$A = \mathbb{Z}, K[x]$ Relazioni di Equivalenza E

$(M, *)$ $E \subseteq M \times M$

Problema: $*$ e E sono compatibili?

<u>Def</u>: Si dice che E è una CONGRUENZA rispetto a $*$ se $\forall a, a', b, b' \in M$

$$aEa', \ bEb' \Rightarrow (a*b)E(a'*b')$$

Esempio: Sia $M = \mathbb{Z}$ $* = +$ $aEa' \overset{def}{\Longleftrightarrow} a' = a + 2h$ $\exists h \in \mathbb{Z}$

R) aEa $\forall a \in \mathbb{Z}$ $\exists h \in \mathbb{Z}$ $a = a + 2h$ $h = 0$

S) aEa' $\exists h \in \mathbb{Z}$ $a' = a + 2h$ $a = a' + 2(-h)$
$-h \in \mathbb{Z}$ $a'Ea$

T) aEa' e $a'Ea''$ $a' = a + 2h$ $h, k \in \mathbb{Z}$
$a'' = a' + 2k = a + 2(h+k)$

aEa''

Congruenza aEa' bEb' $(a+b)E(a'+b')$

$a' = a + 2h$
$b' = b + 2k$ $\exists h, k \in \mathbb{Z}$ $a' + b' = (a+b) + 2(h+k)$

$(a'+b')E(a+b)$

Criterio per Congruenze: E è una congruenza per $*$ sse $\forall a, b, c \in M$ con $aEb \Rightarrow c*a \, E \, c*b$
$a*c \, E \, b*c$

Dim: E congruenza aEb $cEc \Rightarrow c*a \, E \, c*b$
$a*c \, E \, b*c$

Viceversa aEb $a'Eb' \Longrightarrow a*a' \, E \, b*b'$

$a * a' \, E \, \cancel{b * a'} \qquad \cancel{b * a'} \, E \, b * b' \Rightarrow a * a' \, E \, b * b'$

Importanza: $M \quad E \quad M/E = \{ [m]_E : m \in M \}$

$[m]_E = \{ n \in M : n E m \}$ classe di E-equivalenza per m

M/E insieme quoziente (M su E, M modulo E)

Esempio: $M = \mathbb{Z} \quad E_2 \quad a' E a \quad a' = a + 2h \ \exists h \in \mathbb{Z}$

$$M/E = \{ \underset{\substack{\parallel \\ [0]_{E_2}}}{[104]_{E_2}} , \underset{\substack{\parallel \\ [1]_{E_2}}}{[-101]_{E_2}} \} =$$

$$[m]_E *_E [n]_E := [m * n]_E$$

	$[0]_E$	$[1]_E$
$[0]_E$	$[0]_E$	$[1]_E$
$[1]_E$	$[1]_E$	$[0]_E$

$(M/E, *_E)$

Problema: Siccome $[m]_E *_E [n]_E = [m * n]_E$

e.g. $[0]_E = [2]_E$ Non è ovvio che $[m']_E = [m]_E$

Teorema: $(M, *)$ E rel. di equivalenza

Allora $[m]_E *_E [n]_E = [m * n]_E$ è ben posta

ossia non dipende dal NOME o dal RAPPRESENTANTE delle classi di equivalenza

sse E è congruenza

Dim: Se E congruenza $\qquad m' E m \Leftrightarrow [m']_E = [m]_E$

$[m']_E * [n]_E = [m' * n]_E$

$(m * n) \, E \, (m' * n)$ analogamente $m * n \, E \, m * n'$

per $n \, E \, n'$ $\square$

Esercizio: Mostrare viceversa che $*_E$ è ben posta

$\Rightarrow E$ congruenza

ATTENZIONE: $M = \mathbb{Q}$ $\quad \frac{2}{3} \left(= \frac{4}{6} = \frac{2a}{3a} \right) a \in \mathbb{Z} \quad a \neq 0$

$f : \mathbb{Q} \to \mathbb{Z}$ ben posta

$\frac{a}{b} \longmapsto a+b$

$\frac{2}{3} \longmapsto 5 = 2+3$

$\quad \shortparallel \qquad\qquad\quad \nparallel$

$\frac{4}{6} \longmapsto 10$

$g : A \to B \quad \forall a \; \exists ! b$

$G \subseteq A \times B \qquad b = g(a)$

$(a, g(a))$

$A = \mathbb{Z}$

Def Dati $a, b \in \mathbb{Z}$ dico che b DIVIDE a $\to$ $\boxed{b \mid a}$

a MULTIPLO di b

sse $\exists \, k \in \mathbb{Z} \quad a = bk$

Dico inoltre $m \in \mathbb{N}$ b^m è la massima potenza di b che divide a se $b^m \mid a$ ma $b^{m+1} \nmid a$

$b^m \parallel a$

Def Fissiamo $n \in \mathbb{Z}$ $\quad E_n \subseteq \mathbb{Z} \times \mathbb{Z}$

$$a \, E_n \, b \underset{def}{\iff} n \mid b-a \iff b-a = kn \; \exists \, k \in \mathbb{Z}$$

$$\iff b = a + kn$$

Prop: E_n è CONGRUENZA sia per $+$ che per $\cdot$ prodotto

Dim: R) $a \, E_n \, a \qquad a = a + 0 \cdot n$

S) $a E_n b \quad b = a + kn \quad a = b + (-k)n$

τ) $a E_n b$ e $b E_n c \quad \begin{matrix} b = a + kn \\ c = b + hn \end{matrix} \Rightarrow c = a + (k+h)n$

dove $h, k \in \mathbb{Z}$

Osservazione: E_n è di equivalenza poiché $(\mathbb{Z}, +, 0)$

E_n è congruenza $\quad \begin{matrix} a E_n b \\ a' E b' \end{matrix} \Rightarrow a * a' \; E_n \; b * b' \quad * = +, \cdot$

$a E_n b \Rightarrow a * c \; E_n \; b * c$

$b = a + kn \qquad bc = ac + (kc)n$

$(\mathbb{Z}/E_n, +_{E_n}, 0_{E_n})$, $(\mathbb{Z}/E_n, \cdot_{E_n}, 1_{E_n})$

gruppo abeliano $\qquad$ monoide commutativo

Logica proposizionale DNF CNF

$f = \bigwedge_{w \in W} d_w \qquad W = \{ w = (a_1 \; a_n) : f(w) = 0 \}$

CNF $\quad V = \{ (b_1 \; b_n) : b_i \in \{0,1\} \} \quad |V| = 2^n$

$B_n := \{ f : V \to B_0 = \{0,1\} \} \quad |B_n| = 2^{2^n}$

funzione doppiamente esponenziale

$d_w = (w_1^*(x_1) \vee \qquad \vee w_n^*(x_n))$ $\qquad \{ d_v : v \in V \}$

$2^n \qquad\qquad : 2^n$

$d_{\underline{0}}^{\epsilon_1} \wedge d_{w_1} \wedge \qquad \wedge d_{w_{2^n}}$

$k = 0 \quad f = \bigwedge_{v \in \emptyset} d_v = 1$

$k = 1 \quad f = d_w \quad 2^n$

$k = 2 \quad f = d_w \wedge d_z = d_z \wedge d_w \qquad w \neq z$

$$\frac{2^n \cdot (2^n - 1)}{2}$$

$k = 3 \quad f = d_w \wedge d_z \wedge d_u \qquad (u, z, w) \ 6$ scelte

$$\frac{2^n \cdot (2^n - 1) \cdot (2^n - 2)}{3 \cdot 2 \cdot 1} = \binom{2^n}{3}$$

<u>Def</u> $m, k \in \mathbb{N} \quad \binom{m}{k} = |\{K \subseteq M : |K| = k\}|$

$|M| = m \qquad a_1 \quad a_m \qquad K = \{b_1 \quad b_k\}$

$m \cdot (m-1) \qquad (m - (k-1))$

$K = \{c_1 \quad c_k\}$

$k(k-1) \quad (k - (k-1)) = k!$

1

$$\binom{m}{k} = \frac{m \cdot (m-1) \quad (m-k+1)}{k!} =$$

$$= \frac{m \cdot \quad \cdot (m-k+1)}{k!} \frac{(m-k)(m-k-1) \cdot \quad 1}{(m-k)!} = \frac{m!}{k!(m-k)!}$$

Formula del binomio di Newton.

$m = \binom{m}{1} = \frac{m!}{1!(m-1)!} = \frac{m}{1} = m \qquad 1 = \binom{m}{0} = \frac{m!}{0!\, m!} = \frac{1}{0!}$

$0! := 1$

$$\binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1}$$

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

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
1 & & 3 & & 3 & & 1
\end{array}
$$

$\binom{m}{m} = 1 \quad \forall m \in \mathbb{N}$

$M = \{1, 2, 3, 4\}$ $|K| = 1$ $\{1\}, \{2\}, \{3\}, \{4\}$

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

2^m addendi

$(a+b)(a+b)$ $(a+b) = a\,b\,a\,a\,b\,b\,b$ $ab +$

$\binom{m}{k} a^k b^{m-k}$ 1 3, 4 $m-1$

$m = 2$ $(a+b)^2 = a^2 + 2ab + b^2$

$\binom{2}{2} a^2 b^0 + \binom{2}{1} a^1 b^{2-1} + \binom{2}{0} a^0 b^2$

$a^2 + 2ab + b^2$

CNF

$k = 0$ $1 = \binom{m}{0}$ $m = 2^n$

$k = 1$ $m = \binom{m}{1}$ d_w

k $\binom{m}{k}$ $d_w \wedge d_z =$

$d_{w'} \wedge d_{z'}$

$$16 = \sum_{k=0}^{m} \binom{m}{k}$$

$M = \{1, 2, 3, 4\}$

$\emptyset$	$\{a\}$	$\{a, b\}$	$\{a, b, c\}$	M
1	4	$\binom{4}{2} = 6$	4	1

ho 16 sottoinsiemi

$$\binom{m}{k} = \binom{m}{m-k}$$

$K \longleftrightarrow K^c = M \setminus K$

$|M| = m \quad |\{K \subseteq M\}| = 2^m \quad f_K(x) = \begin{cases} 0 & x \notin M \\ 1 & x \in M \end{cases}$

$|2^M| = 2^m \qquad 2^m = \sum_{k=0}^{m} \binom{m}{k}$

Se $m = 2^n = |V_n| \quad |B_n| = 2^{2^n} = 2^m$

$= 2^m = \sum_{k=0}^{m} \binom{m}{k} = |B_n|$

$\wedge v$

unica scrittura $\bigwedge_W dw = \bigwedge_U du$

$\iff W = U$

MAGMA $\left(\binom{m}{0} \right)_{m=0}^{100} \qquad |\{a, a+1, \dots, b\}| = b - a + 1$

$a \leq b$

EDNF exclusive disjunctive normal form

ECNF $\quad f = \bigwedge \oplus e_w \qquad e_w = w_1^*(x_1) + \quad + w_n^*(x_n)$

$n = 2 \quad x, y \qquad e_{\underline{0}} = x + y$

$e_{(1,0)} = 1 + x + y$

$e_{(1,1)} = 1 + x + 1 + y = x + y$

$e_{(0,1)} = x + 1 + y = 1 + x + y$