APPUNTI DEL CORSO DI ALGEBRA
per Informatica

ELEMENTI DI TEORIA DEGLI INSIEMI

1. Insiemi e sottoisiemi

Supponiamo noti i concetti di **insieme**, di **elemento** di un insieme, i numeri interi naturali $\mathbb{N}$, gli interi relativi $\mathbb{Z}$, i razionali $\mathbb{Q}$, i reali $\mathbb{R}$ con le loro più elementari proprietà (per indicare che un elemento x appartiene all'insieme X scriveremo $x \in X$ mentre $x \notin X$ significa che x non è un elemento di X).

Dati due insiemi X e Y diremo che X è **sottoinsieme** di Y se ogni elemento di X è anche elemento di Y (scriveremo $X \subseteq Y$), oppure $X \subset Y$.) per esempio l'insieme $\mathbb{N}$ dei numeri interi positivi è un sottoinsieme dell'insieme $\mathbb{Z}$ dei numeri interi.

Se $X \subseteq Y$ e $Y \subseteq X$ i due insiemi si dicono uguali e si scrive $X = Y$, se $X \subseteq Y$ ma $X \neq Y$ diremo che X è un sottoinsieme **proprio** di Y.
L'insieme privo di elementi si dice insieme **vuoto** e si indica con il simbolo $\emptyset$.

Se X e Y sono insiemi l'intersezione di X e Y (che si indica con $X \cap Y$) è l'insieme di quegli elementi che appartengono sia ad X che a Y.

Due insiemi X e Y tali che $X \cap Y = \emptyset$ si dicono **disgiunti**.

Se X e Y sono insiemi l'unione di X e Y (che si indica con $X \cup Y$) è l'insieme di quegli elementi che appartengono ad X oppure a Y oppure ad entrambi.

Le operazioni di unione e intersezione sono **associative**, cioè se A, B, C sono insiemi, si ha che $A \cup (B \cup C) = (A \cup B) \cup C$ e $A \cap (B \cap C) = (A \cap B) \cap C$

Esercizio 1.1: Provare che per le operazioni di unione e intersezione valgono le proprietà **distributive**, cioè se A, B, C sono insiemi, si ha che
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Se Y è un insieme ed X è un sottoinsieme di Y si dice **differenza** o **complementare** di X in Y e si indica con $Y - X$ oppure $\mathcal{C}_Y(X)$ l'insieme degli elementi di Y che non appartengono a X.

Per descrivere un insieme si possono elencare tutti i suoi elementi tra parentesi graffe, per esempio $X = \{1, 2, 3\}$, oppure usando una proprietà soddisfatta da tutti e soli gli elementi dell'insieme, ad esempio l'insieme dei numeri interi pari si indica con $X = \{n \in \mathbb{N} \mid n \text{ è pari}\}$ [1]

A volte si considerano insiemi i cui elementi sono a loro volta insiemi, per esempio l'insieme di tutti i sottoinsiemi (o parti) di un insieme X si indica con $\mathcal{P}(X)$.

Le definizioni di unione e intersezione di due insiemi si possono generalizzare ad un insieme (o famiglia) $\mathcal{F}$ di insiemi definendo:

$$\bigcup_{A \in \mathcal{F}} A = \{x \mid x \in A \text{ per qualche } A \in \mathcal{F}\} \text{ unione di tutti gli insiemi di } \mathcal{F}$$

$$\bigcap_{A \in \mathcal{F}} A = \{x \mid x \in A \text{ per ogni } A \in \mathcal{F}\} \text{ intersezione di tutti gli insiemi di } \mathcal{F}$$

Definiamo infine l'insieme **prodotto cartesiano** di due insiemi X e Y l'insieme formato da tutte le coppie **ordinate** (x, y) in cui la prima componente x è un elemento di X la seconda y di Y e si indica con $X \times Y$, due coppie ordinate (x, y) e (x', y') sono uguali se e solo se $x = x'$ e $y = y'$.
In generale con $X_1 \times X_2 \times \ldots \times X_n$ indichiamo l'insieme delle n - uple ordinate $(x_1, x_2, \ldots, x_n)$ la cui i - esima componente x_i, è un elemento di X_i. [2]

[1] oppure con $X = \{0, 2, 4, 6, ...\}$ (il simbolo | si legge "tale che").

[2] Il prodotto cartesiano di n copie di X cioè $X \times X \ldots \times X$ si indica di solito con X^n

2. Corrispondenze e applicazioni

Dati due insiemi X e Y diremo **corrispondenza** o **relazione** di X in Y un qualunque sottoinsieme φ del prodotto cartesiano $X \times Y$, se $(x, y) \in \varphi$ diremo che x corrisponde a y nella corrispondenza φ.

Dati due insiemi X e Y un'**applicazione** (o **funzione**) φ di X in Y è una corrispondenza di X in Y che gode della seguente proprietà :

Per ogni $x \in X$ esiste un unico $y \in Y$ tale che $(x, y) \in \varphi$.

Per indicare che φ è un'applicazione di X in Y si scrive $\varphi : X \to Y$ inoltre si scrive $\varphi(x) = y$ invece di $(x, y) \in \varphi$.
X si dice **dominio** di φ, Y si dice **codominio** di φ.

Per descrivere l'applicazione φ è sufficiente specificare per ogni elemento $x \in X$ l'elemento $\varphi(x) \in Y$, $\varphi(x)$ si dice **immagine** di x mediante l'applicazione φ.

Sia $\varphi : X \to Y$ un'applicazione, se A è un sottoinsieme di X, si dice **immagine** di A mediante φ l'insieme $\varphi(A) = \{\varphi(x) \mid x \in A\}$; se $B \subseteq Y$, l'insieme $\varphi^{-1}(B) = \{x \mid x \in X, \varphi(x) \in B\}$ si dice **controimmagine** (o **immagine inversa**) di B, se $y \in Y$ si scrive $\varphi^{-1}(y)$ invece di $\varphi^{-1}(\{y\})$. [1]

Sia $\varphi : X \to Y$ un'applicazione:
φ si dice **iniettiva** se, per ogni $x, x' \in X$, $\varphi(x) = \varphi(x')$ implica che $x = x'$
φ si dice **surgettiva** se $\varphi(X) = Y$
φ si dice **bigettiva** (o **corrispondenza biunivoca** o **bigezione**) se è iniettiva e surgettiva.

Quindi φ è **iniettiva** se e solo se elementi distinti di X hanno immagini distinte, ovvero se e solo se la controimmagine di ogni elemento di Y contiene al più un elemento di X.

φ è **surgettiva** se e solo se per ogni $y \in Y$ esiste almeno un $x \in X$ tale che $\varphi(x) = y$, ovvero se e solo se la controimmagine di ogni elemento di Y è non vuota.

Siano $\varphi : X \to Y$ e $\psi : Y \to Z$ due applicazioni, diremo **applicazione composta** di φ e ψ e scriveremo $(\psi \circ \varphi)$ l'applicazione definita ponendo
$(\psi \circ \varphi)(x) = \psi(\varphi(x))$

[1] quindi $\varphi^{-1}(y) = \{x \mid x \in X, \varphi(x) = y\}$

Teorema 2.1.: *Siano $\varphi : X \to Y$ e $\psi : Y \to Z$: due applicazioni. Allora*
i) *se φ e ψ sono iniettive allora$\psi \circ \varphi$ è iniettiva;*
ii) *se φ e ψ sono surgettive allora $\psi \circ \varphi$ è surgettiva;*
iii) *se φ e ψ sono bigettive allora $\psi \circ \varphi$ è bigettiva.*
Dim.: i) Siano φ e ψ iniettive, se x e $x' \in X$, e $(\psi \circ \varphi)(x) = (\psi \circ \varphi)(x')$ per l'iniettività di $\psi, \psi(\varphi(x)) = \psi(\varphi(x'))$ implica $\varphi(x) = \varphi(x')$ ed essendo φ iniettiva si ha $x = x'$.
ii) Se $z \in Z$ esiste $y \in Y$ tale che $\psi(y) = z$, ma, essendo anche φ surgettiva, esiste $x \in X$ tale che $\varphi(x) = y$, quindi $(\psi \circ \varphi)(x) = \psi(\varphi(x)) = z$, cioè $\psi \circ \varphi$ è surgettiva.
iii) discende direttamente da i) e ii).■

Teorema 2.2.: *Siano $\varphi : X \to Y$ e $\psi : Y \to Z$: due applicazioni. Allora*
i) *se $\psi \circ \varphi$ è iniettiva allora φ è iniettiva;*
ii) *se $\psi \circ \varphi$ è surgettiva allora ψ è surgettiva;*
iii) *se $\psi \circ \varphi$ è bigettiva allora φ è iniettiva e ψ è surgettiva*
Dim.: i) Siano x e $x' \in X$, se $\varphi(x) = \varphi(x')$ per l'iniettività di $\psi \circ \varphi$,
$(\psi \circ \varphi)(x) = (\psi \circ \varphi)(x')$ implica $x = x'$ quindi φ è iniettiva.
ii) Se $z \in Z$ esiste $x \in X$ tale che $(\psi \circ \varphi)(x) = z$, e, posto $y = \varphi(x)$, si ha $\psi(y) = z$ quindi ψ è surgettiva.
iii) discende direttamente da i) e ii). ■

Si prova facilmente che la composizione di applicazioni è **associativa**, cioè se $\varphi : X \to Y,\ \psi : Y \to Z\ \omega : Z \to T$ sono applicazioni, allora

$$\omega \circ (\psi \circ \varphi) = (\omega \circ \psi) \circ \varphi$$

.

Sia X un insieme, chiamiamo **applicazione identica** (o **identità**) su X, l'applicazione $i_X : X \to X$ definita da $i_X(x) = x$ per ogni $x \in X$.

Si prova subito che data un'applicazione $\varphi : X \to Y$, se $i_X : X \to X$ e $i_Y : Y \to Y$ sono le applicazioni identiche rispettivamente su X e Y, allora $\varphi \circ i_X = i_Y \circ \varphi = \varphi$
.

Si provano anche facilmente i seguenti:
Teorema 2.3.: *Sia $\varphi : X \to Y$ un'applicazione iniettiva allora esiste un'applicazione $\psi : Y \to X$ tale che $\psi \circ \varphi = i_X$*
Teorema 2.4.: *Sia $\varphi : X \to Y$ un'applicazione surgettiva, allora esiste un'applicazione $\psi : Y \to X$ tale che $\varphi \circ \psi = i_Y$*
Teorema 2.5.: *Sia $\varphi : X \to Y$ un'applicazione, supponiamo che esistano due applicazioni $\psi_1 : Y \to X$ e $\psi_2 : Y \to X$ tali che $\psi_1 \circ \varphi = i_X$ e $\varphi \circ \psi_2 = i_Y$ allora $\psi_1 = \psi_2$*

3. Principio di induzione.

E' spesso utile in alcuni tipi di dimostrazioni fare ricorso al cosiddetto "principio di induzione"

Principio di induzione aritmetica: *Sia $n_0 \in \mathbb{Z}$ e sia $\mathcal{P}$ una affermazione sui numeri interi $n \geq n_0$. Supponiamo siano soddisfatte le seguenti due condizioni:*

i) *$\mathcal{P}$ è vera per il numero n_0;*

ii) *per ogni intero $n > n_0$ se $\mathcal{P}$ è vera per il numero $n-1$ allora $\mathcal{P}$ è vera per il numero n.*

Allora $\mathcal{P}$ è vera per ogni numero intero $n \geq n_0$.

Esempi:

3.1. Proviamo che per ogni numero reale q, $q \neq 1$ la somma delle sue prime n potenze $(n = 0, 1 \ldots)$

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

L'affermazione è banalmente vera per $n = 0$, supponiamola vera per $n - 1$ cioè

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

e proviamola per n, ovvero aggiungiamo ai due membri dell'uguaglianza q^n, avremo che

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

da cui la tesi.

3.2. Proviamo che per ogni numero intero $n \geq 2$ si ha

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \ldots \left(1 - \frac{1}{n}\right) = \frac{1}{n}$$

L'affermazione è vera per $n = 2$, infatti $1 - \frac{1}{2} = \frac{1}{2}$, supponiamola vera per $n - 1$ cioè

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \ldots \left(1 - \frac{1}{n-1}\right) = \frac{1}{n-1}$$

Moltiplicando ambo i membri dell'uguaglianza per $1 - \frac{1}{n}$ si ottiene la tesi.

3.3. Denotiamo $0! = 1, n! = 1 \cdot 2 \cdot \cdots \cdot n$ per $n > 0$.

Provare per induzione il **Teorema binomiale**:
Sia n un qualunque intero ≥ 1, si ha:

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \ldots + \binom{n}{r}x^{n-r}y^r + \ldots + \binom{n}{n-1}xy^{n-1} + y^n$$

dove

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

Sara' utile nel seguito la seguente formulazione del Principio di Induzione:

Principio di induzione aritmetica (2): *Sia $n_0 \in \mathbb{Z}$ e sia $\mathcal{P}$ una affermazione sui numeri interi $n \geq n_0$. Supponiamo siano soddisfatte le seguenti due condizioni:*

i) *$\mathcal{P}$ è vera per il numero n_0;*

ii) *per ogni intero $n > n_0$ se $\mathcal{P}$ è vera per ogni intero m tale che $n_0 \leq m < n$, allora $\mathcal{P}$ è vera per il numero n.*

Allora $\mathcal{P}$ è vera per ogni numero intero $n \geq n_0$.

Si puo' provare che il Principio di induzione e' equivalente al Principio del buon ordinamento.

Principio del buon ordinamento: Sian n_0 un intero qualunque. Un qualunque insieme di interi $\geq n_0$ ha un elemento minimo.

4. **Relazioni di equivalenza**

Sia $\mathcal{R}$ una corrispondenza tra un insieme A e se stesso, scriveremo $x\mathcal{R}y$ invece di $(x, y) \in \mathcal{R}$.

Definizione 4.1.: una corrispondenza $\mathcal{R}$ si dice **relazione di equivalenza** se verifica le seguenti proprietà:

i) $\forall\ x \in A$ si ha $x\mathcal{R}x$ (**proprietà riflessiva**).
ii) $\forall\ x, y \in A$ tali che $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ (**proprietà simmetrica**)
iii) $\forall\ x, y, z \in A$ per cui $x\mathcal{R}y$ e $y\mathcal{R}z \Rightarrow x\mathcal{R}z$ (**proprietà transitiva**).

Una relazione di equivalenza si indica di solito con $\sim$ oppure $\equiv$.

Se $\sim$ è una relazione di equivalenza diremo che x è equivalente a y se $x \sim y$.

Esempi :

4.1) Sia A un insieme definiamo $x \sim y$ se $x = y$. Si ha una relazione di equivalenza detta eguaglianza.
4.2) Sia data in $\mathbb{N}$ la relazione $m \sim n$ se $m+n$ è pari, $\sim$ è una relazione di equivalenza.
4.3) Fissato un intero $n > 0$, sia data in $\mathbb{Z}$ la relazione $x \sim_n y$ se $x - y$ è un multiplo intero di n, si verifica che $\sim_n$ è una relazione di equivalenza.
4.4) *Relazione di equivalenza associata ad un'applicazione*:
sia $f : A \to B$ una applicazione, definiamo su A la seguente relazione:
$x \sim_f y$ se $f(x) = f(y)$. Si verifica facilmente che $\sim_f$ è una relazione di equivalenza che si dice relazione di equivalenza associata a f.

Sia ora $\sim$ una relazione di equivalenza in un insieme A. sia a un elemento di A, indichiamo con $\overline{a}$ l'insieme degli elementi di A equivalenti ad a:

$$\overline{a} = \{x \in A \mid x \sim a\}$$

$\overline{a}$ si dice **classe di equivalenza** di a modulo $\sim$ (in particolare $a \in \overline{a}$) [1]

Si osservi che $\overline{a}$ è anche la classe di equivalenza individuata da un qualsiasi elemento a' equivalente ad a; inoltre due distinte classi di equivalenza sono sempre disgiunte.

L'insieme di tutte le classi di equivalenza si dice **insieme quoziente** di A modulo $\sim$ e si indica con $A/\sim$.

Sia $\sim_n$ la relazione di equivalenza definita nell'esempio 4.3., si verifica che $\overline{x} = \overline{y}$ se il resto della divisione di x per n e' uguale al resto della divisione di y per n.

[1] la classe di equivalenza di a si indica anche $[a]$ oppure $\overline{\overline{a}}$.

L'insieme $\mathbb{Z}/\sim_n$ e'detto insieme delle classi di resto modulo n e denotato con $\mathbb{Z}_n$. In particolare

$$\mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}.$$

L'applicazione (surgettiva) $\pi : A \to A/\sim$ che associa ad ogni elemento di A la sua classe di equivalenza si dice **proiezione canonica**.

Osserviamo che l'insieme quoziente $A/\sim$ è una partizione di A [1], più precisamente la partizione di A nelle classi di equivalenza modulo $\sim$, cioè ad ogni equivalenza $\sim$ è associata, in modo naturale, la partizione $A/\sim$.
Viceversa, data una partizione $\mathcal{A}$ di A, si può associare ad $\mathcal{A}$ una equivalenza in A.

Sia $\mathcal{A} = \{A_i\}_{i\in I}$ una partizione di A. Associamo ad $\mathcal{A}$ la seguente relazione: $x \sim y \iff \exists\ j \in I$ tale che $x, y \in A_j$, questa è la relazione di equivalenza associata alla partizione $\mathcal{A}$.

[1] una famiglia $\mathcal{A}$ di sottoinsiemi non vuoti di A si dice partizione di A se i sottoinsiemi sono a due a due disgiunti e se la loro unione è tutto A

GLI INTERI

1. FATTORIALITA' IN Z

1.1. Algoritmo Euclideo

La proprietà fondamentale di $\mathbb{Z}$ che useremo per tutto il capitolo è il

Teorema di divisione. *Dati due interi* $a > 0$ *e* $b \geq 0$ *esistono due interi, unicamente determinati* $q \geq 0$ *e* $r, 0 \leq r < a$*, tali che* $b = qa + r$

Dim.: Per induzione.
Dato un divisore $a \neq 0$ dimostreremo che per ogni $b \geq 0$ esistono un *quoziente* q ed un *resto* r con $0 \leq r < a$ tali che $b = qa + r$.
Intanto $0 = a \cdot 0 + 0$, quindi, quando $b = 0$ possiamo porre $q = r = 0$.
Per $b > 0$ usiamo l'induzione.
Supponiamo che per ogni $c, 0 \leq c < b$ esistano q_o, r_o con $0 \leq r_o < a$ e $c = q_o a + r_o$.
Consideriamo ora b. Se $b < a$ allora $b = 0 \cdot a + b$ possiamo quindi porre $q = 0, r = b$.
Se $b \geq a$, sia $c = b - a$. Allora $0 \leq c < b$. Per induzione si ha $c = q_o a + r_o$ per opportuni q_o ed r_o con $0 \leq r_o < a$. Ma allora

$$b = a + c = a + aq_o + r_o = a(q_o + 1) + r_o$$

e $0 \leq r_o < a$. Basta allora porre $q = q_o + 1, r = r_o$.
Per induzione quindi ogni $b \geq 0$ può essere scritto come $b = qa + r$ con $0 \leq r < a$.
Per provare l'unicità supponiamo di avere q e r con $b = qa + r$ e $0 \leq r < a$, e supponiamo anche di avere $b = q'a + r'$ e $0 \leq r' < a$ con q' e r' eventualmente diversi da q e r.
Vogliamo provare che $r = r'$ e $q = q'$, per farlo supponiamo $r' \geq r$ e sottraiamo $b = aq' + r'$ da $b = aq + r$, otterremo $a(q - q') + (r - r') = 0$, ovvero $a(q - q') = r' - r$, poichè $r' - r \geq 0$ ed $a > 0$ si ha $q - q' \geq 0$. Ora $r' - r \leq r' < a$, quindi $a(q - q') < a$ pertanto $q - q' < 1$. Essendo $q - q'$ un numero intero necessariamente avremo $q - q' = 0$, cioè $q = q'$ da cui $r' - r = a(q - q') = 0$ ovvero $r = r'$.

Dati due interi a e b, diremo che a divide b se $b = aq$ per qualche intero q e scriveremo $a|b$ se a divide b.
Se a e b sono interi un divisore comune di a e b è un intero e che divide sia a che b.
Un numero d è il *massimo comun divisore* (MCD) di a e b se:

i) $d|a$ e $d|b$;

ii) se e è un divisore comune di a e b allora e divide d.

Infine a e b si dicono *coprimi* se il loro MCD è 1. Se non c'e' ambiguita' il massimo comun divisore di a e b si denota con (a, b).

La soluzione del problema di trovare il massimo comun divisore di due numeri è stata data da Euclide (300 a.c. circa).
Supponiamo di avere due numeri a e b con $b \leq a$. Se b divide a allora b è il massimo comun divisore di a e b. Se b non divide a, sottraendo continua- mente il minore dei due numeri dal maggiore resterà infine un numero che dividerà quello che lo precede, questo numero è il massimo comun divisore di a e b.

Esempio. Consideriamo i numeri 78 e 32.
Sottraiamo 32 da 78 otterremo 46 e 32, sottraendo 32 da 46 si ha 14 e 32, sottraiamo 14 da 32 e avremo 18 e 14, sottraendo 14 da 18 abbiamo 4 e 14, sottraiamo 4 da 14 otteniamo 10 e 4 sottraiamo 4 da 10, otteniamo 6 e 4, sottraiamo 4 da 6 e otteniamo 2 e 4, ora 2 divide 4 quindi 2 è il massimo comun divisore di 78 e 32.
Possiamo descrivare l'algoritmo in forma compatta usando il teorema di divisione:

$$78 = 32 \cdot 2 + 14$$

$$32 = 14 \cdot 2 + 4$$

$$14 = 4 \cdot 3 + 2$$

$$4 = 2 \cdot 2 + 0$$

E' facile vedere che 2 è il massimo comun divisore di 32 e 78 ma possia- mo motivare in questo modo: 2 divide 4, quindi divide $4 \cdot 3 + 2 = 14$, quindi $14 \cdot 2 + 4 = 32$, quindi $32 \cdot 2 + 14 = 78$. Perciò 2 è divisore comune di 32 e 78. Inoltre, se d è divisore comune di 32 e 78 allora d divide 14 (per la prima equazione), quindi 14 e 32, quindi 4 (dalla seconda equazione), quindi 4 e 14, quindi 2 (dalla terza equazione). Quindi d divide 2.

Possiamo ora enunciare il seguente **Algoritmo di Euclide.**

Dati due numeri naturali a e b il loro massimo comun divisore si determina per divisioni successive come segue:

$$a = bq + r_o \text{ (dividendo } a \text{ per } b)$$
$$b = r_o q_o + r_1 \text{ (dividendo } b \text{ per } r_o)$$
$$r_o = r_1 q_1 + r_2 \text{ (dividendo } r_o \text{ per } r_1)$$
$$r_1 = r_2 q_2 + r_3$$
$$\dots$$
$$\dots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_n + 0$$

Si ha che r_n è il massimo comun divisore di a e b.

1.2. Il massimo comun divisore.

Abbiamo osservato che l'ultimo resto diverso da 0 nell'algoritmo euclideo applicato ad a e b ne è il massimo comun divisore. Quindi trovare il massimo comun divisore è un processo computazionale effettivo. L'algoritmo euclideo ha inoltre la seguente conseguenza:
Identità di Bezout. *Se d è il massimo comun divisore di a e b, allora $d = ax + by$ per opportuni interi x e y.*

Vediamo per esempio come si procede per determinare x e y nel caso in cui a e b siano 365 e 1876.

E' facile scoprire che $d = 1$ cioè che i due numeri sono coprimi * .

Usiamo l'algoritmo euclideo:
$$1876 = 365 \cdot 5 + 51$$
$$365 = 51 \cdot 7 + 8$$
$$51 = 8 \cdot 6 + 3$$
$$8 = 3 \cdot 2 + 2$$
$$3 = 2 \cdot 1 + 1$$

quindi 1 è il massimo comun divisore.

Ricaviamo i resti dalle equazioni precedenti (cioè rileggiamo da destra verso sinistra le equazioni) e avremo:

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

* $365 = 5 \cdot 73$ e nè 5 nè 73 dividono 1876

$$2 = 8 - 3 \cdot 2$$
$$3 = 51 - 8 \cdot 6$$
$$8 = 365 - 51 \cdot 7$$
$$51 = 1876 - 365 \cdot 5$$

e sostituiamo successivamente i resti nell'equazione $1 = 3 - 2 \cdot 1$ partendo da 2 avremo:

$$1 = 3 - 2 \cdot 1$$
$$1 = 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8$$
$$1 = 3(51 - 8 \cdot 6) - 8 = 3 \cdot 51 - 8 \cdot 19$$
$$1 = 3(51 - 19(365 - 51 \cdot 7) = 136 \cdot 51 - 19 \cdot 365$$
$$1 = 136(1876 - 5 \cdot 365) - 19 \cdot 365 = 136 \cdot 1876 - 699 \cdot 365$$

Quindi $x = -699$, $y = 136$.

Possiamo ora dimostrare il seguente :

Teorema. *Se r_n è l'ultimo resto non nullo dell'algoritmo euclideo per a e b, allora r_n è il massimo comun divisore di a e b, e $r_n = ax + by$ per opportuni x e y .*

Dim.: Se r_n è l'ultimo resto non nullo dell'algoritmo euclideo per a e b, allora l'algoritmo comporta $n + 1$ passi. Dimostriamo il teorema per induzione su n.
Se $n = 0$ allora a divide b e il teorema è banale. Se $n = 1$ allora l'algoritmo ha la forma

$$b = aq_1 + r_1$$
$$a = r_1 q_2 + 0$$

In tal caso si vede che r_1 è il massimo comun divisore di a e b; inoltre $r_1 = b \cdot 1 + a \cdot (-q_1)$ quindi l'identità di Bezout è verificata.

Supponiamo il teorema vero per $n - 1$ *. Supponiamo che l'algoritmo euclideo richeda $n + 1$ passi per la coppia (a, b). Sia $b = aq_1 + r_1$ la divisione di b per a che è il primo passo dell'algoritmo di Euclide, allora il resto dell'algoritmo per (a, b) coincide con l'algoritmo di Euclide per (r_1, a). Per induzione r_n è il massimo comun divisore di a e r_1 e quindi $r_n = au + r_1 v$ per opportuni interi u e v.

Ora essendo $b = aq_1 + r_1$ r_n è il massimo comun divisore anche di b e a

* Cioè il teorema è vero per ogni coppia di numeri per cui l'algoritmo di Euclide richiede n passi

e sostituendo $b - aq_1$ al posto di r_1 nell'uguaglianza $r_n = au + r_1 v$ si ottiene $r_n = a(u - vq_1) + bv$ e questo prova il teorema.

1.3. Fattorizzazione unica.

Un numero naturale $p > 1$ è **primo** se l'unico divisore di p maggiore di 1 è p stesso ed ogni numero naturale è primo o prodotto di primi.

Vogliamo provare il *teorema fondamentale dell'aritmetica* ossia che la fattorizzazione di un numero naturale come prodotto di primi è "essenzialmente" unica .

Sia $a \in \mathbb{N}$, se $a = p_1 \dots p_n = q_1 \dots q_m$ sono fattorizzazioni di a come prodotto di primi, diciamo che le due fattorizzazioni sono uguali se l'insieme dei p_i coincide con l'insieme dei q_j (ripetizioni comprese), cioè $m = n$ ed ogni primo compare lo stesso numero di volte tra i p_i e i q_j.**

Teorema. *Ogni numero naturale ≥ 2 si fattorizza in modo unico come prodotto di primi*

Dim.: Per induzione: supponiamo che il risultato sia vero per ogni numero minore di a. Supponiamo che $a = p_1 \dots p_n = q_1 \dots q_m$ siano due fattorizzazioni in primi di a e proviamo che esse coincidono (a meno dell'ordine). Supponiamo che esista un opportuno indice j tale che $p_1 = q_j$. Allora di- videndo a per p_1 avremo che il numero $b = p_2 \dots p_n = q_1 \dots q_{j-1} q_{j+1} \dots q_m$ è minore di a e quindi, per l'ipotesi induttiva ammette un'unica fattorizzazione, ovvero $p_2, \dots, p_n$ coincide con $q_1, \dots, q_{j-1}, q_{j+1}, \dots, q_m$ e quindi, essendo $p_1 = q_j$ il teorema è provato, se dimostriamo che esiste quell'indice j per cui $p_1 = q_j$. Tale fatto si deduce dal seguente:

Lemma. *Se p è un numero primo e p divide ab allora p divide a oppure p divide b.*

Dim.: Sia d il massimo comun divisore di p e a se $d > 1$ allora $d = p$ essendo p primo. In questo caso $p|a$. se $d = 1$ per l'identità di Bezout possiamo scrivere $1 = ax + py$ per opportuni interi x e y.
Quindi $b = bax + bpy$, ma p divide per ipotesi ab e ovviamente bpy e quindi divide $b = abx + bpy$.

Per completare la dimostrazione del teorema basta allora dire che siccome il

** $2 \cdot 2 \cdot 3 \cdot 5$ è la stessa fattorizzazione di $2 \cdot 5 \cdot 3 \cdot 2$

numero primo p_1 divide $q_1 \dots q_m$ deve dividere uno dei fattori q per esempio q_j, ma, essendo q_j primo esso è divisibile solo per se stesso e per uno, ma $p_1 \neq 1$, allora $p_1 = q_j$.

Osservazione Se p e' primo, allora p divide $\binom{p}{r}$ per ogni r, $0 < r < p$.

Infatti $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ e $r!(p-r)!$ divide $p!$ essendo $\binom{p}{r}$ e' un intero. Siccome $MCD(p, r!(p-r)!) = 1$, segue che per $1 \leq r \leq p-1$, abbiamo che $r!(p-r)!$ divide $(p-1)!$ e quindi

$$\binom{p}{r} = p\frac{(p-1)!}{r!(p-r)!}$$

e' un multiplo intero di p.

3. CONGRUENZE

Proposizione Siano $a, b, c \in \mathbb{Z}$. L'equazione

$$ax + by = c$$

ha soluzioni intere se e solo se c e' un multiplo di $MCD(a, b)$.

Dim.: Se $d = MCD(a, b)$, chiaramente d divide a e divide b, quindi se $ax + by = c$ per qualche $x, y \in \mathbb{Z}$, d divde c. Viceversa se $c = kd$ per qualche $k \in \mathbb{Z}$, per l'identita' di Bezout esistono α e $\beta \in \mathbb{Z}$, tali che

$$c = kd = k(a\alpha + b\beta).$$

Quindi $x = k\alpha$ e $y = k\beta$ e' soluzione intera dell'equazione.

Osservazione Nella proposizione precedente osserviamo che se c e' un multiplo di $d = MCD(a, b)$ (sia $c = kd$), sono soluzioni intere dell'equazione $ax + by = c$ tutte le coppie

$$x = k\alpha + bh \qquad y = k\beta - ah \ \ \forall\ h \in \mathbb{Z}.$$

Possiamo definire in $\mathbb{Z}_n$ la somma e il prodotto di due classi rispettivamente come la classe della somma e del prodotto e vedremo nel seguito del corso che tali operazioni defiscono su tale insieme una ben definita struttura algebrica. Quindi per ogni $a, b \in \mathbb{Z}$, $+$ e $\cdot$ cosi' definite:

$$\overline{a} + \overline{b} = \overline{a + b}$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

sono operazioni binarie in $\mathbb{Z}_n$ in quanto definiscono delle applicazioni da $\mathbb{Z}_n \times \mathbb{Z}_n$ in $\mathbb{Z}_n$.

Ovviamente si ha $\overline{a} = \overline{b}$ se e solo se $a \equiv b \ (\mathrm{mod} n)$. In particolare $\overline{a} = \overline{0}$ se e solo se n divide a. L'elemento neutro rispetto alla somma e' $\overline{0}$ e l'elemento neutro rispetto al prodotto e' $\overline{1}$.
Diremo che $\overline{a}$ e' invertibile in $\mathbb{Z}_n$ se esiste $b \in \mathbb{Z}$ tale $\overline{a} \cdot \overline{b} = \overline{1}$.

Teorema *$\overline{a}$ é un elemento invertibile in $\mathbb{Z}_n$ se e solo se $MCD(a, n) = 1$*

Dim.: Se $\overline{a}$ é invertibile allora esiste $b \in \mathbb{Z}$ tale che $\overline{a} \cdot \overline{b} = \overline{1}$, quindi in $\mathbb{Z}$ esiste k tale che $a \cdot b = kn + 1$ e di conseguenza per la proposizione precedente $1 = MCD(a, n)$. Viceversa se $MCD(a, n) = 1$ per l'identitá di Bezout esistono b e k tali che $ab + kn = 1$ e quindi, passando in $\mathbb{Z}_n$ si ha la tesi.

Vediamo alcune proprietá di $\mathbb{Z}_p$ quando p é un numero primo

Teorema di Fermat: *Sia p un numero primo e sia a un intero non divisibile per p, alllora*

$$a^{p-1} \equiv 1 \pmod{p}$$

(da provare quindi che in $\mathbb{Z}$ esiste un intero k tale che $a^{p-1} = 1 + kp$)

Prima dimostrazione del teorema di Fermat:

Indichiamo con $\mathbb{Z}_p^*$ l'insieme $\mathbb{Z}_p - \{\overline{0}\}$ e sia $V = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$.
Si verifica facilmente che due insiemi coincidono, quindi, se si moltiplicano tra loro tutti gli elementi di $\mathbb{Z}_p^*$ e tutti gli elementi di V si ottiene lo stesso risultato, ovvero

$$\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{(p-1)} = \overline{a} \cdot \overline{2a} \cdot \ldots \overline{(p-1)a}$$

Ma il primo membro dell'uguaglianza é $\overline{(p-1)!}$ l'altro vale $\overline{a^{p-1}(p-1)!}$.
Ritornando negli interi ció significa che $(p-1)! - a^{p-1}(p-1)! = kp$ ovvero $(p-1)![1 - a^{p-1}] = tp$ per un opportuno $t \in \mathbb{Z}$. Quindi essendo primo p divide uno dei fattori e siccome $(p-1)!$ non é divisibile per p, necessariamente p divide $[1 - a^{p-1}]$ cioé esiste un intero k tale che $a^{p-1} - 1 = kp$ da cui la tesi.

Seconda dimostrazione del teorema di Fermat:

In $\mathbb{Z}_p$ dobbiamo provare che se $\overline{a} \neq \overline{0}$, allora $\overline{a^{p-1}} = \overline{1}$. Poiche' $\overline{a^{p-1}} = (\overline{a})^{p-1}$, possiamo supporre $a > 0$ cambiando eventualmente il rappresentante di $\overline{a}$. Essendo inoltre per la proposizione precedente $\overline{a}$ invertibile, e' sufficiente provare

$$\overline{a^p} = \overline{a}.$$

Proviamo ora il risultato per induzione su a. Se $a = 1$ l'eguaglianza e' banalmente verificata. Supponiamo che $\overline{a^p} = \overline{a}$ e proviamo che $\overline{a+1}^p = \overline{1}$. Come abbiamo gia' visto $(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}$ e, essendo p primo, $\binom{p}{i}$ per $0 < i < p-1$ un multiplo di p. Segue $(a+1)^p \equiv a^p + 1 \pmod{p}$ e $a^p + 1 \equiv a + 1 \pmod{p}$ per ipotesi induttiva.■

Teorema Cinese del Resto: *Siano $m_1, m_2, \ldots, m_n$ numeri naturali > 1 a due a due primi tra loro e siano $a_1, a_2, \ldots, a_n$ numeri interi qualsiasi, allora ha soluzione il sistema di congruenze*
$x \equiv a_1 \ (mod\ m_1)$
$x \equiv a_2 \ (mod\ m_2)$
.
.
.
$x \equiv a_n \ (mod\ m_n)$
Inoltre se x e x' sono due soluzioni del sistema si ha che $x \equiv x' \ (mod\ M)$ dove $M = m_1 m_2 \ldots m_n$

Dim. (1) : La prima congruenza é risolta da qualunque x del tipo $x = a_1 + m_1 u_1$, per risolvere anche la seconda occorre che $x = a_1 + m_1 u_1 = a_2 + m_2 t_2$ e, risolvendo con Bezout [1] si determinano u_1 e t_2, chiamiamo $x_2 = a_1 + m_1 u_1 = a_2 + m_2 t_2$. Quindi $x = x_2$ risolve le prime due congruenze.
La soluzione generica del sistema formato dalle prime due congruenze é allora

$$x = x_2 + (m_1 m_2) u_2$$

dove u_2 é arbitrario [2]. Se x deve soddisfare anche $x \equiv a_3 \pmod{m_3}$, allora deve essere $x = x_2 + (m_1 m_2) u_2 = a_3 + m_3 t_3$ e, sempre con Bezout, possiamo determinare u_2 e t_3, quindi posto $x_3 = x_2 + (m_1 m_2) u_2 = a_3 + m_3 t_3$, la soluzione generale delle prime tre congruenze é $x = x_3 + (m_1 m_2 m_3) u_3$ con u_3 arbitrario [3], procedendo in modo analogo si giunge alla soluzione del sistema.

[1] essendo $MCD(m_1, m_2) = 1$ esistono α, β tali che $a_1 - a_2 = \alpha m_1 + \beta m_2$, basta scegliere $u_1 = -\alpha, t_2 = \beta$

[2] in realtá é sufficiente il minimo comune multiplo m di m_1, m_2, quindi la soluzione piú generale possibile é $x = x_2 + m u_2$

[3] anche qui basterebbe considerare il minimo comune multiplo tra m_1, m_2, m_3

Esempio

Risolviamo

$$\begin{cases} x \equiv 3 \text{mod} 11 \\ x \equiv 6 \text{mod} 8 \\ x \equiv 12 \text{mod} 15 \end{cases}$$

La prima congruenza dá $x = 3 + 11u_1$ la seconda impone che siano uguali $3 + 11u_1$ e $6 + 8t_2$ da cui si ottiene con Bezout $u_1 = 1, t_2 = 1$. La soluzione generale é allora $x = 14 + 88u_2$.
La terza congruenza impone che $14 + 88u_2 = 12 + 15t_3$ da cui $u_2 = 1, t_3 = 6$, pertanto la soluzione generale del sistema é

$$x = 102 + 1320u_3 \ \forall u_3 \in \mathbb{Z}$$

Presentiamo un'altra dimostrazione del Teorema:

Dim. (2). Cominciamo a considerare dei casi particolari. Fissato i, sia

$$a_i = 1 \ \ e \ \ a_1 = \ldots = a_{i-1} = a_{i+1} = \ldots = a_n = 0.$$

Sia $k_i = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$. Essendo m_i e m_j coprimi se $i \neq j$, k_i e m_i sono coprimi e quindi possiamo trovare interi r e s tali che $rk_i + sm_i = 1$, in particolare $rk_i \equiv 1 \ \text{mod}(m_i)$. Siccome $m_1, m_2, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n$ dividono k_i, allora $x_i \equiv 0 \ \text{mod}(m_j)$ con $j \neq i$, quindi $x_i = rk_i$ e' soluzione del sistema particolare.
Per ogni i, $0 \leq i \leq n$, troviamo un tale x_i. Proviamo che

$$x = a_1x_1 + \ldots a_nx_n$$

e' una soluzione del nostro sistema iniziale. Poiche' $x_j \equiv 0 \ \text{mod}(m_i)$, osserviamo che $x \equiv a_ix_i \ \text{mod}(m_i)$ e come avevamo gia' visto $a_ix_i \equiv a_i \ \text{mod}(m_i)$ essendo $x_i \equiv 1 \ \text{mod}(m_i)$, dunque $x \equiv a_ix_i \equiv a_i \ \text{mod}(m_i)$.
Per l'unicita' supponiamo che anche $x' \equiv a_i \ \text{mod}(m_i)$ per ogni i. Allora $x - x' \equiv 0 \ \text{mod}(m_i)$ per ogni i, quindi $x - x'$ e' multiplo di m_i per ogni i, in particolare e' multiplo del minimo comune multiplo di tutti gli m_i. Essendo gli m_i a due a due coprimi, il minimo comune multiplo di tutti gli m_i e' il prodotto, ossia M.

Sia ora m un intero > 1 e sia G l'insieme degli elementi invertibili in $\mathbb{Z}_m$, ossia l'insieme degli elementi $\overline{a}$ con $(a, m) = 1$ e $a < m$.
Indichiamo con $\varphi(m)$ il numero degli elementi di G.

Teorema di Eulero: *Sia m un intero > 1 e sia a un intero non divisibile per m. Se $(a, m) = 1$, allora*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Chiaramente se m e' un numero primo, allora $\varphi(m) = m - 1$ e si ritrova il teorema di Fermat.

NUMERI COMPLESSI

1. Rappresentazione dei numeri complessi

Consideriamo l'insieme $\mathbb{R} \times \mathbb{R}$ delle coppie ordinate di numeri reali e definiamo in tale insieme le seguenti operazioni binarie.

Dati due elementi in $\mathbb{R} \times \mathbb{R}$, $z = (a, b),\ z' = (c, d)$ definiamo le operazioni di somma e prodotto nel modo seguente:

$z + z' = (a + c, b + d)$

$z \cdot z' = (ac - bd, ad + bc)$

E' facile verificare che la somma e il prodotto così definite sono operazioni associative e commutative, che la coppia $(0, 0)$ è l'elemento neutro rispetto alla somma (cioè $\forall\ z \in \mathbb{R} \times \mathbb{R} \quad z + (0, 0) = (a, b)$) e che ogni elemento di $\mathbb{R} \times \mathbb{R}$ ammette opposto (cioè $(a, b) + (-a, -b) = (0, 0)$). Si ha inoltre che la coppia $(1, 0)$ è l'elemento neutro rispetto al prodotto (cioè $\forall\ z \in \mathbb{R} \times \mathbb{R}$ si ha $z \cdot (1, 0) = z$). Infine

$$\forall\ z = (a, b) \neq (0, 0) \qquad (a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = (1, 0)$$

(cioè $z \neq 0$ ammette inverso moltiplicativo)

Identificheremo un elemento del tipo $(a, 0)$ con il numero reale a, inoltre indichiamo con i l'elemento $(0, 1)$. E' facile vedere che $(0, 1) \cdot (0, 1) = (-1, 0) = -1$, cioè $i^2 = -1$, potremo allora usare la notazione $z = a + ib$ invece di $z = (a, b)$.

Per definizione, poniamo $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, chiamando **numeri complessi** gli elementi di $\mathbb{C}$ con le operazioni sopra definite. Possiamo allora riformulare le operazioni di somma e prodotto con questa nuova notazione[1]:
Dati due numeri complessi $z = a + ib,\ z' = c + id$ si ha:

$z + z' = (a + c) + i(b + d)$

$z \cdot z' = (ac - bd) + i(ad + bc)$

Inoltre se i due numeri reali a e b non sono entrambi nulli, l'inverso moltiplicativo di $z = a + ib$ è

$$\frac{1}{z} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}$$

Definizione : Se $z = a + ib$, a si dice **parte reale** di z e b si dice **parte immaginaria** di z e si indicano rispettivamente con $\mathcal{R}e\ z = a \quad \Im m\ z = b$

[1] questa notazione ha il vantaggio di permettere di operare secondo le note regole del calcolo letterale, tenendo ovviamente conto che $i^2 = -1,\ i^3 = -i,\ i^4 = 1$ ecc.

Definizione : Dato il numero complesso $z = a + ib$ si dice **complesso coniugato** di z e si indica con $\overline{z}$ il numero $\overline{z} = a - ib$

Esercizio: Provare che se $z = a + ib$ allora $z + \overline{z} = 2\mathcal{R}ez$, $z - \overline{z} = 2i\Im m\ z$, $z \cdot \overline{z} = (\mathcal{R}e\ z)^2 + (\Im m\ z)^2$

2. Forma trigonometrica di un numero complesso

Per come abbiamo definito inizialmente $\mathbb{C}$ vi è una corrispondenza biunivoca tra i punti del piano cartesiano $I\!R^2$ e i numeri complessi associando a ciascun numero $z = a + ib$ il punto P di coordinate (a, b) del piano.

La distanza ρ di P dall'origine (che è $\sqrt{a^2 + b^2}$) si dice **modulo** di z e si indica con $|z|$ l'angolo θ formato dal segmento OP con il semiasse positivo delle ascisse, si dice **argomento** di z ([2])

Si prova subito che $a = \rho\cos\theta, \quad b = \rho\sin\theta$ cioè $z = \rho(\cos\theta + i\sin\theta)$ con $\rho \geq 0$ e θ numeri reali[3]

La scrittura $z = \rho(\cos\theta + i\sin\theta)$ si dice **forma trigonometrica** di z.

Si prova facilmente il seguente:

Teorema : *Il prodotto di due numeri complessi ha per modulo il prodotto dei loro moduli e per argomento la somma degli argomenti*

3. Radici n-esime di un numero complesso

Teorema 3.1. : *Dato un numero intero positivo n ed un numero complesso arbitrario α, l'equazione $z^n = \alpha$ ammette n soluzioni distinte se $\alpha \neq 0$, e ammette l'unica soluzione $z = 0$ se $\alpha = 0$.*
Dim.: Il caso $\alpha = 0$ è ovvio. Se $\alpha \neq 0$ scriviamo α e z in forma trigonometrica:

$$\alpha = |\alpha|(\cos\varphi + i\sin\varphi);$$
$$z = |z|(\cos\theta + i\sin\theta).$$

Dal teorema precedente risulta

$$\alpha = |z|^n(\cos n\theta + i\sin n\theta).$$

[2] l'angolo θ si intende sempre misurato in radianti!
[3] l'argomento di $z = 0$ non è definito mentre se $z \neq 0$ l'argomento è determinato a meno di multipli interi di 2π.

quindi l'equazione $z^n = \alpha$ equivale al sistema:

$$\begin{cases} |\alpha| = |z|^n \\ n\theta \equiv \varphi (mod 2\pi) \end{cases}$$

che ha come soluzioni gli n numeri complessi distinti $z_0, z_1, \dots z_{n-1}$ aventi tutti come modulo la radice n-esima (aritmetica) $\sqrt[n]{|\alpha|}$ e come argomenti rispettivamente: $\theta_0 = \dfrac{\varphi}{n},\ \theta_1 = \dfrac{\varphi + 2\pi}{n}, \dots,\ \theta_{n-1} = \dfrac{\varphi + 2(n-1)\pi}{n}$.
Nella rappresentazione geometrica sul piano cartesiano le soluzioni sono quindi disposte sui vertici di un poligono regolare di n lati iscritto in una circonferenza di centro l'origine e raggio $\sqrt[n]{|\alpha|}$.

Corollario 3.2. : *Dato un numero intero positivo n le radici n-esime dell'unità (cioè le n soluzioni dell'equazione $z^n = 1$) sono tutti e soli i numeri*

$$z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1 \dots, n-1$$

Le radici n-esime dell'unità sono quindi disposte sui vertici di un poligono regolare di n lati iscritto in una circonferenza di centro l'origine e raggio 1 e avente uno dei suoi vertici nel punto $(1, 0)$ che corrisponde a $z = 1$

Teorema 3.3. : *Ogni equazione algebrica di secondo grado (a coefficienti in $\mathbb{C}$) ammette sempre soluzioni in $\mathbb{C}$*
Dim.: Consideriamo l'equazione di 2° grado $az^2 + bz + c = 0$ dove
$a, b, c \in \mathbb{C},\ a \neq 0$.
Questa equazione è equivalente all'equazione $(2az + b)^2 = \Delta$ ponendo
$\Delta = b^2 - 4ac$ le soluzioni di questa seconda equazioni saranno quindi le radici quadrate (in senso complesso) di Δ. Per il Teorema 3.1. ci saranno allora due numeri complessi δ_1 e δ_2 (distinti se $\Delta \neq 0$, entrambi nulli se $\Delta = 0$). In definitiva quindi le soluzioni saranno:

$$z_1 = \frac{-b + \delta_1}{2a} \quad z_2 = \frac{-b + \delta_2}{2a} \blacksquare$$

Si può inoltre dimostrare il seguente:

Teorema 3.4. (Teorema fondamentale dell'algebra): *Ogni equazione algebrica di grado n a coefficienti in $\mathbb{C}$ ammette sempre n soluzioni in $\mathbb{C}$ (contate con la loro molteplicità).*

POLINOMI IN UNA INDETERMINATA

Sia $K = \mathbb{Q}$ oppure $\mathbb{R}$ oppure $\mathbb{C}$ oppure $\mathbb{Z}_p$. Specificheremo diversamente quando ne sara' il caso. Ricordiamo che in tali insiemi numerici ogni elemento diverso da zero ha inverso moltiplicativo, in particolare se a e b sono elementi di K e $a \neq 0$, allora $ab = 0$ implica $b = 0$.

Sia $X \notin K$, indichiamo con $K[X]$ l'insieme dei "polinomi a coefficienti in K nell'indeterminata X" cioè gli elementi del tipo

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \text{ con } a_i \in K, i = 0, \ldots, n.$$

Per brevita' di notazione a volte scriveremo f invece di $f(X)$. Si definiscono facilmente in $K[X]$ le operazioni di somma e prodotto (estendendo in modo "ovvio" le operazioni definite su K). Se

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

e

$$g(X) = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m$$

supponendo $a_i = 0$ per $i > n$ e $b_j = 0$ per $j > m$, si ha

$$f(X) + g(X) = (a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_i + b_i)X^i + \ldots$$

$$f(X) \cdot g(X) = (a_0b_0) + (a_0b_1 + a_1b_0)X + \ldots + (\sum_{r+s=i} a_rb_s)X^i + \ldots + a_nb_mX^{m+n}$$

Se $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ con $a_n \neq 0$ si dice che n è il **grado** di f e lo si indica con ∂f [1] ; f si dice **monico** se $a_n = 1$, inltre a_n si dice **coefficiente direttivo** di f.

Si prova facilmente che se f e g sono polinomi non nulli, si ha:

$$\partial(f + g) \leq max(\partial f, \partial g) \text{ oppure } f + g = 0$$

$$\partial(fg) = \partial f + \partial g \ .$$

1. Divisione Euclidea in $K[X]$.

Teorema. (teorema di divisibilità dei polinomi):
Siano $f(X)$ e $g(X)$ polinomi di $K[X]$ con $f(X) \neq 0$. Allora esistono due polinomi $q(X)$ e $r(X)$ tali che

[1] gli elementi non nulli di K (polinomi costanti) hanno grado zero, il polinomio nullo, cioè lo zero di K, non ha grado.

$$g(X) = q(X)f(X) + r(X) \text{ } con \text{ } \partial r(X) < \partial f(X) \text{ } oppure \text{ } r(X) = 0.$$

Inoltre $q(X)$ e $r(X)$ sono univocamente determinati e si dicono rispettivamente **quoziente** *e* **resto** *della divisione di $g(X)$ per $f(X)$.*

Dim. Procediamo per induzione sul grado di $g(X)$.
Se $\partial g < \partial f$ basta prendere $q(X) = 0$ e $r(X) = g(X)$. Supponiamo invece $\partial g = m \geq \partial f = n$ e supponiamo il teorema vero per i polinomi di grado $\leq m-1$. Sia b il coefficiente direttivo di $g(X)$ e a il coefficiente direttivo di $f(X)$. Allora il grado del polinomio $h(X) = g(X) - a^{-1}bX^{m-n}f(X)$ è $\leq m-1$, per l'ipotesi induttiva esistono $q_1(X)$ e $r_1(X)$ tali che
$h(X) = q_1(X)f(X) + r_1(X)$ con $\partial r_1(X) < n$ oppure $r_1(X) = 0$. E' allora sufficiente prendere $q(X) = a^{-1}bX^{m-n} + q_1(X)$ e $r(X) = r_1(X)$.

Proviamo ora l'unicità della decomposizione: supponiamo che
$g(X) = q'(X)f(X) + r'(X)$ con $\partial r' < n$ oppure $r' = 0$. Avremo che
$r' - r = (q - q')f$, ma se $(q - q') \neq 0$ si ha $\partial(q - q')f \geq n$ ma ciò contraddice sia $\partial(r - r') < n$ sia $r - r' = 0$, quindi necessariamente $q - q' = 0 = r - r'$.■

Osservazione. Dalla dimostrazione del teorema di divisione osserviamo che possiamo effettuare la divisione tra due polinomi non solo in $K[X]$, ma anche in $\mathbb{Z}[X]$ o $\mathbb{Z}_n[X]$ se il coefficiente direttivo di $f(X)$ e' invertibile.

Ad esempio in $\mathbb{Z}[X]$ non e' possibile dividere X^2+1 per $2X$, ma e' possibile dividere $X^2 + 1$ per $X + 1$.

Definizione. Diremo che un polinomio $f(X)$ in $K[X]$ è **divisibile** per un polinomio $g(X)$ se esiste un polinomio $h(X) \in K[X]$ tale che $f(X) = g(X)h(X)$.

Esercizio. In $\mathbb{Z}_5[X]$ provare che $X^5 + 1$ e' divisibile per $(X + 1)^2$.

Teorema. *Sia α un elemento di K e $f(X) \in K[X]$. Si ha che $f(\alpha) = 0$ se e solo se $f(X)$ è divisibile per $X - \alpha$.* [1]

Dim. Dal teorema di divisibilitá si ha che $f(X) = q(X)(X - \alpha) + r$ con r di grado zero oppure $r = 0$ (in ogni caso $r \in K$) quindi $f(\alpha) = r = 0$ da cui la tesi.■

Osservazione Il teorema precedente si applica anche a $\mathbb{Z}[X]$ e a $\mathbb{Z}_n[X]$. Come gia' osservato si puo' dividere per $(X - \alpha)$ essendo il coefficiente direttivo e' invertibile.

[1] Se $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ definiamo $f(\alpha) = a_0 + a_1\alpha + +a_2\alpha^2 + \ldots + a_n\alpha^n$.

Si puo' provare per induzione sul grado di $f(X)$:

Corollario. *Siano $a_1, \ldots, a_n$ elementi di K radici distinte di un polinomio non nullo $f(X)$ allora il prodotto*

$$(X - a_1)(X - a_2)\ldots(X - a_n) \text{ divide } f(X) \text{ e quindi } \partial f \geq n.$$

Corollario. *Sia $f(X)$ un polinomio non nullo di grado n. Allora $f(X)$ può avere, al più , n radici distinte.*

Attenzione che nei precedenti corollari e' necessaria l'ipotesi $f(X)$ in $K[X]$. Infatti ad esempio in $\mathbb{Z}_{15}[X]$ si ha che $1, 4, 11, 14$ sono radici distinte del polinomio $X^2 - 1$.

Teorema. (Principio di identità dei polinomi).
Sia K infinito e siano $f(X)$ e $g(X)$ due polinomi di $K[X]$ tali che $f(a) = g(a)$ per ogni $a \in K$. Allora i polinomi $f(X)$ e $g(X)$ coincidono.

Dim. Se $f(X) \neq g(X)$ il polinomio $h(X) = f(X) - g(X)$ non è il polinomio nullo, quindi, per il corollario 2 può avere solo un numero finito di radici distinte contro l'ipotesi che $h(a) = f(a) - g(a)$ sia zero per ogni a di K.■

Definizione. Dati due polinomi $f(X)$ e $g(X)$ un divisore comune di $f(X)$ e $g(X)$ è un polinomio $h(X)$ che li divide entrambi. Un polinomio $k(X)$ è un *massimo comun divisore* (MCD) di $f(X)$ e $g(X)$ se:
i) $k(X)$ é un divisore comune di $f(X)$ e $g(X)$;
ii) se $h(X)$ é un divisore comune di $f(X)$ e $g(X)$ allora $h(X)$ divide $k(X)$.

Il massimo comun divisore di due polinomi é determinato a meno di un coefficiente costante [1]

Il massimo comun divisore tra due polinomi $f(X)$ e $g(X)$ si determina mediante l'**Algoritmo di Euclide.** cioé per divisioni successive come segue:

$$\begin{gathered}
g(X) = f(X)q(X) + r_o(X) \text{ con } \partial r_o < \partial f \text{ (dividendo } g \text{ per } f) \\
f(X) = r_o(X)q_o(X) + r_1(X) \text{ con } \partial r_1 < \partial r_o \text{ (dividendo } g \text{ per } r_o) \\
r_o(X) = r_1(X)q_1(X) + r_2(X) \text{ con } \partial r_2 < \partial r_1 \text{ (dividendo } r_o \text{ per } r_1) \\
r_1(X) = r_2(X)q_2(X) + r_3(X) \text{ con } \partial r_3 < \partial r_2 \\
\ldots \\
\ldots \\
r_{n-2}(X) = r_{n-1}(X)q_{n-1}(X) + r_n(X) \text{ con } \partial r_n < \partial r_{n-1}
\end{gathered}$$

[1] cioé se $k_1(X)$ e $k_2(X)$ sono due massimi comun divisori di $f(X)$ e $g(X)$ esiste un $a \neq 0, a \in K$ tale che $k_1(X) = ak_2(X)$

$$r_{n-1}(X) = r_n(X)q_n(X)$$

Si ha che $r_n(X)$ è il massimo comun divisore di f e g, cioé il massimo comun divisore è l'ultimo resto non nullo delle divisioni successive

Anche per i polinomi vale la
Identità di Bezout. *Se $h(X)$ è un massimo comun divisore di $f(X)$ e $g(X)$, allora $h(X) = p(X)f(X) + q(X)g(X)$ per opportuni polinomi $p(X)$ e $q(X) \in K[X]$.*

Definizione 3.: Un polinomio $f(X) \in K[X]$ non costante si dice **irriducibile** se per ogni decomposizione di $f(X)$ nel prodotto di polinomi uno dei due fattori è invertibile (cioé é una costante non nulla).

I polinomi $f(X)$ e $g(X)$ in $K[X]$ si dicono associati se esiste una costante non nulla $c \in K$ tale che $f(X) = cg(X)$.

Si verifica facilmente che in $K[X]$
1) ogni polinomio $f(X)$ non costante si decompone nel prodotto di un numero finito di fattori irriducibili $f(X) = p_1(X)p_2(X)\dots p_n(X)$;
2) la decomposizione precedente è "essenzialmente" unica nel senso che se $f(X) = q_1(X)q_2(X)\dots q_m(X)$ è un altra decomposizione di $f(X)$ in fattori irriducibili si ha $m = n$ e si possono riordinare i fattori $q_i(X)$ in modo tale che ogni $q_i(X)$ sia associato al corrispondente $p_i(X)$ $(1 \leq i \leq n)$.

Osservazione.
1) In $\mathbb{C}[X]$ i polinomi irriducibili sono tutti e soli i polinomi di primo grado (per il teorema fondamentale dell'algebra).
2) In $\mathbb{Q}[X]$ ci possono essere polinomi irriducibili di grado arbitrario (p.es. $X^n + 2$ é sempre irriducibile in $\mathbb{Q}[X]$).
3) Se $f(X) \in K[X]$ e' un polinomio di grado ≥ 2 che ha almeno una radice in K, allora $f(X)$ e' riducibile. Non e' vero il viceversa, ad esempio $X^4 + X^2 + 1$ e' riducibile in $\mathbb{R}[X]$ ma non ha radici in $\mathbb{R}$.
4) Verificare che i polinomi di $\mathbb{R}[X]$ di grado dispari ≥ 3 sono tutti riducibili in $\mathbb{R}[X]$.

Teorema *Sia $f(X)$ e' un polinomio a coefficienti reali. Allora $f(X)$ e' irriducibile in $\mathbb{R}[X]$ se e solo se:*
i) $f(X)$ ha grado uno
oppure
ii) $f(X) = aX^2 + bX + c$ e $b^2 - 4ac < 0$.

Dim. Chiaramente ogni polinomio di grado uno e' irriducibile. Supponiamo ora $f(X) = aX^2 + bX + c$ e $b^2 - 4ac < 0$. Come abbiamo gia' visto se il discriminante e' negativo $f(X)$ non ha radici reali e quindi $f(X)$ e' irriducibile. Viceversa sia $f(X)$ un polinomio irriducibile di grado > 1. Allora $f(X)$ non ha radici reali. Se il grado di $f(X)$ e' due, allora $b^2 - 4ac < 0$. Supponiamo $f(X)$ di grado ≥ 3 e sia α una radice complessa di $f(X)$ (esiste per il Teorema fondamentale dell'algebra). Se $f(X)$ e' irriducibile, allora α non e' reale. Sia $\overline{\alpha}$ la sua complessa coniugata e sia

$$g(X) = (X - \alpha)(X - \overline{\alpha})$$

Poiche' $g(X) = X^2 - X(\alpha + \overline{\alpha}) + \alpha\overline{\alpha}$ e' un polinomio a coefficienti reali, consideriamo la divisione di $f(X)$ e $g(X)$:

$$f(X) = g(X)q(X) + r(X)$$

con $r(X) = aX + b$ un polinomio reale di grado ≤ 1. Essendo $f(\alpha) = 0$, in particolare $r(\alpha) = a\alpha + b = 0$. Poiche' α non e' reale l'eguaglianza e' possibile se e solo se $a = b = 0$. Segue che $r(X) = 0$ e quindi $f(X)$ e' riducibile. ■

Osservazione. Abbiamo provato in particolare che se $f(X)$ e' un polinomio a coefficienti reali e α e' una radice complessa di $f(X)$, anche $\overline{\alpha}$ e' radice di $f(X)$.

Esercizio. Fattorizzare $f(X) = X^4 - 2X^3 + 11X^2 - 2X + 10$ in $\mathbb{R}[X]$ sapendo che $1 - 3i$ e' radice complessa di $f(X)$.

Definizione 4. Dato un polinomio $f(X) \in K[X]$ una radice α di $f(X)$ si dice radice di molteplicitá $n \in \mathbb{N}$ se $f(X)$ é divisibile per $(X - \alpha)^n$

Esiste un criterio molto semplice per stabilire se un polinomio possiede radici multiple, o, in generale, fattori multipli.

Dato un polinomio $f(X) \in K[X]$ definiamo in modo "formale" la derivata prima $f'(X)$ [1], come é noto dalle proprietá delle derivate, la derivata del prodotto di due polinomi $f(X) \cdot g(X)$ é $f(X) \cdot g'(X) + f'(X) \cdot g(X)$.

[1] se $f(X)a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ definiamo $f'(X) = a_1 + 2a_2X + 3a_3X^2 + \ldots + na_nX^{n-1}$

Possiamo allora enunciare il seguente:

Teorema. *Sia $f(X) \in K[X]$, allora $f(X)$ non ha fattori multipli se solo se il massimo comun divisore di f e f' é 1.*

Dim. Sia $f(X) = p(X)^n \cdot g(X)$ con $n > 1$ allora, per la regola di derivazione del prodotto, avremo

$$f'(X) = n \cdot p(X)^{n-1} \cdot p'(X) \cdot g(X) + p(X)^n \cdot g'(X)$$

quindi $p(X)^{n-1}$ é un fattore non banale di $f(X)$ e $f'(X)$

Viceversa se $d(X)$ é il massimo comun divisore di $f(X)$ e $f'(X)$ e $\partial d(X) \geq 1$ sia $p(X)$ un fattore irriducibile di $d(X)$ allora f e f' sono entrambi multipli di p, quindi $f(X) = p(X) \cdot g(X)$ da cui $f'(X) = p'(X) \cdot g(X) + p(X) \cdot g'(X)$, ma se p divide f', p deve necessariamente dividere $p'(X) \cdot g(X)$ perció p divide p' oppure p divide g. p non divide p' perché $\partial p' < \partial p$ quindi p divide g, cioé $g(X) = p(X) \cdot h(X)$ da cui $f(X) = p(X)^2 g(X)$.■

Esercizio. Provare che $f(X)$ ha un fattore di molteplicitá $k > 1$ se e solo se tutte le derivate di f fino alla $(k-1)$-esima non sono prime con f mentre la derivata k-esima di f é prima con f.

2. Fattorizzazione in $\mathbb{Q}[X]$

In $\mathbb{Q}[X]$ non abbiamo una classificazione completa dei polinomi irriducibili come abbiamo visto in $\mathbb{R}[X]$ oppure in $\mathbb{C}[X]$.

Prima di tutto proviamo che per fattorizzare un polinomio in $\mathbb{Q}[X]$ possiamo limitarci a considerare polinomi a coefficienti interi.

Sia $f(X)$ un polinomio a coefficienti razionali:

$$f(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n.$$

Moltiplichiamo $f(X)$ per il massimo comun divisore dei denominatori dei coefficienti, chiamiamolo d e otteniamo cosi'

$$g(X) = df(X)$$

che e' un polinomio a coefficienti interi. Chiaramente $g(X)$ sara' irriducibile in $\mathbb{Q}[X]$ se e solo se $f(X)$ lo e'. Ai fini della fattorizzazione possiamo anche supporre che il massimo comun divisore dei coefficienti sia 1.

Supponiamo quindi $a_i \in \mathbb{Z}$ e $\mathrm{MCD}(a_1, \ldots, a_n) = 1$.

Si prova quindi

Lemma di Gauss. *Sia $f(X)$ un polinomio a coefficienti interi. Se $f(X) = g(X)h(X)$ in $\mathbb{Q}[X]$, allora $f(X) = g_1(X)h_1(X)$ con $g_1(X)$ e $h_1(X)$ polinomi a coefficienti interi. In particolare $g_1(X)$, $h_1(X)$ e $g(X)$, $h(X)$ sono rispettivamente associati.*

Proviamo un utile criterio per determinare la radici razionali di un polinomio a coefficienti interi.

Teorema. *Sia $f(X) = a_0 + a_1X + \ldots + a_nX^n$ un polinomio a coefficienti interi. Se r/s (con r e s coprimi) e' radice di $f(X)$, allora s divide a_n e r divide a_0.*

Dim. Possiamo supporre a_0 e a_n non nulli. Sappiamo che

$$f(r/s) = 0 = a_0 + a_1(r/s) + \ldots + a_n(r/s)^n.$$

Moltiplicando la precedente eguaglianza per s^n, si ottiene

$$a_0s^n + a_1rs^{n-1} + \ldots + a_{n-1}r^{n-1}s + a_nr^n = 0.$$

Da cio' si deduce che s divide a_nr^n, ma essendo r e s coprimi si deduce che s divide a_n. Analogamente r divide a_0s^n, da cui si deduce che r divide a_0.

Se vogliamo quindi determinare le possibili radici razionali dobbiamo fare ad ogni passo un numero finito di verifiche in quanto a_n e a_0 hanno un numero finito di divisori. Notiamo inoltre che se r/s e' radice di $f(X)$, allora $sX - r$ divide $f(X)$.

Un problema piu' difficile e' determinare una fattorizzazione di un polinomio di $K[X]$ quando questo non ha radici in K. Cominciamo a vedere alcuni criteri per verificare l'irriducibilita' di un polinomio.

Teorema. (*Criterio di irriducibilita' di Eisenstein*) *Sia* $f(X) = a_0 + a_1X + \ldots + a_nX^n$ *un polinomio a coefficienti interi. Se esiste un primo* p *tale che* p *non divida* a_n, p *divida* $a_{n-1}, a_{n-2}, \ldots, a_0$, *ma* p^2 *non divida* a_0, *allora* $f(X)$ *e' irriducibile in* $\mathbb{Z}[X]$ *(e quindi in* $\mathbb{Q}[X]$*).*

Dim. Supponiamo per assurdo che $f(X)$ sia riducibile, in particolare

$$f(X) = g(X)h(X)$$

con

$$g(X) = b_0 + b_1X + \ldots + b_rX^r$$
$$h(X) = c_0 + c_1X + \ldots + c_sX^s$$

Possiamo supporre $r \leq s$. Dopo aver moltiplicato i polinomi, eguagliamo i coefficienti con quelli di $f(X)$, otteniamo le seguenti eguaglianze:

$$a_n = b_rc_s$$
$$\vdots$$
$$a_s = b_rc_{s-r} + b_{r-1}c_{s-r+1} + \ldots + b_0c_s$$
$$\vdots$$
$$a_r = b_rc_0 + b_{r-1}c_1 + \ldots + b_0c_r$$
$$\vdots$$
$$a_2 = b_2c_0 + b_1c_1 + b_0c_2$$
$$a_1 = b_1c_0 + b_0c_1$$
$$a_0 = b_0c_0$$

Siccome p divide a_0, ma p^2 non lo divide, segue che p divide b_0 e non c_0 o viceversa. Supponiamo che p divide b_0 e non c_0, poiche' p divide $a_{n-1}, a_{n-2}, \ldots, a_0$, segue che p divide $b_1, b_2, \ldots, b_r$. Questo e' assurdo perche' forza p a dividere anche a_n, contro l'ipotesi. Analogamente se p divide c_0. Quindi la fattorizzazione assunta non sussiste. ■

Ovviamente ci sono polinomi che non verificano le ipotesi del precedente criterio, ma sono comunque irrudicibili. Il metodo usato nella prova del criterio di Eisenstein puo' essere faticoso, ma puo' essere tentato in ogni caso.

Ad esempio se consideriamo $f(X) = X^5 + X^4 + 2X^3 + 3X^2 - X + 5$ in $\mathbb{Q}[X]$, si prova che $f(X)$ non ha radici razionali, quindi l' eventuale fattorizzazione sara' con un polinomio di grado 3 e con uno di grado 2 a coefficienti interi. Provare a risolvere il sistema che viene determinato eguagliando i coefficienti del prodotto a quelli di $f(X)$.

E' chiaro che in generale il sistema non essendo lineare puo' essere difficile da risolvere, quindi cerchiamo altre tecniche. Un test di irriducibilita' utile e' quello di provare l'irriducibilita' in $\mathbb{Z}_m[X]$ e sollevare l'informazione. Questo, come abbiamo gia' detto, permette di lavorare in un insieme finito dove quindi i possibili divisori del polinomio sono in numero finito.

3. Fattorizzazione in $\mathbb{Z}_n[X]$

Criterio di irriducibilita' modulo m. Se $\overline{f}(X) = \overline{a_0} + \overline{a_1}X + \ldots + \overline{a_n}X^n$ e' irriducibile in $\mathbb{Z}_m[X]$ per un intero m che non divida a_n, allora $f(X)$ e' irriducibile in $\mathbb{Z}[X]$ (e quindi in $\mathbb{Q}[X]$).

Esercizio. i) Provare che $X^4 + 3X + 7$ e' irriducibile in $\mathbb{Q}[X]$.

ii) Provare che $X^5 + X^2 + 1$ e' irriducibile in $\mathbb{Q}[X]$.

Visto che la fattorizzazione dei polinomi in $\mathbb{Z}_m[X]$ si puo' ottenere in un numero finito di passi (ci sono un numero finito di polinomi di grado fissato), ci chiediamo quando una fattorizzazione non banale modulo un intero m si puo' sollevare a $\mathbb{Q}[X]$. Non possiamo sperare di poter sempre sollevare l'informazione in quanto si puo' provare che $X^4 + 1$ e' irriducibile in $\mathbb{Q}[X]$, ma e' riducibile modulo un qualunque primo. L'esempio sara' trattato nelle esercitazioni.
Puo' essere interessante il problema posto nel seguente esempio.

Esempio. Consideriamo $f(X) = X^5 + 17X^4 - 5X^3 - 277x^2 + 144$.
Ad esempio modulo 5

$$f(X) \equiv (X^3 + 3X + 2)(X^2 + 2X + 2).$$

Ora ci sono vari polinomi congrui a X^2+2X+2 modulo 5 che possono essere fattori di $f(X)$ come $X^2 + 7X + 2, X^2 + 2X - 3, X^2 + 17X + 12, X^2 - 13X - 3$, ecc. e ci vorrebbe un po' di sforzo per scoprire che

$$f(X) = (X^3 - 17X + 12)(X^2 + 17X + 12).$$

Se invece di condiderare il polinomio modulo 5, noi avessimo trovato le fattorizzazione modulo m, con m abbastanza grande avremmo avuto piu' informazione (perche?).

Per fattorizzare $f(X)$ in $\mathbb{Z}[X]$ e' interessante determinare un M sufficientemente grande (quanto?) e trovare tutte le fattorizzazioni di $f(X)$ modulo M. Ci sono varie tecniche considerando M una potenza opportuna di un numero primo p.

Per fattorizzare un polinomio in $\mathbb{Z}_p[X]$ con p un numero primo si puo' usare il metodo di fattorizzazione di Berlekamp che consiste nel risolvere sistemi di equazioni in $\mathbb{Z}_p$ e in un problema di ricerca del massimo comun divisore.

Teorema (Fattorizzazione di Berlekamp)
Dato f in $\mathbb{Z}_p[X]$ di grado n, sia g in $\mathbb{Z}_p[X]$ un polinomio di grado ≥ 1 e $< n$ tale che f divida $g^p - g$. Allora

$$f = MCD(f, g) \cdot MCD(f, g-1) \cdots MCD(f, g-(p-1)).$$

Nel corso di esercitazioni vedrete come fattorizzare $f(X) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ in $\mathbb{Z}_2[X]$ usando il metodo di Berlekamp.

GRUPPI

Un **gruppo** $(G,\ *)$ è un insieme G dotato di un'operazione binaria $*$ che soddisfa le seguenti proprietà:

i) $\forall\ a,b,c \in G,\ (a*b)\cdot c = a*(b*c)$ - proprietà associativa -

ii) $\exists\ u_G \in G$ tale che $\forall\ a \in G\ \ u_G * a = a * u_G = a$ - elemento neutro -

iii) $\forall\ a \in G,\ \exists\ b \in G$ tale che $a*b = b*a = u_G$ - inverso - [1]

Un gruppo $(G,*)$ tale che $a*b = b*a\ \forall\ a,b \in G$ si dice **gruppo commutativo** o **abeliano**.

E' facile verificare che $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_n,M_n(k)$ sono gruppi con l'usuale operazione di somma e $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*,\mathbb{Z}_p^*$ con p primo sono gruppi con l'usuale operazione di prodotto.

$G = \{A \in M_n(k)\ \det A \neq 0\}$ e' un gruppo rispetto all'operazione di prodotto di matrici (prodotto righe per colonne). G non e' commutativo se $n > 1$.

$S_n = \{$ applicazioni bigettive $f : S \to S$ con S un insieme di n elementi$\}$ e' un gruppo con l'operazione di composizione tra applicazioni detto gruppo delle permutazioni o gruppo simmetrico su n oggetti. S_n non e' commutativo se $n \geq 3$.

Siano $(G,*)$ e $(G',\circ)$ due gruppi. Nel prodotto cartesiano $G \times G'$ possiamo definire la legge di composizione nel seguente modo :

$$(g,g')\cdot(h,h') = (g*h, g'\circ h')$$

cioe' "componente per componente".
E' immediato verificare che con tale operazione $G\times G'$ e' un gruppo e dicesi *prodotto diretto (esterno) di G e G'* .
Se G e G' hanno notazione additiva, il gruppo $G \times G'$ puo' essere denotato anche $G \oplus G'$ e detto *somma diretta (esterna) di G e G'*.

Se G e' un gruppo e g e' un suo elemento, si puo' definire per induzione la potenza $n-esima$ di g per ogni $n \in \mathbb{Z}$ ponendo
$g^n = u_G$ se $n = 0$
$g^n = g*g*.....*g$ (n fattori) se $n > 0$ e $g^n = g^{-1}*g^{-1}*.....*g^{-1}$ (-n fattori) se $n < 0$.

Proposizione. *Sia G un gruppo e siano a,b elementi di G. Allora $(a*b)^{-1} = b^{-1}*a^{-1}$ e $(a^{-1})^{-1} = a$.*

[1] l'inverso b di a si indica di solito con a^{-1}

Proposizione. *Siano G un gruppo, $g \in G$ e $n, m \in \mathbb{Z}$. Allora $g^n * g^m = g^{n+m}$ e $(g^n)^m = g^{nm}$*

Legge di cancellazione nei gruppi. *Siano a, b, c elementi di un gruppo G tali che $a * b = a * c$ (oppure $b * a = c * a$). Si ha allora $b = c$.*

1. Sottogruppi

Definizione. Sia G un gruppo e S un sottoinsieme di G. Diremo che S è un **sottogruppo** di G se S è un gruppo rispetto alla restrizione di $*$ a S..

Quindi S è un sottogruppo di G se :

i) $u_G \in S$

ii) $\forall\ x \in S,\ x^{-1} \in S$.

iii) $\forall\ x, y \in S,\ x * y \in S$.

Osserviamo che se S è chiuso rispetto alle operazioni di G, le proprieta' soddisfatte da $*$ in G quali l'associativita' o la commutativita' sono automaticamente verificate da S.

Le tre condizioni precedenti possono essere sostituite dalla seguente:

Criterio per sottogruppi.
Sia S un sottoinsieme non vuoto di un gruppo G. Allora S e' un sottogruppo di G se e solo se

$$\forall g, h \in S \quad g * h^{-1} \in S$$

Esempi

1) Sia G un gruppo; esso e' un sottogruppo di G detto improprio. L'insieme costituito dalla sola identita' di G e' un sottogruppo che dicesi anche sottogruppo banale di G.
2) L'insieme $n\mathbb{Z}$ dei numeri relativi multipli di un intero n e' un sottogruppo di $\mathbb{Z}$. Si prova che tutti e soli i sottogruppi di $\mathbb{Z}$ sono del tipo $n\mathbb{Z}$ per qualche intero n.
3) $\mathbb{Z}$ e' un sottogruppo di $\mathbb{Q}$.
4) L'intersezione di sottogruppi e' ancora un sottogruppo.
5) L'unione insiemistica di sottogruppi e' un sottogruppo se e solo se uno e' sottoinsieme dell'altro.
6) $\mathbb{Z}$ con l'operazione $*$ cosi' definita:

$$a * b = a + b + 2$$

e' un gruppo commutativo. Determinare i sottogruppi di $(\mathbb{Z}, *)$.
7) $\{(x, y) \in \mathbb{R}^2 / x + 2y = 0\}$ e' un sottogruppo di $\mathbb{R}^2$.

2. Omomorfismi

Definizione: *Siano* $(G_1, *), (G_2, \circ)$ *gruppi, diremo che una applicazione* $f : G_1 \to G_2$ *è un omomorfismo di gruppi se*:

$$f(x * y) = f(x) \circ f(y) \ \forall \ x, y \in G_1.$$

Un omomorfismo bigettivo si dice *isomorfismo.*

Esempi
1. L'applicazione $f : G_1 \to G_2$ definita da $f(x) = u_{G_2}$ e' un omomorfismo detto banale (o nullo).
2. L'applicazione $f : G \to G$ definita da $f(x) = x$ e' un omomorfismo detto omomorfismo identico.
3. L'applicazione $f : \mathbb{Z}_n \to \mathbb{Z}_{2n}$ definita da $f(x) = 2x$ e' un omomorfismo.
4. L'applicazione $f : \mathbb{R}^2 \to \mathbb{R}^2$ definita da $f(x, y) = (2x+y, 2y)$ e' un omomorfismo.
5. L'applicazione $f : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ definita da $f(x) = logx$ e' un omomorfismo.

Se f: $G_1 \to G_2$ e' un omomorfismo di gruppi, si definisce nucleo di f e si indica con Ker$f$:

$$f^{-1}(u_{G_2}) = \{g \in G_1 \ \ / f(g) = u_{G_2}\}$$

Si verifica che Ker$f$ e' un sottogruppo di G_1 e Imf e' un sottogruppo di G_2.

Proposizione. *Sia f:* $G_1 \to G_2$ *e' un omomorfismo di gruppi. Allora*
a) $f(u_{G_1}) = u_{G_2}$
b) $f(g^{-1} = (f(g))^{-1}$ *per ogni* $g \in G_1$
c) $f(g^n) = (f(g))^n$ *per ogni* $g \in G_1$ *e* $n \in \mathbb{Z}$
d) f e' un omomorfismo iniettivo se e solo se Kerf=$\{u_{G_1}\}$

Definizione. Sia S un sottogruppo di G e x un elemento di G, l'insieme $xS = \{x * s \mid s \in S\}$ si dice **classe laterale sinistra** individuata da x.
Analogamente $Sx = \{s * x \mid s \in S\}$ si dirà **classe laterale destra**.

Definizione. Sia S un sottogruppo di G, S si dice sottogruppo **normale** di G se

$$xS = Sx$$

per ogni elemento x di G.

Se G e' commutativo, ogni sottogruppo di G e' normale.

Teorema. *Sia S un sottogruppo di G, allora la famiglia $\{xS\}_{x\in G}$ (analogamente $\{Sx\}_{x\in G}$) è una partizione di G.*

Dim.: è ovvio che $\{xS\}_{x\in G}$ sia un ricoprimento di G, inoltre $xS \neq \emptyset$ in quanto $x * u_G = x \in xS$, se poi $xS \neq yS$ allora $xS \cap yS = \emptyset$, infatti se esistessero $s_1, s_2 \in S$ tali che $xs_1 = ys_2$, moltiplicando entrambi a destra per l'inverso di s_1 si ha $x = ys_2(s_1)^{-1} \in yS$ da cui $xS \subseteq yS$; analogamente, moltiplicando per l'inverso di s_2 si ha $yS \subseteq xS$, quindi $xS = yS$.■

Essendo $\{Sx\}_{x\in G}$ una partizione, possiamo associare una relazione di equivalenza in G:

$x \sim_S y$ se e solo se x e y appartengono alla stessa classe laterale, cioè $x \sim_S y$ se e solo se esiste $s \in S$ tale che $x = sy$, ovvero $x * y^{-1} \in S$.

Definizione. Supponiamo che il gruppo G sia costituito da un numero finito di elementi: tale numero dicesi **ordine** di G e si denota con ord$G$.

Teorema di Lagrange. L'ordine di un qualsiasi sottogruppo S di un gruppo finito G e' un divisore dell'ordine di G.

Usando il teorema di Lagrange si prova ad esempio che $\mathbb{Z}_p$ con p primo ha come sottogruppi solo quello improprio e quello banale.

Se G e' commutativo e' facile vedere che $\sim_S$ rispetta l'operatore binario di G, ossia in $G/\sim_S$

$$\overline{x} * \overline{y} = \overline{x * y}$$

e' una operazione.

Infatti se in G:

$$\overline{x_1} = \overline{y_1}, \quad \overline{x_2} = \overline{y_2} \Rightarrow \overline{x_1 * x_2} = \overline{y_1 * y_2},$$

ovvero se

$$x_1 * (y_1)^{-1} \in S,\ x_2 * (y_2)^{-1} \in S \Rightarrow x_1 * x_2 * (y_1 * y_2)^{-1} \in S$$

Ora $x_1 * x_2 * (y_1 * y_2)^{-1} = x_1 * x_2 * y_2^{-1} * y_1^{-1}$, poiche' esiste $s \in S$ tale che $x_2 * (y_2)^{-1} = s$, occorre provare che $x_1 * s * y_1^{-1} \in S$. Se G e' commutativo allora

$$x_1 * s * y_1^{-1} = s * x_1 * y_1^{-1} \in S.$$

Piu' in generale si prova che $\sim_S$ rispetta l'operatore binario di G se e solo se S e' un sottogruppo normale di G.

Se S è un sottogruppo normale scriveremo G/S in luogo di $G/\sim_S$ e G/S eredita le buone proprieta' di $*$.

Per semplicita' nel seguito pensate G commutativo, in tal caso abbiamo gia' detto che ogni sottogruppo e' normale.

$G/S = \{\overline{x} | x \in G\}$ con $*$ è un gruppo detto **gruppo quoziente**.

In particolare si ha:
i) $u_{G/S} = \overline{u_G} = S$.
ii) $\forall\ x \in G,\ (\overline{x})^{-1} = \overline{x^{-1}}$.

Osservazione: Se $f : G_1 \to G_2$ è un omomorfismo di gruppi e $\sim_f$ è la congruenza associata a f, si ha che $G_1/\sim_f = G_1/Kerf$.
Infatti in G_1 $x \sim_f y$ se e solo se $f(x) = f(y)$ da cui, moltiplicando a sinistra i due membri per $f(y)^{-1}$, si ha $f(x)f(y)^{-1} = u_{G_2}$. Equivalentemente $y^{-1} * x \in Kerf$, infatti, essendo f un omomorfismo, $f(x)f(y)^{-1} = f(x * y^{-1})$.

Teorema. (primo teorema di omomorfismo per i gruppi).
Siano G_1 e G_2 gruppi $f : G_1 \to G_2$ un omomorfismo di gruppi, $Kerf$ il nucleo di f, $\pi : G_1 \to G_1/Kerf$ la proiezione canonica. Esiste allora un unico omomorfismo $g : G_1/Kerf \to G_2$ tale che $f = g \circ \pi$.
Si ha inoltre :
1) g è un monomorfismo.
2) g è un isomorfismo se e solo se f è epimorfismo .

4. Gruppi ciclici

Definizione. Sia G un gruppo e sia g un elemento di G. Allora

$$\{g^n\ /n \in \mathbb{Z}\}$$

e' un sottogruppo di G detto **sottogruppo ciclico** generato dall'elemento g e denotato con $< g >$

Definizione. Se g e' un elemento di G, diremo **periodo** di g il minimo intero positivo n tale che $g^n = u_G$

Proposizione. Il periodo dell'elemento g e' uguale all'ordine di $< g >$.

Definizione. Siano G un gruppo e g un elemento di G tale che

$$G = \{g^n \ / n \in \mathbb{Z}\}.$$

Allora G dicesi **gruppo ciclico** generato da g.

E' immediato verificare che se G e' ciclico, allora G e' commutativo.

Esempi
1) Il gruppo additivo $\mathbb{Z}$ e' ciclico generato da 1 e da -1.
2) $\mathbb{Z}_n$ e' ciclico generato da $\overline{1}$ e da $\overline{-1}$.
3) S_n con $n \geq 3$ non e' ciclico.
4) $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ non e' ciclico.

Usando il Teorema di Lagrange e' facile provare :

Proposizione. Un gruppo finito di ordine primo $p > 1$ e' ciclico ed e' generato da un qualsiasi elemento $g \in G$, $g \neq u_G$.

Teorema. Ogni sottogruppo di un gruppo ciclico e' ciclico

Usando il I Teorema di omomorfismo si prova che

Teorema. Ogni gruppo ciclico finito G e' isomorfo a $\mathbb{Z}_n$. Se G e' infinito, allora G e' isomorfo a $\mathbb{Z}$.

Anelli e ideali.

Un insieme A si dice un **anello** se in A sono definite due operazioni interne una denotata additivamente e l'altra moltiplicativamente, tali che le seguenti tre condizioni sono soddisfatte:

1. Gli elementi di A formano un gruppo abeliano rispetto alla somma.

2. Il prodotto gode della proprieta' associativa.

3. Proprieta' distributiva : per ogni $a, b, c \in A$ si ha

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc.$$

E' facile verificare che $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$, $M_n(k)$, $k[x]$ sono con le usuali operazioni degli anelli.

Un anello si dice **commutativo** se il prodotto gode della proprieta' commutativa. Per esempio $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono commutativi mentre $M_n(k)$ non e' commutativo.

Un anello si dice che possiede **una identita'** se esiste un elemento neutro rispetto al prodotto. Ad esempio tutti gli anelli sopra considerati sono anelli con identita', ma l'insieme dei numeri pari e' un anello commutativo senza identita'.

L'elemento neutro rispetto alla somma lo indicheremo sempre con 0. Se l'anello A possiede un elemento neutro rispetto al prodotto, tale elemento e' unico e lo indicheremo con 1.

Diremo che un elemento a dell'anello commutativo A e' un **divisore dello** 0, se esiste un elemento $b \in A, b \neq 0$ tale che $ab = 0$. E' chiaro che, a meno del caso banale in cui A sia formato dal solo 0, l'insieme degli 0-divisori di A contiene sempre almeno lo 0.

Un anello commutativo si dira' **integro (o dominio di integrita')** se l'unico 0-divisore di A e' lo zero. Cio' significa che $ab = 0$ implica $a = 0$ o $b = 0$.

Ad esempio $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono tutti anelli integri. L'anello $\mathbb{Z}_n$ non e' sempre integro. Ad esempio in $\mathbb{Z}_{12}$ si ha

$$3 \cdot 4 = 0.$$

Dunque $\mathbb{Z}_{12}$ non e' un anello integro. Se consideriamo invece $\mathbb{Z}_p$ con p un numero primo, allora $\mathbb{Z}_p$ e' integro.

Se A e' un anello commutativo con identita', diremo che un elemento $a \in A$ e' **invertibile (o una unita')** se esiste un elemento $b \in A$ tale che $ab = 1$.

Diremo che un anello commutativo con identita' A e' un **corpo** se tutti gli elementi non nulli di A sono invertibili. Ad esempio $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ con p un numero primo, sono corpi mentre $\mathbb{Z}$ non e' un corpo.

Teorema Ogni corpo e' un anello integro.

Il viceversa di tale teorema non vale: $\mathbb{Z}$ e' un anello integro che non e' un corpo.

Si vede facilmente che l'anello $\mathbb{Z}_n$ e' integro se e solo se e' un corpo, se e solo se il numero n e' primo.

Supponiamo ora che A sia un anello commutativo con identita'. Se S e' un sottoinsieme dell'anello A diciamo che S e' un **sottoanello** di A se S e' un anello rispetto alle operazioni indotte dalle operazioni di A.

Si vede facilmente che affinche' S sia un sottoanello di A bisogna che per ogni coppia di elementi $a, b \in S$ risulti:

$$a - b \in S \quad e \quad ab \in S.$$

Osserviamo che la prima proprieta' dice che $(S, +)$ e' un sottogruppo di $(A, +)$.

Ad esempio $\mathbb{Z}$ e' un sottoanello di $\mathbb{Q}$ mentre l'insieme dei numeri dispari non e' un sottoanello di $\mathbb{Z}$. Ogni anello A e' sottoanello di $A[X]$.

Diciamo invece che un sottoinsieme I dell'anello A e' un **ideale** di A se per ogni coppia di elementi $a, b \in I$ e per ogni elemento $c \in A$ risulta:

$$a - b \in I \quad e \quad ac \in I.$$

E' immediato verificare che un ideale e' anche un sottoanello, mentre ad esempio $\mathbb{Z}$ e' un sottoanello di $\mathbb{Q}$ ma non e' un ideale. Infatti $2 \in \mathbb{Z}$, $1/3 \in \mathbb{Q}$ ma $2/3 \notin \mathbb{Z}$.

Osserviamo che A e $\{0\}$ sono ideali di A. Inoltre se un ideale I contiene un elemento invertibile dell'anello A, allora $I = A$.

Se A e B sono anelli anche non commutativi e

$$f : A \to B$$

e' un applicazione, diciamo che f e' un **omomorfismo di anelli** se

$$f(a + b) = f(a) + f(b), \forall a, b \in A$$

e

$$f(ab) = f(a)f(b), \forall a, b \in A.$$

E' immediato verificare che

$$Im(f) := \{b \in B | b = f(a), a \in A\}$$

e' sempre un sottoanello di B.

Inoltre se A e' un anello commutativo, allora

$$ker(f) := \{a \in A | f(a) = 0\}$$

e' un ideale di A. Si ha anche che f e' iniettivo se e solo se $ker(f) = \{0\}$, mentre f e' surgettivo se e solo se $Im(f) = B$.

Nel corso di algebra tale capitolo sara' svolto solo in parte e di conseguenza sara' programma d'esame cio' che il docente trattera' a lezione.

ALGEBRE OMOGENEE

1. Operazioni

Definizione. Sia A un insieme e n un intero positivo. Un'operazione $*$ **n-aria** su A è un'applicazione da A^n in A che ad ogni n-upla $(a_1, ..., a_n)$ di A^n associa un elemento di A che si indica con $*(a_1, ..., a_n)$. L'intero n si dice **arietà** dell'operazione.

Per convenzione diremo operazione di arietà zero quella che consiste nel fissare un particolare elemento di A

Se $n = 2$ l' operazione si dice **binaria**. In questo caso scriveremo $a_1 * a_2$ invece di $*(a_1, a_2)$.

2. Segnature

Definizione. Un **segnatura** Σ è una famiglia di insiemi Σ_n (n intero non negativo) e ogni $\sigma \in \Sigma_n$ è un simbolo detto **operatore** (che rappresenta un'operazione di arietà n).

Fissato un insieme A e una segnatura Σ, facciamo corrispondere ad ogni operatore $\sigma \in \Sigma_n$ una sua interpretazione in A come operazione $n-$aria di A. Consideriamo cioè la famiglia di applicazioni interpretazione:
$I_n^A : \Sigma_n \to \{A^n \to A \text{ applicazioni}\}$ tali che ad ogni $\sigma \in \Sigma_n$ si associa l'operazione $n-$aria di A : $I_n^A(\sigma) : A^n \to A$.

Definizione. Le applicazioni I_n^A si dicono **interpretazioni** della segnatura Σ.
In particolare l'interpretazione di un operatore di arietà 0 consiste nel fissare un particolare elemento di A. L'insieme degli operatori $0-$ari si indica, di solito, con Σ_λ invece che con Σ_0.

Notazione: nel seguito scriveremo σ^A invece di $I_n^A(\sigma)$.

ESEMPI: Sia Σ la seguente segnatura:
$\Sigma_\lambda = \{0, 1\}, \quad \Sigma_1 = \{\sigma_1\}, \quad \Sigma_2 = \{\sigma_2,\ \sigma_3\}, \quad \Sigma_n = \emptyset\ \forall\ n > 2.$

1) Sia $A = \mathcal{P}(X)$ l'insieme delle parti di un insieme X.
   Possiamo definire le seguenti interpretazioni su A:

$0^A = \emptyset \qquad 1^A = X.$
$\sigma_1^A : A \to A$ "operazione complementare" definita da
$\sigma_1^A(B) = \mathcal{C}_X B \forall\ B\ \in A.$
$\sigma_2^A : A \times A \to A$ "operazione intersezione" definita da
$\sigma_2^A(B, C) = B \cap C\ \forall\ B, C \in A.$
$\sigma_3^A : A \times A \to A$ "operazione unione" definita da
$\sigma_3^A(B, C) = B \cup C\ \forall\ B, C\ \in A.$

2) Sia $B = \mathbb{Z}$. Possiamo definire le seguenti interpretazioni su B:
$0^B = 0 \qquad 1^B = 1.$
$\sigma_1^B : B \to B$ "successore" definita da $\sigma_1^B(n) = n + 1\ \forall n \in \mathbb{Z}.$
$\sigma_2^B : B \times B \to B \quad \sigma_2^B(n, m) = n + m$, usuale operazione di somma in $\mathbb{Z}$.
$\sigma_3^B : B \times B \to B \quad \sigma_3^B(n, m) = nm$, usuale operazione di prodotto in $\mathbb{Z}$.

3. Σ - algebre omogenee.

Definizione. Data una segnatura Σ,una Σ - **algebra** $\mathcal{A}$ è una coppia:

$$\mathcal{A} =< A,\ \{I_n^A\}_{n\in\mathbb{N}} >$$

dove A è un insieme detto **supporto** dell'algebra, $\{I_n^A\}$ è la famiglia delle interpretazioni in A della segnatura Σ

Fissata la segnatura Σ, indicheremo con Alg_Σ la classe di tutte le possibili Σ - algebre.

ESEMPI:

1) Siano $\Sigma,\ A,\ B$, definite come negli esempi precedenti, allora A con le interpretazioni $\{0^A,\ 1^A,\ \sigma_1^A,\ \sigma_2^A,\ \sigma_3^A\}$ e B con le interpretazioni $\{0^B,\ 1^B,\ \sigma_1^B,\ \sigma_2^B,\ \sigma_3^B\}$ sono Σ - algebre.
2) Consideriamo la seguente segnatura Σ :
$\Sigma_\lambda = \{1\}, \qquad \Sigma_1 = \{\otimes,\ \oplus\}, \qquad \Sigma_2 = \{\circ\}, \qquad \Sigma_n = \emptyset\ \forall\ n > 2.$
Sia $A = \{f : \mathbb{R} \to \mathbb{R} \mid f\ \text{ è invertibile}\}$ poniamo
$1^A = \mathrm{Id}_{\mathbb{R}}$ (funzione identica su $\mathbb{R}$)
$\otimes^A(f) = f^{-1} \qquad \oplus^A(f) = -f, \quad \forall\ f\ \in A.$
$\circ^A(f, g) = g \circ f$ (composizione di funzioni) $\forall\ f, g\ \in A.$

ESERCIZIO : Data la segnatura Σ dell'esempio 2) precedente definire altre Σ - algebre.

Definiamo ora l'**algebra dei termini su X** che è una particolare Σ - algebra che sarà fondamentale nel seguito.

Definizione: Sia Σ una segnatura e X un insieme di simboli (ovvero variabili) tali che $X \cap \Sigma = \emptyset$ [1].

L'algebra $T_\Sigma(X)$ dei termini su X è definita induttivamente da:
i) $X \subseteq T_\Sigma(X)$
ii) $\Sigma_\lambda \subseteq T_\Sigma(X)$
iii)$\forall\ \sigma \in \Sigma_n$ e $t_1, \ldots, t_n \in T_\Sigma(X)$ si ha $t = \sigma(t_1, \ldots, t_n) \in T_\Sigma(X)$

Le operazioni di $T_\Sigma(X)$ sono così definite:
i) $\forall\ \sigma \in \Sigma_\lambda,\ \ \sigma^{T_\Sigma(X)} = \sigma$.
ii)$\forall\ \sigma \in \Sigma_n$ e $t_1, \ldots, t_n \in T_\Sigma(X)$ allora $\sigma^{T_\Sigma(X)}(t_1, \ldots, t_n) = \sigma(t_1, \ldots, t_n)$.
Gli elementi $t \in T_\Sigma(X)$ si dicono **termini**.

Osservazione. Se $X = \emptyset$, indicheremo $T_\Sigma(X)$ con T_Σ ; T_Σ è detta anche **algebra dei termini senza variabili** oppure **word-algebra**.

Omettiamo la dimostrazione del seguente risultato

Teorema. (Decomposizione unica dei termini) *Siano Σ una segnatura. X un insieme di variabili. Per ogni $t \in T_\Sigma(X)$ vale una ed una sola delle seguenti affermazioni:*

a) *esiste uno e un solo $x \in X$ tale che $t = x$.*
b) *esiste uno e un solo $\sigma \in \Sigma_n$ e $t_1, \ldots, t_n \in T_\Sigma(X)$ tali che $t = \sigma(t_1, \ldots, t_n)$.*

ESEMPIO. Sia $X = \{x, y, z\}$ e sia Σ la segnatura definita da:
$\Sigma_\lambda = \{0\}, \quad \Sigma_1 = \{\text{succ}\}, \quad \Sigma_\text{n} = \emptyset\ \forall\ \text{n} \geq 2$.
Usando la definizione avremo: $T_\Sigma(X) = \{x, y, z, 0, \text{succ(x)}, \text{succ(succ(x))}, \text{succ(succ(succ(x)))} \ldots, \text{succ(y)}, \text{succ(}$

$\ldots, \text{succ}(0), \text{succ}(\text{succ}(0)), ...\}$

ESERCIZIO Sia Σ la segnatura definita da $\Sigma_\lambda = \{0\},\ \Sigma_1 = \{\text{succ}\},\ \Sigma_2 = \{+\},\ \Sigma_n = \emptyset\ \forall\ n > 2$. Determinare T_Σ.

4. Sottoalgebre

Definizione. Date una segnatura Σ e $A \in \text{Alg}_\Sigma$, sia B un sottoinsieme di A tale che:

i) $\forall\ \sigma \in \Sigma_\lambda, \sigma^A \in B$ (cioè B contiene le costanti).
ii) $\forall\ \sigma \in \Sigma_n$ se $b_1, \ldots, b_n \in B$, allora $\sigma^A(b_1, ..., b_n) \in B$ (cioè B è chiuso rispetto alle operazioni di A).

[1] supporremo sempre che i simboli "(" e ")" non appartengano nè a Σ nè a X.

La Σ - algebra $< B, \{\sigma^B\}_{\sigma\in\Sigma} >$ dove $\sigma^B = \sigma^{A|_B}$ [1] si dice **sottoalgebra** di A.
B si dirà **sottoalgebra propria** di A se $B \neq A$.

In particolare $\emptyset$ è una sottoalgebra di A se e solo se $\Sigma_\lambda = \emptyset$.

ESEMPIO. Consideriamo la segnatura Σ definita da:
$\Sigma_\lambda = \{0\}, \quad \Sigma_1 = \{\text{succ}\}, \quad \Sigma_\text{n} = \emptyset \ \forall\ \text{n} \geq 2.$
e la Σ - algebra $< \mathbb{N}, \{0^{\mathbb{N}}, \text{succ}^{\mathbb{N}}\} >$ dove $0^{\mathbb{N}} = 0$, $\text{succ}^{\mathbb{N}}(\text{n}) = \text{n} + 1\ \forall \text{n} \in \mathbb{N}$.
Si verifica facilmente, usando la definizione, che questa $\Sigma-$ algebra non ammette sottoalgebre proprie.

Definizione. Sia B un sottoinsieme di $A \in \text{Alg}_\Sigma$, diremo **chiusura induttiva** di B in A il più piccolo insieme B_A che soddisfa le seguenti proprietà:
i) $B \subseteq B_A$
ii) $\forall\ \sigma \in \Sigma_\lambda,\ \sigma^A \in B_A$
iii) $\forall\ \sigma \in \Sigma_n$ se $b_1, \ldots, b_n \in B_A$, allora $\sigma^A(b_1, \ldots, b_n) \in B_A$.

Si verifica facilmente che B_A è la più piccola sottoalgebra di A che contiene il sottoinsieme B e che se B è sottoalgebra di A allora $B_A = B$.

ESERCIZIO. Sia B la Σ - algebra definita nell'esempio 7.2 a pag. 14: caratterizzare tutte le possibili sottoalgebre.

Definizione 9.3 : Se $B_A = A$, allora B è detto **sistema di generatori** per A ed A si dice **generata induttivamente** da B.
Ad esempio la Σ - algebra dell'esempio 7.1 è generata induttivamente da $\{0\}$.
Definizione 9.4 $A \in \text{Alg}_\Sigma$ si dice **minimale** o **induttiva** o
term-generated se e solo se A non ammette sottoalgebre proprie.

5. Σ - omomorfismi.

Il concetto di applicazione non è più sufficiente se, invece di insiemi, trattiamo $\Sigma-$ algebre cioè insiemi con strutture, dovremo quindi definire applicazioni che "preservano la struttura" .

Definizione. Date $A, B \in \text{Alg}_\Sigma$, un $\Sigma-$ **omomorfismo** (o, se non ci sono ambiguità, più semplicemente **omomorfismo** $f : A \to B$ è un'applicazione tale che:
i) $\forall\ \sigma \in \Sigma_\lambda,\ f(\sigma^A) = \sigma^B$.
ii) $\forall\ \sigma \in \Sigma_n$ se $a_1, \ldots, a_n \in A$, $f(\sigma^A(a_1, \ldots, a_n)) = \sigma^B(f(a_1), \ldots, f(a_n))$.

[1] con il simbolo $\sigma^{A|_B}$ si intendono le operazioni di A ristrette a B

ESEMPIO. Sia Σ la segnatura definita da:

$\Sigma_\lambda = \{a\}, \quad \Sigma_1 = \emptyset, \quad \Sigma_2 = \{\otimes\}, \quad \Sigma_n = \emptyset \ \forall \ n > 2.$

Consideriamo le seguenti $\Sigma-$ algebre:

$< A, \{a^A, \otimes^A\} >$ dove $A = I\!R_{>0}, \quad a^A = 1, \quad \otimes^A$ prodotto ordinario nei reali positivi e $< B, \{a^B, \otimes^B\} >$ dove $B = I\!R, \quad a^B = 0,$ $\otimes^B$ somma ordinaria nei reali.

L'applicazione $f : A \to B$ definita da $f(x) = \ln x$ è un omomorfismo, infatti: $f(1) = 0$, per ogni $x, y \in A \quad f(xy) = f(x) + f(y)$

ESERCIZIO. Sia Σ la segnatura definita da:

$\Sigma_\lambda = \{a\}, \quad \Sigma_1 = \emptyset, \quad \Sigma_2 = \{\otimes\}, \quad \Sigma_n = \emptyset \ \forall \ n > 2.$

Siano $A = \mathbb{Z}_4, \quad B = \mathbb{Z}_6$ con $a^A = \overline{0}, \ a^B = \overline{\overline{0}},$

$\overline{x} \otimes \overline{y} = \overline{x + y} \quad \overline{\overline{x}} \otimes \overline{\overline{y}} = \overline{\overline{x + y}}$ [1].

Determinare tutti i possibili omomorfismi di A in B.

[1] la sopralineatura rappresenta le classi di interi modulo 4, la doppia sopralineatura rappresenta le classi di interi modulo 6

Teorema. a) *Sia* $A \in \mathrm{Alg}_\Sigma, \mathrm{i_A} : \mathrm{A} \to \mathrm{A}$ *l'applicazione identica, allora* i_A *è un omomorfismo .*
b) *Date* $A, B, C \in \mathrm{Alg}_\Sigma$, *e gli omomorfismi* $f : A \to B$ *e* $g : B \to C$, *l'applicazione composta* $g \circ f : A \to C$ *è un omomorfismo .*

Dim. : a) ovvio b) Poichè $(g \circ f)(a) = g(f(a))$, si ha che $\forall\ \sigma \in \Sigma_\lambda$,
$(g \circ f)(\sigma^A) = g(f(\sigma^A)) = g(\sigma^B) = \sigma^C$.
Inoltre $\forall\ \sigma \in \Sigma_n$ se $a_1, \ldots, a_n \in A$, si ha
$(g \circ f)(\sigma^A(a_1, \ldots, a_n)) = g(f(\sigma^A(a_1, \ldots, a_n))) = g(\sigma^B(f(a_1), \ldots, f(a_n))) = = \sigma^C((g \circ f)(a_1), \ldots, g \circ f)(a_n))$.■

ESERCIZIO : Siano $A, B \in \mathrm{Alg}_\Sigma$, e $f : A \to B$ un omomorfismo di algebre, siano A' e B' sottoalgebre rispettivamente di A e B. Provare che:
a) $f(A')$ è una sottoalgebra di B
b) $f^{-1}(B')$ è una sottoalgebra di A.

Definizione : Siano $A, B \in \mathrm{Alg}_\Sigma$, e $f : A \to B$ un omomorfismo.
$-f$ si dice **monomorfismo** se f è iniettiva,
$-f$ si dice **epimorfismo** se f è surgettiva,
$-f$ si dice **isomorfismo** se f è bigettiva, in questo caso A e B si dicono isomorfe e si scrive $A \simeq B$.

6. Algebre iniziali e algebre finali.

Definizione : Sia C una classe di $\Sigma-$ algebre e A una $\Sigma-$ algebra.
i) A si dice **algebra iniziale** in C se e solo se $A \in$ C e $\forall\ B \in$ C esiste uno e un solo omomorfismo $f : A \to B$
ii) A si dice **algebra finale** in C se e solo se $A \in$ C e $\forall\ B \in$ C esiste uno e un solo omomorfismo $f : B \to A$.

In una classe C $\subseteq \mathrm{Alg}_\Sigma$ sia l'elemento iniziale che quello finale sono determinati a meno di isomorfismi.

Teorema. *Sia C una classe di* $\Sigma-$ *algebre.*
i) *se A e B sono iniziali in C allora* $A \simeq B$.
ii) *siano* $A, B \in C$ *, se A è iniziale in C e* $A \simeq B$, *allora B è iniziale in C.*

Dim. : i) Essendo A e B iniziali per la def. 5.1. esiste un unico omomorfismo $f : A \to B$ ed esiste un unico omomorfismo $g : B \to A$. Inoltre $i_A : A \to A$ e $i_B : B \to B$ sono omomorfismi e per l'unicità dell'omomorfismo si ha $g \circ f = i_A : A \to A$ e $f \circ g = i_B$, quindi f e g sono bigettive.
ii) Supponiamo che esistano due omomorfismi $f_1 : B \to D$ e $f_2 : B \to D$ (dove $D \in$

C), e sia f l'isomorfismo tra A e B, per l'inizialità di A avremo che $f_1 \circ f = f_2 \circ f$ da cui (essendo f invertibile) $f_1 = f_2$.■

L'analogo del teorema precedente si può formulare per gli oggetti finali.

Teorema. *Se $A \in \mathrm{Alg}_\Sigma$, esiste un unico omomorfismo*
$$eval^A : T_\Sigma \to A.$$

Dim.: Per l'unicità della decomposizione dei termini in T_Σ, [1] per ogni $t \in T_\Sigma$ esiste un unico $\sigma \in \Sigma_\lambda$ tale che $t = \sigma$ oppure esistono unici $n > 0$, $\sigma \in \Sigma_n$, $t_1, \ldots, t_n \in T_\Sigma$ tali che $t = \sigma(t_1, \ldots, t_n)$.
Basta quindi definire $eval^A : T_\Sigma \to A.$ nel seguente modo:

i) $eval^A(\sigma) = \sigma^A$ per ogni $\sigma \in \Sigma_\lambda$

ii) $eval^A(\sigma(t_1, \ldots, t_n)) = \sigma^A(eval^A(t_1), \ldots, eval^A(t_n)) \ \forall\ \sigma \in \Sigma_n$, $t_1, \ldots, t_n \in T_\Sigma$. Per 'unicità della decomposizione $eval^A$ è ben definita e, in base alla definizione, è un omomorfismo.

Per provare che $eval^A$ è l'unico omomorfismo da T_Σ in A basta osservare che un omomorfismo $f : T_\Sigma \to A$ deve soddisfare i) e ii).■

Corollario. *T_Σ è iniziale in Alg_Σ. Quindi un'algebra A è iniziale in Alg_Σ se e solo se è isomorfa a T_Σ.*

Vediamo ora le relazioni tra inizialità e minimalità. [1]

Teorema. *Sia $A \in Alg_\Sigma$, A è minimale se e solo se $eval^A$ è surgettivo. Inoltre se A è iniziale in Alg_Σ allora A è minimale.*

Dim.: Osserviamo che $eval^A(T_\Sigma)$ è una sottoalgebra di A (vedi esercizio a pag.19) quindi se A è minimale deve essere $eval^A(T_\Sigma) = A$ poichè A non ammette sottoalgebre proprie. Viceversa supponiamo che $eval^A(T_\Sigma)$ sia surgettivo e sia A' una sottoalgebra di A, sia $i : A' \to A$ il monomorfismo di immersione (cioè $i(a) = a \forall\ a \in A'$), essendo T_Σ iniziale si ha: $i \circ eval^{A'} = eval^A$, ma $eval^A$ è surgettivo quindi i è surgettivo e perciò $A \simeq A'$.■

ESERCIZI. Siano A e $B \in \mathrm{Alg}_\Sigma$.

1) Siano A minimale e $f : A \to B$ un omomorfismo, allora $f(A)$ è minimale.
2) Sia $f : A \to B$ un omomorfismo, allora $\forall\ t \in T_\Sigma$, $f(eval^A(t)) = eval^B(t)$.
3) Se A è minimale, allora esiste, al più, un omomorfismo di A in B.
4) Se B è minimale e $f : A \to B$ un omomorfismo, allora f è surgettivo.
5) Se A e B sono minimali e $f_1 : A \to B$, $f_2 : B \to A$ sono omomorfismi, allora

[1] vedi teor. 8.1 pag. 16

[1] per la definizione di minimale vedi def. 9.4 pag. 18

$A \simeq B$.

7. Σ - algebre con equazioni.

Data una segnatura Σ, consideriamo un insieme X di variabili tali che $\Sigma \cap X = \emptyset$. Indichiamo con $T_\Sigma(X)$ la corrispondente algebra dei termini.

Definizione. Data una terna $< X, t_1, t_2 >$, dove X è un insieme di variabili, $t_1, t_2 \in T_\Sigma(X)$.
Diremo Σ - equazione l'identità $t_1 = t_2 \ \forall \ X$.

ESEMPIO. Sia Σ la segnatura definita da $\Sigma_\lambda = \{0\},\ \Sigma_2 = \{+\}$,
$\Sigma_n = \emptyset \ \forall \ n \neq 2$ e sia $X = \{x, y, z\}$. Sono Σ - equazioni:
a) $+(0, x) = x$ b) $+(x, y) = +(y, x)$ c) $+(x, +(y, z)) = +(+(x, y), z)$.

Definizione. Data una $\Sigma-$ algebra A, diremo **valutazione** o **assegnamento** di valori da X in A un'applicazione $\rho : X \to A$.

Si può verificare che per ogni assegnamento ρ esiste un unico omomorfismo $eval^{A,\rho}$: $T_\Sigma(X) \to A$ che estende ρ e $eval^A$.

Si definisce $eval^{A,\rho}$ come segue:
i) $eval^{A,\rho}(x) = \rho(x) \ \forall \ x \in X$
ii) $eval^{A,\rho}(\sigma) = \sigma^A \ \forall \ \sigma \in \Sigma_\lambda$.
iii) $eval^{A,\rho}(\sigma(t_1, \ldots, t_n)) = \sigma^A(eval^{A,\rho}(t_1), \ldots, eval^{A,\rho}(t_n)) \ \forall \ \sigma \in \Sigma_n$, $t_1, \ldots, t_n \in T_\Sigma(X)$

Definizione. Diremo che $A \in \mathrm{Alg}_\Sigma$ soddisfa la Σ - equazione
$< X, t_1, t_2 >$ se e solo se per ogni assegnamento $\rho : X \to A$ si ha
$eval^{A,\rho}(t_1) = eval^{A,\rho}(t_2)$.

ESEMPIO. Sia Σ la segnatura definita da $\Sigma_\lambda = \{0\},\ \Sigma_2 = \{+\}$,
$\Sigma_n = \emptyset \ \forall \ n \neq 2$, sia $X = \{x, y, z\}$ e sia $A \in \mathrm{Alg}_\Sigma$ con $A = I\!R,\ 0^A = 0$,
$+^A = +$ (somma ordinaria). Poichè 0 è l'elemento neutro rispetto alla somma e la somma gode della proprietà associativa e commutativa, A soddisfa le
$\Sigma-$ equazioni a), b), c) dell'esempio precedente.

ESERCIZI.

1) Data la segnatura Σ con $\Sigma_\lambda = \{0\},\ \Sigma_1 = \{-\},\ \Sigma_2 = \{+\},\ \Sigma_n = \emptyset$ $\forall \ n > 2$.
a) Determinare $A, B \in \mathrm{Alg}_\Sigma$ tali che l'omomorfismo $\varphi : T_\Sigma \to A$ sia iniettivo

ma non surgettivo e l'unico omomorfismo $\psi : T_\Sigma \to B$ sia surgettivo ma non iniettivo .

b) Determinare un'algebra $A \in \mathrm{Alg}_\Sigma$ che sia finale.

2) Sia Σ la segnatura dell'esercizio precedente e siano $A, B \in \mathrm{Alg}_\Sigma$ tali che il supporto di A sia $\mathbb{Z}$, $0^A = 0$, $-^A : \mathbb{Z} \to \mathbb{Z}$ definita da $-^A(n) = -n$, $+^A$ la somma ordinaria in $\mathbb{Z}$.
Il supporto di B sia $\mathbb{R}$, $0^B = 0$, $-^B : \mathbb{R} \to \mathbb{R}$ definita da $-^B(x) = -x$, $+^B$ somma ordinaria in $\mathbb{R}$.
Determinare tutti i $\Sigma-$ omomorfismi di A in B.

3) Data la segnatura Σ con $\Sigma_\lambda = \{t, \mu\}$, $\Sigma_1 = \{f\}$, $\Sigma_n = \emptyset \ \forall\ n > 1$.
Sia A la Σ - algebra di supporto $\mathbb{Z}$ con $t^A = 0$, $\mu^A = -4$, $f^A : \mathbb{Z} \to \mathbb{Z}$ definita da $f^A(n) = n + 2$ e sia B la Σ - algebra di supporto $\mathbb{N}$ con $t^B = 0$, $\mu^B = 4$, $f^B : \mathbb{N} \to \mathbb{N}$ definita da $f^B(n) = n + 2$.

a) A ammette sottoalgebre proprie?

b) B ammette sottoalgebre proprie?

c) Quanti sono i Σ - omomorfismi di A in B?

d) Quanti sono i Σ - omomorfismi di B in A?

4) Sia Σ la segnatura dell'esercizio 1).

a) Stabilire quali tra le seguenti stringhe sono termini (in notazione funzionale):
$-(+(-(0), -(0)))$; $-(+(0))$; $+(+(+(0,0),0)))$;
$+(+(0,0), +(0,0))$.

b) Sia A la Σ - algebra di supporto $\mathcal{P}(\mathbb{N})$ con $0^A = \emptyset$, $-^A : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ definita da $-^A(X) = \mathcal{C}_\mathbb{N}(X)$, [1] $+^A =$ "unione", è possibile determinare $t \in T_\Sigma$ tale che $eval^A(t) = \mathbb{N}$?

5) Data la segnatura Σ con $\Sigma_\lambda = \{0\}$, $\Sigma_1 = \{succ\}$, $\Sigma_n = \emptyset \forall\ n \geq 2$.

a) Determinare un'algebra $A \in \mathrm{Alg}_\Sigma$ che sia finale.

b) Determinare una Σ - algebra A non iniziale e non finale tale che $eval^A : T_\Sigma \to A$ sia surgettivo.

c) Sia B una Σ - algebra con un numero finito di elementi, provare che non esistono omomorfismi $\varphi : B \to C$ dove C è la Σ - algebra con supporto $\mathbb{N}$ e interpretazioni standard di 0 e $succ$ [1].

6) Sia Σ la segnatura definita da $\Sigma_\lambda = \{0\}$, $\Sigma_2 = \{+\}$. Sia A la Σ - algebra con supporto $\mathbb{Z}$ e interpretazioni $0^A = 0$ e $+^A =$ somma ordinaria.

a) A è minimale ?

b) Determinare la più piccola sottoalgebra di A il cui supporto contenga $\{2, 3\}$.

---

[1] dove $\mathcal{C}_\mathbb{N}(X)$ rappresenta il complementare di X in $\mathbb{N}$.

[1] $0^\mathbb{N} = 0$, $succ^\mathbb{N}(n) = n + 1 \forall\ n \in \mathbb{N}$.

7) Sia Σ la segnatura definita da $\Sigma_\lambda = \{a, b\},\ \Sigma_2 = \{F, G\}$. Sia A la Σ - algebra con supporto $\mathcal{P}(I)$ dove $I = \{0, 1\},\ a^A = \emptyset$, $b^A = I$, $F^A =$ "unione", $G^A =$ "intersezione".

a) Quante sono le sottoalgebre di A ?

b) Quanti sono gli omomorfismi $\varphi : A \to A$?

8. Σ-congruenze

Data una segnatura Σ e $A \in \mathrm{Alg}_\Sigma$ caratterizziamo le relazioni di equivalenza che rispettano Σ.

Definizione. sia $\sim$ una relazione di equivalenza su A, diremo che $\sim$ è una Σ **- congruenza** se:

$\forall\ \sigma \in \Sigma_n,\ a_1, \ldots, a_n, b_1, \ldots, b_n \in A,\ a_i \sim b_i \Longrightarrow$
$\sigma^A(a_1, \ldots, a_n) \sim \sigma^A(b_1, \ldots, b_n)$.

ESERCIZIO. Sia Σ la segnatura definita da $\Sigma_1 = \{succ\},\ \Sigma_2 = \{+\}$, consideriamo le Σ - algebre di supporto $\mathbb{Z}$ dove $succ^{\mathbb{Z}}(n) = n + 1 \forall\ n \in \mathbb{Z}$ e $+^{\mathbb{Z}}$ = operazione ordinaria di somma.

Provare che le seguenti relazioni di equivalenza in $\mathbb{Z}$ sono Σ - congruenze:

a) $n \sim m$ se $n^2 + m^2$ è pari.

b) $n \sim m$ se $n - m$ è multiplo di 3.

Teorema. *Sia Σ una segnatura , A e $B \in \mathrm{Alg}_\Sigma$, $f : A \to B$ un omomorfismo. Allora $\sim_f$ è una Σ - congruenza su A.*

Dim.: Ricordando che in A $x \sim_f y$ se $f(x) = f(y)$, proviamo che $\forall\ \sigma \in \Sigma_n$, se $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$, e $x_i \sim y_i\ \forall\ i = 1, \ldots, n$ allora

$$\sigma^A(x_1, \ldots, x_n) \sim_f \sigma^A(y_1, \ldots, y_n) \text{ ossia}$$

$f(\sigma^A(x_1, \ldots, x_n)) = f(\sigma^A(y_1, \ldots, y_n))$; ma, per definizione di omomorfismo,

$f(\sigma^A(x_1, \ldots, x_n)) = \sigma^B(f(x_1), \ldots, f(x_n))$ quindi se $f(x_i) = f(y_i)\ \forall\ i = 1, \ldots, n$ si ha $f(\sigma^A(x_1, \ldots, x_n)) = f(\sigma^A(y_1, \ldots, y_n))$.■

Definizione. Data una segnatura Σ sia $A \in \mathrm{Alg}_\Sigma$ e sia $\sim$ una Σ - congruenza su A, diremo **algebra quoziente su A modulo $\sim$** , e la indicheremo con $A/\sim$, la Σ - algebra di supporto l'insieme quoziente $A/\sim$ e le cui operazioni sono quelle "indotte" da A:

i) $\forall\ \sigma \in \Sigma_\lambda, \quad \sigma^{A/\sim} = \overline{\sigma^A}$

ii) $\forall\ \sigma \in \Sigma_n, \quad \sigma^{A/\sim}(\overline{a_1}, \ldots, \overline{a_n}) = \overline{\sigma^A(a_1, \ldots, a_n)}$.

Osservazione : E' immediato vedere che, essendo $\sim$ una Σ - congruenza, le operazioni in $A/\sim$ sono ben definite. [1]

ESERCIZIO. Siano $A \in \mathrm{Alg}_\Sigma$ e $\sim$ una Σ - congruenza. Provare che la proiezione canonica $\pi : A \to A/\sim$ tale che $\pi(a) = \overline{a}$ è un Σ - epimorfismo.

[1] ricordiamo che se $a_i \sim b_i,\ \overline{\sigma^A(a_1, \ldots, a_n)} = \overline{\sigma^A(b_1, \ldots, b_n)}$.

Teorema. (primo teorema di omomorfismo per le algebre).
Siano Σ *una segnatura* A *e* $B \in \mathrm{Alg}_\Sigma$, f : A $\to$ B *un omomorfismo,* $\sim_f$ *la* Σ *- congruenza associata a* f, $\pi : A \to A/\sim_f$ *la proiezione canonica. Esiste allora un unico omomorfismo* $g : A/\sim_f \to B$ *tale che* $f = g \circ \pi$.
Si ha inoltre :

1) g *è un monomorfismo.*
2) g *è un isomorfismo se e solo se* f *è un epimorfismo .*

Teorema. *Sia* A *una* Σ *- algebra minimale, allora* $A \simeq T_\Sigma/\sim_{eval^A}$ *dove* $\sim_{eval^A}$ *è la relazione di equivalenza associata all'omomorfismo*

$$eval^A : T_\Sigma \to A.$$

Teorema. *Siano* A *e* $B \in \mathrm{Alg}_\Sigma$, f : A $\to$ B *un omomorfismo , allora* $\sim_{eval^A} \subseteq \sim_{eval^B}$ ∎
. [1]

[1] con $\sim_{eval^A} \subseteq \sim_{eval^B}$ si intende che se $t_1 \sim_{eval^A} t_2,\ t_1, t_2 \in T_\Sigma$ allora $t_1 \sim_{eval^B} t_2$.