RELAZIONI E FUNZIONI

$M_{R\cap T} = M_R \cdot M_T$ (termine a termine)
$M_{R\cup T} = M_R + M_T$
$M_{RT} = M_R \cdot M_T$ (matriciale) $\longrightarrow$ PRODOTTO: - ASSOCIATIVO
- COMPATIBILE CON INCL.

$M_{R^{-1}} = M_R^T$ $\longrightarrow$ INVERSIONE: - $R \subseteq T \Rightarrow R^{-1} \subseteq T^{-1}$
- $(RT)^{-1} = T^{-1}R^{-1}$
- $(R\cap T)^{-1} = R^{-1}\cap T^{-1}$ / $(R\cup T)^{-1} = R^{-1}\cup T^{-1}$

$R \subseteq A\times A$
$R^n = \prod_n R \quad n>0 \qquad R^0 = I \longrightarrow M_{R^n} = M_R^n$

SERIALE	$\forall a\in A \ \exists a_1 \in A : (a,a_1)\in R$
RIFLESSIVA	$\forall a \in A \ (a,a)\in R \iff I \subseteq R$
SIMMETRICA	$\forall a_1,a_2 \in A \ (a_1,a_2)\in R \Rightarrow (a_2,a_1)\in R \iff R^{-1}\subseteq R$
ANTISIMMETRICA	$\forall a_1,a_2 \in A \ (a_1,a_2)\in R,\ (a_2,a_1)\in R \Rightarrow a_1 = a_2 \iff R\cap R^{-1}\subseteq I$
TRANSITIVA	$\forall a_1,a_2,a_3 \in A \ (a_1,a_2)\in R \wedge (a_2,a_3)\in R \Rightarrow (a_1,a_3)\in R \iff R^2 \subseteq R$

$T \subset R \subset S$

T	R	S
no	seriale	sì
no	riflessiva	sì
no	simmetrica	no
sì	antisimmetrica	no
no	transitiva	no

R	T	$R\cap T$	$R\cup T$	$R\cdot T$	R^{-1}
seriale	seriale	no	sì	sì	no
riflessiva	riflessiva	sì	sì	sì	sì
simmetrica	simmetrica	sì	sì	no	sì
antisimmetrica	antisimmetrica	sì	no	no	sì
transitiva	transitiva	sì	no	no	sì

* ordine di chiusura irrilevante!

CHIUSURA RIFLESSIVA	$R \cup I$
" SIMMETRICA	$R \cup R^{-1}$
" TRANSITIVA	$\bigcup_{i>0} R^i$
" RIFLESSIVO-SIMMETRICA	chiudere riflessivamente e poi simmetricamente: * $R\cup R^{-1}\cup I$
" RIFLESSIVO-TRANSITIVA	chiudere riflessivamente e poi transitivamente: * $\bigcup_{i\geq 0} R^i$
" TRANSITIVO-SIMMETRICA	chiudere simmetricamente e poi transitivamente: $\bigcup_{i>0}(R\cup R^{-1})^i$
" D'EQUIVALENZA	$\bigcup_{i>0}(R\cup I \cup R^{-1})^i$
" D'ORDINE	R e la sua chiusura riflessivo-transitiva sono antisimmetriche

RELAZIONE D'EQUIVALENZA $\iff$ riflessiva, simmetrica, transitiva
- CLASSE D'EQUIVALENZA: $[a]_\rho = \{b\in A \mid a\rho b\}$
- PARTIZIONE D'INSIEME: $\{B_i\} : \bigcup B_i = A \wedge B_i \cap B_j = \emptyset \ \forall i,j \ i\neq j$
- INSIEME QUOZIENTE: $A/_\rho = \{[a]_\rho \mid a\in A\}$ → insieme delle parti

RELAZIONE D'ORDINE $\iff$ riflessiva, antisimmetrica e transitiva
- $\forall (a,b)\in A \ (a,b)\in \leq \vee (b,a)\in\leq \Rightarrow$ ordine totale
- $(a,b)\notin \leq \wedge (a,b)\notin\leq \Rightarrow (a,b)$ non confrontabili
- $(A,\leq)$ poset $\iff \leq$ rel. d'ordine
- $(A,\leq)$ insieme totalmente ordinato $\iff \leq$ rel. d'ordine totale
- MINIMO: $\forall a\in A \ m\leq a$ / MASSIMO: $\forall a\in A \ a\leq M$
- MINIMALE: $\forall a\in A \ a\leq m \Rightarrow a=m$ / MASSIMALE: $\forall a\in A \ M\leq a \Rightarrow M=a$
- $B\subseteq A$, $(A,\leq)$ poset:
  - MINORANTE: $m\in A \ \forall b\in B \ m\leq b$ / MAGGIORANTE: $M\in A \ \forall b\in B \ b\leq M$
  - inf B : massimo dei minoranti / sup B : minimo dei maggioranti
- RETICOLO: $\forall (a,b)\in A \ \exists \inf\{a,b\} \wedge \exists \sup\{a,b\}$

FUNZIONE: $R \subseteq A \times B$ funzione $\iff \forall a \in A\ \exists^! b \in B : (a,b) \in R$ $\quad b = f(a)$

- INIETTIVA: $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
  - $f \cdot g$ iniettiva $\Rightarrow f$ iniettiva ; f, g iniettive $\Rightarrow f \cdot g$ è iniettiva
- SURIETTIVA: ogni elemento di B ha almeno una controimmagine
  - $f \cdot g$ suriettiva $\Rightarrow g$ suriettiva ; f, g suriettive $\Rightarrow f \cdot g$ suriettiva
- BIETTIVA: è iniettiva e suriettiva ; $f^{-1} : B \to A$ è una funzione
- INVERSA: $g : f \cdot g = g\ f = I$ ↪ RELAZIONE INVERSA!
  - INVERSA SINISTRA: $S : S \cdot f = I \to \exists S \iff f$ è suriettiva
  - INVERSA DESTRA: $D : f \cdot D = I \to \exists D \iff f$ è iniettiva

  se biettiva $\exists S, D$ e $S = D = g = f^{-1}$
- NUCLEO: $a_1 \operatorname{Ker} f\ a_2 \iff f(a_1) = f(a_2)$ → relazione di equivalenza
  - PROIEZIONE CANONICA: $P_\rho : A \to A/\rho$: $\operatorname{Ker} P_\rho = \rho$ → $a \mapsto P_a \to P_\rho(a) = [a]_\rho$
- FATTORIZZAZIONE: $f : A \to B$, $\operatorname{Ker} f$, $P_{\operatorname{Ker} f} : A \to A/\operatorname{Ker} f$, $\exists^! g : A/\operatorname{Ker} f \to B$: $P_{\operatorname{Ker} f} \cdot g = f$

  $g : A/\operatorname{Ker} f \to B$, $\operatorname{Ker} f_a \mapsto f(a)$ →
$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "P_{\operatorname{Ker} f}"'] & & B \\ & A/\operatorname{Ker} f \arrow[ur, "g"'] & \end{tikzcd}$$
  - g iniettiva $\vee$ f suriettiva $\Rightarrow g$ biunivoca

- CARDINALITÀ: $|A| = |B| \Rightarrow \exists f : A \to B$ biunivoca
  - $|A| \leq |B| \Rightarrow \exists f : A \to B$ iniettiva ($|A| < |B|$ se $\exists f$ iniettiva e $\nexists g$ biunivoca)
  - FINITO: $|A| = |\{1, \dots, n\}|$ / INFINITO: $\exists g : A \to B \subseteq A$ biunivoca / NUMERABILE: $|A| = |\mathbb{N}|$
  - CONTINUO: $|A| = |\mathbb{R}|$ / T. CANTOR: $|A| \leq |\mathcal{P}(A)|$ → insieme delle parti

LOGICA PROPOSIZIONALE

FBF: A è FBF ; $\mathcal{A}$ FBF $\Rightarrow \neg\mathcal{A}, \mathcal{A} \vee \mathcal{B}, \mathcal{A} \wedge \mathcal{B}, \mathcal{A} \Rightarrow \mathcal{B}, \mathcal{A} \iff \mathcal{B}$ FBF

PRECEDENZA: $\sim \ \geq \ \wedge \ \geq \ \vee \ \geq \ \Rightarrow \ \geq \ \iff$ / ASSOCIATIVITÀ A SX

INTERPRETAZIONE: $v : \text{FBF} \to \{0,1\}$ che soddisfi:
- $v(\top) = 1$ / $v(\bot) = 0$ / $v(\neg\mathcal{A}) = 1 - v(\mathcal{A})$
- $v(\mathcal{A} \vee \mathcal{B}) = \max(v(\mathcal{A}), v(\mathcal{B}))$ / $v(\mathcal{A} \wedge \mathcal{B}) = \min(v(\mathcal{A}), v(\mathcal{B}))$
- $v(\mathcal{A} \Rightarrow \mathcal{B}) = v(\neg\mathcal{A} \vee \mathcal{B})$ / $v(\mathcal{A} \iff \mathcal{B}) = v[(\neg\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{A} \vee \neg\mathcal{B})]$

FBF PUÒ ESSERE: Espandibile per insiemi di FBF Γ ↰
- SODDISFACIBILE: $\exists v : v(\mathcal{A}) = 1 \to v$ è MODELLO / INSODDISFACIBILE: $\nexists v : v(\mathcal{A}) = 1$
- TAUTOLOGIA: $\forall v\ v(\mathcal{A}) = 1 \to \models \mathcal{A}$
- CONS. SEMANTICA: $\mathcal{A} \models \mathcal{B} \Rightarrow \forall v\ v(\mathcal{A}) = 1 \Rightarrow v(\mathcal{B}) = 1$; $\Gamma \models \mathcal{A} \Rightarrow \forall v\ v(\Gamma) = 1 \Rightarrow v(\mathcal{A}) = 1$

DEDUZIONE SEMANTICA: $\mathcal{A} \models \mathcal{B} \iff \mathcal{B} \Rightarrow \mathcal{A}$ / $\mathcal{A} \models \Gamma \cup \{\mathcal{B}\} \iff \Gamma \models \mathcal{B} \Rightarrow \mathcal{A}$
- $\mathcal{A} \models \Gamma \iff \Gamma \cup \{\neg\mathcal{A}\}$ insodd. / Γ sodd. $\iff \forall \gamma \subseteq \Gamma$ sodd. / $\exists \gamma \in \Gamma$ insod. $\Rightarrow \Gamma$ insod.

EQUIVALENZA SEMANTICA: $\mathcal{A} \equiv \mathcal{B} \iff \mathcal{A} \models \mathcal{B}$ e $\mathcal{B} \models \mathcal{A}$ (tutti i modelli di $\mathcal{A}$ lo sono di $\mathcal{B}$)

$\neg(\neg A) = A \quad A \overset{\vee}{\wedge} A = A \quad A \overset{\vee}{\wedge} B = B \overset{\vee}{\wedge} A \quad (A \overset{\vee}{\wedge} B) \overset{\vee}{\wedge} C = A \overset{\vee}{\wedge} (B \overset{\vee}{\wedge} C) \quad A \overset{\vee}{\wedge} (A \overset{\wedge}{\vee} B) = A$

$A \overset{\vee}{\wedge} (B \overset{\wedge}{\vee} C) = (A \overset{\vee}{\wedge} B) \overset{\wedge}{\vee} (A \overset{\vee}{\wedge} C) \quad \neg(A \overset{\vee}{\wedge} B) = \neg A \overset{\wedge}{\vee} \neg B \quad A \vee \neg A = 1 \quad A \wedge \neg A = 0$

$\mathcal{A}$ deducibile da Γ

DEDUCIBILE: $\Gamma \vdash_H \mathcal{A}$ se $\exists$ sequenza finita assiomi o formule di Γ la cui ultima è $\mathcal{A}$

TEORIA L: corretta e completa: $\vdash_H \mathcal{A} \iff \models \mathcal{A}$; decidibile
- ASSIOMI: $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$; $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$; $(\neg\mathcal{A} \Rightarrow \neg\mathcal{B}) \Rightarrow ((\neg\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow \mathcal{A})$
- INFERENZA: Modus Ponens: $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B} \vdash_L \mathcal{B}$
- CORRETT. E COMPLET.: $\Gamma \vdash_L \mathcal{A} \iff \Gamma \models \mathcal{A}$ / DEDUZIONE: $\Gamma \cup \{\mathcal{B}\} \vdash_L \mathcal{A} \iff \Gamma \vdash_L \mathcal{B} \Rightarrow \mathcal{A}$

RISOLUZIONE: verifica se $\mathcal{A}$ è una tautologia
- CLAUSOLA: $(A \vee B \vee \dots \vee N) \to \{A, B, \dots, N\}$ / FORMA A CLAUSOLE: congiunzione di clausole
- RISOLVENTE: $R = (C_1 - \{\ell\}) \cup (C_2 - \{\bar{\ell}\})$ / $C_1, C_2 \models R$
- RISOLUZIONE: Γ insodd $\iff \Gamma \vdash_R \square$ → $\Gamma \vdash_R \mathcal{A} \iff \Gamma \cup \{\neg\mathcal{A}\} \vdash_R \square$

LOGICA PREDICATIVA

TERMINI: costanti, variabili, $f(t_1, \dots, t_n)$ con t_i termine / F. ATOMICA: $A(t_1, \dots, t_n)$, t_i termini

FBF: formule atomiche; $\mathcal{A}$ FBF $\Rightarrow \neg\mathcal{A}, \forall x \mathcal{A}, \exists x \mathcal{A}$ FBF; $\mathcal{A}, \mathcal{B}$ FBF $\Rightarrow \mathcal{A} \overset{\wedge}{\vee} \mathcal{B}, \mathcal{A} \Rightarrow \mathcal{B}, \mathcal{A} \Leftrightarrow \mathcal{B}$ FBF

PRECEDENZA: $\neg, \forall, \exists \geq \wedge \geq \vee \geq \Rightarrow \geq \Leftrightarrow$ / ASS. A SX, QUANTIF. IN ORDINE

$\forall x \underbrace{A(f(x,y), f'(x,y))}_{\text{campo d'azione}}$

- VAR VINCOLATA: $x \in$ c. d'azione che la quantifica
- VAR LIBERA: non vincolata
- TERM. LIBERO RISP. A x: $\nexists$ x libera $\in$ c. d'azione su $\forall y \in t$
- FORM. CHIUSA: tutte le variabili sono vincolate

C. ESISTENZIALE: precedo $\mathcal{A}$ chiusa con $\exists x$ per ogni x var / C. UNIVERSALE: come esist. ma con $\forall x$

INTERPRETAZIONE: $\langle D, I \rangle$ D dominio, $I = \{ I_1 : a \mapsto b \in D,\ I_2 : f \mapsto \cdot : D \to D,\ I_3 : A \mapsto B \subseteq D \times D \}$

UNA FBF SI DICE:

- SODDISFACIBILE in $\langle D, I \rangle$: esiste assegnamento che la soddisfi
- VERA in $\langle D, I \rangle$: soddisfatta da ogni assegnamento
- FALSA in $\langle D, I \rangle$: nessun assegnamento la soddisfa

} chiusa $\Rightarrow$ vera o falsa

- VALIDA ($\models \mathcal{A}$): vera per ogni interpretazione
- INSODDISFACIBILE: falsa per ogni interpretazione $\rightarrow$ $\neg\mathcal{A}$ è valida
- FNP: ha tutti i quantificatori all'inizio (scomponibile in prefisso e matrice)
  - $\neg \forall x \mathcal{A} \equiv \exists x \neg \mathcal{A}$; $\neg \exists x \mathcal{A} \equiv \forall x \neg \mathcal{A}$
  - $\mathcal{A}(x)$ FBF con x libera e y libera per x, $\mathcal{A}[y/x]$ FBF con y sostituita a x libera; $\mathcal{B}$ FBF, y non libera in $\mathcal{B}$ e y libero per x in $\mathcal{A}(x)$.
    - $\forall x \mathcal{A}(x) \overset{\vee}{\wedge} \mathcal{B} \equiv \forall y (\mathcal{A}[y/x] \overset{\vee}{\wedge} \mathcal{B})$; $\exists x \mathcal{A}(x) \overset{\vee}{\wedge} \mathcal{B} \equiv \exists y (\mathcal{A}[y/x] \overset{\vee}{\wedge} \mathcal{B})$
    - $\forall x \mathcal{A}(x) \Rightarrow \mathcal{B} \equiv \exists y (\mathcal{A}[y/x] \Rightarrow \mathcal{B})$; $\exists x \mathcal{A}(x) \Rightarrow \mathcal{B} \equiv \forall y (\mathcal{A}[y/x] \Rightarrow \mathcal{B})$
    - $\mathcal{B} \Rightarrow \forall x \mathcal{A}(x) \equiv \forall y (\mathcal{B} \Rightarrow \mathcal{A}[y/x])$; $\mathcal{B} \Rightarrow \exists x \mathcal{A}(x) \equiv \exists y (\mathcal{B} \Rightarrow \mathcal{A}[y/x])$
- F. DI SKOLEM: è in FNP e ha solo universali
  - chiudo universalmente $\mathcal{A}$
  - finché ci sono esistenziali: sia x_s quant. da $\exists x_s$, sostituiscici $f^{s-1}(x_1, \dots, x_{s-1})$

DEDUZIONE SEMANTICA: $\Gamma \cup \{\psi\} \models \varphi \Leftrightarrow \Gamma \models \psi \Rightarrow \varphi$ $\rightarrow$ $\Gamma \models \varphi \Leftrightarrow \models \Gamma \Rightarrow \varphi$

RISOLUZIONE:

- FORMA A CLAUSOLE: in F.SK. con matrice $((L_1 \vee \dots L_n) \wedge (L_m, \dots, L_k) \dots)$
- RISOLVENTE: $\{l_1, \dots, l_n\} \in C_1 E_1$, $\{\bar{l}_{n+1}, \dots, \bar{l}_{n+m}\} \in C_2 E_2$, $R = (C_1 E_1 - \{l\})\sigma \cup (C_2 E_2 - \{\bar{l}\})\sigma$
- RISOLUZIONE: Γ insoddisf. $\Leftrightarrow \Gamma \vdash_R \square$ $\rightarrow$ $\Gamma \vdash_R \mathcal{A} \Leftrightarrow \Gamma \cup \{\neg \mathcal{A}\} \vdash_R \square$

TEORIA K

- ASSIOMI: [TEORIA L], $\forall x \mathcal{A}(x) \Rightarrow \mathcal{A}[t/x]$ (t libero per x) ; $\forall x (\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \forall x \mathcal{B})$
- INFERENZA: Modus ponens: $\mathcal{A}, \mathcal{A} \Rightarrow \mathcal{B} \vdash_K \mathcal{B}$; Generalizzazione: $\mathcal{A} \vdash_K \forall x \mathcal{A}$
- CORRETT. COMPL.: $\Gamma \models \mathcal{A} \Leftrightarrow \Gamma \vdash_K \mathcal{A}$ / DEDUZIONE: $\Gamma \cup \{\psi\} \vdash_K \varphi \Leftrightarrow \Gamma \vdash_K \psi \Rightarrow \varphi$

TEORIA CON UGUAGLIANZA: * ; $\forall x E(x,x)$; $E(x,y) \Rightarrow \mathcal{A}(x|x) \Rightarrow \mathcal{A}(x|y/x)$

↳ suddivisione arbitraria in due gruppi

STRUTTURE ALGEBRICHE

SEMIGRUPPO: $(A, \cdot)$ con $\cdot$ binaria interna, associativa, (commutativa) $\rightarrow$ POTENZE

- TEORIA SEMIGRUPPI: [TEORIA K], $\forall x \forall y \forall z (E(P(x, P(y,z)), P(P(x,y),z)))$ con $P(x,y) = x \cdot y$

MONOIDE: $(M, \cdot, e)$ con $(M, \cdot)$ semigruppo, e neutro rispetto a $\cdot$ $\rightarrow$ $a^0 = e$

- TEORIA MONOIDI: [SEMIGRUPPI], $\forall y (E(P(y,e),y) \wedge E(P(e,y),y))$

GRUPPO: $(G, \cdot, e, ^{-1})$ con $(G, \cdot, e)$ monoide, $\forall g \exists h : g \cdot h = h \cdot g = e$; h unico $h = g^{-1}$

- PROPRIETÀ: $(g^{-1})^{-1} = g$; $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$; $\exists! x = a^{-1} \cdot b$ soluzione di $a \cdot x = b$
- COND. SUFFICIENTI: $(A, \cdot)$ semigruppo
  - $\exists e : g \cdot e = g \wedge \exists h : g \cdot h = e$; $\exists e : e \cdot g = g \wedge \exists h : h \cdot g = e$
  - $\exists! x, y : a \cdot x = b \wedge y \cdot a = b$
- CANCELLAZIONE: $\forall a, b, c ((\overset{sx}{a \cdot b = a \cdot c \Rightarrow b = c}) \wedge (\overset{dx}{b \cdot a = c \cdot a \Rightarrow b = c}))$
- TEORIA GRUPPI: [MONOIDI], $\exists x (\forall g\ E(P(g,x), g) \wedge \forall g \exists h\ E(P(g,h), x))$

ANELLO: $(A,+,\cdot)$ con $(A,+)$ gruppo comm., $(A,\cdot)$ semigruppo, $+,\cdot$ con distributività
- TEORIA ANELLI: [GRUPPO COMM.], $\forall a,b,c\ E(P(a,S(b,c)), S(P(a,b),P(a,c)))$
- UNITÀ: $(A,\cdot)$ monoide $\Rightarrow$ anello ha unità 1
- ZERO: elemento neutro di $(A,+)$ ed è zero di $(A,\cdot)$ / ZERO: unico z zero se $\forall s\ s\cdot z = z\cdot s = 0$
  - l'unità di $(A,+)$ è zero di $(A,\cdot)$ / $\forall a,b\ a(-b) = (-a)b = -(ab)$
  - DIVISORE DELLO ZERO: $a\neq 0\ b\neq 0: ab=0$
  - LEGGI DI CANCELLAZIONE: $\forall a\neq 0, b,c\ ((ab=ac \Rightarrow b=c)\wedge(ba=ca\Rightarrow b=c))$
    - $\nexists$ divisori dello zero $\Leftrightarrow$ valgono le leggi di cancellazione

CORPO: anello con $(A-\{0\},\cdot)$ gruppo / CAMPO: corpo con $(A-\{0\},\cdot)$ gruppo abeliano

SOTTOSTRUTTURA: (A,Ω) str., $H\subseteq A$ se (H,Ω) str. esso è sottostruttura di (A,Ω)
- $(H,\cdot)$ sottosemigr. $\Leftrightarrow \forall a,b\in H\ a\cdot b\in H$
- $(H,\cdot,e)$ sottomonoide $\Leftrightarrow (H,\cdot)$ sottosemigr. $\wedge\ e\in H$
- $(H,\cdot,e,^{-1})$ sottogr. $\Leftrightarrow \forall a,b\ (a\cdot b\in H \wedge a^{-1}\in H)$; $\forall a,b\ (a\cdot b^{-1}\in H)$; A finito $\Rightarrow \forall a,b\ a\cdot b\in H$
- $(H,+,\cdot)$ sottoanello $\Leftrightarrow \forall a,b\ (a+(-b)\in H \wedge a\cdot b\in H)$, $\forall a,b\ (a+b\in H\wedge -a\in H\wedge a\cdot b\in H)$

CONGRUENZA: $\rho\overset{\text{EQ.}}{\subseteq} A\times A$, (A,Ω) str. ρ è congruenza se compatibile $\forall * \in\Omega$
- COMPATIBILE: $a_1\rho b_1 \wedge a_2\rho b_2 \Rightarrow (a_1+a_2)\rho(b_1+b_2)$; $[a_1]_\rho=[b_1]\wedge[a_2]_\rho=[b_2]\Rightarrow[a_1+a_2]_\rho=[b_1+b_2]_\rho$
- OP. INDOTTA: (A,Ω) str, $\bullet\in\Omega$, ρ congr. $\bullet_\rho: A/\rho\times A/\rho\to A/\rho$ $\quad [a]_\rho\bullet[b]_\rho\mapsto[a\bullet b]_\rho$
- STR. QUOZIENTE: $(A/\rho,\Omega_\rho)$ con $\Omega_\rho=\{\bullet_\rho, \bullet\in\Omega : [a]_\rho\cdot[b]_\rho=[a\cdot b]_\rho\}$

OMOMORFISMI: funzione tra strutture "simili" che preserva le operazioni
- MONOMORFISMO → INIETTIVA / EPIMORFISMO → SURIETTIVA / ISOMORFISMO → BIETTIVA
- CRITERIO GRUPPI: $(G,+),(H,\cdot)$ gruppi, $f:G\to H$ isomorf $\Leftrightarrow \forall g_1,g_2\ f(g_1+g_2)=f(g_1)\cdot f(g_2)$
- CRITERIO ANELLI: $(A,+,\cdot),(B,\oplus,\odot)$ anelli, $f:A\to B$ omomorf se e solo se
  $\forall a,b\ f(a\cdot b)=f(a)\odot f(b)\ \wedge\ \forall a,b\ f(a+b)=f(a)\oplus f(b)$
- CONGR.-OMOMORF.: (A,Ω), ρ congr, $\pi_\rho: a\mapsto[a]_\rho$ epimorfismo canonico;
  $(A,\Omega),(B,\Omega)$, $f:A\to B$ omomorf., Ker f congruenza su (A,Ω)
- FATTORIZZAZIONE 1: $\varphi:A\to B$ omomorf, $\rho=\mathrm{Ker}\,\varphi$ congr su A, $\exists!\ g: A/\rho\to B$ monomorf: $\varphi=\pi_\rho\circ g$
  - φ è epimorfismo se e solo se g è isomorfismo

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "\rho"'] & & B \\ & A/\rho \arrow[ur, "g"'] & \end{tikzcd}$$

$g\cdot H\cdot g^{-1}\subseteq H$

SOTTOGRUPPI NORMALI: $(H,\cdot)$ sottogr. normale di G se $\forall g\ \exists h: g\cdot h\cdot g^{-1}\in H$
- se G abeliano, tutti i sottogruppi sono normali
- se ρ congruenza, $[e_G]_\rho$ è sottogruppo normale / $\forall\rho\ \exists H$ sottogr. norm /
- $\rho_H: x\rho_H y \Leftrightarrow x\cdot y^{-1}\in H$ / $H=[e_G]_{\rho_H}$
- ρ_H, $H=[e_G]_\rho$ sottogr. norm: $[g]_\rho=H\cdot g$ laterale destro e $[g]_\rho=g\cdot H$ laterale sinistro
  - $[g]_\rho=H\cdot g=g\cdot H$

IDEALI: sottoanello che soddisfa assorb.: $\forall a\ I\cdot a\subseteq I\wedge a\cdot I\subseteq I$
- $\rho: A\to A$ posso associare $I=[0]_\rho$; I ideale posso associare $\rho_I: a\rho_I b \Leftrightarrow a+(-b)\in I$, $[0]_\rho=I$
- $I=[0]\Rightarrow[a]_\rho=I+a=a+I$

MODULO: $x\equiv_n y \Leftrightarrow \exists K\in\mathbb{Z}\ x-y=Kn$; equivalenza: $\mathbb{Z}/\equiv\ = \mathbb{Z}_n$, $[r]: r=x-Kn$
- $[x]_n+[y]_n=[x+y]_n$; $[x]_n[y]_n=[xy]_n$
- $(\mathbb{Z}_n,+)$ gruppo abeliano; $(\mathbb{Z}_n,+,\cdot)$ anello commutativo con unità