1.3 Uguaglianza tra insiemi

Definizione 3.2 (Uguaglianza tra insiemi). Due insiemi A, B si dicono **uguali** se hanno esattamente gli stessi elementi.

$$A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$$

Per gli insiemi costituiti da un solo elemento, possiamo concludere che, se essi sono uguali, allora i due elementi sono uguali.

Lemma 3.1. Per ogni a, b vale

$$\{a\} = \{b\} \Rightarrow a = b$$

Osservazione 4. Si noti che $\{a, b\} = \{c, d\}$ non implica $a = c$ né $b = d$.

3.1.4 Insiemi come elementi (di altri insiemi)

Gli insiemi possono essere elementi di altri insiemi, come nel caso

$$A = \{5, \{4, \{3\}\}, \{7\}\}$$

In tal caso è $|A| = 3$.

L'ordine degli elementi non è importante negli insiemi, i.e. $\{1, 2, 3\} = \{2, 1, 3\}$. Diverso è il discorso per le liste ordinate di elementi, di cui esempio più comune è la **coppia ordinata** (e anche l'unico che trattiamo). In tal caso è:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

per cui

$$(a, b) \neq (b, a)$$

3.1.5 Sottoinsiemi

Un’importante relazione tra insiemi è quella di **inclusione**.

Definizione 3.3 (Sottoinsieme). L’insieme A è **sottoinsieme** di un insieme B , scritto $A \subseteq B$ se ogni elemento di A è anche elemento di B , i.e.:

$$A \subseteq B \leftrightarrow \forall x(x \in A \rightarrow x \in B)$$

Dalle Definizioni 3.2 e 3.3 segue chiaramente che

$$A = B \leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

Abbiamo inoltre che la relazione \subseteq è transitiva, i.e.:

$$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$$

3.1.6 L’insieme vuoto

Definizione 3.4 (Insieme vuoto). Un insieme è detto **vuoto** se non contiene nessun elemento. Viene spesso denotato con \emptyset o $\{\}$. Vale ovviamente $|\emptyset| = 0$.

Lemma 3.2. *Esiste un solo insieme vuoto.*

Dimostrazione. Siano \emptyset, \emptyset' insiemi vuoti differenti. Siccome sono entrambi vuoti, ogni elemento di \emptyset (nessuno) è anche elemento di \emptyset' e viceversa. Dalla Def. 3.2, concludiamo che $\emptyset = \emptyset'$, il che significa che l’insieme vuoto è unico. ■

Lemma 3.3. *L’insieme vuoto è sottoinsieme di ogni insieme, i.e., $\forall A(\emptyset \subseteq A)$.*

Dimostrazione. Assumiamo esista un insieme A per cui valga $\emptyset \not\subseteq A$. Ciò significa che esiste $x \in \emptyset$ con $x \notin A$. Ma un tale x non può esistere, siccome \emptyset contiene, per definizione, 0 elementi. ■

3.1.7 Costruzione di insiemi a partire da \emptyset

È possibile creare degli insiemi a partire dall’insieme vuoto come segue:

$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots$$

tenendo presente che $|\emptyset| = 0$ e $|\{\emptyset\}| = 1$.

3.1.8 Una costruzione dei numeri naturali

Cerchiamo di costruire i numeri naturali a partire da concetti di base di teoria degli insiemi. In **grassetto** scriviamo i nuovi oggetti creati. Scriviamo la seguente successione:

$$\mathbf{0} = \emptyset, \quad \mathbf{1} = \{\emptyset\}, \quad \mathbf{2} = \{\emptyset, \{\emptyset\}\}, \quad \mathbf{3} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots\}$$

dove il successore $s(\mathbf{n})$ di un insieme **n** è definito come

$$s(\mathbf{n}) := \mathbf{n} \cup \{\mathbf{n}\}$$

Notiamo immediatamente che

$$|s(\mathbf{n})| = |\mathbf{n}| + 1$$

Un'operazione $+$ può essere definita ricorsivamente come segue:

$$\mathbf{m} + \mathbf{0} := \mathbf{m}, \quad \mathbf{m} + s(\mathbf{n}) = s(\mathbf{m} + \mathbf{n})$$

Definendo anche una moltiplicazione \cdot e dimostrando commutatività, associatività e distributività, si ottiene una costruzione di \mathbb{N} .

3.1.9 L'insieme potenza

Definizione 3.5 (Insieme potenza). Dato un insieme A , il suo **insieme potenza** $\mathcal{P}(A)$ è l'insieme dei sottoinsiemi di A :

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

Si noti che se $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$, inoltre $A \in \mathcal{P}(A)$.

3.1.10 Unione e intersezione di insiemi

Definizione 3.6 (Unione e intersezione).

- L'**unione** di due insiemi A, B , denotata con $A \cup B$ è l'insieme

$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

- L'**intersezione** di due insiemi A, B , denotata con $A \cap B$ è l'insieme

$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

Tali definizioni possono essere estesi a più di due insiemi. Sia \mathcal{A} un insieme di insiemi finito o infinito. Allora vale:

- $\bigcup \mathcal{A} := \{x \mid x \in A \text{ per qualche } A \in \mathcal{A}\}$
- $\bigcap \mathcal{A} := \{x \mid x \in A \text{ per ogni } A \in \mathcal{A}\}$

Definizione 3.7 (Complemento). Sia dato un universo U . Allora il complemento \overline{A} di un insieme A è l'insieme

$$\overline{A} := \{x \in U \mid x \notin A\}$$

Se comprendiamo l'intersezione insiemistica in modo analogo all'E logico e l'unione in modo analogo all'O logico, allora è naturale interpretare il complemento come il NON logico.

Definizione 3.8 (Differenza di insiemi). La differenza tra due insiemi B e A , denotata con $B \setminus A$ è l'insieme degli elementi contenuti in B senza quelli contenuti in A , i.e.:

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

Teorema 3.4. Detti A, B, C tre insiemi, valgono le seguenti leggi:

<i>Idempotenza</i>	$A \cap A = A$
	$A \cup A = A$
<i>Commutatività</i>	$A \cap B = B \cap A$
	$A \cup B = B \cup A$
<i>Associatività</i>	$A \cap (B \cap C) = (A \cap B) \cap C$
	$A \cup (B \cup C) = (A \cup B) \cup C$
<i>Assorbenza</i>	$A \cap (A \cup B) = A$
	$A \cup (A \cap B) = A$
<i>Distributività</i>	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
<i>Consistenza</i>	$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

Dimostrazione. La dimostrazione segue direttamente da quella analoga per gli operatori logici \wedge e \vee . ■

3.1.11 Il prodotto cartesiano

Definizione 3.9 (Prodotto cartesiano). Il **prodotto cartesiano** $A \times B$ di due insiemi A, B è l'insieme di tutte le coppie ordinate con primo elemento un elemento di A e secondo elemento uno di B , i.e.:

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

Osservazione 5. Per insiemi finiti vale: $|A \times B| = |A| \cdot |B|$.

Il prodotto cartesiano può essere esteso a k insiemi A_1, \dots, A_k considerando un insieme di k -tuple, il cui i -esimo elemento è un elemento di A_i :

$$\bigtimes_{i=1}^k A_i = \{(a_1, \dots, a_k) \mid a_i \in A_i \text{ per } 1 \leq i \leq k\}$$

3.2 Relazioni

3.2.1 Il concetto di relazione

Definizione 3.10 (Relazione). Una **relazione** (binaria) ρ da un insieme A ad un insieme B è un sottoinsieme di $A \times B$. Se $A = B$, allora ρ è detta *relazione su A*.

Se $a \in A$ è in relazione ρ con $b \in B$, si scrive $(a, b) \in \rho$, o, più semplicemente $a \rho b$. In caso contrario, $(a, b) \notin \rho$ o $a \not\rho b$.

Definizione 3.11 (Relazione identità). La **relazione identità** su A , identificata con id_A è la relazione

$$\text{id}_A = \{(a, a) \mid a \in A\}$$

3.2.2 La rappresentazione di una relazione

Esempio 6. Siano $A = \{a, b, c, d\}$ e $B = \{q, r, s, t, u\}$. Si consideri la relazione

$$\rho = \{(a, r), (a, s), (a, u), (b, q), (b, s), (c, r), (c, t), (c, u), (d, s), (d, u)\}$$

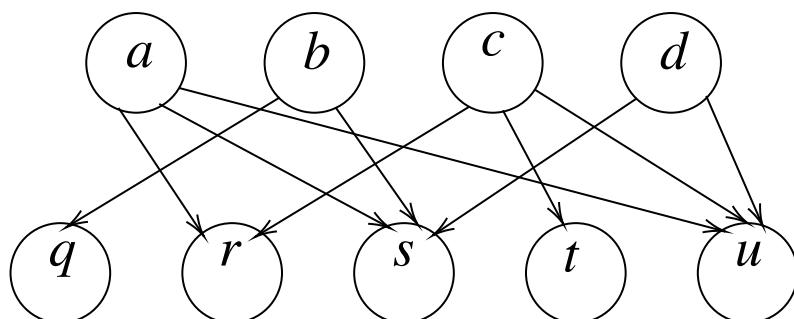
La relazione in questione può essere rappresentata:

- per elencazione (vedi sopra)
- con una matrice binaria di ordine $|A| \times |B|$ che ha per elementi $(m_{ij}) = 1$ se $i \rho j$, 0 altrimenti.
- con un digrafo (*directed graph*) munito di $|A| + |B|$ vertici etichettati con gli elementi di A e di B . Se $a \rho b$, allora esiste un arco orientato da a a b .

La rappresentazione matriciale di ρ è:

$$M^\rho = \begin{array}{c|ccccc} & q & r & s & t & u \\ \hline a & 0 & 1 & 1 & 0 & 1 \\ b & 1 & 0 & 1 & 0 & 0 \\ c & 0 & 1 & 0 & 1 & 1 \\ d & 0 & 0 & 1 & 0 & 1 \end{array}$$

Il seguente digrafo rappresenta ρ



3.2.3 Operazioni insiemistiche sulle relazioni

Le relazioni sono insiemi, quindi si possono applicare le operazioni insiemistiche (\cup , \cap , \neg). Nella rappresentazione matriciale, queste corrispondono alle operazioni logiche \vee , \wedge , \neg posizione-a-posizione.

Esempio 7. In \mathbb{Z} , la relazione $\leq \cup \geq$ è una relazione completa (cioè uguale a $\mathbb{Z} \times \mathbb{Z}$), $\leq \cap \geq$ è id e $\leq \neg \geq$ è $>$.

♦

3.2.4 La relazione inversa

Definizione 3.12 (Relazione inversa). Data una relazione ρ da A a B , la sua **inversa** $\widehat{\rho} : B \rightarrow A$ è così definita:

$$\widehat{\rho} = \{(a, b) \mid (b, a) \in \rho\}$$

Osservazione 6. Vale: $\widehat{\text{id}} = \text{id}$

3.2.5 Composizione di relazioni

Definizione 3.13 (Composizione di relazioni). Siano date le relazioni $\rho : A \rightarrow B$ e $\sigma : B \rightarrow C$. Allora, la **composizione** $\rho \circ \sigma$ (o più semplicemente $\rho\sigma$) è la relazione da A a C :

$$\rho \circ \sigma = \{(a, c) \mid \exists b ((a, b) \in \rho \wedge (b, c) \in \sigma)\}$$

Lemma 3.5. La composizione di relazioni è **associativa**, i.e., $\rho \circ (\sigma \circ \phi) = (\rho \circ \sigma) \circ \phi$.

Dimostrazione.

$$\begin{aligned} (a, d) \in \rho(\sigma\phi) &\implies \exists b((a, b) \in \rho \wedge (b, d) \in \sigma\phi) \\ &\implies \exists b((a, b) \in \rho \wedge \exists c((b, c) \in \sigma \wedge (c, d) \in \phi)) \\ &\implies \exists b \exists c((a, b) \in \rho \wedge ((b, c) \in \sigma \wedge (c, d) \in \phi)) \\ &\implies \exists b \exists c(((a, b) \in \rho \wedge (b, c) \in \sigma) \wedge (c, d) \in \phi) \\ &\implies \exists c \exists b(((a, b) \in \rho \wedge (b, c) \in \sigma) \wedge (c, d) \in \phi) \\ &\implies \exists c(\exists b((a, b) \in \rho \wedge (b, c) \in \sigma) \wedge (c, d) \in \phi) \\ &\implies ((a, c) \in \rho\sigma \wedge (c, d) \in \phi) \\ &\implies (a, d) \in (\rho\sigma)\phi \end{aligned}$$

■

Lemma 3.6. Sia $\rho : A \rightarrow B$ e $\sigma : B \rightarrow C$. Allora l'inversa $\widehat{\rho}\widehat{\sigma}$ di $\rho\sigma$ è la relazione $\widehat{\sigma}\widehat{\rho}$.

3.2.6 Speciali proprietà delle relazioni

Definizione 3.14 (Riflessività). Una relazione ρ su A è detta **riflessiva** se vale

$$a \rho a \quad \forall a \in A$$

ossia se

$$\text{id} \subseteq \rho$$

Definizione 3.15 (Irreflessività). Una relazione ρ su A è detta **irreflessiva** se $a \not\rho a$ per ogni $a \in A$, i.e., $\rho \cap \text{id} = \emptyset$.

Osservazione 7. Si noti che *irreflessiva* non è la negazione di *riflessiva*, i.e., una relazione non riflessiva non è necessariamente irreflessiva.

Definizione 3.16 (Simmetria). Una relazione ρ su A è detta **simmetria** se vale

$$a \rho b \Leftrightarrow b \rho a \quad \forall a, b \in A$$

ossia

$$\rho = \widehat{\rho}$$

Definizione 3.17 (Antisimmetria). Una relazione ρ su A è detta **antisimmetrica** se vale

$$a \rho b \wedge b \rho a \Rightarrow a = b \quad \forall a, b \in A$$

ossia

$$\rho \cap \widehat{\rho} \subset \text{id}$$

Osservazione 8. Si noti che *antisimmetrica* non è la negazione di *simmetrica*.

Definizione 3.18 (Transitività). Una relazione ρ su A è detta **transitiva** se vale

$$a \rho b \wedge b \rho c \Rightarrow a \rho c \quad \forall a, b, c \in A$$

Lemma 3.7. Una relazione ρ è transitiva se e solo se $\rho^2 \subseteq \rho$ (dove $\rho^2 = \rho \circ \rho$)

Dimostrazione.

Dim. \Leftarrow : Questa parte segue dalla definizione di composizione: se $a \rho b$ e $b \rho c$, allora $a \rho^2 c$. Allora vale anche $a \rho c$ siccome $\rho^2 \subseteq \rho$.

Dim. \Rightarrow : Si assuma ρ transitiva. Per mostrare $\rho^2 \subseteq \rho$, assumiamo $a \rho^2 b$ per qualche a, b . Dobbiamo allora mostrare che $a \rho b$. La definizione di $a \rho^2 b$ ci indica che esiste un c per cui $a \rho c$ e $c \rho b$. Ma siccome ρ è transitiva, questo c esiste sicuramente. ■

Osservazione 9. Per ρ transitiva vale $\rho^n \subseteq \rho \quad \forall n > 1$.

3.2.7 La chiusura transitiva

Definizione 3.19 (Chiusura transitiva). La **chiusura transitiva** di una relazione ρ su A , denotata con ρ^* , è:

$$\rho^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \rho^n$$

3.3 Relazioni d'equivalenza

Definizione 3.20 (Relazione d'equivalenza). Una **relazione di equivalenza** è una relazione su un insieme A che è contemporaneamente:

- riflessiva
- simmetrica
- transitiva

Definizione 3.21 (Classe d'equivalenza). Per una relazione d'equivalenza θ su A e per $a \in A$, l'insieme degli elementi di A che sono equivalenti ad a è detto **classe di equivalenza** di a e si indica con $[a]_\theta$.

Esempio 8. Si consideri la relazione d'equivalenza \equiv_n su \mathbb{Z} (congruenza modulo $n \in \mathbb{N}$). Allora, l'insieme delle classi d'equivalenza di \equiv_n , denotato con \mathbb{Z}_n è:

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

Per esempio, se $n = 5$, allora $12 \equiv_5 2$, cioè $12 \in [2]$.

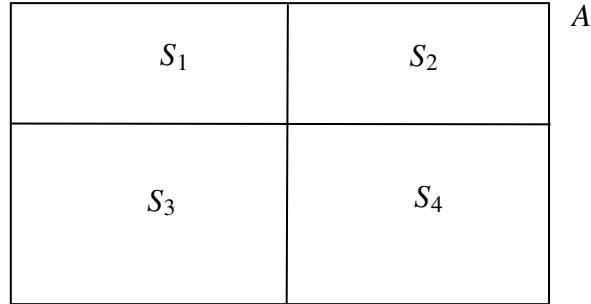
Lemma 3.8. *L'intersezione di due relazioni d'equivalenza è a sua volta una relazione di equivalenza.*

3.3.1 Partizioni formate dalle relazioni di equivalenza

Definizione 3.22 (Partizione). Una **partizione** di un insieme A è un insieme di sottoinsiemi di A tra loro disgiunti che coprono A , i.e., un insieme $S = \{S_i \mid i \in \mathcal{I}\}$ (dove \mathcal{I}) è un insieme degli indici per cui valga:

$$S_i \cap S_j = \emptyset \quad (i \neq j) \quad \text{e} \quad \bigcup_{i \in \mathcal{I}} S_i = A$$

Esempio 9. Nella figura sottostante, gli insiemi S_1, \dots, S_4 formano una partizione di A .



Definizione 3.23 (Insieme quoziante). L'insieme delle classi di equivalenza di una relazione θ su A è detto **insieme quoziante** di A (o A modulo θ o $A \bmod \theta$) ed è denotato con

$$A/\theta = \{[a]_\theta \mid a \in A\}$$

Osservazione 10. La notazione \mathbb{Z}_n è solo una particolare scelta per abbreviare \mathbb{Z}/\equiv_n

Teorema 3.9. L'insieme A/θ è una partizione di A .

Dimostrazione. Dal momento che $a \in [a]$ per ogni a (riflessività di θ), allora $\bigcup [a] = A$. Rimane da dimostrare che le classi d'equivalenza siano disgiunte. Ciò equivale a dimostrare che, per a, b fissi:

$$a \theta b \Rightarrow [a] = [b] \quad (*)$$

e

$$a \not\theta b \Rightarrow [a] \cap [b] = \emptyset \quad (**)$$

Per mostrare (*) consideriamo $c \in [a]$ arbitrario e osserviamo che

$$c \in [a] \Leftrightarrow c \theta a \Rightarrow c \theta b \Leftrightarrow c \in [b]$$

siccome θ è transitiva. Così abbiamo provato $[a] \subseteq [b]$. Per provare che $[a] = [b]$ dovremmo ora mostrare che $[b] \subseteq [a]$ ma tralasciamo la dimostrazione (si ragiona per simmetria).

Per provare (**) ragioniamo per assurdo. Supponiamo quindi sia falsa. Ciò significa che esiste $c \in [a] \cap [b]$, ossia $c \theta a$ e $c \theta b$. Dalla simmetria, sappiamo che $a \theta c$ e quindi arriviamo alla contraddizione $a \theta b$. ■

3.4 Relazioni d'ordine parziale

3.4.1 Definizione

Definizione 3.24 (Relazione d'ordine parziale). Una **relazione d'ordine parziale** (o semplicemente *relazione d'ordine*) su un insieme A è una relazione che è contemporaneamente:

- riflessiva
- antisimmetrica
- transitiva

Un insieme A munito di una relazione d'ordine parziale \leq è detto *insieme parzialmente ordinato* (o, dall'inglese, *poset*) ed è denotato con $(A; \leq)$.

Esempio 10. Le relazioni \leq e \geq sono relazioni d'ordine parziale su $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, ma $<$ e $>$ non lo sono.



A partire dalla relazione d'ordine \leq possiamo definire la relazione $<$ nel modo seguente:

$$a < b \Leftrightarrow a \leq b \wedge a \neq b$$

Definizione 3.25 (Elementi comparabili). Due elementi a, b di un poset $(A; \leq)$ sono **comparabili** se $a \leq b$ o $b \leq a$. Altrimenti, sono detti **incomparabili**.

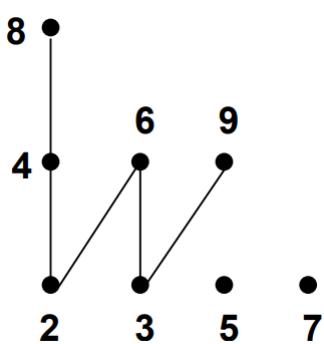
Definizione 3.26 (Relazione d'ordine totale). Se ogni coppia di elementi di un poset $(A; \leq)$ è comparabile, allora \leq è una **relazione d'ordine totale** su A (e A è detto *totalmente ordinato* da \leq).

3.4.2 Diagrammi di Hasse

Definizione 3.27 (Elemento coprente). In un poset $(A; \leq)$, $a \in A$ **copre** $b \in A$ se $a < b$ e se non esiste c con $a < c < b$.

Definizione 3.28 (Diagramma di Hasse di un poset (finito)). Il **diagramma di Hasse** di un poset (finito) è un digrafo i cui vertici sono etichettati secondo gli elementi di A e il cui arco tra a e b significa che b copre a .

Esempio 11. Il poset $(\{2, 3, 4, 5, 6, 7, 8, 9\}; |)$ produce il diagramma di Hasse mostrato in figura.



3.4.3 Combinazione dei posets e dell'ordine lessicografico

Definizione 3.29 (Prodotto diretto). Dati due poset $(A; \leq), (B; \sqsubseteq)$ il loro **prodotto diretto** denotato con $(A; \leq) \times (B; \sqsubseteq)$ è l'insieme $A \times B$ (prodotto cartesiano) munuito della relazione \leq su $A \times B$ così definita:

$$(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow a_1 \prec a_2 \wedge b_1 \sqsubseteq b_2$$

Teorema 3.10. $(A; \leq) \times (B; \sqsubseteq)$ è una relazione d'ordine parziale.

Teorema 3.11. Dati due poset $(A; \leq), (B; \sqsubseteq)$, la relazione \leq_{lex} definita su $A \times B$ è:

$$(a_1, b_1) \leq_{\text{lex}} (a_2, b_2) \Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$$

\leq_{lex} è una relazione d'ordine parziale.

La relazione \leq_{lex} è detta **ordine lessicografico** (di coppie). Di solito si usa tra due posets identici. È interessante, perché se i due posets sono totalmente ordinati, allora lo è anche \leq_{lex} su $A \times B$. Tale concetto è generalizzabile per tutte le k -tuple e per ogni sequenza finita di simboli da un alfabeto Σ (cioè gli elementi di Σ^*). Ad esempio: l'elenco del telefono è ordinato secondo \leq_{lex} su tutte le voci).

3.4.4 Elementi speciali nei posets

Definizione 3.30 (Elementi speciali nei posets). Dato un poset $(A; \leq)$ e un sottoinsieme $S \subseteq A$. Allora:

1. $a \in A$ è detto **minimale (massimale)** se non esiste $b \in A$ con $b < a$ ($b > a$)
2. $a \in A$ è detto **il minimo¹** (**il massimo²**) di A se $a \leq b$ ($a \geq b$) per ogni $b \in A$.
3. $a \in A$ è il **limite inferiore³** (**limite superiore⁴**) di S se $a \leq b$ ($a \geq b$) per ogni $b \in S$
4. $a \in A$ è il **massimo limite inferiore⁵** (**minimo limite superiore⁶**) di S se a è il massimo (minimo) dell'insieme di tutti i limiti inferiori (superiori) di S .

(1.) e (2.) sono facilmente individuabili in un diagramma di Hasse. Il massimo limite inferiore e il minimo limite superiore di S sono a volte denotati con $\text{glb}(S)$ e $\text{lub}(S)$

Esempio 12. Si consideri il poset $(\{1, 2, 3, 4, 6, 8, 12, 24\}; |)$. Si ottiene il seguente diagramma di Hasse:

¹least

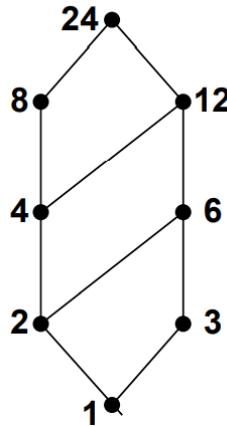
²greatest

³lower bound

⁴upper bound

⁵greatest lower bound

⁶least upper bound



Allora:

- 1 è il minimo, 24 è il massimo;
- il sottoinsieme $\{8, 12\}$ ha tre limiti inferiori, i.e., 1, 2, 4
- $4 = \text{glb}(\{8, 12\})$

♦

Definizione 3.31 (Poset ben ordinato). Un poset $(A; \leq)$ si dice **ben-ordinato** se è totalmente ordinato e se ogni sottoinsieme non vuoto di A ha un elemento minimale (*least*).

3.4.5 Meet, join e reticoli

Definizione 3.32 (Meet e join). Sia dato un poset $(A; \leq)$. Se il sottoinsieme $\{a, b\} \subseteq A$ ha un glb, allora $\text{glb}(\{a, b\})$ è detto **meet** di a e b (spesso scritto $a \wedge b$). Se a, b hanno un lub, allora $\text{lub}(\{a, b\})$ è detto **join** di a e b (spesso scritto $a \vee b$).

Definizione 3.33 (Reticolo). Un poset in cui ogni coppia di elementi ha un *meet* e un *join* si dice **reticolo**⁷.

3.5 Funzioni

Definizione 3.34 (Funzione). Una **funzione** $f : A \rightarrow B$ è una relazione $A \rightarrow B$ con le seguenti proprietà:

1. $\forall a \in A \quad \exists b \in B \quad a \ f \ b \quad (f \text{ è totalmente definita})$
2. $\forall a \in A \quad \forall b, b' \in B \quad (a \ f \ b \wedge a \ f \ b' \rightarrow b = b') \quad (f \text{ è ben definita})$

⁷lattice

Si noti che $a \mapsto b$ corrisponde a $b = f(a)$.

Definizione 3.35 (Insieme delle funzioni). L'insieme delle funzioni $A \rightarrow B$ è denotato con B^A . La notazione è motivata dal fatto che tale insieme ha cardinalità $|B|^{|A|}$.

Definizione 3.36 (Funzione parziale). Una **funzione parziale** $A \rightarrow B$ è una relazione $A \rightarrow B$ per cui vale la condizione (2.) nella Definizione 3.34.

Definizione 3.37 (Immagine di un sottoinsieme). Sia $S \subseteq A$. Allora l'**immagine** di S secondo f è l'insieme

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

Definizione 3.38 (Immagine di una funzione). Il sottoinsieme $f(A)$ di B è detto **immagine** di f e si denota anche con $\text{Im}(f)$.

Definizione 3.39 (Antimmagine). Per un sottoinsieme $T \subseteq B$, l'**antimmagine**⁸ di T , denotata con $f^{-1}(T)$ è l'insieme dei valori di A che vengono mandati in T :

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}$$

Definizione 3.40 (Proprietà delle funzioni). Sia $f : A \rightarrow B$ una funzione. Allora, f si dice:

- **iniettiva** (*one-to-one*) se per $a \neq b$ vale $f(a) \neq f(b)$, i.e., non esistono due argomenti diversi che producono la stessa immagine (non esistono *collisioni*)
- **suriettiva** (*onto*) se $f(A) = B$
- **biiettiva** se è sia iniettiva che suriettiva

Definizione 3.41 (Funzione inversa). Per una biiezione f , la sua **inversa** f^{-1} è la relazione inversa \widehat{f} .

Definizione 3.42 (Composizione di funzioni). Dette $f : A \rightarrow B, g : B \rightarrow C$ due funzioni, la loro **composizione**, denotata con $g \circ f$ (o anche gf) è definita come:

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

Lemma 3.12. *La composizione di funzioni è associativa:*

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

Dimostrazione. Questo lemma è una diretta conseguenza del Lemma 3.5. ■

⁸*Urbild / Preimage*

⁹La composizione di funzioni è analoga alla composizione di relazioni. Tuttavia, viene utilizzata una **notazione differente!** La composizione di due relazioni ρ e σ è denotata con $\rho \circ \sigma$, ma la composizione di due funzioni f, g è denotata con $g \circ f$.

3.6 Insiemi numerabili e non numerabili

3.6.1 Numerabilità

Definizione 3.43 (Numerabilità). Detti A, B, C tre insiemi, vale:

- (i) A e B si dicono **equipollenti**¹⁰, denotati con $A \sim B$ se esiste una biiezione $A \rightarrow B$
- (ii) B **domina** A , scritto $A \leq B$, se $A \sim C$ per un certo $C \subseteq B$ o, equivalentemente, se esiste una funzione iniettiva $A \rightarrow B$.
- (iii) A è detto **numerabile** se $A \leq \mathbb{N}$ e **non numerabile** altrimenti.

Esempio 13. L'insieme $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ è numerabile. Infatti, esiste una biiezione $f : \mathbb{N} \rightarrow \mathbb{Z}$, $f(n) = (-1)^n \lceil \frac{n}{2} \rceil$



Lemma 3.13.

- (i) La relazione \leq è transitiva.

- (ii) $A \subseteq B \Rightarrow A \leq B$

Dimostrazione.

Dim. (i)

Se esiste una funzione iniettiva $A \rightarrow B$ e una da $B \rightarrow C$, allora la loro composizione è una funzione iniettiva $A \rightarrow C$.

Dim. (ii)

Se $A \subseteq B$, allora id_A è una funzione iniettiva $A \rightarrow B$. ■

Teorema 3.14 (Bernstein-Schröder). $A \leq B \wedge B \leq A \Rightarrow A \sim B$

3.6.2 Tra finito e infinito numerabile

Teorema 3.15. Un insieme A è **numerabile** se e solo se A è finito o se $A \sim \mathbb{N}$.

¹⁰equinumerous

Dimostrazione.

Dim. \Leftarrow

Se A è finito, allora è numerabile. Se $A \sim \mathbb{N}$, allora A è numerabile.

Dim. \Rightarrow

Dimostriamo ora che se A è numerabile e infinto, allora $A \sim \mathbb{N}$. Secondo la definizione, $A \leq \mathbb{N}$ significa che esiste una biiezione $f : A \rightarrow C$ per $C \subseteq \mathbb{N}$. Per ogni sottosieme infinito C di \mathbb{N} , è possibile definire una biiezione $g : C \rightarrow \mathbb{N}$ come segue. Secondo il principio di ordine, esiste almeno un $c_0 \in C$ tale che $g(c_0) = 0$. Si definisca ora $C_1 = C \setminus \{c_0\}$. Sempre secondo lo stesso principio, esiste almeno un $c_1 \in C_1$ con $g(c_1) = 1$. Questo processo può essere continuato indefinitamente. Allora, $g \circ f$ è una biiezione $A \rightarrow \mathbb{N}$, il che dimostra che $A \sim \mathbb{N}$. ■

3.6.3 Importanti insiemi numerabili

Teorema 3.16. L'insieme $\{0, 1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \dots\}$ delle sequenze binarie finite è numerabile.

Dimostrazione. Dobbiamo trovare una funzione iniettiva $f : \{0, 1\}^* \rightarrow \mathbb{N}$. Concateniamo un “1” all'inizio di ogni stringa e poi convertiamo la stringa risultante in un numero naturale. Es.: $0010_2 \rightarrow 18_{10}$. ■

Teorema 3.17. L'insieme $\mathbb{N} \times \mathbb{N}$ è numerabile.

Corollario 3.18. Il prodotto cartesiano $A \rightarrow B$ di due insiemi numerabili A, B è numerabile, i.e.,

$$A \leq \mathbb{N} \wedge B \leq \mathbb{N} \implies A \times B \leq \mathbb{N}$$

Dimostrazione. Secondo la Definizione 3.43, dobbiamo scrivere una funzione iniettiva $A \times B \rightarrow \mathbb{N}$. Siano $f_1 : A \rightarrow \mathbb{N}$ e $f_2 : B \rightarrow \mathbb{N}$ le iniezioni esistenti dal momento che A e B sono numerabili. Allora la funzione $g : A \times B \rightarrow \mathbb{N}$, $g(a, b) = (f_1(a), f_2(b))$ è un iniezione. Sia ora $h : \mathbb{N}^2 \rightarrow \mathbb{N}$ la biiezione garantita dal Teorema 3.17. Dato che la composizione di due iniezioni è un iniezione, allora abbiamo correttamente generato $h \circ g : A \times B \rightarrow \mathbb{N}$. ■

Corollario 3.19. L'insieme dei numeri razionali \mathbb{Q} è numerabile.

Dimostrazione. Ogni numero razionale $\frac{m}{n}$ può esser rappresentato con la coppia ordinata (m, n) con $m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}$, dove m e n sono coprimi. Sappiamo già che $\mathbb{Z} \leq \mathbb{N}$, e dal Corollario 3.18 ricaviamo facilmente che $\mathbb{Z} \times \mathbb{N} \leq \mathbb{N}$. Per la transitività di \leq , $\mathbb{Q} \leq \mathbb{N}$. ■

Teorema 3.20. Siano A, A_i per $i \in \mathbb{N}$ insiemi numerabili. Allora:

- (i) Per ogni $n \in \mathbb{N}$, l'insieme A^n delle n -tuple su A è numerabile.
- (ii) L'unione $\bigcup_i A_i$ è numerabile

(iii) *L'insieme A^* delle sequenze finite di elementi di A è numerabile.*

Dimostrazione.

Dim. (i)

Per induzione. La base consiste nel fatto che $A^1 = A$ è numerabile. Il passo d'induzione segue dal Corollario 3.18, siccome sia A che A^n sono numerabili.

Dim. (iii)

L'affermazione (iii) implica (i) e quindi fornisce una dimostrazione alternativa per (i). Definiamo un'iniezione $f : A \rightarrow \{0, 1\}^*$ e un'altra iniezione $g : A^* \rightarrow (\{0, 1\}^*)^*$. Detta (a_1, \dots, a_n) una sequenza qualsiasi, abbiamo

$$g(a_1, \dots, a_n) = (f(a_1), \dots, f(a_n))$$

Dobbiamo ora mostrare un'iniezione $(\{0, 1\}^*)^* \rightarrow \{0, 1\}^*$. La otteniamo come segue. Rimpiazziamo ogni "0" nella sequenza con "00" e ogni "1" con "01". Concateniamo in seguito ogni sequenza (espansa) separandoli con "11". Si tratta di un'iniezione perché sia il separatore che gli "0" aggiuntivi possono essere individuati e rimossi ottenendo così la sequenza originale. ■

3.6.4 Non-numerabilità di $\{0, 1\}^\infty$

Definizione 3.44 ($\{0, 1\}^\infty$). Sia $\{0, 1\}^\infty$ l'insieme delle sequenze binarie semi-infinite.

Teorema 3.21. *L'insieme $\{0, 1\}^\infty$ è non-numerabile.*

Dimostrazione. La dimostrazione avviene per contraddizione. Si assume esista una biiezione $f : \{0, 1\}^\infty \rightarrow \{0, 1\}^\infty$. Sia β_{ij} il j -esimo bit nella i -esima sequenza $f(i)$.

$$f(i) = \beta_{i,0}, \beta_{i,1}, \dots$$

Sia ora \bar{b} il complemento di un bit b . Definiamo una sequenza binaria semi-infinita α come segue:

$$\alpha = \overline{\beta_{0,0}}, \overline{\beta_{1,1}}, \dots$$

Ovviamente è $\alpha \in \{0, 1\}^\infty$ ma non esiste nessun $n \in \mathbb{N}$ per cui $\alpha = f(n)$, siccome α non coincide, almeno nell' n -esimo bit (ma anche altrove), con $f(n)$. Concludiamo quindi che una tale biiezione f non esiste. ■

3.6.5 Esistenza di funzioni incalcolabili

Definizione 3.45 (Funzione calcolabile). Una funzione $f : \mathbb{N} \rightarrow \{0, 1\}$ è detta **calcolabile** se esiste un programma che, preso n in input, restituisca $f(n)$.

Corollario 3.22. *Esistono funzioni incalcolabili $\mathbb{N} \rightarrow \{0, 1\}$*

Un esempio specifico di funzione incalcolabile è dato dal celebre *Problema della terminazione*¹¹. Dato in input un programma e un input per quel programma, si chiede di determinare se il programma termini oppure no (entri cioè in un ciclo infinito). Questo problema è **indecidibile**.

¹¹*Halting Problem*

4 Teoria dei Numeri

4.2 Divisori e divisione

4.2.1 Divisori

Definizione 4.1 (Relazione di divisione). Per due interi a, b si dice che a **divide** b , denotato con $a \mid b$ se esiste un intero c tale che $b = ac$. Allora, a è detto il **divisore** di b , e b è un **multiplo** di a . Se $a \neq 0$ e c esiste, allora c è detto **quoziente**. La relazione negata è denotata con $a \nmid b$.

Osservazione 11. Tutti gli interi non nulli sono divisori di 0. Inoltre, 1 e -1 sono divisori di ogni intero.

4.2.2 Divisione con resto

Teorema 4.1 (Euclide). *Per tutti gli interi a e $d \neq 0$ esistono interi unici q e r per cui vale:*

$$a = dq + r \wedge 0 \leq r < |d|$$

In questo caso, a è detto **dividendo**, d è detto **divisore** e r è il **resto**. Il resto r è spesso denotato con $R_d(a)$ o anche $a \mod d$

Dimostrazione. Sia S l'insieme dei resti non negativi:

$$S := \{s \mid s \geq 0 \text{ e } a = dt + s \text{ per qualche } t \in \mathbb{Z}\}$$

Dimostriamo le seguenti tre affermazioni in un ciclo di implicazioni:

- (1) $S \neq \emptyset$
- (2) $S \ni r < |d|$
- (3) Il valore di r nell'affermazione (2) è unico.

Dim. (1)

Effettuiamo una distinzione dei casi:

- $\boxed{a \geq 0}$ Allora $a = d \cdot 0 + a \implies a \in S$
- $\boxed{a < 0, d > 0}$ Allora $a = da + (1 - d)a \implies (1 - d)a \in S$

- $a < 0, d < 0$ Allora $a = d(-a) + (1+d)a \implies (1+d)a \in S$

Dim. (1) \implies (2)

Siccome $S \neq \emptyset$, allora possiede un elemento minimo, che denotiamo con r . Dimostriamo ora che $r < |d|$ per contraddizione, ossia assumendo $r \geq d$. Dalla definizione di S sappiamo che vale $a = dq + r$ per un certo q . Effettuiamno una distinzione dei casi a proposito del simbolo d'ordine:

- $d > 0$ Allora vale

$$a = d(q+1) + (r - |d|)$$

ossia $r - |d| \geq 0$ e quindi $r - |d| \in S$, il che significa che r non è il più piccolo elemento di S , contraddicendo la nostra assunzione

- $d < 0$ Allora

$$a = d(q-1) + (r - |d|)$$

il che ancora una volta significa che $r - |d| \in S$, provocando una contraddizione.

Dim. (2) \implies (3)

Ci rimane da dimostrare che r è unico. Dimostriamo solo il caso $d > 0$; il caso $d < 0$ è del tutto analogo. Supponiamo esista un altro $r' \neq r$ per cui valga $0 \leq r' < |d|$ e $a = dq' + r'$ per un certo q' . Allora: se $q' = q$, allora $r' = a - dq' = a - dq = r$ contraddicendo l'ipotesi iniziale. Se $q' < q$, allora $q - q' \geq 1$, quindi:

$$r' = a - dq' = (a - dq) + d(q - q') \geq r + d$$

Dal momento che $r' \geq r + d \geq d$, la condizione $0 \leq r' < |d|$ viene violata. Per $q' > q$ vale un ragionamento analogo. ■

4.2.3 Massimi comuni divisori

Definizione 4.2 (Massimi comuni divisori). Per due interi a, b (non entrambi nulli), un intero d è detto un **massimo comun divisore** di a e di b se d divide sia a che b e se ogni comun divisore di a e b divide d , ossia se vale:

$$(d \mid a) \wedge (d \mid b) \wedge \forall c ((c \mid a \wedge c \mid b) \rightarrow c \mid d)$$

Definizione 4.3 (Massimo comun divisore (definizione canonica)). Per $a, b \in \mathbb{Z}$ (non entrambi nulli), si definisce l'unico massimo comun divisore positivo con la notazione $\gcd(a, b)$ ¹². Questo valore è detto solitamente *il* massimo comun divisore. Se $\gcd(a, b) = 1$, allora a e b sono coprimi.

Lemma 4.2. *Detti m, n, q degli interi, vale:*

$$\gcd(m, n - qm) = \gcd(m, n)$$

¹²DE: ggT(a, b) ; IT: MCD(a, b)

Dimostrazione. Ogni divisore comune di m e $n - qm$ è anche divisore di n e m e viceversa. ■

Il Lemma precedente implica in particolare che:

$$\gcd(m, R_m(n)) = \gcd(m, n)$$

Tale principio è alla base dell'algoritmo di Euclide. Si parte con $m < n$ e si rimpiazza ripetutamente la coppia (m, n) con $(R_m(n), m)$ fino ad ottenere resto nullo. A quel punto, l'ultimo valore $\neq 0$ è proprio il $\gcd(m, n)$.

Definizione 4.4 (Ideale). Detti $a, b \in \mathbb{Z}$, l'**ideale** generato da a e b è l'insieme

$$(a, b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$$

cioè l'insieme di tutte le combinazioni lineari di a e b .

In modo analogo, l'ideale di un intero a è l'insieme

$$(a) = \{ua \mid u \in \mathbb{Z}\}$$

Il seguente Lemma implica che ogni ideale in \mathbb{Z} può essere generato da un singolo intero.

Lemma 4.3. Per $a, b \in \mathbb{Z}$ esiste $d \in \mathbb{Z}$ tale che $(a, b) = (d)$

Dimostrazione. Se $a = b = 0 \implies d = 0$. Assumiamo ora che almeno uno fra a e b sia non-nullo. Allora, sia d il minimo tra gli elementi positivi in (a, b) . È allora chiaro che $(d) \subseteq (a, b)$, dal momento che ogni multiplo di d è anche in (a, b) . Rimane da dimostrare che $(a, b) \subseteq (d)$. Per ogni $c \in (a, b)$ esistono q, r con $0 \leq r < d$ tali che $c = qd + r$. Dal momento che sia c che d sono elementi di (a, b) , allora lo è anche $r = c - qd$. Siccome l'assunto era $0 \leq r < d$ e d è, per ipotesi, il minimo elemento positivo di (a, b) , allora dev'essere $r = 0$ che porta alla conclusione $c = qd \in (d)$. ■

Lemma 4.4. Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Se $(a, b) = (d)$, allora d è un massimo comun divisore di a e di b .

Dimostrazione. Siccome $a \in (d)$ e $b \in (d)$, possiamo dire che d è divisore comune di a e di b . Per affermare che è un massimo comun divisore, basta osservare che ogni divisore comune di a, b (diciamo c) divide ogni intero della forma $ua + vb$, in particolare d . ■

Corollario 4.5. Per $a, b \in \mathbb{Z}$ non entrambi nulli, esistono $u, v \in \mathbb{Z}$ tali che

$$\gcd(a, b) = ua + vb$$

4.2.4 Minimo comune multiplo

Definizione 4.5 (Minimo comune multiplo). Il **minimo comune multiplo** di due interi a, b , scritto $\text{lcm}(a, b)$, è il multiplo comune di a e di b che divide ogni multiplo comune di a e di b , i.e.,

$$a \mid \ell \wedge b \mid \ell \wedge \forall m ((a \mid m \wedge b \mid m) \rightarrow \ell \mid m)$$

dove $\ell = \text{lcm}(a, b)$.

4.3 Scomposizione in fattori primi

4.3.1 Numeri primi e Teorema Fondamentale dell’Aritmetica

Definizione 4.6 (Numero primo). Un intero positivo $p > 1$ è detto **primo** se possiede esattamente due divisori positivi: 1 e p . Un intero che non soddisfa la presente definizione è detto *composto*.

Teorema 4.6 (Fondamentale dell’Aritmetica). *Ogni intero positivo può essere scomposto in un unico prodotto di fattori primi (a meno dell’ordine).*

4.3.3 Espressione di gcd e lcm

Il Teorema fondamentale dell’Aritmetica ci assicura che gli interi a e b possono essere scritti come:

$$a = \prod_i p_i^{e_i} \quad \text{e} \quad b = \prod_i p_i^{f_i}$$

Da questo ricaviamo che:

$$\gcd(a, b) = \prod_i p_i^{\min(e_i, f_i)}$$

e

$$\operatorname{lcm}(a, b) = \prod_i p_i^{\max(e_i, f_i)}$$

da cui concludiamo

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$$

dal momento che per ogni i si ha:

$$\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$$

4.5 Congruenze e aritmetica modulare

4.5.1 Congruenze modulari

Definizione 4.8 (Relazione di congruenza modulo m). Detti $a, b, m \in \mathbb{Z}$ con $m \geq 1$, si dice che a è **congruente a b modulo m** se m divide $a - b$. Si scrive $a \equiv b \pmod{m}$ o, più semplicemente $a \equiv_m b$, i.e.,

$$a \equiv_m b \Leftrightarrow m \mid (a - b)$$

Lemma 4.13. *Per ogni $m \geq 1$, la relazione \equiv_m è una relazione d’equivalenza in \mathbb{Z} .*

Le congruenze modulari sono compatibili con le canoniche operazioni aritmetiche in \mathbb{Z} .

Lemma 4.14. *Se $a \equiv_m b$ e $c \equiv_m d$, allora:*

$$a + c \equiv_m b + d \quad \text{e} \quad ac \equiv_m bd$$

Dimostrazione. Dimostriamo solo la prima affermazione; la seconda si dimostra in modo del tutto analogo. Sappiamo che $m \mid (a - b)$ e $m \mid (c - d)$. Allora, $m \mid ((a - b) + (c - d))$ che è equivalente ad affermare che $m \mid ((a + c) - (b + d))$. ■

Corollario 4.15. *Sia $f(x_1, \dots, x_k)$ un polinomio multivariabile in k variabili a coefficienti interi. Sia ora $m \geq 1$. Se $a_i \equiv_m b_i$ per $1 \leq i \leq k$, allora:*

$$f(a_1, \dots, a_k) \equiv_m f(b_1, \dots, b_k)$$

Dimostrazione. La valutazione di un polinomio è, alla base, una sequenza di addizioni e moltiplicazioni. Pertanto, la congruenza modulo m è mantenuta, come afferma il Lemma 4.14. Tale Corollario è quindi dimostrabile per induzione. ■

4.5.2 Aritmetica modulare

Data la relazione di congruenza modulo m , esistono m classi di equivalenza, ossia $[0], \dots, [m - 1]$. Ogni classe $[a]$ possiede un rappresentante $R_m(a) \in \mathbb{Z}_m$ dove

$$\mathbb{Z}_m = \{0, \dots, m - 1\}$$

Lemma 4.16. *Per ogni $a, b, m \in \mathbb{Z}, m \geq 1$ si ha:*

- (i) $a \equiv_m R_m(a)$
- (ii) $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$

Corollario 4.17. *Sia $f(x_1, \dots, x_k)$ un polinomio in k variabili a coefficienti interi, e sia $m \geq 1$. Allora vale:*

$$R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$$

Dimostrazione. Dal Lemma 4.16 (i) abbiamo $a_i \equiv_m R_m(a_i)$. Quindi, usando il Corollario 4.15 otteniamo $f(a_1, \dots, a_k) = f(R_m(a_1), \dots, R_m(a_k))$. Usando infine il punto (ii) del Lemma 4.16 otteniamo la tesi. ■

Esempio 14. Vogliamo calcolare $R_{24}(7^{100})$. È facile osservare che $7^2 = 49 \equiv_{24} 1$. Allora vale:

$$R_{24}(7^{100}) = R_{24}((7^2)^{50}) = R_{24}(R_{24}(7^2)^{50}) = R_{24}(1^{50}) = 1$$

4.5.3 Inversi moltiplicativi

Vogliamo trovare le soluzioni x dell'equazione modulare

$$ax \equiv_m b$$

È ovvio che, detta x una soluzione dell'equazione, allora anche $x + km$ per ogni $k \in \mathbb{Z}$ è soluzione. In particolare, ci interessiamo ai casi in cui $\gcd(a, m) = 1$ e $b = 1$.

Lemma 4.18. *L'equazione modulare*

$$ax \equiv_m 1$$

ha una soluzione $x \in \mathbb{Z}_m$ se e solo se $\gcd(a, m) = 1$.

Dimostrazione.

Dim. \Rightarrow

Se x soddisfa $ax \equiv_m 1$, allora $ax = km + 1$ per un certo k . Osserviamo che $\gcd(a, m)$ divide sia a che m , e quindi anche $ax - km = 1$. Pertanto, $\gcd(a, m) = 1$. Se fosse $\gcd(a, m) > 1$, non si avrebbe soluzione.

Dim. \Leftarrow

Si assuma che $\gcd(a, m) = 1$. Secondo il Corollario 4.5, esistono degli interi u, v per cui vale $ua + vm = \gcd(a, m)$. Dal momento che $vm \equiv_m 0$ abbiamo $ua \equiv_m 1$. Pertanto, $x = u$ è soluzione in \mathbb{Z} e $R_m(u)$ è soluzione in \mathbb{Z}_m .

Per dimostrare l'unicità di x in \mathbb{Z}_m , supponiamo esista un'altra soluzione $x' \in \mathbb{Z}_m$. Allora $ax - ax' = 0$ e quindi $a(x - x') \equiv_m 0$. Pertanto, m divide $a(x - x')$. Ora, dal momento che $\gcd(a, m) = 1$, m deve dividere $(x - x')$. Si ha infine $R_m(x) = R_m(x')$ ed è quindi provata l'unicità della soluzione. ■

Definizione 4.9 (Inverso moltiplicativo). Se $\gcd(a, m) = 1$, la soluzione unica $x \in \mathbb{Z}_m$ dell'equazione modulare $ax \equiv_m 1$ è detta **inverso moltiplicativo** di a modulo m , ed è denotata con $x \equiv_m a^{-1}$ o $x \equiv_m 1/a$

Osservazione 12. Se $\gcd(a, m) \neq 1$ allora a non possiede nessun inverso modulo m .

4.5.4 Il Teorema Cinese del Resto (CRT)

Teorema 4.19 (Cinese del Resto (CRT)). *Siano m_1, \dots, m_r numeri primi distinti fra loro e sia $M = \prod_{i=1}^r m_i$. Per ogni lista a_1, \dots, a_r con $0 \leq a_i < m_i$ per ogni $i = 1, \dots, r$, il sistema di equazioni modulari*

$$\begin{cases} x \equiv_{m_1} a_1 \\ \vdots \\ x \equiv_{m_r} a_r \end{cases}$$

possiede un'unica soluzione x che soddisfa $0 \leq x < M$.

Dimostrazione. Sia $M_i = M/m_i$. Allora vale $\gcd(M_i, m_i) = 1$ siccome ogni fattore m_k (con $k \neq i$) di M_i è coprimo a m_i e quindi lo è anche M_i . Quindi esiste un N_i che soddisfa la relazione

$$M_i N_i \equiv_{m_i} 1$$

Si noti che per ogni $k \neq i$ abbiamo $M_i \equiv_{m_k} 0$ che implica

$$M_i N_i \equiv_{m_k} 0$$

Pertanto è

$$\sum_{i=1}^r a_i M_i N_i \equiv_{m_k} a_k \quad (\forall k)$$

Allora l'intero

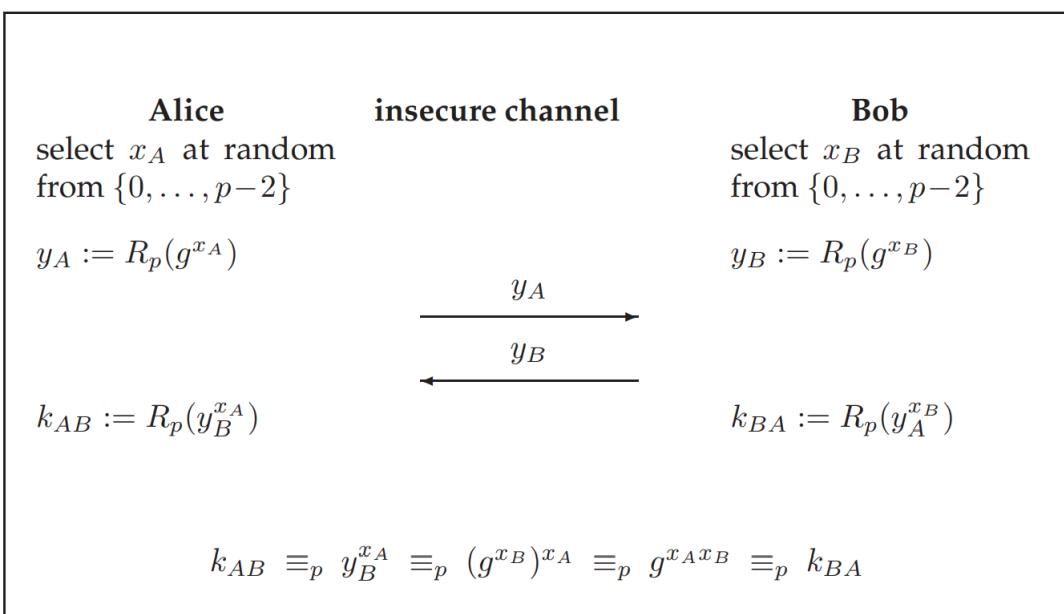
$$x := R_M \left(\sum_{i=1}^r a_i M_i N_i \right)$$

soddisfa tutte le congruenze. Per provare l'unicità della soluzione x , si osservi che per altre due soluzioni, diciamo x' e x'' , vale $x' - x'' \equiv_{m_i} 0$ per ogni i . Questo significa che $x' - x''$ è un multiplo di tutti gli m_i e quindi anche di $\text{lcm}(m_1, \dots, m_r) = M$. Pertanto $x' \equiv_M x''$. ■

Esempio 15. Vogliamo calcolare $R_{35}(2^{1000})$. Dal CRT, sappiamo che possiamo farlo separatamente modulo 5 e modulo 7 (i fattori primi di 35). Notiamo che $2^4 \equiv_5 1$, e quindi concludiamo che $2^{1000} \equiv_5 1$. Notiamo anche che $2^3 \equiv_7 1$ e quindi $2^{1000} \equiv_7 2$. Questo ci porta alla soluzione finale $2^{1000} \equiv_{35} 16$, dal momento che $x = 16$ è l'unico intero nell'intervallo $[0, 34]$ che soddisfa $x \equiv_5 1$ e $x \equiv_7 2$



4.6 Applicazione: Lo scambio di chiavi Diffie-Hellman



5 Algebra

5.1 Introduzione

5.1.2 Strutture algebriche

Definizione 5.1 (Arietà). Un'operazione su un insieme S è una funzione¹³ $S^n \rightarrow S$, dove $n \geq 0$ è detto **arietà**¹⁴ dell'operazione.

Osservazione 13. Nel linguaggio comune è raramente usato il termine “arietà”. Infatti, si usa di frequente aggiungere il prefisso “-aria”. La somma è quindi detta *operazione binaria* (e non “operazione di arietà 2”).

n	Nome	Esempio
0	Nullaria, costante	$f() = 2$
1	Unaria	$f(x) = 2x$
2	Binaria	$f(x, y) = 2xy$
3	Ternaria	$f(x, y, z) = 2xyz$
4	Quaternaria	$f(x, y, z, w) = 2xyzw$
5	Quinaria	$f(x, y, z, w, v) = 2xyzwv$
:	:	:
n	n -aria	$f(a_1, \dots, a_n) = \sum_{i=0}^n a_i$

Definizione 5.2 (Algebra). Un'**algebra** (o *struttura algebrica*, o Ω -algebra) è una coppia $\langle S; \Omega \rangle$, dove S è l'**insieme sostegno**¹⁵ e Ω è una lista $\Omega = (\omega_1, \dots, \omega_n)$ di operazioni su S .

5.2 Monoidi e gruppi

In questa sezione ci interessiamo in particolare delle strutture algebriche del tipo $\langle S; * \rangle$ di un insieme S munito di un'operazione binaria, unaria o nullaria $*$. Le comuni addizione (+) e moltiplicazione (\cdot) sono entrambe operazioni binarie. È importante tuttavia notare che $*$ è un'operazione arbitraria: il nome ad essa assegnato non ha alcuna rilevanza matematica.

5.2.1 Elementi neutri

Definizione 5.3 (Elemento neutro). Un **elemento neutro** a sinistra [a destra] di un'algebra $\langle S; * \rangle$ è un elemento $e \in S$ tale che $e * a = a$ [$a * e = a$] per ogni $a \in S$. Se $e * a = a * e = a$ per ogni $a \in S$, allora e è detto semplicemente **elemento neutro**.

¹³A volte anche una funzione parziale

¹⁴DE: *Stelligkeit*, EN: *arity*

¹⁵DE: *Trägermenge*, EN: *carrier set*

Per l'addizione, $e = 0$; per la moltiplicazione è $e = 1$.

Lemma 5.1. *Se $\langle S; * \rangle$ ha sia un elemento neutro a sinistra che a destra, allora tali elementi sono uguali. In particolare, $\langle S; * \rangle$ può avere al massimo un elemento neutro.*

Dimostrazione. Supponiamo esistano e, e' rispettivamente elemento neutro a sinistra e a destra. Allora, per definizione, $e * e' = e'$ (detto e elemento neutro a sinistra), ma anche $e * e' = e$ (detto e' elemento neutro a destra). Pertanto, $e' = e$. ■

5.2.2 Associatività e monoidi

Definizione 5.4 (Associatività). Un'operazione binaria $*$ su un insieme S si dice **associativa** se vale

$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in S$$

L'associatività è una proprietà molto particolare per un'algebra, siccome consente di non doversi preoccupare dell'ordine in cui i termini vengono operati.

Definizione 5.5 (Monoide). Un **monoide** è un'algebra $\langle M; *, e \rangle$ dove $*$ è associativa, e e è l'elemento neutro.

Esempio 16. Di seguito elenchiamo alcuni monoidi comuni:

- $\langle \mathbb{Z}; +, 0 \rangle, \langle \mathbb{Z}; \cdot, 1 \rangle$
- $\langle \mathbb{Q}; +, 0 \rangle, \langle \mathbb{Q}; \cdot, 1 \rangle$
- $\langle \mathbb{R}; +, 0 \rangle, \langle \mathbb{R}; \cdot, 1 \rangle$
- $\langle \mathbb{Z}_m; \oplus_m, 0 \rangle, \langle \mathbb{Z}_m; \odot_m, 1 \rangle$ dove \oplus_m e \odot_m rappresentano rispettivamente l'addizione e la moltiplicazione modulo m
- $\langle A^A; \circ, \text{id} \rangle$



5.2.3 Elementi inversi e gruppi

Definizione 5.6 (Elemento inverso). Un **elemento inverso** a sinistra [a destra] di un elemento a in un'algebra $\langle S; *, e \rangle$ con elemento neutro e , è un elemento $b \in S$ tale che $b * a = e$ [$a * b = e$]. Se $b * a = a * b = e$, allora b è detto semplicemente **elemento inverso** di a .

Per dimostrare l'unicità dell'inverso (se esiste), è necessario che $*$ sia associativa.

Lemma 5.2. *In un monoide $\langle M; *, e \rangle$, se $a \in M$ possiede sia un elemento inverso a sinistra che a destra, allora essi sono uguali. In particolare, a ha al massimo un inverso.*

Dimostrazione. Siano b e c due inversi di a (rispettivamente a sinistra e a destra). Ciò significa che vale $b * a = e$ e $a * c = e$. Allora vale anche

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

■

Segue ora la definizione di uno dei più importanti concetti di Algebra.

Definizione 5.7 (Gruppo). Un **gruppo** è un algebra $\langle G; *, \widehat{\cdot}, e \rangle$ che soddisfa i tre seguenti assiomi:

- (G1) $*$ è associativa;
- (G2) e è l'elemento neutro, i.e., $a * e = e * a = a$ per ogni $a \in G$
- (G3) Ogni $a \in G$ possiede un elemento inverso \widehat{a} , i.e., $a * \widehat{a} = \widehat{a} * a = e$

Esempio 17. Seguono degli esempi di gruppi comuni:

- $\langle \mathbb{Z}; +, -, 0 \rangle$
- $\langle \mathbb{Q}; +, -, 0 \rangle$
- $\langle \mathbb{Q} \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$
- $\langle \mathbb{R}; +, -, 0 \rangle$
- $\langle \mathbb{R} \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$
- $\langle \mathbb{Z}_m; \oplus, \ominus, 0 \rangle$

◆

Definizione 5.8 (Gruppo abeliano). Un gruppo $\langle G; * \rangle$ (o un monoide) si dice **abeliano** (o **commutativo**) se $a * b = b * a$ per ogni $a, b \in G$

Lemma 5.3. Detto $\langle G; *, \widehat{\cdot}, e \rangle$ un gruppo, valgono le seguenti proprietà per ogni $a, b, c \in G$

- (i) $(\widehat{\widehat{a}}) = a$
- (ii) $\widehat{a * b} = b * a$
- (iii) $a * b = a * c \implies b = c$ (*Legge di cancellazione a sinistra*)
- (iv) $b * a = c * a \implies b = c$ (*Legge di cancellazione a destra*)
- (v) L'equazione $a * x = b$ ha una soluzione x unica per ogni a, b . Lo stesso vale per $x * a = b$

5.2.4 (Non)-minimalità degli assiomi dei gruppi

In Matematica, si richiede generalmente che gli assiomi su cui ci si basa siano minimali. È possibile dimostrare che l'assioma (G2) della Definizione 5.7 (di Gruppo) può essere semplificato richiedendo solamente che $a * e = a$ (lo si chiami assioma (G2')). L'equazione $e * a = a$ è allora implicata dagli altri assiomi. In modo analogo, dimostriamo qui di seguito che l'assioma (G3) può essere semplificato richiedendo solamente $a * \widehat{a} = e$ (si dica (G3')).

Dimostrazione.

$$\begin{aligned}
 \widehat{a} * a &= (\widehat{a} * a) * e && (G2') \\
 &= (\widehat{a} * a) * (\widehat{a} * \widehat{\widehat{a}}) && (G3') \\
 &= \widehat{a} * (a * (\widehat{a} * \widehat{\widehat{a}})) && (G1) \\
 &= \widehat{a} * ((a * \widehat{a}) * \widehat{\widehat{a}}) && (G1) \\
 &= \widehat{a} * (e * \widehat{\widehat{a}}) && (G3) \\
 &= (\widehat{a} * e) * \widehat{\widehat{a}} && (G1) \\
 &= \widehat{a} * \widehat{\widehat{a}} && (G2') \\
 &= e && (G3')
 \end{aligned}$$

■

5.3 La struttura dei gruppi

5.3.1 Il prodotto diretto di gruppi

Definizione 5.9 (Prodotto diretto di gruppi). Il **prodotto diretto** di n gruppi $\langle G_1; *_1 \rangle, \dots, \langle G_n; *_n \rangle$ è l'algebra

$$\left\langle \bigtimes_{i=1}^n G_i; \star \right\rangle$$

dove l'operazione \star agisce componente per componente:

$$(a_1, \dots, a_n) \star (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$$

Lemma 5.4. $\left\langle \bigtimes_{i=1}^n G_i; \star \right\rangle$ è un gruppo in cui l'elemento neutro e l'operazione di inversione è definita componente per componente nei rispettivi gruppi.

Esempio 18. Si consideri il gruppo $\langle \mathbb{Z}_5; \oplus \rangle \times \langle \mathbb{Z}_7; \oplus \rangle$. Allora, l'insieme di sostegno è $\mathbb{Z}_5 \times \mathbb{Z}_7$, l'elemento neutro è $(0, 0)$. Se chiamiamo \star l'operazione in tale gruppo, allora abbiamo ad esempio $(2, 6) \star (4, 3) = (1, 2)$. Ciò segue direttamente dalla definizione di \star : $(2, 6) \star (4, 3) = (2 \oplus_5 4, 6 \oplus_7 3) = (1, 2)$. Inoltre, $\widehat{(2, 6)} = (3, 1)$. In effetti, basta notare che $2 \oplus_5 3 = 5 \equiv_5 0$ e $6 \oplus_7 1 = 7 \equiv_7 0$. Grazie al CRT, possiamo affermare che $\langle \mathbb{Z}_5; \oplus \rangle \times \langle \mathbb{Z}_7; \oplus \rangle$ è isomorfo a $\langle \mathbb{Z}_{35}; \oplus \rangle$, un concetto affrontato nella prossima sezione.

◆

5.3.2 Omomorfismo di gruppi

Definizione 5.10 (Omomorfismo). Dati due gruppi $\langle G; *, \hat{e} \rangle$ e $\langle H; \star, \tilde{e}' \rangle$, una funzione $\psi : G \rightarrow H$ è detta **omomorfismo di gruppi**, se per ogni a, b vale

$$\psi(a * b) = \psi(a) \star \psi(b)$$

Lemma 5.5. Un omomorfismo ψ tra i gruppi $\langle G; *, \hat{e} \rangle$ e $\langle H; \star, \tilde{e}' \rangle$ soddisfa le seguenti proprietà:

- (i) $\psi(e) = e'$
- (ii) $\widetilde{\psi(\hat{a})} = \widetilde{\psi(a)}$ per ogni a

5.3.3 Sottogruppi

Definizione 5.11 (Sottogruppo). Un sottoinsieme $H \subseteq G$ di un gruppo $\langle G; *, \hat{e} \rangle$ è detto **sottogruppo** di G se $\langle H; *, \hat{e} \rangle$ è un gruppo, i.e., se H è chiuso rispetto a tutte le operazioni:

- (i) $a * b \in H$ per ogni $a, b \in H$
- (ii) $e \in H$
- (iii) $\hat{a} \in H$ per ogni $a \in H$

Osservazione 14. Per ogni gruppo con elemento neutro e , esistono sempre i due sottogruppi triviali $\{e\}$ e G stesso.

5.3.4 L'ordine di un gruppo e dei suoi elementi

Definizione 5.12 (Ordine di un elemento). Sia G un gruppo e $a \in G$. L'**ordine** di a , denotato con $\text{ord}(a)$, è il più piccolo $m \geq 1$ tale che $a^m = e$. Se un tale m non esiste, allora è convenzione scrivere $\text{ord}(a) = \infty$

Osservazione 15. Per definizione vale $\text{ord}(e) := 1$. Inoltre, se $\text{ord}(a) = 2$, allora significa che $a^{-1} = a$. Un tale a è un'**involuzione**¹⁶.

Lemma 5.6. In un gruppo finito, ogni elemento ha un'ordine finito.

Dimostrazione. Dal momento che G è finito, dev'essere $a^r = a^s = b$ per qualche $r < s$ e qualche b . Allora $a^{s-r} = a^s \cdot a^{-r} b \cdot b^{-1} = e$ ■

Definizione 5.13 (Ordine di un gruppo). Per un gruppo finito G , $|G|$ è detto **ordine** di G .

¹⁶self-inverse

5.3.5 Gruppi ciclici

Detto G un gruppo e $a \in G$ tale che $\text{ord}(a) < \infty$, allora per ogni $m \in \mathbb{Z}$ vale

$$a^m = a^{R_{\text{ord}(a)}(m)}$$

Definizione 5.14 (Gruppo generato). Per un gruppo G e un elemento $a \in G$, il **gruppo generato da a** , denotato con $\langle a \rangle$ è definito come:

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

Osservazione 16. $\langle a \rangle$ è il più piccolo sottogruppo contenente a . Infatti, per un gruppo finito G , abbiamo:

$$\langle a \rangle = \{e, a, a^2, \dots, a^{\text{ord}(a)-1}\}$$

Definizione 5.15 (Gruppo ciclico). Un gruppo $G = \langle g \rangle$ è detto **ciclico**, e g è detto **generatore** di G .

Osservazione 17. Non tutti i gruppi sono ciclici! Inoltre, un gruppo ciclico può avere più di un generatore. In particolare, se g è un generatore, allora lo è anche g^{-1} .

Osservazione 18. Il gruppo $\langle \mathbb{Z}_n; \oplus_n \rangle$ è ciclico per ogni n , dove 1 è un generatore. Inoltre, i generatori di $\langle \mathbb{Z}_n; \oplus_n \rangle$ sono tutti i $g \in \mathbb{Z}_n$ per cui vale $\gcd(g, n) = 1$.

Teorema 5.7. *Un qualsiasi gruppo ciclico di ordine n è isomorfo a $\langle \mathbb{Z}_n; \oplus_n \rangle$ e quindi è abeliano.*

Dimostrazione. Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n con elemento neutro e . Allora la biezione

$$\mathbb{Z}_n \rightarrow G : i \rightarrow g^i$$

è un isomorfismo, dal momento che $i \oplus j \mapsto g^{i+j} = g^i * g^j$ ■

5.3.7 L'ordine dei sottogruppi

Teorema 5.8 (Lagrange). *Sia G un gruppo finito e sia H un sottogruppo di G . Allora $|H| \mid |G|$.*

I seguenti corollari sono applicazioni dirette del Teorema di Lagrange.

Corollario 5.9. *Per un gruppo finito G , l'ordine di ogni elemento divide l'ordine del gruppo, i.e.,*

$$\text{ord}(a) \mid |G| \quad \forall a \in G$$

Dimostrazione. $\langle a \rangle$ è un sottogruppo di G di ordine $\text{ord}(a)$, che, secondo il Teorema 5.8, deve dividere $|G|$ ■

Corollario 5.10. *Sia G un gruppo finito. Allora $a^{|G|} = e$ per ogni $a \in G$.*

Dimostrazione. Abbiamo $|G| = k \cdot \text{ord}(a)$ per un certo k . Quindi:

$$a^{|G|} = a^{k \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^k = e^k = e$$

■

Corollario 5.11. *Ogni gruppo il cui ordine è un numero primo è ciclico, e in un tale gruppo, ogni elemento eccetto l'elemento neutro è un generatore.*

Dimostrazione. Sia $|G| = p$ per un certo primo p . Per ogni $a \in G$, sappiamo che $\text{ord}(a) \mid p$. Allora deve valere $\text{ord}(a) = 1$ o $\text{ord}(a) = p$. Nel primo caso, $a = e$; nel secondo, $G = \langle a \rangle$. ■

5.3.8 Il gruppo \mathbb{Z}_m^* e la funzione φ di Eulero

Nelle sezioni precedenti abbiamo affermato che $\langle \mathbb{Z}_m; \oplus_m \rangle$ è un gruppo. Tuttavia, lo stesso insieme con la moltiplicazione modulare, \odot_m , non è un gruppo, siccome non tutti gli elementi di \mathbb{Z}_m hanno inverso moltiplicativo (ad es. $8 \in \mathbb{Z}_{12}$ non possiede inverso moltiplicativo in \mathbb{Z}_{12}). Per rendere \mathbb{Z}_m con \odot_m un gruppo, dobbiamo togliere tutti gli elementi che non possiedono inverso moltiplicativo.

Definizione 5.16 (Insieme delle classi resto invertibili modulo m). L'insieme delle classi resto **invertibili** modulo m è definito come:

$$\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$$

Osservazione 19. Per un modulo p primo vale:

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$$

Definizione 5.17 (Funzione di Eulero). La **funzione di Eulero** $\varphi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ è definita come la **cardinalità** di \mathbb{Z}_m^* :

$$\varphi(m) = |\mathbb{Z}_m^*|$$

Osservazione 20. Dall'Osservazione precedente otteniamo immediatamente

$$\varphi(p) = p - 1 \quad (p : \text{primo})$$

Lemma 5.12. *Se la fattorizzazione di m è $m = \prod_{i=1}^r p_i^{e_i}$, allora*

$$\varphi(m) = \prod_{i=1}^r (p_i - 1)p_i^{e_i-1} = \prod_{p \text{ primo } p \mid m} \left(1 - \frac{1}{p}\right)$$

Dimostrazione. Per un primo p e $e \geq 1$ abbiamo

$$\varphi(p^e) = p^{e-1}(p - 1)$$

dal momento che ogni p -esimo intero in \mathbb{Z}_{p^e} contiene un fattore p e quindi i $\varphi(p^e) = p^{e-1}(p - 1)$ non contengono alcun fattore p . Siccome i $p_i^{e_i}$ sono coprimi, il Teorema Cinese del Resto implica che esiste un'iniezione tra gli elementi di \mathbb{Z}_m e le liste (a_1, \dots, a_r) con $a_i \in \mathbb{Z}_{p_i^{e_i}}$. Pertanto, esiste anche un'iniezione tra gli elementi di \mathbb{Z}_m^* e le liste (a_1, \dots, a_r) con $a_i \in \mathbb{Z}_{p_i^{e_i}}^*$. Infine, ci sono $\prod_{i=1}^r (p_i - 1)p_i^{e_i-1}$ liste di questo tipo. ■

Teorema 5.13. $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ è un gruppo.

Dimostrazione. \mathbb{Z}_m^* è chiuso rispetto a \odot , siccome se $\gcd(a, m) = 1$ e $\gcd(b, m) = 1$, allora anche $\gcd(ab, m) = 1$. Questo è vero dal momento che se ab e m hanno un comun divisore > 1 , allora hanno anche un comun divisore primo > 1 , che sarebbe un divisore di a oppure di b , e quindi un comune divisore di a e m o di b e m , il che porta ad una contraddizione.

L'associatività di \odot è ereditata dall'associatività della moltiplicazione in \mathbb{Z} . Inoltre, 1 è elemento neutro e gli inversi esistono (vedi sezione 4.5.3). ■

Corollario 5.14 (Fermat, Eulero). *Per ogni $m \geq 2$ e per ogni a per cui valga $\gcd(a, m) = 1$, vale:*

$$a^{\varphi(m)} \equiv_m 1$$

In particolare, detto p un numero primo, allora per ogni a non divisibile per p :

$$a^{p-1} \equiv_p 1$$

Dimostrazione. La tesi segue direttamente dal Corollario 5.10 per il gruppo \mathbb{Z}_m^* di ordine $\varphi(m)$. ■

5.4 Applicazione: Crittosistema RSA

5.4.1 Radici e -esime in un gruppo

Teorema 5.16. *Sia G un gruppo finito e sia $e \in \mathbb{Z}$ coprimo a $|G|$. La funzione $x \mapsto x^e$ è una biiezione e l'unica radice e -esima di $y \in G$, ossia $x \in G : x^e = y$, è:*

$$x = y^d$$

dove d è l'inverso moltiplicativo di e modulo $|G|$, i.e.:

$$ed \equiv_{|G|} 1$$

Dimostrazione. $(x^e)^d = x^{ed} = x^{k \cdot |G| + 1} = \underbrace{(x^{|G|})^k}_{=1} \cdot x = x$ ■

il che significa che la funzione $y \mapsto y^d$ è l'inversa di quella data sopra.

Quando $|G|$ è conosciuto, allora d può essere calcolato da $ed \equiv_{|G|} 1$ usando l'algoritmo di Euclide esteso. Non è tuttavia conosciuto alcun metodo generale per calcolare le radice e -esime in un gruppo senza conoscere il suo ordine. Questo fatto può essere sfruttato a proprio vantaggio per creare un crittosistema a chiave pubblica.

5.4.2 Descrizione dell'RSA

Sia $n = pq$ un numero intero composto dai due fattori primi p, q sufficientemente grandi. Consideriamo il gruppo \mathbb{Z}_n^* . Mantenuti segreti i due fattori p e q , consideriamo l'ordine di tale gruppo:

$$|\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$$

Il seguente schema mostra un'applicazione *naif* dell'RSA.

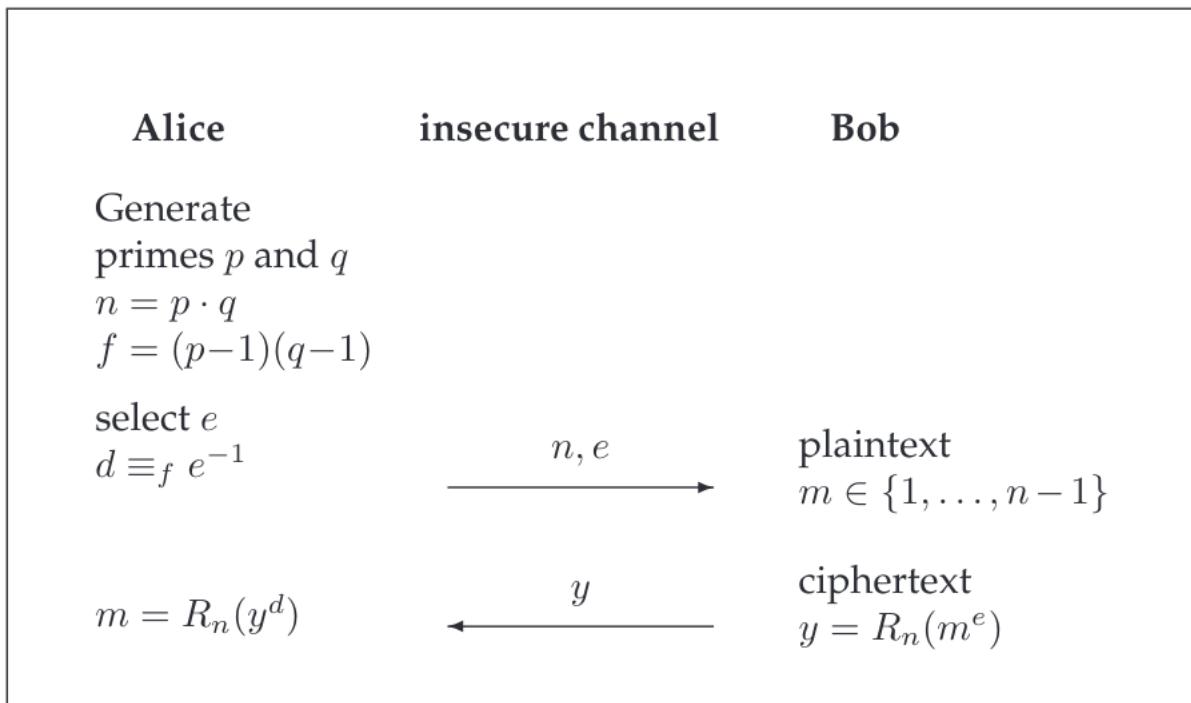


Figure 5.1: The naïve RSA public-key cryptosystem. Alice's public key is the pair (n, e) and her secret key is d . The public key must be sent to Bob via an authenticated channel. Bob can encrypt a message, represented as a number in \mathbb{Z}_n , by raising it to the e th power modulo n . Alice decrypts a ciphertext by raising it to the d th power modulo n .

Notiamo che $\varphi(n)$ può essere calcolato solo se i fattori p, q sono conosciuti. Nello schema sopra, d può essere calcolato secondo

$$ed \equiv_{(p-1)(q-1)} 1$$

5.5 Anelli e campi

5.5.1 Definizione di anello

Definizione 5.18 (Anello). Un **anello** $\langle R; +, -, 0, \cdot, 1 \rangle$ è un'algebra per cui:

- (i) $\langle R; +, -, 0 \rangle$ è un gruppo abeliano
- (ii) $\langle R; \cdot, 1 \rangle$ è un monoide
- (iii) $a(b+c) = (ab) + (ac)$ e $(b+c)a = (ba) + (ca)$, per ogni $a, b, c \in R$ (distributività a sinistra e a destra)

Un anello è detto **commutativo** se la moltiplicazione è commutativa ($ab = ba$).

Esempio 19. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono anelli (commutativi), come pure $\langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle$



Lemma 5.17. Per ogni anello $\langle R; +, -, 0, \cdot, 1 \rangle$ e per ogni $a, b \in R$ valgono le seguenti affermazioni:

- (i) $0a = a0 = 0$
- (ii) $(-a)b = -(ab)$
- (iii) $(-a)(-b) = ab$
- (iv) Se R è **non triviale** (cioè ha più di un elemento), allora $1 \neq 0$.

Dimostrazione. Dimostriamo solo (i).

$$\begin{aligned}
 0 &= -(a0) + a0 && (0 = -b + b \quad \forall b \in R) \\
 &= -(a0) + a(0 + 0) && (0 + 0 = 0) \\
 &= -(a0) + (a0 + a0) && (\text{Distributività}) \\
 &= ((-a0) + a0) + a0 && (\text{Associatività di } +) \\
 &= 0 + a0 && (0 = -b + b \quad \forall b \in R) \\
 &= a0
 \end{aligned}$$



In ogni caso, è mostrato che 0 non possiede inverso moltiplicativo. Pertanto, richiedere che $\langle R; \cdot, 1 \rangle$ sia un gruppo (e non un monoide) non avrebbe alcun senso.

Definizione 5.19 (Caratteristica). La caratteristica di un anello è l'ordine di 1 nel gruppo additivo (se è finito), altrimenti è posta a 0 per definizione.

Esempio 20. La caratteristica dell'anello $\langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle$ è m . La caratteristica di \mathbb{Z} è 0.



5.5.2 Divisori

Per quanto segue, R è un anello commutativo.

Definizione 5.20 (Divisore). Per $a, b \in R$ con $a \neq 0$, diciamo che a **divide** b , scritto $a | b$ se esiste $c \in R$ tale che $b = ac$. In tal caso, a è detto **divisore** di b e b **multiplo** di a .

Lemma 5.18. *In ogni anello commutativo:*

- (i) *La relazione $|$ è transitiva*
- (ii) *Se $a | b$ allora $a | bc$ per ogni c*
- (iii) *Se $a | b$ e $b | c$ allora $a | (b + c)$*

Dimostrazione. Dimostriamo solo (i). $a | b \implies \exists d : (b = ad)$. Inoltre, $b | c \implies \exists e : (c = be)$. Quindi, $c = be = (ad)e = a(de)$, cioè $a | c$ ■

Definizione 5.21 (Massimo comun divisore). Per $a, b \in R$ (non entrambi nulli), un elemento $d \in R$ è detto un **massimo comun divisore** di a e b se d divide a, b e ogni divisore comune di a e b divide d :

$$d | a \wedge d | b \wedge \forall c : ((c | a \wedge c | b) \rightarrow c | d)$$

5.5.3 Unità e gruppo moltiplicativo di un anello

Definizione 5.22 (Unità). Un elemento u di un anello commutativo R è detto **unità** se u è invertibile, i.e., se esiste $v \in R$ tale che $uv = vu = 1$ (si scrive $v = u^{-1}$). L'insieme delle unità di R è denotato con R^* .

Lemma 5.19. *Per un anello R , R^* è un gruppo moltiplicativo.*

Dimostrazione. Dobbiamo mostrare che R^* è chiuso rispetto alla moltiplicazione, i.e., che per ogni $u, v \in R^*$, anche $uv \in R^*$, il che significa che anche uv possiede un inverso. In effetti, l'inverso di (uv) è $(uv)^{-1} = v^{-1}u^{-1}$. R^* contiene anche l'1, inoltre, l'associatività della moltiplicazione è ereditata da R . ■

5.5.4 Divisori di zero e dominio d'integrità

Definizione 5.23 (Divisore di zero). Un elemento $a \neq 0$ di un anello commutativo R è detto **divisore di zero** se $ab = 0$ per un certo $b \neq 0$ in R .

Definizione 5.24 (Dominio d'integrità). Un **dominio d'integrità** è un anello commutativo non-triviale privo di divisori di zero:

$$\forall a \forall b : (ab = 0 \rightarrow a = 0 \wedge b = 0)$$

Esempio 21. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono domini d'integrità; \mathbb{Z}_m lo è solo per m primo.



Lemma 5.20. In un dominio d'integrità, se $a \mid b$, allora il c che soddisfa $b = ac$ è **unico** ed è chiamato **quoziante** (scritto $c = b/a$).

Dimostrazione. Supponiamo che sia $b = ac = ac'$ per $c \neq c'$. Allora

$$0 = ac + (-ac') = a(c + (-c'))$$

e quindi, siccome $a \neq 0$ per ipotesi e non ci sono divisori di zero, dev'essere $c + (-c') = 0$ e pertanto $c = c'$. ■

5.5.5 Anelli di polinomi

Definizione 5.25 (Anello di polinomio). Un polinomio $a(x)$ su un anello R nell'indeterminata x è un'espressione del tipo:

$$a(x) = \sum_{i=0}^d a_i x^i$$

per un certo d intero non-negativo e $a_i \in R$. Il **grado** di $a(x)$, denotato con $\deg(a(x))$ è il valore più grande di i per cui $a_i \neq 0$. Il polinomio nullo $o(x) = 0$ ha grado $\deg(o(x)) := -\infty$. L'insieme $R[x]$ è l'insieme dei polinomi in x con coefficienti in R .

Teorema 5.21. Per ogni anello R , $R[x]$ è pure un anello.

Dimostrazione. Dobbiamo dimostrare le condizioni della Definizione 5.18 per $R[x]$, assumendo che esse siano soddisfatte per R .

- (i) È richiesto che $R[x]$ sia un gruppo abeliano con l'addizione. La condizione è trivialmente soddisfatta, dal momento che la commutatività e l'associatività dell'addizione polinomiale è ereditata da quella fra gli elementi di R . Inoltre, $o(x) = 0$ è l'elemento neutro e l'inverso (additivo) di $a(x)$ è $-a(x) = \sum_{i=0}^d (-a_i)x^i$
- (ii) Qui è richiesto che $R[x]$ sia un monoide con la moltiplicazione. L'elemento neutro è $e(x) = 1$. L'associatività è dimostrabile come segue: sia $c(x) = \sum_{i=0}^{d''} c_i x^i$. Allora vale:

$$(a(x)b(x))c(x) = \sum_{i=0}^{d+d'+d''} \left(\sum_{j=0}^i \left(\sum_{u+v=j} a_u b_v \right) c_{i-j} \right) x^i$$

Se si prova a calcolare $a(x)(b(x)c(x))$ si arriverebbe allo stesso risultato, usando l'associatività in R .

- (iii) La distributività è ereditata da R .



Lemma 5.22.

- (i) Detto D un dominio d'integrità, allora $D[x]$ è pure un dominio di integrità
- (ii) Vale $D[x]^* = D^*$.

5.5.6 Campi

Definizione 5.26 (Campo). Un **campo**¹⁷ è un anello commutativo non triviale F in cui ogni elemento non nullo è un'unità, i.e., $F^* = F \setminus \{0\}$. In altre parole, un anello F è un campo se e solo se $\langle F \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$ è un gruppo abeliano.

Esempio 22. Sono campi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ma non \mathbb{Z} e $R[x]$ per ogni anello R .



Teorema 5.23. \mathbb{Z}_p è un campo se e solo se p è primo.

Dimostrazione. $\mathbb{Z}_p \setminus \{0\}$ è un gruppo moltiplicativo se e solo se p è primo. ■

Osservazione 21. Indicheremo i campi composti da p elementi con $\text{GF}(p)$, dove l'abbreviazione sta per *Galois Field*. Il vantaggio di lavorare con dei campi è che si può dividere per ogni elemento non nullo!

Teorema 5.24. Un campo è un dominio d'integrità.

Dimostrazione. In un campo, ogni elemento non nullo è un'unità, e in un dominio d'integrità, ogni elemento non nullo *non* dev'essere un divisore di zero. Pertanto, è sufficiente provare che in ogni anello commutativo R , un'unità $u \in R$ non è un divisore di zero. Per giungere ad una contraddizione, si assuma $uv = 0$ per un certo v . Allora, dev'essere $v = 0$ siccome:

$$v = 1v = v^{-1}uv = u^{-1}0 = 0$$

e quindi u non è divisore di zero. ■

5.6 Polinomi su un campo

5.6.1 Fattorizzazione e polinomi irriducibili

Definizione 5.27 (Polinomio monico). Un polinomio $a(x) \in F[x]$ si dice **monico** se il coefficiente del termine di grado massimo è 1.

Definizione 5.28 (Polinomio irriducibile). Un polinomio $a(x) \in F[x]$ con $\deg(a(x)) \geq 1$ è detto **irriducibile** se è divisibile solo per polinomi costanti e multipli di $a(x)$ stesso.

Definizione 5.29 (Massimo comun divisore). Il polinomio monico $g(x)$ di grado massimo tale che $g(x) \mid a(x)$ e $g(x) \mid b(x)$ è detto **il massimo comun divisore** di $a(x)$ e $b(x)$, ed è denotato con $\gcd(a(x), b(x))$.

¹⁷DE: *Körper*

5.6.2 Divisibilità in $F[x]$

Teorema 5.25. Sia F un campo. Allora, per ogni $a(x), b(x) \neq 0 \in F[x]$ esiste un polinomio **unico** $q(x)$ (il quoziente) e un polinomio **unico** $r(x)$ (il resto) tali che:

$$a(x) = b(x) \cdot q(x) + r(x) \wedge \deg(r(x)) < \deg(b(x))$$

Dimostrazione. Dimostriamo dapprima l'esistenza di $q(x)$ e $r(x)$ e successivamente l'unicità. Se $\deg(b(x)) > \deg(a(x))$, allora $q(x) = 0$ e $r(x) = a(x)$. Assumiamo pertanto $\deg(b(x)) \leq \deg(a(x))$. Sia $a(x) = a_m x^m + \dots$ e $b(x) = b_n x^n + \dots$ con $n \leq m$. Il primo passo della divisione di polinomi consiste nel sottrarre $a_m b_n^{-1} b(x) x^{m-n}$ da $a(x)$, risultando in un polinomio di grado al massimo $m-1$. Reiterando la divisione di polinomi, si ottengono $q(x)$ e $r(x)$ con $\deg(r(x)) < \deg(b(x))$.

Per dimostrare l'unicità, supponiamo che

$$a(x) = b(x)q(x) + r(x) = b(x)q'(x) + r'(x)$$

dove $\deg(r(x)) < \deg(b(x))$ e $\deg(r'(x)) < \deg(b(x))$. Allora vale:

$$b(x)[q(x) - q'(x)] = r(x) - r'(x)$$

Dal momento che $\deg(r'(x) - r(x)) < \deg(b(x))$, deve valere $q(x) - q'(x) = 0$, ossia $q(x) = q'(x)$, che implica $r(x) = r'(x)$ ■

Osservazione 22. In analogia con la notazione $R_m(a)$ per $a \pmod{m}$, utilizziamo qui la notazione $R_{b(x)}(a(x))$ per $a(x) \pmod{b(x)}$

5.7 Polinomi come funzioni

5.7.2 Radici

Definizione 5.33 (Radice). Sia $a(x) \in R[x]$ (con R : anello). Un elemento $\alpha \in R$ per il quale $a(\alpha) = 0$ è detto **radice**¹⁸ di $a(x)$.

Lemma 5.28. Detto F un campo, $\alpha \in F$ è radice di $a(x)$ se e solo se $(x - \alpha) \mid a(x)$.

Dimostrazione.

Dim. \implies : Assumiamo che α sia radice di $a(x)$, cioè $a(\alpha) = 0$. Allora, grazie al Teorema 5.25, possiamo scrivere $a(x)$ come

$$a(x) = (x - \alpha)q(x) + r(x)$$

dove $\deg(r(x)) < \deg(x - \alpha) = 1$, i.e., $r(x)$ è una costante r :

$$r = a(x) - (x - \alpha)q(x)$$

¹⁸DE: Nullstelle, Wurzel

Inseriamo ora $x = \alpha$ per ottenere

$$r = a(\alpha) - (\alpha - \alpha)q(\alpha) = 0 - 0q(\alpha) = 0$$

Pertanto, $x - \alpha$ divide $a(x)$.

Dim. \Leftarrow : Assumiamo ora che $x - \alpha$ divida $a(x)$, cioè $a(x) = (x - \alpha)q(x)$. Allora $a(\alpha) = (\alpha - \alpha)q(\alpha) = 0$, i.e., α è radice di $a(x)$. ■

Osservazione 23. Il Lemma 5.28 implica che un polinomio irriducibile di grado ≥ 2 non ha radici.

Corollario 5.29. *Un polinomio $a(x)$ di grado 2 o 3 su un campo F è irriducibile se e solo se non ha radici¹⁹.*

Dimostrazione. Un polinomio riducibile di grado 2 o 3 ha un fattore di grado 1 e quindi una radice. Un polinomio irriducibile non ha radici perché, secondo il Lemma 5.28, una tale radice corrisponderebbe a un fattore lineare. ■

Definizione 5.34 (Molteplicità). Se α è una radice di $a(x)$, allora la sua **molteplicità** è la potenza massima di $x - \alpha$ che divide $a(x)$.

Teorema 5.30. *Per un campo F , un polinomio non nullo $a(x) \in F[x]$ di grado d ha al massimo d radici, contate con la loro molteplicità.*

Dimostrazione. Per assurdo. Supponiamo che $a(x)$ abbia grado d ma $e > d$ radici, diciamo $\alpha_1, \dots, \alpha_e$. Allora il polinomio $\prod_{i=1}^e (x - \alpha_i)$ divide $a(x)$. Dal momento che si tratta di un polinomio di grado e , $a(x)$ deve avere grado almeno $e > d$, il che costituisce una contraddizione. ■

5.7.3 Interpolazione polinomiale

Lemma 5.31. *Un polinomio $a(x) \in F[x]$ di grado massimo d è determinato univocamente da $d + 1$ valori qualsiasi di $a(x)$, i.e., da $a(\alpha_1), \dots, a(\alpha_{d+1})$.*

Dimostrazione. Sia $\beta_i = a(\alpha_i)$ per $i = 1, \dots, d+1$. Allora $a(x)$ è dato dalla Formula di Interpolazione di Lagrange:

$$a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$$

dove

$$u_i(x) = \frac{(x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_{i+1}) \cdots (x - \alpha_{d+1})}{(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_{d+1})}$$

¹⁹Nota che questo non vale se $\deg(a(x)) \geq 4!$

5.8 Campi finiti

5.8.1 L'anello $F[x]_{m(x)}$

Così come è possibile calcolare modulo m su \mathbb{Z} , è possibile farlo su $F[x]$:

$$a(x) \equiv_{m(x)} b(x) \Leftrightarrow m(x) \mid (a(x) - b(x))$$

Lemma 5.32. *La congruenza modulo $m(x)$ è una relazione di equivalenza su $F[x]$, e ogni classe di equivalenza possiede un rappresentante univoco di grado $< \deg(m(x))$.*

Definizione 5.35 (Anello dei polinomi su F ridotti modulo $m(x)$). Sia $m(x)$ un polinomio di grado d su F . Allora

$$F[x]_{m(x)} := \{a(x) \in F[x] \mid \deg(a(x)) < d\}$$

Lemma 5.33. *Sia F un campo finito di cardinalità q e sia $m(x)$ un polinomio di grado d su F . Allora, $|F[x]_{m(x)}| = q^d$.*

Dimostrazione. Abbiamo

$$F[x]_{m(x)} = \{a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \mid a_0, \dots, a_{d-1} \in F\}$$

Ci sono q^d scelte per i termini a_i ■

Lemma 5.34. *$F[x]_{m(x)}$ è un anello con l'addizione e la moltiplicazione modulo $m(x)$.*

Dimostrazione. $F[x]_{m(x)}$ è un gruppo con l'addizione polinomiale. L'elemento neutro è il polinomio nullo e l'opposto di $a(x) \in F[x]_{m(x)}$ è $-a(x)$. L'associatività è ereditata da $F[x]$.

Inoltre, $F[x]_{m(x)}$ è un monoide con la moltiplicazione polinomiale. L'elemento neutro è il polinomio 1. L'associatività e distributività sono ereditate da $F[x]$. ■

Lemma 5.35. *L'equazione modulare*

$$a(x)b(x) \equiv_{m(x)} 1$$

ha soluzione $b(x) \in F[x]_{m(x)}$ se e solo se $\gcd(a(x), m(x)) = 1$. Tale soluzione è unica. In altre parole:

$$F[x]_{m(x)}^* = \{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1\}$$

5.8.2 Costruzione dei campi estesi

Teorema 5.36. *L'anello $F[x]_{m(x)}$ è un campo se e solo se $m(x)$ è irriducibile.*

Dimostrazione. Per un polinomio irriducibile $m(x)$, abbiamo $\gcd(a(x), m(x)) = 1$ per ogni $a(x) \neq 0$ con $\deg(a(x)) < \deg(m(x))$ e pertanto, secondo il Lemma 5.35, $a(x)$ è invertibile in $F[x]_{m(x)}$. In altre parole, $F[x]_{m(x)}^* = F[x]_{m(x)} \setminus \{0\}$. Se $m(x)$ non è irriducibile, allora $F[x]_{m(x)}$ non è un campo, poiché i fattori non triviali di $m(x)$ non hanno inverso moltiplicativo. ■

6 Logica

6.2 Sistemi di dimostrazione

6.2.1 Definizione

Definizione 6.1 (Sistema di dimostrazione). Un **sistema di dimostrazione** è una quaterna

$$\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$$

dove:

- $\mathcal{S} \subseteq \Sigma^*$ è un insieme di (rappresentazioni sintattiche di) affermazioni matematiche
- $\mathcal{P} \subseteq \Sigma^*$ è un insieme di (rappresentazioni sintattiche di) dimostrazioni
- τ è la **funzione di verità**, ossia una funzione $\tau : \mathcal{S} \rightarrow \{0, 1\}$ che assegna un valore di verità $\tau(s)$ a un'affermazione $s \in \mathcal{S}$
- ϕ è la **funzione di verifica**, ossia una funzione $\phi : \mathcal{S} \times \mathcal{P} \rightarrow \{0, 1\}$ che restituisce 1 (VERO logico) se e solo se una dimostrazione $p \in \mathcal{P}$ è valida per un'affermazione $s \in \mathcal{S}$.

Definizione 6.2 (Correttezza). Un sistema di dimostrazione si dice **corretto** (*sound*) se nessuna affermazione falsa possiede una dimostrazione.

Definizione 6.3 (Completezza). Un sistema di dimostrazione si dice **completo** se ogni affermazione vera possiede una dimostrazione.

6.2.2 Esempi

Tratti direttamente dallo script (pp. 131-133).

6.2.2 Examples

Example 6.1. An undirected *graph* consists of a set V of nodes and a set E of edges between nodes. Suppose that $V = \{0, \dots, n - 1\}$. A graph can then be described by the so-called *adjacency matrix*, an $n \times n$ -matrix M with $\{0, 1\}$ -entries, where $M_{i,j} = 1$ if and only if there is an edge between nodes i and j . A graph with n nodes can hence be represented by a bit-string of length n^2 , by reading out the entries of the matrix row by row.

We are now interested in proving that a given graph has a so-called *Hamiltonian cycle*, i.e., that there is a closed path from node 1 back to node 1, following edges between nodes, and visiting every node exactly once. We are also interested in the problem of proving the negation of this statement, i.e., that a given graph has *no* Hamiltonian cycle. Deciding whether or not a given graph has a Hamiltonian cycle is considered a computationally very hard decision problem (for large graphs).¹¹

To prove that a graph has a Hamiltonian cycle, one can simply provide the sequence of nodes visited by the cycle. A value in $V = \{0, \dots, n - 1\}$ can be represented by a bit-string of length $\lceil \log_2 n \rceil$, and a sequence of n such numbers can hence be represented by a bit-string of length $n \lceil \log_2 n \rceil$. We can hence define $\mathcal{S} = \mathcal{P} = \{0, 1\}^*$.

Now we can let τ be the function defined by $\tau(s) = 1$ if and only if $|s| = n^2$ for some n and the n^2 bits of s encode the adjacency matrix of a graph containing a Hamiltonian cycle. If $|s|$ is not a square or if s encodes a graph without a Hamiltonian cycle, then $\tau(s) = 0$.¹² Moreover, we can let ϕ be the function defined by $\phi(s, p) = 1$ if and only if, when s is interpreted as an $n \times n$ -matrix M and when p is interpreted as a sequence of n different numbers (a_1, \dots, a_n) with $a_i \in \{0, \dots, n - 1\}$ (each encoded by a bit-string of length $\lceil \log_2 n \rceil$), then the following is true:

$$M_{a_i, a_{i+1}} = 1$$

for $i = 1, \dots, n - 1$ and

$$M_{a_n, a_1} = 1.$$

This function ϕ is efficiently computable. The proof system is sound because a graph without Hamiltonian cycle has no proof, and it is complete because every graph with a Hamiltonian cycle has a proof. Note that each s with $\tau(s) = 1$ has at least n different proofs because the starting point in the cycle is arbitrary.

Example 6.2. Let us now consider the opposite problem of proving the inexistence of a Hamiltonian cycle in a given graph. In other words, in the above example we define $\tau(s) = 1$ if and only if $|s| = n^2$ for some n and the n^2 bits

¹¹The best known algorithm has running time exponential in n . The problem is actually NP-complete, a concept that will be discussed in a later course on theoretical Computer Science.

¹²Note that τ defines the meaning of the strings in \mathcal{S} , namely that they are meant to encode graphs and that we are interested in whether a given graph has a Hamiltonian cycle.

of s encode the adjacency matrix of a graph *not* containing Hamiltonian cycle. In this case, no sound and complete proof system (with reasonably short and efficiently verifiable proofs) is known. It is believed that no such proof system exists.

Example 6.3. Let again $\mathcal{S} = \mathcal{P} = \{0, 1\}^*$, and for $s \in \{0, 1\}^*$ let $n(s)$ denote the natural number whose (standard) binary representation is s , with the convention that leading 0's are ignored. (For example, $n(101011) = 43$ and $n(00101) = 5$.) Now, let τ be the function defined as follows: $\tau(s) = 1$ if and only if $n(s)$ is *not* a prime number. Moreover, let ϕ be the function defined by $\phi(s, p) = 1$ if and only if $n(s) = 0$, or if $n(s) = 1$, or if $n(p)$ divides $n(s)$ and $1 < n(p) < n(s)$. This function ϕ is efficiently computable. This is a proof system for the non-primality (i.e., compositeness) of natural numbers. It is sound because every s corresponding to a prime number $n(s)$ has no proof since $n(s) \neq 0$ and $n(s) \neq 1$ and $n(s)$ has no divisor d satisfying $1 < d < n(s)$. The proof system is complete because every natural number n greater than 1 is either prime or has a prime factor q satisfying $1 < q < n$ (whose binary representation can serve as a proof).

Example 6.4. Let us consider the opposite problem, i.e., proving primality of a number $n(s)$ represented by s . In other words, in the previous example we replace “not a prime” by “a prime”. It is far from clear how one can define a verification function ϕ such that the proof system is sound and complete. However, such an efficiently computable function ϕ indeed exists. Very briefly, the proof that a number $n(s)$ (henceforth we simply write n) is prime consists of (adequate representations of):

- 1) the list p_1, \dots, p_k of distinct prime factors of $n - 1$,
- 2) a (recursive) proof of primality for each of p_1, \dots, p_k ¹³
- 3) a generator g of the group \mathbb{Z}_n^* .

The exact representation of these three parts of the proof would have to be made precise, but we omit this here as it is obvious how this could be done.

The verification of a proof (i.e., the computation of the function ϕ) works as follows.

- If $n = 2$ or $n = 3$, then the verification stops and returns 1.¹⁴
- It is tested whether p_1, \dots, p_k all divide $n - 1$ and whether $n - 1$ can be written as a product of powers of p_1, \dots, p_k (i.e., whether $n - 1$ contains no other prime factor).

¹³recursive means that the same principle is applied to prove the primality of every p_i , and again for every prime factor of $p_i - 1$, etc.

¹⁴One could also consider a longer list of small primes for which no recursive primality proof is required.

- It is verified that

$$g^{n-1} \equiv_n 1$$

and, for all $i \in \{1, \dots, k\}$, that

$$g^{(n-1)/p_i} \not\equiv_n 1.$$

(This means that g has order $n - 1$ in \mathbb{Z}_n^*).

- For every p_i , an analogous proof of its primality is verified (recursively).

This proof system for primality is sound because if n is not a prime, then there is no element of \mathbb{Z}_n^* of order $n - 1$ since the order of any element is at most $\varphi(n)$, which is smaller than $n - 1$. The proof system is complete because if n is prime, then $GF(n)$ is a finite field and the multiplicative group of any finite field, i.e., \mathbb{Z}_n^* , is cyclic and has a generator g . (We did not prove this statement in this course.)¹⁵

6.3 Concetti generali di Logica

6.3.1 Obiettivo della Logica

Un obiettivo della Logica è di fornire un sistema di dimostrazione $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ per cui un grande numero di affermazioni matematiche possa essere espresso come elemento di \mathcal{S} .

6.3.2 Sintassi, semantica, interpretazione e modello

Una logica è completamente definita dalla sua sintassi e dalla sua semantica. Il concetto di base è quello di *formula*.

Definizione 6.4 (Sintassi). La **sintassi** di una logica definisce un alfabeto Λ (di simboli ammessi) e specifica quali stringhe in Λ^* sono effettivamente delle **formule** (cioè sono sintatticamente corrette).

Definizione 6.5 (Semantica). La **semantica** di una logica definisce una funzione *free* che assegna ad ogni formula $F = (f_1, \dots, f_k) \in \Lambda^*$ un sottoinsieme $\text{free}(F) \subseteq \{1, \dots, k\}$ di indici. Se l'indice $i \in \text{free}(k)$, allora si dice che il simbolo f_i è **libero** in F .

Esempio 23.

- In logica proposizionale ogni letterale A, B, \dots è libero.
- In logica predicativa, è libera ogni variabile che non è vincolata da un quantificatore.



Definizione 6.6 (Interpretazione). Un'**interpretazione** consiste di:

- un insieme $\mathcal{Z} \subseteq \Lambda$ di simboli di Λ
- un dominio, i.e., un insieme di possibili valori per ogni simbolo in \mathcal{Z}
- una funzione che assegna ad ogni simbolo in \mathcal{Z} un valore nel suo dominio associato.

Definizione 6.7 (Interpretazione adatta). Un'interpretazione è detta **adatta**²⁰ per una formula F se assegna un valore a tutti i simboli $\beta \in \Lambda$ che sono liberi in F .

Definizione 6.8 (Valore di verità). La semantica di una logica definisce pure una funzione σ che assegna ad ogni formula F e ad ogni interpretazione adatta \mathcal{A} un **valore di verità** $\sigma(F, \mathcal{A})$ in $\{0, 1\}$. Spesso si scrive $\mathcal{A}(F)$ in luogo di $\sigma(F, \mathcal{A})$.

Definizione 6.9 (Modello). Un'interpretazione adatta \mathcal{A} per cui una formula F è vera (i.e., $\mathcal{A}(F) = 1$) è detta **modello** per F e si scrive

$$\mathcal{A} \models F$$

Tale definizione può essere estesa per un insieme M di formule. La relazione negata è data da $\not\models$.

²⁰DE: *passend*, EN: *suitable*

6.3.4 Soddisfabilità, tautologia, conseguenza, equivalenza

Definizione 6.10 (Soddisfabilità). Una formula F (o un insieme M di formule) è detta **soddisfabile** se esiste un modello per F (o M), e **insoddisfabile** altrimenti. Una formula insoddisfabile viene indicata con \perp . **Nota:** Il fatto che un insieme M di formule sia soddisfabile *non* è equivalente al fatto che ogni formula in M sia soddisfabile.

Definizione 6.11 (Tautologia). Una formula F è detta **tautologia** se è vera per ogni interpretazione adatta. Una tautologia è denotata dal simbolo \top oppure $\models F$.

Definizione 6.12 (Conseguenza logica). Una formula G è detta **conseguenza logica** di una formula F (o di un insieme di formule M), scritto

$$F \models G \quad (\text{o } M \models G)$$

se ogni interpretazione adatta sia ad F (o M) sia a G che è un modello per F (o M) è anche un modello per G .

Definizione 6.13 (Equivalenza). Due formule F e G si dicono **equivalenti**, denotato con $F \equiv G$, se ogni interpretazione adatta sia per F che per G produce gli stessi valori di verità per F, G , i.e., l'una è la logica conseguenza dell'altra (e viceversa):

$$F \equiv G \Leftrightarrow F \models G \text{ e } G \models F$$

Osservazione 24. Un insieme M di formule può venir interpretato come la congiunzione (E logico) di tutte le formule in esso contenute, dal momento che un'interpretazione è un modello per M solo se lo è per ogni formula in M . Inoltre, per definizione, l'insieme vuoto corrisponde ad una tautologia.

6.3.5 Gli operatori logici \wedge, \vee e \neg

Definizione 6.15. Se F e G sono formule, allora lo sono anche $\neg F$, $(F \wedge G)$ e $(F \vee G)$.

Definizione 6.16.

$$\begin{aligned} \mathcal{A}((F \wedge G) = 1 &\quad \text{se e solo se } \mathcal{A}(F) = 1 \text{ e } \mathcal{A}(G) = 1 \\ \mathcal{A}((F \vee G) = 1 &\quad \text{se e solo se } \mathcal{A}(F) = 1 \text{ o } \mathcal{A}(G) = 1 \\ \mathcal{A}(\neg F) = 1 &\quad \text{se e solo se } \mathcal{A}(F) = 0 \end{aligned}$$

Lemma 6.1 (Regole di calcolo). *Dette F, G, H formule logiche, valgono le seguenti regole di calcolo:*

- (1) **Idempotenza:** $F \wedge F \equiv F$; $F \vee F \equiv F$.
- (2) **Commutatività di \wedge e \vee :** $F \wedge G \equiv G \wedge F$; $F \vee G \equiv G \vee F$
- (3) **Associatività:** $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$; $(F \vee G) \vee H \equiv F \vee (G \vee H)$
- (4) **Assorbimento:** $F \wedge (F \vee G) \equiv F$; $F \vee (F \wedge G) \equiv F$
- (5) **Distributività I:** $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$

- (6) **Distributività II:** $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
- (7) **Doppia negazione:** $\neg(\neg F) \equiv F$
- (8) **Leggi di De Morgan:** $\neg(F \wedge G) \equiv \neg F \vee \neg G$; $\neg(F \vee G) \equiv \neg F \wedge \neg G$
- (9) **Regole di tautologia:** $F \vee \top \equiv \top$; $F \wedge \top \equiv F$
- (10) **Regole di insoddisfabilità:** $F \vee \perp \equiv F$; $F \wedge \perp \equiv \perp$
- (11) **Verum e falsum:** $F \vee \neg F \equiv \top$; $F \wedge \neg F \equiv \perp$

Dimostrazione. La dimostrazione segue direttamente dalla Def. 6.16. ■

6.3.6 Conseguenza logica vs. insoddisfabilità

Lemma 6.2. Una formula F è una tautologia se e solo se $\neg F$ è insoddisfabile.

Lemma 6.3. Le seguenti tre affermazioni sono equivalenti:

- (1) $\{F_1, \dots, F_k\} \models G$
- (2) $(F_1 \wedge \dots \wedge F_k) \rightarrow G$ è una tautologia
- (3) $\{F_1, \dots, F_k, \neg G\}$ è insoddisfabile

6.4 Calcoli logici

6.4.2 Sistema di Hilbert (*Hilbert-Style Calculi*)

Definizione 6.17 (Regola di derivazione). Una **regola di derivazione** è una regola per derivare una formula da un insieme di formule. Si scrive

$$\{F_1, \dots, F_k\} \vdash_R G$$

se G può esser derivata dall'insieme $\{F_1, \dots, F_k\}$ usando la regola R . Una notazione alternativa è:

$$\frac{F_1 \quad F_2 \cdots F_k}{G} \quad (R)$$

Definizione 6.19 (Calcolo logico). Un **calcolo logico** K è un insieme finito di regole di derivazione: $K = \{R_1, \dots, R_m\}$.

Definizione 6.20 (Derivazione). Una **derivazione** di una formula G da un insieme M di formule è una sequenza finita (di lunghezza n) di applicazione delle regole di derivazione di K che conduce a G . Più precisamente abbiamo:

- $M_0 := M$,

- $M_i := M_{i-1} \cup \{G_i\}$ per $1 \leq i \leq n$ dove $N \vdash_{R_j} G_i$ per un qualche $N \subseteq M_{i-1}$ e per qualche $R_j \in K$ e dove
- $G_n = G$

Scriviamo

$$M \vdash_K G$$

se esiste in K una derivazione di G da M .

Definizione 6.21 (Correttezza di una regola di derivazione). Una regola di derivazione R si dice **corretta** se per ogni insieme M di formule e per ogni formula F , $M \vdash_R F$ implica $M \models F$.

Definizione 6.22 (Correttezza e completezza di un calcolo logico). Un calcolo logico K si dice **corretto** (*sound*) se per ogni insieme M di formule e per ogni formula F , vale che se F può essere derivata da M , allora F è anche una conseguenza logica di M :

$$M \vdash_K F \implies M \models F$$

Il calcolo si dice **completo** se per ogni M e F , vale che se F è logica conseguenza di M , allora F può essere derivata da M :

$$M \models F \implies M \vdash_K F$$

Un calcolo è quindi corretto e completo se

$$M \vdash_K F \Leftrightarrow M \models F$$

i.e., se conseguenza logica e derivabilità sono la stessa cosa.

6.4.3 Derivazioni dalle assunzioni

Un modo naturale di dimostrare $F \rightarrow G$ è assumere la veridicità di F e derivare G usando un calcolo logico.

Lemma 6.4. Se $\{F_1, \dots, F_k\} \vdash_K$ è vero per un calcolo corretto, allora

$$\models ((F_1 \wedge \dots \wedge F_k) \rightarrow G)$$

6.5 Logica proposizionale

6.5.1 Sintassi

Definizione 6.23 (Sintassi). Una **formula atomica** è della forma A_i con $i \in \mathbb{N}$. Una formula è definita come segue:

- Una formula atomica è una formula
- Vale la Def. 6.15.

6.5.2 Semantica

Definizione 6.24 (Semantica). Per un insieme Z di formule atomiche, un'interpretazione \mathcal{A} , detta **assegnazione di verità**, è una funzione $\mathcal{A} : Z \rightarrow \{0, 1\}$. Un'assegnazione di verità \mathcal{A} è adatta per una formula F se Z contiene tutte le formule atomiche che appaiono in F . La **semantica** (i.e., il valore di verità $\mathcal{A}(F)$ di una formula F sotto un'interpretazione \mathcal{A}) è definito come $\mathcal{A}(F) = \mathcal{A}(A_i)$ per ogni formula atomica $F = A_i$. Vale inoltre la Def. 6.16.

6.5.4 Forme normali

Definizione 6.25 (Letterale). Un **letterale** è una formula atomica o la negazione di una formula atomica.

Definizione 6.26 (CNF). Una formula F è in **CNF** (*conjunctive normal form*) se è della forma

$$(L_{11} \vee \cdots \vee L_{1m_1}) \wedge \cdots \wedge (L_{n1} \vee \cdots \vee L_{nm_n})$$

per qualche letterale L_{ij} .

Definizione 6.27 (DNF). Una formula F è in **DNF** (*disjunctive normal form*) se è della forma

$$(L_{11} \wedge \cdots \wedge L_{1m_1}) \vee \cdots \vee (L_{n1} \wedge \cdots \wedge L_{nm_n})$$

per qualche letterale L_{ij} .

Teorema 6.5. *Ogni formula è equivalente a una formula in CNF e ad una in DNF.*

Dimostrazione. Si consideri una formula F composta di n letterali, con una tavola di verità di ordine 2^n . Si può usare la tavola di verità per derivare una formula equivalente in DNF come segue. Per ogni riga della tavola valutata 1, si prende la congiunzione (\wedge) degli n letterali definiti come segue: se $A_i = 0$, allora si prende $\neg A_i$, altrimenti si prende A_i stesso. In seguito, si effettua la disgiunzione (\vee) di tutte le congiunzioni trovate prima.

Per derivare da F una formula in CNF, si procede come segue. Per ogni riga della tavola valutata a 0, si prende la disgiunzione (\vee) degli n letterali così definiti: se $A_i = 0$, si prende A_i , altrimenti $\neg A_i$. In seguito, si prende la congiunzione (\wedge) di tutte le disgiunzioni trovate prima. ■

Esempio 24. Si consideri la formula $F = (A \wedge \neg B) \vee (B \wedge \neg C)$. La sua tavola di verità è:

A	B	C	$(A \wedge \neg B) \vee (B \wedge \neg C)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

La sua forma DNF è:

$$F \equiv (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$$

La sua forma CNF è:

$$F \equiv (A \vee B \vee C) \wedge (A \vee B \vee \neg C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C)$$



6.5.6 Il calcolo risolutivo

Definizione 6.28 (Proposizione). Una **proposizione**²¹ è un insieme di letterali.

Definizione 6.29 (Proposizioni associate ad una formula). L'insieme delle proposizioni associato ad una formula

$$F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})$$

in CNF è l'insieme

$$\mathcal{K}(F) := \{\{L_{11}, \dots, L_{1m_1}\}, \dots, \{L_{n1}, \dots, L_{nm_n}\}\}$$

L'insieme associato ad un insieme $M = \{F_1, \dots, F_k\}$ di formule è l'unione dei singoli insiemi di proposizioni:

$$\mathcal{K}(M) := \bigcup_{i=1}^k \mathcal{K}(F_i)$$

Definizione 6.30 (Risolvente). Una proposizione K è detta **risolvente** delle proposizioni K_1, K_2 se esiste un letterale L tale che $L \in K_1, \neg L \in K_2$ e

$$K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$$

Osservazione 25. È importante notare che i passi di risoluzioni devono essere compiuti **uno ad uno**. Se si compiono due o più passaggi alla volta, si può giungere a risultati errati.

Dato un insieme \mathcal{K} di proposizioni, un passaggio risolutivo prende due proposizioni K_1, K_2 , calcola un risolvente K e aggiunge K a \mathcal{K} :

$$\{K_1, K_2\} \vdash_{\text{res}} K$$

Il calcolo risolutivo, denotato con **Res**, è composto di una sola regola:

$$\text{Res} = \{\text{res}\}$$

Lemma 6.6. *Il calcolo risolutivo è corretto, i.e., se $\mathcal{K} \vdash_{\text{Res}} K$ allora $\mathcal{K} \models K$*

²¹EN: clause

Proof. We only need to show that the resolution rule is correct, i.e., that if K is a resolvent of clauses $K_1, K_2 \in \mathcal{K}$, then K is logical consequence of $\{K_1, K_2\}$, i.e.,

$$\{K_1, K_2\} \vdash_{\text{res}} K \implies \{K_1, K_2\} \models K.$$

Let \mathcal{A} be an arbitrary truth assignment suitable for $\{K_1, K_2\}$ (and hence also for K). Recall that \mathcal{A} is a model for $\{K_1, K_2\}$ if and only if \mathcal{A} makes at least one literal in K_1 true and also makes at least one literal in K_2 true.

We refer to Definition 6.30 and distinguish two cases. If $\mathcal{A}(L) = 1$, then \mathcal{A} makes at least one literal in $K_2 \setminus \{\neg L\}$ true (since $\neg L$ is false). Similarly, if $\mathcal{A}(L) = 0$, then \mathcal{A} makes at least one literal in $K_1 \setminus \{L\}$ true (since L is false). Because one of the two cases occurs, \mathcal{A} makes at least one literal in $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$ true, which means that \mathcal{A} is a model for K . \square

Teorema 6.7. *Un insieme M di formule è insoddisfacibile se e solo se $\mathcal{K}(M) \vdash_{\text{Res}} \emptyset$.*

Proof. The “if” part (soundness) follows from Lemma 6.6: If $\mathcal{K}(M) \vdash_{\text{Res}} \emptyset$, then $\mathcal{K}(M) \models \emptyset$, i.e., every model for $\mathcal{K}(M)$ is a model for \emptyset . Since \emptyset has no model, $\mathcal{K}(M)$ also does not have a model. This means that $\mathcal{K}(M)$ is unsatisfiable.

It remains to prove the “only if” part (completeness with respect to unsatisfiability). We need to show that if a clause set \mathcal{K} is unsatisfiable, then \emptyset can be derived by some sequence of resolution steps. The proof is by induction over the number n of atomic formulas appearing in \mathcal{K} . The induction basis (for $n = 1$) is as follows. A clause set \mathcal{K} involving only literals A_1 and $\neg A_1$ is unsatisfiable if and only if it contains the clauses $\{A_1\}$ and $\{\neg A_1\}$. One can derive \emptyset exactly if this is the case.

For the induction step, suppose that for every clause set \mathcal{K}' with n atomic formulas, \mathcal{K}' is unsatisfiable if and only if $\mathcal{K}' \vdash_{\text{Res}} \emptyset$. Given an arbitrary

clause set \mathcal{K} for the atomic formulas A_1, \dots, A_{n+1} , define the two clause sets \mathcal{K}_0 and \mathcal{K}_1 as follows. \mathcal{K}_0 is the clause set for atomic formulas A_1, \dots, A_n obtained from \mathcal{K} by setting $A_{n+1} = 0$, i.e.,

- by eliminating all clauses from \mathcal{K} containing $\neg A_{n+1}$ (which are satisfied since $\neg A_{n+1} = 1$), and
- by eliminating from each remaining clause the literal A_{n+1} if it appears in it (since having A_{n+1} in it can not contribute to the clause being satisfied).

\mathcal{K} is satisfiable under the constraint $A_{n+1} = 0$ if and only if \mathcal{K}_0 is satisfiable.

Analogously, \mathcal{K}_1 is obtained from \mathcal{K} by eliminating all clauses containing A_{n+1} and by eliminating from each remaining clause the literal $\neg A_{n+1}$ if it appears in it. \mathcal{K} is satisfiable under the constraint $A_{n+1} = 1$ if and only if \mathcal{K}_1 is satisfiable.

If \mathcal{K} is unsatisfiable, it is unsatisfiable both for $A_{n+1} = 0$ and for $A_{n+1} = 1$, i.e., both \mathcal{K}_0 and \mathcal{K}_1 are unsatisfiable. Therefore, by the induction hypothesis, we have $\mathcal{K}_0 \vdash_{\text{Res}} \emptyset$ and $\mathcal{K}_1 \vdash_{\text{Res}} \emptyset$. Now imagine that the same resolution steps leading from \mathcal{K}_0 to \emptyset are carried out on \mathcal{K} , i.e., with A_{n+1} . This derivation may or may not involve clauses (of \mathcal{K}) that contain A_{n+1} . In the latter case (i.e., A_{n+1} not contained), the derivation of \emptyset from \mathcal{K}_0 is also a derivation of \emptyset from \mathcal{K} , and in the other case it corresponds to a derivation of $\{A_{n+1}\}$ from \mathcal{K} .

Analogously, the derivation of \emptyset from \mathcal{K}_1 corresponds to a derivation of \emptyset from \mathcal{K} or to a derivation of $\{\neg A_{n+1}\}$ from \mathcal{K} .

If in any of the two cases we have a derivation of \emptyset from \mathcal{K} , we are done (since \emptyset can be derived from \mathcal{K} , i.e., $\mathcal{K} \vdash_{\text{Res}} \emptyset$). If this is not the case, then we have a derivation of $\{A_{n+1}\}$ from \mathcal{K} , i.e., $\mathcal{K} \vdash_{\text{Res}} \{A_{n+1}\}$ as well as a derivation of $\{\neg A_{n+1}\}$ from \mathcal{K} , i.e., $\mathcal{K} \vdash_{\text{Res}} \{\neg A_{n+1}\}$. From these two clauses one can derive \emptyset by a final resolution step. This completes the proof. \square

6.6 Logica predicativa

6.6.1 Sintassi

Definizione 6.31 (Sintassi).

- Un **simbolo di variabile** ha la forma x_i con $i \in \mathbb{N}$
- Un **simbolo di funzione** è della forma $f_i^{(k)}$ dove $k \in \mathbb{N}$ è l'arità della funzione.
- Un **simbolo di predicato** ha la forma $P_i^{(k)}$ dove k è l'arità del predicato
- Un **termine** è definito per induzione: una variabile è un termine e se t_1, \dots, t_k sono termini, allora $f_i^{(k)}(t_1, \dots, t_k)$ è un termine.

- Una **formula** è definita per induzione:

- Per ogni i, k , se t_1, \dots, t_k sono termini, allora $P_i^{(k)}(t_1, \dots, t_k)$ è una formula, detta formula atomica
- Se F, G sono formule, vale la Def. 6.15.
- Se F è una formula, allora, per ogni i , $\forall x_i F$ e $\exists x_i F$ sono formule.

6.6.2 Variabili libere e sostituzione

Definizione 6.32. Ogni occorrenza di una variabile in una formula è libera o legata. Se una variabile x appare in una (sotto-)formula $\forall x$ o $\exists x$, allora è legata, altrimenti è libera. Una formula è **chiusa** se non ha variabili libere.

Definizione 6.33 (Sostituzione). Per una formula F , una variabile x e un termine t , $F[x/t]$ denota la formula ottenuta sostituendo ogni occorrenza libera di x con t in F .

6.6.3 Semantica

Definizione 6.34 (Interpretazione). Un'interpretazione è una quaterna $\mathcal{A} = (U, \phi, \psi, \xi)$ dove:

- U è un insieme non vuoto, detto **universo**
- ϕ è una funzione che assegna, ad ogni simbolo di funzione, una funzione, dove per un simbolo funzionale k -ario f , $\phi(f) : U^k \rightarrow U$
- ψ è una funzione che assegna ad ogni simbolo di predicato una funzione, dove per un predicato k -ario P , $\psi(P) : U^k \rightarrow \{0, 1\}$
- ξ è una funzione che associa ad ogni simbolo di variabile un valore in U .

La notazione può essere snellita come segue: per un'interpretazione $\mathcal{A} = (U, \phi, \psi, \xi)$ vale:

- $f^{\mathcal{A}}$ in luogo di $\phi(f)$
- $P^{\mathcal{A}}$ in luogo di $\psi(P)$
- $x^{\mathcal{A}}$ in luogo di $\xi(x)$
- $U^{\mathcal{A}}$ per rendere \mathcal{A} esplicita.

Definizione 6.35. Un'interpretazione \mathcal{A} è detta **adatta** per una formula F se definisce tutti i simboli funzionali, i simboli di predicato e le variabili libere in F

Definizione 6.36. Per un'interpretazione $\mathcal{A} = (U, \phi, \psi, \xi)$ definiamo il valore (in U) dei termini e i valori di verità delle formule come segue:

- Il valore $\mathcal{A}(t)$ di un termine t è definito ricorsivamente come segue:

- Se t è una variabile, cioè $t = x_i$, allora $\mathcal{A}(t) = \xi(x_i)$
- Se t è della forma $f(t_1, \dots, t_k)$, allora $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$
- Il valore di verità di una formula F è definito ricorsivamente dalla Def. 6.16 e
 - Se F è della forma $F = P(t_1, \dots, t_k)$, allora $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$
 - Se F è della forma $\forall x G$ o $\exists x G$, allora sia $\mathcal{A}_{[x \rightarrow u]}$ per $u \in U$ la stessa interpretazione \mathcal{A} ma con $\xi(x) = u$:

$$\mathcal{A}(\forall x G) = \begin{cases} 1 & \text{se } \mathcal{A}_{[x \rightarrow u]}(G) = 1 \text{ per ogni } u \in U \\ 0 & \text{altrimenti} \end{cases}$$

$$\mathcal{A}(\exists x G) = \begin{cases} 1 & \text{se } \mathcal{A}_{[x \rightarrow u]}(G) = 1 \text{ per qualche } u \in U \\ 0 & \text{altrimenti} \end{cases}$$

6.6.4 Logica predicativa con uguaglianza

Dalle definizioni date, si evince che il simbolo di uguaglianza “=” non è permesso. Ossia, per esempio, $\exists x f(x) = g(x)$ non è una formula. È tuttavia possibile estendere sintassi e semantica per includere “=” con il suo significato usuale.

6.6.5 Alcune equivalenze riguardanti i quantificatori

Lemma 6.8. *For any formulas F , G , and H , where x does not occur free in H , we have*

- 1) $\neg(\forall x F) \equiv \exists x \neg F;$
- 2) $\neg(\exists x F) \equiv \forall x \neg F;$
- 3) $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G);$
- 4) $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G);$
- 5) $\forall x \forall y F \equiv \forall y \forall x F;$
- 6) $\exists x \exists y F \equiv \exists y \exists x F;$
- 7) $(\forall x F) \wedge H \equiv \forall x (F \wedge H);$
- 8) $(\forall x F) \vee H \equiv \forall x (F \vee H);$
- 9) $(\exists x F) \wedge H \equiv \exists x (F \wedge H);$
- 10) $(\exists x F) \vee H \equiv \exists x (F \vee H).$

Lemma 6.9. *Se si sostituisce una sottoformula G di una formula F con una formula H equivalente a G , allora la formula risultante è equivalente a F .*

6.6.7 Instanziazione universale

Lemma 6.10. *Per ogni formula F e termine t , vale:*

$$\forall x F \models F[x/t]$$

6.6.8 Forme normali

Definizione 6.37 (Forma prenessa). Una formula della forma

$$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n G$$

dove Q_i sono dei quantificatori e G una formula priva di quantificatori, si dice **in forma prenessa**²²

Teorema 6.11. *Per ogni formula ne esiste una equivalente in forma prenessa.*

6.6.9 Un teorema e le sue interpretazioni

Sia dato il seguente

Teorema 6.12.

$$\neg \exists x \forall y (P(y, x) \leftrightarrow \neg P(y, y))$$

²²EN: *prenex form*

Recall that the statement of the theorem means that the formula $\neg\exists x \forall y (P(y, x) \leftrightarrow \neg P(y, y))$ is a tautology, i.e., true for any suitable structure, i.e., for any universe and any choice of the predicate P .

Proof. We can transform the formula by equivalence transformations:

$$\begin{aligned} \neg\exists x \forall y (P(y, x) \leftrightarrow \neg P(y, y)) &\equiv \forall x \neg\forall y (P(y, x) \leftrightarrow \neg P(y, y)) \\ &\equiv \forall x \exists y \neg(P(y, x) \leftrightarrow \neg P(y, y)) \\ &\equiv \forall x \exists y (P(y, x) \leftrightarrow P(y, y)), \end{aligned}$$

where we have made use of $\neg(F \leftrightarrow \neg G) \equiv (F \leftrightarrow G)$, which is easily checked to hold by comparing the truth tables of $\neg(A \leftrightarrow \neg B)$ and $(A \leftrightarrow B)$

To see that the latter formula (i.e., $\forall x \exists y (P(y, x) \leftrightarrow P(y, y))$) is a tautology, let \mathcal{A} be an arbitrary suitable interpretation, which defines the universe $U^{\mathcal{A}}$ and the predicate $P^{\mathcal{A}}$. Below we omit the superscripts \mathcal{A} and write simply U and P . Since \mathcal{A} is arbitrary, it suffices to show that

$$\mathcal{A}(\forall x \exists y (P(y, x) \leftrightarrow P(y, y))) = 1.$$

This can be shown as follows: For every $u \in U$ we have

$$\mathcal{A}(P(u, u) \leftrightarrow P(u, u)) = 1.$$

Hence for every $u \in U$ we have

$$\mathcal{A}_{[x \rightarrow u][y \rightarrow u]}(P(y, x) \leftrightarrow P(y, y)) = 1,$$

and therefore for every fixed $u \in U$ we have

$$\mathcal{A}_{[x \rightarrow u]}(\exists y P(y, x) \leftrightarrow P(y, y)) = 1,$$

and therefore we have

$$\mathcal{A}(\forall x \exists y P(y, x) \leftrightarrow P(y, y)) = 1,$$

as was to be shown. □

Let us now interpret Theorem 6.13. We can instantiate it for different universes and predicates. The first interpretation is Russel's paradox:

Corollary 6.14. *There exists no set that contains all sets S that do not contain themselves, i.e., $\{S \mid S \notin S\}$ is not a set.*

Proof. We consider the universe of all sets⁵⁹ and, to be consistent with the chapter on set theory, use the variable names R instead of x and S instead of y .⁶⁰

⁵⁹The universe of all sets is not a set itself. Formally, the universe in predicate logic need not be a set (in the sense of set theory), it can be a “collection” of objects.

⁶⁰The particular variable names (R and S) are not relevant and are chosen simply to be compatible with the chapter on set theory where sets were denoted by capital letters and Russel's proposed set was called R . Here we have deviated from the convention to use only small letters for variables.

Moreover, we consider the specific predicate P defined as $P(S, R) = 1$ if and only if $S \in R$. Then Theorem 6.13 specializes to

$$\neg \exists R \forall S (S \in R \leftrightarrow S \notin S).$$

This formula states that there is no set R such that for a set (say S) to be in R is equivalent to not being contained in itself ($S \notin S$). \square

It is interesting to observe that Russell's paradox is a fact that holds more generally than in the universe of sets and where $P(x, y)$ is defined as $x \in y$. We state another corollary:

Example 6.23. The reader can investigate as an exercise that Theorem 6.13 also explains the so-called barber paradox (e.g. see Wikipedia) which considers a town with a single barber as well as the set of men that do not shave themselves.

The following corollary was already stated as Theorem 3.21.

Corollary 6.15. *The set $\{0, 1\}^\infty$ is uncountable.*

We prove the equivalent statement: Every enumeration of elements of $\{0, 1\}^\infty$ does not contain all elements of $\{0, 1\}^\infty$.

Proof. We consider the universe \mathbb{N} and a fixed enumeration of elements of $\{0, 1\}^\infty$, and we interpret $P(y, x)$ as the y th bit of the x th sequence of the enumeration. Then Theorem 6.13, $\neg \exists x \forall y (P(y, x) \leftrightarrow \neg P(y, y))$, states that there exists no index x , i.e., no sequence in the enumeration, such that for all y , the y th bit on that sequence is equal to the negation of the y th bit on the y th sequence. But the sequence given by $y \mapsto \neg P(y, y)$ is a well-defined sequence in $\{0, 1\}^\infty$, and we just proved that it does not occur in the enumeration. \square

Note that the proof of this corollary contains Cantor's diagonalization argument, which is hence implicit in Theorem 6.13.

We discuss a further use of the theorem. If we understand a program as describable by a finite bit-string, or, equivalently, a natural number (since there is a bijection between finite bit-strings and natural numbers), and if we consider programs that take a natural number as input and output 0 or 1, then we obtain the following theorem. (Here we ignore programs that do not halt (i.e., loop forever), or, equivalently, we interpret looping as output 0.) The following corollary was already stated as Corollary 3.22.⁶¹

Corollary 6.16. *There are uncomputable functions $\mathbb{N} \rightarrow \{0, 1\}$.*

⁶¹Explaining the so-called Halting problem, namely to decide whether a given program halts for a given input, would require a more general theorem than Theorem 6.13, but it could be explained in the same spirit.

Proof. We consider the universe \mathbb{N} , and a program is thought of as represented by a natural number. Let $P(y, x) = 1$ if and only if the bit that program x outputs for input y is 1. Theorem 6.13, $\neg\exists x \forall y (P(y, x) \leftrightarrow \neg P(y, y))$, states that there exists no program x that (for all inputs y) computes the function $y \mapsto \neg P(y, y)$, i.e., this function is uncomputable. \square

The above corollary was already discussed as Corollary 3.22, as a direct consequence of Corollary 6.15 (i.e., of Theorem 3.21). The proof given here is stronger in the sense that it provides a concrete function, namely the function $y \mapsto \neg P(y, y)$, that is not computable.⁶² We state this as a corollary:

Corollary 6.17. *The function $\mathbb{N} \rightarrow \{0, 1\}$ assigning to each $y \in \mathbb{N}$ the complement of what program y outputs on input y , is uncomputable.*

Indice delle definizioni

Definizione 2.1 (Proposizione)	7	Definizione 3.3 (Sottoinsieme)	16
Definizione 2.4 (Valori di verità)	7	Definizione 3.4 (Insieme vuoto)	16
Definizione 2.5 (E, O, e NON logico) . .	7	Definizione 3.5 (Insieme potenza)	17
Definizione 2.6 (Formula)	7	Definizione 3.6 (Unione e intersezione)	17
Definizione 2.7 (Equivalenza tra formule)	7	Definizione 3.7 (Complemento)	18
Definizione 2.8 (Conseguenza logica) . .	8	Definizione 3.8 (Differenza di insiemi) .	18
Definizione 2.9 (Tautologia)	9	Definizione 3.9 (Prodotto cartesiano) . .	18
Definizione 2.10 (Formula soddisfacibile)	9	Definizione 3.10 (Relazione)	19
Definizione 2.11 (Predicato k -ario) . . .	9	Definizione 3.11 (Relazione identità) . .	19
Definizione 2.12 (Quantificatori)	10	Definizione 3.12 (Relazione inversa) . .	20
Definizione 2.13 (Composizione di implicazioni)	11	Definizione 3.13 (Composizione di relazioni)	20
Definizione 2.14 (Dimostrazione diretta di un'implicazione)	11	Definizione 3.14 (Riflessività)	21
Definizione 2.15 (Dimostrazione indiretta di un'implicazione)	11	Definizione 3.15 (Irreflessività)	21
Definizione 2.16 (<i>Modus Ponens</i>)	12	Definizione 3.16 (Simmetria)	21
Definizione 2.17 (Distinzione dei casi) .	12	Definizione 3.17 (Antisimmetria)	21
Definizione 2.18 (Dimostrazione per assurdo)	13	Definizione 3.18 (Transitività)	21
Definizione 2.19 (Dimostrazioni d'esistenza)	13	Definizione 3.19 (Chiusura transitiva) .	22
Definizione 2.20 (Dimostrazione con controesempio)	13	Definizione 3.20 (Relazione d'equivalenza)	22
Definizione 2.21 (Dimostrazione per induzione)	14	Definizione 3.21 (Classe d'equivalenza)	22
Definizione 3.1 (Cardinalità)	15	Definizione 3.22 (Partizione)	22
Definizione 3.2 (Uguaglianza tra insiemi)	15	Definizione 3.23 (Insieme quoziante) .	23
		Definizione 3.24 (Relazione d'ordine parziale)	23
		Definizione 3.25 (Elementi comparabili)	24
		Definizione 3.26 (Relazione d'ordine totale)	24

Definizione 3.27 (Elemento coprente)	24	Definizione 4.4 (Ideale)	34
Definizione 3.28 (Diagramma di Hasse di un poset (finito))	24	Definizione 4.5 (Minimo comune multiplo)	34
Definizione 3.29 (Prodotto diretto)	25	Definizione 4.6 (Numero primo)	35
Definizione 3.30 (Elementi speciali nei posets)	25	Definizione 4.8 (Relazionre di con- gruenza modulo m)	35
Definizione 3.31 (Poset ben ordinato)	26	Definizione 4.9 (Inverso moltiplicativo)	37
Definizione 3.32 (<i>Meet</i> e <i>join</i>)	26	Definizione 5.1 (Arietà)	39
Definizione 3.33 (Reticolo)	26	Definizione 5.2 (Algebra)	39
Definizione 3.34 (Funzione)	26	Definizione 5.3 (Elemento neutro)	39
Definizione 3.35 (Insieme delle funzioni)	27	Definizione 5.4 (Associatività)	40
Definizione 3.36 (Funzione parziale)	27	Definizione 5.5 (Monoide)	40
Definizione 3.37 (Immagine di un sottoinsieme)	27	Definizione 5.6 (Elemento inverso)	40
Definizione 3.38 (Immagine di una funzione)	27	Definizione 5.7 (Gruppo)	41
Definizione 3.39 (Antimmagine)	27	Definizione 5.8 (Gruppo abeliano)	41
Definizione 3.40 (Proprietà delle fun- zioni)	27	Definizione 5.9 (Prodotto diretto di gruppi)	42
Definizione 3.41 (Funzione inversa)	27	Definizione 5.10 (Omomorfismo)	43
Definizione 3.42 (Composizione di funzioni)	27	Definizione 5.11 (Sottogruppo)	43
Definizione 3.43 (Numerabilità)	28	Definizione 5.12 (Ordine di un elemento)	43
Definizione 3.44 ($\{0, 1\}^\infty$)	30	Definizione 5.13 (Ordine di un gruppo)	43
Definizione 3.45 (Funzione calcolabile)	30	Definizione 5.14 (Gruppo generato)	44
Definizione 4.1 (Relazione di divisione)	32	Definizione 5.15 (Gruppo ciclico)	44
Definizione 4.2 (Massimi comuni divisori)	33	Definizione 5.16 (Insieme delle classi resto invertibili modulo m)	45
Definizione 4.3 (Massimo comun divisore (definizone canonica))	33	Definizione 5.17 (Funzione di Eulero)	45
		Definizione 5.18 (Anello)	48
		Definizione 5.19 (Caratteristica)	48

Definizione 5.20 (Divisore)	49	Definizione 6.9 (Modello)	59
Definizione 5.21 (Massimo comun divisore)	49	Definizione 6.10 (Soddisfabilità)	60
Definizione 5.22 (Unità)	49	Definizione 6.11 (Tautologia)	60
Definizione 5.23 (Divisore di zero) . . .	49	Definizione 6.12 (Conseguenza logica) .	60
Definizione 5.24 (Dominio d'integrità) .	49	Definizione 6.13 (Equivalenza)	60
Definizione 5.25 (Anello di polinomio) .	50	Definizione 6.17 (Regola di derivazione)	61
Definizione 5.26 (Campo)	51	Definizione 6.19 (Calcolo logico)	61
Definizione 5.27 (Polinomio monico) . .	51	Definizione 6.20 (Derivazione)	61
Definizione 5.28 (Polinomio irriducibile)	51	Definizione 6.21 (Correttezza di una regola di derivazione)	62
Definizione 5.29 (Massimo comun divisore)	51	Definizione 6.22 (Correttezza e completezza di un calcolo logico) . . .	62
Definizione 5.33 (Radice)	52	Definizione 6.23 (Sintassi)	62
Definizione 5.34 (Molteplicità)	53	Definizione 6.24 (Semantica)	63
Definizione 5.35 (Anello dei polinomi su F ridotti modulo $m(x)$)	54	Definizione 6.25 (Letterale)	63
Definizione 6.1 (Sistema di dimostrazione)	55	Definizione 6.26 (CNF)	63
Definizione 6.2 (Correttezza)	55	Definizione 6.27 (DNF)	63
Definizione 6.3 (Completezza)	55	Definizione 6.28 (Proposizione)	64
Definizione 6.4 (Sintassi)	59	Definizione 6.29 (Proposizioni associate ad una formula)	64
Definizione 6.5 (Semantica)	59	Definizione 6.30 (Risolvente)	64
Definizione 6.6 (Interpretazione)	59	Definizione 6.31 (Sintassi)	66
Definizione 6.7 (Interpretazione adatta) .	59	Definizione 6.33 (Sostituzione)	67
Definizione 6.8 (Valore di verità)	59	Definizione 6.34 (Interpretazione)	67
		Definizione 6.37 (Forma prenessa) . . .	69

Indice dei Teoremi, dei lemmi e dei corollari

Lemma 2.1 (Regole di calcolo)	8	Teorema 3.14 (Bernstein-Schröder)	28
Lemma 2.2	9	Teorema 3.15	28
Lemma 2.3	9	Teorema 3.16	29
Lemma 2.4	11	Teorema 3.17	29
Lemma 2.5	11	Corollario 3.18	29
Lemma 2.6	12	Corollario 3.19	29
Lemma 2.7	12	Teorema 3.20	29
Lemma 2.8	12	Teorema 3.21	30
Lemma 2.9	13	Corollario 3.22	31
Teorema 2.10 (<i>Principio dei cassetti</i>) . .	13	Teorema 4.1 (Euclide)	32
Teorema 2.11	14	Lemma 4.2	33
Lemma 3.1	15	Lemma 4.3	34
Lemma 3.2	16	Lemma 4.4	34
Lemma 3.3	16	Corollario 4.5	34
Teorema 3.4	18	Teorema 4.6 (Fondamentale dell'Aritmetica)	35
Lemma 3.5	20	Lemma 4.13	35
Lemma 3.6	20	Lemma 4.14	35
Lemma 3.7	21	Corollario 4.15	36
Lemma 3.8	22	Lemma 4.16	36
Teorema 3.9	23	Corollario 4.17	36
Teorema 3.10	25	Lemma 4.18	37
Teorema 3.11	25	Teorema 4.19 (Cinese del Resto (CRT))	37
Lemma 3.12	27	Lemma 5.1	40
Lemma 3.13	28	Lemma 5.2	40
		Lemma 5.3	41
		Lemma 5.4	42

Lemma 5.5	43	Lemma 5.28	52
Lemma 5.6	43	Corollario 5.29	53
Teorema 5.7	44	Teorema 5.30	53
Teorema 5.8 (Lagrange)	44	Lemma 5.31	53
Corollario 5.9	44	Lemma 5.32	54
Corollario 5.10	44	Lemma 5.33	54
Corollario 5.11	45	Lemma 5.34	54
Lemma 5.12	45	Lemma 5.35	54
Teorema 5.13	46	Teorema 5.36	54
Corollario 5.14 (Fermat, Eulero)	46	Lemma 6.1 (Regole di calcolo)	60
Teorema 5.16	46	Lemma 6.2	61
Lemma 5.17	48	Lemma 6.3	61
Lemma 5.18	49	Lemma 6.4	62
Lemma 5.19	49	Teorema 6.5	63
Lemma 5.20	50	Lemma 6.6	64
Teorema 5.21	50	Teorema 6.7	65
Lemma 5.22	50	Lemma 6.9	68
Teorema 5.23	51	Lemma 6.10	69
Teorema 5.24	51	Teorema 6.11	69
Teorema 5.25	52	Teorema 6.12	69