

• Una relazione di equivalenza è simmetrica, riflessiva e transitiva. é di ordine parziale se è riflessiva e transitiva ed antisimmetrica ( $a\rho b \wedge b\rho a \implies a=b$ ). • **Risoluzione equazione diofantea** : si ha  $ax+by=c$  (1) Bisogna prima verificare che l'equazione sia risolvibile, si calcoli quindi  $MCD(a,b)=d$ , se esso divide c, l'equazione ammette soluzione. (2) Usare l'algoritmo euclideo per trovare un'identità di Bézout per  $d$ , esprimendolo nella forma  $d=ax_0+by_0$ , utilizzeremo proprio tali coefficienti  $(x_0,y_0)$ . (3) Considero  $(\tilde{x},\tilde{y})=(\frac{c}{d}\cdot x_0,\frac{c}{d}\cdot y_0)$  (4) Le soluzioni saranno  $(\tilde{x}+k\cdot\frac{b}{d},\tilde{y}-k\cdot\frac{a}{d})$ . • Siano  $a=p_1^{h_1}p_2^{h_2}\dots p_s^{h_s}$  e  $b=p_1^{k_1}p_2^{k_2}\dots p_s^{k_s}$ , allora  $MCD(a,b)=p_1^{m_1}p_2^{m_2}\dots p_s^{m_s}$  e  $mcm(a,b)=p_1^{M_1}p_2^{M_2}\dots p_s^{M_s}$  con  $m=\min(h_i,k_i)$  e  $M=\max(h_i,k_i)$ . • **Proprietà anello** : (1)  $a\cdot(-b)=-(ab)=(-a)\cdot b$  (2)  $(-a)\cdot(-b)=ab$  (3)  $a\cdot(b-c)=(a\cdot b)-(a\cdot c)$ . • **Teorema**: Sia A un anello unitario con finiti elementi e privo di divisori dello zero. Allora A è un anello di divisione. • **Costruzione di  $\mathbb{Z}_n$**  : Considero la relazione  $a\sim b \iff a-b$  è divisibile per  $n$ . L'insieme  $\mathbb{Z}_n:=\mathbb{Z}/\sim$  è l'insieme delle classi di equivalenza. • Una **congruenza lineare** del tipo  $ax=b \bmod n$  è equivalente al risolvere l'eq. diofantea  $ax+ny=b$ . Un'eq. congruenziale ammette soluzione se e solo se  $MCD(a,n)$  divide  $b$ . La **funzione di Eulero** associa ad  $a$  il numero degli elementi coprimi con  $a$  minori di  $a$ . Se  $p$  è primo, allora  $\varphi(p^h)=p^h-p^{h-1}$ . Teo di Eulero : Se  $MCD(a,n)=1$  allora  $a^{\varphi(n)}\equiv 1 \bmod n$ . Picc. Teo di Fermat : Se  $p$  è primo  $\forall a \not\equiv 0 \bmod p \quad a^p\equiv a \bmod p$ . • **Costruzione di  $\mathbb{Z}$**  : si considera  $\mathbb{N}\times\mathbb{N}$  e la relazione  $(n,m)\sim(n',m') \iff n+m'=m+n'$  Si ha che  $\mathbb{Z}=\mathbb{N}\times\mathbb{N}/\sim$ . il prodotto :  $[(n,m)]\cdot[(n',m')]=[(nn'+mm',nm'+n'm)]$ . Ogni  $a,b\neq 0\in\mathbb{Z}$  esistono unici  $q,r$  tali che  $a=bq+r$  con  $0\leq r<|b|$ . • **Teo. cinese** un sistema cinese ha gli argomenti dei moduli co-primi fra loro e l'incognita ha come coefficiente 1 ( $x=c_k \bmod r_k$ ). Siano  $r_1,r_2\dots r_s$  gli argomenti dei moduli, sia  $R=r_1\dots r_s$  ed  $R_k=\frac{R}{r_k}$ . Sia  $t_k$  la sol di  $R_k t_k + r_k g_k = 1$ , e  $\bar{x}_k = c_k t_k$ . L'unica soluzione del sistema è  $\sum_{i=1}^s \bar{x}_i R_i$ . • Un'equazione in un sistema cinese  $x\equiv c \bmod rs$ , se  $MCD(r,s)=1$  diventa due equazioni  $\begin{cases} x\equiv c \bmod r \\ x\equiv c \bmod s \end{cases}$ . • **Costruzione di  $\mathbb{Q}$**  : Si considera  $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$  con la relazione  $(a,b)\sim(c,d) \iff ad=bc$ .  $\mathbb{Q}=\mathbb{Z}\times\mathbb{Z}\setminus\{0\}/\sim$ . Il prodotto è banale si moltiplicano le coordinate, somma :  $[(a,b)]+[(c,d)]=[(ad+bc,bd)]$ . • **Criterio sottogruppo normale** Sia  $h\in H$ ,  $H\trianglelefteq G \iff a* h * (a^{-1})\in H \forall a\in G$  • sugli **ordini**, si ha che  $o(g^s)=\frac{mcm(o(g),s)}{s}$ . La partizione fornita dalle classi laterali stabilisce una relazione  $a\rho_S b \iff \exists g\in G | a\in gH \wedge b\in gH$ . • sia  $\varphi$  un omomorfismo :  $o(\varphi(g))$  divide  $o(g)$ , se è iniettivo  $o(\varphi(g))=o(g)$ . • **Gruppo Simmetrico** due perm. sono coniugate se hanno la stessa struttura ciclica. Decomposizione in trasposizione :  $(a_1 \ a_2 \ a_3\dots a_n)=(a_1 \ a_n)\dots(a_1 \ a_3)(a_1 \ a_2)$ . Se  $\sigma_i(a)=b\wedge\tau(a)=s$  allora  $\tau\sigma_i\tau^{-1}(s)=\tau\sigma_i(a)=\tau(b)$  • **Teo. fond. omomorfismo** :  $f:G\rightarrow G'$  un omomorfismo. sappiamo che  $Ker f\trianglelefteq G$ , consideriamo il gruppo quoziente  $G/Ker f$ . Sia  $\pi:G\rightarrow G/Ker f | \pi(g)=gKer f$ . Esiste unico isomorfismo  $F:G/Ker f\rightarrow Im(G)$  tale che  $f=F\circ\pi$ .

• Sviluppo di laplace :  $\det(A) = \sum_{k=1}^n (-1)^{i+k} a_{ik} \det(A_{(i,k)})$ .  $A_{(i,k)}$  è la matrice  $A$  senza la riga  $i$  e la colonna  $j$ . • Sia  $S \in M_{n,m}$  una matrice a scala di  $n$  righe ed  $m$  colonne, di rango  $r$ , il sistema  $S\bar{x} = \bar{b}$  ha soluzione se e solo se le ultime  $m - r$  coordinate di  $\bar{c}$  sono 0, ed lo spazio delle soluzioni di  $S\bar{x} = \bar{0}$  ha dimensione  $n - r$ . • La matrice associata a T (applic. lineare) con scelta di basi  $\mathcal{B} = \{b_1 \dots, b_n\}$  ed  $\mathcal{E} = \{e_1 \dots, e_m\}$  e la matrice che ha come j-ma colonna le coordinate di  $T(b_j)$  nella base  $\mathcal{E}$ , ed è una matrice di di  $m$  righe e  $n$  colonne. • Due matrici  $A, B$  sono **simili** se  $\exists C | A = C^{-1}BC$ . Se  $M_{\mathcal{B},\mathcal{B}}$  è una matrice associata ad un'applicazione, nelle basi  $\mathcal{B}$  in partenza e  $\mathcal{B}$  in arrivo, allora è *simile* alla matrice  $M_{\mathcal{E},\mathcal{E}}$ , mi basta trovare  $M_{\mathcal{E},\mathcal{B}}$  e si ha che  $M_{\mathcal{B},\mathcal{B}} = M_{\mathcal{E},\mathcal{B}}^{-1} \cdot M_{\mathcal{E},\mathcal{E}} \cdot M_{\mathcal{E},\mathcal{B}}$ . • **proprietà del determinante** : (1) - se  $A_i = A_j \implies \det(A_1 \dots, A_i \dots, A_j \dots, A_n) = 0$  (2) -  $\det(A_1 \dots, \lambda A_i \dots, A_n) = \lambda \det(A_1 \dots, A_i \dots, A_n)$  (3) -  $\det(A_1 \dots, A_i + A_j \dots, A_n) = \det(A_1 \dots, A_i \dots, A_n) + \det(A_1 \dots, A_j \dots, A_n)$ . ne seguono : (i)-  $\det(A_1 \dots, \bar{0} \dots, A_n) = 0$  (ii)-  $\det(A_1 \dots, A_i \dots, A_j \dots, A_n) = \det(A_1 \dots, A_i \dots, A_j \dots, A_n)$  (iii)-  $\det(A_1 \dots, A_i \dots, A_j \dots, A_n) = (-1) \det(A_1 \dots, A_j \dots, A_i \dots, A_n)$ . • **Teo. di Rouché Capelli** Sia  $A$  una mat.  $n \times n$  e  $A\bar{x} = \bar{b}$  un sistema. Il sistema ha soluzione solo se  $\text{rg}(A) = \text{rg}(A|\bar{b})$ . Ammette unica soluzione solo se  $\text{rg}(A) = n$ .