• Sviluppo di laplace : $\det(A) = \sum_{k=1}^{n}(-1)^{i+k}a_{i_k}\det(A_{(i,k)})$. $A_{(i,k)}$ 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 $M_{\mathcal{B},\mathcal{B}} = M_{\mathcal{E},\mathcal{B}}^{-1} \cdot M_{\mathcal{E},\mathcal{E}} \cdot M_{\mathcal{E},\mathcal{B}}$. • **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 Bèzout per d, esprimendolo nella forma $d = ax_0 + by_0$, utilizzeremo proprio tali coefficenti (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 $(\tilde{x} + k \cdot \frac{b}{d}, \tilde{y} - k \cdot {}^{a}/_{d})$.• 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) $a \cdot (b-c) = (a \cdot b) - (a \cdot c)$. **Costruzione di** $\mathbb{Z}_n$: Considero la relazione $a \sim b \iff a - b$ è divisbile per n. L'insieme $\mathbb{Z}_n := {}^{\mathbb{Z}}/_{\sim}$ è l'insieme delle classi di equivalenza. • Una **congruenza lineare** del tipo $ax = b \mod n$ 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 $a^{\varphi(n)} = 1 \mod n$. Picc. Teo di Fermat : Se p è primo $\forall a \quad a^p = a \mod p$. • **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 ($x = c_k \mod r_k$). Siano $r_1, r_2 \dots r_s$ gli argomenti dei moduli, sia $R = r_1 \cdot ... r_s$ 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 $x = c \mod rs$, se $MCD(r,s) = 1$ diventa due equazioni $\begin{cases} x = c \mod r \\ x = c \mod s \end{cases}$. • **Costruzione** di $\mathbb{Q}$: Si considera $\mathbb{Z} \times \mathbb{Z}\backslash\{0\}$ con la relazione $(a,b) \sim (c,d) \iff ad = bc$. $\mathbb{Q} = {}^{\mathbb{Z}\times\mathbb{Z}\backslash\{0\}}/_{\sim}$. Il prodotto è banale si moltiplicano le coordinate, somma : $[(a,b)] + [(c,d)] = [(ad + bc, bd)]$. • Criterio sottogruppo normale $H \trianglelefteq G \iff a * h * (a^{-1}) \in H \forall a \in G$ • sugli **ordini**, si ha che $o(g^s) = \dfrac{mcm(o(g), s)}{s}$. • sia φ un omomorfismo : $o(\varphi(g))$ divide $o(g)$, se è iniettivo $o(\varphi(g)) = o(g)$.