fattorizzazione di f

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"'] & Y \\ X/\sim \arrow[r, hook, two heads, "\phi"', "\text{biettiva}"] & f(X) \arrow[u, "i"'] \end{tikzcd}$$

irriducibile

$a \in A \setminus A^\times \wedge a \neq 0$

$\forall b,c \in A,\ a=bc \Rightarrow b\in A^\times$ oppure $c \in A^\times$

primo primo $\Leftrightarrow$ irriducibile

$a \in A \setminus A^\times \wedge a \neq 0$

$\forall b,c \in A,\ a|bc \Rightarrow a|b$ oppure $a|c$

divisori di zero

A anello, $a \in A$ → in campo $\exists! = 0_A$

$\exists b \in A\setminus\{0\}$ t.c. $ab = 0_A$

complessi ($z = x+iy$)

opposto → $-x+i(-y)$

coniugazione → isomorfismo

$\bar z = x - iy = h(z)$

① $\overline{z+z'} = \bar z + \bar z'$

② $\overline{z\cdot z'} = \bar z \cdot \bar z'$

③ $\overline{-z} = -\bar z$

④ biezione → $h^{-1} = h$

eulero ($\theta \in \mathbb{R}$)

$e^{i\theta} = \cos\theta + i\sin\theta$

$e^{i\theta}\cdot e^{i\eta} = e^{i(\theta+\eta)}$

① $|e^{i\theta}| = 1$

② $(e^{i\theta})^{-1} = \overline{e^{i\theta}} = e^{-i\theta}$

assoluto

$|z| = \sqrt{z\bar z} = \sqrt{x^2+y^2}$

① $|z| = 0 \Leftrightarrow z = 0$

② $|zz'| = |z||z'|$

③ $|z+z'| \leq |z| + |z'|$

polare

$z = \rho e^{i\theta},\ \rho = \sqrt{x^2+y^2}$

$\bar z = z^{-1} \Leftrightarrow \rho = 1$

minimo comune multiplo

$m = mcm(m_1, \dots, m_\ell)$

① $m_1, \dots, m_\ell | m$

② $\exists m'$ t.c. se $m_1,\dots,m_\ell | m' \Rightarrow m | m'$

$mcm(a,b) = a\mathbb{Z} \cap b\mathbb{Z}$

lagrange

$\forall H < G\ \#H | \#G$ sottogruppo generato di G

$\forall d | n\ \exists! H_d < H$ t.c. $\#H_d = d$

anello commutativo unitario ∃ el neutro per ·

$(A, +, -, \cdot, 0, 1)$

① $\forall a,b \in A\ a+b = b+a$

② $\forall a,b,c \in A\ (a+b)+c = a+(b+c)$

③ $\forall a \in A\ a + 0_A = 0_A + a = a$ (∃ unico)

④ $\forall a \in A\ a + (-a) = 0_A$

⑤ $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

⑥ $a\cdot(b+c) = a\cdot b + a\cdot c$

⑦ $a \cdot 1_A = 1_A \cdot a = a$ (∃ unico)

⑧ $a\cdot b = b \cdot a$

$\forall a \in A\setminus\{0\}\ a \in A^\times \Rightarrow A$ è campo ($\mathbb{C}$, $K[X]$)

unico div di zero è $0_A \Rightarrow A$ è dominio

$\mathbb{Z}/n\mathbb{Z}$ dominio $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ campo $\Leftrightarrow n$ primo

massimo comun divisore

$(a,b) \in \mathbb{Z}^2$ con $(a,b) \neq (0,0)$

d è $MCD(a,b)$ se (∃ unico)

① $d|a \wedge d|b$

② $d' \in \mathbb{N}^*$ t.c. $d'|a \wedge d'|b \Rightarrow d'|d$

$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$

se $a,b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$ e $MCD(a,b) = 1$ $\Rightarrow a|bc \to a|c$

$MCD(a,b) = \prod_p p^{\min(v_p(a), v_p(b))}$

$MCD(a,b,c) | MCD(a,b)\cdot MCD(b,c)$

$a^x \equiv 1 \wedge a^y \equiv 1 \Rightarrow a^{MCD(x,y)} \equiv 1$

gruppi

$(G, *, e)$ ↳ 1 not molt, 0 not add

① $\forall a,b,c \in G\ a*(b*c) = (a*b)*c$

② $\forall a \in G\ a*e = e*a = a$

③ $\forall a \in G\ \exists a'$ t.c. $a*a' = e$

$(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$

sottogruppo

$H < G,\ \forall a,b \in H\ (ab^{-1}) \in H$

$Ker(f) := \{g \in G_1$ t.c. $f(g) = 1_{G_2}\} < G_1$

f omom, $Ker(f) \triangleleft G_1$

f omom, $Ker(f) = \{1_{G_1}\} \Leftrightarrow f$ iniettiva

$f(G_1) = \{y \in G_2$ t.c. $\exists x \in G_1$ con $f(x) = y\} < G_2$

sottogruppi di $\mathbb{Z}$ sono $\{0\}$ e $\{n\mathbb{Z}\}$

$\sigma = (a_1\ a_2 \dots a_m) = (a_m\ a_{m-1}) \dots (a_m\ a_1)$ NON unica (unica mod 2)

segnatura di σ omom $S_r \xrightarrow{\varepsilon} \mathbb{Z}^\times$

$\varepsilon(\sigma) = (-1)^s \in \mathbb{Z}^\times$ con s numero di trasposizioni della fatt di σ

fattorizzazioni

$H = \lambda \prod_{p \in A \text{ irr}} p^{v_p(H)}$, $\lambda \in A^\times$

in $\mathbb{R}[X]$: $H = \lambda \prod_{a \in \text{sol } H} (X-a)^{v_a(F)}$, $\lambda \in \mathbb{R}^\times$

in $K[X]$ campo: $\lambda \prod_{\substack{x \in K \\ (v_x \neq 0)}} (X-x)^{v_x(G)}$, $\lambda \in K^\times$

inverso

① $A^\times$ non è vuoto

② se $a \in A^\times$ allora $a^{-1} \in A^\times$

③ se $a,b \in A^\times \Rightarrow ab \in A^\times \to (ab)^{-1} = a^{-1}\cdot b^{-1}$

modulo

$a \equiv b \pmod n \Leftrightarrow n | a-b \wedge n | b-a$

① $\forall a,a' \in \mathbb{Z}\ a \equiv_n a' \Leftrightarrow -a \equiv_n -a'$

② $a,a',b,b' \in \mathbb{Z}\ a \equiv_n a' \wedge b \equiv_n b' \Rightarrow a+b \equiv_n a'+b'$

③ $a,a',b,b' \in \mathbb{Z}\ a \equiv_n a' \wedge b \equiv_n b' \Rightarrow ab \equiv_n a'b'$

$n^p \equiv_p n$ $n^{p-2} \equiv_p n^{-1}$ $n^{p-1} \equiv_p 1$ p primo

grado polinomio

$deg(P) := \max\{j \in \mathbb{N}$ t.c. $a_j \neq 0\}$

① $deg(a) = -\infty \Leftrightarrow a = 0$

② $deg(ab) = deg(a) + deg(b)$

③ $deg(a+b) \leq \max(deg(a), deg(b))$

④ $deg(a+b) = \max(deg(a), deg(b)) \Leftrightarrow deg(a) \neq deg(b)$

omomorfismo di gruppi

$f: G_1 \to G_2$ omomorfismo se

① $f(1_{G_1}) = 1_{G_2}$ ↳ iniettivo $\Leftrightarrow Ker(f)$ banale

② $\forall a \in G_1\ f(a^{-1}) = f(a)^{-1}$

③ $\forall a,b \in G_1\ f(ab) = f(a)f(b)$

omomorfismo $\Leftrightarrow f(ab) = f(a)f(b)\ \forall a,b \in G_1$

isomorfismo → f omomorfismo e f biettiva

sottogruppo coniugato

G e $H < G$ se G abeliano $H^g = H$

$H^g := \{g' \in G$ t.c. $\exists h \in H$ t.c. $g' = g^{-1}hg\} = gHg^{-1}$

$H^g < G$

$1 \triangleleft G$ $G \triangleleft G$

sottogruppo normale $H \triangleleft G$

$\forall x \in G\ xH = Hx$ ← i sottogruppi di un gruppo commutativo sono normali

condizioni equivalenti

① $H \triangleleft G$

② $\forall g \in G, \forall h \in H\ \exists h' \in H$ t.c. $gh = h'g$

③ $\forall g \in G,\ H^g = H$

$g \in G \Rightarrow \bar g = gH = Hg$ ($\pi_G = H$)

c-grado

sia $P \in A[X]\setminus\{0\}$ e $c > 1$

$|P|_c := c^{deg(P)}$

$|0|_c := 0 = c^{-\infty}$

① $|a|_c = 0 \Leftrightarrow a = 0$

② $|ab|_c = |a|_c \cdot |b|_c$

③ $|a+b|_c \leq \max(|a|_c, |b|_c) \leq |a|_c + |b|_c$

si trovano in un poligono regolare di n lati in cui sono presenti i vertici i, 1 e −1 se e solo se n è pari

$X^n - 1 = \prod_{i=0}^{n-1} (X - x_i)$ $x = \frac{2\pi i}{n}$ fattorizzato in $\mathbb{C}$

divisibilità (rifl, tran, NO simm/antis)

$a|b \Rightarrow \exists k \in A$ t.c. $b = ka$

se $a|b \wedge a|c \Rightarrow a|b+c$

$a,b,c \in \mathbb{Z}$ $a,b|c$ e $MCD(a,b) = 1 \Rightarrow ab|c$

$a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$

polinomi

$P = \sum_{i=0}^n a_i X^i$

monici → $a_n = 1$

$K[X]^\times = K^\times$

$MCD(P, P')$ è monico

valutazione omomorfismo

① $ev_x(F+G) = ev_x(F) + ev_x(G)$

② $ev_x(F\cdot G) = ev_x(F)\cdot ev_x(G)$

③ $\forall \lambda \in K\ ev_x(\lambda) = \lambda$

$ev_x^{-1}(\{0\}) = (X-x)K[X]$

radice in $x \Leftrightarrow X - x | P$

$deg(P) = 2n+1 \Rightarrow \exists x$ t.c. $ev_x(P) = 0$

campo è alg. chiuso se $\exists$ radice $\forall P \in K[X]$ (es $\mathbb{C}$)

alg chiuso $\Leftrightarrow$ poli irriducibili e monici $X - x$

K campo $\Rightarrow \exists L \supset K$ alg chiuso

sottogruppo generato più piccolo sottogruppo di G che contiene I

$I \neq \emptyset \subset G$ $\langle I \rangle := \bigcap_{\substack{H < G \\ I \subset H}} H$

G (not molt) $g \in G$ $\langle g \rangle = g^{\mathbb{Z}}$

G (not add) $g \in G$ $\langle g \rangle = g\mathbb{Z}$

$\#G < \infty \Rightarrow \forall g \in G\ \exists n > 0$ t.c. $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/ord(g)\mathbb{Z}$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d, "\pi"'] & G \\ \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/Ker(f) \arrow[r, hook, two heads, "\phi"] & f(\mathbb{Z}) = g^{\mathbb{Z}} = \langle g \rangle \arrow[u, "i"'] \end{tikzcd}$$

↳ sottogruppo normale

ordine di un elemento

G (notazione moltiplicativa)

$ord(g) := \min\{d \in \mathbb{N}^*$ t.c. $g^d = 1_G\}$

G (notazione additiva)

$ord(g) := \min\{d \in \mathbb{N}^*$ t.c. $g\cdot d = 0_G\}$

dato n-ciclo di S_r $\sigma \Rightarrow ord(\sigma) = n$

$ord(\sigma) = mcm(ord(c_1), \dots, ord(c_s))$ cicli disgiunti

soluzioni

CTR ha sol $\Leftrightarrow r_1, \dots, r_n$ coprimi, ed è unica mod $R := r_1 \cdot \dots \cdot r_n$ $E = x_0 + R\mathbb{Z}$

$ax + by = c$ ha sol se $MCD(a,b)|c$

$x = x_0 + \frac{b}{MCD(a,b)}\mathbb{Z}$

$ax \equiv_n y$ ha sol se $MCD(a,n)|y$

$aX = b$ in $\mathbb{Z}$ $\exists!$ sol

equazione diofantea $a_0x+b_0y=d$

$$\left\{\left(a_0-k\frac{y}{d},\ b_0+k\frac{x}{d}\right) \text{ t.c. } k\in\mathbb{Z}\right\}$$

$\mathbb{Z} \leftarrow d\,|\,x,y \rightarrow \mathbb{Z}$

spazio vettoriale

dato K campo e $V\neq\emptyset$ con operazione binaria $V\times V\longrightarrow V$, $(a,b)\longmapsto a+b$ e $K\times V\longrightarrow V$, $(\lambda,v)\longmapsto\lambda\cdot v$

V è uno s.v. su K se

1. $(V,+)$ gruppo abeliano $(e=0_V)$
2. $\alpha(v+w)=\alpha v+\alpha w$
3. $(\alpha+\beta)\cdot v=\alpha v+\beta v$
4. $(\alpha\beta)v=\alpha(\beta\cdot v)$
5. $1\cdot v=v$

sottospazio vettoriale contiene sempre 0

V s.v. su K, W sottospazio se

1. $W\subset V$ $(W\neq 0)$
2. $W\leq V$
3. $\forall w\in W\ \forall\lambda\in K\ \ \lambda w\in W$

definizioni alternative

1. $\forall w,w'\in W\ \ w+w'\in W$
2. $\forall w\in W,\ \lambda\in K\ \ \lambda w\in W$ → stabile per moltiplicazione

$\forall w,w'\in W\ \ \forall\lambda,\lambda'\in K\ \ \lambda w+\lambda' w'\in W$

$\forall w,w'\in W\ \ \forall\lambda\in K\ \ w+\lambda w'\in W$

sottospazio vett generato → sottosp di V

$$\langle v_1,\dots,v_n\rangle=Vett(\{v_1,\dots,v_n\})=\bigcap_{\substack{W\subseteq V \text{ sott}\\ W\supseteq\{v_1\dots v_n\}}} W$$

linearmente indipendenti

$\lambda_1v_1+\dots+\lambda_nv_n=0 \iff \lambda_1=\dots=\lambda_n=0$

colonne di $M\in\mathcal{M}_n(\mathbb{R})$ l.i. $\iff$
$\iff m_{11},m_{22},\dots,m_{nn}$ non nulli

prodotto di matrici

$$A=\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\quad B=\begin{pmatrix}1&4\\2&5\\3&6\end{pmatrix}$$

$$AB=\begin{pmatrix}1\cdot1+2\cdot2+3\cdot3 & 1\cdot4+2\cdot5+3\cdot6\\ 4\cdot1+5\cdot2+6\cdot3 & 4\cdot4+5\cdot5+6\cdot6\end{pmatrix}$$

$$BA=\begin{pmatrix}1\cdot1+4\cdot4 & 1\cdot2+4\cdot5 & 1\cdot3+4\cdot6\\ 2\cdot1+5\cdot4 & 2\cdot2+5\cdot5 & 2\cdot3+5\cdot6\\ 3\cdot1+6\cdot4 & 3\cdot2+6\cdot5 & 3\cdot3+6\cdot6\end{pmatrix}$$

sistema lineare prop

$Sol(A|b)$ sott di $\mathbb{R}^n \iff b=0$

$X_0\in Sol(A|b)\Rightarrow Sol(A|b)=X_0+Sol(A|0)$

per risolvere un sistema lineare basta ridurlo a gradini ridotti e prendere i nuovi coefficienti di b

rouché-capelli $AX=b$ (*)

(*) compatibile $\iff rg(A)=rg(A|b)$

se (*) compatibile $\Rightarrow \delta:=n-rg(A)$ (incognite)

riformulazione $M:=(A|b)$

1. (*) compatibile $\iff \dim(M^1,\dots,M^{n+1})=\dim(A^1,\dots,A^n)$
2. $\dim(Sol(A|0))=n-rg(A)$
3. $rg(A)=\dim(Vett(A_1,\dots,A_m))=\dim(Vett(A^1,\dots,A^n))$

sistema di generatori

se W sott e $W=Vett(S)\Rightarrow S\subset V$ è sistema di generatori per W

se $\exists S$ t.c. $W=Vett(S)\Rightarrow W$ è finitamente generato

base

W sottosp e $S\subset W$. base se

1. S sist di gen $W=Vett(S)$
2. S libero

$\forall\mathcal{B}_1\dots\mathcal{B}_n\ \ \#\mathcal{B}_1=\dots=\#\mathcal{B}_n=m$

dimensione

dato V/K f.g. $\dim_K(V)=\#\mathcal{B}_V$

prop 1

$\forall\ V/K\ \ \exists\mathcal{B}\subset V$

date $\mathcal{B},\mathcal{B}'\subset V\Rightarrow\exists f:\mathcal{B}\hookrightarrow\!\!\!\!\rightarrow\mathcal{B}'$

prop 2

se W sott di V f.g. e $\dim(V)=n\Rightarrow W$ f.g. e $\ell:=\dim(W)$ $\ell\leq n$

$\mathcal{B}_V$ contiene almeno tutte le $\mathcal{B}$ dei sott

prop 3

V s.v. su K di dim n

1. S libero $\Rightarrow\#S<\infty$ e $\#S\leq n$
2. S generatore $\Rightarrow$ o $\#S=\infty$ o $\#S<\infty$ con $\#S\geq n$
3. S base $\iff\#S<\infty,\ \#S=n$, S libero $\iff\#S<\infty$, $\#S=n$, S generatore

prop 4 V/K s.v.

$\{v_1\dots v_n\}$ base $\iff\forall v\in V\ \exists!$ comb. lin. di $v_1\dots v_n$ che la descrive

trasposizioni di matrici

$$A=\begin{pmatrix}\boxed{\begin{matrix}1\\3\\5\end{matrix}}&\begin{matrix}2\\4\\6\end{matrix}\end{pmatrix}\ (A^1)\quad\in\mathcal{M}_{3,2}(\mathbb{R})$$

$$^tA=\begin{pmatrix}\boxed{1\ \ 3\ \ 5}\\2\ \ 4\ \ 6\end{pmatrix}\ ((^tA)_1)\quad\in\mathcal{M}_{2,3}(\mathbb{R})$$

$rg(A)=rg(^tA)$

1. $^t(^tA)=A$
2. $^t(\alpha A+\beta B)=\alpha\,^tA+\beta\,^tB$
3. $^t(AB)=\,^tB\,^tA$

matrice simmetrica

simm se $A=\,^tA$

antisimm se $A=-\,^tA$

matrice inversa

C'è equivalenza tra:

1. $A\in GL_n(K)$ (A invertibile)
2. $rg(A)=n$ → senza zeri (base) — trasformabile in gradini ridotta
3. le righe di A sono una base di K^n
4. le colonne di A sono una base di K^n ↑ base mantenuta in ^tA

vettore delle coordinate di v sulla base $\mathcal{B}$

dato $v=\lambda_1b_1+\dots+\lambda_nb_n$ allora $\begin{pmatrix}\lambda_1\\\vdots\\\lambda_n\end{pmatrix}\in K^n$ è $[v]_{\mathcal{B}}$

applicazione lineare

$f: V\longrightarrow V'$

$f(x+\lambda y)=f(x)+\lambda f(y)$ oppure $f(\alpha v+\alpha'v')=\alpha f(v)+\alpha' f(v')$

f biettiva $\Rightarrow f$ isomorfo $(V\cong V')$ → lineare

restrizione del dominio su $\mathcal{B}$

V/K s.v. f.g. e $f:\mathcal{B}\to V\Rightarrow\exists!\ \tilde f: V\longrightarrow V'$ t.c. $\tilde f|_{\mathcal{B}}=f$

immagine e nucleo

$Ker(f)=\{v\in V \text{ t.c. } f(v)=0\}=f^{-1}(\{0\})$

$Im(f)=\{v'\in V' \text{ t.c. } \exists v\in V\ f(v)=v'\}$

$Ker(f)$ e $Im(f)$ sottosp vett

somma di sottospazi vettoriali V_1,V_2 sott di V

$V_1+V_2=\{v\in V \text{ t.c. } \exists\ v_1\in V_1, v_2\in V_2 \text{ t.c. } v=v_1+v_2\}$

$$V_1+V_2=\bigcap_{\substack{W \text{ sott di } V\\ W\supseteq V_1\cup V_2}} W$$

V_1+V_2 sott di V

formula di Grassmann

$\dim(V_1)+\dim(V_2)=\dim(V_1+V_2)+\dim(V_1\cap V_2)$

lemma $f: V\longrightarrow V'$ $\dim(V)=n\Rightarrow\dim(Ker(f))+\dim(Im(f))=n$

CRT: 1) ridurre solo x a sx
2) R, Ri 3) Si = inv. Ri mod ri
4) yi = Si ci 5) x0 = yiRi
6) E = x0 + RZ

Dato $f: G_1\to G_2$ omom, $Ker(f)\lhd G_1$

d: $h\in Ker(G_1)$, $f(x^{-1}hx)=1_{G_2}$

$H\lhd G\implies H=Ker(\pi_H)$

$\pi_H(g)=1_{G/H}=H\iff gH=H\iff g\in H$

primo teorema isomorfismo:

$$\begin{tikzcd} G_1 \arrow[r, "f"] \arrow[d, "\pi"'] & G_2 \\ G_1/\sim \arrow[r, hook, two heads, "\varphi"] & f(G_1) \arrow[u, "i"'] \end{tikzcd}$$

$G_1/Ker(f)$

$x\sim x'\iff x(x')^{-1}\in H$

perché il quoziente assuma una struttura di gruppo, serve che H sia normale

~ è una relazione di equivalenza ed è equivalente a R (per H ker)

$xRx'\iff f(x)=f(x')$