

Algebra I

AlpT (@freaknet.org)

August 16, 2013

Abstract

Questo testo e' una rielaborazione personale degli appunti presi durante il corso di Algebra I, tenuto dal Prof. Alfio Ragusa presso il dipartimento di Matematica, Catania, A.A. 2006/2007.

Saro' ben lieto di correggere ogni eventuale errore che mi comunicherai.

Buon lettura.

~ ~

Copyright ©2012 Andrea Lo Pumo aka AlpT <alpt@freaknet.org>. All rights reserved.

This document is free; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this document; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Contents

1	Gli insiemi	1
1.1	Concetto primitivo	1
1.2	L'elemento	1
1.3	L'insieme	1
1.3.1	Insieme vuoto	2
1.3.2	Insieme identico	2
1.4	Sottoinsieme	2
1.4.1	Proprieta'	2
1.5	Insiemi uguali	2
1.5.1	Sottoinsieme proprio e improprio	2
1.6	Intersezione	3
1.6.1	Proprieta'	3
1.7	Insiemi disgiunti	3
1.8	Insiemi coincidenti	3
1.9	Insieme delle parti	3
1.9.1	Proprieta'	4
1.10	Insieme di indici	4
1.11	Famiglia	4
1.11.1	Notazioni indicizzate	4
1.12	Unione	5
1.12.1	Proprieta'	5
1.13	Unione e intersezione	5
1.14	Differenza	5
1.14.1	Proprieta'	6
1.15	Differenza simmetrica	6
1.15.1	Proprieta'	7
1.16	Unione disgiunta (o somma disgiunta)	7
1.17	Partizione di A	7
1.18	Prodotto cartesiano	8
2	Funzioni	8
2.1	Funzione (applicazione)	8
2.1.1	Dominio e Codominio	8
2.1.2	Immagine e Controimmagine	8
2.1.3	Proprieta'	9
2.2	Unione di funzioni	10
2.3	Funzione surriettiva	10
2.4	Funzione iniettiva	10
2.5	Funzione biettiva	11
2.6	Composizione di funzioni	11
2.6.1	Proprieta'	11
2.7	Funzione inversa	12
2.7.1	Proprieta'	12
2.8	Insieme di tutte le applicazioni $A \rightarrow B$	13
2.8.1	Numero di funzioni	13
2.9	Funzione caratteristica	14
2.10	Operazione binaria interna	14

3	Relazioni	14
3.1	Relazione binaria	14
3.1.1	Esempio	14
3.2	Relazione binaria interna	14
3.3	Relazione binaria diagonale	15
3.4	Relazione binaria inversa	15
3.4.1	Esempio	15
3.5	Composizione tra relazioni binarie interne	15
3.5.1	Esempio	15
3.6	Relazione binaria interna riflessiva	15
3.7	Relazione binaria interna simmetrica	15
3.8	Relazione binaria interna antisimmetrica	16
3.8.1	Esempio	16
3.9	Relazione binaria interna transitiva	16
3.9.1	Esempio	16
4	Relazioni di equivalenza	16
4.1	Classe d'equivalenza	16
4.1.1	Proprieta'	17
5	Relazioni di ordine	18
5.1	Insieme parzialmente ordinato	18
5.2	Insieme totalmente ordinato	18
5.2.1	Esempio	19
5.3	Minimo	19
5.3.1	Proprieta'	19
5.4	Insieme ben ordinato	19
5.5	Massimo	19
5.5.1	Proprieta'	20
5.6	Minimale	20
5.6.1	Proprieta'	20
5.6.2	Esempio	20
5.7	Massimale	20
5.7.1	Proprieta'	20
5.7.2	Esempio	20
5.8	Minorante	21
5.8.1	Esempio	21
5.9	Maggiorante	21
5.9.1	Esempio	21
5.10	Estremo inferiore	21
5.10.1	Esempio	22
5.11	Estremo superiore	22
5.12	POSET completo	22
6	L'insieme $\mathbb{N}$	22
6.1	Assiomatizzazione di Peano	22
6.2	Dimostrazione per induzione	23
6.3	Principii di induzione	24
6.4	Altre note sull'induzione	26

6.5	Addizione in $\mathbb{N}$	27
6.5.1	Proprieta' dell'addizione	28
6.6	Moltiplicazione	28
6.6.1	Proprieta' della moltiplicazione	28
6.7	Elemento neutro	29
7	Teoria della divisibilita'	29
7.1	Divisibilita'	29
7.1.1	Proprieta'	29
7.2	Massimo Comune Divisore	30
7.2.1	Proprieta'	30
7.3	Algoritmo di divisione in $\mathbb{N}$	30
7.4	Algoritmo Euclideo per il MCD	31
8	Teoria degli insiemi	32
8.1	Cardinalita' (o Potenza)	32
8.2	Insieme finito (infinito)	32
8.2.1	Esempio	33
8.3	Insieme numerabile	33
8.3.1	Proprieta'	33
8.4	Insiemi equipotenti	33
8.4.1	Proprieta'	34
8.5	Diagonalizzazione di Cantor	35
8.6	Potenza del continuo	37
8.7	Ipotesi del continuo	37
9	L'insieme $\mathbb{Z}$	37
9.1	Addizione	37
9.1.1	Proprieta'	38
9.2	Moltiplicazione	38
9.2.1	Proprieta'	38
9.3	Simbolismo	38
9.4	$\mathbb{N}$ immerso in $\mathbb{Z}$	39
9.5	$\mathbb{Z}$ e' un totet	39
9.6	Teoria della divisibilita' in $\mathbb{Z}$	39
9.6.1	Proprieta'	39
9.7	Numeri irriducibili e primi	40
9.8	MCD in $\mathbb{Z}$	40
9.9	Minimo Comune Multiplo	40
9.9.1	Proprieta'	41
9.10	Algoritmo di divisione in $\mathbb{Z}$	42
9.11	Identita' di Bezout	42
9.12	Teorema fondamentale dell'aritmetica	43
10	Aritmetica modulare	44
10.1	Somma	45
10.1.1	Prodotto	45
10.2	Proprieta'	45
10.3	Elementi invertibili	46
10.3.1	Insieme degli invertibili	46

10.4	Equazione modulare	46
10.5	Sistemi lineari di congruenze	48
10.5.1	Teorema cinese del resto	48
10.5.2	Applicazione del teorema cinese del resto	49
10.5.3	Metodo di sostituzione	49
10.6	Altri sistemi di congruenze	50
11	Equazioni diofantee	52
11.0.1	Risoluzione	54
12	I numeri primi	54
12.1	La funzione di Eulero	54
12.2	Teorema di Fermat	56
12.3	Teorema di Eulero	57
12.4	Proprieta' dei primi	57
12.5	Teorema di Wilson	57
12.6	R.S.A	58
12.7	La chiave pubblica	58
12.8	Messaggio criptato	58
12.9	Chiave privata	58
12.10	Messaggio decriptato	59
13	L'insieme $\mathbb{Q}$	59
13.1	Addizione	59
13.1.1	Proprieta'	59
13.2	Moltiplicazione	60
13.2.1	Proprieta'	60
13.3	Immersione di $\mathbb{Z}$ in $\mathbb{Q}$	60
14	L'insieme $\mathbb{R}$	60
15	L'insieme $\mathbb{C}$	61
15.1	Inverso	61
15.2	Radici n-esime dell'unita'	61
16	Polinomi	62
16.1	Funzione polinomiale	62
16.2	Somma	62
16.3	Prodotto	62
16.4	Polinomio	63
16.5	Grado di un polinomio	64
16.5.1	Proprieta'	64
16.6	Polinomi invertibili	64
16.7	Algoritmo di divisione in $K[x]$	64
16.8	Polinomi associati	65
16.9	Polinomi primi	65
16.10	Polinomio irriducibile	65
16.11	MCD di polinomi	66
16.12	Fattorizzazione unica di un polinomio	66
16.13	Teorema di Ruffini	66

16.14	Molteplicità	67
16.15	Irriducibilità di un polinomio in $\mathbb{C}[x]$	67
16.15.1	Coniugato di un polinomio	67
16.15.2	Fattorizzazione in $\mathbb{C}$	67
16.16	Irriducibilità di un polinomio in $\mathbb{R}$	68
16.17	Irriducibilità di un polinomio in $\mathbb{Q}$	69
16.18	Polinomio primitivo	69
16.19	Lemma di Gauss	70
16.20	Corollario del lemma di Gauss	70
16.21	Irriducibilità in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$	70
16.22	Teorema di Gauss	71
16.23	Criterio di Eisenstein	72
16.24	Criterio di riduzione modulo p	72
17	Anelli	74
17.1	I quaternioni	76
17.2	Domini finiti	77
17.3	Sottoanello	77
17.4	Omomorfismo	78
17.4.1	Proprietà	78
17.5	Immagine e nucleo	79
17.6	Anello quoziente	81
17.6.1	Esempio	83
17.7	Suriezione naturale	83
17.8	Ideale	83
17.8.1	Proprietà degli ideali	84
17.9	Omomorfismo e ideali	85
17.10	Teorema dell'omomorfismo	86
17.10.1	Corollario I	87
17.10.2	Corollario II	87
17.11	Teorema dell'isomorfismo II	87
17.12	Teorema dell'isomorfismo III	89
18	Ideali generati	89
18.1	Sistema di generatori	89
18.2	Ideale primo	90
18.3	Ideale massimale	91
18.4	Ideali e $\mathbb{Z}$	93
19	Campo dei quozienti di D	93
19.0.1	Esempi	95
20	Principal Ideal Domain	95
21	Domini euclidei	96
21.1	Esempi di domini euclidei	97
21.2	Proprietà dei domini euclidei	97
21.3	ED, PID e UFD	100
21.3.1	Caratterizzazione di un UFD	101
21.3.2	PID $\Rightarrow$ UFD	103

21.4	$ED \Rightarrow PID \Rightarrow UFD$, e controesempi	104
22	Interi di Gauss	105
22.1	Somma di quadrati	107
22.1.1	Esempio	110
23	Polinomi UFD	111
23.1	Teorema di Gauss	111
23.1.1	Esempi	112
23.2	Criteri di irriducibilita'	112
23.3	Algoritmo di divisione in un UFD	112

1 Gli insiemi

L'*insieme* e' uno dei concetti piu' generali della matematica. E' talmente generale, che rende possibile ricostruire quasi tutta la matematica moderna a partire dalla teoria degli insiemi.

1.1 Concetto primitivo

L'insieme e' definito come elemento *primitivo*.

Un elemento primitivo e' un concetto che si definisce senza ricorrere a nessun'altra precedente definizione.

I concetti primitivi sono necessari per poi poter porre altre definizioni che si basano su essi.

Poiche' il concetto d'insieme e' facilmente comprensibile dalla maggior parte degli esseri umani, i matematici lo hanno scelto come elemento primitivo.

Questo, pero', non e' sempre vero, un concetto primitivo non e' universale. Per spiegare il semplice concetto d'insieme a un computer e' necessario istruirlo con migliaia e migliaia di righe di codice. D'altronde, lo stesso vale per un essere umano di pochi anni: e' un compito arduo, se non impossibile chiarire il concetto d'insieme a un bambino appena nato.

In conclusione, sarebbe piu' corretto dire che l'insieme e' un concetto primitivo per gli esseri umani che hanno raggiunto un minimo di allenamento mentale. Poiche', tu lettore, stai leggendo questo testo, sarai anche in grado di comprendere il concetto d'insieme, e di conseguenza quasi tutta la matematica moderna.

1.2 L'elemento

Un elemento puo' essere qualsiasi un qualsiasi simbolo che possa essere riconosciuto e distinto da altri simboli. In questo caso "simbolo" e' sinonimo di "informazione".

1.3 L'insieme

Un *insieme* e' formato da una lista non ordinata di elementi di qualsiasi tipo.

Per descrivere un insieme, bisogna includere la lista di tutti i suoi elementi all'interno di parentesi graffe.

Ad esempio, questo e' l'insieme di alcuni linguaggi di programmazione:

$$\{C, Perl, TCL, Awk, Python, Bash, Lisp\}$$

Possiamo anche assegnare un nome all'insieme:

$$\mathbb{L} = \{C, Perl, TCL, Awk, Python, Bash, Lisp\}$$

Che tradotto in parole diventa: "L e' l'insieme che contiene i seguenti linguaggi di programmazione: *C, Perl, TCL, Awk, Python, Bash, Lisp*"

Poiche' un insieme puo' contenere qualsiasi tipo di elemento possiamo anche definire l'insieme di tutti i linguaggi di programmazione:

$$\mathbb{L} = \{\text{Tutti i linguaggi di programmazione esistenti fino a oggi}\}$$

Per indicare il numero degli elementi di un insieme (che viene chiamato cardinalità dell'insieme), si usano le sbarrette del valore assoluto:

$$|L| = 7$$

Il numero degli elementi di L è 7.

1.3.1 Insieme vuoto

L'insieme vuoto è quell'insieme che non contiene alcun elemento.

1.3.2 Insieme identico

L'insieme identico dell'insieme A è l'insieme A stesso.

1.4 Sottoinsieme

L'insieme B è un sottoinsieme di A , se tutti gli elementi di B sono contenuti in A .

$$B \subseteq A \Leftrightarrow \forall b \in B / b \in A$$

1.4.1 Proprietà

1. L'insieme vuoto è sempre un sottoinsieme di qualsiasi insieme.

$$\emptyset \subseteq A$$

2. Qualsiasi insieme contiene l'insieme identico come sottoinsieme.

$$A \subseteq A$$

3. Se n è il numero degli elementi dell'insieme A , allora il numero totale di tutti i suoi possibili sottoinsiemi è pari a 2^n

1.5 Insiemi uguali

Due insiemi B e A sono uguali se B è un sottoinsieme di A ed A è un sottoinsieme di B ,

$$B = A \Leftrightarrow B \subseteq A \wedge A \subseteq B$$

1.5.1 Sottoinsieme proprio e improprio

Il sottoinsieme *improprio* di A , è quell'insieme che contiene tutti gli elementi di A , ovvero, è uguale ad A stesso.

Il sottoinsieme *proprio* di A , è invece un qualsiasi sottoinsieme che non contiene almeno un elemento di A .

I simboli utilizzati per indicare un sottoinsieme generale (improprio o proprio) e quello per indicare un sottoinsieme proprio sono rispettivamente $\subseteq$ e $\subset$. Per analogia si possono confrontare con i simboli $\leq$ e $<$: se il numero degli elementi di B è $\leq$ di quelli di A scriveremo $B \subseteq A$, altrimenti $B \subset A$.

1.6 Intersezione

L'intersezione di A e B e' quell'insieme che contiene tutti gli elementi che sono sia in A che in B. Nell'algebra booleana, l'intersezione corrisponde all'operazione AND.

$$(x \in A \cap B) \Leftrightarrow (x \in A \wedge x \in B)$$

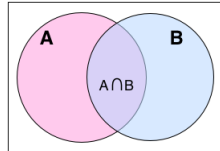


Figure 1: Intersezione di A e B

1.6.1 Proprieta'

1. $A \cap B = B \cap A$ (proprietà commutativa)
2. $A \cap A = A$
3. $A \cap \emptyset = \emptyset$
4. $(A \cap B) \cap C = A \cap (B \cap C)$ (proprietà associativa)
5. $B \subseteq A \Leftrightarrow B \cap A = B$

1.7 Insiemi disgiunti

Due insiemi A e B sono disgiunti se non hanno nessun elemento in comune.

$$A, B \text{ sono disgiunti} \Leftrightarrow A \cap B = \emptyset$$

1.8 Insiemi coincidenti

Due insiemi A e B sono coincidenti se hanno tutti gli elementi in comune, ovvero sono insiemi uguali (vedi 1.5).

$$A, B \text{ sono coincidenti} \Leftrightarrow A = B$$

1.9 Insieme delle parti

Si dice *insieme delle parti* (o *insieme potenza*) dell'insieme A, quell'insieme che contiene come elementi, tutti i sottoinsiemi di A. L'insieme delle parti si indica con $\mathcal{P}(A)$.

1.9.1 Proprieta'

1. $B \subseteq A \Leftrightarrow B \in \mathcal{P}(A)$
2. $a \subseteq A \Leftrightarrow \{a\} \subseteq A \Leftrightarrow \{a\} \in \mathcal{P}(A)$
3. $|\mathcal{P}(A)| = 2^{|A|}$ Ovvero, il numero degli elementi di $\mathcal{P}(A)$ e' pari a 2 elevato al numero degli elementi di A . (questa proprieta' vale solo se $\mathcal{P}(A)$ e' finito).

Proof: Poniamo $n = |A|$ e $p \in \mathcal{P}(A)$

Rappresentiamo p come un numero a n -bit. L' n -esimo bit e' uguale a 1 se l' n -esimo elemento di A e' presente in p , altrimenti e' uguale a 0.

Poiche' di numeri a n -bit ne esistono 2^n , il numero di tutti gli $p \in \mathcal{P}(A)$ e' pari a 2^n . $\square$

1.10 Insieme di indici

Consideriamo un insieme I e un insieme A . E' possibile indicizzare gli elementi di A utilizzando gli elementi di I , cosi', se $i \in I$, $a_i \in A$ e' l'elemento i -esimo di A .

L'insieme I viene chiamato *insieme degli indici*.

Ad esempio, indicizziamo l'insieme $\mathbb{L}$ con l'insieme $I = \mathbb{N}$,

$$I = \mathbb{N}$$

$$\mathbb{L} = \{C, Perl, TCL, Awk, Python, Bash, Lisp\}$$

e otteniamo:

$$l_0 = C$$

$$l_1 = Perl$$

$$l_2 = TCL$$

$$\vdots$$

$$l_6 = Lisp$$

1.11 Famiglia

Una famiglia e' costituita da due insiemi: l'insieme degli indici I e l'insieme A . Ad ogni elemento di A e' associato un indice $i \in I$.

Una famiglia e' indicata come $\{A_i\}_{i \in I}$, dove I e' l'insieme degli indici, e A_i e' l'elemento della famiglia associato a i .

Riprendendo il precedente esempio (1.10), possiamo scrivere:

$$\{L_i\}_{i \in \mathbb{N}}$$

1.11.1 Notazioni indicizzate

Gli indici vengono anche usati per abbreviare e semplificare la scrittura di proposizioni matematiche.

Ad esempio: per indicare l'intersezione di tutti gli elementi della famiglia $\{A_i\}_{i \in I}$ possiamo scrivere:

$$A_1 \cap A_2 \cap A_{\dots} \cap A_n = \{x | x \in A_1, x \in A_2, x \in A_{\dots}, x \in A_n\}$$

Oppure, possiamo scrivere in forma abbreviata:

$$\bigcap_{i \in I} A_i = \{x | x \in A_i, \forall i \in I\}$$

1.12 Unione

L'unione di A con B viene indicata con $A \cup B$, ed e' definita come:

$$A \cup B = \{x | x \in A \vee x \in B\}$$

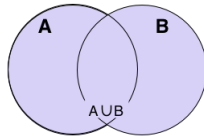


Figure 2: Unione di A e B

Nell'algebra booleana, l'unione corrisponde all'operazione logica OR.

1.12.1 Proprieta'

1. $A \cup \emptyset = A$
2. $A \cup A = A$ (proprietà riflessiva)
3. $A \cup B = B \cup A$ (proprietà commutativa)
4. $A \cup (B \cup C) = (A \cup B) \cup C$ (proprietà associativa)
5. $B \subseteq A \Leftrightarrow B \cup A = A$

1.13 Unione e intersezione

Ecco alcune identità che fanno uso sia dell'intersezione (1.6) che dell'unione (1.12):

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (proprietà distributiva dell'intersezione rispetto all'unione).
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (proprietà distributiva dell'unione rispetto all'intersezione).

1.14 Differenza

La differenza " B meno A " si indica con $B \setminus A$, e viene definita come:

$$B \setminus A = \{x | \forall x \in B, x \notin A\}$$

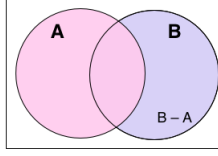


Figure 3: Differenza tra B ed A

1.14.1 Proprieta'

1. $A \setminus \emptyset = A$
2. $A \setminus \emptyset = \emptyset$
3. $B \subseteq A \Rightarrow B \setminus A = \emptyset$
4. **Leggi di De Morgan:**

$$\begin{aligned} A \setminus (B \cup C) &\Leftrightarrow (A \setminus B) \cap (A \setminus C) \\ A \setminus (B \cap C) &\Leftrightarrow (A \setminus B) \cup (A \setminus C) \end{aligned}$$

Proof: Dimostriamo il primo caso.

Per la definizione di differenza:

$$A \setminus (B \cup C) = \{x | x \in A, x \notin (B \cup C)\}$$

Per la definizione di unione:

$$x \notin (B \cup C) \Rightarrow (x \notin B) \wedge (x \notin C) \quad [1]$$

Dato che $(x \notin B)$ e che $(x \in A)$, sempre per la definizione di differenza possiamo scrivere:

$$(x \notin B, (x \in A) \Rightarrow x \in (A \setminus B))$$

Lo stesso vale per A e C :

$$(x \notin C), (x \in A) \Rightarrow x \in (A \setminus C)$$

Possiamo quindi riscrivere la [1]:

$$x \notin (B \cup C) \Rightarrow (x \notin B) \wedge (x \notin C) \Rightarrow x \in (A \setminus B) \wedge (A \setminus C) \Rightarrow x \in (A \setminus B) \cap (A \setminus C)$$

In conclusione:

$$A \setminus (B \cup C) = \{x | x \in A, x \notin (B \cup C)\} = (A \setminus B) \cap (A \setminus C)$$

□

5. Siano $A, B \subseteq \Omega$, con A^c indichiamo $\Omega \setminus A$, allora si ha

$$A \cap B^c = A \setminus B = A \setminus (A \cap B)$$

1.15 Differenza simmetrica

La differenza simmetrica corrisponde all'operazione *XOR* nell'algebra booleana e si indica con il simbolo Δ .

$$A \Delta B = \{x | (x \in A \vee x \in B) \wedge \overline{(x \in A \wedge x \in B)}\} = \{x : (x \in A) \text{ XOR } (x \in B)\}$$

Ovvero, x appartiene o ad A o a B , ma mai a entrambi.

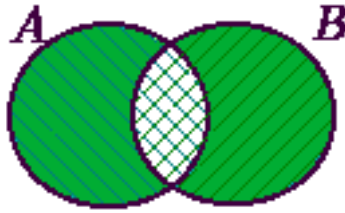


Figure 4: Differenza simmetrica

1.15.1 Proprieta'

1. $A \Delta B = B \Delta A$ (proprietà commutativa)
2. $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ (proprietà associativa)
3. $A \Delta A = \emptyset$
4. $A \Delta \emptyset = A$
5. $A \Delta B = (A \setminus B) \cup (B \setminus A)$,
6. $A \Delta B = (A \cup B) \setminus (A \cap B)$
7. $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$ (proprietà distributiva dell'intersezione sulla differenza simmetrica)

1.16 Unione disgiunta (o somma disgiunta)

Dati due insiemi A e B , la loro somma disgiunta equivale all'insieme delle coppie formate da un simbolo che denota l'appartenenza ad A oppure a B e l'elemento dell'insieme. L'unione disgiunta si indica con il simbolo $\oplus$.

Nota: la scrittura (a, b) indica una coppia ordinata di due elementi a e b .

$$A \oplus B = \{(0, a) | \forall a \in A\} \cup \{(1, b) | \forall b \in B\}$$

O usando il prodotto cartesiano (vedi 1.18)

$$A \oplus B = (A \times \{0\}) \cup (B \times \{1\})$$

1.17 Partizione di A

Una partizione di un insieme X e' un insieme P di sottoinsiemi di X tale che

0. $a \in P \Rightarrow a \subseteq X$
1. $a, b \in P : a \neq b \Rightarrow a \cap b = \emptyset$
2. $\bigcup_{a \in P} a = X$

ovvero, due elementi distinti di P sono due sottoinsiemi disgiunti di X , e l'unione di tutti gli elementi di P e' proprio X .

1.18 Prodotto cartesiano

Il prodotto cartesiano dei due insiemi A e B si definisce come:

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

Dove, (a, b) indica una coppia ordinata di due elementi a e b .

Il piano cartesiano e' un prodotto cartesiano $\mathbb{R} \times \mathbb{R}$:

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) | \forall x, y \in \mathbb{R}\}$$

2 Funzioni

2.1 Funzione (applicazione)

$$f : X \rightarrow Y$$

La funzione f e' un sottoinsieme di $X \times Y$, tale che

$$\begin{aligned} f &\subseteq X \times Y \\ \forall x \in X \quad \exists! y \in Y : (x, y) &\in f \end{aligned}$$

Ovvero, la funzione $f : X \rightarrow Y$ e' un sottoinsieme del prodotto cartesiano $X \times Y$ tale che per ogni $x \in X$ esiste uno ed un solo elemento $y \in Y$, tale che $(x, y) \in f$.

In altre parole, possiamo pensare f come una legge che associa ad ogni elemento di X , uno e un solo elemento di Y .

2.1.1 Dominio e Codominio

L'insieme X viene chiamato *dominio* della funzione f , mentre l'insieme Y *codominio*.

2.1.2 Immagine e Controimmagine

L'immagine della funzione f e' l'insieme:

$$Im(f) = f(X) = Im f = \{y \in Y : \exists x \in X : f(x) = y\}$$

Ovvero, e' quell'insieme del codominio ai cui elementi corrisponde sempre almeno un elemento del dominio.

L'immagine di f si indica con $Im(f), f(X), Im f$.

La controimmagine della funzione f e' l'insieme:

$$f^{-1}(X) = \{x \in X : f(x) \in Y\}$$

Ovvero, e' quel sottoinsieme del dominio, i cui elementi hanno tutti un corrispondente nel codominio.

L'immagine di un insieme $A \subseteq X$ si indica con $f(A)$ ed e':

$$f(A) = \{f(a) | a \in A\}$$

La controimmagine di un insieme $B \subseteq Y$ e':

$$f^{-1}(B) = \{x \in X | f(x) \in B\}$$

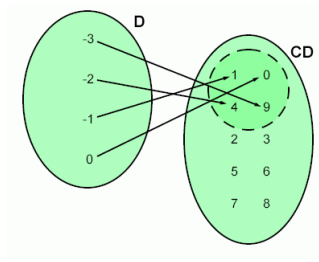


Figure 5: L'immagine della funzione e' quella parte tratteggiata che si trova all'interno dell'insieme CD (codominio)

2.1.3 Proprieta'

1. $f(A \cup B) = f(A) \cup f(B)$

2. $f(A \cap B) \subseteq f(A) \cap f(B)$

Se e' iniettiva vale l'uguaglianza.

3. $f(f^{-1}(V)) \subseteq V$

Proof:

$$z \in f(f^{-1}(V)) = f(\{x \in X \mid f(x) \in V\}) = \{f(x) \mid x \in X, f(x) \in V\} = \{f(x) \in V \mid x \in X\}$$

$$\Rightarrow z = f(x) \in V$$

Se e' surriettiva vale l'uguaglianza.

4. $V \subseteq f^{-1}(f(V))$

Proof:

$$v \in V \Rightarrow f(v) \in f(V) \Rightarrow v \in f^{-1}(f(V))$$

Se e' iniettiva vale l'uguaglianza.

Proof:

$$v \in f^{-1}(f(V)) \Leftrightarrow f(v) \in f(V) \Leftrightarrow f(v) = f(\underbrace{\bar{v}}_{\in V}) \underset{f \text{ iniettiva}}{\Rightarrow} v = \bar{v} \in V$$

5. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

Proof:

$$z \in f^{-1}(A \cap B) \Leftrightarrow f(z) \in A \cap B \Leftrightarrow f(z) \in A \wedge f(z) \in B \Leftrightarrow z \in f^{-1}(A) \wedge z \in f^{-1}(B)$$

6. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

7. Data $f : A \rightarrow B$ iniettiva, se $|A| = |B|$, e A, B sono finiti, allora f e' anche surriettiva.

Proof: Supponiamo per assurdo che $\text{Im } f \neq B$, cioe' che $\text{Im } f \subset B$. Poiche' stiamo lavorando su insiemi finiti, $|\text{Im } f| < |B|$. Allora,

$$|\text{Im } f| < |B| = |A|$$

ma questo e' assurdo, perche' f e' iniettiva. Infatti, essendo f iniettiva,

$$\forall b \in \text{Im } f \exists ! a \in A : f(a) = b$$

e d'altronde per definizione di funzione,

$$\forall a \in A \exists! b \in \text{Im } f : f(a) = b$$

quindi $|\text{Im } f| = |A|$.

2.2 Unione di funzioni

Proposition 2.1. *Siano date due funzioni $f : A \longrightarrow B$, $g : A' \longrightarrow B'$. Si ha che*

$$f(x) = g(x) \quad \forall x \in A \cap A' \Rightarrow h = f \cup g \text{ e' una funzione.}$$

E piu' precisamente, la legge di h e'

$$h(x) = \begin{cases} f(x) & x \in A \\ g(x) & x \in A' \end{cases}$$

$$h : A \cup A' \longrightarrow B \cup B'$$

ovvero, $h(x) = f(x)$ se $x \in A$, altrimenti se $x \in A'$ si ha $h(x) = g(x)$.

Proof: Per definizione, $f \subseteq A \times B$, $g \subseteq A' \times B'$. Quindi, ha senso considerare la loro unione:

$$h = f \cup g \subseteq A \times B \cup A' \times B' \subseteq A \cup A' \times B \cup B'$$

. Inoltre, poiche' $f(x) = g(x) \quad \forall x \in A \cap A'$, e per l'unicita' di $f(x)$ e $g(x)$, si ha che

$$\forall x \in A \cup A' \exists! y \in B \cup B' : (x, y) \in h$$

quindi h e' una funzione a tutti gli effetti, che puo' anche essere descritta dalla seguente legge:

$$h(x) = \begin{cases} f(x) & x \in A \\ g(x) & x \in A' \end{cases}$$

□

2.3 Funzione surriettiva

In una funzione surriettiva il codominio coincide con la sua immagine.

Formalmente possiamo scrivere:

$$f : X \rightarrow Y \text{ e' surriettiva} \Leftrightarrow \forall y \in Y, \exists x \in X | f(x) = y$$

Una funzione surriettiva da A in B si indica con:

$$f : A \twoheadrightarrow B$$

Per dimostrare che una funzione e' surriettiva basta provare che $\forall y \in Y, \exists x \in X | f(x) = y$

2.4 Funzione iniettiva

In una funzione iniettiva, a un elemento dell'immagine corrisponde uno e un solo elemento del dominio.

Formalmente possiamo scrivere:

$$f : X \rightarrow Y \text{ e' iniettiva} \Leftrightarrow \forall x_1, x_2 \in X, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

oppure

$$f : X \rightarrow Y \text{ e' iniettiva} \Leftrightarrow \forall x_1, x_2 \in X, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Una funzione iniettiva da A in B si indica con:

$$f : A \hookrightarrow B$$

Per dimostrare che una funzione e' iniettiva basta provare $f(x) = f(y) \Rightarrow x = y$

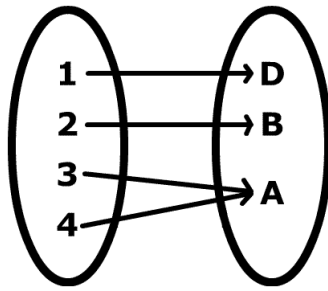


Figure 6: Funzione surriettiva e non iniettiva

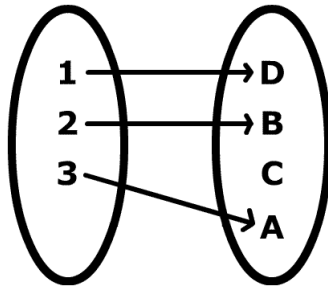


Figure 7: Funzione iniettiva e non surriettiva

2.5 Funzione biettiva

Una funzione è biettiva quando è sia iniettiva che surriettiva. Una funzione biettiva da A in B si indica con:

$$f : A \leftrightarrow B$$

2.6 Composizione di funzioni

Date due funzioni $f : X \rightarrow Y$ e $g : Y \rightarrow Z$, possiamo *comporre* in un'unica funzione $g \circ f : X \rightarrow Z$, ponendo $(g \circ f)(x) = g(f(x)) \forall x \in X$.

2.6.1 Proprietà

1. La composizione di funzioni non gode della proprietà commutativa, infatti, quasi sempre è vero che $(g \circ f) \neq f \circ g$.
2. $g \circ (f \circ h) = (g \circ f) \circ h$ (proprietà associativa)
3. Se f e g sono iniettive, la loro composizione è iniettiva.
4. Se f e g sono surriettive, la loro composizione è surriettiva.
5. Se f e g sono biettive, la loro composizione è biettiva.
6. Se $f \circ g$ è surriettiva, f è sicuramente surriettiva, ma g può non esserlo.

7. Se $f \circ g$ e' iniettiva, g e' sicuramente iniettiva, ma f puo' non esserlo.
8. Se $f \circ g$ e' biettiva, possiamo dedurre che g e' iniettiva e f e' surriettiva.

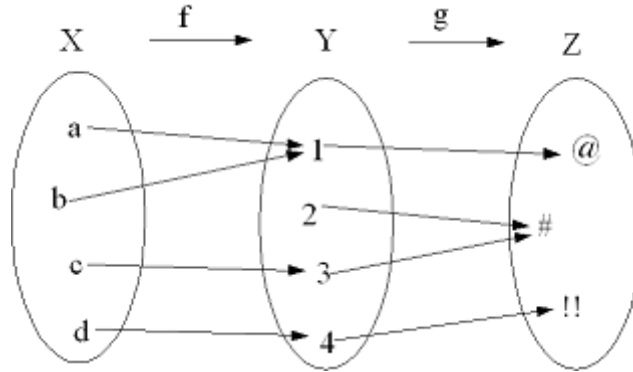


Figure 8: Composizione di due funzioni

2.7 Funzione inversa

La funzione inversa della funzione f , e' indicata con f^{-1} , e corrisponde a quella funzione che associa a ogni elemento del codominio di f l'elemento corrispondente del dominio. La funzione inversa esiste se e solo se f e' biettiva.

$$f(f^{-1}(y)) = y, \quad \forall y \in Y$$

$$f^{-1}(f(x)) = x, \quad \forall x \in X$$

2.7.1 Proprieta'

1. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$
2. $f^{-1} \circ f : X \rightarrow X$. Identita' assoluta in X, che si indica con: $f^{-1} \circ f = i_X$
3. $f \circ f^{-1} : Y \rightarrow Y$. Identita' assoluta in Y, che si indica con: $f \circ f^{-1} = i_Y$.
4. Data la funzione $f : A \rightarrow B$

$$\exists g : B \rightarrow A \text{ tale che } f \circ g = i_B \Leftrightarrow f \equiv \text{surriettiva}$$

$\langle 1 \rangle$ Dim $\Rightarrow$

Sia $b \in B$, vogliamo dimostrare che $\exists a \in A : f(a) = b$.

Sia allora $a = g(b)$,

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

$\langle 2 \rangle$ Dim $\Leftarrow$

Sia $b \in B$. Poiche' f e' surriettiva, $\exists a \in A : f(a) = b$ allora poniamo $g(b) := a$. Abbiamo cosi' creato la funzione g , e inoltre:

$$f(g(b)) = b \quad \forall b \in B$$

□

Se, invece, $g \circ f = i_A$, allora:

$$\exists g : B \rightarrow A \text{ tale che } g \circ f = i_A \Leftrightarrow f \equiv \text{iniettiva}$$

Se sono entrambi vere, allora f e' biettiva.

2.8 Insieme di tutte le applicazioni $A \rightarrow B$

Consideriamo un dominio A e un codominio B . Indichiamo con B^A l'insieme di tutte le funzioni $A \rightarrow B$.

$$B^A = \{ \text{insieme di tutte le funzioni } , A \rightarrow B \}$$

possiamo anche scrivere:

$$B^A = \text{hom}(A, B)$$

2.8.1 Numero di funzioni

Se A, B sono finiti, possiamo contare esattamente quante funzioni esistono: sia $A = \{a_1, a_2, \dots, a_m\}$, $B = \{b_1, b_2, \dots, b_n\}$,

1. Il numero di funzioni iniettive e':

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

che e' il numero di disposizioni semplici di n oggetti in classi di m oggetti.

Si deve anche avere che $m \leq n$, altrimenti non ci sarebbero funzioni iniettive.

Proof: Poiche' le funzioni sono iniettive, ogni f assegna a un a elementi distinti di A elementi distinti di B .

Quindi la m -upla $(a_1, a_2, \dots, a_m)$, che contiene tutti gli elementi (distinti) di A viene associata a una m -upla di elementi distinti B .

Tutte le possibili m -uple di elementi distinti B sono in numero

$$\binom{n}{m}$$

che e' il numero di combinazioni semplici di n oggetti in classi di m oggetti.

Fissiamo una associazione f tra queste che abbiamo gia' considerato:

$$(a_1, a_2, \dots, a_m) \longrightarrow (f(a_1), f(a_2), \dots, f(a_m))$$

e' chiaro che da questa associazione, possiamo creare quelle del tipo $\alpha \longrightarrow (f(a_1), f(a_2), \dots, f(a_m))$, dove α e' una qualsiasi m -upla che e' una permutazione di $(a_1, a_2, \dots, a_m)$. Tutte le possibili permutazioni di m oggetti sono in numero $m!$.

Quindi per ogni associazione di prima, abbiamo altre $m!$ associazioni.

Il totale e' percio':

$$\binom{n}{m} m!$$

2. Il numero di funzioni biettive e' $n!$. Dove $m = n$.

Proof: Se per assurdo $m < n$, allora non si avrebbero funzioni surriettive. Se per assurdo $m > n$, allora non si avrebbero funzioni iniettive. Allora $m = n$.

Basta utilizzare la formula del numero di funzioni iniettive:

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

3. Il numero di funzioni surriettive $A \rightarrow B$ e':

$$\sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^n$$

2.9 Funzione caratteristica

La funzione caratteristica, applicata a un insieme B , associa 1 ad ogni elemento del dominio che e' contenuto in B , e a tutti gli altri elementi associa 0.

$$\varphi_B(x) = \begin{cases} 1, & x \in B; \\ 0, & x \notin B. \end{cases}$$

2.10 Operazione binaria interna

Un'operazione binaria interna su A e' un'applicazione:

$$S : A \times A \rightarrow A$$

Ovvero $s((a, b)) \in A, \quad \forall (a, b) \in A \times A$.

3 Relazioni

3.1 Relazione binaria

Una *relazione binaria* su A e B e' un qualsiasi sottoinsieme di $A \times B$.

Per indicare che la coppia (x, y) appartiene alla relazione, e che quindi x e y sono in relazione, si puo' usare una delle seguenti scritture:

$$(x, y) \in R$$

$$x \stackrel{R}{\sim} y$$

$$x \stackrel{R}{\equiv} y$$

3.1.1 Esempio

$$R \subseteq N \times N$$

$$R = \{x | x \text{ divide } y \quad (y \text{ e' multiplo di } x)\}$$

$$(5, 10) \in R$$

$$(5, 7) \notin R$$

3.2 Relazione binaria interna

Una relazione su A e' interna quando

$$R \subseteq A \times A$$

3.3 Relazione binaria diagonale

Una relazione binaria diagonale e' definita come:

$$\begin{aligned} R &\subseteq A \times A \\ R &= \Delta_A = \{(a, a) \mid \forall a \in A\} \end{aligned}$$

3.4 Relazione binaria inversa

La relazione binaria inversa di una relazione R e' semplicemente la relazione R con le coppie invertite:

$$R^{-1} = \{(x, y) \mid (y, x) \in R\}$$

3.4.1 Esempio

$$(1, 0) \in R \quad \Leftrightarrow \quad (0, 1) \in R^{-1}$$

3.5 Composizione tra relazioni binarie interne

Possiamo anche comporre due o piu' relazioni:

$$\begin{aligned} R, S &\subseteq A \times A \\ R \circ S &= \{(x, y) \mid \exists z \in A (x, z) \in R \wedge (z, y) \in S\} \end{aligned}$$

3.5.1 Esempio

$$\begin{aligned} R, S &\subseteq A \times A, \quad A = \mathbb{N} \\ R &= \{(5, 7), (3, 2), (2, 1), (10, 20)\} \\ S &= \{(20, 1), (2, 4), (5, 7)\} \\ R \circ S &= \{(3, 4), (10, 1)\} \\ S \circ R &= \emptyset \end{aligned}$$

3.6 Relazione binaria interna riflessiva

$R \subseteq A \times A$ e' riflessiva se $\forall a \in A \Rightarrow a \stackrel{R}{\sim} a$, ovvero, quando ogni elemento $a \in A$ e' relazione con se stesso. Possiamo anche esprimere lo stesso concetto usando la relazione diagonale (vedi 3.3):

$$\Delta_A \in R$$

3.7 Relazione binaria interna simmetrica

$R \subseteq A \times A$ e' simmetrica se $a \stackrel{R}{\sim} b$ e $b \stackrel{R}{\sim} a$, ovvero $(a, b) \in R$ e $(b, a) \in R$. Possiamo anche dire la stessa cosa scrivendo:

$$R = R^{-1}$$

3.8 Relazione binaria interna antisimmetrica

$R \subseteq A \times A$ e' antisimmetrica se

$$a \stackrel{R}{\sim} b, \quad b \stackrel{R}{\sim} a \quad \Rightarrow \quad a = b$$

Ovvero, quando possiamo dedurre che a sia uguale a b dal fatto che a e b siano in relazione simmetricamente.

3.8.1 Esempio

$$\begin{aligned} x \stackrel{R}{\sim} y \quad \text{se} \quad y = mx, \quad \forall m \in R \\ y = mx, \quad x = ny \\ x = nmx \quad \Rightarrow \quad mn = 1 \quad \Rightarrow \quad x = x \end{aligned}$$

3.9 Relazione binaria interna transitiva

$R \subseteq A \times A$ e' transitiva se

$$a \stackrel{R}{\sim} b, \quad b \stackrel{R}{\sim} c \quad \Rightarrow \quad a \stackrel{R}{\sim} c$$

Possiamo anche definirla come quella relazione per cui vale

$$R \circ R \subseteq R$$

3.9.1 Esempio

$$\begin{aligned} x \stackrel{R}{\sim} y \quad \text{se} \quad y = mx, \quad \forall m \in R \\ y = mx, \quad z = ny \\ z = nmx \quad \Rightarrow \quad z \stackrel{R}{\sim} x \end{aligned}$$

Nell'ultima parte abbiamo visto che poiche' $z = nmx$, allora z e' in relazione con x .

4 Relazioni di equivalenza

Le relazioni che godono della proprieta' riflessiva (3.6), simmetrica (3.7) e transitiva (3.9), si chiamano *relazioni di equivalenza*.

4.1 Classe d'equivalenza

Consideriamo un insieme A e sia $R \subseteq A \times A$ una relazione d'equivalenza su A .

La classe d'equivalenza dell'elemento $a \in A$ e' definita come:

$$[a] = \{x \in A \mid x \stackrel{R}{\sim} a\}$$

Ovvero e' quel sottoinsieme di A , che contiene tutti gli elementi che sono in relazione con a .

Definiamo l'insieme quoziente di A su R come:

$$A/R = \{[a]_R \mid a \in A\}$$

ovvero, l'insieme di tutte le classi d'equivalenza indotte da R .

4.1.1 Proprieta'

1. Certamente possiamo dire che $[a] \neq \emptyset$, poiche' in $[a]$ esiste almeno a che e' in relazione con se stesso ($a \stackrel{R}{\sim} a$) per la proprieta' riflessiva della relazione d'equivalenza.
2. Due classi d'equivalenza distinte tra loro sono disgiunte:

$$[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$$

Proof: Supponiamo per assurdo che

$$[a] \cap [b] \neq \emptyset$$

da questo segue che:

$$\exists c \in [a], [b] \Leftrightarrow c \sim a, c \sim b \Leftrightarrow a \sim c, c \sim b \Rightarrow a \sim b$$

$$a \sim b \Rightarrow [a] = [b]$$

assurdo. □

3. $\bigcup_{a \in A} [a] = A$ (L'unione di tutte le classi di equivalenza che appartengono ad A formano lo stesso insieme A .)

Proof:

$\langle 1 \rangle \text{ Dim } \subseteq$

$$b \in \bigcup_{a \in A} [a] \Rightarrow \exists a \in A : b \in [a] \subseteq A \Rightarrow b \in A$$

$\langle 2 \rangle \text{ Dim } \supseteq$

$$b \in A \Rightarrow b \in [b] \subseteq \bigcup_{a \in A} [a]$$

□

4. Grazie alle precedenti tre proprieta' possiamo dire che A/R e' una partizione di A . (vedi 1.17)
5. La partizione P di A induce la seguente relazione di equivalenza:

$$x \sim y \Leftrightarrow \exists p \in P : x, y \in p$$

si vede facilmente che e' una relazione di equivalenza.

Proof:

$\langle 1 \rangle x \sim x$

$$x \sim x \Leftrightarrow \exists p \in P : x \in p$$

e questo e' vero perche'

$$x \in A = \bigcup_{p \in P} p$$

$\langle 2 \rangle x \sim y \Rightarrow y \sim x$

$$x \sim y \Leftrightarrow \exists p \in P : x, y \in p \Leftrightarrow y \sim x$$

$\langle 3 \rangle x \sim y, y \sim z \Rightarrow x \sim z$

$$x \sim y \Leftrightarrow \exists p \in P : x, y \in p$$

$$y \sim z \Leftrightarrow \exists p' \in P : y, z \in p'$$

$$y \in p, y \in p' \Rightarrow p \cap p' \neq \emptyset$$

ma poiche' gli elemnti di X sono a due a due disgiunti, segue che $p = p'$ e quindi

$$x, y, z \in p \Rightarrow x \sim z$$

5 Relazioni di ordine

Le relazioni che godono della proprieta' riflessiva (3.6), antisimmetrica (3.8) e transitiva (3.9), si chiamano *relazioni di ordine*.

Per dire che a e' in relazione d'ordine con b , si scrive: $a \leq b$. Nota che la relazione d'ordine $a \leq b$ puo' anche indicare una relazione diversa da quella dell'usuale minore-uguale.

Esempio

Diremo che $x \stackrel{R}{\sim} y$ se esiste un numero $z \in \mathbb{R}^+$ tale che $x + z = y$. In altre parole stiamo definendo la relazione di minore-uguale ($\leq$).

Dimostriamo che gode delle tre proprieta':

Riflessiva Deve essere che $x \leq x$, infatti:

$$x + 0 = x$$

Antisimmetrica Dobbiamo verificare che $x \leq y, \quad y \leq x \quad \Leftrightarrow \quad x = y$:

$$\begin{aligned} z_1, z_2 &\in \mathbb{R}^+ \\ x + z_1 &= y \\ y + z_2 &= x \end{aligned}$$

$$x + z_1 = x - z_2 \quad \Rightarrow \quad z_2 = z_1 = 0$$

Sostituendo z_2 e z_1 , nelle prime equazioni otteniamo: $x = y$ e $y = x$.

Transitiva Verifichiamo che $x \leq y, y \leq z \Rightarrow x \leq z$:

$$\begin{aligned} x + \alpha &= y \\ y + \beta &= z \\ x + \alpha &= z - \beta \\ x + (\alpha + \beta) &= z \quad \Rightarrow \quad x \leq z \end{aligned}$$

5.1 Insieme parzialmente ordinato

Per indicare che su un insieme A abbiamo fissato una relazione d'ordine $\leq$, si scrive $(A, \leq)$.

Se sull'insieme A e' stata fissata un relazione d'ordine, allora, e' un insieme **parzialmente ordinato**. In inglese si dice *Partially ordered Set* (**poset**).

5.2 Insieme totalmente ordinato

Un poset in cui due elementi sono sempre confrontabili ($a \leq b$, oppure $b \leq a$) si dice insieme totalmente ordinato (TOTET).

Un totet si dice anche *catena*.

5.2.1 Esempio

Associamo in R l'usuale rel. d'ordine minore-uguale:

$$(R, \leq)$$

Notiamo che se

$$x, y \in R$$

, allora o accade che:

$$x \leq y$$

oppure

$$y \leq x$$

. Quindi $(R, \leq)$ e' un insieme totalmente ordinato.

5.3 Minimo

Dato un poset $(A, \leq)$, un elemento $m \in A$ si dice minimo se:

$$m \leq x, \quad \forall x \in A$$

5.3.1 Proprieta'

Se il minimo esiste, allora e' unico

Proof: Supponiamo per assurdo che esistano due minimi m_1, m_2 , allora per la definizione di minimo deve accadere che:

$$m_1 \leq m_2$$

e

$$m_2 \leq m_1$$

Ma per la proprieta' antisimmetrica, otteniamo che

$$m_1 = m_2$$

□

5.4 Insieme ben ordinato

Se ogni sottoinsieme di $A \neq \emptyset$ possiede un minimo, allora A si dira' *insieme ben ordinato*.

Se A e' ben ordinato, segue che A e' anche totalmente ordinato. (ma non sempre il viceversa).

Proof: Supponiamo che A sia un insieme ben ordinato, e consideriamo il sottoinsieme

$$\{a, b\} \subseteq A, \quad \forall a, b \in A$$

. Allora, dato che per definizione questo ogni sottoinsieme di A deve avere un minimo, sara' che o $a \leq b$ oppure $b \leq a$. Si puo' ripetere questo ragionamento per ogni sottoinsieme di A , quindi A e' un insieme totalmente ordinato. □

5.5 Massimo

Dato un poset $(A, \leq)$, un elemento $M \in A$ si dice massimo se:

$$M \geq x, \quad \forall x \in A$$

Ovvero:

$$x \leq M, \quad \forall x \in A$$

5.5.1 Proprieta'

Se il massimo esiste, allora e' unico.

5.6 Minimale

Un elemento $a \in A$ di un poset $(A, \leq)$ si dice **minimale** se $\forall x \in A$ risulta

$$x \leq a, \Leftrightarrow x = a$$

Ovvero, oltre ad a , elementi "piu' piccoli" non ce ne sono. Od anche: se x e' l'unico elemento di A tale che $x \leq a$, allora x e' a stesso.

5.6.1 Proprieta'

Il minimo di un poset, e' l'unico minimale del poset stesso.

5.6.2 Esempio

$$A = \{5, 6, 10, 11, 12, 49\}$$

Definiamo il seguente poset:

$$(A, /)$$

dove $/$ e' la relazione di divisibilita' ($a \sim b$ se $\exists n \in \mathbb{N}^* | an = b$). Nel poset definito i minimali sono: 5, 6, 11, 49. Infatti, considerando il 5, la relazione $x/5$ vale solo per $5/5$, quindi 5 e' un elemento minimale.

5.7 Massimale

Un elemento $a \in A$ di un poset $(A, \leq)$ si dice **massimale** se $\forall x \in A$ risulta:

$$a \leq x, \Leftrightarrow x = a$$

Ovvero, oltre ad a , elementi "piu' grandi" non ce ne sono. Od anche: se x e' l'unico elemento di A tale che $a \leq x$, allora x e' a stesso.

5.7.1 Proprieta'

Il massimo di un poset, e' l'unico massimale del poset stesso.

5.7.2 Esempio

$$A = \{5, 6, 10, 11, 12, 49\}$$

Definiamo il seguente poset:

$$(A, /)$$

Nel poset definito i massimali sono: 10, 11, 12, 49. Infatti, considerando il 10, la relazione $10/x$ vale solo per $10/10$, quindi 10 e' un elemento massimale.

5.8 Minorante

Consideriamo un insieme A e un suo sottoinsieme $B \subseteq A$. Fissiamo in A una relazione d'ordine:

$$(A, \leq)$$

In B , possiamo fissare la stessa rel. d'ordine

$$(B, \leq)$$

Un elemento $l \in A$ si dice **minorante** di B se :

$$l \leq b, \quad \forall b \in B$$

5.8.1 Esempio

$$\begin{aligned} A &= (\mathbb{N}^*, /) \\ B &= \{20, 24, 28, 36\} \end{aligned}$$

I minoranti di B sono: 1, 2, 4.

5.9 Maggiorante

Consideriamo un insieme A e un suo sottoinsieme $B \subseteq A$. Fissiamo in A una relazione d'ordine:

$$(A, \leq)$$

In B , possiamo fissare la stessa rel. d'ordine

$$(B, \leq)$$

Un elemento $L \in A$ si dice **maggiorante** di B se :

$$b \leq L, \quad \forall b \in B$$

5.9.1 Esempio

$$\begin{aligned} A &= (\mathbb{N}^*, /) \\ B &= \{20, 24, 28, 36\} \end{aligned}$$

I maggioranti di B sono: 2520, $2520 * 2$, $2520 * 3$, $\dots$. Ovvero tutti i multipli del minimo comune multiplo dei numeri in B .

5.10 Estremo inferiore

Consideriamo un insieme A e un suo sottoinsieme $B \subseteq A$. Fissiamo in A una relazione d'ordine:

$$(A, \leq)$$

In B , possiamo fissare la stessa rel. d'ordine

$$(B, \leq)$$

Chiamiamo *Min* l'insieme di tutti i minoranti di B in A . Sappiamo che $\text{Min} \in A$.

Si dice **estremo inferiore** di B in A , il massimo dei suoi minoranti e si indica con $\inf B$

5.10.1 Esempio

$$A = (\mathbb{N}^*, /)$$

$$B = \{20, 24, 28, 36\}$$

I minoranti di B sono: 1, 2, 4. L'estremo inferiore di B in A e' 4 (ma non perche' 4 e' maggiore di 2 e di 1, ma perche' 1 divide 4 e 2 divide 4 e quindi 4, secondo la definizione e' il massimo dell'insieme $\{1, 2, 4\}$).

5.11 Estremo superiore

Si dice **estremo inferiore** di B in A , il minimo dei suoi maggioranti e si indica con $\sup B$.

5.12 POSET completo

$(A, \leq)$ e' un POSET completo $\Leftrightarrow$ per ogni sottoinsieme $\emptyset \neq B \subseteq A$ si ha $\exists \inf B, \exists \sup B$.

6 L'insieme $\mathbb{N}$

6.1 Assiomatizzazione di Peano

Definition 6.1. Consideriamo un insieme N che goda delle seguenti proprieta':

1. Esiste la seguente applicazione iniettiva:

$$s : N \rightarrow N$$

Chiameremo l'immagine dell'elemento n il successivo di n : $s(n) = \text{successivo di } n$.

2. L'insieme $N \setminus \text{Im}(s)$ contiene un solo elemento. ($\text{Im}(s)$ e' l'immagine di s). Chiameremo quest'unico elemento *zero* e lo indicheremo con **0**.
In altre parole, lo zero e' l'unico elemento che non e' il successivo di nessun altro elemento.

3. **Principio (o assioma) di induzione.**

Per ogni sottoinsieme $U \subseteq N$ per cui valgono le seguenti proposizioni

(a) $\mathbf{0} \in U$

(b) $u \in U \Rightarrow s(u) \in U$

si ha che $U = N$

Un insieme N , con le suddette proprieta' si dira' "insieme dei numeri naturali".

Nota: il principio di induzione e' un assioma perche' N e' *infinito*. Se N fosse stato finito, allora non avremmo avuto alcun bisogno del principio di induzione.

Example 6.2. Non esiste un solo insieme di numeri naturali. Infatti,

1. L'insieme $\{0, 1, 2, 3, 4, \dots\}$ e' un insieme di numeri naturali. La funzione $s()$ e' quella standard:

$$1 \mapsto 2 \mapsto 3 \mapsto \dots$$

E lo zero e' $\mathbf{0} = 0$.

2. Anche l'insieme $\{2, 4, 6, 8, \dots\}$ e' un insieme di numeri naturali. La funzione $s()$ e'

$$0, \mapsto 2 \mapsto 4 \mapsto 6 \mapsto$$

Lo zero e' $\mathbf{0} = 2$

3. Anche i seguenti insiemi sono insiemi naturali:

$$\begin{aligned} &\{5, 6, 7, \dots\} \\ &\{5, 10, 15, 20, \dots\} \end{aligned}$$

Definition 6.3. Definiamo il seguente insieme:

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

Come abbiamo visto prima $\mathbb{N}$ e' un insieme di numeri naturali. Da ora in poi, "l'insieme dei numeri naturali" sara' $\mathbb{N}$.

Nota: $0, 1, 2, \dots$, sono solo dei simboli.

6.2 Dimostrazione per induzione

Proposition 6.4. Sia N un qualsiasi insieme di numeri naturali, sia $\mathbf{0}$ lo zero e $s()$ la funzione successivo, allora

$$\begin{cases} P(\mathbf{0}) \\ P(n) \Rightarrow P(s(n)) \end{cases} \Rightarrow P(n) \quad \forall n \in N$$

In altre parole, per provare che una proposizione $P(n)$ e' vera $\forall n \in N$, si puo' procedere cosi':

1. Si dimostra $P(\mathbf{0})$
2. Si dimostra $P(n) \Rightarrow P(s(n))$

ovvero

1. Dimostro che $P(\mathbf{0})$ e' vera
2. Suppongo vera $P(n)$
3. Dimostro che $P(s(n))$ e' vera
4. A questo punto possiamo affermare che $U = N$

Proof: Consideriamo l'insieme

$$U = \{n \mid P(n) \text{ e' vera}\}$$

Per ipotesi:

$$\begin{aligned} P(\mathbf{0}) \text{ vera} &\Rightarrow \mathbf{0} \in U \\ (P(n) \Rightarrow P(s(n))) &\Leftrightarrow (n \in U \Rightarrow s(n) \in U) \\ \begin{cases} \mathbf{0} \in U \\ n \in U \Rightarrow s(n) \in U \end{cases} &\xRightarrow{\text{assioma di induzione}} U = N \\ U = N &\Leftrightarrow \forall n \in N \quad P(n) \text{ e' vera} \end{aligned}$$

□

Example 6.5. Sia $N = \mathbb{N}$, ovvero $N = \{1, 2, 3, \dots\}$. Dimostriamo che la somma dei primi n numeri dispari e' pari a n^2 . (Nota¹)

Proof: Ecco la prova.

1. Verifichiamo direttamente $P(1)$ e $P(2)$:

$$\begin{aligned} 1 &= 1^2 \\ 1 + 3 &= 2^2 \end{aligned}$$

2. Suppiamo che la seguente identita' sia vera:

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

3. Dimostriamo che quest'ultima identita' e' vera anche per $n + 1$:

$$\underbrace{1 + 3 + \dots + (2n - 1)}_{n^2} + (2(n + 1) - 1) = (n + 1)^2$$

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

$$n^2 + 2n + 1 = n^2 + 2n + 1$$

$$0 = 0$$

q.e.d

□

6.3 Principii di induzione

Proposition 6.6. Sia N un insieme di numeri naturali, $\mathbf{0}$ lo zero e $s()$ la funzione successivo. Allora, le seguenti proposizioni sono equivalenti:

1. Induzione: $\forall U \subseteq N$

$$\begin{cases} \mathbf{0} \in U \\ n \in U \Rightarrow s(n) \in U \end{cases} \Rightarrow U = N$$

2. Induzione forte: $\forall U \subseteq N$

$$\begin{cases} \mathbf{0} \in U \\ \{k \in N \mid \mathbf{0} \leq k < n\} \subseteq U \Rightarrow n \in U \end{cases} \Rightarrow U = N$$

3. Buon ordinamento di N :

N e' un insieme ben ordinato secondo la relazione $\leq$ (vedi [5.4,pg.19])

La relazione d'ordine $(N, \leq)$ e' quella usuale:

$$a \leq b \Leftrightarrow \exists c \in N : a + n = b$$

L'operazione $+$ e' definita in [6.5,pg.27]

Proof: Bastera' dimostrare $2. \Rightarrow 1. \Rightarrow 3. \Rightarrow 2$

(1) Dim $2. \Rightarrow 1.$

Sia $U \subseteq N$. Dobbiamo dimostrare l'implicazione

$$\begin{cases} \mathbf{0} \in U \\ n \in U \Rightarrow s(n) \in U \end{cases} \Rightarrow U = N$$

¹in effetti, non abbiamo ancora definito la somma di numeri naturali, ne' i numeri pari o dispari. Per semplicita', in questo esempio, usiamo i concetti usuali.

Supponiamo che la premessa sia vera:

$$\begin{cases} \mathbf{0} \in U \\ n \in U \Rightarrow s(n) \in U \end{cases} \quad (1)$$

e dimostriamo $U = N$ sfruttando la 2.

Supponiamo che

$$\{k \in N \mid \mathbf{0} \leq k < s(n)\} \subseteq U$$

allora,

$$n \in N \Rightarrow \mathbf{0} \leq n < s(n) \Rightarrow n \in \{k \in N \mid \mathbf{0} \leq k < s(n)\} \subseteq U \Rightarrow n \in U \underset{(1)}{\Rightarrow} s(n) \in U$$

Così facendo abbiamo dimostrato l'implicazione:

$$\{k \in N \mid \mathbf{0} \leq k < s(n)\} \subseteq U \Rightarrow s(n) \in U \quad (*)$$

Allora, anche la seguente implicazione è vera:

$$\{k \in N \mid \mathbf{0} \leq k < m\} \subseteq U \Rightarrow m \in U \quad (2)$$

infatti, se $m = \mathbf{0}$,

$$\{k \in N \mid \mathbf{0} \leq k < \mathbf{0}\} = \emptyset \subseteq U \Rightarrow \mathbf{0} \in U$$

$$\emptyset \subseteq U \Rightarrow \mathbf{0} \in U \quad [\text{che è vera per la (1)}]$$

se invece $m \neq \mathbf{0}$,

$$m \neq \mathbf{0} \quad \underbrace{\Rightarrow}_{\text{Il assioma di Peano}} \quad m \in \text{Im } s \Leftrightarrow \exists n : m = s(n)$$

E quindi la (*) si riscrive come:

$$\{k \in N \mid \mathbf{0} \leq k < s(n)\} \subseteq U \Rightarrow s(n) \in U$$

ovvero la (2).

Adesso entra in gioco la 2.:

$$(1) \Rightarrow \mathbf{0} \in U$$

$$\begin{cases} \mathbf{0} \in U \\ (2) \end{cases} \quad \underbrace{\Rightarrow}_{2.} \quad U = N$$

che era ciò che volevamo dimostrare.

(2) Dim. 1. $\Rightarrow$ 3.

Sia $U \subseteq N$, $U \neq \emptyset$. Dobbiamo dimostrare che U ha il minimo.

Sia

$$T = \{t \in N \mid t \leq u \quad \forall u \in U\} \quad \text{l'insieme dei minoranti di } U$$

$$\mathbf{0} \leq n \quad \forall n \in N \Rightarrow \mathbf{0} \in T \Rightarrow T \neq \emptyset$$

CASE: Supponiamo vera l'implicazione $t \in T \Rightarrow s(t) \in T$

Se $t \in T \Rightarrow s(t) \in T$, si ha

$$\begin{cases} \mathbf{0} \in T \\ t \in T \Rightarrow s(t) \in T \end{cases} \quad \underbrace{\Rightarrow}_{1.} \quad T = N \Rightarrow U \subseteq T \Rightarrow \exists \min U$$

CASE: Supponiamo falsa l'implicazione $t \in T \Rightarrow s(t) \in T$

Ovvero $\exists t \in T : s(t) \notin T$.

$$t \in T \Rightarrow t \leq u \quad \forall u \in U \quad (1)$$

CASE: $\exists u \in U : t = u$

In questo caso, $t = \min U$ e non abbiamo più nulla da dimostrare.

CASE: $t \neq u \quad \forall u \in U$

In questo caso, la (1) diventa

$$t < u \quad \forall u \in U \Leftrightarrow s(t) \leq u \quad \forall u \in U \Rightarrow s(t) \in T$$

assurdo.

(3) Dim 3. $\Rightarrow$ 2.

Sia $U \subseteq N$. Dobbiamo dimostrare la seguente implicazione:

$$\begin{cases} \mathbf{0} \in U \\ \{k \in N \mid \mathbf{0} \leq k < n\} \subseteq U \Rightarrow n \in U \end{cases} \Rightarrow U = N$$

Supponiamo vera la premessa:

$$\begin{cases} \mathbf{0} \in U \\ \{k \in N \mid \mathbf{0} \leq k < n\} \subseteq U \Rightarrow n \in U \end{cases} \quad (1)$$

e dimostriamo $U = N$.

Supponiamo per assurdo che $U \neq N$. Sia $V = N \setminus U$

$$U \neq N \Rightarrow V \neq \emptyset \xRightarrow{3.} \exists m = \min V$$

Consideriamo l'insieme $K = \{k \in N \mid \mathbf{0} \leq k < m\}$

$$k \in K \Rightarrow k < m = \min V \Rightarrow k \notin V = N \setminus U \xRightarrow{k \in N} k \in U$$

$$\forall k \in K \quad k \in U \Rightarrow K \subseteq U \xRightarrow{(1)} m \in U$$

$$m = \min V \Rightarrow m \in V$$

$$m \in U, m \in V = N \setminus U$$

assurdo.

□

Proposition 6.7. Alcune precisazioni sul principio di induzione forte.

Sia N un qualsiasi insieme di numeri naturali, sia $\mathbf{0}$ lo zero e $s()$ la funzione successivo.

Analogamente a come abbiamo fatto in [6.2,pg.23], possiamo sfruttare l'Induzione forte per dimostrare $P(n) \quad \forall n \in N$. Infatti, si ha:

$$\begin{cases} P(\mathbf{0}) \\ (P(k) \quad \forall k : \mathbf{0} \leq k < n) \Rightarrow P(n) \end{cases} \Rightarrow P(n) \quad \forall n \in N$$

Il metodo e' quindi:

1. Dimostro che $P(\mathbf{0})$ e' vera
2. Suppongo vera $P(k)$ per tutte le k che sono $\mathbf{0} \leq k < n$
3. Dimostro che $P(n)$ e' vera
4. A questo punto possiamo affermare che $U = N$

In alcune situazioni questo metodo risulta piu' semplice di quello di induzione debole, infatti, il passo la 2. permette di supporre vera $P(k)$ per tutti i k minori di n . Invece, il principio di induzione debole, permette solo di supporre vera $P(n-1)$.

Proof: Si procede analogamente alla dimostrazione di [6.2,pg.23].

□

6.4 Altre note sull'induzione

L'induzione e' un assioma. Non si puo' dimostrare a partire dalla teoria degli insiemi (ZFC), ne' dai due primi assiomi di Peano. Ecco un appunto che chiarifica la situazione:

The four statements I give below are all equivalent, meaning that if you assume one of them to be true, the others follow as consequences, but none of them can be proven from the other fundamental axioms in Zermelo-Fraenkel set theory alone.

Axiom of Choice

Given a collection of nonempty sets A , it is possible to form a new set that includes one element from every set in A .

Zorn's Lemma

If in a set A it is possible to give a partial ordering of this set (a partial ordering is analogous to the relationship "less than or equal" in the real numbers) and if every chain of partially ordered elements in A has an upper bound (an upper bound is an element p such that all elements in the chain are "less than or equal" to p) then A has a maximal element (means that there is an element m in A such that all other elements in A are "less than or equal" to m).

Well-Ordering Principle

Every nonempty subset of the natural numbers (positive integers) contains a least member.

Mathematical Induction

If A is a subset of natural numbers such that

i) 1 is in A

ii) if a natural number k is in A then $k + 1$ must also be in A

Then A is the set of natural numbers.

6.5 Addizione in $\mathbb{N}$

Definiamo l'operazione (vedi 2.10) di addizione che indichiamo con il simbolo $+$.

$$add : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$m + n \in \mathbb{N} \quad \forall (m, n) \in \mathbb{N} \times \mathbb{N}$$

Costruiamo per induzione su n , l'operazione di addizione.

Base dell'induzione : $m + 0 = m$

Conoscendo $m + u$, $m + s(u) = s(m + u)$

Esempio

$$m + 1 = s(m + 0) = s(m) \Rightarrow m + 1 = s(m)$$

6.5.1 Proprieta' dell'addizione

Associativa : $(m + n) + p = m + (n + p)$

Proof: Dimostriamo la proprieta' associativa per induzione su p .

1. $(m + n) + 0 = m + (n + 0)$, poiche' per la definizione di addizione $m + 0 = m$, possiamo riscriverla come:

$$m + n = m + n$$

Quindi la proprieta' associativa e' dimostrata per $p = 0$

2. Supponiamo che $(m + n) + p = m + (n + p)$ sia vera.
3. Dimostriamo la precedente per $p + 1$:

$$(m + n) + s(p) = m + (n + s(p))$$

$$s(\underbrace{(m + n) + p}_{m + (n + p)}) = m + s(n + p)$$

$$s(m + (n + p)) = m + s(n + p)$$

$$m + s(n + p) = m + s(n + p)$$

$$0 = 0$$

□

Commutativa : $m + n = n + m$

Legge di cancellazione : $m + p = n + p \Rightarrow m = n$

6.6 Moltiplicazione

$$mul : N \times N \rightarrow N$$

$$mn \in N \quad \forall (m, n) \in N \times N$$

Costruiamo per induzione su n , l'operazione di moltiplicazione.

Base dell'induzione : $m0 = 0$

Conoscendo mu , $ms(u) = mu + m$

Esempio

$$m1 = ms(0) = m0 + m = m$$

$$m2 = ms(1) = m1 + m = m + m$$

$$m3 = ms(2) = m2 + m = m + m + m$$

6.6.1 Proprieta' della moltiplicazione

Associativa : $(mn)p = m(np)$

Commutativa : $mn = nm$

Distributiva del prodotto rispetto all'addizione : $m(n + p) = mn + mp$

Legge di cancellazione : Se $m = n \Rightarrow mp = np$

Se $mp = np \wedge p \neq 0 \Rightarrow m = n$

6.7 Elemento neutro

Lo 0 e' l'elemento neutro dell'addizione perche' $m + 0 = m$.

Lo 1 e' l'elemento neutro della moltiplicazione perche' $m1 = m$.

7 Teoria della divisibilita'

7.1 Divisibilita'

Definiamo la relazione d'ordine di divisibilita':

$$a/b \Leftarrow \exists n \in \mathbb{N}^* | an = b$$

7.1.1 Proprieta'

1. Poiche' la divisibilita' e' una relazione d'ordine, gode della proprieta' antisimmetrica e quindi: $a/b \wedge b/a \Rightarrow b = a$.

2.

$$c/a \Rightarrow c/ma$$

ovvero c divide anche i multipli di

3.

$$c/x, c/y \Rightarrow c/(x+y)$$

Proof:

$$x = cq_1 + r_1$$

$$y = cq_2 + r_2$$

$$x + y = cq_1 + r_1 + cq_2 + r_2$$

$$x + y = c(q_1 + q_2) + (r_1 + r_2) \Rightarrow c/(x+y)$$

□

4.

$$\begin{cases} x = y + z \\ c/x, c/y \end{cases} \Rightarrow c/z$$

Proof:

$$x = cq_1, \quad y = cq_2$$

$$x = y + z \Rightarrow cq_1 = cq_2 + z$$

$$c(q_1 - q_2) = z \Rightarrow c/z$$

□

5. Questa proprieta' utilizza concetti che vedremo piu' avanti:

$$\begin{cases} a = bc \\ d/a, d \nmid b \\ (d, b) = 1 \end{cases} \Rightarrow d/c$$

Proof: Per Bezout (vedi [9.1,pg.42]) abbiamo

$$(d, b) = 1 \Leftrightarrow 1 = \lambda d + \mu b$$

$$c = \lambda dc + \mu bc$$

$$\begin{cases} d/\mu bc = \mu a \\ d/\lambda dc \end{cases} \Rightarrow d/(\lambda dc + \mu bc) = c$$

□

7.2 Massimo Comune Divisore

Il MCD e' definito il questo modo:

$$a, b, d, d' \in \mathbb{N}$$

$$d = MCD(a, b) \Leftrightarrow d/a \wedge d/b \wedge ((d'/a \wedge d'/b) \Rightarrow d'/d)$$

Ovvero, d e' un MCD di a e b se divide sia a sia b e se e' diviso da qualsiasi altro divisore comune ad a e a b .

7.2.1 Proprieta'

Il MCD esiste sempre ed e' unico.

Proof: Dobbiamo dimostrare che se d_1 e d_2 sono $MCD(a, b)$, allora $d_1 = d_2$.

d_1 e' $MCD(a, b)$ e quindi per definizione d_2/d_1 .

d_2 e' $MCD(a, b)$ e quindi per definizione d_1/d_2 . Allora per la proprieta' asym segue che: $d_2 = d_1$

□

7.3 Algoritmo di divisione in $\mathbb{N}$

Data una coppia $(a, b) \in \mathbb{N}^2$, $b \neq 0$, allora esistono e sono unici due

$$q, r \in \mathbb{N} \mid a = bq + r$$

Proof: Definiamo l'insieme T :

$$T = \{x \in \mathbb{N} \mid xb > a\}$$

Sicuramente $T \neq \emptyset$ perche' contiene almeno $a + 1$. Inoltre, $T \subset \mathbb{N}$, quindi dato che $\mathbb{N}$ e' ben ordinato, sappiamo che T avra' un minimo

$$q' = \min T \neq 0$$

. Quindi q' e' almeno il successivo di qualche numero q :

$$q' = q + 1$$

Ma $q \notin T$ perche' q' e' il minimo di T , allora:

$$qb \leq a \Rightarrow \exists r \mid qb + r = a$$

E questo conclude la prima parte della dimostrazione. Ora dimostriamo che $r < b$.

$$\begin{aligned}
 q'b &> a \\
 a &< q'b \\
 a &= qb + r \\
 qb + r &< q'b \\
 qb + r &< (q+1)b \\
 qb + r &< qb + b \\
 r &< b
 \end{aligned}$$

□

Proof: Dimostriamo adesso che il q ed r sono unici. Supponiamo per assurdo che:

$$\begin{aligned}
 r &< b \\
 r' &< b' \\
 q \neq q' &\Rightarrow q < q' \Rightarrow q + n = q', \quad n \neq 0 \\
 a &= qb + r = q'b + r' \\
 qb + r &= (q+n)b + r' \\
 qb + r &= bq + nb + r' \\
 r &= nb + r' \\
 (r = nb + r') &\geq b \\
 r &\geq b
 \end{aligned}$$

E l'ultima diseuguaglianza e' un assurdo perche' abbiamo prima dimostrato che $r < b$. Quindi q e r sono unici. □

7.4 Algoritmo Euclideo per il MCD

Dati $a, b \neq 0$, ecco l'algoritmo in Calc:

```

define MCD(a,b) {
    return !b ? a : MCD(b, a%b);
}

```

Le operazioni che esegue:

$$\begin{aligned}
 a &= bq_1 + r_1 \\
 b &= r_1q_2 + r_2 \\
 r_1 &= r_2q_3 + r_3 \\
 r_2 &= r_3q_4 + r_4 \\
 &\vdots \\
 r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \\
 r_{n-2} &= r_{n-1}q_n + r_n \\
 r_{n-1} &= r_nq_{n+1} + 0
 \end{aligned}$$

Il MCD di a, b sara' l'ultimo resto non nullo, ovvero r_n .

Proof: Intanto osserviamo che l'algoritmo finisce sempre compiendo un numero finito di passi, infatti, come abbiamo visto nella sezione 7.3, sappiamo che $r < b$, quindi:

$$\begin{aligned} r_1 &< b \\ r_2 &< r_1 \\ r_3 &< r_2 \\ &\vdots \end{aligned}$$

Dato che stiamo operando in $\mathbb{N}$, prima o poi si arriverà allo zero. Il numero massimo di passaggi è b .

Dobbiamo dimostrare che r_n è il $MCD(a, b)$, quindi deve accadere che r_n/a e r_n/b . Prima di tutto sappiamo che r_n/r_{n-1} perché:

$$r_{n-1} = r_n q_{n+1} + 0$$

E quindi divide anche $r_{n-1}q_n$ e se stesso r_n , quindi per la proprietà della divisibilità divide anche $r_{n-1}q_n + r_n$ che corrisponde a r_{n-2} .

Per lo stesso motivo r_n divide $r_{n-2}q_{n-1}$ e r_{n-1} , e quindi divide r_{n-3} . Procedendo a questo modo si risale tutta la scala delle operazioni e si arriva a r_n/a e r_n/b . Ovvero abbiamo dimostrato che r_n è un divisore comune di a e di b . Adesso dobbiamo dimostrare che se esiste un altro divisore comune, allora dividerà r_n . Supponiamo che quest'altro divisore comune si chiami c .

$$a = \lambda c$$

$$b = \mu c$$

$$a = bq_1 + r_1 \Rightarrow \lambda c = \mu c q_1 + r_1 \Rightarrow c/r_1$$

Quindi c/r_1 (c divide r_q), e dato che $b = r_1 q_2 + r_2$, vuol dire che c/r_2 , e poiché $r_1 = r_2 q_3 + r_3$ allora c/r_3 . Procedendo in questa maniera si arriva a c/r_n . $\square$

8 Teoria degli insiemi

8.1 Cardinalità (o Potenza)

Con la notazione, $\underline{n}$ intendiamo il seguente insieme:

$$\underline{n} = \{0, 1, 2, \dots, n-1\}$$

Così ad esempio, $\underline{4} = \{0, 1, 2, 3\}$.

Diamo la definizione di cardinalità dell'insieme A , che indichiamo con $|A|$:

$$|A| = \underline{n} \Leftrightarrow \exists f : A \leftrightarrow \underline{n}$$

Ovvero, l'insieme $|A|$ ha cardinalità n se esiste un'applicazione biettiva che associa a ogni elemento di A un elemento di $\underline{n}$. Se l'insieme A è finito, $|A|$ è uguale al numero degli elementi contenuti in A , se invece non è finito si scrive

$$|A| = \infty$$

8.2 Insieme finito (infinito)

Un insieme A è finito se è possibile porlo in relazione biunivoca con un $\underline{n} \in \mathbb{N}$, altrimenti si dice infinito.

È possibile usare anche questa definizione: un insieme A si dice infinito se è possibile porre in relazione biunivoca l'insieme stesso con un suo sottoinsieme proprio ($\neq A$).

8.2.1 Esempio

Poiche' possiamo porre in corrispondenza biunivoca l'insieme $2\mathbb{N}$ con l'insieme $\mathbb{N}$ deduciamo che $2\mathbb{N}$ e' infinito. ($2\mathbb{N}$ e' l'insieme dei numeri pari).

8.3 Insieme numerabile

A si dice numerabile se:

$$\exists \varphi : A \leftrightarrow \mathbb{N}$$

8.3.1 Proprieta'

1. In ogni insieme infinito esiste un sottoinsieme numerabile.

Proof: Supponiamo che X sia il nostro insieme infinito. Allora prendiamo un elemento $b_1 \in X$. Poi prendiamo un altro elemento b_2 dal sottoinsieme $X \setminus \{b_1\}$. Poi $b_3 \in (X \setminus \{b_1\}) \setminus \{b_2\}$. E cosi' via.

Per l'assioma della scelta esistera' un unico insieme che contiene:

$$b_1, b_2, \dots, b_t$$

E questo e' proprio il nostro insieme numerabile. $\square$

2. Se X e' infinito e A e' finito o numerabile, allora $|X \cup A| = |X|$.

Proof: Dobbiamo dimostrare che esiste una funzione biettiva tra $X \cup A$ e X .

Sia $B \subset X$ numerabile (abbiamo visto nella proprieta' 1 che in un insieme infinito B esiste).

Quindi sia

$$B = \{b_1, b_2, \dots, b_t\}$$

Adesso scegliamo questa applicazione:

$$f(x) = \begin{cases} x & x \notin B \\ b_{2i} & x \in B \\ b_{2i+1} & x \in A \end{cases}$$

A questo punto e' facile vedere come prendendo dei qualsiasi valori da $X \cup \{a_1, a_2, \dots, a_s\}$ questa applicazione rimanga biettiva. $\square$

8.4 Insiemi equipotenti

Due insieme A e B sono equipotenti se e' possibile stabilire una relazione biunivoca tra di loro, ovvero se:

$$|A| = |B| \Leftrightarrow \exists \varphi : A \leftrightarrow B$$

Possiamo quindi dire che A e' numerabile se e' equipotente a $\mathbb{N}$.

Definiamo anche le seguenti relazioni:

$$|A| \leq |B| \Leftrightarrow \exists \varphi : A \hookrightarrow B$$

$$|A| < |B| \Leftrightarrow \exists \varphi : A \hookrightarrow B, \nexists \psi : A \leftrightarrow B$$

$$|A| \geq |B| \Leftrightarrow \exists \varphi : A \twoheadrightarrow B$$

$$|A| > |B| \Leftrightarrow \exists \varphi : A \twoheadrightarrow B, \nexists \psi : A \leftrightarrow B$$

8.4.1 Proprieta'

1. $|A| < |P(A)| \quad \forall A$.

Questo e' il teorema di Cantor.

Proof: Basta dimostrare che

$$\exists \varphi : A \hookrightarrow P(A), \quad \nexists \psi : A \mapsto P(A)$$

La prima parte e' semplice, perche' dobbiamo trovare almeno una φ iniettiva. Scegliamo allora una funzione $f(a)$ che ritorna un insieme che contiene a :

$$f(a) = \{a\}$$

Dimostriamo che e' iniettiva:

$$x, y \in A$$

$$f(x) = f(y) \Rightarrow \{x\} = \{y\} \Rightarrow x = y$$

E dato che $\{x\}, \{y\} \in P(A)$, possiamo concludere che:

$$|A| \leq |P(A)|$$

Per la seconda parte ragioniamo per assurdo: supponiamo che esiste una funzione surriettiva $\psi : A \mapsto P(A)$. Prendiamo l'insieme B che contiene tutti gli elementi che sono in A ma non nella loro immagine di ψ :

$$B = \{x \in A \mid x \notin \psi(x)\} \subseteq A$$

$$B \subseteq A \Rightarrow B \in P(A)$$

Per l'ipotesi della surriettivita' di ψ possiamo scrivere:

$$\exists y \in A \mid \psi(y) = B$$

Ora possono verificarsi due casi: 1) $y \in B$ 2) $y \notin B$. Analizziamoli:

$y \in B$ Per la definizione di B , allora accade che $y \notin \psi(y)$, ma $\psi(y) = B$. E questo e' assurdo, perche' y non puo' contemporaneamente appartenere e non appartenere a B .

$y \notin B$ Per la definizione di B : $y \in \psi(y) = B$. Il che e' assurdo.

Dato che abbiamo trovato un assurdo in entrambi i casi, vuol dire che la nostra ipotesi e' assurda, ovvero ψ non e' surriettiva. $\square$

2. $|P(A)| = |2^A|$ Dove 2^A e' l'insieme di tutte le applicazioni che vanno da A a 2 .

Proof: Dobbiamo dimostrare che $P(A)$ e 2^A sono equipotenti, ovvero che esiste un'applicazione biettiva tra di loro.

Intanto diamo un po' di definizioni.

$$\varphi_B(x) = \begin{cases} 1, & x \in B; \\ 0, & x \notin B. \end{cases}$$

φ_B e' la funzione caratteristica.

Definiamo A_f :

$$f \in 2^A$$

$$A_f = \{a \in A \mid f(a) = 1\}$$

$$A_f \subseteq A \Rightarrow A_f \in P(A)$$

Ora scegliamoci due funzioni opportune:

$$\varphi : P(A) \rightarrow 2^A, \quad \forall B \in P(A) \quad \varphi(B) = \varphi_B$$

$$\psi : 2^A \rightarrow P(A), \quad \forall f \in 2^A \quad \psi(f) = A_f \in P(A)$$

Se riuscissimo a dimostrare che

$$\varphi \circ \psi = 1_{2^A} \tag{1}$$

$$\psi \circ \varphi = 1_{P(A)} \tag{2}$$

vorrebbe dire che ψ e' biettiva, e quindi avremmo finito.

Cominciamo con la (1). Dobbiamo verificare che:

$$\forall f \in 2^A, \quad \varphi \circ \psi(f) = f \quad \Rightarrow \quad [\varphi \circ \psi(f)](a) = f(a), \quad \forall a \in A$$

Procediamo per sostituzione:

$$[\varphi(A_f)](a) = \varphi_{A_f}(a) = \begin{cases} 1 & a \in A_f \\ 0 & a \notin A_f \end{cases}$$

Notiamo che se $a \in A_f$ allora $f(a) = 1$ (per la stessa definizione di A_f), ovvero, in questo caso $f(a) = \varphi_{A_f}(a)$.

Se $a \notin A_f$ allora $f(a) = 0$, quindi, anche in questo caso $f(a) = \varphi_{A_f}(a)$.

Dato che in entrambi i casi $f(a)$ coincide con la composizione, possiamo concludere che $[\varphi \circ \psi(f)](a) = f(a)$ e quindi che $\varphi \circ \psi = 1_{2^A}$.

Ok, adesso abbiamo finito la prima parte della dimostrazione, ci resta da verificare che

$$\psi \circ \varphi = 1_{P(A)} \quad \Rightarrow \quad \forall B \in P(A), \quad \psi \circ \varphi(B) = B$$

Sostituiamo:

$$\psi \circ \varphi(B) = \psi(\varphi_B) = A_{\varphi_B}$$

Ma A_{φ_B} e' l'insieme che contiene tutti gli elementi $a \in A$ tale che $\varphi_B(a) = 1$, ovvero contiene tutti gli elementi che stanno in A e in B . Ma dato che $B \in P(A)$, B e' un sottoinsieme di A , quindi "tutti gli elementi che stanno in A e in B " formano l'insieme B stesso. In poche parole:

$$A_{\varphi_B} = B$$

Che e' quello che volevamo dimostrare.

Fine dimostrazione $\hat{_}$

□

8.5 Diagonalizzazione di Cantor

Proposition 8.1. *Vale il seguente teorema:*

$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$$

che si puo' facilmente estendere per induzione:

$$|\mathbb{N}| = |\mathbb{N}^n| \quad \forall n \in \mathbb{N}$$

Queste formule definiscono una relazione biettiva tra $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$:

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad n = f(a, b) = \binom{a+b+1}{2} + a$$

Per l'inverso conosciamo n e vogliamo calcolare a e b :

$$T = \left\{ x \mid \binom{x}{2} \leq n \right\}$$

$$d = \max T$$

$$g : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$$

$$a = n - \binom{d}{2}$$

$$b = d - a - 1$$

Piu' in generale, vale il seguente risultato: considerato l'insieme

$$A = \{A_1, A_2, \dots, \}$$

si ha

$$|A| = |A_i| = |\mathbb{N}| \quad \forall A_i \in A \Rightarrow \left| \bigcup_{A_i \in A} A_i \right| = |\mathbb{N}|$$

ovvero, l'unione di un numero finito o infinitamente numerabile di insiemi numerabili, e' ancora un insieme numerabile.

Ad esempio,

$$\mathbb{Z} = \mathbb{N} \cup \{-1, -2, \dots\}$$

quindi $\mathbb{Z}$ e' numerabile.

Proposition 8.2. $|\mathbb{R}| = |\mathbb{R}^n|$

Proof:

(1) Dimostriamo che $|[0, 1]| = |[0, 1] \times [0, 1]|$

Rappresentiamo ogni numero reale $\alpha \in [0, 1]$ come

$$\alpha = 0, d_1 d_2 d_3 \dots, \quad d_i \in 0, 1, \dots, 9$$

I numeri razionali non periodici, li rappresentiamo con infiniti 9 al posto dello zero finale, ad esempio:

$$0.5 = 0.50 = 0.59999 \dots$$

Consideriamo $(a, b) \in [0, 1] \times [0, 1]$,

$$a = 0.a_1 a_2 \dots$$

$$b = 0.b_1 b_2 \dots$$

Raggruppiamo le cifre decimali di a con la seguente legge: partendo da un a_i , consideriamo $a_{i+1}, a_{i+2}, \dots$, fino a quando non giungiamo a $a_{i+j} \neq 0$. Il gruppo creato e' $A_1 = a_i a_{i+1} \dots a_{i+j}$. Il prossimo gruppo verra' creato a partire da a_{i+j+1} , e cosi' via...

Procediamo allo stesso modo per b .

Creiamo il seguente numero reale $c \in [0, 1]$:

$$a = 0.A_1 A_2 \dots$$

$$b = 0.B_1 B_2 \dots$$

$$c = 0.A_1 B_1 A_2 B_2 \dots$$

Ad esempio,

$$a = 0.12034100100089 \dots = 0. \ 1 \ 2 \ 03 \ 4 \ 1 \ 001 \ 0008 \ 9 \dots$$

$$b = 0.0330041301 \dots = 0. \ 03 \ 3 \ 004 \ 1 \ 3 \ 01 \ \dots$$

$$c = 0. \ 1 \ 03 \ 2 \ 3 \ 03 \ 004 \ 4 \ 1 \ \dots$$

Abbiamo cosi' definito una legge $f : [0, 1] \times [0, 1] \rightarrow [0, 1]$.

f e' invertibile, e quindi biettiva, infatti, dato

$$f(a, b) = c = 0.c_1 c_2 \dots$$

possiamo scomporre le cifre decimali di c usando la stessa legge di prima. Otteniamo cosi' $C_1, C_2, \dots$. Quindi

$$f^{-1}(c) = (a, b)$$

con

$$a = 0.C_1 C_3 C_5 \dots$$

$$b = 0.C_2 C_4 C_6 \dots$$

E' chiaro che

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

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

(2) Q.E.D.

In topologia.pdf (1.19 Omeomorfismo) abbiamo visto che due intervalli qualsiasi di $\mathbb{R}$ sono omeomorfi, e quindi equipotenti. In particolare allora $|[0, 1]| = |\mathbb{R}|$

□

8.6 Potenza del continuo

Un insieme A ha la potenza del continuo se:

$$|A| = |P(\mathbb{N})|$$

Sappiamo che $|\mathbb{R}| = |P(\mathbb{N})|$, quindi si può anche dire che A ha la potenza del continuo se $|A| = |\mathbb{R}|$.

8.7 Ipotesi del continuo

L'ipotesi del continuo afferma che dato un insieme A :

$$|\mathbb{N}| \leq |A| \leq |P(\mathbb{N})| \Leftrightarrow |A| = |\mathbb{N}| \vee |A| = |P(\mathbb{N})|$$

Cioè, se $|\mathbb{N}| < |A| \leq |P(\mathbb{N})|$, allora $|A| = |P(\mathbb{N})|$

9 L'insieme $\mathbb{Z}$

Definiamo in $\mathbb{N} \times \mathbb{N}$ la seguente relazione, che si rileva essere una relazione d'equivalenza:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Si può facilmente verificare che gode delle tre proprietà (rifl., simm., trans.).

Adesso prendiamo

$$\mathbb{N} \times \mathbb{N} / \sim = \{\text{insieme di tutte le classi d'equivalenza}\} = \mathbb{Z}$$

$\mathbb{Z}$ non è nient'altro che questo insieme. Un suo elemento qualsiasi è quindi la classe d'equivalenza $[(a, b)]$

Per questo motivo, insiemisticamente parlando, la scrittura $\mathbb{N} \subset \mathbb{Z}$ è errata.

Ora ridefiniamo tutte le operazioni abituali.

9.1 Addizione

$$[(a, b)] + [(c, d)] = [(a + c), (b + d)]$$

In realtà, $[(a, b)]$ è una classe di equivalenza, e quindi esiste anche $(a', b') \sim (a, b) \Rightarrow [(a', b')] = [(a, b)]$ che rientra nella stessa classe.

Allora, la seguente equivalenza è vera?

$$[(a, b)] + [(c, d)] = [(a', b')] + [(c, d)] = [(a + c), (b + d)] = [(a' + c), (b' + d)]$$

Verifichiamolo:

$$(a', b') \sim (a, b) \Rightarrow a' + b = b' + a \quad (3)$$

$$((a + c), (b + d)) \sim ((a' + c), (b' + d)) \Rightarrow (a + c) + (b' + d) = (b + d) + (a' + c) \quad (4)$$

$$a + b' + c + d = a' + b + c + d \Rightarrow a + b' = a' + b \quad (5)$$

$$0 = 0 \quad \text{per la (1)} \quad (6)$$

9.1.1 Proprieta'

L'addizione in $\mathbb{Z}$ gode di queste proprieta':

1. Associativa
2. Commutativa
3. 0 e' l'elemento neutro
4. Legge di cancellazione: $a + c = b + c \Rightarrow a = b$

9.2 Moltiplicazione

$$[(a, b)][(c, d)] = [(ac + bd), (ad + bc)]$$

9.2.1 Proprieta'

La moltiplicazione in $\mathbb{Z}$ gode di queste proprieta':

1. Associativa
2. Commutativa
3. Distributiva rispetto alla somma
4. $[1, 0] = +1$ e' l'elemento unita'
5. Esiste l'opposto (che non esisteva in $\mathbb{N}$: $\forall a \in \mathbb{Z} \exists a' : a + a' = a' + a = 0$)

9.3 Simbolismo

Adesso ritorniamo all'usuale rappresentazione dei numeri interi relativi:

$$[a, b] = \begin{cases} a > b & \exists n : a = b + n & [a, b] \rightarrow +n \\ a < b & \exists n : b = a + n & [a, b] \rightarrow -n \\ a = b & & [a, b] = 0 \end{cases}$$

($[a, b] \rightarrow +n$ significa che a $[a, b]$ associamo $+n$, ad esempio $[7, 3] \rightarrow +4$)
Siamo sicuri che $[a, b] \rightarrow +n$ per ogni coppia in $[a, b]$?

Proof: Verifichiamolo per $a > b$.

$$\begin{aligned} (a', b') &\sim (a, b) \\ a' + b &= b' + a \\ a > b &\Rightarrow a = b + n \\ a' + b &= b' + b + n \Rightarrow a' = b' + n \Rightarrow a' > b' \end{aligned}$$

□

9.4 $\mathbb{N}$ immerso in $\mathbb{Z}$

Consideriamo una funzione iniettiva:

$$f : \mathbb{N} \hookrightarrow \mathbb{Z}$$

Se gode di queste proprietà, si dice che è un'immersione:

1. $f(m+n) = f(m) + f(n)$
2. $f(mn) = f(m)f(n)$

In poche parole $f()$ eredita le operazioni di N . Poiché questo è vero per $\forall m, n \in \mathbb{N}$, possiamo dire che $\mathbb{N}$ è immerso in $\mathbb{Z}$ e scriveremo $N \subset Z$.

Proof: Proviamo che $f(n) = [n, 0] = +n$ è un'immersione.

1. È iniettiva?

$$\begin{aligned} f(m) = f(n) &\Rightarrow m = n \\ [m, 0] &= [n, 0] \\ (m, 0) &\sim (n, 0) \\ m + 0 &= n + 0 \\ m &= n \end{aligned}$$

2. Ereditare l'addizione?

$$\begin{aligned} f(m+n) &= f(m) + f(n) \\ [m+n, 0] &= [m, 0] + [n, 0] = [m+n, 0] \end{aligned}$$

3. Ereditare la moltiplicazione?

$$\begin{aligned} f(mn) &= f(m)f(n) \\ [mn, 0] &= [m, 0][n, 0] = [mn + 0 \cdot 0, m0 + 0n] = [mn, 0] \end{aligned}$$

□

9.5 $\mathbb{Z}$ è un totet

$\mathbb{Z}$ non è più ben ordinato, infatti, non ha più un minimo, però rimane sempre totalmente ordinato.

Inoltre, $(\mathbb{Z}, +, \cdot)$ è un dominio d'integrità e $(\mathbb{Z}, +, \cdot, \leq)$ è un dominio ordinato. Con questo intendiamo che la relazione d'ordine $\leq$ rimane compatibile con le operazioni di somma e prodotto:

1. se $a \leq b \Rightarrow a + c \leq b + c$
2. se $a \leq b, c \geq 0 \Rightarrow ac \leq bc$

9.6 Teoria della divisibilità in $\mathbb{Z}$

$$a/b \Leftrightarrow az = b, \quad a, b, z \in \mathbb{Z}$$

9.6.1 Proprietà

1. Se $m, n \in \mathbb{Z}, mn = 1 \Rightarrow m = n = \pm 1$
2. Se $a/b \wedge b/a \Rightarrow b = \pm a$

9.7 Numeri irriducibili e primi

Un numero $z \in \mathbb{Z}$ e' irriducibile se i suoi unici divisori sono $\pm 1, \pm z$, ovvero

$$z = bc \Rightarrow b \equiv \text{invertibile} \vee c \equiv \text{invertibile}$$

Nota: gli unici invertibili in $\mathbb{Z}$ sono ± 1 .

Un numero $p \in \mathbb{Z}$ e' primo se e' vera la seguente implicazione:

$$p/ab \Rightarrow p/a \vee p/b$$

Un numero $p \neq 0$ e' primo se e solo se e' irriducibile:

$$\text{primo} \Leftrightarrow \text{irriducibile}$$

Proof: Dimostriamo il verso $\Rightarrow$.

Per ipotesi $p = ab$ e' primo, quindi $p/a \vee p/b$

Se p/a , allora:

$$a = \lambda p$$

$$p = ab \Rightarrow p = \lambda pb \xRightarrow[p \neq 0]{} 1 = \lambda b$$

$$b = \pm 1$$

Se invece p/b allora:

$$b = \mu p$$

$$p = ab \Rightarrow p = a\mu p \xRightarrow[p \neq 0]{} 1 = a\mu$$

$$a = \pm 1$$

□

Proof: Dimostriamo l'altro verso $\Leftarrow$

Ipotesi: p e' irriducibile.

Supponiamo che p sia effettivamente primo, allora scriviamo che:

$$p/ab$$

e supponiamo anche che p non divida a . Se allora riusciamo a dimostrare che divide b , abbiamo finito. Dato che p non divide a : $MCD(a, p) = 1$. Applichiamo l'identita' di Bezout:

$$1 = ma + np$$

Moltiplichiamo la precedente per b :

$$b = bma + bnp = (bm)a + (pn)b$$

Poiche' per Hp p/ab allora $p/(ab)_m$, e poiche' p/pnb , allora p divide la loro somma e quindi

$$p/b$$

□

9.8 MCD in $\mathbb{Z}$

Il MCD in $\mathbb{Z}$ e' definito allo stesso modo di come e' stato prima definito in $\mathbb{N}$:

$$d = MCD(a, b) \Leftrightarrow d/a, d/b, \exists d' | d'/a, d'/b \Rightarrow d'/d$$

9.9 Minimo Comune Multiplo

Il $mcm(a, b)$ e' semplicemente il contrario del MCD:

$$m = mcm(a, b) \Leftrightarrow a/m, b/m, \exists m' | a/m', b/m' \Rightarrow m/m'$$

9.9.1 Proprieta'

1. Possiamo calcolare il MCD e il mcm in questo modo:

$$\begin{aligned} a &= q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s}, \quad m_i \geq 0 \\ b &= q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}, \quad t_i \geq 0 \\ \alpha_i &= \min(m_i, t_i) \\ \beta_i &= \max(m_i, t_i) \\ MCD(a, b) &= q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s} \\ mcm(a, b) &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s} \end{aligned}$$

Proof: Sia $m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$. Poiche'

$$\beta_i = \max(m_i, t_i) \geq m_i, t_i$$

e' chiaro che m e' un multiplo sia di a che di b .

Supponiamo che m' sia un multiplo di a e di b , allora

$$m' = kab = kq_1^{m_1+t_1} q_2^{m_2+t_2} + \cdots + q_s^{m_s+t_s}$$

Si ha anche che

$$\beta_i = m_i \vee t_i \Rightarrow \beta_i \leq m_i + t_i$$

e quindi e' chiaro che $m \mid m'$.

Percio' $m = mcm(a, b)$.

In modo analogo si procede per il MCD . □

- 2.

$$mcm(a, b) \cdot MCD(a, b) = ab$$

Proof: Procedendo come nella prop. precedente, decomponiamo ab :

$$ab = (q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s})(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}) = q_1^{m_1+t_1} q_2^{m_2+t_2} + \cdots + q_s^{m_s+t_s}$$

Per la prop. precedente abbiamo

$$mcm(a, b)MCD(a, b) = (q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s})(q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}) = q_1^{\alpha_1+\beta_1} q_2^{\alpha_2+\beta_2} + \cdots + q_s^{\alpha_s+\beta_s}$$

Ma poiche'

$$\alpha_i + \beta_i = \min(m_i, t_i) + \max(m_i, t_i) = m_i + t_i$$

si ha la tesi. □

- 3.

$$mcm(a, b) = ab \Leftrightarrow MCD(a, b) = 1$$

Proof: Immediata conseguenza della prec. prop. □

- 4.

$$a \mid n, \quad b \mid n \Leftrightarrow mcm(a, b) \mid n$$

Proof:

⟨1⟩ ($\Rightarrow$)

Semplice conseguenza della 1.

⟨2⟩ ($\Leftarrow$)

$$\begin{aligned} &\text{per definizione } mcm(a, b) = \lambda a = \mu b \\ &mcm(a, b) \Big/ n \\ &\Rightarrow a, b \Big/ n \end{aligned}$$

□

9.10 Algoritmo di divisione in $\mathbb{Z}$

Non e' altro che l'estensione di quello in $\mathbb{N}$:

$$\forall a, b \in \mathbb{Z}, \exists! q, r \in \mathbb{Z} \mid a = qb + r, \quad 0 \leq r < |b|$$

Proof: Proviamolo.

1. In questo primo caso poniamo $a \geq 0$ e procediamo per induzione su a .

Base: $a = 0 \Rightarrow (a = 0) = 0 + 0$

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

Dim: Aggiungiamo 1 ad ambo i membri di $a = qb + r$:

$$a + 1 = qb + (r + 1) = qb + r', \quad r' = r + 1$$

Se dimostriamo che $0 \leq r' < |b|$ abbiamo finito.

Sicuramente $r' \geq 0$ perche' e' $r \geq 0$ per l'ipotesi induttiva.

E' anche vero che $(r' = r + 1) \leq |b|$ perche' per Hp $r < |b|$. Allora si possono verificare due casi:

a. $r' < |b|$. E qui abbiamo finito.

b. $r' = |b|$. Allora:

$$a + 1 = qb + |b|$$

$$a + 1 = qb + |b| = b(q \pm 1) + 0$$

Questo significa che siamo riusciti a dividere $a + 1$ per b e che il suo resto e' $0 < |b|$. Fine.

□

9.11 Identita' di Bezout

Proposition 9.1.

$$d = MCD(a, b) \Rightarrow \exists \lambda, \mu \in \mathbb{Z} : d = \lambda a + \mu b$$

Per calcolare λ e μ si utilizza l'algoritmo Euclideo (vedi [7.4, pg. 31]):

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

$$r_2 = r_3q_4 + r_4$$

$$\vdots$$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$$

$$r_{n-2} = r_{n-1}q_n + r_n$$

$$r_{n-1} = r_nq_{n+1} + 0$$

$$d = r_n$$

Si parte dalla prima equazione e si procede per sostituzioni successive:

$$\begin{aligned}
r_1 &= -q_1b + a = \lambda_0b + \mu_0a \\
r_2 &= b - r_1q_2 = b - (\lambda_0b + \mu_0a)q_2 = (1 - \lambda_0)b - q_2\mu_0a = \lambda_1b + \mu_1a \\
r_3 &= r_1 - r_2q_3 = (\lambda_0b + \mu_0a) - (\lambda_1b + \mu_1a)q_3 = \lambda_2b + \mu_2a \\
&\vdots \\
r_n &= r_{n-2} - r_{n-1}q_n = (\lambda_{n-3}b + \mu_{n-3}a) - (\lambda_{n-2}b + \mu_{n-2}a)q_n = \lambda_{n-1}b + \mu_{n-1}a \\
d &= r_n = \lambda_{n-1}b + \mu_{n-1}a
\end{aligned}$$

9.12 Teorema fondamentale dell'aritmetica

$\forall n \in \mathbb{Z}^*$, non invertibile, si può esprimere in maniera “unica” come prodotto di numeri primi. Questa “unicità” vale a meno dell'ordine e del segno.

Proof: Poiché l'unicità è a meno del segno e che $n \neq 1$, supponiamo che $n > 1$ e procediamo per induzione su n :

base: $n = 2$. Questo è vero perché 2 è primo.

Hp: se $m < n$, allora $m = q_1q_2 \cdots q_r$, dove q_i è primo.

Ts:

$$n = \begin{cases} \text{primo} \\ \text{non primo, riducibile} \end{cases}$$

Nel primo caso non abbiamo nulla da dimostrare.

Nel secondo caso, n ammette dei divisori diversi da ± 1 e da n , quindi scriviamo:

$$n = ab$$

Ma $a, b < n$, e quindi per Hp:

$$\begin{aligned}
a &= q_1q_2 \cdots q_r \\
b &= p_1p_2 \cdots p_s \\
n &= ab = q_1q_2 \cdots q_rp_1p_2 \cdots p_s
\end{aligned}$$

Quindi abbiamo dimostrato l'induzione, ovvero che ogni numero $\mathbb{Z}$ si può scrivere come prodotto di primi. Ci resta da verificare l'unicità.

Supponiamo che n si possa fattorizzare in due modi diversi:

$$\begin{aligned}
r, s &\in \mathbb{N} \\
n &= q_1q_2 \cdots q_r \\
n &= p_1p_2 \cdots p_s \\
q_1q_2 \cdots q_r &= p_1p_2 \cdots p_s
\end{aligned}$$

Supponiamo intanto $r < s$.

Supponiamo per assurdo che preso un q_j non esiste un p_i tale che $q_j = p_i$. Consideriamo q_1 , allora si ha

$$\begin{aligned}
q_1 / n &\Rightarrow q_1 / p_1p_2 \cdots p_s \\
\text{Sia } p &= p_2 \cdots p_s \\
q_1 \text{ primo} &\Rightarrow q_1 \neq p
\end{aligned}$$

Se per assurdo $(q_1, p) \neq 1$, allora

$$(q_1, p) \neq 1 \Rightarrow \exists d \neq 1 : d \mid q_1 \wedge d \mid p$$

$$d \mid q_1 \underbrace{\Leftrightarrow}_{q_1 \text{ e' primo}} d = 1 \vee d = q_1 \underbrace{\Rightarrow}_{d \neq 1} d = q_1$$

$$d \mid p \Leftrightarrow q_1 \mid p = p_2 \cdots p_s \underbrace{\Rightarrow}_{q_1 \text{ e' primo}} q_1 \mid p_k, \quad 2 \leq k \leq s \underbrace{\Rightarrow}_{q_1 \text{ e' primo}} q_1 = p_k$$

assurdo, contro la nostra supposizione iniziale. Quindi $(q_1, p) = 1$.

$$\begin{cases} n = p_1 p \\ q_1 \mid n, \quad q_1 \nmid p \\ (q_1, p) = 1 \end{cases} \underbrace{\Rightarrow}_{\text{prop. divisibilita' [5,pg.30]}} q_1 \mid p_1$$

$$\begin{cases} q_1 \text{ primo}, \quad q_1 \neq 1 \\ q_1 \mid p_1 \end{cases} \Rightarrow q_1 = p_1$$

E questo e' assurdo.

Allora, concludiamo che

$$\exists i : q_1 = p_i$$

E analogamente per qualsiasi altro q_j .

Quindi $q_1 = p_i$. Per semplicita', a meno di riordinare i fattori, poniamo $i = 1$.

Quindi riscriviamo l'equazione di partenza, semplificando q_1 e p_1 da entrambi i membri:

$$q_2 \cdots q_r = p_2 \cdots p_s$$

Ora possiamo ripetere questa stessa procedura r volte, fino a quando arriviamo a:

$$1 = p_{r+1} \cdots p_s$$

Ma questo e' assurdo perche' il prodotto di numeri primi, di certo, non e' uguale a 1, quindi, se questo e' assurdo, e' assurda l'ipotesi che $r < s$. Poiche' possiamo ripetere questa stessa dimostrazione per $r > s$ e arriveremmo anche qui a un assurdo, allora $r = s$. Da quanto abbiamo dimostrato prima n si puo' fattorizzare in fattori primi, ma se ogni sua fattorizzazione ha esattamente r fattori, allora tutte queste sono equivalenti. In poche parole, esiste una sola fattorizzazione di n . $\square$

10 Aritmetica modulare

Sappiamo che possiamo scrivere ogni numero $x \in \mathbb{Z}$ come $x = mn + y$, allora possiamo inventarci questa relazione:

$$x \sim y \Leftrightarrow x - y = nm$$

e diciamo che x e' congruo a y modulo n . In altre parole $x \sim y$ se $x - y$ e' un multiplo di n , ovvero se x diviso n e y diviso n hanno lo stesso resto.

Questa relazione e' una relazione d'equivalenza. Possiamo costruire allora le classi di equivalenza:

$$[a]_n = \bar{a} = \{x \in \mathbb{Z} \mid x \sim a\} = \{x \in \mathbb{Z} \mid x - a = mn\}$$

Creiamo l'insieme quoziente $\mathbb{Z}/\sim$, ovvero:

$$\mathbb{Z}_n = \mathbb{Z}/\sim = \{\text{classi di equivalenza}\}$$

$[a]_n$ sono tutti quei numeri che divisi per n hanno lo stesso resto di a diviso n . Poiche' sappiamo per l'algoritmo di divisione in $\mathbb{Z}$ che il resto e' sempre $0 \leq r < n$, allora ci saranno

esattamente $n - 1$ classi d'equivalenza, ovvero:

$$\mathbb{Z}_n = \{[1], [2], \dots, [n - 1]\}$$

Il numero di elementi di $\mathbb{Z}_n$ e' uguale a n .

A questo punto definiamo le solite operazioni su $\mathbb{Z}_n$.

10.1 Somma

$$[a] + [b] = [a + b]$$

Dobbiamo pero' verificare che questo discorso sia realmente valido, cioe' se io prendo $[a'] = [a]$ e $[b'] = [b]$ deve risultare $[a' + b'] = [a + b]$

Proof: Hp: $[a'] = [a]$ e $[b'] = [b]$

Ts: $[a' + b'] = [a + b]$

$$a' - a = \lambda n \Rightarrow a' = \lambda n + a$$

$$b' - b = \mu n \Rightarrow b' = \mu n + b$$

$$(a' + b') - (a + b) = \lambda n + a + \mu n + b - a - b = (\lambda + \mu)n$$

$$(a' + b') - (a + b) = (\lambda + \mu)n \Rightarrow (a' + b') \sim (a + b) \Rightarrow [a' + b'] = [a + b]$$

□

10.1.1 Prodotto

$$[a][b] = [ab]$$

Ora verifichiamo che sia una definizione ben posta, cosi' come abbiamo fatto prima.

Proof: Hp: $[a'] = [a]$, $[b'] = [b]$

Ts: $[a'b'] = [ab]$

$$a' - a = \lambda n \Rightarrow a' = \lambda n + a$$

$$b' - b = \mu n \Rightarrow b' = \mu n + b$$

$$a'b' - ab = (\lambda n + a)(\mu n + b) - ab = \lambda\mu n^2 + \lambda bn + a\mu n + ab - ab = n(\lambda\mu n + \lambda b + \mu a)$$

$$a'b' - ab = n(\lambda\mu n + \lambda b + \mu a) \Rightarrow a'b' \sim ab \Rightarrow [a'b'] = [ab]$$

□

10.2 Proprieta'

La moltiplicazione e il prodotto formano un anello commutativo abeliano, ovvero godono delle seguenti otto proprieta':

1. $[a] + ([b] + [c]) = ([a] + [b]) + [c]$ (associativa)
2. $[a] + [b] = [b] + [a]$ (commutativa)
3. $[0] + [a] = [a] + [0] = [a]$ (elem. neutro dell'addizione)
4. $\exists [a'] \in \mathbb{Z}_n \mid [a] + [a'] = [0]$ (elem. opposto)
Inoltre $[a'] = [n - a] = [-a]$
5. $[a]([b][c]) = ([a][b])[c]$ (associativa)

6. $[a][b] = [b][a]$ (commutativa)
7. $[a]([b] + [c]) = [a][b] + [a][c]$ (distributiva)
8. $[1][a] = [a][1] = 1$ (elem. neutro del prodotto)

10.3 Elementi invertibili

Proposition 10.1. *In $\mathbb{Z}_n$ accade che $[a]_n$ e' invertibile se:*

$$[a]_n \equiv \text{invertibile} \Leftrightarrow \text{MCD}(a, n) = 1$$

Ovvero, se a, n sono coprimi (primi fra loro, non hanno primi in comune).

Ricordiamoci che un elem. $[a]$ e' invertibile se $\exists [a'] \mid [a][a'] = [1]$.

Proof: Dimostriamo $\Rightarrow$.

Hp: $[a]_n \equiv \text{invertibile}$

Ts: $\text{MCD}(a, n) = 1$

Per definizione $\exists [a'] \mid [a][a'] = [1]$. Ovvero,

$$[aa'] = [1] \Rightarrow aa' - 1 = \lambda n$$

$$aa' - \lambda n = 1$$

Adesso supponiamo che d sia un divisore comune di a e n , allora d divide aa' , $d/\lambda n$ e divide λn . Ma allora a maggior ragione divide la loro differenza. Ma $aa' - \lambda n = 1$, quindi d divide 1. Questo significa che necessariamente $d = 1$. $\square$

Proof: Adesso dimostriamo $\Leftarrow$.

Hp: $\text{MCD}(a, n) = 1$

Ts: $[a]_n \equiv \text{invertibile}$

Per Bezout possiamo scrivere:

$$1 = \lambda a + \mu n$$

Ma allora:

$$[1] = [\lambda a] + [\mu n] = [\lambda a] + [0] = [\lambda a] = [\lambda][a]$$

Cioe',

$$[1] = [a][\lambda]$$

$\square$

Una conseguenza di questo fatto e' che la legge dell'annullamento del prodotto vale solo in $\mathbb{Z}_p$ dove p e' un numero primo. Ad esempio se in $\mathbb{Z}_{10}$, $[5][4] = [0]$.

10.3.1 Insieme degli invertibili

$$U_n = \{\text{gli invertibili distinti di } \mathbb{Z}_n\}$$

10.4 Equazione modulare

Proposition 10.2. *Se $\text{MCD}(a, n) = 1$, allora l'equazione*

$$ax = b \pmod{n}$$

ammette una e una sola soluzione in $\mathbb{Z}_n$

Proof:

$$(a, n) = 1 \quad \underbrace{\Leftrightarrow}_{[10.1, \text{pg. 46}]} \quad a \text{ e' invertibile in } \mathbb{Z}_n \Leftrightarrow \exists a^{-1} \text{ in } \mathbb{Z}_n$$

$$ax = b \ (\mathbb{Z}_n) \Rightarrow a^{-1}ax = a^{-1}b \Leftrightarrow x = a^{-1}b \ (\mathbb{Z}_n)$$

Vogliamo dimostrare che e' unica. Supponiamo per assurdo che esistano due soluzioni:

$$\begin{cases} ax_1 = b \ (\mathbb{Z}_n) \\ ax_2 = b \ (\mathbb{Z}_n) \end{cases} \Rightarrow ax_1 = ax_2 \ (\mathbb{Z}_n) \Rightarrow a^{-1}ax_1 = a^{-1}ax_2 \ (\mathbb{Z}_n) \Leftrightarrow x_1 = x_2$$

□

Proposition 10.3.

$$ax = b \ (\mathbb{Z}_n) \text{ ammette soluzioni} \Leftrightarrow (a, n) \mid b$$

dove $(a, n) = \text{MCD}(a, n)$

Proof:

$$ax = b \ (\mathbb{Z}_n) \Leftrightarrow ax - b = \mu n \quad \underbrace{\Leftrightarrow}_{y=-\mu} \quad ax + ny = b$$

Quest'ultima e' una equazione diofantea. Per quanto visto in [11.1,pg.52], ammette soluzioni in x, y se e solo se $(a, n) \mid b$. □

Proposition 10.4. Sia $d = \text{MCD}(a, n)$. Se $d \mid b$, allora l'equazione

$$ax = b \ (\mathbb{Z}_n)$$

ammette d soluzioni distinte in $\mathbb{Z}_n$.

Data la soluzione x_0 , tutte e sole le soluzioni sono:

$$x_i = x_0 + \frac{n}{d}i \quad i \in \mathbb{Z}$$

Quelle distinte in $\mathbb{Z}_n$ si ottengono per $i = 0, \dots, d-1$.

L'algoritmo per calcolarle e':

1. Per Bezout possiamo scrivere:

$$d = \lambda a + \mu n$$

2. Quest'ultima e' un'equazione diofantea che possiamo risolvere in diversi modi (vedi 11.0.1). Troviamo quindi λ e μ .

3. Tutte le soluzioni saranno:

$$\begin{cases} x_0 = \lambda \frac{b}{d} \quad \text{mod}, n \\ x_i = x_0 + i \frac{n}{d} \quad \text{mod}, n \end{cases}$$

4. Le soluzioni distinte sono solo d , e cioe' x_i per $i = 0, \dots, d-1$

10.5 Sistemi lineari di congruenze

10.5.1 Teorema cinese del resto

Proposition 10.5. Sia $(m_i, m_j) = 1 \quad \forall i \neq j$ e sia dato il sistema

$$\begin{cases} a_1 x = b_1 & (\mathbb{Z}_{m_1}) \\ \vdots \\ a_n x = b_n & (\mathbb{Z}_{m_t}) \end{cases} \quad (1)$$

tale che ogni equazione ammetta soluzione. Allora il sistema (1) e' equivalente al sistema del tipo

$$\begin{cases} x = c_1 & (\mathbb{Z}_{m'_1}) \\ \vdots \\ x = c_n & (\mathbb{Z}_{m'_t}) \end{cases}$$

dove $(m'_i, m'_j) = 1 \quad \forall i \neq j$.

Proof: Ogni singola equazione del sistema e' risolvibile e quindi $d_i = (a_i, m_i) \mid b_i$ (vedi [10.4,pg.47]).

Dividendo ogni equazione per d_i , ci riconduciamo al sistema equivalente

$$\begin{cases} a'_1 x = b'_1 & (\mathbb{Z}_{m'_1}) \\ \vdots \\ a'_n x = b'_n & (\mathbb{Z}_{m'_t}) \end{cases}$$

dove $a'_i = \frac{a_i}{d_i}$, $b'_i = \frac{b_i}{d_i}$, $m'_i = \frac{m_i}{d_i}$.

Continua a valere la condizione $(m'_i, m'_j) = 1 \quad \forall i \neq j$. Inoltre,

$$\begin{cases} d_i = (a_i, m_i) \\ a'_i = \frac{a_i}{d_i} \\ m'_i = \frac{m_i}{d_i} \end{cases} \Rightarrow (a'_i, m'_i) = 1$$

Quindi per la prop [10.2,pg.46], ogni equazione i ammette un'unica soluzione in $\mathbb{Z}_{m'_i}$.

Risolvendo ogni singola equazione abbiamo il sistema:

$$\begin{cases} x = c_1 & (\mathbb{Z}_{m'_1}) \\ \vdots \\ x = c_n & (\mathbb{Z}_{m'_t}) \end{cases}$$

□

Theorem 10.6. Se $\text{MCD}(m_i, m_j) = 1 \quad \forall i \neq j$, allora il sistema

$$\begin{cases} x = c_1 & (\mathbb{Z}_{m_1}) \\ \vdots \\ x = c_n & (\mathbb{Z}_{m_t}) \end{cases}$$

ammette soluzioni. Non vale il viceversa.

Inoltre, tutte le soluzioni sono uguali in $\mathbb{Z}_R$, dove $R = m_1 m_2 \cdots m_t$.

Il metodo risolutivo e' esposto nella dimostrazione.

Proof: Poniamo

$$R = m_1 m_2 \dots m_t = \text{mcm}(m_1, \dots, m_t)$$

$$R_i = \frac{R}{m_i} = m_1 \dots m_{j-1} m_{j+1} \dots m_t$$

Consideriamo l'equ:

$$R_i x_i = c_i \pmod{m_i}$$

Questa equazione ha un'unica soluzione (vedi [10.2, pg.46]), proprio perché R_i non contiene m_i , tutti gli m_i sono coprimi e quindi $\text{MCD}(R_i, m_i) = 1$.

La soluzione del sistema è:

$$x = x_1 R_1 + \dots + x_t R_t$$

Per provare che questo è vero consideriamo $[x]_{m_1}$, cioè:

$$x = x_1 R_1 + \dots + x_t R_t \pmod{m_1}$$

Poiché in $\mathbb{Z}_{m_1}$ tutti i $R_2, \dots, R_t$ sono 0, perché multipli di m_1 , si ha:

$$x = x_1 R_1 = c_1 \pmod{m_1}$$

Lo stesso vale per tutte le altre equazioni:

$$x = c_i \pmod{m_i}$$

questo vuol dire che ogni equazione del sistema originale è soddisfatta.

Sia adesso x una qualsiasi soluzione del sistema. Allora, tutte e sole le soluzioni del sistema sono:

$$x + \lambda R, \quad \lambda \in \mathbb{Z}$$

Infatti, in ogni $\mathbb{Z}_{m_i}$ succede che $R = 0$ e quindi

$$x + \lambda R = x = c_i \pmod{m_i}$$

Viceversa, se y è una soluzione del sistema allora

$$x = c_i = y \pmod{m_i} \quad \forall i \Leftrightarrow x - y = 0 \pmod{m_i} \quad \forall i \Leftrightarrow$$

$$\Leftrightarrow m_i \mid x - y \quad \forall i \quad \underbrace{\Rightarrow}_{(m_i, m_j)=1 \quad \forall i \neq j} \quad m_1 m_2 \dots m_t \mid x - y \Leftrightarrow x - y = 0 \pmod{R} \Leftrightarrow y = x \pmod{R}$$

e quindi

$$y = x + \lambda R$$

□

10.5.2 Applicazione del teorema cinese del resto

Il teorema cinese del resto può essere usato per dimostrare che la seguente funzione è surriettiva, se e solo se $\text{MCD}(m, n) = 1$:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

Proof: Dobbiamo dimostrare che:

$$\forall (\alpha, \beta) \in \mathbb{Z}_m \times \mathbb{Z}_n \quad \exists x \in \mathbb{Z} : f(x) = (\alpha, \beta)$$

Ovvero:

$$\begin{cases} x = \alpha \pmod{m} \\ x = \beta \pmod{n} \end{cases}$$

Dato che $\text{MCD}(m, n) = 1$, il teorema cinese del resto afferma che questo sistema ammette soluzioni. □

10.5.3 Metodo di sostituzione

Un secondo metodo per risolvere i sistemi modulari consiste in:

1. prendere due equazioni del sistema

2. convertirle in $\mathbb{Z}$ applicando la definizione di congruenza. Es: $y = 5 \pmod{7} \Rightarrow y = 5 + 7\lambda$.
3. eguagliare le due equazioni, ottenendo una equazione diofantea
4. risolvere l'equazione diofantea ottenendo le due incognite λ, μ
5. sostituendo una incognita in una delle due equazioni otteniamo un numero n . Ad esempio, se abbiamo trovato che $\lambda = 9$, allora $n = 5 + 7 \cdot 9$.
6. Creiamo l'equazione:

$$y = n + h \cdot \text{mcm}(m_1, m_2)$$

dove $h \in \mathbb{Z}$ e' un parametro variabile, e m_1, m_2 sono i moduli rispettivi delle nostre due equazioni precedenti. Tutte queste y , al variare di h sono soluzione del sistema formato dalle due equazioni modulari.

7. Se il sistema modulare era formato solo da due equazioni, abbiamo finito, altrimenti creiamo un sistema che comprende quest'ultima equazione e un'altra scelta dal sistema originale.
8. Ora riandiamo al passo 2, e reiteriamo tutto questo procedimento fino a quando non possiamo piu' scegliere nuove equazioni dal sistema originale.

10.6 Altri sistemi di congruenze

Proposition 10.7.

$$\begin{cases} z' = z \pmod{m} \\ n/m \end{cases} \Rightarrow z' = z \pmod{n}$$

Proof:

$$\begin{aligned} n/m &\Rightarrow m = 0 \pmod{n} \quad (1) \\ z' = z \pmod{m} &\Leftrightarrow \exists \mu : z' = z + \mu m \underbrace{\Rightarrow}_{(1)} z' = z + 0 \pmod{n} \end{aligned}$$

□

Example 10.8.

$$\begin{aligned} 710923 &= 7 \pmod{12} \\ 7 &= 1 \pmod{3} \end{aligned}$$

Utilizzando la prop [10.7,pg.50] possiamo dire:

$$710923 = 1 \pmod{3}$$

Proposition 10.9. Possiamo sfruttare le idee della prop [10.7,pg.50] per risolvere sistemi del tipo:

$$\begin{cases} f_1(x) = 0 \pmod{m_1} \\ f_2(x) = 0 \pmod{m_2} \\ \vdots \\ f_n(x) = 0 \pmod{m_n} \end{cases}$$

$$f_i : \mathbb{Z}_{m_i} \longrightarrow \mathbb{Z}_{m_i} \quad \forall i = 1, \dots, n$$

$$m_i / m_{i+1} \quad \forall i = 1, \dots, n-1$$

Nota² Sia

$$X_1 = \{0 \leq x < m_1 \mid f_1(x) = 0 \text{ } \mathbb{Z}_{m_1}\}$$

$$X_2 = \{x + \lambda m_1 \mid 0 \leq x + \lambda m_1 < m_2, x \in X_1, \lambda \in \mathbb{Z}, f_2(x + \lambda m_1) = 0 \text{ } \mathbb{Z}_{m_2}\}$$

$\vdots$

$$X_n = \{x + \lambda m_{n-1} \mid 0 \leq x + \lambda m_{n-1} < m_n, x \in X_{n-1}, \lambda \in \mathbb{Z}, f_n(x + \lambda m_{n-1}) = 0 \text{ } \mathbb{Z}_{m_n}\}$$

allora, X_n e' l'insieme delle soluzioni del sistema modulo m_n . Tutte le soluzioni intere sono date da:

$$y = x + \lambda m_n \quad \forall x \in X_n \quad \forall \lambda \in \mathbb{Z}$$

Nota: il sistema potrebbe anche essere non risolubile.

Un possibile algoritmo risolutivo consiste nel costruire in ordine gli insiemi $X_1, \dots, X_n$.

Proof: Dimostriamo che

$$\{\text{soluzioni del sistema}\} = \{y \in \mathbb{Z} \mid \exists x \in X_n, \exists \lambda \in \mathbb{Z} : y = x + \lambda m_n\}$$

(1) Dim $\supseteq$

Per induzione su n dimostriamo che $X_n \subseteq \{\text{soluzioni del sistema}\}$, cioe' che

$$x \in X_n \Rightarrow f_i(x) = 0 \text{ } \mathbb{Z}_{m_i} \quad \forall i = 1, \dots, n \quad (1')$$

Se $n = 1$ allora $x \in X_n = X_1$, e quindi, per definizione di X_1 , soddisfa l'unica equazione f_1 .

Supponiamo $x \in X_{n+1}$, allora

$$x \in X_{n+1} \Rightarrow \exists \lambda : x = z + \lambda m_n, z \in X_n, f_{n+1}(x) = 0 \quad (1)$$

$$z \in X_n \quad \underbrace{\Rightarrow}_{\text{Hp induttiva}} \quad z \text{ soddisfa il sistema delle equazioni } f_1, \dots, f_n \Leftrightarrow f_i(z) = 0 \text{ } \mathbb{Z}_{m_i} \quad \forall i = 1, \dots, n \quad (2)$$

$$m_i \mid m_n \Rightarrow z + \lambda m_n = z \text{ } \mathbb{Z}_{m_i} \quad \underbrace{\Rightarrow}_{(2), f_i \text{ definita su } \mathbb{Z}_{m_i}} \quad f(x) = f(z + \lambda m_n) = f_i(z) = 0 \text{ } \mathbb{Z}_{m_i} \quad \forall i = 1, \dots, n \quad (3)$$

(1), (3) $\Rightarrow x$ soddisfa tutte le $n + 1$ equazioni

Con la (1') possiamo cosi' concludere che:

$$\exists x \in X_n, \lambda \in \mathbb{Z} \quad \underbrace{\Rightarrow}_{m_i \mid m_n} \Rightarrow x + \lambda m_n = x \text{ } \mathbb{Z}_{m_i} \quad \forall i \leq n \quad \underbrace{\Rightarrow}_{f_i \text{ definita su } \mathbb{Z}_{m_i}} \quad f_i(x + \lambda m_n) = f_i(x) \underbrace{=}_{(1')} 0 \quad \forall i = 1, \dots, n$$

Quindi $x + \lambda m_n$ e' una soluzione del sistema.

(2) Dim $\subseteq$

Viceversa, supponiamo che y sia una soluzione del sistema e dimostriamo che $\exists x \in X_n, \exists \lambda \in \mathbb{Z} : y = x + \lambda m_n$. Procediamo per induzione su n .

² f_i e' una funzione definita su $\mathbb{Z}_{m_i}$ nel senso che:

$$x = y \text{ } \mathbb{Z}_{m_i} \Rightarrow f_i(x) = f_i(y)$$

$$x \in \mathbb{Z} \Rightarrow f(x) = f([x]_{m_i})$$

Una tale f_i potrebbe essere un polinomio, in quanto le operazioni $\cdot, +$ rispettano la congruenza.

Per $n = 1$,

$$\begin{aligned}
 y \text{ soluzione} &\Rightarrow f_1(y) = 0 \pmod{m_1} \\
 \text{Sia } \bar{y} &= \min \{y' \in \mathbb{N} \mid y' \equiv y \pmod{m_1}\} \\
 0 \leq \bar{y} &< m_1, \quad y = \bar{y} + \mu m_1 \\
 0 = f_1(y) &= f_1(\bar{y} + \mu m_1) \stackrel{\substack{= \\ f_1 \text{ definita su } \mathbb{Z}_{m_1}}}{=} f_1(\bar{y}) \\
 &\Rightarrow \bar{y} \in X_1
 \end{aligned}$$

Quindi ponendo $x = \bar{y}$, $\lambda = \mu$ abbiamo la tesi

Caso $n + 1$,

$$y \text{ soluzione di } f_1, \dots, f_{n+1} \Rightarrow y \text{ soluzione di } f_1, \dots, f_n \stackrel{\substack{= \\ \text{Hp indutt.}}}{\Rightarrow} y = x + \lambda m_n, \text{ con } x \in X_n$$

$$\text{Sia } \bar{y} = \min \{y' \in \mathbb{N} \mid y' \equiv y \pmod{m_{n+1}}\} \quad (1)$$

$$(1) \Rightarrow 0 \leq \bar{y} < m_{n+1} \quad (1.1)$$

$$(1) \Rightarrow x + \lambda m_n = y = \bar{y} + \mu m_{n+1} \stackrel{m_n / m_{n+1}}{\Rightarrow} \bar{y} = x + (\lambda + \mu^*) m_n, \quad x \in X_n \quad (1.2)$$

$$(1) \stackrel{f_{n+1} \text{ def. su } \mathbb{Z}_{m_{n+1}}}{\Rightarrow} f_{n+1}(\bar{y}) = f_{n+1}(y) \stackrel{y \text{ soluzione}}{=} 0 \pmod{m_{n+1}} \quad (1.3)$$

$$(1.1), (1.2), (1.3) \Rightarrow \bar{y} \in X_{n+1}$$

$$\begin{cases} \bar{y} \in X_{n+1} \\ y = \bar{y} + \mu m_{n+1} \end{cases} \text{ che e' la tesi}$$

□

11 Equazioni diofantee

Proposition 11.1.

$$ax + by = c, \quad a, x, b, y, c \in \mathbb{Z}$$

e' una equazione diofantea.

Una equazione diofantea ha soluzioni (infinite) se e solo se:

$$\text{MCD}(a, b) \mid c$$

Proof: Dimostriamo $\Rightarrow$.

Supponiamo che (α, β) e' una soluzione.

$$\begin{aligned}
 a\alpha + b\beta &= c \\
 d &= \text{MCD}(a, b) \\
 a &= md, \quad b = nd \\
 md\alpha + nd\beta &= c \Rightarrow d \mid c
 \end{aligned}$$

Dimostriamo $\Leftarrow$.

$$\begin{aligned}
 d &= ma + nb, \quad d \mid c \\
 dh &= c \\
 dh &= mha + nhb \\
 c &= (mh)a + (nh)b
 \end{aligned}$$

(mh) e (nh) sono le soluzioni. □

Proof: Adesso dimostriamo che ha infinite soluzioni.

$$ax_0 + by_0 = c$$

$$a(x_0 + \lambda b) + b(y_0 + \lambda a) = c$$

$$ax_0 + a\lambda b + by_0 - a\lambda b = ax_0 + by_0 = c$$

□

Tutte le soluzioni di un'equazione diofantea lineare sono del tipo:

$$(x_0 + \lambda \frac{b}{d}, y_0 - \lambda \frac{a}{d})$$

dove (x_0, y_0) e' una soluzione qualsiasi, $d = MCD(a, b)$ e $\lambda \in \mathbb{Z}$.

Proof: Dimostriamo che tutte le soluzioni sono di quel tipo.

Consideriamo un'altra soluzione (x_1, y_1) :

$$ax_0 + by_0 = c$$

$$ax_1 + by_1 = c$$

$$ax_0 + by_0 = ax_1 + by_1$$

$$a(x_0 - x_1) = b(y_1 - y_0)$$

$$\frac{a}{d}(x_0 - x_1) = \frac{b}{d}(y_1 - y_0)$$

$$MCD(\frac{a}{d}, \frac{b}{d}) = 1$$

Scegliamo un primo p tale che divida $\frac{a}{d}$. p non dividera' $\frac{b}{d}$ perche' e' coprimo con $\frac{a}{d}$.

$$p/\frac{a}{d} \Rightarrow p/\frac{a}{d}(x_0 - x_1)$$

$$\frac{a}{d}(x_0 - x_1) = \frac{b}{d}(y_1 - y_0) \Rightarrow p/\frac{b}{d}(y_1 - y_0)$$

Ma p non divide $\frac{b}{d}$, quindi deve per forza dividere $(y_1 - y_0)$. Poiche' $\frac{a}{d}$ divide il secondo membro, e poiche' il suo divisore p non divide $\frac{b}{d}$, allora dividera' solo $(y_1 - y_0)$ Ovvero:

$$y_1 - y_0 = \mu \frac{a}{d}$$

Ripetendo lo stesso discorso otteniamo:

$$x_0 - x_1 = \lambda \frac{b}{d}$$

Sostituiamo cio' che abbiamo ottenuto in $a(x_0 - x_1) = b(y_1 - y_0)$:

$$a\lambda \frac{b}{d} = b\mu \frac{a}{d}$$

$$\lambda = \mu$$

$$x_0 - x_1 = \lambda \frac{b}{d}$$

$$y_1 - y_0 = \lambda \frac{a}{d}$$

Cioe':

$$\begin{cases} x_1 = x_0 + \lambda \frac{b}{d} \\ y_1 = y_0 + \lambda \frac{a}{d} \end{cases}$$

□

11.0.1 Risoluzione

Un primo metodo per risolvere una diofantea è quello di usare l'identità di Bezout. Sappiamo che la soluzione esiste se

$$(d = \text{MCD}(a, b)) \mid c \Rightarrow c = hd$$

Per Bezout:

$$d = ma + nb \Rightarrow hd = (mh)a + (nh)b \Rightarrow c = (mh)a + (nh)b$$

Per trovare m e n si adotta l'algoritmo euclideo.

Un secondo metodo sfrutta l'aritmetica modulare:

$$\begin{aligned} 18n + 35m &= 1000 \\ [18n + 35m] &= [1000] \pmod{18} \\ [18n] + [35m] &= [1000] \pmod{18} \\ [17m] &= [10] \pmod{18} \\ [-1m] &= [10] \pmod{18} & [m] &= [-10] = [8] \pmod{18} \\ m - 8 &= \lambda 18 \\ m &= 8 + \lambda 18 \end{aligned}$$

Usiamo lo stesso sistema in $\mathbb{Z}_{35}$ e otteniamo:

$$n = 5 + \mu 35$$

Sostituiamo nell'equazione originale:

$$\begin{aligned} 18(5 + \mu 35) + 35(8 + \lambda 18) &= 1000 \\ 18 \cdot 35(\mu + \lambda) &= 630 \\ \mu + \lambda &= 1 \\ \lambda &= 1 - \mu \end{aligned}$$

Adesso abbiamo legato μ a λ , e abbiamo tutte le soluzioni, cioè:

$$\begin{cases} n = 5 + 35\mu \\ m = 26 - 18\mu \end{cases}$$

12 I numeri primi

12.1 La funzione di Eulero

Definition 12.1. Ecco la funzione di Eulero:

$$\varphi(n) = |U_n|$$

Dove U_n era stato definito in [10.3.1,pg.46]. In altre parole, $\varphi(n)$ è il numero di tutti i coprimi a n , minori di n .

Proposition 12.2. Dati $m, n \in \mathbb{N}$ si ha

$$(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

Proof: $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ sono due insiemi che si possono legare da una applicazione biettiva, cioè:

$$\begin{aligned} f : \mathbb{Z}_{mn} &\leftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \\ [z]_{mn} &\mapsto ([z]_m, [z]_n) \end{aligned}$$

1. Suriettività:

$$\forall (\alpha, \beta) \in \mathbb{Z}_m \times \mathbb{Z}_n \quad \exists x \in \mathbb{Z}_{mn} : f(x) = (\alpha, \beta)$$

Ovvero:

$$\begin{cases} x = \alpha \pmod{m} \\ x = \beta \pmod{n} \end{cases}$$

Dato che $MCD(m, n) = 1$, il teorema cinese del resto afferma che questo sistema ammette soluzioni (vedi [10.6, pg.48]).

2. Iniettività:

Presi $x, y \in \mathbb{Z}_{mn}$, dobbiamo dimostrare che $f(x) = f(y) \Rightarrow x = y$.

$$f(x) = ([x]_m, [x]_n) = f(y) = ([y]_m, [y]_n) \Rightarrow \begin{cases} x = y \pmod{m} \\ x = y \pmod{n} \end{cases} \quad (1)$$

Consideriamo il sistema

$$\begin{cases} \xi = y \pmod{m} \\ \xi = y \pmod{n} \end{cases} \quad (2)$$

Due soluzioni di (2) sono $\xi = y$ e $\xi = x$ (per la (1)).

Sempre per il teorema cinese del resto tali soluzioni sono uguali in $\mathbb{Z}_{mn}$, e quindi

$$x = y \pmod{mn}$$

Sia data la seguente funzione

$$g : U_{mn} \longrightarrow U_m \times U_n$$

$$g(x) = f(x)$$

Dimostriamo intanto che g è ben posta, ovvero che $g(x) \in U_m \times U_n \quad \forall x \in U_{mn}$.

$$x \in U_{mn} \Leftrightarrow x \text{ è invertibile in } \mathbb{Z}_{mn} \quad \Leftrightarrow \quad (x, mn) = 1$$

[10.1, pg.46]

$$g(x) = ([x]_m, [x]_n) \in U_m \times U_n \Leftrightarrow \begin{cases} (x, m) = 1 \\ (x, n) = 1 \end{cases}$$

se per assurdo $(x, m) = d \neq 1$, allora anche $(x, mn) \neq 1$, assurdo. Analogamente deve essere $(x, n) = 1$. Quindi, g è ben posta.

Dimostriamo che g è biettiva.

1. Suriettività: Sappiamo già che f è suriettiva, quindi

$$f \text{ suriettiva} \Rightarrow \forall (a, b) \in U_m \times U_n \subseteq \mathbb{Z}_m \times \mathbb{Z}_n \quad \exists x \in \mathbb{Z}_{mn} : f(x) = (a, b) \Leftrightarrow \begin{cases} x = a \pmod{m} \\ x = b \pmod{n} \end{cases}$$

Resta da dimostrare che $x \in U_{mn}$.

$$x \in U_{mn} \Leftrightarrow x \text{ è invertibile in } \mathbb{Z}_{mn} \quad \Leftrightarrow \quad (x, mn) = 1$$

[10.1, pg.46]

Quindi basta dimostrare che $(x, mn) = 1$. Supponiamo per assurdo che $\exists p$ primo: $p \nmid x, p \nmid mn$

$$a \in U_m \Leftrightarrow (a, m) = 1 \quad \underbrace{\Leftrightarrow}_{x=a \in \mathbb{Z}_m} (x, m) = 1$$

$$b \in U_n \Leftrightarrow (b, n) = 1 \quad \underbrace{\Leftrightarrow}_{x=b \in \mathbb{Z}_n} (x, n) = 1$$

$$\begin{cases} p \nmid mn \\ p \text{ primo} \end{cases} \Rightarrow p \nmid m \vee p \nmid n \quad \underbrace{\Rightarrow}_{p \nmid x} \Rightarrow (x, m) \neq 1 \vee (x, n) \neq 1$$

in ogni caso arriviamo ad un assurdo.

2. Iniettività:

essendo f iniettiva, anche g lo è.

In conclusione:

$$\begin{cases} U_{mn} \leftrightarrow U_m \times U_n \\ U_{mn}, U_m, U_n \text{ insiemi finiti} \end{cases} \Rightarrow |U_{mn}| = |U_m \times U_n| = |U_m| |U_n| \Leftrightarrow \varphi(mn) = \varphi(m) \varphi(n)$$

che è la tesi. □

Proposition 12.3. Sia $n \in \mathbb{N}$, allora

$$\varphi(n = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right)$$

Dove $p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}$, con $m_i > 0$, è la fattorizzazione di n .

Proof: Per la prop [12.2,pg.54] possiamo scrivere:

$$\varphi(n = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}) = \varphi(p_1^{m_1}) \varphi(p_2^{m_2}) \dots \varphi(p_t^{m_t})$$

Adesso consideriamo un primo p e un numero m tale che:

$$m < p^h, \quad \text{MCD}(m, p^h) \neq 1 \Leftrightarrow m = \lambda p$$

Tutti i possibili m , cioè i multipli di p minori di p^h sono p^{h-1} , infatti:

$$px < p^h$$

$$x < p^{h-1}$$

Quindi tutti i coprimi con p^h sono:

$$\varphi(p^h) = p^h - p^{h-1} = p^h \left(1 - \frac{1}{p}\right)$$

E così ritorniamo alla tesi:

$$\begin{aligned} \varphi(n = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}) &= \\ &= p_1^{m_1} \left(1 - \frac{1}{p_1}\right) p_2^{m_2} \left(1 - \frac{1}{p_2}\right) \dots p_t^{m_t} \left(1 - \frac{1}{p_t}\right) \\ \varphi(n) &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right) \end{aligned}$$

□

12.2 Teorema di Fermat

$$p \equiv \text{primo}, a \neq \lambda p \Rightarrow a^{p-1} = 1 \quad (\text{in } \mathbb{Z}_p)$$

Ovvero, se p è primo e non divide a , allora a^{p-1} è congruo 1 modulo p . Il teorema di Fermat è un caso particolare del teorema di Eulero. Una sua forma equivalente è:

$$p \equiv \text{primo}, a \in \mathbb{Z} \Rightarrow a^p = a \quad (\text{in } \mathbb{Z}_p)$$

12.3 Teorema di Eulero

$$MCD(a, n) = 1 \Rightarrow a^{\varphi(n)} = 1 \pmod{n}$$

Proof: Dimostriamo $\Leftrightarrow$.

Poniamo $t = \varphi(n) = |U_n|$, inoltre:

$$U_n = \{u_1, \dots, u_t\}$$

U_n e' l'insieme degli invertibili distinti in $\mathbb{Z}_n$, quindi $MCD(u_i, n) = 1$. Allora, per Hp, anche $a \in U_n$.

Se moltiplichiamo due $u_i u_j$ otteniamo sempre un invertibile $\in U_n$:

$$u_j u_j^{-1} = 1$$

$$u_i u_i^{-1} = 1$$

$$u_j u_i u_j^{-1} u_i^{-1} = 1$$

Quindi au_i e' sempre $\in U_n$, cioe':

$$au_1, au_2, \dots, au_t \in U_n$$

Ci domandiamo se $\{au_1, au_2, \dots, au_t\}$ sia proprio U_n . Supponiamo per assurdo che non lo sia, cioe' $au_i = au_j$, $i \neq j$, allora:

$$aa^{-1}u_i = aa^{-1}u_j$$

$$u_i = u_j$$

Ma questo e' assurdo, perche' per ipotesi abbiamo detto che ogni elemento di U_n e' distinto. Poiche' $|\{au_1, au_2, \dots, au_t\}| = |U_n|$, concludiamo che i due insiemi coincidono. Allora possiamo scrivere:

$$au_1 au_2 \dots au_t = u_1 u_2 \dots u_t$$

$$a^t (u_1 u_2 \dots u_t) = (u_1 u_2 \dots u_t)$$

$$a^t = 1$$

Cioe' la tesi. □

12.4 Proprieta' dei primi

1. Sono infiniti.

Proof: Supponiamo che non lo siano e creiamo l'insieme che li contiene tutti:

$$P = \{p_1, p_2, \dots, p_t\}$$

Ma il numero $q = p_1 p_2 \dots p_t + 1$ e' primo rispetto ai primi definiti in P , infatti, $q \equiv 1 \pmod{p_i}$ □

2. $2^m + 1$ e' primo solo se $m = 2^n$.

Proof: Per assurdo $m = ph$, $p \neq 2$, allora m e' dispari: $m = 2h + 1$. Allora:

$$2^{(2h+1)h} + 1 = 2^{h^{2h+1}} + 1$$

L'ultima e' una somma di potenze dispari e quindi si puo' scrivere come:

$$2^{h^{2h+1}} + 1 = (2^h + 1)(\dots)$$

Quindi $2^m + 1$ non e' primo, perche' prodotto di due fattori. □

Ancora non e' stato provato se $2^{2^n} + 1$ e' primo per $n > 4$.

12.5 Teorema di Wilson

$$p \equiv \text{primo} \Leftrightarrow (p-1)! = -1 \pmod{p} \Leftrightarrow (p-1)! = p-1 \pmod{p}$$

Proof: Dimostriamo $\Leftarrow$.

L'ipotesi, tradotta in $\mathbb{Z}$ e':

$$(p-1)! + 1 = \lambda p$$

Supponiamo per assurdo che p non e' primo, allora:

$$\exists 1 < d < p : d/p \Rightarrow d/\lambda p$$

Inoltre $d/(p-1)!+1$, ma questo e' assurdo, perche' siccome $d/(p-1)!$ dovrebbe anche essere $d/1$. $\square$

Proof: Dimostriamo $\Rightarrow$.

Quando p e' primo, tutti gli elementi in $\mathbb{Z}_p^*$ sono invertibili. Quali sono gli elementi invertibili che hanno come inverso se stessi? Ovvero,

$$xx = 1 \Leftrightarrow x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \quad (\mathbb{Z}_p^*)$$

$$(x-1)(x+1) = 0$$

$$x = 1 \vee x = -1 = p-1 \quad (\mathbb{Z}_p^*) \text{ in } \mathbb{Z}_p \text{ vale la legge dell'annullamento del prodotto}$$

Cioe', $x = \pm 1$ sono gli elementi invertibili che hanno come inverso se stessi. Invece, l'inverso di $y \neq \pm 1$ sara' $y^{-1} \neq y \in 0, \dots, p-1$, quindi:

$$2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) = 1 \quad (\mathbb{Z}_p^*)$$

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2)(p-1) = (p-1) \quad (\mathbb{Z}_p^*)$$

$$(p-1)! = (p-1) \quad (\mathbb{Z}_p^*)$$

$\square$

12.6 R.S.A

Ecco un'applicazione moderna dei teoremi sui numeri primi: la crittografia a chiave asimmetrica RSA.

12.7 La chiave pubblica

La chiave pubblica e' una coppia di numeri (n, e) . n e' un prodotto di due primi $p \cdot q$. e e' invece un numero coprimo con $(p-1)$ e $(q-1)$, cioe'

$$MCD(e, p-1) = 1 \wedge MCD(e, q-1) = 1$$

12.8 Messaggio criptato

M e' il nostro messaggio e deve essere $< n$ e inoltre deve essere coprimo con n . Il messaggio criptato M' e' semplicemente:

$$M' = M^e \quad (\mathbb{Z}_n)$$

12.9 Chiave privata

La chiave privata e' costituita da $(\varphi(n), d)$, dove $\varphi(n) = (p-1)(q-1)$ e' la funzione di eulero applicata a n .

d e' l'inverso di e in $\mathbb{Z}_{\varphi(n)}$. Quindi:

$$de = 1 \quad (\mathbb{Z}_{\varphi(n)})$$

e inoltre:

$$de - 1 = \lambda \varphi(n) \Rightarrow de = 1 + \lambda \varphi(n)$$

Nota: l'inverso di e esiste sicuramente in $\mathbb{Z}_{\varphi(n)}$ perche' e e' coprimo con $(p-1)$ e $(q-1)$.

12.10 Messaggio decriptato

Per decriptare il messaggio basta fare:

$$M = M'^d \pmod{\mathbb{Z}_n}$$

Proof: Dimostriamo che la procedura per decriptare il messaggio e' valida:

$$M'^d = M^{ed} = M^{ed} \pmod{\mathbb{Z}_n}$$

Per quello che abbiamo visto nel precedente paragrafo, possiamo scrivere ed come $1 + \lambda\varphi(n)$, quindi:

$$M^{ed} = M^{1+\lambda\varphi(n)} = M \left(M^{\varphi(n)} \right)^\lambda$$

Poiche' M e' coprimo con n , allora per il teorema di Eulero, $M^{\varphi(n)} = 1 \pmod{\mathbb{Z}_n}$, quindi:

$$MM^{\varphi(n)\lambda} = M1^\lambda = M \pmod{\mathbb{Z}_n}$$

□

13 L'insieme $\mathbb{Q}$

Prendiamo due coppie $(a, b), (c, d) \in \mathbb{Z}$, con l'unica condizione che $b, d \neq 0$.

Definiamo la seguente relazione di equivalenza:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

La classe $[(a, b)]$ la denoteremo con $\frac{a}{b}$.

Ed ecco nato $\mathbb{Q}$:

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim$$

Definiamo le operazioni.

13.1 Addizione

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad b \neq 0, c \neq 0$$

Questa e' una definizione ben posta, perche' se prendiamo due classe equivalenti a $\frac{a'}{b'}$ e ad $\frac{c'}{d'}$, la loro somma sara' identica a quella fra $\frac{a}{b}$ e ad $\frac{c}{d}$.

13.1.1 Proprieta'

1. $+$ e' commutativa
2. $+$ e' associativa
3. In $+$ esiste l'elemento neutro:

$$\frac{a}{b} + \frac{0}{b} = \frac{a}{b}$$

L'elemento neutro e' $\frac{0}{b}$, $b \neq 0$

4. In $+$ esiste l'opposto:

$$\frac{a}{b} + \frac{-a}{b} = \frac{0}{b}$$

Queste quattro proprieta' rendono $(\mathbb{Q}, +)$ un gruppo abeliano commutativo.

13.2 Moltiplicazione

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad b \neq 0, c \neq 0$$

Anche questa e' una definizione ben posta.

13.2.1 Proprieta'

1. $\cdot$ e' commutativa

2. $\cdot$ e' associativa

3. In $\cdot$ esiste l'elemento neutro:

$$\frac{a}{b} \cdot \frac{c}{c} = \frac{a}{b}$$

L'elemento neutro e' $\frac{c}{c} = \frac{1}{1}$, $c \neq 0$

4. $\cdot$ e' distributivo rispetto alla somma

Queste proprieta' unite a quelle dell'addizione rendono $(\mathbb{Q}, +, \cdot)$ un anello abeliano commutativo.

L'ultima proprieta': in $\cdot$ esiste l'inverso, anzi, per ogni numero $\mathbb{Q}$ diverso da 0 esiste il suo inverso:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{c}{c}, \quad a \neq 0, b \neq 0$$

Come conseguenza, vale la legge dell'annullamento del prodotto.

Con quest'ultima proprieta' $\mathbb{Q}$ e' diventato un campo.

13.3 Immersione di $\mathbb{Z}$ in $\mathbb{Q}$

Insiemeisticamente, e' sbagliato scrivere che $\mathbb{Z} \subseteq \mathbb{Q}$. E' pero' vero che $\mathbb{Z}$ e' immerso in $\mathbb{Q}$.

Proof: Per provare questo dobbiamo trovare una funzione iniettiva:

$$f : \mathbb{Z} \hookrightarrow \mathbb{Q}$$

tale che

$$f(x+y) = f(x) + f(y) \quad \wedge \quad f(xy) = f(x)f(y)$$

La funzione cercata e':

$$f(x) = \frac{x}{1}$$

□

14 L'insieme $\mathbb{R}$

In $\mathbb{Q}$, non tutti i sottoinsiemi hanno l'estremo inferiore. $\mathbb{R}$ colma questa lacuna.

Un elemento di $\mathbb{R}$ e' una coppia (A, B) che e' una sezione di $\mathbb{Q}$, ovvero

$$A \cup B = \mathbb{Q}$$

$$A \cap B = \emptyset$$

$$\forall a \in A, \quad \forall b \in B, \quad a < b$$

Ad esempio $\sqrt{2}$ e' la coppia

$$(\{x \in \mathbb{Q} \mid x^2 < 2\}, \{x \in \mathbb{Q}^+ \mid x^2 > 2\})$$

$\mathbb{R}$ e' un campo ed e' anche un *campo ordinato*, ovvero e' un insieme totalmente ordinato (TOTET) e valgono queste due proprieta':

$$\begin{aligned} a \leq b &\Rightarrow a + c \leq b + c \\ a \leq b, c \geq 0 &\Rightarrow ac \leq bc \end{aligned}$$

Per tutti i campi ordinati valgono queste due proprieta':

$$\begin{aligned} a \in K^* &\Rightarrow a^2 > 0 \\ a > 0 &\Rightarrow -a < 0 \end{aligned}$$

15 L'insieme $\mathbb{C}$

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

Ecco fatto.

$\mathbb{C}$ e' un campo, ma non e' ordinato.

Proof: Dimostriamo che $\mathbb{C}$ non e' un campo ordinato.

Per assurdo supponiamo che esista una relazione d'ordine che trasforma $\mathbb{C}$ in un campo ordinato.

Allora per le proprieta' dei campi ordinati accade che:

$$\begin{aligned} \forall z \in \mathbb{C}^* \quad z^2 &> 0 \\ z = (1, 0) = 1, \quad 1 = 1^2 &> 0 \Rightarrow -1 < 0 \\ i^2 > 0 &\Rightarrow -1 > 0 \end{aligned}$$

Le ultime due relazioni a destra sono in contrasto, quindi siamo arrivati a un assurdo. $\square$

15.1 Inverso

L'inverso di (a, b) si calcola ponendo $(a, b)(x, y) = 1$. Svolgendo quest'ultimo sistema lineare, otteniamo:

$$(x, y) = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right)$$

15.2 Radici n-esime dell'unita'

Le radici ennesime complesse dell'unita' sono tutte quelle x che $x^n = 1$.

Chiameremo U_n l'insieme di tutte queste radici.

Le radici ennesime dell'unita' godono di queste proprieta'.

Sia $u_{j_1}, u_{j_2} \in U_n$

1. $u_{j_1} + u_{j_2} = u_{(j_1+j_2 \bmod n)}$
2. $u_{j_1} u_{j_2} = u_{(j_1 j_2 \bmod n)}$

16 Polinomi

16.1 Funzione polinomiale

Sia K un campo. Una funzione $f : K \longrightarrow K$ si dice polinomiale se appartiene all'insieme di tutte le funzioni polinomiali, ovvero:

$$\mathcal{I}_k = \{f : K \longrightarrow K \mid \exists d \in \mathbb{N} : a_0, \dots, a_d \in K \mid f(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d, \forall x \in K\}$$

Su $\mathcal{I}_k$ possiamo definire le operazioni di somma e prodotto.

16.2 Somma

$$(f + g)(x) = f(x) + g(x)$$

Ovvero,

$$\begin{aligned} f(x) &= \sum_{i=0}^d a_i x^i \\ g(x) &= \sum_{i=0}^{d'} b_i x^i \\ (f + g)(x) &= \sum_{i=0}^{\max(d, d')} (a_i + b_i) x^i \end{aligned}$$

16.3 Prodotto

$$(f \cdot g)(x) = f(x)g(x)$$

Ovvero,

$$\begin{aligned} f(x) &= \sum_{i=0}^d a_i x^i \quad \text{con } a_i = 0 \quad \forall i > d \\ g(x) &= \sum_{i=0}^{d'} b_i x^i \quad \text{con } b_i = 0 \quad \forall i > d' \\ c_t &= \sum_{i=0}^t a_i b_{t-i} \\ (f \cdot g)(x) &= \sum_{i=0}^{d+d'} c_i x^i \end{aligned}$$

Con queste operazioni, $(\mathcal{I}_k, +, \cdot)$ e' un gruppo abeliano (+ ass, + comm, + elem. neutro, + opposto), e' un anello commutativo ($\cdot$ ass., $\cdot$ comm, $\cdot$ distr rispetto a +), e' un anello unitario (esiste l'elem. unita'), e poiche' esiste la legge dell'annullamento del prodtto e' un dominio di integrita'.

16.4 Polinomio

Consideriamo un campo K .

$$S_k = \{s : \mathbb{N} \longrightarrow K\}$$

S_k e' l'insieme di tutte le funzioni che vanno da $\mathbb{N}$ a K , ovvero di tutte le successioni in K . Consideriamo ora un suo sottoinsieme $P_k \subset S_k$:

$$P_k = \{s : \mathbb{N} \longrightarrow K \mid \exists d \in \mathbb{N} : \forall m > d, s(m) = 0\}$$

Ovvero, P_k e' l'insieme delle successioni definitivamente nulle, cioe' di quelle successioni che a partire da un certo punto sono sempre 0.

$$s = (s_0, s_1, \dots, s_d, 0, 0, 0, \dots)$$

Un polinomio a coefficienti in K e' un elemento che appartiene a P_k .

Anche sui polinomi possiamo definire la somma e il prodotto: esattamente come abbiamo fatto prima. $(P_k, +, \cdot)$ e' un dominio di integrita', perche' gode delle nove proprieta'.

Ma cosa c'entra tutto questo con i polinomi usuali? Questa e' la risposta:

poniamo $a := (a, 0, 0, 0, \dots)$, $\forall a \in K$ e diamo anche queste definizioni:

$$\begin{aligned} x &:= (0, 1, 0, 0, 0, \dots) \\ x^2 &= x \cdot x = (0, 1, 0, 0, 0, \dots)(0, 1, 0, 0, 0, \dots) = (0, 0, 1, 0, 0, 0, \dots) \\ x^n &= (0, \dots, \underbrace{1}_{n+1 \text{ pos.}}, 0, \dots) \end{aligned}$$

Allora una qualsiasi successione $s \in P_k$, si puo' scrivere come:

$$\begin{aligned} s &= (a_0, a_1, \dots, a_d, 0, 0, 0, \dots) \\ &= (a_0, 0, \dots) + (a_1, 0, \dots)(0, 1, 0, \dots) + (a_2, 0, \dots)(0, 0, 1, \dots) + \\ &\quad + \dots + (a_d, 0, \dots)(0, 0, \dots, \underbrace{1}_{d+1 \text{ pos.}}, 0, \dots) \\ &= a_0 + a_1x + a_2x^2 + \dots + a_dx^d \end{aligned}$$

$P_k = K[x]$ e' l'anello dei polinomi a coefficienti in K sulla indeterminata x .

Ovviamente i polinomi sono legati alle funzioni polinomiali, possiamo infatti far corrispondere a un polinomio $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$, la funzione polinomiale $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_d\alpha^d$, $\alpha \in K$. Consideriamo allora la funzione

$$\varphi : K[x] \longrightarrow \mathcal{I}_k, \quad \varphi(f(x)) = \text{funzione polinomiale definita da } f(x)$$

che associa a ogni polinomio la sua funzione polinomiale corrispondente. Questa funzione e' sicuramente suriettiva, infatti, a ogni funzione polinomiale corrisponde il polinomio che ha gli stessi coefficienti. φ non e' pero' sempre iniettiva, anzi, nei campi finiti non lo e' il piu' delle volte. Ad esempio, considerando in $\mathbb{Z}_3$:

$$\begin{aligned} f(x) &= x^3 + x^2 + x + 1 & g(x) &= x^2 + 2x + 1 \\ f(0) &= 0 & g(0) &= 0 \\ f(1) &= 1 & g(1) &= 1 \\ f(2) &= 0 & g(2) &= 0 \end{aligned}$$

I polinomi $f(x), g(x)$ sono diversi tra loro, ma le funzioni polinomiali che gli corrispondono in $\mathbb{Z}_3$ sono uguali.

Se invece K e' infinito, φ e' anche iniettiva.

Proof: Proviamo l'iniettivita' di φ in K , campo infinito $|K| = \infty$.

Dire che e' iniettiva equivale a:

$$\varphi(f(x)) = \varphi(g(x)) \Rightarrow f(x) = g(x)$$

Supponiamo per assurdo che $f(x) \neq g(x)$.

Scegliamo questa funzione:

$$F(x) = f(x) - g(x) \neq 0$$

Dire $\varphi(f(x)) = \varphi(g(x))$ equivale ad affermare che:

$$\forall \alpha \in K, \varphi(f(x))(\alpha) = \varphi(g(x))(\alpha) \Leftrightarrow f(\alpha) = g(\alpha) \forall \alpha \in K$$

Allora tutte le α sono radici di $F(x)$, ma questo e' in assurdo con il corollario del teorema di ruffini (vedi [16.1,pg.66]), perche' vorrebbe dire che possiede infinite radici, invece, ruffini dice che ce ne sono al piu' $\deg F(x)$. Percio' $F(x)$ e' il polinomio nullo e quindi $f(x) = g(x)$ come polinomi. $\square$

16.5 Grado di un polinomio

Il grado di un polinomio

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$$

e' il massimo $i \in \mathbb{N} \mid a_i \neq 0$ e si indica con $\deg f(x)$. Ad esempio,

$$\deg(3^7 + 9x^2 + 0 \cdot x^{19} - 4x^3) = 3$$

Nota da questa definizione segue che il polinomio nullo non ha grado.

16.5.1 Proprieta'

Dato $\deg f(x) = m, \deg g(x) = n$, con $f(x), g(x) \neq 0$, allora

1. $\deg f(x) + g(x) \leq \max(m, n)$
2. $\deg f(x)g(x) = m + n$

16.6 Polinomi invertibili

Gli unici polinomi invertibili sono i polinomi costanti non nulli, cioe' che hanno grado 0, ovvero tutti gli elementi che appartengono al campo K .

Proof: Se per assurdo un polinomio $f(x)$ con grado $m \geq 1$ fosse invertibile, allora esisterebbe $g(x)$ t.c. $f(x)g(x) = 1$, ma questo e' impossibile perche' $\deg f(x)g(x) \geq 1$ $\square$

Quindi in $\mathbb{R}[x]$ esistono infiniti invertibili, mentre in $\mathbb{Z}_p$ ne esistono $p - 1$ (p primo).

16.7 Algoritmo di divisione in $K[x]$

Cosi' come abbiamo fatto nei campi numerici, possiamo stabilire una relazione di divisione anche in $K[x]$, cioe', dati $f(x), g(x) \in K[x]$

$$f(x)/_{g(x)} \Leftrightarrow \exists h(x) : g(x) = h(x)f(x)$$

A questo punto possiamo dedurre molte delle proprietà che avevamo visto in $\mathbb{Z}$. Ad esempio, possiamo ricavare l'algoritmo di divisione:

$$\forall f(x), g(x) \neq 0 \in K[x] \exists! q(x), r(x) \in K[x] \mid f(x) = q(x)g(x) + r(x)$$

e inoltre

$$r(x) = 0 \vee \deg r(x) < \deg g(x)$$

Proof: (non dimostriamo l'unicità).

Prendiamo i due polinomi: $f(x) = a_0 + a_1x + \dots + a_mx^m$, e $g(x) = b_0 + b_1x + \dots + b_nx^n$ e $m = \deg f(x)$, $n = \deg g(x)$.

Se $f(x)$ è il polinomio nullo, allora: $f(x) = 0 \cdot g(x) + 0$. Se $m < n$ allora abbiamo $f(x) = 0 \cdot g(x) + f(x)$. Quindi da adesso supponiamo $m \geq n$.

Procediamo per induzione:

1. Base: la base è stata già dimostrata con $f(x) = 0$.
2. Hp: supponiamo che per i polinomi di grado $< m$ il teorema sia vero.
3. Dimostriamo allora per il polinomio $f(x)$ che ha grado m .

Scegliamo questo opportuno polinomio:

$$F(x) = f(x) - a_mb_n^{-1}x^{m-n}g(x)$$

Il coefficiente $a_mb_n^{-1}x^{m-n}$ serve per sostituire b_mx^n con a_mx^m in $g(x)$, infatti, $(a_mb_n^{-1}x^{m-n})(b_nx^n) = a_mx^m$. Poiché a_mx^m è presente in $f(x)$, quando facciamo $f(x) - a_mx^m$, viene eliminato da $F(x)$, quindi $\deg F(x) < m$. Allora per l'Hp induttiva, possiamo scrivere:

$$f(x) - a_mb_n^{-1}x^{m-n}g(x) = q'(x)g(x) + r(x)$$

$$f(x) = a_mb_n^{-1}x^{m-n}g(x) + q'(x)g(x) + r(x)$$

$$= (a_mb_n^{-1}x^{m-n} + q'(x))g(x) + r(x)$$

Inoltre sempre per l'Hp induttiva $\deg r(x) < \deg g(x)$ oppure $r(x) = 0$

□

16.8 Polinomi associati

$$f(x), g(x) \equiv \text{associati} \Leftrightarrow f(x)/g(x) \wedge g(x)/f(x)$$

L'associato di $f(x)$ è

$$f(x)a, \quad \forall a \in K^*$$

16.9 Polinomi primi

$$f(x) \equiv \text{primo} \Leftrightarrow (f(x)/g(x)h(x) \Rightarrow f(x)/g(x) \vee f(x)/h(x))$$

16.10 Polinomio irriducibile

$f(x)$ è irriducibile $\Leftrightarrow$ vale la seguente implicazione:

$$f(x) = g(x)h(x) \Rightarrow h(x) \equiv \text{invertibile} \vee g(x) \equiv \text{invertibile}$$

Ovvero $f(x)$ è irriducibile se tutti i suoi fattori, tranne uno, sono costanti non nulle. Un polinomio di primo grado e una costante sono entrambi irriducibili.

Vale sempre il seguente teorema:

$$f(x) \equiv \text{irriducibile} \Leftrightarrow f(x) \equiv \text{primo}$$

16.11 MCD di polinomi

Il MCD di due polinomi è definito come quello che abbiamo usato su $\mathbb{Z}$:

$$d = \text{MCD}(f(x), g(x)) \Leftrightarrow d \mid f(x) \wedge d \mid g(x) \wedge (d' \mid f(x) \wedge d' \mid g(x) \Rightarrow d' \mid d)$$

Il MCD si può calcolare con l'algoritmo euclideo, che si può applicare sui polinomi. (In questo caso l'algoritmo compie un numero finito di passi perché il grado del resto diminuisce sempre più, fino a quando si arriva al resto-polinomio-nullo).

Dall'algoritmo euclideo si ricava sempre l'identità di Bezout:

$$\text{MCD}(f(x), g(x)) = \lambda(x)f(x) + \mu(x)g(x)$$

16.12 Fattorizzazione unica di un polinomio

Così come in $\mathbb{Z}$ un polinomio si può fattorizzare in maniera unica. Stavolta, però, non solo a meno dell'ordine e del segno, ma anche a meno di invertibili.

Ad esempio:

$$x^2 - 1 = (x - 1)(x + 1) = \left(\frac{1}{2}x - \frac{1}{2}\right)(2x + 2) = x^2 - 1$$

La dimostrazione è identica a quella usata in $\mathbb{Z}$.

16.13 Teorema di Ruffini

$\alpha \in K$ è una radice di $f(x) \in K[x]$ se $f(\alpha) = 0$.

Il teorema di Ruffini dice che:

$$f(\alpha) = 0 \Rightarrow f(x) = (x - \alpha)f'(x)$$

Come corollario deduciamo che se $\deg f(x) \geq 2 \wedge f(\alpha) = 0$ allora $f(x)$ è riducibile.

Proof: Per l'algoritmo di divisione di un polinomio possiamo scrivere:

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

Se $\deg r(x) < \deg(x - \alpha)$ allora $\deg r(x) < 1$, ovvero $r(x) = c$ è un polinomio costante.

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha)$$

$$f(\alpha) = 0, \quad r(\alpha) = c$$

$$0 = 0 \cdot q(\alpha) + c$$

$$0 = c$$

E questo è assurdo, quindi l'algoritmo di divisione ci dice che necessariamente $r(x) = 0$, ovvero

$$f(x) = (x - \alpha)q(x)$$

□

Proposition 16.1. Sia $f(x) \in K[x] \setminus \{0\}$, $\deg f(x) = n$, allora $f(x)$ ha al più n radici.

Proof: Se $f(x)$ è irriducibile³, allora ha ≤ 1 radici, infatti, se $f(\alpha) = 0$, per Ruffini si ha $f(x) = (x - \alpha)q(x) \Rightarrow f(x)$ riducibile $\vee q(x) = c \in F \xRightarrow{f(x) \text{ irriducibile}} q(x) = c \Rightarrow f(x) = c(x - \alpha)$ ha 1 radice

Supponiamo allora che $f(x)$ sia riducibile.

Lavoriamo per induzione.

Base: $n = 0$, il polinomio di grado 0 ha 0 radici.

³essendo irriducibile, per definizione, non è invertibile, e quindi $\deg f(x) \geq 1$

Hp: tutti i polinomi di grado $n - 1$ hanno al più $n - 1$ radici.

Ts: Per Ruffini, il polinomio $f(x)$ con grado n , e' $f(x) = (x - \alpha)q(x)$. Poiche' $f(x)$ e' riducibile, si ha $\deg q(x) = n - 1$, quindi per l'Hp induttiva, $q(x)$ ha al più $n - 1$ radici. E in definitiva, essendo α una radice di $f(x)$, concludiamo che $f(x)$ ha al più n radici. $\square$

16.14 Molteplicita'

Una radice α di $f(x)$ ha molteplicita' m se:

$$f(x) = (x - \alpha)^m h(x)$$

dove $h(x) \neq 0$.

Possiamo esprimere il corollario di ruffini dicendo che la somma delle molteplicita' delle radici di un $f(x)$ e' al più $\deg f(x)$.

16.15 Irriducibilita' di un polinomio in $\mathbb{C}[x]$

Un polinomio in $\mathbb{C}[x]$ e' irriducibile $\Leftrightarrow$ ha grado 1. Ovvero, tutti i polinomi con grado > 1 sono riducibili.

A questo risultato si arriva attraverso il teorema fondamentale dell'Algebra che dice che tutti i polinomi in $\mathbb{C}[x]$ di grado ≥ 1 hanno almeno una radice.

Inoltre, sempre dal TFA possiamo affermare che $f(x) \in \mathbb{C}[x]$ ha esattamente $\deg f(x)$ radici.

Proof: Proviamo questo a partire dal TFA e usando l'induzione.

Base: per $n = 1$, e' ovviamente vero.

Hp: tutti i polinomi di grado $m < n$ hanno esattamente m radici.

Ts: Prendiamo $f(x) \in \mathbb{C}[x]$, $\deg f(x) = n$. Per il teorema fondamentale dell'algebra sappiamo che $f(x)$ ha almeno una radice $f(\alpha_1)$, allora per ruffini:

$$f(x) = (x - \alpha_1)h(x)$$

Poiche' $\deg h(x) = n - 1 < n$, entra in gioco l'Hp induttiva, e quindi $h(x)$ ha esattamente $n - 1$ radici. Dato che α_1 e' una radice di $f(x)$, $f(x)$ avra' in totale n radici. $\square$

16.15.1 Coniugato di un polinomio

Dato

$$f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{C}[x]$$

chiamiamo $\overline{f(x)}$ coniugato di $f(x)$

$$\overline{f(x)} = \overline{a_0} + \overline{a_1}x + \dots + \overline{a_d}x^d$$

Dove $\overline{a_i}$ e' il coniugato di a_i .

Vale la seguente proprieta':

$$f(\alpha) = 0 \Rightarrow \overline{f(\alpha)} = 0$$

α e' radice di $f(x)$ e $\overline{\alpha}$ e' radice di $\overline{f(x)}$.

16.15.2 Fattorizzazione in $\mathbb{C}$

In $\mathbb{C}[x]$, conoscendo le radici di $f(x)$, possiamo fattorizzare $f(x)$ in:

$$f(x) = (x - a_1) \dots (x - a_r)g_1(x) \dots g_t(x)$$

dove $a_i \in \mathbb{R}$ sono le radici reali di $f(x)$ e

$$g_i(x) = x^2 - (\alpha_i + \overline{\alpha_i})x + \alpha_i \overline{\alpha_i}$$

e dove α_i sono le radici complesse di $f(x)$.

16.16 Irriducibilit  di un polinomio in $\mathbb{R}$

Osserviamo che $\mathbb{R}[x] \subseteq \mathbb{C}[x]$.

Data $f(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$, accade che

$$f(x) = \overline{f(x)}$$

, perche' i coefficienti di $f(x)$ sono nella forma $(a, 0)$ e quindi $(a, 0) = (a, -0)$.

Questo significa che se un polinomio in $\mathbb{R}[x]$ ammette una radice complessa, allora ammetter  anche la sua coniugata. Quindi in $\mathbb{R}[x]$ le radici complesse vanno sempre a coppia.

Accade che:

$$f(x) \in \mathbb{R}[x] \equiv \text{irriducibile} \Leftrightarrow \deg f(x) = 1 \vee (\deg f(x) = 2 \wedge \Delta < 0)$$

In tutti gli altri casi e' riducibile, cioe' per

$$\deg f(x) > 2 \vee (\deg f(x) = 2 \wedge \Delta \geq 0)$$

Proof: Dimostriamo $\Leftarrow$.

Se e' di grado 1 e' ovviamente irriducibile.

Se e' di grado 2 e $\Delta < 0$, allora non ha radici in $\mathbb{R}$, quindi non puo' essere ridotto. $\square$

Proof: Sia $f(x)$ il nostro polinomio di grado n .

Dimostriamo $\Rightarrow$, facendo vedere che per

$$n > 2 \vee (n = 2 \wedge \Delta \geq 0)$$

e' riducibile. Se $n = 2 \wedge \Delta \geq 0$, allora $f(x)$ ha radici in $\mathbb{R}$ e quindi per il corollario di ruffini, puo' essere ridotto.

Adesso andiamo in $n > 2$.

Distinguiamo due casi:

1. Se n e' dispari, e' della forma $n = 2m + 1$, $m \geq 1$. Per quando abbiamo visto prima, ogni radice complessa in $f(x)$ e' in coppia con il suo coniugato, quindi nel peggiori dei casi ci sarebbero m coppie di radici complesse.

L'ultima radice rimanente α_m deve essere necessariamente reale perche' dato che non esistono piu' altre radici deve essere uguale alla sua coniugata (che e' sempre ammessa da $f(x)$, cioe':

$$\alpha_m = \overline{\alpha_m}$$

Ovvero:

$$(a, b) = (a, -b) \Rightarrow b = 0$$

e quindi $\alpha_m \in \mathbb{R}$.

2. Se n e' pari allora distinguiamo due ulteriori casi:

- a. $f(x)$ ammette delle radici in $\mathbb{R}$. In questo caso abbiamo finito, dato che per il corollario di ruffini e' riducibile.

- b. $f(x)$ ha solo radici complesse, cioe':

$$f(x) = (x - \alpha_1)(x - \overline{\alpha_1}) \dots (x - \alpha_n)(x - \overline{\alpha_n})$$

Analizziamo $(x - \alpha_1)(x - \overline{\alpha_1})$:

$$\begin{aligned} (x - \alpha_1)(x - \overline{\alpha_1}) &= \\ &= x^2 - (\alpha_1 + \overline{\alpha_1})x + \alpha_1 \overline{\alpha_1} \end{aligned}$$

Ma poiche' $\alpha_1 + \overline{\alpha_1} \in \mathbb{R}$ e $\alpha_1 \overline{\alpha_1} \in \mathbb{R}$, allora

$$x^2 - (\alpha_1 + \overline{\alpha_1})x + \alpha_1 \overline{\alpha_1} \in \mathbb{R}[x]$$

Possiamo ripetere questo per tutti gli altri blocchi di coppie di radici complesse, ottenendo:

$$f(x) = (x^2 - (\alpha_1 + \overline{\alpha_1})x + \alpha_1 \overline{\alpha_1}) \dots (x^2 - (\alpha_n + \overline{\alpha_n})x + \alpha_n \overline{\alpha_n})$$

□

16.17 Irriducibilita' di un polinomio in $\mathbb{Q}$

Dato $f(x) \in \mathbb{Q}[x]$, cioe':

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \dots + \frac{a_n}{b_n}x^n$$

possiamo ricondurlo come prodotto di un polinomio con i coefficienti in $\mathbb{Z}$ per una costante, cioe':

$$f(x) = \frac{1}{m} (a'_0 + a'_1x + \dots + a'_nx^n)$$

Dove m e' il mcm tra $b_0, \dots, b_n$ e

$$a'_i = a_i \frac{m}{b_i}$$

. Le radici di $f(x)$ si ottengono con questo procedimento:

$$D_0 = \{\text{divisori di } a'_0\}$$

$$D_n = \{\text{divisori di } a'_n\}$$

$$S = \left\{ \frac{\alpha}{\beta} \mid \alpha \in D_0, \beta \in D_n \right\}$$

$$R = \{ \text{Radici razionali di } f(x) \}$$

$$R \subseteq S$$

Se si trovano le radici del polinomio, allora per ruffini si puo' ridurre, pero' se non si trovano non c'e' alcun modo per sapere se si puo' ridurre o no.

Proof: Dimostriamo che le radici razionali di $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ sono contenute nell'insieme S , ovvero, dati $r, s \in \mathbb{Z} : MCD(r, s) = 1$,

$$f\left(\frac{r}{s}\right) = 0 \Rightarrow r/a_0, s/a_n$$

quindi, per Hp:

$$a_0 + a_1 \frac{r}{s} + \dots + a_n \left(\frac{r}{s}\right)^n = 0$$

$$a_0 s^n + a_1 s^{n-1} r + \dots + a_n r^n = 0$$

$$a_n r^n = -s(a_0 s^{n-1} + a_1 s^{n-2} r + \dots + a_{n-1} r^{n-1})$$

Prendiamo un primo $p : p/s$, ovvero un divisore di s . p divide il secondo membro e quindi divide anche il primo, cioe' $p/a_n r^n$, poiche' $MCD(r, s) = 1$ deduciamo che p , divisore di s , deve necessariamente dividere a_n . Poiche' possiamo ripetere lo stesso ragionamento per tutti i divisori di s deduciamo che s/a_n . Analogamente si vede che r/a_0 □

16.18 Polinomio primitivo

Definition 16.2. Dato $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$, il contenuto di $f(x)$ e'

$$c(f) = MCD(a_0, \dots, a_n)$$

Se $c(f) = 1$, allora si dice che $f(x)$ e' un polinomio primitivo.

Dato un polinomio non primitivo $f(x)$, lo possiamo esprimere come:

$$f(x) = c(f)f'(x)$$

basta mettere in evidenza il MCD dei coefficienti di $f(x)$ e ottenere quindi $f'(x)$. $f'(x)$ sara' primitivo.

16.19 Lemma di Gauss

$$f(x), g(x) \in \mathbb{Z}[x], c(f) = 1, c(g) = 1 \Rightarrow c(f(x)g(x)) = 1$$

Proof: Dimostriamolo per assurdo.

Dati:

$$\begin{aligned} f(x) &= a_0 + a_1x + \dots + a_ix^i \\ g(x) &= b_0 + b_1x + \dots + b_jx^j \\ f(x)g(x) &= c_0 + c_1x + \dots + c_{i+j}x^{i+j} \\ d &= MCD(c_0, c_1, \dots, c_{i+j}) \neq 1 \end{aligned}$$

Sia p primo tale che p/d , allora $p/c_i \forall i$. Poiche' $c(f) = 1$, ci sara' una a_i che non e' divisa da p , analogamente ci sara' una b_j che non e' divisa da p , allora dato che

$$c_{i+j} = (a_0b_{i+j} + a_1b_{i+j-1} + \dots) + a_ib_j + (\dots + a_{i+j}b_j)$$

e che p/c_{i+j} e che p divide la prima parentesi e la seconda allora p deve dividere anche a_ib_j . Poiche' p e' primo, possono accadere due casi:

$$p/a_i \vee p/b_j$$

ma tutte e due casi sono assurdi. □

16.20 Corollario del lemma di Gauss

$$c(f \cdot g) = c(f)c(g)$$

Proof: Possiamo scrivere i due polinomi come abbiamo visto in 16.2:

$$f(x) = c(f)f'(x)$$

$$g(x) = c(g)g'(x)$$

Moltiplichiamo membro a membro e otteniamo:

$$f(x)g(x) = c(f)c(g)f'(x)g'(x)$$

Inoltre,

$$c(c(f)c(g)f'(x)g'(x)) = c(f)c(g) \cdot 1$$

$(c(f'(x)g'(x))) = 1$ perche' f' e g' sono primitivi). allora ecco la tesi:

$$c(f(x)g(x)) = c(c(f)c(g)f'(x)g'(x)) = c(f)c(g)$$

□

16.21 Irriducibilita' in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$

Proposition 16.3. Se $f(x) \in \mathbb{Z}[x]$ e' primitivo allora:

$$f \text{ irriducibile in } \mathbb{Z}[x] \Leftrightarrow \text{irriducibile in } \mathbb{Q}[x]$$

Proof: Dim $\Rightarrow$.

Per assurdo supponiamo che $f(x) \in \mathbb{Q}[x]$ sia riducibile, ovvero:

$$\begin{aligned} f(x) &= h(x)g(x), \quad h(x), g(x) \in \mathbb{Q}[x] \\ \deg h(x), \deg g(x) &> 0 \end{aligned}$$

Riesprimiamo in $\mathbb{Z}$ h e g :

$$h(x) = \frac{a}{b}h'(x), \quad h'(x) \in \mathbb{Z}[x], \text{ primitivo}$$

$$g(x) = \frac{c}{d}g'(x), \quad g'(x) \in \mathbb{Z}[x], \text{ primitivo}$$

sostituiamo:

$$f(x) = \frac{a}{b}h'(x)\frac{c}{d}g'(x)$$

normalizziamo:

$$bdf(x) = ach'(x)g'(x)$$

prendiamo il contenuto del primo e del secondo membro:

$$c(bdf(x)) = bd \text{ perche' } f(x), \text{ per Hp e' primitivo, } bd \text{ e' una costante}$$

$$c(ach'(x)g'(x)) = ac \text{ i polin } h', g' \text{ sono primitivi}$$

$$bd = ac \Rightarrow bdf(x) = bdh'(x)g'(x) \Rightarrow f(x) = h'(x)g'(x) \in \mathbb{Z}[x]$$

ma $f(x) = h'(x)g'(x)$ e' assurdo perche' abbiamo supposto che fosse irriducibile in $\mathbb{Z}[x]$ □

Proof: Dim $\Leftarrow$.

Supponiamo per assurdo che f e' riducibile in $\mathbb{Z}[x]$, quindi:

$$f(x) = h(x)g(x) \quad h(x), g(x) \in \mathbb{Z}[x]$$

$$h(x) \neq \pm 1 \quad g(x) \neq \pm 1$$

Inoltre $\deg h(x), \deg g(x)$ devono essere necessariamente > 0 , infatti, se fosse $\deg h(x) = 0 \Rightarrow h(x) = h \neq \pm 1 \in \mathbb{Z}$ il che' implicherebbe che $f(x)$ non e' primitivo, contro ipotesi. Quindi:

$$\deg h(x), \deg g(x) > 0$$

Poiche' possiamo pensare $g(x), h(x)$ come polinomi di $\mathbb{Q}[x]$,cioe':

$$g(x), h(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$$

segue che: $f(x)$ e' riducibile in $\mathbb{Q}[x]$, e questo e' assurdo, contro l'Hp iniziale. □

16.22 Teorema di Gauss

Per qualunque dominio D che sia UFD (dominio a fattorizzazione unica), vale che $D[x]$ e' UFD.

Proof: Dimostreremo il teorema solo per $\mathbb{Z}[x]$.

Dato $f(x) \in \mathbb{Z}[x]$, possiamo esprimerlo come

$$f(x) = c(f)f'(x)$$

$c(f) \in \mathbb{Z}$ e' un numero intero, quindi si puo' fattorizzare. Resta quindi da fattorizzare $f'(x)$, polinomio primitivo.

Sappiamo che in $\mathbb{Q}[x]$ e' fattorizzabile, quindi:

$$f'(x) = q_1(x) \dots q_t(x), \quad q_i(x) \in \mathbb{Q}[x]$$

Mettiamo in evidenza al solito modo il MCD dei coefficienti di q_i :

$$f'(x) = \frac{a_1}{b_1}q'_1(x) \dots \frac{a_t}{b_t}q'_t(x), \quad q'_i(x) \in \mathbb{Z}[x]$$

dove b_i e' il mcm dei denominatori dei coefficienti di $q_i(x)$, e a_i e' il contenuto di $\frac{b_i}{b_i}q_i(x)$.

Normalizziamo:

$$b_1 \dots b_t f'(x) = a_1 \dots a_t q'_1(x) \dots q'_t(x)$$

tenendo a mente che $f'(x), q'_i(x)$ sono primitivi, prendendo i contenuti di ambo i membri otteniamo:

$$b_1 \dots b_t = a_1 \dots a_t$$

e quindi

$$f'(x) = q'_1(x) \dots q'_t(x)$$

ed ecco che abbiamo fattorizzato $f'(x)$ in $\mathbb{Z}[x]$. □

16.23 Criterio di Eisenstein

Sia

$$f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbb{Z}[x]$$

e sia primitivo, allora

$$\begin{cases} f \equiv \text{primitivo} \\ \exists p, \text{primo} : p/a_i, i = 0, \dots, d-1 \\ p^2 \nmid a_0 \end{cases} \Rightarrow f(x) \equiv \text{irriducibile in } \mathbb{Z}[x], \mathbb{Q}[x]$$

Proof: Supponiamo che per assurdo $f(x)$ sia riducibile, ovvero che:

$$\begin{aligned} f(x) &= g(x)h(x) \\ g(x) &= b_0 + b_1x + \cdots + b_rx^r, \quad h(x) = c_0 + c_1x + \cdots + c_sx^s \\ 0 &< r < d \wedge 0 < s < d \end{aligned}$$

$g(x), h(x)$ sono polinomi primitivi, perche' per Hp $f(x)$ lo e' pure e quindi per il Lemma di Gauss anche loro devono esserlo. $a_0 = b_0c_0$ e per Hp il primo p divide a_0 , cioe'

$$p/a_0 \Rightarrow p/b_0 \vee p/c_0$$

In questo caso pero', possiamo sicuramente affermare che $p \nmid c_0$, infatti, se cosi' fosse, e se p/b_0 , accadrebbe che:

$$\begin{aligned} \lambda p &= b_0 & \mu p &= c_0 \\ \lambda \mu p^2 &= a_0 \Rightarrow p^2/a_0 \end{aligned}$$

Ma per Hp $p^2 \nmid a_0$.

Adesso ricordandoci che $g(x)$ e' primitivo, possiamo dedurre che p potra' dividere al piu' tutti i suoi coefficienti, tranne uno, cioe':

$$p/b_0, p/b_1, \dots, p/b_{i-1}, p \nmid b_i, i < r$$

Adesso, consideriamo

$$a_i = c_0b_i + c_1b_{i-1} + \cdots + c_{i-1}b_1 + c_ib_0$$

Per Hp sappiamo che p/a_i e abbiamo visto che p divide tutti i b_j , $j = 0, \dots, i-1$, quindi dividera' anche

$$K = c_1b_{i-1} + \cdots + c_{i-1}b_1 + c_ib_0$$

allora, dividera' pure $a_i - K$, ma poiche'

$$a_i - K = c_0b_i$$

segue che

$$p/c_0 \vee p/b_i$$

Ma in entrambi i casi abbiamo visto che questo e' impossibile, quindi tutto questo e' assurdo. $\square$

16.24 Criterio di riduzione modulo p

Prima di tutto premettiamo alcune definizioni.

Un polinomio si dice monico se il coefficiente dell'indeterminata di grado massimo e' 1.

In $\mathbb{Z}_n[x]_d$, possono esistere n^{d+1} polinomi distinti, dove d e' il loro grado, infatti, ogni coefficiente di un'indeterminata puo' assumere i valori da $0, 1, \dots, n-1$, percio' se abbiamo $d+1$ coefficienti, tutte le possibili combinazioni sono

$$\underbrace{n \cdot n \cdots n}_{d+1 \text{ volte}}$$

Se invece stiamo considerando polinomi monici in $\mathbb{Z}_n[x]_d$, allora in totale sono n^d , perche' il coefficiente di x^d sara' sempre 1.

Facciamo un esempio di come si controlla se un polinomio in $\mathbb{Z}n[x]$ e' irriducibile. Consideriamo il polinomio

$$f(x) = x^4 + x + 4 \in \mathbb{Z}_5[x]$$

Prima di tutto controlliamo se ha radici:

$$\begin{aligned} f(0) &= 4 & f(1) &= 1 & f(2) &= 2 \\ f(3) &= (-2)^4 - 2 + 4 = 18 = 3 & f(4) &= (-1)^4 - 1 + 4 = 4 \end{aligned}$$

Quindi non ha radici in $\mathbb{Z}_5[x]$, e quindi sappiamo che non si puo' scomporre come prodotto di un polinomio di terzo grado e uno di primo. Adesso controlliamo se si puo' scomporre come prodotto di due polin. di secondo grado, ovvero dobbiamo risolvere questo:

$$x^4 + x + 4 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (bc + ad)x + bd$$

che corrisponde a risolvere questo:

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ bc + ad = 1 \\ bd = 4 \end{cases} \Rightarrow \begin{cases} c = -a \\ b - a^2 + d = 0 \\ a(d - b) = 1 \\ bd = 4 \end{cases}$$

$bd = 4$ e' vera solo in questi casi:

$$\begin{aligned} b = 1 & \quad d = 4 \\ b = 2 & \quad d = 2 \\ b = 3 & \quad d = 3 \\ b = 4 & \quad d = 1 \end{aligned}$$

Se fossero veri il secondo e il terzo caso allora $a(d - b) = 1$ non avrebbe senso, perche' $a \cdot 0 \neq 1$. Se, invece, fosse vero il primo o l'ultimo caso si avrebbe che $b - a^2 + d = 5 - a^2 = -a^2 = 0 \Rightarrow a = 0$. Ma questo rende sempre assurdo $a(d - b) = 1$. Quindi, in conclusione, il sistema non ammette soluzioni e percio' il polinomio e' irriducibile in $\mathbb{Z}_5[x]$.

Adesso arriviamo al criterio vero e proprio.

Sia

$$f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}[x]$$

e sia primitivo, allora

$$\exists p, \text{ primo} : p \nmid a_d, \wedge f(x) \text{ irriducibile in } \mathbb{Z}_p[x] \Rightarrow f(x) \text{ irriducibile in } \mathbb{Z}[x]$$

Proof: Dimostriamo per assurdo, e supponiamo quindi che $f(x)$ sia riducibile in $\mathbb{Z}$, ovvero:

$$\begin{aligned} f(x) &= g(x)h(x) \\ g(x) &= b_0 + b_1x + \dots + b_rx^r, \quad h(x) = c_0 + c_1x + \dots + c_sx^s \\ 0 &< r < d \wedge 0 < s < d, \quad r + s = d \end{aligned}$$

$g(x), h(x)$ sono polinomi primitivi, perche' per Hp $f(x)$ lo e' pure e quindi per il Lemma di Gauss anche loro devono esserlo. $a_d = b_rc_s$ e per Hp il primo p non divide a_d , cioe'

$$p \nmid a_d \Rightarrow p \nmid b_r \wedge p \nmid c_s$$

Adesso andiamo in $\mathbb{Z}_p[x]$.

$$\deg[f(x)]_p = d$$

Ovvero il grado di $f(x)$ in $\mathbb{Z}_p[x]$ non cambia, perche' dato che $p \nmid a_d$ la classe $[a_d] \neq 0$ e quindi l'indeterminata col grado d non viene eliminata. Lo stesso accade per $[g(x)], [h(x)]$ perche'

$$p \nmid b_r \wedge p \nmid c_s$$

Quindi,

$$f(x) = g(x)h(x) \pmod{\mathbb{Z}_p[x]}$$

ma questo e' assurdo perche' abbiamo scomposto $f(x) \in \mathbb{Z}_p[x]$ quando per Hp avevamo supposto che questo non era possibile. $\square$

Un esempio. Considera

$$f(x) = x^4 + 25x^3 + 6x + 84 \in \mathbb{Q}[x]$$

Poniamo $p = 5$:

$$[f(x)]_5 = x^4 + x + 4 \in \mathbb{Z}_5[x]$$

ma, per quanto abbiamo calcolato prima, sappiamo che $x^4 + x + 4$ e' irriducibile in $\mathbb{Z}_5[x]$, quindi $f(x)$ e' irriducibile in $\mathbb{Z}[x]$ e conseguentemente in $\mathbb{Q}[x]$.

17 Anelli

Dato un insieme A e due operazioni binarie interne su A indicate con $+$ e $\cdot$, possono valere queste proprieta':

1. $+$ e' associativa:

$$\forall a, b, c \in A \quad (a + b) + c = a + (b + c)$$

2. $+$ e' commutativa:

$$\forall a, b \in A \quad a + b = b + a$$

3. Esiste l'elemento neutro dell'addizione:

$$\exists 0_A \in A : \forall a \in A \quad 0_A + a = a + 0_A = a$$

4. In $+$ esiste l'opposto:

$$\forall a \in A \quad \exists -a \in A \mid a + (-a) = (-a) + a = 0_A$$

5. $\cdot$ e' associativa:

$$\forall a, b, c \in A \quad (ab)c = a(bc)$$

6. $\cdot$ e' distributiva rispetto all'addizione:

$$\forall a, b, c \in A \quad a(b + c) = ab + ac \wedge (a + b)c = ac + bc$$

7. $\cdot$ e' commutativa:

$$\forall a, b \in A \quad ab = ba$$

8. Esiste l'elemento neutro del prodotto:

$$\exists 1_A \in A : \forall a \in A \quad 1_A a = a 1_A = a$$

a Le proprietà' dalla 1 alla 4 rendono $(A, +)$ un gruppo abeliano (cioe' un gruppo commutativo).
 Le proprietà' dalla 1 alla 6 rendono $(A, +, \cdot)$ un anello.
 Le proprietà' dalla 1 alla 7 rendono $(A, +, \cdot)$ un anello commutativo.
 Le proprietà' dalla 1 alla 6 e la otto rendono $(A, +, \cdot)$ un anello unitario.
 Le proprietà' dalla 1 alla 8 rendono $(A, +, \cdot)$ un anello commutativo unitario.

Theorem 17.1. *Dato un anello $(A, +, \cdot)$ qualsiasi, possiamo dedurre che*

$$0 \cdot x = x \cdot 0 = 0 \quad \forall x \in A$$

Proof:

$$\begin{aligned} y &= 0x = (0 + 0)x \quad \text{prop. 3} \\ (0 + 0)x &= 0x + 0x = y + y \quad \text{prop. 6} \\ y &= y + y \\ (-y) + y &= y + y + (-y) \\ y + y + (-y) &= y + (y + (-y)) \quad \text{prop. 1} \\ y + (y + (-y)) &= y + 0 = y \quad \text{prop. 4, 3} \\ (-y) + y &= y \Rightarrow 0 = y \\ 0x &= 0 \end{aligned}$$

□

Puo' accadere che il prodotto di due elementi non nulli sia uguale a 0, ad esempio in $\mathbb{Z}_{10}$ $2 \cdot 5 = 0$, o anche in $M \in Q^{2,2}$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Questo significa che in generale la legge dell'annullamento del prodotto

$$ab = 0 \Rightarrow a = 0 \vee b = 0$$

non vale. Allora, dato un elemento $u \in A, u \neq 0$

$$u \equiv \text{divisore dello zero} \Leftrightarrow \exists u', u'' \neq 0 \mid uu' = 0 = u''u = 0$$

Un *dominio d'integrita'* e' un anello commutativo, non necessariamente unitario, dove non esistono divisori dello zero, ovvero dove vale la legge dell'annullamento del prodotto.

Sia A un anello unitario, allora

$$u \in A \equiv \text{invertibile} \Leftrightarrow \exists u' \in A : uu' = u'u = 1_A$$

u' si denotera' con u^{-1} .

Per quanto abbiamo dimostrato prima ($0x = 0$), lo zero non potra' mai essere un elemento invertibile.

La proprietà' 9) e': tutti gli elementi dell'anello $(A, +, \cdot)$ unitario, tranne lo zero, sono invertibili.

Un *corpo* e' un anello unitario in cui tutti gli elementi diversi da zero sono invertibili.

Un *campo* e' un corpo commutativo, cioe' e' un corpo in cui il prodotto e' commutativo. Quindi in un campo valgono tutte e nove le proprietà'.

Proposition 17.2. *Un corpo e' un dominio d'integrita':*

$$D \text{ corpo} \Rightarrow D \text{ dominio}$$

Proof: Se $a \neq 0$, $ab = 0$, allora, poiche' siamo in un corpo $\exists a^{-1}$ e quindi:

$$a^{-1}ab = a^{-1}0 \Rightarrow b = 0$$

□

Un teorema afferma che ogni corpo finito e' un campo.

17.1 I quaternioni

I quaternioni sono un corpo infinito non commutativo, ovvero non sono un campo. I quaternioni sono stati inventati come generalizzazioni dei numeri complessi e sono descritti dal seguente insieme di matrici 2×2 :

$$\mathbb{Q}_R = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$$

Per verificare che i quaternioni sono un campo, dobbiamo controllare prima di tutto che le operazioni tra due elementi sono delle operazioni interne:

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} + \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha + \gamma & \beta + \delta \\ -\bar{\beta} - \bar{\delta} & \bar{\alpha} + \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha + \gamma & \beta + \delta \\ -\overline{\beta + \delta} & \overline{\alpha + \gamma} \end{pmatrix}$$

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\bar{\beta}\gamma - \bar{\alpha}\bar{\delta} & -\bar{\beta}\delta + \bar{\alpha}\bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\overline{\alpha\delta + \beta\bar{\gamma}} & \overline{\alpha\gamma - \beta\bar{\delta}} \end{pmatrix}$$

Le 8 proprieta' si verificano facilmente, anche perche', valendo nell'anello delle matrici quadrate 2×2 valgono anche qui. Verifichiamo quindi che tutti gli elementi diversi dall'elemento nullo sono invertibili. Poiche' una matrice e' invertibile sse il suo det e' diverso da zero, controlliamo

$$\begin{vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{vmatrix} = \alpha\bar{\alpha} + \beta\bar{\beta} \neq 0$$

Poiche' $(a + ib)(a - ib) = a^2 + b^2$, allora

$$\alpha\bar{\alpha} + \beta\bar{\beta} = a^2 + b^2 + c^2 + d^2$$

che e' = 0 solo per $a = b = c = d = 0$.

Per dimostrare che questo corpo non e' commutativo basta portare un esempio:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \neq \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

I quaternioni possono essere scritti in forma algebrica ponendo:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = j \quad \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = k$$

e quindi avendo $\alpha = a + ib$, $\beta = c + id$:

$$\mathbb{Q}_R = \{a + ib + jc + kd \mid a, b, c, d \in \mathbb{R}\}$$

17.2 Domini finiti

Ogni dominio finito e' un campo.

Ovvero in ogni anello commutativo finito in cui vale la legge dell'annullamento del prodotto e' un campo, cioe' tutti gli elementi diversi da 0 ammettono l'inverso. Formalmente:

$$D \equiv \text{dominio}, |D| = n \in \mathbb{N} \Rightarrow D \equiv \text{campo}$$

Proof: Prima di tutto dobbiamo mostrare che D possiede l'elemento unita' del prodotto.

Se D e' finito e ha n elementi possiamo scrivere:

$$D = \{a_1, \dots, a_n\}$$

Prendiamo un qualsiasi $a \neq 0 \in D$ e consideriamo questo suo sottoinsieme:

$$C = \{aa_1, \dots, aa_n\}$$

(abbiamo moltiplicato tutti gli elementi di D per a).

Due elementi di C non coincidono mai, infatti, per assurdo:

$$a_i \neq a_j \quad i \neq j$$

$$aa_i = aa_j$$

$$a(a_i - a_j) = 0 \Rightarrow a_i = a_j$$

Quindi $|C| = n$ e quindi $C = D$. Allora, dato che $a \in D$, possiamo scrivere:

$$a = aa_u$$

Quindi a_u e' un elemento unitario. Dobbiamo dimostrare pero' che e' unitario anche per tutti gli altri elementi di D , cioe'

$$\forall b \in D \Rightarrow b \in C \Rightarrow b = aa_k$$

$$ba_u = aa_k a_u$$

$$ba_u = aa_u a_k = aa_k = b \Rightarrow ba_u = b$$

Ok, poniamo $1 := a_u$ e adesso mostriamo che tutti gli elementi di D diversi da zero sono invertibili, infatti,

$$1 \in D \Rightarrow 1 \in C \Rightarrow 1 = aa_t$$

$$1 = aa_t \Rightarrow a^{-1} = a_t$$

In questo caso, abbiamo visto che a ha l'inverso, ma inizialmente, a e' stato scelto come un elemento qualsiasi di D , quindi ogni elemento di D ha l'inverso. □

17.3 Sottoanello

Un sottoanello $(S, +, \cdot)$ di $(A, +, \cdot)$ e' un sottoinsieme $S \subseteq A$ che mantiene le stesse operazioni di A su se stesso.

Per verificare che S sia un sottoanello basta controllare le seguenti tre proprieta', tutte le altre sono poi conseguenza del fatto che S e' un sottoinsieme di A :

1. Dobbiamo verificare che le operazioni sono interne a S , cioe', $\forall x, y \in S$,

$$x + y \in S \quad \wedge \quad xy \in S$$

2. Deve esistere lo zero in S :

$$\exists 0 \in S$$

3. e l'opposto di ogni elemento di S :

$$\forall s \in S \quad \exists -s \in S$$

Proposition 17.3. Dato $S \subseteq A$, si ha

$$S \text{ sottoanello di } A \Leftrightarrow \forall x, y \in S \begin{cases} x - y \in S \\ xy \in S \end{cases}$$

Proof: infatti,

$$\begin{aligned} x - x \in S &\Rightarrow 0 \in S \\ x - (-y) \in S &\Rightarrow x + y \in S \\ 0 - y \in S &\Rightarrow \exists -y \in S \end{aligned}$$

□

17.4 Omomorfismo

Consideriamo ora particolari applicazioni tra anelli.

Dati due anelli $(A, +, \cdot)$, $(A', +, \cdot)$ (con le loro rispettive operazioni che possono anche essere diverse), una applicazione

$$f : A \longrightarrow A'$$

è un *omomorfismo*, se

$$f \equiv \text{omomorfismo} \Leftrightarrow \forall x, y \in A \begin{cases} f(x + y) = f(x) + f(y) \\ f(xy) = f(x)f(y) \end{cases}$$

L'*omomorfismo nullo* è $f(a) = 0 \forall a \in A$.

Se l'applicazione f è iniettiva, allora si dice che f è una *immersione*.

Se l'applicazione f è suriettiva, allora si dice che f è una *suriezione*.

Se l'applicazione f è biettiva, allora si dice che f è un *isomorfismo*.

17.4.1 Proprietà

$$1. f(0) = 0' \in A'$$

Proof:

$$\begin{aligned} f(0) &= f(0 + 0) = f(0) + f(0) \\ f(0) &= f(0) + f(0) \\ f(0) - f(0) &= f(0) + f(0) - f(0) \\ f(0) &= 0' \end{aligned}$$

□

$$2. f(-a) = -f(a)$$

Proof:

$$\begin{aligned} f(-a) &= -f(a) \\ f(-a) + f(a) &= 0' \\ f(-a + a) &= f(0) = 0' \end{aligned}$$

□

Proposition 17.4. Dato $f : A \longrightarrow A'$ omomorfismo. In generale la proprieta' $f(1_A) = 1_{A'}$ non vale, si hanno pero' questi due risultati:

1. A, A' domini unitari, $\text{Im } f \neq \{0\} \Rightarrow f(1_A) = 1_{A'}$
2. f surriettiva $\Rightarrow f(1_A) = 1_{A'}$

Proof:

(1) Dim. 1.

$$\begin{aligned} f(1) &= f(1 \cdot 1) = f(1)f(1) \\ f(1) - f(1)f(1) &= 0 \\ f(1)(1 - f(1)) &= 0 \Rightarrow f(1) = 1 \end{aligned}$$

Nota che $f(1) \neq 0$, infatti, se per assurdo lo fosse:

$$f(1) = 0 \Rightarrow f(a) = f(a \cdot 1) = f(a)f(1) = 0 \Rightarrow f(a) = 0 \forall a \in A$$

e questo e' assurdo contro l'Hp che f e' un omomorfismo non nullo.

(2) Dim. 2.

$f(1) = u' \in A'$, poiche' f e' surriettiva, allora $a' \in A'$, $a' = f(a)$ per qualche $a \in A$, quindi

$$\begin{aligned} a'u' &= f(a)f(1) = f(a) = a' \\ a'u' &= a' \end{aligned}$$

Percio' $f(1) = u'$ e' l'unita' di A' .

□

Proposition 17.5. Dato $f : A \longrightarrow A'$ omomorfismo, e preso $a \in A$, si ha

$$f(1_A) = 1_{A'}, \exists a^{-1} \Rightarrow f(a)^{-1} = f(a^{-1})$$

Proof:

$$f(a)f(a^{-1}) \underset{f \text{ omomorfismo}}{=} f(aa^{-1}) = f(1_A) \underset{Hp}{=} 1_{A'}$$

$$f(a^{-1})f(a) = f(1) = 1_{A'}$$

Quindi $f(a^{-1})$ e' l'inverso di $f(a)$, ovvero

$$f(a)^{-1} = f(a^{-1})$$

□

Proposition 17.6. Sia $f : K \longrightarrow A'$ un omomorfismo, dove K e' un campo, e A' un anello, allora

$$\text{Im } f \neq \{0\} \Rightarrow f \text{ iniettiva}$$

Proof: Vedi [18.2,pg.90].

□

17.5 Immagine e nucleo

Dato l'omomorfismo $f : A \longrightarrow A'$,

$$\text{Immagine di } f := \text{Im } f := \{a' \in A' \mid \exists a \in A : f(a) = a'\}$$

$$\text{nucleo di } f := \ker f := \{a \in A \mid f(a) = 0' \in A'\}$$

Sicuramente $\text{Im } f, \ker f$ non sono vuoti, perche' contengono almeno $0', 0$.

Valgono le seguenti proprieta'

1. $\ker f$ e' un sottoanello di A ,

$$\ker f \leq A$$

Proof:

$$x, y \in \ker f \Leftrightarrow f(x) = f(y) = 0$$

$$x - y \in \ker f? \text{ Si, infatti}$$

$$f(x - y) = f(x) - f(y) = 0$$

$$xy \in \ker f? \text{ Si, infatti}$$

$$f(xy) = f(x)f(y) = 0$$

□

2. Questa e' una proprieta' piu' forte della precedente

$$\forall x \in \ker f, \forall a \in A \Rightarrow xa, ax \in \ker f$$

Ovvero $\ker f$ e' un ideale di A (vedi 17.8):

$$\ker f \triangleleft A$$

Proof:

$$f(xy) = \underbrace{f(x)}_0 f(y) = 0$$

□

3. $\text{Im } f$ e' un sottoanello di A' .

$$\text{Im } f \leq A'$$

Proof:

$$x', y' \in \text{Im } f \Leftrightarrow \exists x, y \in A : f(x) = x', f(y) = y'$$

$$x' - y' \in \text{Im } f? \text{ Si, infatti}$$

$$x' - y' = f(x) - f(y) = f(x - y) \in \text{Im } f$$

$$x'y' \in \text{Im } f? \text{ Si, infatti}$$

$$f(x'y') = f(x)f(y) = f(xy) \in \text{Im } f$$

□

4. La composizione di omomorfismi e' un omomorfismo, cioe' dati tre anelli A, A', A'' e

$$f : A \longrightarrow A' \quad g : A' \longrightarrow A''$$

$g \circ f : A \longrightarrow A''$ e' un omomorfismo, infatti,

Proof:

$$g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y))$$

$$g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y))$$

□

5. f e' un omomorfismo iniettivo (immersione), se

$$f \equiv \text{immersione} \Leftrightarrow \ker f = \{0\}$$

Cioe', se l'unico elemento di $\ker f$ e' lo zero di A .

Proof: Dim $\Rightarrow$.

$f(0) = 0'$, e poiche' f e' iniettiva, allora lo zero l'unico elemento $0 \rightarrow 0'$.

Dim $\Leftarrow$.

Dobbiamo dimostrare che

$$\forall x, y \in A \quad f(x) = f(y) \Rightarrow x = y$$

Se $f(x) = f(y)$, allora

$$f(x) - f(y) = 0 \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \ker f$$

e poiche' $\ker f = \{0\} \Rightarrow x = y$

□

17.6 Anello quoziente

Sia A un anello e $S \leq A$. Stabiliamo adesso la seguente rel. d'equivalenza tra due elementi del sottoanello S di A .

$$x, y \in A \quad x \sim y \Leftrightarrow x - y \in S$$

E' facile verificare che e' una rel d'equ

Proof:

$$x \sim x \Leftrightarrow x - x = 0 \in S$$

e dato che S e' un sottoanello $0 \in S$ e' vera.

$$x \sim y \Rightarrow y \sim x$$

infatti

$$\begin{aligned} x \sim y &\Leftrightarrow x - y \in S \\ -(x - y) \in S &\Rightarrow y - x \in S \Rightarrow y \sim x \\ x \sim y \wedge y \sim z &\Rightarrow x \sim z \end{aligned}$$

infatti

$$\begin{aligned} x \sim y &\Leftrightarrow x - y \in S \\ y \sim z &\Leftrightarrow y - z \in S \\ (x - y) + (y - z) \in S &\Leftrightarrow x - z \in S \end{aligned}$$

Per l'ultima implicazione abbiamo sfruttato il fatto che

$$a, b \in S \Rightarrow a + b \in S$$

□

Allora, a questo punto possiamo creare il quoziente di A , ovvero, l'insieme di tutte le classi di equivalenza di A secondo, questo insieme lo indichiamo con A/S :

$$A/S := \{[a] \mid a \in A\}$$

Definiamo anche il seguente insieme, chiamato laterale di S , fissando un $a \in A$:

$$a + S := \{a + s \mid s \in S\}$$

Ovvero e' l'insieme di tutti gli elementi di S a cui abbiamo sommato $a \in A$. Vale questa uguaglianza tra insiemi:

$$[x] = x + S$$

Proof: Dimostriamo che $[x] \subseteq x + S$

$$\begin{aligned} y \in [x] &\Leftrightarrow y \sim x \Leftrightarrow y - x \in S \\ y - x = s \in S &\Rightarrow y = s + x \in x + S \Leftrightarrow y \in x + S \end{aligned}$$

Dimostriamo che $x + S \subseteq [x]$

$$\begin{aligned} y \in x + S &\Leftrightarrow y = x + s, s \in S \Leftrightarrow y - x = s \in S \\ y - x = s \in S &\Leftrightarrow y \sim x \Leftrightarrow y \in [x] \end{aligned}$$

Quindi:

$$[x] \subseteq x + S \wedge x + S \subseteq [x] \Rightarrow [x] = x + S$$

□

Allora possiamo ridefinire A/S in questa maniera:

$$A/S := \{a + S \mid a \in A\}$$

cioe' l'insieme di tutti i laterali di S .

Adesso cerchiamo di rendere A/S un anello. Definiamo l'addizione:

$$(a + S) + (b + S) := a + b + S$$

Questa operazione e' ben posta.

Proof: Vogliamo dimostrare che l'addizione e' ben posta, cioe' che non dipende dai rappresentati degli addendi, ma solo dalle loro classi. Infatti, scegliamo $a' \in a + S$ (cioe' $[a'] = [a]$) e anche $b' \in b + S$, vogliamo dimostrare che:

$$(a + S) + (b + S) = (a' + S) + (b' + S) \Leftrightarrow a + b + S = a' + b' + S$$

che equivale a dire

$$(a + b) \sim (a' + b') \Leftrightarrow (a + b) - (a' + b') \in S \Leftrightarrow (a - a') + (b - b') \in S$$

Poiche' per Hp $a \sim a'$ allora $(a - a') \in S$ e lo stesso per $(b - b') \in S$, quindi la loro somma

$$(a - a') + (b - b') \in S$$

e questo dimostra la catena di doppie implicazioni

□

Definiamo adesso il prodotto:

$$(a + S)(b + S) := ab + S$$

Verifichiamo che e' ben posto:

Proof: Prendiamo $a' + S = a + S$, $b' + S = b + S$ e dimostriamo che

$$(a + S)(b + S) = (a' + S)(b' + S)$$

Nel primo membro:

$$(a + S)(b + S) = ab + S$$

nel secondo:

$$(a' + S)(b' + S) = a'b' + S$$

quindi dobbiamo dimostrare che

$$ab + S = a'b' + S \Leftrightarrow ab - a'b' \in S$$

Per Hp

$$a' + S = a + S \Rightarrow a' \sim a \Rightarrow a' \in [a] \Rightarrow a' \in a + S \Rightarrow a' = a + s_1, s_1 \in S$$

e anche:

$$b' = b + s_2, s_2 \in S$$

Quindi sostituendoli:

$$ab - a'b' \in S \Leftrightarrow ab - (a + s_1)(b + s_2) \in S \Leftrightarrow as_2 + s_1b + s_1s_2 \in S$$

Sicuramente $s_1s_2 \in S$, ma per as_2 , bs_1 non possiamo dire nulla, quindi non possiamo essere certi del fatto che

$$as_2 + s_1b + s_1s_2 \in S$$

In conclusione, questo prodotto non e' ben posto □

Per riuscire ad avere un prodotto ben posto dobbiamo utilizzare delle ipotesi piu' forti. Se poniamo come ipotesi che $S \triangleleft A$, cioe' che S sia un ideale di A (vedi 17.8), allora il prodotto diventa ben posto. Inoltre, e' facile verificare che le 6 proprieta' degli anelli valgono per $(A/S, +, \cdot)$. Lo di $(A/S, +, \cdot)$ e' $0 + S = S$, infatti, $(a + S) + (0 + S) = a + S$. Ricapitolando, $(A/S, +, \cdot)$ e' un anello, e si chiama l'*anello quoziente* rispetto all'ideale S .

17.6.1 Esempio

Prendiamo $\mathbb{Z}$, allora fissato $n \in \mathbb{N}$, accade che

$$n\mathbb{Z} \triangleleft \mathbb{Z}$$

dove $n\mathbb{Z} = \{\lambda n \mid \lambda \in \mathbb{Z}\}$, cioe' l'insieme di tutti i multipli di n . E' facile verificare che $n\mathbb{Z}$ e' l'ideale di $\mathbb{Z}$, infatti, differenze tra multipli di n sono multipli di n e multipli di multipli di n sono sempre multipli di n .

Prendiamo allora $\mathbb{Z}/n\mathbb{Z}$, questo non e' altro che:

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

infatti,

$$x \sim x' \Leftrightarrow x - x' \in n\mathbb{Z} \Leftrightarrow x - x' = \lambda n \Leftrightarrow x = x' (\mathbb{Z}_n)$$

e quindi

$$[x]_n = x + n\mathbb{Z}$$

17.7 Suriezione naturale

Dato l'anello A e $S \triangleleft A$, definiamo un'applicazione che chiameremo *surrezione naturale*:

$$\pi : A \mapsto A/S$$

$$\pi(a) = [a] = a + S$$

Questa funzione e' un omomorfismo ed e' anche suriettiva.

Proof: E' facile verificare che e' suriettiva, dimostriamo solo che e' un omomorfismo. Devono valere le due proprieta':

$$\pi(a + b) = \pi(a) + \pi(b) \quad \wedge \quad \pi(ab) = \pi(a)\pi(b)$$

allora

$$\pi(a + b) = a + b + S \quad \pi(a) = a + S, \pi(b) = b + S$$

$$\pi(a) + \pi(b) = (a + S) + (b + S) = a + b + S = \pi(a + b)$$

$$\pi(ab) = ab + S \quad \pi(a)\pi(b) = (a + S)(b + S) = ab + S = \pi(ab)$$

□

17.8 Ideale

Definiamo prima di tutto il concetto di *Ideale*

Dato l'anello A e $I \leq A$

$$I \triangleleft A \Leftrightarrow \forall i \in I, \forall a \in A \quad ai, ia \in I$$

Noto che questa definizione e' l'analogo dei laterali definiti per il $+$ di un anello. Un laterale e' un qualcosa del tipo $a + S$, dato che il $+$ commuta $a + S = S + a$. Un laterale per il $\cdot$ sarebbe

$a \cdot S$. Il $\cdot$ non commuta, quindi e' possibile che ci sia un qualche anello A e sottoanello S tale che $a \cdot S \neq S \cdot a$, allora, ha senso una definizione del tipo "un laterale del prodotto e' qualcosa del tipo $a \cdot S \cup S \cdot a$ ". Il sottoanello I di A e' un ideale di A se e solo se possiede la proprieta' di assorbimento, ovvero qualsiasi elemento di A moltiplicato per un elemento di I appartiene a I . Esiste anche l'ideale destro in cui vale solo che

$$\forall a \in A \quad ia \in I$$

invece, nell'ideale sinistro:

$$\forall a \in A \quad ai \in I$$

Per verificare che un insieme $I \subseteq A$ (A anello) e' un ideale, basta controllare che:

$$I \equiv \text{ideale di } A \Leftrightarrow \begin{cases} \forall x, y \in I \quad x - y \in I \\ \forall x \in I, \forall a \in A \quad ax, xa \in I \end{cases}$$

17.8.1 Proprieta' degli ideali

L'intersezione di due ideali e' ancora un ideale:

$$I, J \triangleleft A \Rightarrow I \cap J \triangleleft A$$

Proof: Consideriamo $i \in I, j \in J$ e prendiamo un elemento

$$t \in I \cap J \Leftrightarrow t \in I \wedge t \in J$$

abbiamo che

$$ta, at \in I \wedge ta, at \in J$$

ovvero

$$ta, at \in I \cap J$$

e poiche' l'intersezione di sottoanelli e' ancora un sottoanello, concludiamo che

$$I \cap J \triangleleft A$$

□

Dati $I, J \triangleleft A$

$$I \cup J \triangleleft A \Leftrightarrow I \subseteq J \vee J \subseteq I$$

Proof: Dimostrare $\Leftarrow$ e' semplice, infatti se J contiene I , allora $J \cup I = J \triangleleft A$. Dimostriamo $\Rightarrow$ negando tutta l'implicazione:

$$I \cup J \not\triangleleft A \Leftarrow I \not\subseteq J \wedge J \not\subseteq I$$

Le ipotesi di questa nuova implicazione equivalgono a:

$$I \not\subseteq J \Leftrightarrow \exists i \in I : i \notin J$$

$$J \not\subseteq I \Leftrightarrow \exists j \in J : j \notin I$$

e quindi $i, j \in I \cup J$.

Se per assurdo $I \cup J \triangleleft A$, e quindi se $I \cup J$ fosse un sottoanello

$$i - j \in I \cup J$$

ovvero

$$i - j \in I \vee i - j \in J$$

ma poiche' $j \notin I$ il primo caso e' assurdo, e poiche' $i \notin J$ anche il secondo lo e'. Quindi $I \cup J$ non e' un sottoanello di A , e quindi $I \cup J$ non e' un ideale di A . □

Terza proprieta': dato un anello A

$$I \triangleleft A, S \leq A \Rightarrow I \cap S \triangleleft S$$

Proof: Poiche' intersezione tra sottoanelli e' sempre un sottoanello, dobbiamo solo provare che:

$$\forall x \in I \cap S, \forall s \in S \Rightarrow sx, xs \in I \cap S$$

quindi,

$$x \in I \cap S \Leftrightarrow x \in I \wedge x \in S$$

$$\forall a \in A, ax, xa \in I, s \in S \subseteq A \Rightarrow sx, xs \in I$$

$$x \in S \Rightarrow sx, xs \in S$$

$$sx, xs \in I \wedge sx, xs \in S \Rightarrow sx, xs \in I \cap S$$

□

17.9 Omomorfismo e ideali

Dati due anelli A, A' e l'omomorfismo $f : A \longrightarrow A'$, valgono le seguenti proprieta':

1. L'immagine di un sottoanello di A e' un sotto anello di A' :

$$S \leq A \Rightarrow f(S) \leq A'$$

Proof: Dimostriamo usando la caratterizzazione dei sottoanelli:

$$x', y' \in f(S) \exists x, y \in S : f(x) = x', f(y) = y'$$

$$x' - y' = f(x) - f(y) = f(x - y) \in f(S)$$

$$x'y' = f(xy) \in f(S)$$

e poiche' $\text{Im } f \leq A'$, lo sara' anche $f(S)$, cioe':

$$f(S) \leq \text{Im } f \leq A'$$

□

2. La controimmagine di un sottoanello di A' e' un sottoanello di A , e per di piu' contiene $\ker f$:

$$S \leq A' \Rightarrow f^{-1}(S) \leq A \wedge \ker f \subseteq f^{-1}(S)$$

Proof: Dimostriamo usando la caratterizzazione dei sottoanelli:

$$x, y \in f^{-1}(S) \exists x', y' \in S : f^{-1}(x') = x, f^{-1}(y') = y$$

$$x - y = f^{-1}(x') - f^{-1}(y') = f^{-1}(x' - y') \in f^{-1}(S)$$

$$xy = f^{-1}(x')f^{-1}(y') = f^{-1}(x'y') \in f^{-1}(S)$$

□

3. La controimmagine di un ideale di A' e' un ideale di A , e per di piu' contiene $\ker f$:

$$I' \triangleleft A' \Rightarrow f^{-1}(I') \triangleleft A \wedge \ker f \subseteq f^{-1}(I')$$

Proof: Dobbiamo provare che

$$\begin{cases} x, y \in f^{-1}(I') \Rightarrow x - y \in f^{-1}(I') \\ x \in f^{-1}(I'), a \in A \Rightarrow ax, xa \in f^{-1}(I') \end{cases}$$

Procediamo allora in questo modo:

$$f(x) \in I', f(y) \in I' \Rightarrow f(x) - f(y) \in I' \Rightarrow f(x - y) \in I'$$

$$\Rightarrow x - y \in f^{-1}(I')$$

e sempre usando $f(\cdot)$:

$$f(a) \in A', f(x) \in I'$$

$$f(a)f(x) \in I' \Rightarrow f(ax) \in I' \Rightarrow ax \in f^{-1}(I')$$

□

4. Se I e' un ideale di A , allora $f(I)$ e' un ideale dell'immagine di f :

$$I \triangleleft A \Rightarrow f(I) \triangleleft \text{Im } f$$

Proof: Dobbiamo dimostrare che:

$$\begin{cases} x', y' \in f(I) \Rightarrow x' - y' \in f(I) \\ \forall x' \in f(I), \forall z' \in \text{Im } f \Rightarrow x'z', z'x' \in f(I) \end{cases}$$

Intanto riscriviamo tutte le nostre ipotesi in forma conveniente:

$$x' = f(x), x \in I, y' = f(y), z' = f(z)$$

Quindi sostituendo:

$$x' - y' = f(x) - f(y) = f(x - y) \in f(I)$$

lo stesso per la seconda proprieta':

$$x'z' = f(x)f(z) = f(xz)$$

$$xz \in I \Rightarrow f(xz) \in f(I)$$

□

17.10 Teorema dell'omomorfismo

Data un omomorfismo $f : A \longrightarrow A'$, e' possibile fattorizzare f come composizione di due funzioni, ovvero data la suriezione naturale π , esistera' un omomorfismo ω tale che $\omega \circ \pi = f$. Graficamente la situazione e' questa:

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ \downarrow \pi & \nearrow \omega & \\ A/\ker f & & \end{array}$$

(nota: $\ker f \triangleleft A$)

Proof: Poniamo per convenienza $K = \ker f$. Definiamo π :

$$\pi : A \mapsto A/\ker f \quad \pi(a) = K + a$$

Definiamo ω :

$$\omega : A/\ker f \longrightarrow A' \quad \omega(K + a) = f(a)$$

Verifichiamo che e' ben posta:

$$K + a = K + a' \Rightarrow \omega(K + a) = \omega(K + a') \text{ ? Si, infatti}$$

$$\omega(K + a) = f(a), \omega(K + a') = f(a')$$

$$K + a = K + a' \Rightarrow a - a' \in K = \ker f \Rightarrow f(a - a') = 0 \Rightarrow f(a) - f(a') = 0$$

$$\Rightarrow f(a) = f(a') \Rightarrow \omega(K + a) = \omega(K + a')$$

Verifichiamo adesso che e' un omomorfismo, ovvero proviamo queste due proprieta':

$$\begin{cases} \omega((K + a) + (K + b)) = \omega(K + a) + \omega(K + b) \\ \omega((K + a)(K + b)) = \omega(K + a)\omega(K + b) \end{cases}$$

procediamo:

$$\omega((K + a) + (K + b)) = \omega(a + b + K) = f(a + b) = f(a) + f(b) = \omega(K + a) + \omega(K + b)$$

$$\omega((K + a)(K + b)) = \omega(ab + K) = f(ab) = f(a)f(b) = \omega(K + a)\omega(K + b)$$

Manca adesso di far vedere che $\omega \circ \pi = f$:

$$\forall a \in A \quad \omega(\pi(a)) = \omega(K + a) = f(a)$$

dobbiamo pero' essere sicuri che ω sia iniettivo, quindi adesso dimostriamo che $\ker \omega = \{0\}$:

$$\ker \omega = \{a + K \mid \omega(a + K) = 0\}$$

$$a + K \in \ker \omega, \quad \omega(a + K) = f(a) = 0 \Rightarrow a \in \ker f = K \Rightarrow a + K = 0 + K$$

$$\Rightarrow \ker \omega = \{0 + K\} = \{\bar{0}\}$$

ecco fatto. □

17.10.1 Corollario I

$$A/\ker f \approx \operatorname{Im} f$$

Ovvero, $A/\ker f$ e' isomorfo a $\operatorname{Im} f$.

Proof: Consideriamo una restrizione di f :

$$f : A \mapsto \operatorname{Im} f$$

Questa restrizione e' sicuramente suriettiva. Adesso applichiamo il teorema dell'omomorfismo:

$$\begin{array}{ccc} A & \xrightarrow{f} & \operatorname{Im} f \\ \downarrow \pi & \nearrow \omega & \\ A/\ker f & & \end{array}$$

Poiche' f e' suriettiva, lo sara' anche ω :

$$z' = f(z), \quad z \in A$$

$$\omega(\pi(z)) = \omega(K + z) = f(z) = z'$$

L'ultima uguaglianza mostra che per ogni $z' \in \operatorname{Im} f$, esiste una $z \in A$, tale che $\omega(\pi(z)) = z'$. In altre parole, ω e' suriettiva. Poiche' abbiamo prima dimostrato che ω e' iniettivo, allora ω diventa un isomorfismo. □

17.10.2 Corollario II

Se f e' suriettiva:

$$f : A \mapsto A' \Rightarrow A/\ker f \approx A'$$

Questo e' vero semplicemente perche' $A' = \operatorname{Im} f$.

17.11 Teorema dell'isomorfismo II

Alcune premesse, dati:

$$S < A, \quad I \triangleleft A, \quad S + I = \{s + i \mid s \in S, i \in I\}$$

Valgono le seguenti proprieta':

$$S + I < A$$

Proof:

Infatti, $(s + i) - (s' + i') = (s - s') + (i - i') \in S + I$ e lo stesso vale per il prodotto. □

$$I \subseteq S + I < A \Rightarrow I \triangleleft S + I$$

Proof:

Questo perche' essendo I ideale di A , lo e' anche sicuramente di $S + I$ che e' un sottonello di A . $\square$

$$I \cap S \triangleleft S$$

Proof: Dobbiamo provare che

$$\begin{cases} x, y \in I \cap S, \Rightarrow x - y \in I \cap S \\ x \in I \cap S, s \in S \Rightarrow xs, sx \in I \cap S \end{cases}$$

La prima e' semplice, infatti, $x \in I, S$ e $y \in I, S$.

Nella seconda sappiamo che $xs \in I$ perche' I e' un ideale e $x \in I$, ma e' anche vero che $x \in S$ e quindi essendo $s \in S$ si ha che $xs \in I, S$. $\square$

Data $\pi : A \longrightarrow A/I$, vale il seguente fatto:

$$S < A \Rightarrow \pi(S) < A/I \Rightarrow \pi^{-1}(\pi(S)) = S + I < A$$

Proof: $\pi(S) < A/I$ e $\pi^{-1}(\pi(S)) < A$ sono vere per le proprieta' dimostrate in 17.9.

$$\pi(S) = \{I + s \in A/I \mid s \in S\}$$

$$\begin{aligned} \pi^{-1}(\pi(S)) &= \{a \in A \mid \pi(a) = I + s, s \in S \Leftrightarrow a - s \in I\} = \\ &= \{a \in S + I\} \end{aligned}$$

Tutte le a che stanno in $\pi^{-1}(\pi(S))$ sono in definitiva $\{a \in S + I\}$, perche' rispettano la condizione $a - s \in I$, infatti:

$$(s' + i') - s = (s' - s) + i'$$

e poiche' $I \triangleleft A$,

$$\underbrace{(s' - s)}_{\in S \subseteq A} + i' \in I$$

$\square$

Theorem 17.7. Ora arriviamo al teorema dell'isomorfismo II.

$$S < A, I \triangleleft A \Rightarrow \frac{S + I}{I} \simeq \frac{S}{I \cap S}$$

Proof: Consideriamo questa funzione:

$$f : S \mapsto \frac{S + I}{I}$$

$$f(s) = s + 0 + I = s + I \in \frac{S + I}{I}, A/I$$

Questa funzione e' surriettiva, infatti,

$$\forall x + I \in \frac{S + I}{I}, x = s + i, s \in S, i \in I$$

$$x + I = s + i + I = (s + I) + (i + I) = s + I \Rightarrow x + I = s + I$$

$$f(s) = s + I = x + I$$

Quindi per il corollario II (17.10.2):

$$S/\ker f \approx \frac{S + I}{I}$$

quindi ci resta da dimostrare che $\ker f = I \cap S$:

$$\ker f = \{s \in S \mid f(s) = s + I = 0 \Leftrightarrow s \in I\} = \{s \in S \cap I\} = S \cap I$$

$\square$

17.12 Teorema dell'isomorfismo III

Premesse a questo teorema. Consideriamo:

$$I \triangleleft J \triangleleft A$$

Ecco tutti i sottoanelli/ideali che possiamo costruire a partire da I, J, A :

$$A/J, A/I, J/I, J/I \triangleleft A/I, A/I \big/ J/I$$

Il teorema dice:

$$I \triangleleft J \triangleleft A \Rightarrow A/I \big/ J/I \approx A/J$$

Proof: Consideriamo questa composizione di suriezioni naturali:

$$A \xrightarrow{\pi} A/I \xrightarrow{\pi'} A/I \big/ J/I$$

$\pi' \circ \pi$ e' un omomorfismo surriettivo e quindi per il primo teorema:

$$A/\ker \pi' \circ \pi \approx A/I \big/ J/I$$

Quindi non rimane altro che dimostrare che $\ker \pi' \circ \pi = J$. Dimostriamolo per doppia inclusione.

$$j \in J, \pi'(\pi(j)) = \pi'(j + I) = \underbrace{j + I}_{\in J/I} + J/I = J/I = 0 \Rightarrow j \in \ker \pi' \circ \pi$$

$$\Rightarrow J \subseteq \ker \pi' \circ \pi$$

l'altra inclusione:

$$x \in \ker \pi' \circ \pi \Rightarrow \pi'(\pi(x)) = 0 \Rightarrow (x + I) + J/I = 0$$

$$x + I \in J/I \Rightarrow x + I = j + I \Rightarrow x - j \in I \subseteq J \Rightarrow x - j = j' \Rightarrow x = j' - j \in J$$

Quindi $\ker \pi' \circ \pi = J$ □

18 Ideali generati

Da questo momento in poi, gli anelli che consideriamo sono anelli commutativi.

Prendiamo un anello commutativo A e un suo qualsiasi sottoinsieme non vuoto $T \subseteq A$, allora, nasce l'insieme di tutte le combinazioni lineari degli elementi di T con quelli di A :

$$(T) = \{a_1 t_1 + \dots + a_n t_n \mid a_i \in A, t_i \in T\}$$

Vale che

$$(T) \triangleleft A$$

E' facile verificarlo usando le due proprieta'.

(T) viene chiamato *l'ideale di A generato da T* .

18.1 Sistema di generatori

Dato A , anello commutativo unitario, e $S \subseteq A$, S si chiamera' *sistema di generatori* per I se e solo se ogni elemento di $x \in I$ si puo' esprimere come

$$x = \sum_{i=1}^n a_i s_i \quad a_i \in A, s_i \in S$$

cioe' se ogni elemento di I e' combinazione lineare degli elementi di S .

Se $n \in \mathbb{N}$, S e' un sistema di generatori finito e si dira' finitamente generato (f.g.).

Se I e' generato da un solo elemento, ($n = 1$), allora si dira' *ideale principale*.

Theorem 18.1.

$$A \equiv \text{campo} \Leftrightarrow \text{gli unici ideali di } A \text{ sono } \{\{0\}, A\}$$

($\{\{0\}, A\}$ vengono anche chiamati *gli ideali banali*).

Proof: Dim $\Rightarrow$

Sia $B \triangleleft A, B \neq \{0\}$. Dimostreremo che necessariamente per $B \neq \{0\}$, deve essere $B = A$, e quindi in caso contrario $B = \{0\}$.

$$\begin{aligned} b \in B, \exists b' \in B : bb' = 1 \quad (A \text{ e' un campo}) \\ bb' = 1 \in B \quad (B \text{ e' un'ideale, quindi assorbe}) \\ \forall a \in A, 1 * a \in B \Rightarrow B = A \end{aligned}$$

Dim $\Leftarrow$

$$I = (a) \text{ Ideale principale di } A \text{ generato da } a \in A$$

$$\text{Per Hp } I = A \Rightarrow (a) = A$$

$$1 \in A \Leftrightarrow 1 \in (a) \Rightarrow 1 = aa' \Rightarrow A \equiv \text{campo}$$

□

Corollary 18.2. Sia $f : K \longrightarrow A'$ un omomorfismo, dove K e' un campo, e A' un anello, allora

$$\text{Im } f \neq \{0\} \Rightarrow f \text{ iniettiva}$$

Proof:

$$\ker f \leq K$$

ma per il thm [18.1,pg.90], gli unici ideali di K sono quelli banali, quindi

$$\ker f = (0) \vee \ker f = K$$

Se per assurdo $\ker f = K$,

$$\ker f = K \Leftrightarrow \forall k \in K \ f(k) = 0 \Leftrightarrow \text{Im } f = \{0\}$$

assurdo, contro Hp. Quindi,

$$\ker f = \{0\} \Rightarrow f \text{ iniettiva}$$

□

18.2 Ideale primo

Dato $P \triangleleft A$,

$$P \equiv \text{primo} \Leftrightarrow (ab \in P \Rightarrow a \in P \vee b \in P)$$

Theorem 18.3.

$$P \equiv \text{primo} \Leftrightarrow A/P \equiv \text{dominio}$$

Proof: Dim $\Rightarrow$

Dobbiamo dimostrare che in A/P vale la legge dell'annullamento del prodotto.

$$(x + P), (y + P) \in A/P : (x + P)(y + P) = [0]$$

$$xy + P = [0] \Leftrightarrow xy \in P$$

$$xy \in P \Rightarrow x \in P \vee y \in P \quad \text{perche' } P \text{ primo}$$

$$x \in P \Leftrightarrow (x + P) = [0]$$

$$y \in P \Leftrightarrow (y + P) = [0]$$

Dim $\Leftarrow$

Poiche' abbiamo usato solo doppie implicazioni, tranne una sola volta, dobbiamo solamente dimostrare:

$$x \in P \vee y \in P \Rightarrow xy \in P$$

Poiche' P e' un ideale, e poiche' almeno x o y sono in P , segue immediatamente (per l'assorbimento) che $xy \in P$. $\square$

Proposition 18.4. Sia D un PID. Dato $(p) \triangleleft D$, $p \neq 0$, si ha

$$(p) \equiv \text{primo} \Leftrightarrow p \equiv \text{primo}$$

Proof:

(1) Dim. $\Rightarrow$

Dobbiamo dimostrare la seguente implicazione:

$$p \nmid ab \Rightarrow p \nmid a \vee p \nmid b$$

Supponiamo che $p \nmid ab$

$$p \nmid ab \Leftrightarrow ab = \lambda p \Leftrightarrow ab \in (p)$$

$$ab \in (p) \underset{(p) \text{ primo}}{\Rightarrow} a \in (p) \vee b \in (p) \Leftrightarrow a = \mu_1 p \vee b = \mu_2 p \Leftrightarrow p \nmid a \vee p \nmid b$$

(1) Dim. $\Leftarrow$

Dobbiamo dimostrare la seguente implicazione:

$$ab \in (p) \Rightarrow a \in (p) \vee b \in (p)$$

Sia $ab \in (p)$

$$ab \in (p) \Leftrightarrow p \nmid ab \underset{p \text{ primo}}{\Rightarrow} p \nmid a \vee p \nmid b \Leftrightarrow a \in (p) \vee b \in (p)$$

$\square$

18.3 Ideale massimale

Dato $M \triangleleft A$,

$$M \equiv \text{massimale} \Leftarrow \left(\exists I \triangleleft A, M \subseteq I \Rightarrow I = M \vee I = A \right)$$

Ovvero, M e' massimale se tutti gli altri ideali di A che lo contengono sono o A oppure M stesso, in altre parole, al di sopra di M non esiste alcun ideale piu' grande.

Theorem 18.5. In ogni anello comm unitario ci sono ideali massimali, anzi vale un risultato piu' forte: partendo da un qualsiasi ideale proprio di A e' possibile trovare un ideale che lo contenga e che sia massimale. Cioe':

$$A \equiv \text{anello comm. unitario}, I \triangleleft A, I \neq A, \Rightarrow I \subseteq M \equiv \text{ideale mass. di } A$$

Prima di dimostrare questo teorema accenniamo il lemma di Zorn (che e' equivalente all'assioma della scelta):

sia A un poset,

$$\text{ogni catena di elementi di } A \text{ possiede un maggiorante} \Rightarrow A \text{ possiede elementi massimali}$$

(Nota: "catena" == "totet")

Proof: Dim: $I \subseteq M \equiv$ ideale mass. di A

Consideriamo questo insieme:

$$F_I = \{\text{tutti gli ideali propri di } A \text{ che contengono } I\}$$

cioe'

$$F_I = \{N \mid N \triangleleft A, N \neq A, I \subseteq N\}$$

che non e' vuoto perche' $I \in F_I$. Usando la relazione di inclusione, abbiamo il poset $(F_I, \subseteq)$.

Sia

$$\{J_\alpha\}_\alpha \equiv \text{una catena di elementi di } F_I$$

Se dimostriamo che $\{J_\alpha\}_\alpha$ e' un totet, allora potremo applicare Zorn.

Consideriamo

$$J = \bigcup_\alpha J_\alpha$$

e' un maggiorante? Poiche' include tutti i J_α , basta verificare che $J \in F_I$:

$$J \in F_I \Leftrightarrow \begin{cases} 1) J \triangleleft A \\ 2) J \neq A \\ 3) I \subseteq J \end{cases}$$

Proof: Dim: 3)

$$I \subseteq J_\alpha \subseteq J \Rightarrow I \subseteq J$$

□

Proof: Dim: 1)

$$\forall x, y \in J \Rightarrow x - y \in J?$$

$$x \in J_a, y \in J_b, J_a, J_b \in J$$

$$J_a \subseteq J_b \Rightarrow x \in J_b$$

$$x \in J_b, y \in J_b \Rightarrow x - y \in J_b \subseteq J$$

□

Proof: Dim: 2)

per assurdo $J = A$

$1 \in A$ A e' un anello unitario

$$1 \in A = J \Leftrightarrow 1 \in J_b \Rightarrow$$

$J_b = A$ e' assurdo perche' $J_b \in F_I$ e F_I contiene solo ideali propri

□

A questo punto, sappiamo che ogni catena di F_I ha maggiorante, quindi applicando Zorn, deduciamo che $(F_I, \subseteq)$ ha almeno un massimale che chiamiamo M .

M e' un ideale massimale? Proviamolo.

$$I \subseteq M \triangleleft A, M \neq A \text{ [per definizione]}$$

$$M \triangleleft H \triangleleft A \Rightarrow H = M \vee H = A \text{ [e' quello che dobbiamo provare]}$$

supponiamo che $H \neq A$

$$I \subseteq M \triangleleft H \triangleleft A \Rightarrow H \in F_I$$

$$M \subseteq H, H \subseteq M \Rightarrow M = H \text{ } M \text{ e' il massimale di } F_I$$

□

Theorem 18.6.

$$M \equiv \text{massimale} \Leftrightarrow A/M \equiv \text{campo}$$

Proof: $Dim \Rightarrow$

$$\begin{aligned}
 (a + M) &\in A/M, (a + M) \neq 0 \\
 M + (a) &\text{ e' il piu' piccolo ideale contenente } M \text{ e } A \\
 M + (a) &= A \text{ per Hp di massimalita' di } M \\
 1 \in A &\Rightarrow 1 \in M + (a) \Rightarrow 1 = m + aa' \\
 1 = m + aa' &\Rightarrow 1 + M = m + aa' + M = aa' + M = (a + M)(a' + M) \\
 1 + M &= (a + M)(a' + M) \\
 (a' + M) &\equiv \text{ inverso di } (a + M)
 \end{aligned}$$

$Dim \Leftarrow$

$$\begin{aligned}
 B \triangleleft A : M &\subset B \\
 \exists b \in B : b &\notin M \Rightarrow b + M \neq [0] \\
 \exists b' + M \in A/M : (b' + M)(b + M) &= 1 + M \text{ poiche' } A/M \text{ e' un campo} \\
 (b' + M)(b + M) &= 1 + M \Rightarrow bb' + M = 1 + M \Rightarrow \\
 \underbrace{bb'}_{\in B} - \underbrace{m}_{\in M \subset B} &= 1 \in B \\
 1 \in B &\Rightarrow B = A \text{ per la prop di assorbimento}
 \end{aligned}$$

□

Corollary 18.7.

$$M \equiv \text{ massimale} \Rightarrow M \equiv \text{ primo}$$

Semplicemente perche' ogni campo e' anche un dominio, e quindi basta applicare [18.6,pg.92] e [18.3,pg.90].

18.4 Ideali e $\mathbb{Z}$

Proposition 18.8. Tutti gli ideali di $\mathbb{Z}$ sono principali

Proof:

$$\begin{aligned}
 I \triangleleft \mathbb{Z}, a &:= \text{ il piu' piccolo intero } > 0 \text{ di } I \\
 \text{dobbiamo dim che } I &= (a) \\
 x \in I, x &= aq + r \quad 0 \leq r \leq a - 1 \\
 r &= x - aq \in I \\
 r > 0, a &\text{ non sarebbe piu' il "piu' piccolo", quindi} \\
 r = 0 &\Rightarrow x = aq \Rightarrow I = (a)
 \end{aligned}$$

□

Proposition 18.9. Tutti gli ideali primi di $\mathbb{Z}$ sono solo quelli generati da (p) , con p primo.

Proof: Basta usare la proposizione [18.4,pg.91].

□

19 Campo dei quozienti di D

Da ora in poi studieremo gli anelli commutativi che sono *domini d'integrita'*, ovvero quegli anelli commutativi dove vale la legge di annullamento del prodotto.

Adesso vedremo che e' possibile immergere un dominio in un campo, ovvero e' possibile trovare un omomorfismo iniettivo che va dal dominio al campo. (Questo e' quello che abbiamo fatto quando abbiamo dimostrato l'immersione di $\mathbb{Z}$ in $\mathbb{Q}$.)

Sia D un dominio e creiamo a partire da esso un insieme quoziente:

$$\begin{aligned}(a, b), (c, d) &\in D \times D^* \\ (a, b) \sim (c, d) &\Leftrightarrow ad = bc \\ D \times D^* / \sim &= K = \{\text{tutte le classi d'equiv.}\} \\ \frac{a}{b} &:= [(a, b)]\end{aligned}$$

definiamo sull'insieme quoziente K due operazioni:

$$\begin{aligned}[(a, b)] + [(c, d)] &:= [(ad + bc, bd)] = \frac{ad + bc}{bd} \\ [(a, b)][(c, d)] &:= [(ac, bd)] = \frac{ac}{db}\end{aligned}$$

Queste due operazioni risultano ben poste.

Proof:

$$\begin{aligned}(a', b') \sim (a, b) &\Rightarrow [(a', b')] = [(a, b)], \quad a'b = b'a \\ [(a', b')] + [(c, d)] &= [(a'd + b'c, b'd)] \\ [(a, b)] + [(c, d)] &:= [(ad + bc, bd)] \\ [(a'd + b'c, b'd)] &= [(ad + bc, bd)] \Rightarrow (a'd + b'c)(bd) = (b'd)(ad + bc) \Rightarrow \\ a'bd^2 + bb'cd &= ab'd^2 + bb'cd \Rightarrow a'bd^2 = ab'd^2 \\ (a, b), (a, b'), (c, d) &\in D \times D^* \Rightarrow b, b', d \neq 0 \\ a'bd^2 = ab'd^2 &\Rightarrow a'b = ab' \quad \text{per la legg. di annull.} \\ a'b = ab' &\text{ e' vero, per Hp}\end{aligned}$$

□

$(K, +, \cdot)$ risulta essere un campo, e si chiama il *campo dei quozienti di D* , che si puo' indicare con $Q(D)$. (L'elemento neutro e' $\frac{b}{b}$, e l'inverso di $\frac{a}{b}$ e' $\frac{b}{a}$).

A questo punto ricerchiamo l'immersione che "affoga" il dominio D in K :

$$\varphi : D^* \longrightarrow K$$

$$\varphi(a) = [(ab, b)] = \frac{ab}{b}, \quad b \in D^*$$

φ e' un omomorfismo.

Proof: Prima proprieta':

$$\begin{aligned}\varphi(a + b) &= \frac{(a + b)c}{c} \\ \varphi(a) + \varphi(b) &= \frac{ad}{d} + \frac{be}{e} = \frac{ade + bed}{ed} = \frac{(a + b)ed}{ed} \\ \frac{(a + b)c}{c} &\stackrel{?}{=} \frac{(a + b)ed}{ed} \quad \text{si, infatti} \\ (a + b)edc &= (a + b)ced\end{aligned}$$

seconda:

$$\begin{aligned}\varphi(ab) &= \frac{abc}{c} \\ \varphi(a)\varphi(b) &= \frac{ad}{d} \frac{be}{e} = \frac{abde}{de} \\ \frac{abc}{c} &\stackrel{?}{=} \frac{abde}{de} \quad \text{si, infatti} \\ (ab)dec &= (ab)cde\end{aligned}$$

□

φ e' iniettivo, ovvero $\ker \varphi = \{0\}$.

Proof:

$$\begin{aligned}\ker \varphi &= \{a \in D^* \mid \varphi(a) = 0\} \\ \varphi(a) = 0 &\Rightarrow \frac{ab}{b} = \frac{0}{c} \Leftrightarrow abc = 0 \\ b, c \neq 0 &\Rightarrow a = 0 \Rightarrow \ker \varphi = \{0\}\end{aligned}$$

□

Abbiamo dimostrato quindi che φ e' una immersione.

19.0.1 Esempi

$2\mathbb{Z}$ e' il dominio degli interi pari, il suo campo dei quozienti $Q(2\mathbb{Z}) = \mathbb{Q}$

Proof:

$$\begin{aligned}(a, b) \in 2\mathbb{Z} \times 2\mathbb{Z}^* &\Rightarrow a = 2m, b = 2n \neq 0 \\ [(a, b)] &= \frac{a}{b} = \frac{2m}{2n} = \frac{m}{n}\end{aligned}$$

Si puo' anche mostrare che esiste l'immersione:

$$\begin{aligned}\varphi : 2\mathbb{Z} &\longrightarrow Q(2\mathbb{Z}) = \mathbb{Q} \\ \varphi(a) &= \frac{a2}{2}\end{aligned}$$

□

20 Principal Ideal Domain

Definition 20.1. Sia D un dominio,

$$D \equiv \text{PID} \stackrel{\text{def}}{\Leftrightarrow} \forall I \trianglelefteq D \quad I \text{ e' principale}$$

ovvero, ogni ideale di D e' principale.

Esempio: $\mathbb{Z}$ e' un PID (vedi [18.8,pg.93]).

Definition 20.2. Definizione di elemento primo per i domini: dato D dominio, $p \in D$, $p \neq 0$, p non invertibile, poniamo:

$$p \equiv \text{primo} \stackrel{\text{def}}{\Leftrightarrow} \left(p/ab \Rightarrow p/a \vee p/b \right)$$

Definizione di elemento irriducibile: sia $q \in D$, $q \neq 0$, q non invertibile, poniamo:

$$\begin{aligned}q \equiv \text{irriducibile} &\stackrel{\text{def}}{\Leftrightarrow} \text{ i suoi unici divisori sono gli invertibili o i suoi associati } \Leftrightarrow \\ &\Leftrightarrow \left(q = ab \Rightarrow a \equiv \text{invertibile} \vee b \equiv \text{invertibile} \right)\end{aligned}$$

Proposition 20.3. *In un dominio con unita', vale che*

$$p \equiv \text{primo} \Rightarrow p \equiv \text{irriducibile}$$

Proof:

$$\begin{aligned} p = ab &\Rightarrow p \nmid ab \xRightarrow[p \text{ primo}]{} p \nmid a \vee p \nmid b \\ p \text{ primo} &\xRightarrow[\text{per definizione}]{} p \neq 0 \end{aligned}$$

CASE: $p \nmid a$

$$p \nmid a \Leftrightarrow p\lambda = a$$

$$p = ab \Leftrightarrow p = p\lambda b \Leftrightarrow p(1 - \lambda b) = 0 \xLeftrightarrow[D \text{ dominio}]{} p = 0 \vee 1 - \lambda b = 0 \xRightarrow[p \neq 0]{} \lambda b = 1 \Rightarrow b \text{ invertibile}$$

CASE: $p \nmid b$

analogamente a prima.

□

Proposition 20.4. *Sia D un PID o un UFD, e $p \in D^*$, allora*

$$p \equiv \text{irriducibile} \Leftrightarrow p \equiv \text{primo}$$

Proof:

CASE: D PID

Supponiamo che $p \nmid ab$ e che $p \nmid a$, allora

$$\text{MCD}(p, a) = 1$$

$$1 = \lambda p + \mu a \Rightarrow b = \lambda pb + \mu ab$$

$$p \nmid \lambda pb, \quad p \nmid \mu ab \Rightarrow p \nmid b \Rightarrow$$

$$p \equiv \text{primo}$$

CASE: D UFD

Basta applicare la caratterizzazione degli UFD: vedi [21.3.1,pg.101].

□

21 Domini euclidei

$$D \equiv \text{dominio euclideo (ED)} \Leftrightarrow \exists v : D^* \longrightarrow \mathbb{N} :$$

$$\begin{cases} v(a) \leq v(ab) \quad a, b \in D^* \\ \forall a \in D, b \in D^* \exists q, r \in D^* : a = qb + r, \quad r = 0 \vee v(r) < v(b) \end{cases}$$

In sostanza, stiamo costruendo un dominio in cui valga l'algoritmo euclideo della divisione. A ogni elemento di D^* associamo una sua grandezza. Nella divisione imponiamo che $v(r) < v(b)$, così facendo potremmo ritrovare tutto ciò che avevamo già visto sulla divisione: MCD, Bezout, primi=irriducibili. L'unica differenza è che questo discorso potrà essere applicato non solo a $\mathbb{Z}$ e a $K[x]$, ma anche a un'infinita di altri domini. ($v(a)$ si chiama *valutazione* di a).

Nota: ED sta per "Euclidean Domain".

21.1 Esempi di domini euclidei

K , campo, e' un dominio euclideo.

Proof:

$$\begin{aligned} v : K^* &\longrightarrow \mathbb{N} & v(a) &:= 1 \\ v(a) &= 1 \leq v(ab) = 1 \\ q &= ab^{-1} \quad a = qb + r = ab^{-1}b + 0 = a \end{aligned}$$

□

Vediamo come $\mathbb{Z}$ sia un dominio euclideo:

Proof:

$$\begin{aligned} v : \mathbb{Z}^* &\longrightarrow \mathbb{N} \\ v(a) &:= |a| \\ a, b \in \mathbb{Z}^* \quad v(a) &= |a| \leq v(ab) = |a||b| \quad b \geq 1 \\ a &= qb + r \quad r = 0 \vee 0 \leq r < |b| \quad \text{per la divisione in } \mathbb{Z} \\ v(r) &= |r| < v(b) = |b| \end{aligned}$$

□

Infine, vediamo come $K[x]$ sia pure un dominio euclideo:

Proof:

$$\begin{aligned} v : K[x]^* &\longrightarrow \mathbb{N} \\ v(f(x)) &:= \deg f(x) \\ v(f(x)) &= \deg f(x) \leq v(f(x)g(x)) = \deg f(x)g(x) = \deg f(x) + \deg g(x) \\ f(x) &= q(x)g(x) + r(x) \quad r(x) = 0 \vee \deg r(x) < \deg g(x) \\ v(r(x)) &= \deg r(x) < v(g(x)) = \deg g(x) \end{aligned}$$

□

21.2 Proprieta' dei domini euclidei

Proposition 21.1. *In D , dominio euclideo, esiste l'elemento unita', ovvero*

$$D \text{ dominio euclideo} \Rightarrow D \text{ dominio unitario}$$

Proof:

$$\begin{aligned} \emptyset &\neq \text{Im } v \subseteq \mathbb{N} \\ m &= \min \text{Im } v \quad (\text{m esiste perche' } \mathbb{N} \text{ e' ben ordinato}) \\ m &= v(d), \quad d \in D^* \\ \forall a \in D \quad a &= dq + r \quad r = 0 \vee v(r) < v(d) \\ v(r) &< v(d) \quad \text{e' imp. perche' } v(d) = m \text{ e' il minimo!} \Rightarrow \\ r &= 0 \Rightarrow a = dq \\ d &= dq := du \quad (\text{poiche' abbiamo considerato } \forall a \in D) \\ \forall a \in D, \quad au &= dqu = dq = d = a \Rightarrow u = 1 \end{aligned}$$

□

Proposition 21.2.

$$D \text{ dominio euclideo} \Rightarrow D \text{ PID}$$

ovvero, ogni dominio euclideo e' un PID.

Proof: Dato

$$I \triangleleft D$$

dobbiamo dimostrare che

$$I = \{\lambda i, i \in I^*\}$$

(non serve considerare $I = (0)$, perche' altrimenti avremmo gia' finito), allora:

$$\emptyset \neq v(I^*) \subseteq \mathbb{N}$$

$$m = \min v(I^*) \Rightarrow \forall t \in v(I^*), m < t$$

$$m = v(i), i \in I^*$$

dimostriamo che $(i) \subseteq I$:

$$\forall x \in (i), x = \lambda i \in I \text{ per la prop. di assorbimento degli ideali}$$

dimostriamo che $I \subseteq (i)$:

$$\forall x \in I, x = qi + r$$

$$r = 0 \vee v(r) < v(i) = m$$

$$r = x - qi \in I \text{ quindi ha senso considerare } v(r)$$

$$v(r) < m \text{ e' imp. perche' } m \text{ e' il minimo} \Rightarrow$$

$$r = 0 \Rightarrow x = qi \in (i)$$

□

Proposition 21.3.

$$\forall a, b \in D^*, \exists MCD(a, b) = d, d = \lambda a + \mu b$$

Proof: Dimostreremo in un colpo solo Bezout e l'esistenza del MCD.

$$I = (a, b) = \{ma + nb \mid m, n \in D^*\} \triangleleft D$$

$$D \equiv \text{PID} \Leftrightarrow \exists d \in I : I = (d)$$

$$(a, b) = (d) \Rightarrow (a, b) \subseteq (d)$$

$$a \in (a, b) \subseteq (d) \Rightarrow a = \lambda d \Rightarrow d/a$$

$$b \in (a, b) \subseteq (d) \Rightarrow b = \mu d \Rightarrow d/b$$

$$d \in (d) \subseteq (a, b) \Rightarrow d = ma + nb$$

$$d'/a \wedge d'/b \Rightarrow d'/ma \wedge d'/mb \Rightarrow d'/d \Rightarrow$$

$$d = ma + nb = MCD(a, b)$$

□

Proposition 21.4. Un dominio euclideo e' un UFD.

Proof: Dimostreremo questa proprieta' piu' avanti.

□

Proposition 21.5.

$$v(a) = v(ab) \Leftrightarrow b \equiv \text{invertibile}$$

Proof: Dim $\Rightarrow$

Prendiamo $I = (a)$, $J = (ab)$, allora

$$J \subseteq I \Rightarrow ab \in I$$

a ha la valutazione minima in I

$$v(a) = v(ab) \Rightarrow ab \text{ ha la valutazione minima in } I \Rightarrow$$

$$a = q(ab) + r = (qb)a + r$$

$$v(r) < v(ab) \quad [\text{imp. perche' } ab \text{ ha val. minima}]$$

$$v(r) < v(a) \quad [\text{imp. perche' } a \text{ ha val. minima}]$$

$$\Rightarrow r = 0 \Rightarrow a = qba \Rightarrow 1 = qb$$

$$b \equiv \text{invertibile}$$

Dim $\Leftarrow$

$$v(a) \leq v(ab), \exists b^{-1}$$

$$v(a) \leq v(ab) \leq v(abb^{-1}) = v(a) \Rightarrow$$

$$v(a) = v(ab)$$

□

Proposition 21.6. Dato $(a) = I \triangleleft D$, $a \neq 0$, dove D e' un ED, si ha

$$(a) \equiv \text{massimale} \Leftrightarrow a \equiv \text{irriducibile}$$

E poiche' $ED \Rightarrow UFD$ (vedi [21.10,pg.104]), grazie alla [20.4,pg.96], si ha

$$(a) \equiv \text{massimale} \Leftrightarrow a \equiv \text{primo} \Leftrightarrow a \equiv \text{irriducibile}$$

Proof: Dim $\Rightarrow$

Dobbiamo dimostrare che

$$a = bc \Rightarrow b \equiv \text{invertibile} \vee c \equiv \text{invertibile}$$

$$a = bc \Rightarrow (a) \subseteq (b) \Rightarrow$$

$$\Rightarrow (b) = D \vee (b) = (a) \quad \text{poiche' } (a) \text{ e' massimale per Hp}$$

If $(b) = D$:

$$1 \underbrace{\in}_{[21.1,pg.97]} D \Rightarrow 1 \in (b) \Rightarrow$$

$$1 = \lambda b \Rightarrow b \equiv \text{invertibile}$$

If $(b) = (a)$:

$$b = am$$

$$a = bc \Rightarrow a = amc \Rightarrow 1 = mc \Rightarrow$$

$$c \equiv \text{invertibile}$$

Dim: $\Leftarrow$

Ts:

$$(a) \triangleleft J \triangleleft D \Rightarrow J = (a) \vee J = D$$

$(a) \triangleleft J \Rightarrow a \in J$
 $J \equiv \text{PID, perche' } D \text{ e' un ED} \Rightarrow J = (j)$
 $a \in J \Rightarrow a = \lambda j$
 $a \equiv \text{irriducibile (per Hp)} \Rightarrow$
 $\lambda \equiv \text{invertibile} \vee j \equiv \text{invertibile}$
If: $\lambda \equiv \text{invertibile} :$
 $\lambda^{-1}a = j \Rightarrow j \in (a) \Rightarrow J \subseteq (a) \Rightarrow J = (a)$
If: $j \equiv \text{invertibile}$
 $(j) = D$ [per la proprieta' degli ideali: se $1 \in I$, allora $I = D$]

□

Example 21.7. Ad esempio in $\mathbb{Z}$,

$$(m) = m\mathbb{Z} \equiv \text{massimale} \Leftrightarrow m \equiv \text{primo}$$

Nota: (0) e' primo, infatti se

$$ab \in (0) \Rightarrow ab = 0 \Rightarrow a = 0 \vee b = 0 \Leftrightarrow a \in (0) \vee b \in (0)$$

(proprio perche' siamo un un dominio d'integrita'.

Proposition 21.8. Dato D dominio euclideo, $I, J \triangleleft D$, $I = (a)$, $J = (b)$, vale che:

$$I + J = (MCD(a, b))$$

$$I \cap J = (mcm(a, b))$$

Proposition 21.9. Dato D anello, $I \triangleleft D$, $\frac{D}{I}$,

$$J \triangleleft D, I \subseteq J \Rightarrow J + I \triangleleft \frac{D}{I}$$

21.3 ED, PID e UFD

Ritorniamo alla proprieta' V: ogni ED e' un UFD. La dimostreremo come corollario di un fatto piu' generale: ogni PID e' un UFD. Per dimostrare questo, useremo una comoda caratterizzazione di un UFD.

Ma prima di tutto diamo la definizione di UFD:

$$D \equiv \text{UFD} \Leftrightarrow \forall p \in D, p = q_1 q_2 \dots q_t, q_i \equiv \text{irriducibile}$$

e inoltre la fattorizzazione di p e' unica a meno di invertibili o dell'ordine.

Diamo anche la definizione di *lunghezza* che ci servira' in seguito: sia D un UFD, $a \in D, a \neq \text{invert.}$, fattorizziamo a , $a = p_1 \dots p_t$, allora

$$\text{lunghezza di } a := l(a) := t$$

Ad esempio, in $\mathbb{Z}$, $l(12) = l(2^2 \cdot 3) = l(2 \cdot 2 \cdot 3) = 3$. Vale anche questa banale proprieta':

$$a = bm \Leftrightarrow l(a) \geq l(b)$$

21.3.1 Caratterizzazione di un UFD

$$D \equiv \text{UFD} \Leftrightarrow \begin{cases} 1) \forall r \in D, r \equiv \text{irriducibile} \Rightarrow r \equiv \text{primo} \\ 2) \text{ Vale la c.c.a.f per gli ideali principali di } D \end{cases}$$

La c.c.a.f e' la *condizione delle catene ascendenti finite*, che dice che data una catena (in questo caso di ideali)

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

allora

$$\exists \bar{n} : \forall m > n, (a_m) = (a_n)$$

cioe', da un certo $\bar{n}$, la catena si stabilizza, finisce.

Dimostriamo questa caratterizzazione.

Proof: Dim $\Rightarrow$.

Ts: vale la 1) e la 2).

Proof: Dim: 1)

Ts: $a \equiv \text{irriducibile} \Rightarrow a \equiv \text{primo} \Leftrightarrow (a/bc \Rightarrow a/b \vee a/c)$

$$a/bc \Rightarrow am = bc$$

$$b = b_1 b_2 \dots b_r, b_i \equiv \text{irr.} \quad [\text{applicando la fattorizzazione}]$$

$$c = c_1 c_2 \dots c_s, c_j \equiv \text{irr.}$$

$$m = m_1 m_2 \dots m_t, m_k \equiv \text{irr.}$$

$$a = a$$

$$am = bc \Leftrightarrow (b_1 b_2 \dots b_r)(c_1 c_2 \dots c_s) = (m_1 m_2 \dots m_t)a$$

Poiche' la fatt. e' unica, il primo membro deve essere uguale al II a meno di invertibili, e poiche' a e' irriducibile, e quindi non invertibile, deve essere l'associato di qualche b_i o c_j , quindi:

If $a \equiv \text{associato di } b_i :$

$$a = b_i u_i, u_i \equiv \text{invert.}$$

$$u_i^{-1} a = b_i \Leftrightarrow a/b_i \Rightarrow a/b$$

allo stesso modo:

If $a \equiv \text{associato di } c_i :$

$$a = c_i u_i, u_i \equiv \text{invert.}$$

$$u_i^{-1} a = c_i \Leftrightarrow a/c_i \Rightarrow a/c$$

quindi:

$$a/b \vee a/c$$

□

Proof: Dim: 2)

Consideriamo la catena:

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots \Rightarrow$$

$$a_1 \in (a_2), a_2 \in (a_3), a_3 \in (a_4), \dots \Rightarrow$$

$$a_1 = \lambda_2 a_2, a_2 = \lambda_3 a_3, a_3 = \lambda_4 a_4, \dots$$

$$l(a_1) \geq l(a_2) \geq l(a_3) \geq \dots$$

Ora consideriamo l'insieme formato da tutte le lunghezze di ogni a_i :

$$A := \{l(a_i) \mid i \in \mathbb{N}\} \subseteq \mathbb{N}$$

e poiche' ogni $l(a_i) \in \mathbb{N}$, possiamo considerare il minimo di A :

$$\exists \bar{n} : \forall i, \bar{l} := l(a_{\bar{n}}) \leq l(a_i)$$

Prendiamo adesso un $m \in \mathbb{N} : m > n$:

$$(a_{\bar{n}}) \subseteq (a_m)$$

$$l(a_m) \leq l(a_{\bar{n}}) \text{ per quanto visto sopra}$$

$$l(a_{\bar{n}}) \leq l(a_m) \text{ perche' } l(a_{\bar{n}}) \text{ e' il minimo di } A$$

$$\text{quindi: } l(a_{\bar{n}}) = l(a_m)$$

$$a_{\bar{n}} = \lambda_m a_m$$

$$\begin{cases} l(a_{\bar{n}}) = l(a_m) \\ a_{\bar{n}} = \lambda_m a_m \end{cases} \Rightarrow \lambda_m \equiv \text{invert.}$$

$$\lambda_m^{-1} a_{\bar{n}} = a_m \Rightarrow (a_m) \subseteq (a_{\bar{n}}) \Rightarrow$$

$$(a_{\bar{n}}) = (a_m)$$

□

Proof: Dim: $\Leftarrow$

Ts: $1) \wedge 2) \Rightarrow D \equiv UFD$

Quindi dato $a \in D$, non invert., dobbiamo riuscirlo a fattorizzarlo in maniera "unica".

Prima di procedere, dimostriamo un altro fatto:

$$a \in D, a \neq \text{invert.} \Rightarrow a \text{ ha almeno un divisore irriducibile}$$

Proof: Se a e' irriducibile, allora abbiamo finito, altrimenti, sia $a = a_1 b_1$.

Riguardo ad a_1 ci sono questi due possibili casi:

$$\begin{cases} a_1 \equiv \text{irrid.} \Rightarrow \text{fine dim.} \\ a_1 = a_2 b_2 \end{cases}$$

anche per a_2 esistono i due casi: i

$$\begin{cases} a_2 \equiv \text{irrid.} \Rightarrow \text{fine dim: } a_2/a \\ a_2 = a_3 b_3 \end{cases}$$

possiamo procedere all'infinito? No, perche' la 2) ci viene in aiuto: consideriamo la catena creata fin'ora:

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

per la 2):

$$\exists \bar{n} : m = \bar{n} + 1, (a_m) = (a_{\bar{n}})$$

$$a_{\bar{n}+1} = \lambda a_{\bar{n}}$$

$$a_{\bar{n}} = a_{\bar{n}+1} b_{\bar{n}+1} = \lambda a_{\bar{n}} b_{\bar{n}+1} \Rightarrow$$

$$\lambda, b_{\bar{n}+1} \equiv \text{invertibili} \Rightarrow a_{\bar{n}} \equiv \text{irriducibile}$$

quindi abbiamo dimostrato che $a_{\bar{n}}$, irriducibile, divide a .

□

Ritorniamo alla nostra dimostrazione **21.3.1**.

Supponiamo che $a = a_1 b_1$, dove stavolta $a_1 \equiv \text{irriducibile}$.

Questa supposizione e' lecita perche' abbiamo dimostrato poco fa che a ha almeno un divisore irriducibile.

Allora, per b_1 si presentano i due soliti casi:

$$\begin{cases} b_1 \equiv \text{irrid.} \Rightarrow \text{fine dim: } a = a_1 b_1 \\ b_1 = a_2 b_2, \quad a_2 \equiv \text{irrid.} \end{cases}$$

anche qui reiteriamo e abbiamo i casi di b_2 :

$$\begin{cases} b_2 \equiv \text{irrid.} \Rightarrow \text{fine dim: } a = a_1 a_2 b_2 \\ b_2 = a_3 b_3, \quad a_3 \equiv \text{irrid.} \end{cases}$$

Possiamo continuare all'infinito? No, perche' per la 2), la seguente catena finisce:

$$(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \dots$$

cioe'

$$\exists \bar{n} : (b_m) = (b_{\bar{n}}), \quad m = \bar{n} + 1$$

$$b_{\bar{n}+1} = \lambda b_{\bar{n}}$$

$$b_{\bar{n}} = a_{\bar{n}+1} b_{\bar{n}+1} = a_{\bar{n}+1} \lambda b_{\bar{n}}$$

$$\lambda, a_{\bar{n}+1} \equiv \text{invertibili} \Rightarrow b_{\bar{n}} \equiv \text{irriducibile}$$

in definitiva

$$a = a_1 a_2 a_3 \dots a_{\bar{n}} b_{\bar{n}}$$

□

Ancora pero' non abbiamo utilizzato la 1). E' inutile? No! Ci manca da dimostrare l'unicita' della fattorizzazione ;)

Proof: Dim: unicity della fattorizzazione

Ts: $z = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \quad p_i, q_j \equiv \text{irr.} \Rightarrow$

$$r = s \wedge \text{I membro e' uguale al II a meno dell'ordine e di invertibili}$$

Per assurdo supponiamo che $r < s$.

$$p_1 / \text{I membro} = \text{II membro} \Rightarrow p_1 / q_1 \quad [\text{a meno di riordinare le } q_i]$$

$$p_1 \equiv \text{primo per la 1)!} \Rightarrow$$

$$p_1 = q_1 u_1, \quad u_1 \equiv \text{inv.}$$

$$q_1 u_1 p_2 \dots p_r = q_1 q_2 \dots q_s \Rightarrow u_1 p_2 \dots p_r = q_2 \dots q_s$$

Reiterando tutto questo, finiamo in:

$$u_1 u_2 \dots u_r = q_{r+1} \dots q_s \quad \text{che e' assurdo!}$$

e in modo analogo troviamo l'assurdo per $r > s$, quindi, $r = s$, e in particolare:

$$p_1 = q_1 u_1$$

$$p_2 = q_2 u_2$$

$$\vdots$$

$$p_r = q_r u_r$$

Questo vuol dire che a meno di invertibili e dell'ordine il I membro e il II sono la stessa cosa, quindi la fattorizzazione di z e' unica. □

La dimostrazione della caratterizzazione degli UFD e' conclusa. □

Adesso possiamo ritornare in 21.3.

21.3.2 PID $\Rightarrow$ UFD

Vogliamo mostrare che

$$D \equiv \text{PID} \Rightarrow D \equiv \text{UFD}$$

Proof: Dire che $D \equiv UFD$ equivale a dimostrare le due proprietà della caratterizzazione degli UFD.

La prima è banale, perché ogni $p \in D$, $p \equiv$ irriducibile e' anche primo (vedi 20).

Dimostriamo quindi la seconda proprietà, considerando questa catena di ideali:

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

Adesso consideriamo l'unione di tutti questi ideali:

$$J = \bigcup_{i \in \mathbb{N}} (a_i)$$

$J \triangleleft D$? Non possiamo subito rispondere usando la proprietà 17.8.1, perché la J ha un numero infinito di elementi, allora lo dimostriamo direttamente:

Proof: Dim: $J \triangleleft D$

$$x, y \in J \Rightarrow x - y \in J?$$

$$x \in (a_i), y \in (a_j), i < j$$

$$(a_i) \subseteq (a_j) \Rightarrow x \in (a_j) \Rightarrow$$

$$x - y \in (a_j) \subseteq J$$

$$d \in D, xd \in J?$$

$$x \in (a_i), xd \in (a_i) \subseteq J \text{ [prop. di assorbimento]}$$

□

Poiché per Hp $D \equiv PID$, allora anche J lo è, e quindi $J = (j)$, ma allora

$$J = (j), j \in (a_n) \Rightarrow (j) \subseteq (a_n) \Rightarrow$$

$$J \subseteq (a_n) \subseteq J \Rightarrow J = (a_n)$$

$$\text{Dato } m > n \quad J = (a_n) \subseteq (a_m) \subseteq J \Rightarrow$$

$$(a_m) = J$$

che è quello che volevamo dimostrare.

□

21.4 ED $\Rightarrow$ PID $\Rightarrow$ UFD, e controesempi

Ricapitolando tutto quello visto fin'ora:

Theorem 21.10.

$$\text{Campo} \Rightarrow \text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{Dominio} \Rightarrow \text{Anello comm} \Rightarrow \text{Anello}$$

Nessuna di queste implicazioni ha l'inverso.

Proof:

(1) **Dim:** Anello comm $\not\Leftarrow$ Anello

Basta considerare le matrici.

(2) **Dim:** Dominio $\not\Leftarrow$ Anello comm

Basta considerare $\mathbb{Z}_{10}$. $\mathbb{Z}_{10}$ ha divisori dello zero, ad esempio $2 \cdot 5 = 0$.

(3) **Dim:** Campo $\not\Leftarrow$ ED

Basta considerare $\mathbb{Z}$, dove abbiamo visto che è un ED qui 21.1.

(4) **Dim:** UFD $\not\Leftarrow$ Dominio

Consideriamo $D \subseteq R[x]$ (che è un dominio):

$$D := \{f(x) \in R[x] \mid f'(0) = 0\}$$

Mostriamo che la 1) della caratterizzazione degli UFD non vale.

$$x^2, x^3 \in D, \quad x \notin D$$

$$x^2 / x^3 x^3 = x^6 = x^2 x^4$$

$$x^3 \neq x^2 x \text{ perche' } x \notin D \Rightarrow$$

$$x^2 \nmid x^3 \Rightarrow x^2 \neq \text{primo}$$

Un'altro controesempio. Consideriamo $D \subseteq \mathbb{C}$,

$$D = \{a + ib\sqrt{3} \mid a, b \in \mathbb{Z}\}$$

Vediamo che esistono due fattorizzazioni diverse di uno stesso elemento.

$$2, 1 + i\sqrt{3}, 1 - i\sqrt{3} \in D, \text{ e sono irriducibili}$$

$$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$$

(5) **Dim:** $\text{PID} \not\Leftarrow \text{UFD}$

$\mathbb{Z}[x]$, per il teorema di Gauss ($A \equiv \text{UFD} \Rightarrow A[x] \equiv \text{UFD}$), e' un UFD. Pero' non e' un PID.

Ts: $\mathbb{Z}[x] \neq \text{PID} \Leftrightarrow \exists I \triangleleft \mathbb{Z}[x] : I \neq \text{principale}$

$$I := (2, x) = \{2a(x) + xb(x) \mid a(x), b(x) \in \mathbb{Z}[x]\}$$

Per assurdo $I = (h(x))$

$$(h(x)) = (2, x) \Rightarrow 2 \in (h(x)) \Rightarrow 2 = \lambda h(x) \Rightarrow$$

$$h(x)/2 \Rightarrow h(x) = \pm 1 \vee h(x) = \pm 2$$

$$\text{If } h(x) = \pm 1$$

$$(1) = I = \mathbb{Z}[x] \text{ [assurdo: } I \text{ non ha termine noto dispari]}$$

$$\text{If } h(x) = \pm 2$$

$$(2) = I = (2, x) \Rightarrow x = 2\lambda(x) \Rightarrow \lambda(x) = \frac{1}{2}x \text{ [assurdo: } 1/2 \notin \mathbb{Z}]$$

(6) **Dim:** $\text{ED} \not\Leftarrow \text{PID}$

Il controesempio e'

$$D = \{a + ib\sqrt{19} \mid a, b \in 2\mathbb{Z}\}$$

la dimostrazione di questo controesempio e' troppo complessa per adesso.

□

22 Interi di Gauss

Nelle profondita' dello spazio...

Creiamo questo insieme:

$$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

e anche questo:

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Gli elementi di $\mathbb{Z}[i]$ sono gli *interi di Gauss*.

$\mathbb{Q}[i]$ e' un dominio, perche' e' un sottoinsieme di $\mathbb{C}$, ma e' anche un campo perche' ha l'inverso:

$$\frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}$$

$\mathbb{Z}[i]$ e' dominio, ma non un campo, infatti i suoi unici invertibili sono $\pm 1, \pm i$.

Proof: Consideriamo la formula dell'inverso:

$$\frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2} \in \mathbb{Z}[i] \Leftrightarrow \frac{a}{a^2 + b^2} \in \mathbb{Z} \wedge \frac{b}{a^2 + b^2} \in \mathbb{Z}$$

allora

$$\begin{aligned} a^2 + b^2 &\neq 0 \\ \frac{a}{a^2 + b^2} \in \mathbb{Z} &\Leftrightarrow \frac{a}{a^2 + b^2} = z, \quad z \in \mathbb{Z} \Leftrightarrow \\ a &= z(a^2 + b^2) \Leftrightarrow a = \pm 1, b = 0, z = 1 \end{aligned}$$

analogamente per l'altro caso □

(1) Ecco una prova piu' elegante

Siano $x = m + ni, x' \in \mathbb{Z}[i]$ non invertibili, con x' inverso di x , allora

$$\begin{aligned} xx' = 1 &\Rightarrow |xx'| = |x||x'| = 1 \Rightarrow |x| = 1 \\ |x| = 1 &\Rightarrow m^2 + n^2 = 1 \Rightarrow \begin{cases} m = \pm 1 & n = 0 \\ m = 0 & n = \pm 1 \end{cases} \end{aligned}$$

□

Vale questa proprieta':

$$Q(\mathbb{Z}[i]) = \mathbb{Q}[i]$$

cioe' il campo dei quozienti di $\mathbb{Z}[i]$ e' $\mathbb{Q}[i]$.

Proof:

$$\begin{aligned} Q(\mathbb{Z}[i]) &= \left\{ \frac{a + ib}{c + id} \mid a, b, c, d \in \mathbb{Z} \right\} \\ \frac{a + ib}{c + id} &= \frac{(a + ib)(c - id)}{(c + id)(c - id)} = \\ &= \frac{i(bc - ad) + (bd + ac)}{c^2 + d^2} = \\ &= \underbrace{\frac{bd + ac}{c^2 + d^2}}_{\in \mathbb{Q}} + i \underbrace{\frac{bc - ad}{c^2 + d^2}}_{\in \mathbb{Q}} \in \mathbb{Q} \Rightarrow \\ Q(\mathbb{Z}[i]) &= \mathbb{Q}[i] \end{aligned}$$

□

Theorem 22.1.

$$\mathbb{Z}[i] \equiv ED$$

Questo teorema e' importante perche' potremo applicare tutte le proprieta' degli ED, dei PID e degli UFD a $\mathbb{Z}[i]$.

Proof:

$$\exists v : \mathbb{Z}[i]^* \longrightarrow \mathbb{N} \quad v(a + ib) := |a + ib| = a^2 + b^2$$

$$v(a + ib) \leq v((a + ib)(c + id)) ?$$

$$|a + ib| \leq |(a + ib)(c + id)| = |a + ib||c + id|$$

$$z_1, z_2 \neq 0 \in \mathbb{Z}[i] \quad \exists q, r \in \mathbb{Z}[i] : z_1 = qz_2 + r \quad r = 0 \vee v(r) < v(z_2)$$

Ritorniamo in $\mathbb{Q}[i]$:

$$z_2 \neq 0 \in \mathbb{Z}[i] \subseteq \mathbb{Q}[i] \Rightarrow z_2 \in \mathbb{Q}[i]$$

$$\exists z_2^{-1} \in \mathbb{Q}[i]$$

$$z_1 z_2^{-1} \in \mathbb{Q}[i] \Leftrightarrow z_1 z_2^{-1} = \frac{m}{n} + i \frac{r}{s}$$

$$\frac{m}{n} + i \frac{r}{s} = u + \frac{m'}{n} + i(v + \frac{r'}{s})$$

Quest'ultimo passaggio si puo' fare, ad esempio, aggiungendo e sottraendo $1 + i$, cioè:

$$u = v = 1$$

$$\frac{m}{n} + 1 - 1 = \frac{m - n}{n} + 1, \quad m - n = m'$$

$$i(\frac{r}{s} + 1 - 1) = i(\frac{r - s}{s} + 1), \quad r - s = r'$$

In questo modo abbiamo che

$$\left| \frac{m'}{n} \right|, \left| \frac{r'}{s} \right| \leq \frac{1}{2}$$

continuiamo,

$$\begin{aligned} z_1 z_2^{-1} &= u + \frac{m'}{n} + i(v + \frac{r'}{s}) = \frac{m'}{n} + iv + u + i \frac{r'}{s} = \\ &= u + iv + \left(\frac{m'}{n} + i \frac{r'}{s} \right) \end{aligned}$$

moltiplichiamo ambo i membri per z_2 :

$$z_1 = \underbrace{z_2(u + iv)}_{=q \in \mathbb{Z}[i]} + \underbrace{z_2 \left(\frac{m'}{n} + i \frac{r'}{s} \right)}_{=r}$$

$$r = z_1 - q \in \mathbb{Z}[i] \quad [\text{cosi' abbiamo diviso } z_1 \text{ per } z_2]$$

controlliamo che $v(r) < v(z_2)$:

$$\begin{aligned} v(r) &= v(z_2) v \left(\left(\frac{m'}{n} + i \frac{r'}{s} \right) \right) = v(z_2) \left(\left(\frac{m'}{n} \right)^2 + \left(\frac{r'}{s} \right)^2 \right) \leq \\ &\leq v(z_2) \left(\frac{1}{4} + \frac{1}{4} \right) = \frac{1}{2} v(z_2) \\ v(r) &\leq \frac{1}{2} v(z_2) < v(z_2) \end{aligned}$$

□

22.1 Somma di quadrati

Stranamente per rispondere a una semplicemente domanda, abbiamo bisogno dell'aiuto degli interi di Gauss! La domanda e': dato n e' vero che

$$n = a^2 + b^2, \quad a, b \in \mathbb{Z}$$

Cioe', e' vero che posso scrivere n come somma di due quadrati? Quali sono questi due quadrati?

Dimostriamo un teorema preliminare

Theorem 22.2. Dato $p > 2$ primo.

$$p = a^2 + b^2 \Leftrightarrow p = 1 \pmod{4}$$

⟨1⟩ **Dim** $\Rightarrow$

$$p = a^2 + b^2$$

p e' dispari, quindi a, b devono essere uno pari e l'altro dispari

$$a = 2m \quad b = 2n + 1$$

$$p = 4m^2 + 4n^2 + 4n + 1 = 1 \pmod{4}$$

□

⟨2⟩ **Dim** $\Leftarrow$

PROOF SKETCH: Proveremo che p non e' primo in $\mathbb{Z}[i]$ e che $p^2 = (a^2 + b^2)(c^2 + d^2)$. Infine faremo vedere che $p = a^2 + b^2$.

⟨2.1⟩ **Step I**

ASSUME: 1. $n \in \mathbb{N}$

$$2. p = 4n + 1$$

3. p primo

PROVE: $\exists x : x^2 = -1 \pmod{p}$

Proof:

$$\text{LET: } x = 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}$$

$$\frac{p-1}{2} = 2n$$

$$x = (-1)(-2)(-3) \cdots (-2n)$$

[$2n$ e' pari]

$$x^2 = xx = (1 \cdot 2 \cdot \dots \cdot 2n)((-1)(-2)(-3) \cdots (-2n))$$

$$x^2 = (1 \cdot 2 \cdot \dots \cdot 2n)((p-1)(p-2)(p-3) \cdots (p-2n)) \pmod{p}$$

$$p-2n = 2n+1, \quad p-2n-1 = 2n, \quad p-2n-2 = 2n-1, \quad \dots, \quad p-1 = 4n$$

$$x^2 = 1 \cdot 2 \cdot \dots \cdot 2n \cdot (2n+1)(2n+2) \cdots (4n) \pmod{p}$$

$$x^2 = 4n! = (p-1)! \pmod{p}$$

$$(p-1)! = -1 \pmod{p} \quad [\text{thm di Wilson}]$$

$$x^2 = -1 \pmod{p}$$

□

⟨3⟩ **Step II**

PROVE: $\exists y < \frac{p}{2} : y^2 = -1 \pmod{p}$

Proof:

$$\text{LET: } x : x^2 = -1 \pmod{p}$$

$$\text{CASE: } x < \frac{p}{2}$$

□

$$\text{CASE: } x > \frac{p}{2}$$

$$\text{LET: } y = p - x$$

$$y = p - x < \frac{p}{2}$$

$$y^2 = p^2 + x^2 - 2px$$

$$y^2 = x^2 = -1 \pmod{p}$$

□

⟨4⟩ p non e' primo in $\mathbb{Z}[i]$

$$\text{LET: } z < \frac{p}{2} : z^2 = -1 \pmod{p}$$

PROVE: Se $p/ab \Rightarrow p \nmid a \wedge p \nmid b$

Proof:

$$z^2 = -1 \pmod{p} \Leftrightarrow z^2 + 1 = \lambda p \Leftrightarrow$$

$$p \mid z^2 + 1$$

$$z^2 + 1 = (z + i)(z - i) \in (\mathbb{Z}[i])$$

$$p \in \mathbb{Z} \subseteq \mathbb{Z}[i] \Rightarrow p \mid (z+i)(z-i)$$

ASSUME: 1. $p \nmid z-i$

PROVE: proviamo che si cade in assurdo

$\langle 4.1 \rangle$ Q.E.D.

$$p \nmid z-i \Rightarrow z-i = \mu p, \mu \in \mathbb{Z}[i]$$

$$\varepsilon p = \text{coniugato di } \mu p, \quad z+i = \text{coniugato di } z-i \Rightarrow$$

$$z+i = \varepsilon p \Rightarrow p \mid z+i$$

$$p \mid z+i \wedge p \nmid z-i \Rightarrow p^2 \mid z^2+1 \Rightarrow$$

$$mp^2 = z^2 + 1 = \lambda p \Rightarrow$$

$$mp = \lambda \Rightarrow p \mid \lambda \quad (1)$$

$$z < \frac{p}{2} \Rightarrow z^2 < \frac{p^2}{4} \Rightarrow$$

$$z^2 + 1 < \frac{p^2}{4} + 1 \Rightarrow \lambda p < \frac{p^2}{4} + 1 < p^2 \Rightarrow$$

$$\lambda < p \quad (2)$$

La (1) e (2) sono in contrasto, assurdo! Possiamo ripetere lo stesso ragionamento per dimostrare che $p \nmid z+i$, quindi, in conclusione:

$$(p \nmid z^2+1 \Rightarrow p \nmid z+i \wedge p \nmid z-i) \Rightarrow p \text{ non e' primo in } \mathbb{Z}[i]$$

□

□

$\langle 5 \rangle$ Divisori di p^2

Poiche' p non e' primo in $\mathbb{Z}[i]$ e poiche' $\mathbb{Z}[i]$ e' un ED, allora p e' riducibile (in $\mathbb{Z}[i]$), ovvero:

$$p = (a+ib)(c+id), \quad a+ib, c+id \equiv \text{non invert.}$$

Poiche' gli unici invertibili in $\mathbb{Z}[i]$ sono $\pm i, \pm 1$, allora

$$a+ib, c+id \neq \pm i, \pm 1 \Rightarrow a, b, c, d \neq \pm 1$$

prendendo il coniugato di p abbiamo:

$$p = (a-ib)(c-id)$$

allora

$$p = (a+ib)(c+id)$$

$$p = (a-ib)(c-id)$$

$$p^2 = pp = (a+ib)(a-ib)(c+id)(c-id) = (a^2+b^2)(c^2+d^2) \Rightarrow$$

$$(a^2+b^2)/p^2$$

ma poiche' p e' primo in $\mathbb{Z}$, gli unici divisori di p^2 in $\mathbb{Z}$ sono:

$$D = \{1, p, p^2\}$$

1 lo scartiamo perche' sappiamo che $(a^2+b^2) \neq 1$.

Se $(a^2+b^2) = p^2$, si avrebbe che

$$p^2 = p^2(c^2+d^2)$$

ma anche in questo caso sappiamo che $c^2 + d^2 \neq 1$.

Quindi l'unico divisore lecito e' p , cioè'

$$a^2 + b^2 = p$$

che e' proprio quello che volevamo dimostrare ;) □

Theorem 22.3. Adesso possiamo trattare tutti i numeri.

Dato $n \in \mathbb{Z}$, e la sua fattorizzazione

$$n = 2^t q_1^{m_1} q_2^{m_2} \dots q_r^{m_r} p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$$

dove

$$t \geq 0, \quad \forall i \quad q_i = 1 \pmod{4}, \quad p_i = 3 \pmod{4}$$

allora

$$n = a^2 + b^2 \Leftrightarrow \forall i, n_i \in 2\mathbb{N}$$

In altre parole, n e' somma di quadrati, se e solo se, gli esponenti dei suoi fattori primi che sono della forma $4\lambda + 3$, hanno esponente pari.

Nota: un primo p , poiche' dispari, e' sempre nella forma

$$p = 1 \pmod{4} \vee p = 3 \pmod{4}$$

⟨2⟩ Dimostriamo solo $\Leftarrow$

Proof:

⟨1⟩ Il prodotto della somma di due quadrati e' ancora somma di due quadrati

PROVE: $(a^2 + b^2)(c^2 + d^2) = (x^2 + y^2)$

Proof: Basta considerare la norma dei numeri complessi:

$$a^2 + b^2 = |a + ib|^2$$

$$c^2 + d^2 = |c + id|^2$$

$$|a + ib||c + id| = |(a + ib)(c + id)| = |x^2 + y^2|$$

□

Quindi,

2^t e' sempre somma di quadrati:

$$2^t = \begin{cases} 2^{t-1} + 2^{t-1} & t \notin 2\mathbb{N} \\ 0 + 2^t & t \in 2\mathbb{N} \end{cases}$$

Tutti i q_i sono somma di quadrati (l'abbiamo dimostrato in 22.2).

E infine, tutti i p_i sono somma di quadrati perche' hanno l'esponente pari, e quindi sono quadrati:

$$n_i = 2s, \quad p_i^{n_i} = 0 + p_i^{2s}$$

□

22.1.1 Esempio

Scomponiamo 1530 come somma di quadrati:

$$1530 = 2 \cdot 3^2 \cdot 5 \cdot 17$$

$$1530 = |1 + i| \cdot |3| \cdot |1 + i2| \cdot |1 + i4| =$$

$$= |(3 + i3)(1 + i2)(1 + i4)| = |-39 - i3| = 39^2 + 3^2$$

$$1530 = 39^2 + 3^2$$

Nota: la scomposizione non e' necessariamente unica:

$$\begin{aligned} 1530 &= |1+i| \cdot |3| \cdot |1+i2| \cdot |1-i4| = \\ &= |(3+i3)(1+i2)(1-i4)| = |33+i21| = 33^2 + 21^2 \\ 1530 &= 33^2 + 21^2 \end{aligned}$$

23 Polinomi UFD

Alcune premesse:

In un UFD, e' possibile calcolare il MCD (anche se non siamo in un ED): e' sufficiente usare il metodo descritto in 9.9.1.

L'insieme dei polinomi a indeterminate x, y e a coefficienti in K si puo' pensare come l'insieme dei polinomi a indeterminata x e a coefficienti in $k[x]$. Esempio:

$$x^3 + xy^2 + 2x^2 + y^2 + 4x - 4y + 5 \in \mathbb{R}[x, y]$$

$\mathbb{R}[x, y]$ lo possiamo pensare come $(\mathbb{R}[x])[y]$:

$$(x+1)y^2 - 4y + x^3 + 4x + 5 \in \mathbb{R}[x][y]$$

qui, $(x+1) \in \mathbb{R}[x]$ e' un coefficiente della indeterminata y^2 , e $x^3 + 4x + 5$ e' il termine noto. Se, invece, consideriamo $(\mathbb{R}[y])[x]$:

$$x^3 + 2x^2 + (y^2 + 4)x + y^2 + 5 \in \mathbb{R}[y][x]$$

Proposition 23.1. *Sia A un UFD, e $f(x) \in A[x]$ un suo polinomio primitivo. Allora,*

$$f(x) \text{ irriducibile in } A[x] \Leftrightarrow f(x) \text{ irriducibile in } Q(A)[x]$$

dove $Q(A)$ e' il campo dei quozienti di A .

Proof: La dimostrazione e' analoga a quella della prop [16.3,pg.70]. □

23.1 Teorema di Gauss

Theorem 23.2.

$$A \equiv UFD \Rightarrow A[x] \equiv UFD$$

Proof: La dimostrazione del teorema e' identica a quella che abbiamo fatto per $\mathbb{Z}[x]$:

1. Si dimostra il Lemma di Gauss (vedi 16.19)
2. il suo corollario (vedi 16.20)
3. e il teorema (vedi 16.22)

Le uniche accortezze a cui bisogna fare attenzione sono le seguenti sostituzioni:

$$\begin{aligned} \mathbb{Z} &\longrightarrow A \\ \mathbb{Z}[x] &\longrightarrow A[x] \\ \mathbb{Q} &\longrightarrow Q(\mathbb{A}) \\ \mathbb{Q}[x] &\longrightarrow Q(\mathbb{A})[x] \end{aligned}$$

Dove $Q(\mathbb{A})$ e' il campo dei quozienti di $\mathbb{A}$. ($Q(\mathbb{A})$ e' un campo, quindi e' UFD). □

23.1.1 Esempi

1. $\mathbb{Z}[x]$ e' UFD
2. Dato K campo, $K[x]$ e' UFD, ma lo e' anche $K[x, y]$ perche' lo possiamo esprimere come $(K[x])[y]$, dove $K[x]$ e' UFD, e quindi per Gauss $(K[x])[y]$ e' sempre UFD.
3. Allora possiamo reiterare e quindi

$$K[x_1, x_2, \dots, x_n] \equiv UFD$$

23.2 Criteri di irriducibilita'

Valgono gli stessi criteri di irriducibilita' che abbiamo visto in $\mathbb{Z}[x]$, e le loro dimostrazioni:

1. Criterio di Eisenstein (vedi 16.23):

Sia $A \equiv UFD$ e

$$f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{A}[x]$$

e sia primitivo, allora

$$\begin{cases} \exists p, \text{ primo} : p/a_i, i = 0, \dots, d-1 \\ p^2 \nmid a_0 \end{cases} \Rightarrow f(x) \equiv \text{irriducibile in } \mathbb{A}[x]$$

2. Criterio di riduzione modulo p (vedi 16.24):

Sia $A \equiv UFD$ e

$$f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{A}[x]$$

e sia primitivo, allora

$$\exists p, \text{ primo} : p \nmid a_d, \wedge f(x) \text{ irriducibile in } \frac{A}{(p)}[x] \Rightarrow f(x) \text{ irriducibile in } \mathbb{A}[x]$$

dove (p) e' l'ideale principale generato da p , $\frac{A}{(p)}$ e' A quozientato da (p) , e inoltre $\frac{A}{(p)}$ e' un campo perche' p e' primo (vedi 18.2).

23.3 Algoritmo di divisione in un UFD

Dato $A[x] \equiv UFD$, se A non e' un campo, $A[x]$ non sara' necessariamente un ED . Questo significa che in $A[x]$ l'algoritmo di divisione non vale sempre. Esistono pero' dei casi in cui vale: dati

$$f(x) = a_mx^m + \dots + a_0, \quad g(x) = b_nx^n + \dots + b_0 \in A[x]$$

l'algoritmo di divisione si puo' applicare su

$$f(x) = q(x)g(x) + r(x)$$

se il coefficiente dell'indeterminata di grado massimo di $g(x)$ e' invertibile, cioe' se $\exists b_n^{-1}$.

Proof: Basta osservare che b_n^{-1} e' l'unico invertibile richiesto nella dimostrazione fatta in 16.7 $\square$

Index

elemento
 irriducibile, 97
 primo, 97