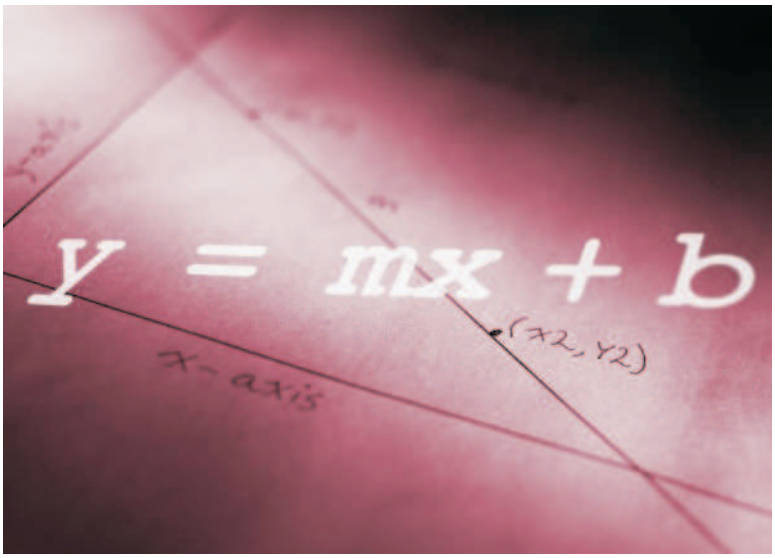
Appunti di Algebra I



Paolo Magoni, Luca Nizzardo, Federico Pasini, Andrea Savoldi

Indice

Prefazione

Nelle seguenti pagine abbiamo riscritto parte degli appunti presi durante le lezioni di Algebra I, svolte dal prof. Thomas Weigel, nell'Anno Accademico 2007/8, integrandoli laddove ritenuto utile.

Il testo, sebbene a un livello introduttivo compatibile col programma di un primo corso in materia, fornisce una panoramica delle principali *strutture algebriche* che qualsiasi studente di Matematica deve assimilare per il proseguimento dei suoi studi.

L'algebra moderna studia i prodotti che si ottengono manipolando gli elementi di un insieme secondo determinate caratteristiche, ovvero costruendo su quell'insieme *mappe* che godono di specifiche proprietà; una struttura algebrica è perciò un 'intreccio' indissolubile fra insiemi e funzioni, che in questo campo non si possono studiare separatamente: un cambiamento di una delle due componenti porta inevitabilmente a una modifica, magari radicale, dell'oggetto che si sta osservando. Affermare la presenza di un 'gruppo' è qualcosa di più che dichiarare l'esistenza di un insieme G e l'esistenza di una funzione dal prodotto cartesiano $G \times G$ in G: la funzione costruisce su G un'architettura che permette di manipolare gli elementi di G in un modo essenzialmente unico, ed è in questa architettura tutto l'interesse dell'algebra.

Ci siamo sforzati per far risaltare questo aspetto, indicando (laddove si potesse dare adito ad un'errata interpretazione) nella forma completa *insieme–funzione* ogni nuovo oggetto introdotto e differenziando esplicitamente le varie operazioni, anche qualora definissero la medesima struttura (non si dirà quindi 'sia $\mathbb{K}$ un campo', bensì 'sia $(\mathbb{K}, +, \cdot)$ un campo': $\mathbb{K}$ è un insieme, $+$ e $\cdot$ sono due operazioni; se si introdurrà un'altra struttura di campo sullo stesso insieme, sarà dichiarata ad esempio come 'il campo $(\mathbb{K}, \oplus, \odot)$' e nel seguito le operazioni saranno mantenute distinte).

Talvolta ciò potrebbe sembrare deleterio nei confronti della scorrevolezza, ma siamo sicuri che, specialmente quando nel procedere della lettura le strutture e le mappe che servono a definirle si moltiplicano, il lettore apprezzerà il guadagno in chiarezza. Non solo: ci auguriamo che grazie a tali accorgimenti gli studenti che affrontano il primo impatto con l'algebra sviluppino fin da subito le capacità di discernere chiaramente l'area di pertinenza degli oggetti manipolati e di comprendere e apprezzare il ruo-

lo che ciascun singolo oggetto riveste, nel suo piccolo, nel concerto di una definizione o un teorema.

Ciascuna unità in cui è suddiviso il testo, sia essa una definizione, una proposizione o anche un singolo esempio, se non diversamente indicato, è strutturata in modo da essere dotata di completezza e autonomia rispetto alle altre, cioè ciascuna si apre con la dichiarazione degli oggetti di cui abbisogna ed essi cessano di valere al termine dell'unità; ancora una volta il fine che ci proponiamo è la massima chiarezza espositiva.

Ad eccezione di alcuni risultati dell'ultimo capitolo, di importanza indubbia ma di natura inadatta a un corso di base, tutte le proposizioni sono corredate da dimostrazione.

Dopo una breve introduzione concernente insiemi e funzioni, il testo si apre con lo studio dei gruppi; un capitolo è riservato alle azioni di gruppo; si passa quindi alle strutture con più operazioni: ad anelli, domini d'integrità e campi è dedicato il capitolo 3; si conclude infine con una breve trattazione dei moduli.

La stesura è stata completata nel Marzo del 2009.

Ci scusiamo per eventuali errori presenti nel testo.

P.Magoni, L. Nizzardo, F. Pasini, A. Savoldi

Capitolo 1

Insiemi, relazioni, funzioni

1.1 Insiemi

Prima di tutto, assumeremo come primitiva la nozione di insieme, così come si impara alle elementari: un'insieme è una famiglia (o collezione) di elementi due a due distinti. Non ci addentremo oltre riguardo il concetto di "insieme" in quanto esula dagli obiettivi di questo insegnamento.

Esempi 1.1.

1. $\{\} = \varnothing$ (insieme vuoto);
2. $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$;
3. $\mathbb{R}$
4. Sia X un insieme. Allora $\mathcal{P}(X) = \{\mathcal{A} \mid \mathcal{A} \subseteq X\}$ è l'insieme delle parti.

Richiamiamo ora un paio di concetti che torneranno utili in seguito: cardinalità di un insieme e prodotto fra insiemi.

Cardinalità Si dice che due insiemi X e Y hanno la stessa *cardinalità* se esiste una mappa biettiva $\beta : X \longrightarrow Y$. La cardinalità di un insieme X si indica con il simbolo $|X|$.

Insiemi prodotto Si considerino due insiemi $X, Y (X \neq \varnothing \wedge Y \neq \varnothing)$. L'insieme delle coppie ordinate (x, y) con $x \in X \wedge y \in Y$ viene chiamato *prodotto cartesiano* di X e Y e lo si indica con il simbolo $X \times Y$.
Estendiamo ora la nozione di prodotto di insiemi a una famiglia qualsiasi di insiemi: sia $(X_i)_{i \in I}$ una famiglia di insiemi (I insieme). Allora
$\times X_i = \{(x_i)_{i \in I} \mid x_i \in X_i\}$ è l'*insieme prodotto* di $(X_i)_{i \in I}$.

Esempi 1.2.

1. $R^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \times(\mathbb{R}_i)_{i \in \{1,2,3\}}$ con $\mathbb{R}_i = \mathbb{R}$;
2. Sia $I \subseteq \mathbb{R}$ un intervallo e sia $S^1 \subseteq \mathbb{R}^2$ la sfera in due dimensioni. Allora $I \times S^1$ rappresenta il *cilindro* e $S^1 \times S^1$ il *toro*.

1.2 Relazioni

Definizione 1.1. Sia X un insieme non vuoto. Una *relazione* $\sim$ è una mappa di $X \times X$ in $\{v, f\}$ (vero o falso). Scriviamo $x \sim y$ se $\sim(x, y) = v$.

Definizione 1.2. Sia X un insieme non vuoto.

- Una relazione $\sim$ su X si dice *relazione d'equivalenza* se $\sim$ è:
  (r) riflessiva: $\forall\, x \in X \Longrightarrow x \sim x$;
  (s) simmetrica: $\forall\, x, y \in X$ t.c $x \sim y \Longrightarrow y \sim x$;
  (t) transitiva: $\forall\, x, y, z$ t.c. $x \sim y \wedge y \sim z \Longrightarrow x \sim z$.
- Sia $\sim$ una relazione d'equivalenza e sia $x \in X$. Allora
$$[\, x \,] = \{y \in X \mid y \sim x\}$$
si dice la *classi di equivalenza* che contiene x.
- Nelle ipotesi precedenti
$$X/\sim = \{[\, x \,] \mid x \in X\} \subseteq \mathcal{P}(X)$$
si dice *spazio quoziente* (modulo $\sim$) o insieme delle classi di equivalenza.
- La mappa $\tau_\sim : X \longrightarrow X/\sim$, $\tau_\sim = [\, x \,]$ si dice la *mappa canonica* o mappa quoziente. Questa mappa è suriettiva.
- Una mappa $\sigma : X/\sim \longrightarrow X$, $[\, \sigma([\, x \,])] = [\, x \,]$ si dice una *sezione* di $\sim$.

L'esistenza della sezione è garantita dall'*assioma della scelta*, il cui enunciato stabilisce che: data una famiglia non vuota di insiemi non vuoti esiste una funzione che ad ogni insieme della famiglia fa corrispondere un suo elemento.
Assioma della scelta Sia X un insieme e sia $M \subseteq \mathcal{P}(X)$. Allora $\exists$ una funzione $f : M \longrightarrow X$ t.c. per$S \in M$ vale $f(S) \in S$.

Definizione 1.3. Sia X un insieme non vuoto con una relazione di equivalenza $\sim$. Un sottoinsieme $\mathcal{R} \subseteq X$ si dice *sistema di rappresentanti* se $\forall\, x \in X \quad |\mathcal{R} \cap [\, x \,]| = 1$.

Proposizione 1.1. *Nelle ipotesi precedenti si ha* $X = \overset{\circ}{\bigcup}_{r \in \mathcal{R}} [\, r \,]$.

Dim. Ogni elemento di X appartiene ad una classe di equivalenza; bisogna solo mostrare che le classi di equivalenza sono disgiunte. Questo è banale, infatti se $a \sim b$, allora $[\, a \,] = [\, b \,]$ ovvero le due classi coincidono. Riassumendo, se due classi $[\, x \,]$ e $[\, y \,]$ non coincidono, esse sono disgiunte, cioè non hanno elementi in comune.

CVD

Proposizione 1.2. *Sia X un insieme e sia $\sim$ una relazione di equivalenza.*

(a) Sia $\sigma : X/\sim \longrightarrow X$ una sezione. Allora $\mathcal{R} = im(\sigma) = \sigma(X/\sim)$.

(b) Sia $\mathcal{R} \subseteq X$ un sistema di rappresentanti per $\sim$ e sia $r_{[x]} \in \mathbb{R}$ $\{r_{[x]}\} = \mathcal{R} \cap [\,x\,]$ per $[\,x\,] \in X/\sim$. Allora $\sigma : X/\sim \longrightarrow X$, $\sigma([\,x\,]) = r_{[\,x\,]}$ è una sezione.

Dim.

(a) Sia $\mathcal{R} = im(\sigma)$.$\mathcal{R} \cap [\,x\,] = \{\sigma([\,y\,]) \mid [\,y\,] \in X/\sim\} \cap [\,x\,] = \{\sigma([\,x\,])\}$.

(b) Sia $\sigma : X/\sim \longrightarrow X$ e sia $\tau_\sim : X \longrightarrow X/\sim$, $\tau_\sim(x) = [\,x\,]$. Allora

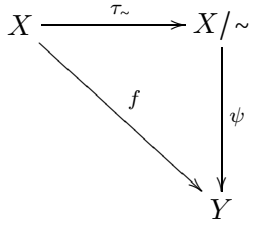
$$\tau_\sim \circ \sigma([\,x\,]) = \tau_\sim(r_{[\,x\,]}) = [\,r_{[\,x\,]}\,]$$

Per ipotesi $r_{[\,x\,]} \in [\,x\,] \Longrightarrow r_{[\,x\,]} \sim x \Longrightarrow [\,r_{[\,x\,]}\,] = [\,x\,] \Rightarrow \tau_\sim \circ \sigma = Id_{x/\sim}$.
Quindi σ è una sezione.

CVD

1.3 L'estensione di funzioni

Sia dato il seguente diagramma (ne incontreremo altri simili nel corso della trattazione):



Ci poniamo il seguente problema: quando $\exists\, \psi : X/\sim \longrightarrow Y$ t.c. $\psi \circ \tau_\sim = f$?
Consideriamo $x_1 \sim x_2$:

- se $f(x_1) \neq f(x_2)$ allora ψ non esiste;
- se invece $f(x_1) = f(x_2)$ definiamo $\psi([\,x\,]) := f(x)$.

Capitolo 2

Gruppi

2.1 Gruppi

Definizione 2.1. Un insieme G con una mappa (moltiplicazione) $G \times G \longrightarrow G$ si dice *gruppo* se

(a) $\forall\, x, y, z \in G$ vale $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associatività);

(b) $\exists\, 1_G \in G$ t.c. $\forall\, g \in G$ vale $1_G g = g 1_G = g$ (esistenza dell'elemento neutro);

(c) $\forall\, g \in G \quad \exists\, g^{-1} \in G$ t.c. $g \cdot g^{-1} = 1_G$ (esistenza dell'inverso).

Osservazioni.

1. L'elemento neutro è univoco: sia anche $1'_G \in G$ t.c. $1'_G \cdot g = g \cdot 1'_G = g \quad \forall\, g \in G$, allora $1_G = 1_G \cdot 1'_G = 1'_G$;

2. L'ememento neutro soddisfa anche $g^{-1} \cdot g = 1_G$, infatti $g^{-1} \cdot (g \cdot g^{-1}) = g^{-1} \cdot 1_G = g^{-1} \Longrightarrow 1_G = g^{-1} \cdot (g^{-1})^{-1} = ((g^{-1} \cdot g) \cdot g^{-1}) \cdot (g^{-1})^{-1} = (g^{-1} \cdot g) \cdot (g^{-1} \cdot (g^{-1})^{-1}) = (g^{-1} \cdot g) \cdot 1_G = g^{-1} \cdot g$;

3. L'elemento inverso è univoco: sia anche $g_1^{-1} \in G$ t.c. $g \cdot g_1^{-1} = 1_G$, allora $g_1^{-1} = 1_G \cdot g_1^{-1} = (g^{-1} \cdot g) \cdot g_1^{-1} = g^{-}1 \cdot (g \cdot g_1^{-1}) = g^{-1} \cdot 1_G = g^{-1}$;

4. $(g^{-1})^{-1} = g \quad \forall\, g \in G$; infatti $g^{-1} \cdot (g^{-1})^{-1} = 1_G$. Per quanto osservato al punto (2) abbiamo anche $g^{-1} \cdot g = 1_G$ e, per il punto (3), $g = (g^{-1})^{-1}$.

Esempi 2.1.

1. $G = \{1_G\}$, $1_G \cdot 1_G = 1_G \Longrightarrow G$ è un gruppo; lo chiameremo *gruppo banale*;

2. Sia X un insieme e sia $G = B_{ij}(x) := \{\alpha : X \longrightarrow X \mid \alpha \text{ è biettiva}\}$; $\forall\, \alpha, \beta \in B_{ij}(x)$ abbiamo $(\alpha \cdot \beta)(x) = (\alpha \circ \beta)(x) = \alpha(\beta(x))$ per $x \in X$. Allora $\circ$ è associativa; come elemeno neutro consideriamo la matrice identità, $1_G = Id_x$; infine ogni mappa biettiva è invertibile e la sua

inversa è a sua volta biettiva, quindi $\forall\, \alpha \in G \quad \exists\, \alpha^{-1} \in G$. Segue che $G = B_{ij}(x)$ è un gruppo.

3. Sia $X = \{1; \dots; n\} \subseteq \mathbb{N}$; $S_n = B_{ij}(\{1, \dots, n\})$ si chiama *gruppo simmetrico* di grado n. Si può descrivere ogni $\alpha \in S_n$ in una tabella:

x	1	2	...	n
$\alpha(x)$	$\alpha(1)$	$\alpha(2)$	...	$\alpha(n)$

Ad esempio:

x	1	2	...	n
Id_x	1	2	...	n

allora si ha $|S_n| = n!$. Esiste tuttavia anche una seconda descrizione di S_n chiamata *per cicli*: $\forall\, \alpha \in S_n$ si scrive

$$(1, \alpha(1), \alpha^2(1), \alpha^3(1), \dots, \alpha^{k-1}(1))$$

dove $\alpha(\alpha(1)) \coloneqq \alpha^2(1)$; quando $\alpha^k(1) = 1$ si chiudono le parentesi.
Allo stesso modo sia $m \in \{1, 2, \dots, n\} \setminus \{\alpha^j(1) \mid 0 \leq j \geq k_1 - 1\}$; $(m, \alpha(m), \dots, \alpha^{k_2-1}(m))$ e chiudiamo la parentesi se $\alpha^{k_2}(m) = m$.
Sia $m_r \in \{1, \dots, n\} \setminus \bigcup_{i=1}^{r-1} \{\alpha^j(m_i) \mid 0 \leq j \geq k_i - 1\}$;
$(m_r, \alpha(m_r), \dots, \alpha^{k_r-1}(m_r))$ se $\alpha^{k_r}(m_r) = m_r$.

4. $(1,2) \longleftrightarrow$

x	1	2	3	...	n
$\alpha(x)$	2	1	3	...	n

5. $(1, 2, \dots, n) \longleftrightarrow$

x	1	2	...	n-1	n
$\alpha(x)$	2	3	...	n	1

Osservazioni.

1. Una parentesi si definisce un *ciclo*;
2. Il numero delle cifre in una parentesi si chiama *lunghezza del ciclo*;
3. Nelle notazioni ometteremo i cicli di lunghezza 1;
4. Questa decomposizione si chiama *decomposizione in cicli*.

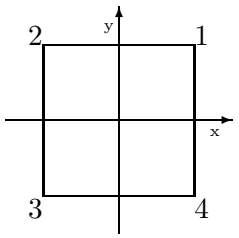
Definizione 2.2. Un gruppo G si dice *abeliano* se $\forall\, g, h \in G$ vale $g \cdot h = h \cdot g$.

Esempi 2.2.

1. S_n non è abeliano per $n \geq 3$;
2. $(\mathbb{Z}, +)$ è un gruppo abeliano;

3. Sia $\mathbb{K}$ un campo ($\mathbb{Q}; \mathbb{R}; \mathbb{C}; \mathbb{F}_2 := \{0,1\}; \mathbb{F}_p$, con p primo). Allora $(\mathbb{K}, +)$ e $\mathbb{K}^* := (\mathbb{K} \setminus \{0\}, \cdot)$ sono gruppi abeliani.

4. Introduciamo innanzitutto una definizione: il *gruppo diedrale* di ordine $2n$ è il gruppo formato dalle isometrie del piano che lasciano immutati i poligoni regolari a n lati.
   Vogliamo ora definire tutte le simmetrie del quadrato.



   $D_8 = \{Id; (1,2)(3,4); (1,4)(2,3); (1,3); (2,4); (1,2,3,4); (1,3)(2,4); (1,4,3,2)\} \subseteq S_4$. D_8 è il gruppo diedrale di ordine 8.

2.2 Sottogruppi e sottogruppi normali

Definizione 2.3. Sia $(G, \cdot)$ un gruppo. Un sottoinsieme $H \subseteq G$ si dice *sottogruppo* se $(H, \cdot|_{H\times H})$ è un gruppo. Useremo la notazione $H \leqslant G$.

Definizione 2.4. Sia $(G, \cdot)$ un gruppo e sia $N \leqslant G$. N si dice *sottogruppo normale* se $\forall\, n \in N$ e $\forall\, g \in G$ vale $g{\cdot}n{\cdot}g^{-1} \in N$. Useremo la notazione $N \triangleleft G$.

Osservazioni.

1. Se G è un gruppo abeliano, ogni sottogruppo è anche normale:

2. Se $\forall\, n \in N \wedge \forall\, h \in G$ vale $h{\cdot}n{\cdot}h^{-1} \in N \vee h^{-1}{\cdot}n{\cdot}h \in N$ allora N è sottogruppo normale di G. (Vale anche il viceversa).

Proposizione 2.1. *Sia $(G, \cdot)$ un gruppo e sia $H \subseteq G$, $H \neq \varnothing$. Se $\forall\, h, k \in H$ vale $h^{-1}{\cdot}k \in H$ allora H è un sottogruppo.*

Dim. Dobbiamo dimostrare dapprima che esistono l'elemento neutro e l'inverso. Se $H \neq \varnothing$ allora $\exists\, h \in H \Longrightarrow h^{-1}{\cdot}h \in H$ per ipotesi; ma $h \in H \subseteq G \Longrightarrow h \in G$. Allora $h{\cdot}h^{-1} = 1_G \Longrightarrow 1_G \in H$ ($\exists$ elemento neutro).
Per ipotesi $h, 1_G \in H \Longrightarrow h^{-1}{\cdot}1_G \in H \Longrightarrow h^{-1} \in H$ ($\exists$ inverso).
Ora ci resta da verificare che dati $h_1, h_2 \in H \Longrightarrow h_1{\cdot}h_2 \in H$. Per quanto dimostrato prima (inverso) abbiamo che $h_1 \in H \Longrightarrow h_1^{-1} \in H$ e per ipotesi $(h_1^{-1})^{-1}{\cdot}h_2 \in H$, ma $(h_1^{-1})^{-1} = h_1 \Longrightarrow h_1{\cdot}h_2 \in H$.

CVD

Esempi 2.3.

1. Sia $G = \mathbb{Z}$ e sia $n \in \mathbb{N}$. Consideriamo $n.\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Siano $n \cdot k, n \cdot h \in n.\mathbb{Z}$; abbiamo $(-n \cdot k) + n \cdot h = n \cdot (k - h) \in n.\mathbb{Z} \Longrightarrow$ Per la proposizione 2.1 $n.\mathbb{Z}$ è un sottogruppo.

2. Sia $Aff_1(\mathbb{R}) = \{f_{a,b}(x) = a \cdot x + b \mid a, b \in \mathbb{R}, a \neq 0\} \subseteq B_{ij}(\mathbb{R})$. Mostriamo che è un sottogruppo.

$$\begin{aligned} f_{a,b}^{-1}(x) &= \frac{1}{a} \cdot x - \frac{b}{a} = f_{\frac{1}{a}, -\frac{b}{a}} \\ f_{a,b}^{-1}(f_{a,b}(x)) &= \frac{1}{a}(a \cdot x + b) - \frac{b}{a} = x \end{aligned}$$

   Siano $f_{a,b}, f_{c,d} \in Aff_1(\mathbb{R})$.

$$\begin{aligned} (f_{a,b}^{-1} \circ f_{c,d})(x) &= f_{\frac{1}{a}, -\frac{b}{a}}(c \cdot x + d) \\ &= (\frac{c}{a} \cdot x + \frac{d}{a}) - \frac{b}{a} \\ &= f_{\frac{c}{a}, (\frac{c}{a} - \frac{b}{a})}(x) \in Aff_1(\mathbb{R}) \\ &\Downarrow \end{aligned}$$

   Per la proposizione 2.1 $Aff_1(\mathbb{R})$ è un sottogruppo di $B_{ij}(\mathbb{R})$;

3. Definiamo l'insieme delle matrici invertibili:

$$Gl_n(\mathbb{R}) = \{\mathcal{A} \in Mat_{n \times n}(\mathbb{R}) \mid det(\mathcal{A}) \neq 0\}$$

   Consideriamo ora

$$Aff_n(\mathbb{R}) = \{f_{A,b} : \mathbb{R}^n \longrightarrow \mathbb{R}^n \mid f_{A,b}(x) = A.x + b\} \subseteq B_{ij}(\mathbb{R}^n)$$

$$A \in Gl_n(\mathbb{R}), b \in \mathbb{R}^n$$

   Siano $f_{A,b}, f_{C,d} \in Aff_n(\mathbb{R})$.

$$\begin{aligned} f_{A,b}^{-1}(x) &= f_{A^{-1}, -A^{-1}.b}(x) \\ (f_{A,b}^{-1} \circ f_{C,d})(x) &= f_{A^{-1}, -A^{-1}.b}(C.x + d) \\ &= A^{-1}.C.x + A^{-1}.d - A^{-1}.b \\ &= f_{A^{-1}.C, A^{-1}.(d-b)}(x) \in Aff_n(\mathbb{R}) \\ &\Downarrow \end{aligned}$$

   Per la proposizione 2.1 $Aff_n(\mathbb{R})$ è un sottogruppo di $B_{ij}(\mathbb{R}^n)$;

4. Definiamo ora $T_n \subseteq Aff_n(\mathbb{R})$:

$$T_n = \{f_b : R^n \longrightarrow \mathbb{R}^n \mid f_b(x) = x + b\}$$

Mostriamo che T_n è un sottogruppo abeliano e normale. Indicheremo con $b_1 + b_2$ la somma di vettori in $\mathbb{R}^n$.
Siano $f_{b_1}, f_{b_2} \in T_n$.

$$(f_{b_1}^{-1} \circ f_{b_2})(x) = (f_{b_1} \circ f_{b_2})(x) = f_{b_1+b_2}(x) \in T_n$$

$\Longrightarrow T_n$ è un sottogruppo per la proposizione 2.1.

$$(f_{b_1} \circ f_{b_2})(x) = f_{b_1+b_2}(x) = f_{b_2+b_1}(x) = (f_{b_2} \circ f_{b_1})(x)$$

$\Longrightarrow T_n$ è abeliano.
Sia $f_{A,b'} \in Aff_n\mathbb{R}$. Detta I la matrice identità abbiamo $f_{I,b} \in T_n$, consideriamo:

$$(f_{A,b'} \circ f_{I,b} \circ f_{A,b'}^{-1})(x)$$

Se possiamo scriverla nella forma $f_{I,c}$ abbiamo la tesi.

$$\begin{aligned}(f_{A,b'} \circ f_{I,b} \circ f_{A,b'}^{-1})(x) &= (f_{A,b'} \circ f_{I,b} \circ f_{A^{-1},-A^{-1}.b'})(x)\\ &= (f_{A,b'} \circ f_{A^{-1},-A^{-1}.b'+b})(x)\\ &= f_{A.A^{-1},-A.(A^{-1}.b'-b)+b'}(x)\\ &= f_{I,A.b}(x) \in T_n\end{aligned}$$

$\Longrightarrow T_n$ è normale.

2.3 Omomorfismi di gruppi

Definizione 2.5. Siano G e H gruppi. Una mappa $\varphi : G \longrightarrow H$ si dice *omomorfismo* di gruppi se:

(a) $\varphi(1_G) = 1_H$;

(b) $\forall\, g, h \in G$ vale $\varphi(g \cdot h) = \varphi(g) \cdot \varphi(h)$.

Osservazioni.

1. $im(\varphi) = \{\varphi(g) \mid g \in G\} \subseteq H$ è un sottogruppo:
   $\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(1_G) = 1_H \Longrightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$; siano $\varphi(g)$ e $\varphi(h) \in im(\varphi)$, allora $\varphi(g)^{-1} \cdot \varphi(h) = \varphi(g^{-1}) \cdot \varphi(h) = \varphi(g^{-1} \cdot h) \in im(\varphi)$; per la proposizione 2.1 $im(\varphi)$ è un sottogruppo;

2. $ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\} \subseteq G$ è un sottogruppo normale:
   siano $g, h \in ker(\varphi)$, allora $\varphi(g^{-1} \cdot h) = \varphi(g^{-1}) \cdot \varphi(h) = \varphi(g)^{-1} \cdot \varphi(h) = 1_H \cdot 1_H = 1_H \Longrightarrow g^{-1} \cdot h \in ker(\varphi) \Longrightarrow ker(\varphi)$ è un sottogruppo (per la proposizione 2.1).
   Siano $x \in G$ e $h \in ker(\varphi) : \varphi(x \cdot h \cdot x^{-1}) = \varphi(x) \cdot \varphi(h) \cdot \varphi(x^{-1})$, ma $\varphi(h) = 1_H$ perché $h \in ker(\varphi)$, allora $\varphi(x) \cdot \varphi(h) \cdot \varphi(x^{-1}) = \varphi(x) \cdot \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(1_G) = 1_H$. Quindi $x \cdot h \cdot x^{-1} \in ker(\varphi) \Longrightarrow ker(\varphi)$ è un sottogruppo normale.

Esempi 2.4. Sia $G = Gl_n(\mathbb{R})$, abbiamo $det : Gl_n(\mathbb{R}) \longrightarrow \mathbb{R}^* := \mathbb{R} \setminus 0$. Sappiamo per il teorema di Binet che $det(\mathcal{A})\cdot det(\mathcal{B}) = det(\mathcal{A}\cdot\mathcal{B})$. Allora la funzione det è un omomorfismo di gruppi.

2.4 Laterali

Definizione 2.6. Sia G un gruppo e sia $H \leqslant G$.

- La relazione $\sim_H$: $G \times G \longrightarrow \{v, f\}$ dove $g \sim_H g' \iff \exists\, h \in H$ t.c. $g' = g\cdot h$ è una relazione di equivalenza;
- Una classe di equivalenza $[\, g \,] = \{g\cdot h \mid h \in H\} = g\cdot H$ si dice *H–laterale* (di destra).

Mostriamo che $\sim_H$ è una relazione di equivalenza:

(r) $\forall\, g \in G$ vale $g \sim_H g$ poiché $1_H \in H$;

(s) Sia $g \sim_H g' \Longrightarrow \exists\, h \in H$ t.c. $g' = g\cdot h$
$g'\cdot h^{-1} = (g\cdot h)\cdot h^{-1} = g$ per associatività della moltiplicazione
$\Longrightarrow g' \sim_H g$;

(t) Siano $g \sim_H g' \wedge g' \sim_H g''$. Allora sappiamo che:
$\exists\, h, h' \in H$ t.c. $g' = g\cdot h \wedge g'' = g'\cdot h' \Longrightarrow g'' = (g\cdot h)\cdot h' = g\cdot(h\cdot h')$. Poiché $h\cdot h' \in H$ definisco $h\cdot h' = h''$; allora abbiamo $g'' = g\cdot h'' \Longrightarrow g \sim_H g''$.

L'insieme delle classi di equivalenza $G/\sim_H := G/H$ si dice l'insieme degli *H–laterali di destra di G*.

Proposizione 2.2. *Sia G un gruppo e sia $H \leqslant G$.*

(a) Sia $\mathcal{R}$ un sistema di rappresentanti per la relazione $\sim_H$.
Allora $G = \overset{\circ}{\bigcup}_{g\in\mathcal{R}} g\cdot H$.

(b) Sia G un gruppo finito. Allora $|g\cdot H| = |H| \quad \forall\, g \in G$.

Dim. Osserviamo innanzitutto che se $|G| < \infty$, allora anche $|H| < \infty$.

(a) Segue dalla proposizione 1.2 (data una relazione di equivalenza, l'insieme è unione disgiunta delle classi di equivalenza).

(b) Sia $\beta_g : H \to g\cdot H$, $\beta_g(h) = g\cdot h$. Abbiamo che β_g è iniettiva: siano $h, k \in H$ t.c $\beta_g(h) = \beta_g(k) \Longrightarrow g\cdot h = g\cdot k \Longrightarrow g^{-1}\cdot g\cdot h = g^{-1}\cdot g\cdot k \Longrightarrow h = k$; β_g è suriettiva: sia $g' \in G$ t.c $g \sim_H g'$. Per la definizione 2.6 $\exists\, h \in H$ t.c. $g' = g\cdot h = \beta_g(h) \Longrightarrow g' \in im(\beta_g) \Longrightarrow |H| = |g\cdot H|$.

CVD

Teorema 2.3 (di Lagrange)**.** *Sia G un gruppo finito e sia $H \leqslant G$. Allora $|G| = |G/H|\cdot|H|$. In particolare $|H|$ divide $|G|$.*

Dim. Sia $\mathcal{R}$ un sistema di rappresentanti per $\sim_H$, in particolare $|R| = |G/H|$. Allora per la proposizione 2.2 abbiamo:

$$|G| = |\overset{\circ}{\bigcup}_{g\in\mathcal{R}} g\cdot H| = \sum_{g\in\mathcal{R}} |g\cdot H| = \sum_{g\in\mathcal{R}} |H| = |\mathcal{R}|\cdot|H| \Longrightarrow |G| = |G/H|\cdot|H|$$

CVD

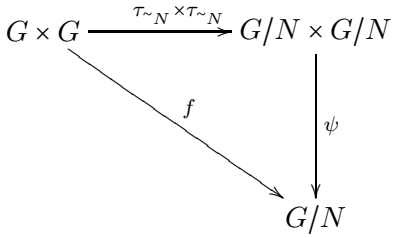
2.5 Il quoziente canonico

Proposizione 2.4. *Sia G un gruppo e sia $N \triangleleft G$. Allora la mappa:*

$$\psi : G/N \times G/N \longrightarrow G/N \quad \psi(g\cdot N, h\cdot N) = g\cdot h\cdot N$$

è ben definita e definisce canonicamente la struttura di un gruppo su G/N.

Dim.



Definiamo una funzione

$$\tau_\sim \text{ t.c. } \sim : (G\times G)\times(G\times G) \to \{v, f\}$$
$$(g,h) \sim_N (g',h') \Leftrightarrow \exists\, n, m \in N \text{ t.c. } g' = g\cdot n \wedge h' = h\cdot m$$

Mostriamo che $\sim$ è una relazione di equivalenza:

(r) $\forall\, (g,h) \in G\times G$ vale $(g,h) \sim (g,h)$. Basta scegliere $m = n = 1$;

(s) Sia $(g,h) \sim (g',h') \Longrightarrow \exists\, n, m \in N$ t.c. $g' = g\cdot n \wedge h' = h\cdot m$
$\Longrightarrow g = g'\cdot n^{-1} \wedge h = h'\cdot m^{-1} \Longrightarrow (g',h') \sim (g,h)$

(t) Siano $(g,h) \sim (g',h') \wedge (g',h') \sim (g'',h'')$. Allora
$\exists\, n, m, n', m' \in N$ t.c. $g' = g\cdot n \wedge h' = h\cdot m \wedge g'' = g'\cdot n' \wedge h'' = h'\cdot m'$
$\Longrightarrow g'' = g\cdot(n\cdot n') \wedge h'' = h\cdot(m\cdot m') \Longrightarrow (g,h) \sim (g'',h'')$

Possiamo quindi affermare che:

$$\begin{aligned} \sim \;&:\; (g,h) \sim (g',h') \Leftrightarrow g \sim_N g' \wedge h \sim_N h' \\ [\,(g,h)\,] \;&=\; \{(g',h') \in G\times G \mid g \sim_N g' \wedge h \sim_N h'\} \\ \tau_\sim((g,h)) \;&=\; [\,(g,h)\,] = [\,g\,]\times[\,h\,] = \tau_{\sim_N}(g)\times\tau_{\sim_N}(h) \end{aligned}$$

Quindi le due mappe coincidono. Ora mostriamo che elementi in relazione tra loro hanno la stessa immagine (mediante la mappa f).
Siano $(g,h) \sim (g',h') \Longrightarrow \exists\, n,m \in N$ t.c. $g' = g{\cdot}n \wedge h' = h{\cdot}m$. Applichiamo f:

$$f(g',h') = f(g{\cdot}n, h{\cdot}m) = (g{\cdot}n{\cdot}h{\cdot}m){\cdot}N$$

Poiché N è normale in G, $\exists\, n' \in N$ t.c. $h^{-1}{\cdot}n{\cdot}h = n'$
Moltiplicando entrambi i membri a sinistra per h otteniamo

$$h^{-1}{\cdot}n{\cdot}h = n' \Longrightarrow h{\cdot}h^{-1}{\cdot}n{\cdot}h = h{\cdot}n' \Longrightarrow n{\cdot}h = h{\cdot}n'$$

Quindi

$$f(g',h') = (g{\cdot}n{\cdot}h{\cdot}m){\cdot}N = (g{\cdot}h{\cdot}n'{\cdot}m){\cdot}N$$

Ora, poiché $n' \wedge m \in N \Longrightarrow g{\cdot}h{\cdot}n'{\cdot}m{\cdot}N = g{\cdot}h{\cdot}N$

$$\Longrightarrow f(g',h' = (g{\cdot}h){\cdot}N = f(g,h)$$

Concludiamo con il considerare la nostra funzione ψ

$$\psi(g{\cdot}N, h{\cdot}N) = g{\cdot}h{\cdot}N$$

- è associativa: $\forall\, a,b,c \in G$ vale $((a{\cdot}N){\cdot}(b{\cdot}N)){\cdot}(c{\cdot}N) = a{\cdot}b{\cdot}c{\cdot}N = (a{\cdot}N){\cdot}((b{\cdot}N){\cdot}(c{\cdot}N))$;
- esiste l'elemeno neutro: $1_{G/N} = 1{\cdot}N = N$;
- esiste l'inverso: $\forall\, g{\cdot}N \in G/N, (g{\cdot}N)^{-1} = g^{-1}{\cdot}N$.

CVD

Definizione 2.7. G/N si dice il *quoziente canonico* di G modulo N.

2.6 Gruppi ciclici

Definizione 2.8. Un gruppo G si dice *ciclico* se esiste un elemento $g \in G$ tale che $G = \{g^k \mid k \in \mathbb{Z}\}$.

Esempi 2.5.

1. Sia $G = \mathbb{Z}$, dove $1_G = 0$ e l'operazione è la somma $+$.

$$\begin{aligned} G &= \{1^k \mid k \in \mathbb{Z}\} \\ &= \{k+1 \mid k \in \mathbb{Z}\} \\ &= \{k \mid k \in \mathbb{Z}\} \end{aligned}$$

2. Sia $G = 1; -1 \subseteq (\mathbb{R}, \cdot)$. Definiamo la moltiplicazione " $\cdot$ ": $G \times G \longrightarrow G$ secondo la tabella, detta *tabella di moltiplicazione*.

$\curvearrowright$	1	-1
1	1	-1
-1	-1	1

$G = \{-1^k \mid k \in \mathbb{Z}\}$

3. Sia $G = \{1; -1; i; -i\} \subseteq (\mathbb{C}, \cdot)$. Definiamo la moltiplicazione secondo la tabella.

$\curvearrowright$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$G = \{i^k \mid k \in \mathbb{Z}\}$

4. Mostriamo ora un esempio di gruppo non ciclico.
Definiamo i quaternioni di Hamilton $\mathbb{H} := \mathbb{R}.1 \oplus \mathbb{R}.i \oplus \mathbb{R}.j \oplus \mathbb{R}.k$ e una moltiplicazione sulla base:

   - 1 è l'elemento neutro;
   - $i \cdot i = j \cdot j = k \cdot k = -1$;
   - $i \cdot j = k, \quad i \cdot i \cdot j = i \cdot k \Longrightarrow i \cdot k = -j$.

$\curvearrowright$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$(\mathbb{H}, +, \cdot)$ è un corpo

   Sia $Q_8 = \{1; -1; i; -i; j; -j; k; -k\}$ il gruppo dei quaternioni.

$\curvearrowright$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

   Q_8 non è cicliclo.

Proposizione 2.5. *Sia G un gruppo ciclico e sia $N \leqslant G$:*

(a) allora G è abeliano;

(b) allora $N \triangleleft G$ e G/N è ciclico.

Dim.

(a) Siano $x, y \in G$, dove per ipotesi $\exists\, g \in G$ t.c $G = \{g^k \mid k \in \mathbb{Z}\}$.
$\Longrightarrow \exists\, m, n \in \mathbb{Z}$ t.c. $x = g^m \wedge y = g^n \Longrightarrow x{\cdot}y = g^m{\cdot}g^n = g^{m+n}$ ma $\mathbb{Z}$ è abeliano
$\Longrightarrow g^{m+n} = g^{n+m} = g^n{\cdot}g^m = x{\cdot}y \Longrightarrow G$ è abeliano.

(b) N è normale perché ogni sottogruppo di un gruppo abeliano è normale. Sia G/N il quoziente canonico di G modulo N.

$$\begin{aligned} G/N &= \{h{\cdot}N \mid h \in G\} \\ &= \{g^k{\cdot}N \mid k \in \mathbb{Z}\} \\ &= \{(gN)^k \mid k \in \mathbb{Z}\} \end{aligned}$$

Questo è possibile perché dati $a, b \in G$ vale che $(a{\cdot}N){\cdot}(b{\cdot}N) = (a{\cdot}b){\cdot}N$
$\Longrightarrow (g{\cdot}N)^k = g^k{\cdot}N$.
Definiamo ora $\bar{g} := g{\cdot}N$. Allora:

$$G/N = \{\bar{g}^k \mid k \in \mathbb{Z}\}$$

CVD

Osservazioni. Sia $n \in \mathbb{N}$. Allora $n.\mathbb{Z} = \{n{\cdot}\alpha \mid \alpha \in \mathbb{Z}\}$ è un sottogruppo normale di $\mathbb{Z}$ e così $C_n : \mathbb{Z}/n.\mathbb{Z}$ è un gruppo ciclico di ordine $|\mathbb{Z}/n.\mathbb{Z}| = n$.

2.7 Teoremi dell'Omomorfismo

Teorema 2.6 (1° Teorema dell'Omomorfismo o Teorema dell'Isomorfismo)**.** *Siano $(G, \cdot)$ e $(H, \star)$ due gruppi e sia $\Phi : G \longrightarrow H$ un omomorfismo di gruppi. Allora esiste un isomorfismo canonico*

$$\widetilde{\Phi} : \frac{G}{Ker(\Phi)} \longrightarrow im(\Phi)$$

Dim. Sia $N := Ker(\Phi)$ e sia $\Phi_1 : G \longrightarrow im(\Phi)$ la restrizione di Φ sul secondo argomento. Allora Φ_1 rimane un omomorfismo, è suriettivo e $Ker(\Phi_1) = Ker(\Phi) = N$.

Siano $g, h \in G$, $g \sim_N h$, esista cioè $n \in N$ tale che $h = g \cdot n$; allora

$$\Phi_1(h) = \Phi_1(g \cdot n) = \Phi_1(g) \star \Phi_1(n) = \Phi_1(g) \star 1_G = \Phi_1(g)$$

perciò è ben definita la mappa

$$\begin{aligned} \widetilde{\Phi} : G/N &\longrightarrow im(\Phi) \\ \widetilde{\Phi}(g \cdot N) &= \Phi_1(g), \end{aligned}$$

cioè, detta τ_N la proiezione canonica al quoziente da G a G/N, $\widetilde{\Phi} \circ \tau_n = \Phi_1$.

(1) $\widetilde{\Phi}$ è un omomorfismo: $\forall\, x, y \in G$,

$$\begin{aligned} & \widetilde{\Phi}((x\cdot N)\cdot(y\cdot N)) = \widetilde{\Phi}((x\cdot y)\cdot N) && \text{(def. di quoziente canonico)} \\ = \quad & \Phi_1(x\cdot y) = \Phi_1(x)\star\Phi_1(y) && (\Phi_1 \text{ è omomorfismo}) \\ = \quad & \widetilde{\Phi}(x\cdot N)\star\widetilde{\Phi}(y\cdot N). \end{aligned}$$

(2) $\widetilde{\Phi}$ è suriettivo:

$$\text{sia } z \in im(\Phi) \implies \exists\, a \in G \text{ t.c. } z = \Phi(a) = \Phi_1(a) = \widetilde{\Phi}(a\cdot N).$$

(3) $\widetilde{\Phi}$ è iniettivo:

$$\begin{aligned} & \text{sia } x\cdot N \in ker(\widetilde{\Phi}) \implies \Phi_1(x) = \widetilde{\Phi}(x\cdot N) = 1_H \quad \implies \\ \implies \quad & x \in ker(\Phi_1) = ker(\Phi) = N = 1_G\cdot N \implies x \sim_N 1_G \quad \implies \\ \implies \quad & x\cdot N = 1_G\cdot N = N = 1_{G/N} \implies ker(\widetilde{\Phi}) = \{1_{G/N}\} \end{aligned}$$

CVD

Teorema 2.7 (2° Teorema dell'Omomorfismo)**.** *Sia $(G,\cdot)$ un gruppo e siano $H \leq G, N \lhd G$. Allora $(H\cap N) \lhd G$ e, con le strutture di quoziente canonico,*

$$\frac{H}{H\cap N} \simeq \frac{H\cdot N}{N}$$

Dim. Basta dimostrare che che $H\cap N \lhd H$ così da poter passare al quoziente. Sia

$$\begin{aligned} \tau : G &\longrightarrow G/N \\ \tau(g) &= g\cdot N \end{aligned}$$

l'omomorfismo canonico. Restringendolo ad H, $\tau|_H : H \longrightarrow G/N$ non è più suriettiva:

$$\tau(H) = \{h\cdot N \mid h \in H\} = \tfrac{H\cdot N}{N} \qquad \implies$$

$\implies$ $\tau|_H : H \longrightarrow \frac{H\cdot N}{N}$ è suriettiva e rimane un omomorfismo.

Che cos'è $ker(\tau|_H) \lhd G$?

$$h \in ker(\tau|_H) \iff h \in H \ \wedge\ \tau(h) = N \iff h \in H \ \wedge\ h \in N,$$

ovvero $ker(\tau|_H) = H\cap N \lhd G$. Ma allora, per il 1° *Th. dell'isomorfismo*,

$$\frac{H}{Ker(\tau|_H)} = \frac{H}{H\cap N} \simeq \frac{H\cdot N}{N}.$$

CVD

Teorema 2.8 (3° Teorema dell'Omomorfismo)**.** *Sia* $(G,\cdot)$ *un gruppo e siano* $N, M \triangleleft G$ *con* $N \leq M$*. Allora*

$$\frac{G/N}{M/N} \simeq \frac{G}{M}$$

(dove tutti i quozienti hanno la struttura di gruppo del quoziente canonico).

Dim. Sia

$$\varphi : \frac{G}{N} \longrightarrow \frac{G}{M}$$

$$\varphi(g \cdot N) = g \cdot M.$$

φ è ben definita, perché $g_1 \cdot N = g_2 \cdot N \implies \varphi(g_1 \cdot N) = \varphi(g_2 \cdot N)$. Infatti

$$g_1 \cdot N = g_2 \cdot N \iff \exists\, n \in N \text{ t.c. } g_1 \cdot n = g_2$$
$$\text{ma } N \subseteq M \implies n \in M \implies g_1 \cdot M = g_2 \cdot M.$$

φ è un omomorfismo perché per definizione di quoziente canonico

$$\varphi((g_1 \cdot N) \cdot (g_2 \cdot N)) = \varphi((g_1 \cdot g_2) \cdot N) = (g_1 \cdot g_2) \cdot M =$$
$$= (g_1 \cdot M) \cdot (g_2 \cdot M) = \varphi(g_1 \cdot N) \cdot \varphi(g_2 \cdot N).$$

Inoltre φ è banalmente suriettivo, perché, variando g in tutto G, ogni classe d'equivalenza $g \cdot M \in G/M$ ha una controimmagine $g \cdot N \in G/N$ mediante φ. Ora,

$$h \cdot N \in ker(\varphi) \iff \varphi(h \cdot N) = M \iff h \cdot M = M \iff h \in M,$$

quindi $ker(\varphi) = M/N$.
(*NOTA:* se $N \triangleleft G$ e $N \leq M \leq G$, a maggior ragione $N \triangleleft M$, dunque ha senso definire su M/N la struttura di gruppo del quoziente canonico).

Applicando il 1° *Th. dell'isomorfismo* si ottiene infine

$$\frac{G/N}{M/N} \simeq \frac{G}{M}.$$

CVD

Capitolo 3

Azioni di gruppi

3.1 G-insiemi

Sia X un insieme, sia $G = Bij(X)$, (ovvero $G = Symm(X)$); si vuole definire una struttura sull'insieme X, partendo dal gruppo G.

Definizione 3.1. Sia $(G, \cdot)$ un gruppo. Un insieme X dotato di una mappa prodotto

$$\begin{array}{rcl} \bullet : G \times X & \longrightarrow & X \\ \bullet\,(g\,,\,x) & := & g \bullet x \end{array}$$

si dice un *G-insieme* se:

(a) $\forall\ x \in X,\ 1_G \bullet x = x$

(b) $\forall\ g, h \in G,\ \forall\, x \in X,\ (g \cdot h) \bullet x = g \bullet (h \bullet x)$.

La mappa $\bullet$ si dice *azione* di G su X.

Esempi 3.1.

1. Siano X un insieme, $(G, \cdot) = (Bij(X), \circ)$ (dove $\circ$ denota l'abituale composizione di funzioni) e

$$\begin{array}{rcl} \bullet : G \times X & \longrightarrow & X \\ \alpha \bullet x & = & \alpha(x); \end{array}$$

   è immediato verificare che $\bullet$ è un'azione di G su X, quindi $(X, \bullet)$ è un G-insieme.

2. Sia $(G, \cdot)$ un gruppo e sia $X = G$. Allora $\bullet_{SX} : G \times X \longrightarrow X$, definita come $\bullet_{SX}(g, x) = g \cdot x$ (il prodotto del gruppo *a sinistra*) è un'azione, detta *rappresentazione regolare sinistra*. $(X, \bullet_{SX})$ si dice anche *G-insieme regolare sinistro*.

Se si volesse definire similmente un'azione di G su se stesso usando il prodotto *a destra* occorre qualche cautela: la mappa

$$\begin{array}{rcl} \bullet : G \times X & \longrightarrow & X \\ g \bullet x & = & x \cdot g \end{array}$$

non è in generale un'azione in quanto se G non è abeliano $(g \cdot h) \bullet x = x \cdot g \cdot h \neq x \cdot h \cdot g = g \bullet (h \bullet x)$ per almeno una coppia $(g, h) \in G \times G$; invece con la definizione

$$\begin{array}{rcl} \bullet_{DX} : G \times X & \longrightarrow & X \\ g \bullet_{DX} x & = & x \cdot g^{-1} \end{array}$$

si risolve l'inconveniente (verificare, prego!). Questa ultima azione si chiama *rappresentazione regolare destra* e ovviamente $(X, \bullet_{DX})$ è il *G-insieme regolare destro*.

3. Sia $(G, \cdot)$ un gruppo e sia $H \leq G$ un sottogruppo. Sia $X = G/H = \{x \cdot H \mid x \in G\}$ e sia

$$\begin{array}{rcl} \bullet : G \times X & \longrightarrow & X \\ g \bullet (x \cdot H) & = & (g \cdot x) \cdot H. \end{array}$$

$1_G \bullet (x \cdot H) = x \cdot H$ e $(g_1 \cdot g_2) \bullet (x \cdot H) = (g_1 \cdot g_2 \cdot x) \cdot H = g_1 \bullet (g_2 \bullet (x \cdot H))$, dunque $(X, \bullet)$ è un G-insieme, detto *canonico*.

Definizione 3.2. Sia $(G, \cdot)$ un gruppo e sia $(X, \bullet)$ un G-insieme.

(a) Sia $x \in X$. Allora $Stab_G(x) = G_x = \{g \in G \mid g \bullet x = x\}$ è un sottogruppo di G chiamato *stabilizzatore* di x in G.

(b) Sia $\sim : X \times X \longrightarrow \{v, f\}$ la relazione per la quale $x \sim y \iff \exists g \in G$ t.c. $g \bullet x = y$. Allora $\sim$ è una relazione di equivalenza, cui ci si riferirà in seguito come la relazione *indotta dall'azione di G*. La classe di equivalenza $[x] = G \bullet x$ si dice *G-orbita* che contiene x.

(c) L'insieme $Ker(G, X) = \{g \in G \mid g \bullet x = x \quad \forall x \in X\}$ è un sottogruppo normale di G. Tale insieme è chiamato *nucleo* del G-insieme X.

Dim. verifica:

(a) G_x è un sottogruppo di G: Siano $g, h \in G_x \Longrightarrow g \bullet x = x \ \wedge \ h \bullet x = x$. Allora $h^{-1} \bullet x = h^{-1} \bullet (h \bullet x) = (h^{-1} \cdot h) \bullet x = 1 \bullet x = x \Longrightarrow h^{-1} \in G_x$. Inoltre $(g \cdot h^{-1}) \bullet x = g \bullet (h^{-1} \bullet x) = g \bullet x = x \Longrightarrow g \cdot h^{-1} \in G_x$

(b) $\sim$ è una relazione di equivalenza:

(r) $x \sim x \qquad (x = 1 \bullet x)$.

(s) $x \sim y$ implica che $\exists\, g \in G$ t.c. $y = g \bullet x \Longrightarrow g^{-1} \bullet y = g^{-1} \bullet (g \cdot x) =$
$= (g^{-1} \cdot g) \bullet x = 1 \bullet x = x \Longrightarrow y \sim x.$

(t) Siano $x, y, z \in X$ tali che $x \sim y \ \wedge \ y \sim z$, ovvero $\exists\, g, h \in G$ t.c. $y =$
$g \bullet x \ \wedge \ z = h \bullet y \Longrightarrow z = h \bullet (g \bullet x) = (h \cdot g) \bullet x \Longrightarrow x \sim z.$

(c) $Ker(G, X) = \{g \in G \mid g \cdot x = x \quad \forall\, x \in X\} = \bigcap_{x \in X} G_x \Longrightarrow Ker(G, X)$ è un sottogruppo. Ora, $\forall\, n \in Ker(G, X),\ \forall\, g \in G,\ \forall\, x \in X,$

$$\begin{aligned} & (g \cdot n \cdot g^{-1}) \bullet x = g \bullet (n \bullet (g^{-1} \bullet x)) \coloneqq g \bullet (n \bullet y) \quad = \\ = \quad & g \bullet y = g \bullet (g^{-1} \bullet x) = (g \cdot g^{-1}) \bullet x = 1 \bullet x = x \quad \Longrightarrow \\ \Longrightarrow \quad & g \cdot n \cdot g^{-1} \in Ker(G, X) \Longrightarrow Ker(G, X) \lhd G. \end{aligned}$$

Proposizione 3.1. *Sia $(G, \cdot)$ un gruppo e sia $(X, \bullet)$ un G-insieme.*

(a) Sia $g \in G$. Allora la funzione

$$\begin{array}{ccc} \chi_g : X & \longrightarrow & X \\ \chi_g(x) & = & g \bullet x \end{array}$$

è biiettiva.

(b) La mappa $\chi : G \longrightarrow \mathrm{Bij}(X), \quad \chi(g) = \chi_g$ è un omomorfismo di gruppi con $Ker(\chi) = Ker(G, X)$.

Dim. (a) Siano $x, y \in X$ t.c. $\chi_g(x) = \chi_g(y) \Longrightarrow g \bullet x = g \bullet y \Longrightarrow$

$\Longrightarrow x = g^{-1} \bullet (g \bullet x) = g^{-1} \bullet (g \bullet y) = y \Longrightarrow \chi_g$ è iniettiva.

Sia $y \in X \Longrightarrow \chi_g(g^{-1} \bullet y) = g \bullet (g^{-1} \bullet y) = y \Longrightarrow \chi_g$ è suriettiva.

(b) $(\mathrm{Bij}(X), \circ)$ è un gruppo; inoltre, per il punto (a), χ è ben posta.

$$\forall\, x \in X,\ \chi(1_G)(x) = 1_G \bullet x = x \Longrightarrow \chi(1_G) = id_X = 1_{\mathrm{Bij}(X)}$$

Siano $g, h \in G$; $\forall\, x \in X,$

$$\begin{aligned} & (\chi(g) \circ \chi(h))(x) = (\chi_g \circ \chi_h)(x) = \chi_g(\chi_h(x)) = g \bullet (h \bullet x) \quad = \\ = \quad & (g \cdot h) \bullet x = \chi_{g \cdot h}(x) = \chi(g \cdot h)(x) \Longrightarrow \chi(g \cdot h) = \chi(g) \circ \chi(h). \end{aligned}$$

Ovviamente $Ker(\chi) = Ker(G, X)$.

CVD

Teorema 3.2 (di Cayley)**.** *Sia $(G, \cdot)$ un gruppo finito ($|G| = n < +\infty$). Allora G è isomorfo a un sottogruppo di $(S_n, \circ)$.*

Dim. Si utilizzi la notazione della proposizione precedente. Sia $(X, \bullet)$ il G-insieme regolare sinistro; in tal caso $(\mathrm{Bij}(X), \circ) = (S_n, \circ)$. Ora, se $x \in G$ si ha $G_x = \{g \in G \mid g \cdot x = x\} = \{1\}$: infatti $g \cdot x = x \iff g = g \cdot x \cdot x^{-1} = = x \cdot x^{-1} = 1$. Ne segue che a maggior ragione $Ker(\chi) = \{1\} \implies \chi$ è iniettivo $\implies G \simeq im(\chi) \leq S_n$ (*Th dell' omomorfismo*).

CVD

Definizione 3.3. Sia $(G, \cdot)$ un gruppo e sia $H \leq G$. Allora $|G/H|$ si dice *ordine* di H in G.

Proposizione 3.3. *Sia $(G, \cdot)$ un gruppo e sia $H \leq G$, con $|G/H| = n < +\infty$. Allora $\exists$ un sottogruppo normale $N \triangleleft G$ t.c. $N \leq H \ \wedge \ |G/N| \mid n!$*

Dim. Siano $X = G/H$ e $(X, \bullet)$ il G-insieme canonico. Dalla proposizione (3.1) segue che $\chi : G \longrightarrow Symm(X) \simeq S_n$ è omomorfismo di gruppi. Perciò, applicando il *Th dell' omomorfismo* e il *Th di Lagrange*, risulta

$$\left| \frac{G}{Ker(\chi)} \right| = |im(\chi_x)| \ \Big| \ n!$$

Sia $N := Ker(\chi) \triangleleft G$. Allora $|G/N| \mid n!$
Inoltre

$$N = Ker(\chi) = \bigcap_{x \in X} G_x \leq G_x \ \forall \ x \in X.$$

Allora, per $x = H = 1 \cdot H \in X$, $g \cdot H = H \iff g \sim_H 1 \iff \exists\, h_1, h_2 \in H$ t.c. $g \cdot h_1 = h_2 \iff g = h_2 \cdot {h_1}^{-1} \in H$, cioè $G_H = H$, da cui in conclusione $N \leq H$. Quindi N soddisfa tutte le richieste.

CVD

Definizione 3.4. Sia $(G, \cdot)$ un gruppo e siano $(X, \odot)$ e $(Y, \widetilde{\odot})$ due G-insiemi. Una mappa $\Phi : X \longrightarrow Y$ si dice *omomorfismo di G-insiemi* se $\forall\, x \in X, \forall\, g \in G,\ \Phi(g \odot x) = g \,\widetilde{\odot}\, \Phi(x)$.
Se Φ è anche biiettiva, si dice *isomorfimo di G-insiemi* e si scrive $X \simeq Y$.

Uno schema può aiutare a chiarire la situazione:

$$\begin{array}{ccc} G \times X & \xrightarrow{\ \odot\ } & X \\ \Big\downarrow{\scriptstyle Id_G \times \Phi} & & \Big\downarrow{\scriptstyle \Phi} \\ G \times Y & \xrightarrow{\ \tilde{\odot}\ } & Y \end{array}$$

Si dice che un simile diagramma *commuta* se i due percorsi sono equivalenti:

$$\Phi \circ \odot = \widetilde{\odot} \circ (id_G \times \Phi)$$

Quindi equivalentemente Φ si dice omomorfismo di G-insiemi se il suo diagramma commuta.

Esempi 3.2.

1. Siano $(G,\cdot)$ un gruppo, $H, K \leq G$, $H \leq K$; siano $X = G/H$, $Y = G/K$ e $(X,\bullet)$ e $(Y,\odot)$ i due rispettivi G-insiemi canonici.
   Siano $g_1, g_2 \in G$ t.c. $g_1 \sim_H g_2 \implies \exists\, h \in H$ t.c. $g_1 \cdot h = g_2$; ma è a maggior ragione $h \in K \implies g_1 \sim_K g_2$. Come conseguenza, la mappa

$$\begin{aligned} \Phi : X &\longrightarrow Y \\ \Phi(g \cdot H) &= g \cdot K \end{aligned}$$

   è ben definita.
   È anche un omomorfismo di G-insiemi: comunque dati $a \in G$, $g \cdot H \in X$,

$$\begin{aligned} \Phi(a \bullet (g \cdot H)) = \Phi((a \cdot g) \cdot H) = (a \cdot g) \cdot K \\ a \odot \Phi(g \cdot H) = a \odot (g \cdot K) = (a \cdot g) \cdot K \end{aligned}$$

Definizione 3.5. Sia $(G,\cdot)$ un gruppo; un G-insieme $(X,\bullet)$ si dice *transitivo* se ha una sola orbita, cioè se $\forall x \in X$, $G \bullet x = X$, cioè se $\forall x, y \in X$, $\exists g \in G$ t.c. $g \bullet x = y$. Si dice equivalentemente che l'azione $\bullet$ di G su X è transitiva.

Proposizione 3.4. *Sia $(G,\cdot)$ un gruppo e sia $(X,\bullet)$ un G-insieme transitivo. Allora $\forall\, x \in X$, $\exists\, \Phi_x : G/G_x \longrightarrow X$ isomorfismo di G-insiemi (considerando (G/G_x) come G-insieme canonico).*

Dim. Sia $x \in X$; si definisca

$$\begin{aligned} \Phi_x : G/G_x &\longrightarrow X \\ \Phi_x(h \cdot G_x) &= h \bullet x \end{aligned}$$

(1) Φ_x è ben definita: siano $h, k \in G$ t.c. $h \sim_{G_x} k \implies \exists\, y \in G_x$ t.c. $h = k \cdot y \implies (k \cdot y) \bullet x = k \bullet (y \bullet x) = k \bullet x$ (si ricordi che y è nello stabilizzatore di x). Ma è anche $(k \cdot y) \bullet x = h \bullet x$, da cui si ricava $h \bullet x = k \bullet x \implies \Phi_x(h \cdot G_x) = \Phi_x(k \cdot G_x)$.

(2) Φ_x è un omomorfismo di G-insiemi:

$$\begin{aligned} \Phi_x\,(\,g \bullet (\,h \cdot G_x\,)) \;&=\; \Phi_x\,((\,g \cdot h\,) \cdot G_x\,) \;= \\ =\;\; (g \cdot h) \bullet x = g \bullet (h \bullet x) &= g \bullet \Phi_x(h \cdot G_x). \end{aligned}$$

(3) Φ_x è iniettivo: siano $h, k \in G$ tali che

$$\begin{aligned} &\Phi_x(h \cdot G_x) = \Phi_x(k \cdot G_x) \implies h \bullet x = k \bullet x \implies \\ \implies\;& (k^{-1} \cdot h) \bullet x = k^{-1} \bullet (h \bullet x) = k^{-1} \bullet (k \bullet x) = (k^{-1} \cdot k) \bullet x = x \implies \\ \implies\;& k^{-1} \cdot h := y \in G_x \implies h = (k \cdot k^{-1}) \cdot h = k \cdot y \implies h \sim_{G_x} k \implies \\ \implies\;& h \cdot G_x = k \cdot G_x. \end{aligned}$$

(4) Φ_x è suriettivo: infatti, sia $z \in X \implies \exists\, g \in G$ t.c. $z = g \bullet x$ (per la transitività) $\implies \Phi_x(g \cdot G_x) = g \bullet x = z$.

CVD

Esempi 3.3.

1. Siano $n \in \mathbb{N}$, $(G, \cdot)$ il gruppo $(S_n, \circ)$, $X = \{1, ..., n\}$. La mappa

$$\begin{aligned} \bullet : G \times X &\longrightarrow X \\ \sigma \bullet x &= \sigma(x) \end{aligned}$$

è un'azione di G su X ed è anche transitiva: siano infatti $m \in 1, ..., n$ qualunque e

$$g_m := \begin{cases} id & \text{se } m = n \\ (n, m, ...) & \text{(ciclo di lunghezza } n\text{) se } n \neq m \end{cases} \in G.$$

In queste ipotesi, $m = g_m \bullet n$ e $S_{n-1} \simeq_{gruppi} G_m$ (le permutazioni su n elementi che lasciano fisso uno di essi) $\implies X \simeq_{G\text{-insieme}} S_n/S_{n-1}$.

2. Sia $G = Aff_1(\mathbb{R}) = \{f_{a,b} : \mathbb{R} \to \mathbb{R} \mid f_{a,b}(x) = ax + b;\ a, b \in \mathbb{R};\ a \neq 0\}$. $(G, \circ)$ è un gruppo e, ponendo

$$\begin{aligned} \bullet : G \times \mathbb{R} &\longrightarrow \mathbb{R} \\ f_{a,b} \bullet x &= f(x) = ax + b, \end{aligned}$$

$(\mathbb{R}, \bullet)$ è un G-insieme transitivo (siano $x, y \in \mathbb{R}$, sia $b = x - y \implies f_{1,b} \bullet x = x + b = x + y - x = y$).
Cos'è G_0? $G_0 = \{f_{a,b} \in G \mid f_{a,b}(0) = a \cdot 0 + b = 0\} = \{f_{a,0} \mid a \in \mathbb{R} \setminus 0\}$. Perciò $\mathbb{R} \simeq G/G_0$ (identificazione di tutte le affinità con a uguale).

3.2 Formula delle Orbite

Osservazioni. 1. Sia $(G, \cdot)$ un gruppo e siano $(X, \bullet)$ e $(Y, \odot)$ due G-insiemi disgiunti. Allora G agisce su $X \overset{\circ}{\bigcup} Y$ mediante la mappa che coincide con $\bullet$ su $G \times X$ e con $\odot$ su $G \times Y$. È altresì chiaro che si può estendere il ragionamento a una quantità arbitraria, anche infinita, di G-insiemi disgiunti.

2. Siano $(G, \cdot)$ un gruppo e $(X, \bullet)$ un G-insieme. È immediato verificare che $\forall\, x \in X$, l'orbita $((G \bullet x), \bullet)$ è un G-insieme ed è per definizione transitivo; ad esso si può dunque applicare la proposizione (3.4). Inoltre, una qualunque loro unione è ancora un G-insieme.

Proposizione 3.5. *Sia $(G,\cdot)$ un gruppo e sia $(X,\bullet)$ un G-insieme. Sia $\mathcal{R} \subseteq X$ un sistema di rappresentanti finito per $\sim_G$ (la relazione di equivalenza indotta dall'azione di gruppo), allora*

$$X = \overset{\circ}{\bigcup}_{r\in\mathcal{R}} [r]_{\sim_G} = \overset{\circ}{\bigcup}_{r\in\mathcal{R}} G\bullet r \simeq \overset{\circ}{\bigcup}_{r\in\mathcal{R}} G/G_r.$$

Dim. Le due uguaglianze seguono direttamente dalle proprietà di relazione di equivalenza e dalla definizione di orbita.
Riguardo la relazione di isomorfismo (di G-insiemi), si utilizzino i due punti dell'osservazione precedente: $G\bullet r \simeq_G G/G_r$ e la mappa

$$\begin{array}{rcl} \Phi : \overset{\circ}{\bigcup}_{r\in\mathcal{R}} G/G_r & \longrightarrow & X = \overset{\circ}{\bigcup}_{r\in\mathcal{R}} G\bullet r \\ \Phi(g\cdot G_r) & = & g\bullet r \end{array}$$

è l'isomorfismo cercato

CVD

Teorema 3.6. *(Formula delle orbite) Sia $(G,\cdot)$ un gruppo finito e sia $(X,\bullet)$ un G-insieme finito. Allora, per qualunque sistema di rappresentanti $\mathcal{R} \subseteq X$ rispetto alla relazione $\sim_G$, si ha*

$$|X| = \sum_{r\in\mathcal{R}} \frac{|G|}{|G_r|}$$

Dim. $X \simeq \overset{\circ}{\bigcup}_{r\in\mathcal{R}} G/G_r \implies |X| = \sum_{r\in\mathcal{R}} \left|\frac{G}{G_r}\right| = \sum_{r\in\mathcal{R}} \frac{|G|}{|G_r|}$ per il *Th. di Lagrange.*

CVD

3.3 Automorfismi di gruppi

Definizione 3.6. Sia $(G,\cdot)$ un gruppo. Una mappa $\alpha : G \longrightarrow G$ si dice *automorfismo di gruppo* se è un omomorfismo biunivoco, cioè se

(a) α è biunivoca.

(b) $\alpha(1) = 1$.

(c) $\forall\, x,y \in G,\ \alpha(x\cdot y) = \alpha(x)\cdot\alpha(y)$.

L' insieme di tutti gli automorfismi di G si denota con $Aut(G)$. In particolare, un automorfismo della forma

$$\begin{array}{rcll} i_g : G & \longrightarrow & G & (3.1) \\ i_g(x) & = & g\cdot x\cdot g^{-1} & (3.2) \end{array}$$

si chiama *automorfismo interno* oppure *coniugazione (di sinistra)* tramite g. Si pone infine $Inn(G) := \{i_g \mid g \in G\} \subseteq Aut(G)$.

Proposizione 3.7. *Sia $(G,\cdot)$ un gruppo:*

(a) $(Aut(G),\circ)$ è un gruppo e $Inn(G) \leq Aut(G)$.

(b) Sia $\alpha \in Aut(G)$ e sia $g \in G$. $\alpha \circ i_g \circ \alpha^{-1} = i_{\alpha(g)}$, $\Longrightarrow$ $Inn(G) \triangleleft Aut(G)$.

(c) La mappa

$$\begin{array}{ccc} i : G & \longrightarrow & Aut(G) \\ i(g) & = & i_g \end{array}$$

*è un omomorfismo di gruppi, con $im(i) = Inn(G)$ e $Ker(i) = \{g \in G \mid g \cdot x = x \cdot g \quad \forall x \in G\} =: Z(G)$ (**Nota:** $Z(G)$ viene chiamato* centro del gruppo G*).*

Dim. (a) Anzitutto $Aut(G) \subseteq Symm(G)$ (e $(Symm(G),\circ)$ è un gruppo). Siano $\alpha, \beta \in Aut(G)$ e siano $x, y \in G$; allora anche β^{-1} è biunivoca ed

$$\begin{array}{rcl} & \exists\, u, v \in G \text{ t.c. } \beta(u) = x, \beta(v) = y & \Longrightarrow \\ \Longrightarrow \quad \beta^{-1}(\,x \cdot y\,) \;=\; \beta^{-1}(\,\beta(\,u\,) \cdot \beta(\,v\,)\,) & = \\ = \quad \beta^{-1}(\beta(u \cdot v)) = u \cdot v = \beta^{-1}(x) \cdot \beta^{-1}(y), & \end{array}$$

da cui β^{-1} è un automorfismo di G, ovvero $\beta^{-1} \in Aut(G)$.
Resta da dimostrare che $(\alpha \circ \beta) \in Aut(G)$:

$$\begin{array}{rl} & (\alpha \circ \beta)(x \cdot y) = \alpha(\beta(x \cdot y)) = \alpha(\beta(x) \cdot \beta(y)) \quad = \\ = \quad \alpha(\beta(x)) \cdot \alpha(\beta(y)) = (\alpha \circ \beta)(x) \cdot (\alpha \circ \beta)(y); & \end{array}$$

inoltre la composizione di funzioni biiettive è biiettiva $\Longrightarrow$ $\alpha \circ \beta$ è un automorfismo di G.
Pertanto $(Aut(G),\circ) \leq (Symm(G),\cdot)$.
Riguardo $Inn(G)$, anzitutto si osservi che, siccome $\forall\, g \in G, \forall\, x \in G$,

$$\begin{cases} (i_g \circ i_{g^{-1}})(x) = g \cdot g^{-1} \cdot x \cdot g \cdot g^{-1} = x = id_G(x) \\ (i_{g^{-1}} \circ i_g)(x) = g^{-1} \cdot g \cdot x \cdot g^{-1} \cdot g = x = id_G(x) \end{cases},$$

vale $(i_g)^{-1} = i_{g^{-1}}$, percui $Inn(G)$ è chiuso rispetto agli inversi; per dimostrare che è sottogruppo di $Aut(G)$, basta verificare che è chiuso anche rispetto al prodotto. Sia $x \in G$;

$$(i_g \circ i_h)(x) = (g \cdot h) \cdot x \cdot (h^{-1} \cdot g^{-1}) = i_{g \cdot h}(x),$$

cioè $i_g \circ i_h = i_{g \cdot h} \in Inn(G)$ ed è fatta.

(b) Siano $\alpha \in Aut(G), i_g \in Inn(G)$ qualunque. Allora $\forall\, x \in G$,

$$\begin{array}{rl} & (\alpha \circ i_g \circ \alpha^{-1})(x) \;=\; \alpha\,(i_g(\alpha^{-1}(x))) \;=\; \alpha\,(g \cdot \alpha^{-1}(x) \cdot g^{-1}) \quad = \\ = \quad \alpha(g) \cdot \alpha(\alpha^{-1}(x)) \cdot \alpha(g^{-1}) = \alpha(g) \cdot x \cdot (\alpha(g))^{-1} = i_{\alpha(g)}(x) & \Longrightarrow \\ \Longrightarrow \qquad \alpha \circ i_g \circ \alpha^{-1} \in Inn(G) & \end{array}$$

(c) è stato già dimostrato che $\forall\, g, h \in G$,

$$i(g \cdot h) = i_{g \cdot h} = i_g \circ i_h = i(g) \circ i(h),$$

il che significa che i è omomorfismo di gruppi.
Chiaramente $im(i) = Inn(G)$. infine

$$\begin{aligned} & Ker(i) = \{g \in G \mid i_g(x) = x \ \ \forall x \in G\} \quad = \\ = \quad & \{\, g \in G \ \mid \ g \cdot x \cdot g^{-1} \ = \ x \quad \forall\, x \in G \,\} \quad = \\ = \quad & \{g \in G \mid g \cdot x = x \cdot g \ \ \forall x \in G\} =: Z(G). \end{aligned}$$

CVD

Il centro di un gruppo gode di una notevole proprietà:

Proposizione 3.8. *Sia $(G, \cdot)$ un gruppo e sia $A \leq Z(G)$. Allora $A \lhd G$.*

Dim. $\forall\, g \in G, \forall\, a \in A,\ g \cdot a \cdot g^{-1} = a \cdot g \cdot g^{-1} = a \in A.$

CVD

Definizione 3.7. Sia $(G, \cdot)$ un gruppo. L'insieme $X = G$ con la mappa

$$\begin{aligned} \bullet : G \times X \quad & \longrightarrow \quad X \\ g \bullet x \quad & = \quad g \cdot x \cdot g^{-1} \end{aligned}$$

diviene un G-insieme detto *G-insieme aggiunto* di G. Inoltre:

(a) $Ker(G, X) = Z(G) \qquad (\chi = i)$;

(b) Un'orbita $G \bullet x = \{g \cdot x \cdot g^{-1} \mid g \in G\} =: {}^G x$ si dice *classe di coniugio* che contiene x. Lo stabilizzatore $G_x = \{g \in G \mid g \cdot x \cdot g^{-1} = x\} =: C_G(x)$ si dice *centralizzante* di x in G.

(c) $|{}^G x| = 1 \iff x \in Z(G)$

(d) Sia $N \lhd G$: Allora $N = \bigcup_{n \in N} {}^G n$

Definizione 3.8. Sia p un numero primo. Se $(G, \cdot)$ è un gruppo finito, tale che $|G| = p^k$, con $k \geq 0$, allora G si dice un *p-gruppo.*

Proposizione 3.9. *Sia $(G, \cdot)$ un p-gruppo, $|G| \neq 1$. Allora $|Z(G)| \neq 1$.*

Dim. Sia $(X, \bullet)$ il G-insieme aggiunto. Sia $\mathcal{R} \subseteq X$ un sistema di rappresentanti per la relazione di equivalenza $\sim$ indotta dall'azione di G. Per $r \in \mathcal{R}$ si ha $[r]_\sim = {}^G r$ e $r \in Z(G) \iff |{}^G r| = 1$. Sia $\mathcal{R}_1 = \{r \in \mathcal{R} \ \mid \ |{}^G r\,| = 1\} \subseteq \mathcal{R}$ e

sia $\mathcal{R}' = \mathcal{R} \setminus \mathcal{R}_1$.
Per la *formula delle orbite*,

$$|G| = |X| = \sum_{r\in\mathcal{R}} |{}^G r| = \sum_{r\in\mathcal{R}_1} |{}^G r| + \sum_{r\in\mathcal{R}'} |{}^G r| =$$
$$= |Z(G)| + \sum_{r\in\mathcal{R}'} |{}^G r| = |Z(G)| + \sum_{r\in\mathcal{R}'} \frac{|G|}{|C_G(r)|}.$$

Per $r \in \mathcal{R}'$,

$$|{}^G r| \neq 1 \implies p \;\Big|\; \frac{|G|}{|C_G(r)|} \implies p \;\Big|\; \sum_{r\in\mathcal{R}'} \frac{|G|}{|C_G(r)|}\,.$$

(Th. di Lagrange).
Sia per assurdo $|G| \neq 1 \;\wedge\; |Z(G)| = 1$:

$$p \;\Big|\; |G| \implies p \;\Big|\; \left(|Z(G)| + \sum_{r\in\mathcal{R}'} \frac{|G|}{|C_G(r)|}\right).$$

Ma allora, vale anche

$$p \;\Big|\; \left(|G| - \sum_{r\in\mathcal{R}'} \frac{|G|}{|C_G(r)|}\right) = |Z(G)|,$$

assurdo.

CVD

3.4 Classi di Coniugio di S_n

Proposizione 3.10. *Sia $\tau \in S_n$, rappresentata come composizione di k cicli disgiunti (il che è sempre possibile) da*

$$\tau = (t_{r_0+1}, \ldots, t_{r_1})(t_{r_1+1}, \ldots, t_{r_2}) \cdots (t_{r_{k-1}+1}, \ldots, t_{r_k}),$$

e sia $\sigma \in S_n$.

Allora $\sigma \circ \tau \circ \sigma^{-1} = (\sigma(t_{r_0+1}), \ldots, \sigma(t_{r_1})) \cdots (\sigma(t_{r_{k-1}+1}), \ldots, \sigma(t_{r_k}))$, cioè $\sigma \circ \tau \circ \sigma^{-1}$ è ancora composta da k cicli disgiunti, ciascuno di lunghezza pari al corrispondente ciclo di τ, i cui elementi si ottengono applicanto σ ai corrispondenti elementi di τ.

Dim. Per snellire le formule, si convenga di sottointendere il prodotto del gruppo $(S_n, \circ)$. Poiché σ è per definizione un'applicazione biunivoca da $\{1, \ldots, n\} \subset \mathbb{N}$ in sé stesso, nulla vieta di caratterizzare la mappa biunivoca $\sigma\tau\sigma^{-1}$ mediante i valori che assume sulle immagini tramite σ degli elementi

di $\{1,\dots,n\}$.
Sia allora $j \in \{r_{s-1}+1,...,r_s\}$ per $s \in \{1,...,k\}$; $\sigma\tau\sigma^{-1}\big(\sigma(t_j)\big) = \sigma\tau(t_j) =$

$$= \begin{cases} \sigma(t_{j+1}) & \text{se } \forall\, s \in \{1,...,k\},\ t_j \neq t_{r_s} \\ \sigma(t_{r_{s-1}+1}) & \text{se } \exists\, s \in \{1,...,k\} \text{ t.c. } t_j = t_{r_s} \end{cases}$$

(questo per la definizione di ciclo: ogni elemento di un ciclo viene mappato nel successivo, l'ultimo nel primo); per gli eventuali elementi $a_i \in \{1,\dots,n\}$ che non compaiono nella rappresentazione a cicli di τ, è ancora più semplice: essendo punti fissi per τ,

$$\sigma\tau\sigma^{-1}\big(\sigma(a_i)\big) = \sigma\tau(a_i) = \sigma(a_i),$$

quindi le immagini tramite σ dei punti fissi di τ sono punti fissi di $\sigma\tau\sigma^{-1}$.
In conclusione

$$\sigma\tau\sigma^{-1} =$$

$$= (\sigma(t_1),\sigma(t_2),\dots,\sigma(t_{r_1}))(\sigma(t_{r_1+1}),\dots,\sigma(t_{r_2}))\cdots(\sigma(t_{r_{k-1}+1}),\dots,\sigma(t_{r_k})).$$

CVD

La proposizione permette una classificazione degli elementi di S_n che ne rende facile la manipolazione: un coniugato qualsiasi di un elemento di S_n avrà la sua stessa forma in cicli, dunque non può stare nella classe di coniugio di un elemento con un'altra forma.

Esempi 3.4.

1. Sia $(G,\cdot) = (S_5,\circ) \implies |G| = 5! = 120$. Ricordando che un ciclo è equivalente a tutti quelli ottenuti permutando ciclicamente i suoi elementi (così ad esempio i cicli (a,b,c), (b,c,a) e (c,a,b) rappresentano la stessa permutazione, dunque occorre contarne solo 1), con un po' di calcolo combinatorio si ottiene la partizione in classi di coniugio:

   $^G1$ $\to$ $(\ )(\ )(\ )(\ )(\ )$ $\Rightarrow |^G1| = 1$

   $^G(1,2)$ $\to$ $(\ ,\ )(\ )(\ )(\ )$ $\Rightarrow |^G(1,2)| = \frac{5\cdot4}{2} = 10$

   $^G(1,2,3)$ $\to$ $(\ ,\ ,\ )(\ )(\ )$ $\Rightarrow |^G(1,2,3)| = \frac{5\cdot4\cdot3}{3} = 20$

   $^G(1,2,3,4)$ $\to$ $(\ ,\ ,\ ,\ )(\ )$ $\Rightarrow |^G(1,2,3,4)| = \frac{5\cdot4\cdot3\cdot2}{4} = 30$

   $^G(1,2,3,4,5)$ $\to$ $(\ ,\ ,\ ,\ ,\ )$ $\Rightarrow |^G(1,2,3,4,5)| = \frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$

   $^G((1,2)(3,4))$ $\to$ $(\ ,\ )(\ ,\ )$ $\Rightarrow |^G((1,2)(3,4))| = \frac{\frac{5\cdot4}{2}\cdot\frac{3\cdot2}{2}}{2} = 15$

   $^G((1,2)(3,4,5))$ $\to$ $(\ ,\ )(\ ,\ ,\ )$ $\Rightarrow |^G((1,2)(3,4,5))| = \frac{5\cdot4}{2}\ \frac{3\cdot2\,1}{3} = 20$

Poiché la somma delle cadinalità dà $120 = |G|$, la classificazione è completa: ciascuna permutazione su 5 elementi sta in esattamente una delle precedenti orbite.

Siano $(G, \cdot) = (S_n, \circ)$ e $V = \mathbb{Q}^n = span_{\mathbb{Q}}\{e_1, \ldots, e_n\}$, dove $\{e_1, \ldots, e_n\} = \mathcal{C}$ è la base canonica di $\mathbb{Q}^n$. Si possono rappresentare gli elementi di G anche in forma matriciale in questo modo: anzitutto, si definisca la mappa

$$\begin{aligned} \Pi : G \times \mathcal{C} &\longrightarrow \mathcal{C} \\ \Pi(\sigma, e_k) &= e_{\sigma(k)} \end{aligned}$$

(si osservi che, per la biunivocità di σ, $e_j \neq e_k \implies \Pi(\sigma, e_j) \neq \Pi(\sigma, e_k)$); ricordando ora che un'applicazione lineare è univocamente determinata dalle immagini dei vettori di una base, grazie a Π si può associare ad ogni permutazione di S_n la matrice che rappresenta un'applicazione lineare rispetto alla base canonica. Se si chiama P questa corrispondenza, allora

$$P : S_n \longrightarrow Gl_n(\mathbb{Q})$$

è un omomorfismo iniettivo di gruppi, come il lettore dovrebbe aver cura di verificare.
(*traccia di dimostrazione:* la scelta della base canonica induce un isomorfismo fra lo spazio delle matrici $Gl_n(\mathbb{Q})$ e quello degli endomorfismi $Gl_{\mathbb{Q}}(V)$, quindi anzichè studiare le matrici, si può operare con gli endomorfismi associati; in tal modo si ottiene

$$\begin{aligned} P(\sigma) &= S : (e_k \mapsto e_{\sigma(k)}) \in GL_{\mathbb{Q}}(V) \\ p(\tau) &= T : (e_k \mapsto e_{\tau(k)}) \in GL_{\mathbb{Q}}(V) \\ P(\sigma \circ \tau) &= R : (e_k \mapsto e_{\sigma \circ \tau(k)}) \in GL_{\mathbb{Q}}(V) \\ P(\sigma) \cdot P(\tau) &= S \circ T : (e_k \mapsto e_{\tau(k)} \mapsto e_{\sigma(\tau(k))} = e_{\sigma \circ \tau(k)}) \end{aligned}$$

da cui $P(\sigma \circ \tau) = P(\sigma) \cdot P(\tau)$; l'iniettività è ovvia, perché permutazioni diverse scambiano gli indici dei vettori di $\mathcal{C}$ in modo diverso.)

Esempi 3.5.

1. Sia $n = 3, \sigma = (1, 2)$. Quindi $\Pi(\sigma, e_1) = e_2$, $\Pi(\sigma, e_2) = e_1$ e $\Pi(\sigma, e_3) = e_3$, perciò
$$\sigma \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Le matrici associate a permutazioni di S_n mediante P hanno per costruzione una forma particolare: si ottengono a partire dalla matrice identità permutando opportunamente i suoi vettori colonna (si riveda la definizione della mappa Π), quindi sono sicuramente invertibili.

Grazie al teorema di Binet, la funzione $det : GL_n(\mathbb{Q}) \longrightarrow \mathbb{Q} \setminus 0$ è un omomorfismo di gruppi. D'altra parte, il determinante di una matrice di permutazione è sempre 1 oppure -1, a seconda che si scambino un numero rispettivamente pari o dispari di vettori colonna rispetto alla matrice identità.

Definizione 3.9. Sia $sgn := det \circ P : S_n \longrightarrow \{\pm 1\}$. Allora sgn è un omomorfismo di gruppi, suriettivo se $n > 1$.

Il nucleo dell'omomorfismo sgn, che come è noto è un sottogruppo normale di S_n, si dice *gruppo alternante* e si indica con A_n.

$\forall\, n > 1$, $|A_n| = \frac{1}{2}n!$: infatti, per il *Th dell'omomorfismo* si ha che

$$\frac{|S_n|}{|A_n|} = |\{\pm 1\}| \implies |A_n| = \frac{|S_n|}{|\{\pm 1\}|} = \frac{|S_n|}{2} = \frac{n!}{2} \tag{3.3}$$

Definizione 3.10. Sia $(G, \cdot)$ un gruppo. G si dice *semplice* se non possiede sottogruppi normali propri, cioè se $\forall\, N \leq G$,

$$N \lhd G \implies N = \{1_G\} \ \vee \ N = G.$$

Esempi 3.6.

1. Se $n > 1$, $(S_n, \circ)$ non è semplice perché $A_n \lhd S_n$ e $A_n \neq \{1_G\} \wedge A_n \neq G$.

Storiella. Tutti i gruppi semplici finiti sono conosciuti. La dimostrazione di questo fatto è lunga circa 15000 pagine ed è stata completata attorno al 1980 da un gruppo internazionale di ricercatori, coordinati da Daniel Gorenstein.

La lista di tali gruppi comprende

- C_p (gruppi ciclici con p primo)
- A_n per $n \geq 5$
- $PSl_n(\mathbb{F}) := Sl_n(\mathbb{F})/Z(Sl_n(\mathbb{F}))$ e fratelli
- 26 esempi strani, cioè difficilmente classificabili:
  - i gruppi di Mathieu (conosciuti già intorno al 1900)
  - il *Baby Monster B*
  - *the Monster M*, la cui cardinalità è dell'ordine di 10^{55}

La cattiva notizia è che è estremamente probabile che l'enorme mole di 15000 pagine prodotta contenga almeno un errore.

Teorema 3.11. *$(A_5, \circ)$ è semplice.*

Dim. Anzitutto, sia $\sigma \in S_n$ una permutazione rappresentata da un unico ciclo di lunghezza k con $k \leq n$; allora $sgn(\sigma) = (-1)^{k+1}$. Infatti, si supponga $k = 2$: in tal caso, $\sigma = (a, b)$ con $a, b \in \{1, \dots, n\}, a \neq b$, perciò $det(P(\sigma)) = -1 = (-1)^{2+1}$; si supponga ora l'asserto valido per cicli di lunghezza fino a $k-1$: giacché $(a_1, \dots, a_{k-1}, a_k) = (a_1, \dots, a_{k-1})(a_{k-1}, a_k)$,

$$sgn(a_1, \dots, a_{k-1}, a_k) = sgn(a_1, \dots, a_{k-1})sgn(a_{k-1}, a_k) = (-1)^{k-1+1}(-1)$$

(P è omomorfismo di gruppi).

Si consideri ora una permutazione τ rappresentata da r cicli disgiunti, di lunghezze rispettive $l_1, \dots, l_r$; invocando ancora il fatto che P sia omomorfismo,

$$sgn(\tau) = (-1)^{l_1+1}(-1)^{l_2+1} \dots (-1)^{l_r+1} = (-1)^{r+\sum_{j=1}^{r} l_r}$$

Riassumendo, una permutazione $\pi \in S_n$ rappresentata da r cicli disgiunti di lunghezze rispettive $l_1, \dots, l_r$ appartiene ad A_n se e solo se

$$r + \sum_{j=1}^{r} l_r = 2n \text{ per un certo } n \in \mathbb{N} \text{ (cioè se e solo se è un numero pari)}$$

Ma grazie alla proposizione (3.10), si può ottenere una maneggevole partizione degli elementi di S_n in classi caratterizzate proprio da numero e lunghezza dei cicli, cioè esattamente gli attributi che servono per stabilire l'appartenensa ad A_n.

Le classi di coniugio di S_5 sono state già elencate negli esempi (3.4); quelle di $A_5 =: G$ sono (poiché $A_5 \lhd S_5$, A_5 deve includere interamente le classi di coniugio di ciascun suo elemento):

i) ${}^{G}id$ di ordine 1

ii) ${}^{G}(12)(34)$ di ordine 15

iii) ${}^{G}(1, 2, 3)$ di ordine 20

iv) ${}^{G}(12345)$ di ordine 24

Sia $N \lhd G$ e si supponga per assurdo $N \neq \{id\}$ e $N \neq G$. Dal *Th di Lagrange*,

$$|N| \mid |G| = 60; \tag{3.4}$$

ma per l'assunzione precedente, $\exists \sigma \in G \setminus \{id\}$ e, poiché N è normale, ${}^{G}\sigma \subseteq G$, da cui, tenuto conto che obbligatoriamente ${}^{G}id \subset N$, segue che le possibilità sono solo

$$|N| \in \{16, 21, 25, 36, 40, 45\} \tag{3.5}$$

(formula ottenuta combinando in tutti i modi concessi gli ordini delle orbite sopraindicate).

Le condizioni (3.4) e (3.5) sono palesemente incompatibili, percui non può esistere un sottogruppo di A_5 che le soddisfi entrambe e si è così giunti all'assurdo: la contraddizione nasce dall'aver supposto l'esistenza di un sottogruppo normale *non banale* di A_n, che in conclusione risulta semplice.

CVD

Capitolo 4

Anelli

4.1 Anelli

Definizione 4.1. Un gruppo abeliano $(R, +)$ con una mappa (moltiplicazione) $R \times R \Longrightarrow R$ si dice *anello* se

(a) $\forall\, r, s, u, v \in R$ vale $(r+s)\cdot(u+v) = r\cdot u + r\cdot v + s\cdot u + s\cdot v$;

(b) $\forall\, r, s, t \in R$ vale $(r\cdot s)\cdot t = r\cdot(s\cdot t)$;

(c) $\exists\, 1_R \in R$ t.c. $\forall\, r \in R$ vale $1_R\cdot r = r\cdot 1_R = r$.

Definizione 4.2. Un'anello R si dice *commutativo* se $\forall\, r, s \in R, r\cdot s = s\cdot r$.

Definizione 4.3. Un'anello commutativo R si dice un *dominio d'integrità* se $1 \neq 0$ e $r\cdot s = 0 \Longrightarrow r = 0 \vee s = 0$.

Definizione 4.4. Un'anello R si dice un *campo* se R è un dominio d'integrità e $\forall\, r \in R, r \neq 0 \quad \exists\, r^{-1} \in R$ t.c. $r\cdot r^{-1} = 1_R$.

Esempi 4.1.

1. $\mathbb{K} = \mathbb{R}$ è un campo (anche $\mathbb{C}$, $\mathbb{Q}$ sono campi).
2. $\mathbb{Z}$ è un dominio d'integrità ($\mathbb{Z} \subseteq \mathbb{Q}$).
3. Sia $R = \mathrm{Mat}_{n\times n}(\mathbb{R})$. R è un'anello non commutativo (per $n \geq 2$).
4. Sia X un'insieme, $R = \mathcal{F}(X, \mathbb{R})$. Allora R con

$$(f+g)(x) = f(x) + g(x)$$

$$(f\cdot g)(x) = f(x)\cdot g(x)$$

è un'anello commutativo.
$0(x) = 0 \quad \forall\, x \in X$
$1(x) = 1 \quad \forall\, x \in X$

Sia $X = A \overset{\circ}{\cup} B, \quad A, B \neq \emptyset$.
Sia $M \subseteq X$:

$$1_M(X) = \begin{cases} 1 & \text{per } x \in M \\ 0 & \text{per } x \notin M \end{cases}$$

$1_A + 1_B = 1 \quad (= 1_X)$
$1_A \cdot 1_B = 1_{A \cap B} = 1_\emptyset = 0$
$\Longrightarrow R$ non è un dominio d'integrità.

5. Siano R, S anelli. Allora

$$R \oplus S = \{(r, s) | r \in R, s \in S\}$$

$(r, s) + (t, u) = (r + t, s + u)$
$(r, s) \cdot (t, u) = (r \cdot t, s \cdot u)$
$\Longrightarrow R \oplus S$ è un'anello.
$(1_R, 0) \cdot (0, 1_S) = (0, 0) \Longrightarrow R$ non è un dominio d'integrità.

6. $\mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2 \cdot \mathbb{Z}$
$\mathbb{Z}/n \cdot \mathbb{Z}$ è un campo se e solo se n è un numero primo.
$\mathbb{F}_p = \mathbb{Z}/p \cdot \mathbb{Z}$

Nota. $\mathbb{R} \oplus \mathbb{R} = \mathcal{F}(\{0, 1\}, \mathbb{R})$
$\underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{n \text{ volte}} = \mathcal{F}(\{0, \cdots, n-1\}, \mathbb{R})$

Definizione 4.5. Sia R un anello. $S \subseteq R$ si dice *sottoanello* se $(S, +)$ è un sottogruppo, $1 \in S$, $S \cdot S \subseteq S$.

Definizione 4.6. Sia R un anello. $I \subseteq R$ si dice *ideale* di R se I è un sottogruppo abeliano, $R \cdot I \subseteq I$, $I \cdot R \subseteq I$. Useremo la notazione $I \lhd R$.

Esempi 4.2.

1. $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ (sono sottoanelli).
$\mathbb{R} \lhd \mathbb{R}$, $(0) \lhd \mathbb{R}$ (sono tutti gli ideali di $\mathbb{R}$).

2. $R = \mathbb{Z}$ non contiene sottogruppi propri.
$2 \cdot \mathbb{Z} = \{z \mid z \text{ pari}\}$
$n \cdot \mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$ sono tutti gli ideali di $\mathbb{Z}$.

4.2 Il quoziente canonico

Proposizione 4.1. *Sia R un'anello e sia $I \lhd R$. Allora $(R/I, +, \cdot)$ dove*

$$(r + I) \cdot (s + I) := r \cdot s + I$$

diventa un'anello.

Dim. Siano $u, v \in R$, $r + I = u + I$, $s + I = v + I$. Cioè

$$r - u = i \in I, s - v = j \in I$$

Per verificare che $\cdot\colon R/I \times R/I \longrightarrow R/I$ è ben definita basta dimostrare che

$$u \cdot v + I = r \cdot s + I$$

$r = u + i$, $s = v + j$
$r \cdot s + I = (u + i) \cdot (v + j) + I = u \cdot v + u \cdot j + i \cdot v + i \cdot j + I = u \cdot v + I$
$\Longrightarrow$ il prodotto è ben definito.

(a) $((r + I) + (s + I)) \cdot ((u + I) + (v + I)) = (r + s + I) \cdot (u + v + I) =$
$= ((r + s) \cdot (u + v) + I) = (r \cdot u + s \cdot u + r \cdot v + s \cdot v + I) = (r \cdot u + I) + (s \cdot u + I) +$
$+ (r v + I) + (s v + I) = (r + I)(u + I) + (s + I)(u + I) + (r + I)(v + I) + (s + I)(v + I)$

(b) $((r + I) \cdot (s + I)) \cdot (u + I) = (r \cdot s + I) \cdot (u + I) = (r \cdot s) \cdot u + I$
$(r + I) \cdot ((s + I) \cdot (u + I)) = (r + I) \cdot ((s \cdot u) + I) = r \cdot (s \cdot u) + I$

(c) $(1 + I) \cdot (r + I) = 1 \cdot r + I = r + I$
$(r + I) \cdot (1 + I) = (r \cdot 1 + I) = r + I$
$\Longrightarrow 1_R + I$ è l'elemento neutro.

CVD

4.3 Domini d'integrità e domini principali

Definizione 4.7. Sia R un'anello e sia $I \lhd R$ un'ideale. I si dice *massimale* se $I \neq R$ e $\forall\, J \lhd R$, $J \neq R$, $I \leq J \Longrightarrow I = J$.

Definizione 4.8. Sia R un dominio d'integrità e sia $I \lhd R$. I si dice un *ideale primo* se $I \neq R$ e per $a, b \in R$ t.c. $a \cdot b \in I \Longrightarrow a \in I \vee b \in I$.

Definizione 4.9. Sia R un diminio d'integrità e sia $I \lhd R$. I si dice *principale* se $\exists\, a \in R$ t.c.

$$I = R \cdot a = \{r \cdot a \mid r \in R\}$$

Sia R un anello commutativo, $a \in R$. Allora

$$R \cdot a = \{r \cdot a \mid r \in R\} \lhd R$$

Esempi 4.3.
$R = \mathbb{Z}$
$I_n = n \cdot \mathbb{Z}$ è un ideale principale ($n \in \mathbb{N}_0$).
$I_1 = R$
I_n è primo se e solo se n è un numero primo.

Se n non è primo allora $\exists\, k,\, m \in \mathbb{Z},\, k,\, m \notin \{1,-1\}$ t.c. $n = k \cdot m$
$\Longrightarrow k \cdot m \in n \cdot \mathbb{Z}$ ma $k,\, m \notin n \cdot \mathbb{Z} \Longrightarrow n \cdot \mathbb{Z}$ non è primo.
Sia p un numero primo e siano $a, b, k \in \mathbb{Z}$ t.c. $a \cdot b = k \cdot p \in p \cdot \mathbb{Z}$
Ma a o b deve essere divisibile da p ($\Longleftrightarrow a \in p \cdot \mathbb{Z} \vee b \in p \cdot \mathbb{Z}$)
$\Longrightarrow p \cdot \mathbb{Z}$ è un'ideale primo.

$$\begin{aligned} a &= \mathcal{E}_a \cdot P_1^{\alpha_1} \cdot \ldots \cdot P_r^{\alpha_r} \quad \mathcal{E}_a,\, \mathcal{E}_b \in \{\pm 1\} \\ b &= \mathcal{E}_b \cdot P_1^{\beta_1} \cdot \ldots \cdot P_r^{\beta_r} \quad \alpha^j,\, \beta^j \in \mathbb{N}_0 \\ a \cdot b &= \mathcal{E}_a \cdot \mathcal{E}_b \cdot P_1^{\alpha_1 + \beta_1} \cdot \ldots \cdot P_r^{\alpha_r + \beta_r} \end{aligned}$$

$$\exists\, j \text{ t.c. } p = p_j \Longrightarrow \alpha_j + \beta_j \geq 1 \Longrightarrow \alpha_j \geq 1 \vee \beta_j \geq 1$$

Proposizione 4.2. *Sia R un'anello, $I \lhd R$. Allora $R = I \Longleftrightarrow 1 \in I$.*

Dim. Se $R = I, 1_R \in R = I$
Se $1_R \in R, r \in R \Longrightarrow r = r \cdot 1_R \in I$

CVD

Proposizione 4.3. *Sia R un dominio d'integrità e sia $I \lhd R$.*

(a) R/I è un campo $\Longleftrightarrow$ I è massimale

(b) R/I è un dominio d'integrità $\Longleftrightarrow$ I è primo

Dim.

(a) Sia R/I un campo e sia $J \lhd R$, $I \leq J$.

$$J/I \lhd R/I \quad ((r + I) \cdot (j + I) = r \cdot j + I \in J/I)$$

$$\Longrightarrow J/I = (0) \text{ o } J/I = R/I$$

Se $J/I = R/I \Longrightarrow J = R$

$$\Longrightarrow J/I = (0) \Longrightarrow J = I$$

$\Longrightarrow I$ è massimale.
Viceversa, sia $I \lhd R$ massimale.

$$0_{R/I} = I = 0 + I$$

$$1_{R/I} = 1 + I$$

Se $0_{R/I} = 1_{R/I} \Longrightarrow 1 \in I \Longrightarrow R = I$, assurdo

$$\Longrightarrow 0_{R/I} \neq 1_{R/I}$$

Sia $a+I \in R/I$, $a+I \neq I (\iff a \notin I)$
Sia $J = R\cdot a + I$, $J \lhd R$. Infatti J è un sottogruppo abeliano e per

$$r \in R,\ b = s\cdot a + i \text{ con } s \in R,\ i \in I \Longrightarrow r\cdot b = (r\cdot s)\cdot a + r\cdot i \in R\cdot a + I$$

Poichè $a \notin I$ ma $a \in J \Longrightarrow I \neq J$.

$$I \leq J \Longrightarrow J = R$$

$$\Longrightarrow \exists\, r \in R,\ i \in I \text{ t.c } 1 = r\cdot a + i$$

$$(r+i)\cdot(a+i) = r\cdot a + I = (1-i) + I = 1 + I$$

$$\Longrightarrow (r+I) = (a+I)^{-1}$$

$\Longrightarrow R/I$ è un campo.

(b) Sia $I \lhd R$ un'ideale primo.
Se $0+I = 1+I \Longrightarrow 1 \in I \Longrightarrow I = R$, assurdo
$\Longrightarrow 0+I \neq 1+I$
Siano $a, b \in R$ t.c. $(a+I)\cdot(b+I) = 0+I$

$$(a+I)\cdot(b+I) = a\cdot b + I = I \Longrightarrow a\cdot b \in I \Longrightarrow a \in I \vee b \in I$$

$$a \in I \Longrightarrow a + I = I = 0_{R/I}$$

$$b \in I \Longrightarrow b + I = I = 0_{R/I}$$

$\Longrightarrow R/I$ è un dominio d'integrità.
Viceversa, sia R/I un dominio d'integrità.

$$1 + I \neq 0 + I \Longrightarrow 1 \notin I \Longrightarrow I \neq R$$

Siano $a, b \in R$ t.c. $a\cdot b \in I$

$$\Longrightarrow (a+I)\cdot(b+I) = a\cdot b + I = I = 0_{R/I}$$

$$\Longrightarrow a + I = 0_{R/I} = I (\iff a \in I) \vee b + I = 0_{R/I} = I (\iff b \in I)$$

$\Longrightarrow I$ è primo.

CVD

Proposizione 4.4. *Sia R un dominio d'integrità, $|R| < \infty \Longrightarrow R$ è un campo.*

Dim. Sia $a \in R \setminus \{0\}$. Allora $\Phi_a : R \longrightarrow R$, $\Phi_a(r) = a\cdot r$ è un'omomorfismo di gruppi (abeliani).

$$\ker(\Phi_a) = \{r \in R \mid r\cdot a = 0\} = (0)$$

$$\Longrightarrow |im(\Phi_a)| = |R|/|(0)| = |R|$$

$$\Longrightarrow im(\Phi_a) = R$$

$$1 \in im(\Phi_a) \Longrightarrow \exists\, r \in R \text{ t.c. } 1 = r\cdot a$$

$\Longrightarrow R$ è un campo.

CVD

Esempi 4.4.

1. Sia K un campo.
   $R = K[x, y]$
   $I = R \cdot x$
   $\Longrightarrow R/I \cong K[y]$
   I è primo ma non è massiamale.
   $J = R \cdot x + R \cdot y \quad (R/J \cong K)$
   J è massimale .

2. $R = \mathbb{Z}$, $I = (0) \Longrightarrow I$ è primo ma non massimale.

4.4 L'aritmetica di $\mathbb{Z}$

(1) $\mathbb{Z}$ contiene tutti i numeri naturali $\mathbb{N} = \{1, 2, \cdots\}$

(2) $\mathbb{Z}^* = \{a \in \mathbb{Z} \mid \exists\, b \in \mathbb{Z} \text{ t.c } a \cdot b = 1\} = \{1, -1\}$

(3) Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Si dice che a *divide* b se $\exists\, k \in \mathbb{Z}$ t.c. $b = a \cdot k$. Scriviamo $a \,\big|\, b$.

(4) Siano $a, b \in \mathbb{Z} \setminus \{0\}$. Il numero $d \in \mathbb{N}$ si dice *massimo comune divisore* di a e b se $d = \max\{n \in \mathbb{N} \mid n \,\big|\, a \wedge n \,\big|\, b\}$ $(\leq \min\{|a|, |b|\})$. Scriviamo $d = \mathrm{MCD}(a, b)$.

(5) Il *minimo comune multiplo* di $a, b \in \mathbb{Z}$ è $m = \min\{n \in \mathbb{N} \mid a \,\big|\, n \wedge b \,\big|\, n\}$. Scriviamo $m = \mathrm{mcm}(a, b)$.

- Sia $n \in \mathbb{Z} \setminus \{0\}, a, b \in \mathbb{Z} \setminus \{0\}$ t.c. $n|a \wedge n|b \Longrightarrow n|MCD(a, b)$
- Sia $n \in \mathbb{Z} \setminus \{0\}, a, b \in \mathbb{Z} \setminus \{0\}$ t.c. $n \wedge b|n \Longrightarrow mcm(a, b)|n$

(6) $a, b \in \mathbb{Z} \setminus \{0\}$ si dicono *coprìmi* se $\mathrm{MCD}(a, b) = 1$
$(\Longleftrightarrow \exists\, k_1, k_2 \in \mathbb{Z}$ t.c. $1 = a \cdot k_1 + b \cdot k_2)$

(7) Divisione con resto: esiste una funzione $\delta : \mathbb{Z} \longrightarrow \mathbb{N}_0$ tale che
$\forall\, a, b \in \mathbb{Z}, a \neq 0\ \exists\, q, r \in \mathbb{Z}$ t.c. $b = a \cdot q + r$, $\delta(r) < \delta(a)$.
$(\delta^{-1}(\{0\}) = \{0\})$

Proposizione 4.5. *Ogni ideale di $\mathbb{Z}$ si può scrivere come $a \cdot \mathbb{Z}$, $a \in \mathbb{Z}$.*

Dim. Sia $I \lhd \mathbb{Z}, I \neq (0)$.
Sia $a \in I \setminus \{0\}$ t.c. $\delta(a) = \min\{\delta(x) \mid x \in I \setminus \{0\}\}$.
Supponiamo che $\exists\, b \in I / a \cdot \mathbb{Z} \Longrightarrow \exists\, q, r \in \mathbb{Z}$ t.c. $b = q \cdot a + r, \delta(r) < \delta(a)$.
$\Longrightarrow r \neq 0$ (altrimenti $b \in a \cdot \mathbb{Z}$, assurdo).
$\Longrightarrow r \neq 0 \wedge \delta(r) < \delta(a), r = b - q \cdot a \in I \setminus \{0\}$, assurdo .
$\Longrightarrow I = a \cdot \mathbb{Z}$.

CVD

(8) Per tutti gli ideali $I \lhd \mathbb{Z}$ esiste un'unico elemento $n_I \in \mathbb{N}_0$ t.c. $I = n_I \cdot \mathbb{Z}$.
(Se $n, m \in \mathbb{N}_0$ t.c. $n\cdot\mathbb{Z} = m\cdot\mathbb{Z} \Longrightarrow m \,|\, n \wedge n \,|\, m \Longrightarrow n = m$).

(9) Divisione con resto in $\mathbb{N}_0$.
$\forall\, a, b \in \mathbb{Z}$, $a \neq 0$ t.c. $\exists\, q, r \in \mathbb{Z}$, $r \geq 0$ t.c. $b = q\cdot a + r$
Sia $d \in \mathbb{N}$ t.c. $d \,|\, a \wedge d \,|\, b \Longrightarrow d \,|\, r$
$\Longrightarrow d \,|\, a \wedge d \,|\, r \Longrightarrow \cdots$

(10) Sia $I = n\cdot\mathbb{Z}$, $J = m\cdot\mathbb{Z}$.
$J + I = d\cdot\mathbb{Z}$ dove $d = \mathrm{MCD}(n, m)$
Sia $d = \mathrm{MCD}(n, m) \Longrightarrow d \,|\, n \wedge d \,|\, m$
$\Longrightarrow \exists\, k_1, k_2 \in \mathbb{Z}$ t.c. $m = k_1\cdot d$, $n = k_2\cdot d$
$\Longrightarrow m, n \in d\cdot\mathbb{Z} \Longrightarrow m\cdot\mathbb{Z} + n\cdot\mathbb{Z} \leq d\cdot\mathbb{Z}$
Sia $e \in \mathbb{N}$ t.c. $m\cdot\mathbb{Z} + n\cdot\mathbb{Z} = e\cdot\mathbb{Z}$
$\Longrightarrow \exists\, l_1, l_2 \in \mathbb{Z}$ t.c. $e = m\cdot l_1 + n\cdot l_2 \Longrightarrow d \,|\, e$
$e \,|\, m \wedge e \,|\, n \Longrightarrow e \,|\, d \Longrightarrow e = d$
$I \cap J = \mathrm{mcm}(n, m)\cdot\mathbb{Z}$

4.5 Domini principali ed euclidei

Definizione 4.10. Un dominio d'integrità R si dice *dominio principale* se tutti gli ideali $I \lhd R$ sono principali, cioè $\exists\, a \in R$ t.c. $I = R\cdot a$.

Definizione 4.11. Un dominio d'integrità R si dice un *dominio euclideo* se esiste una mappa $\delta : R \longrightarrow \mathbb{N}_0$ tale che:

(a) R soddisfa la seguente proprietà:
sia $r \in R$. Allora $\delta(r) = 0 \Longleftrightarrow r = 0$

(b) R soddisfa la divisione con resto (rispetto a δ), cioè
$a, b \in R \setminus 0 \Longrightarrow \exists\, q, r \in R$ t.c. $b = q\cdot a + r \wedge \delta(r) < \delta(a)$.

Proposizione 4.6. *R dominio euclideo $\Longrightarrow$ R dominio principale*

Dim. Sia $I \lhd R, I \neq 0, R$ ($\Longrightarrow$ in questi casi $0 = R\cdot 0$ o $R = R\cdot 1$)
Sia $\delta(a) = \min\{\delta(b) \mid b \in I \setminus \{0\}\}$
Supponiamo per assurdo che $I \neq R\cdot a$.
Sappiamo che $R\cdot a \subseteq I$
$\Longrightarrow \exists\, c \in I \setminus R\cdot a \Longrightarrow c = q\cdot a + r$, $\delta(r) < \delta(a)$
$r = 0 \Longrightarrow c = q\cdot a \in R\cdot a$, assurdo.
$r \neq 0 \Longrightarrow r = c - q\cdot a \in I \setminus \{0\}$ e
$\delta(r) < \delta(a) = \min\{\delta(b) \mid b \in I \setminus \{0\}\}$, assurdo.
$\Longrightarrow I = R\cdot a$

CVD

Esempi 4.5.

1. $R = \mathbb{Z}$, $\delta : \mathbb{Z} \longrightarrow \mathbb{N}_0$, $\delta = |\quad|$ (valore assoluto)
2. Sia K un campo e sia $R = K[x]$

   $$grad : K[x] \longrightarrow \mathbb{N}_0 \text{ (associa a un polinomio il suo grado)}$$
   $$grad(f \cdot g) = grad(f) + grad(g), \quad f, g \neq 0$$

   I polinomi invertibili sono

   $$K[x]^* = \{f \in K[x] \mid \exists\, g \in K[x] \text{ t.c. } f \cdot g = 1\} =$$
   $$= \{f \in K[x] \mid grad(f) = 0, f \neq 0\} = K^*$$

   - $K[x]$ è un dominio d'integrità
     Siano $f, g \in K[x]$ t.c. $f \cdot g = 0$
     Supponiamo per assurdo che $f, g \neq 0$

     $$0 = grad(f \cdot g) = grad(f) + grad(g)$$
     $$\Longrightarrow grad(f) = grad(g) = 0$$
     $$\Longrightarrow f, g \in K[x]^* = K^* \text{ (elementi costanti non nulli)}$$

     Ma K è un campo, quindi

     $$f \cdot g = 0 \Longrightarrow f = 0 \vee g = 0, \text{ assurdo}$$

     $\Longrightarrow K[x]$ è un dominio d'integrità.
   - $K[x]$ è un dominio euclideo per $\delta : K[x] \longrightarrow \mathbb{N}_0$

     $$\delta(f) = \begin{cases} 0 & \text{per } f = 0 \\ 1 + grad(f) & \text{per } f \neq 0 \end{cases}$$

     Sia $f \in K[x]$. Allora

     $$\delta(f) = 0 \Longleftrightarrow f = 0$$

     Siano $a, b \in K[x]$, $b \neq 0$, $grad(a) \geq 1$

     $$\Longrightarrow \exists\, q, r \in K[x] \text{ t.c. } b = a \cdot q + r, grad(r) \leq grad(a)$$
     $$\Longrightarrow \begin{cases} r = 0 : \delta(r) = 0 < grad(a) < \delta(a) \\ r \neq 0 : \delta(r) = 1 + grad(r) < 1 + grad(a) = \delta(a) \end{cases}$$

     Sia $a \in K[x] \setminus \{0\}, grad(a) = 0$

     $$\Longrightarrow b = a \cdot \frac{b}{a} \Longrightarrow q = \frac{b}{a}, r = 0$$
     $$\Longrightarrow \delta(r) = 0 < \delta(a) = 1$$

     $\Longrightarrow K[x]$ è un dominio euclideo.

4.6 Interi di Gauss

$\mathbb{C} = \mathbb{R} + i\cdot\mathbb{R}$, $i^2 = -1$

- $(a+ib)\cdot(c+id) = (a\cdot c - b\cdot d) - i(a\cdot d + b\cdot c)$
- $(a+ib) + (c+id) = (a+c) + i(b+d)$
- $\overline{a+ib} = a - ib$. Il passaggio al coniugato è un'automorfismo di $\mathbb{C}$. Infatti
  $\overline{(a+ib)\cdot(c+id)} = (a\cdot c - b\cdot d) - i(a\cdot d + b\cdot c)$
  $\overline{(a+ib)}\cdot\overline{(c+id)} = (a-ib)\cdot(c-id) = (a\cdot c - b\cdot d) - i(a\cdot d + b\cdot c)$

$$\Longrightarrow \overline{(a+ib)\cdot(c+id)} = \overline{(a+ib)}\cdot\overline{(c+id)}$$

$$\overline{(a+ib)} + \overline{(c+id)} = (a+c) - i(b+d) = \overline{(a+ib)+(c+id)}$$

- $(a+ib)\cdot\overline{(a+ib)} = (a+ib)\cdot(a+ib) = a^2 + b^2 \geq 0$
- $\overline{(a+ib)} = a + ib \Longleftrightarrow b = 0$
- $|a+ib| = \sqrt{a^2+b^2} = \sqrt{(a+ib)\cdot(a-ib)}$
- $\exp(it) = \sum_{n=0}^{+\infty} \frac{1}{n!}\cdot(it)^n$ converge assolutamente su ogni compatto di $\mathbb{C}$ ed è una funzione olomorfa (differenziabile nel campo complesso).

$$\exp(it) = \sum_{k\in\mathbb{N}_0}^{+\infty} \frac{1}{(2k)!}\cdot(it)^{2k} + \sum_{k\in\mathbb{N}_0}^{+\infty} \frac{1}{(2k+1)!}\cdot(it)^{2k+1} =$$

$$= \sum_{k\in\mathbb{N}_0}^{+\infty} \frac{1}{(2k)!}\cdot(-1)^k\cdot t^{2k} + i\sum_{k\in\mathbb{N}_0}^{+\infty} \frac{1}{(2k+1)!}\cdot(-1)^k\cdot t^{2k+1} =$$

$$= cos(t) + i\,sin(t)$$

$\Longrightarrow |\exp(it)| = 1$

Definizione 4.12. Il sottoanello $R = \mathbb{Z} + i\cdot\mathbb{Z} \subseteq \mathbb{C}$ si definisce gli *interi di Gauss* ($R = \mathbb{Z}[i]$).

- R è un dominio d'integrità.
- $\mathbb{C}$ è il piano di Gauss.
- Sia $z \in \mathbb{C} \Longrightarrow \exists\, y \in \mathbb{Z}[i]$ t.c. $|z-y| \leq \frac{\sqrt{2}}{2} \leq 1$
- $\mathbb{Z}[i]$ è un dominio euclideo.

$$\delta : \mathbb{Z}[i] \longrightarrow \mathbb{N}_0 \text{ t.c. } \delta(n+im) = n^2 + m^2 = (n+im)^2$$

Siano $a, b \in \mathbb{Z}[i] \setminus \{0\}$

$$\implies b \cdot a^{-1} \in \mathbb{C} \implies \exists\, q \in \mathbb{Z}[i] \text{ t.c. } |b \cdot a^{-1} - q|^2 < 1$$

$$\implies |b - q \cdot a|^2 < |a|^2$$

$$\implies \exists\, q,\ r = b - q \cdot a \in \mathbb{Z}[i] \text{ t.c. } b = q \cdot a + r \wedge \delta(r) < \delta(a)$$

- $\mathbb{Z}[i]$ è un dominio principale, cioè

$$\forall\, I \lhd \mathbb{Z}[i] \exists\, a \in \mathbb{Z}[i] \text{ t.c. } I = \mathbb{Z}[i] \cdot a$$

- $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

4.7 Elementi irriducibili

Nota. Sia R un dominio d'integrità.

- Siano $a, b \in R \setminus \{0\}$. Allora $a \,|\, b \iff b \in R \cdot a \iff \exists\, k \in R$ t.c. $b = k \cdot a$.
- Un elemento $q \in R^*$ si dice un'unità.
- Sia $q \in R$. Allora $q \in R^* \iff R \cdot q = R$
  $q \in R^* \implies \exists\, q^{-1} \in R \implies 1 = q \cdot q^{-1} \in R \cdot q \implies R \cdot q = R$
  Viceversa, $R \cdot q = R \implies \exists\, r \in R$ t.c. $r \cdot q = 1 \quad (r = q^{-1})$

Definizione 4.13. Sia R un dominio d'integrità. Un elemento $q \in R \setminus R^*$ si dice *primo* se

$$q \,|\, x \cdot y \text{ per } x, y \in R \setminus \{0\} \implies q \,|\, x \vee q \,|\, y$$

Definizione 4.14. Sia R un dominio d'integrità. Un elemento $q \in R \setminus \{0\}$ si dice *irriducibile* se

$$q = x \cdot y \text{ per } x, y \in R \setminus \{0\} \implies x \in R^* \vee y \in R^*$$

Proposizione 4.7. *$q \in R$ è primo $\iff$ $R \cdot q$ è un ideale primo*

Dim. Sia q primo e siano $a, b \in R$ t.c. $a \cdot b \in R \cdot q$

$$\implies q \,|\, a \cdot b \implies q \,|\, a \vee q \,|\, b$$

Se $q \,|\, a \implies a \in R \cdot q$, se $q \,|\, b \implies b \in R \cdot q$
Viceversa, sia $R \cdot q$ un ideale primo e sia $q \,|\, a \cdot b$ per $a, b \in R$

$$\implies a \cdot b \in R \cdot q \implies a \in R \cdot q \vee b \in R \cdot q \quad (\iff q \,|\, a \vee q \,|\, b)$$

CVD

Proposizione 4.8. *Sia R un dominio d'integrità e sia $q \in R \setminus R^*$.*

(a) $R{\cdot}q$ massimale $\Longrightarrow$ q primo

(b) q primo $\Longrightarrow$ $q = 0$ o q irriducibile

Dim.

(a) $R{\cdot}q$ massimale $\Longrightarrow$ $R{\cdot}q$ primo $\Longrightarrow$ q primo

(b) Sia q primo, $q \neq 0$ e siano $x, y \in R$ t.c. $q = x{\cdot}y \Longrightarrow q|x \vee q|y$

$$q|x \Longleftrightarrow \exists\, r \in R \setminus \{0\} \text{ t.c. } x = q{\cdot}r \Longleftrightarrow q = q{\cdot}r{\cdot}y \Longleftrightarrow q{\cdot}(1 - r{\cdot}y) = 0$$

$$\Longleftrightarrow (1 - r{\cdot}y) = 0 \Longleftrightarrow y \in R^*$$

$$q|y \Longleftrightarrow \exists\, s \in R \setminus \{0\} \text{ t.c. } y = q{\cdot}s \Longleftrightarrow q = q{\cdot}s{\cdot}x \Longleftrightarrow q{\cdot}(1 - s{\cdot}x) = 0$$

$$\Longleftrightarrow (1 - s{\cdot}x) = 0 \Longleftrightarrow x \in R^*$$

CVD

Proposizione 4.9. *Sia R un dominio principale e sia $q \in R \setminus R^*$, $q \neq 0$. Allora le seguenti affermazioni sono equivalenti:*

(i) q è irriducibile

(ii) q è primo

(iii) $R{\cdot}q$ è massimale

Dim. R dominio d'integrità: $R{\cdot}q$ massimale $\Longrightarrow$ q primo .
Per la Proposizione 3.7, q primo $\Longrightarrow$ q irriducibile.
Basta dimostrare che (i) $\Longrightarrow$ (iii).
Sia $q \in R \setminus R^*$, $q \neq 0$ irriducibile e sia $I \lhd R$ t.c. $R{\cdot}q \subset I \quad (R{\cdot}q \neq I)$.
$I = R{\cdot}a$, $q \in R{\cdot}a \Longrightarrow q = r{\cdot}a$ per un certo $r \in R$.
q irriducibile $\Longrightarrow a \in R^* \vee r \in R^*$
$a \in R^* \Longrightarrow R{\cdot}a = R$
$r \in R^* \Longrightarrow \exists\, r^{-1} \in R$ t.c. $a = q{\cdot}r^{-1} \Longrightarrow R{\cdot}a \subseteq R{\cdot}q \Longrightarrow R{\cdot}q = I$, assurdo.
$I = R \Longrightarrow R{\cdot}q$ è massimale.

CVD

4.8 Omomorfismi di anelli

Definizione 4.15. Siano R, S anelli. Una mappa $\Phi : R \longrightarrow S$ si dice un'*omomorfismo di anelli* se:

(a) $\Phi : (R, +) \longrightarrow (S, +)$ è un'omomorfismo di gruppi abeliani

(b) $\Phi(1_R) = 1_S$

(c) $\Phi(r \cdot t) = \Phi(r) \cdot \Phi(t),\ \forall\, r, t \in R$

Esempi 4.6.

1. Se $R \leq S$, l'inclusione $i : R \longrightarrow S$ è un'omomorfismo di anelli.
2. Se $I \lhd R$, la proiezione canonica $\Pi_I : R \longrightarrow R/I$ è un'omomorfismo di anelli. Infatti

$$\Pi_I(r \cdot s) = r \cdot s + I = (r + I) \cdot (s + I) = \Pi_I(r) \cdot \Pi_I(s)$$

Proposizione 4.10. *Sia $\Phi : R \longrightarrow S$ un'omomorfismo di anelli. Allora $im(\Phi)$ è un sottoanello si S e $\ker(\Phi)$ è un'ideale di R.*

Dim.

$$(\Phi(R), +) \subseteq (S, +),\ \Phi(1_R) = 1_S \in im(\Phi)$$

Sia $s_1 = \Phi(r_1), s_2 = \Phi(r_2) \in im(\Phi)$

$$\Longrightarrow s_1 \cdot s_2 = \Phi(r_1) \cdot \Phi(r_2) = \Phi(r_1 \cdot r_2) \in im(\Phi)$$

$\Longrightarrow im(\Phi)$ è un sottoanello di S.
Sia $I = \ker(\Phi), (I, +) \leq (R, +)$. Sia $i \in I, r \in R$

$$\Phi(r \cdot i) = \Phi(r) \cdot \Phi(i) = \Phi(r) \cdot 0 = 0$$

In ogni anello
$r \cdot 0 = 0, 0 \cdot r = 0$
$r \cdot 0 = r \cdot (1 - 1) = r \cdot 1 + r \cdot (-1) = r + (-r) = 0$
$0 \cdot r = (1 - 1) \cdot r = (1 + (-1)) \cdot r = r - r = 0$

$$\Phi(i \cdot r) = \Phi(i) \cdot \Phi(r) = 0 \cdot \Phi(r) = 0$$

$\Longrightarrow I$ è un'ideale di R.

CVD

Proposizione 4.11. *Sia $\Phi : R \longrightarrow S$ un omomorfismo di anelli. Allora esiste un isomorfismo $\Phi_* : R/\ker(\Phi) \longrightarrow \mathrm{im}(\Phi)$*

Dim. Poiché R, S sono gruppi abeliani e Φ è anche un omomorfismo di gruppi abeliani, sappiamo che $\Phi_* : R/\ker(\Phi) \longrightarrow \mathrm{im}(\Phi)$ t.c.

- $\Phi_*(r + \ker(\Phi)) = \Phi(r)$ è un isomorfismo di gruppi abeliani
- $\Phi_*((r + \ker(\Phi))(s + \ker(\Phi))) = \Phi_*(r \cdot s + ker(\Phi)) = \Phi(r \cdot s)$
  $\Phi_*(r + \ker(\Phi)) \cdot \Phi_*(s + \ker(\Phi)) = \Phi(r) \cdot \Phi(s) = \Phi(r \cdot s)$
- $\Phi_*(1 + \ker(\Phi)) = \Phi(1_R) = 1_S$

CVD

Proposizione 4.12. *Sia R un anello, sia $S \subseteq R$ un sottoanello e siano $I, J \lhd R$.*

(a) $I + J = \{i + j \mid i \in I, j \in J\} \lhd R$

(b) $I \cap J \lhd R$

(c) $I \cdot J = \{\sum_{k=1}^{n} i_k \cdot j_k \mid i_k \in I, j_k \in J\} \subseteq I \cap J$ *e* $I \cdot J \lhd R$

(d) $S + I = \{s + i \mid s \in S, i \in I\}$ *è un sottoanello di* R

(e) $S \cap I \lhd S$

(f) Sia $J \leq I$. *Allora* $I/J \lhd R/J$

Dim.

(a) $I + J$ è un sottogruppo abeliano di R.
$r \cdot (i + j) = r \cdot i + r \cdot j \in I + J$ (stessa cosa per $(i + j) \cdot r$)

(b) $I \cap J$ è un sottogruppo abeliano di R.
Sia $i \in I \cap J$, $r \in R$ t.c. $r \cdot i \in I \wedge r \cdot i \in J \Longrightarrow r \cdot i \in I \cap J$ (stessa cosa per $i \cdot r$)

(c) $I \cdot J$ è un sottogruppo abeliano di R.
$I \cdot J \subseteq I$, $I \cdot J \subseteq J \Longrightarrow I \cdot J \subseteq I \cap J$
$r \cdot \sum_{k=1}^{n} i_k \cdot j_k = \sum_{k=1}^{n} (r \cdot i_k) \cdot j_k, (r \cdot i_k \in I)$ (stessa cosa per $(\sum_{k=1}^{n} i_k \cdot j_k) \cdot r$))

(d) Siano $r, s \in S$, $i, j \in I$. Allora
$(r + i) \cdot (s + j) = r \cdot s + i \cdot s + r \cdot j + i \cdot j \in S + I$

(e) Sia $i \in S \cap I$, $s \in S$. Allora
$s \cdot i \in I$, $s \cdot I \in S \Longrightarrow s \cdot i \in I \cap S$ (stessa cosa per $i \cdot s$)

(f) $I/J = \{i + J \mid i \in I\}$
$(r + J) \cdot (s + J) = (r \cdot i + J) \subseteq I/J$ (stessa cosa per $(i + J) \cdot (r + J)$)

CVD

Proposizione 4.13. *Sia R un anello, $S \subseteq R$ un sottoanello, $I \lhd R$. Allora esiste un ismomorfismo di anelli*

$$\Phi_* : S/S \cap I \longrightarrow S + I/I$$

Dim. $\widetilde{\Phi} : S \longrightarrow S + I/I$, $\widetilde{\Phi}(s) = s + I$, ($\widetilde{\Phi} = \Pi|_S$, dove $\Pi : R \longrightarrow R/I$)
$\ker(\widetilde{\Phi}) = S \cap I$. Per la Proposizione 3.9 $\widetilde{\Phi_*} = \Phi$ è un isomorfismo di anelli.

CVD

Proposizione 4.14. *Sia R un anello, $I, J \lhd R$, $J \leq I$. Allora esiste un isomorfismo*

$$\Phi : \frac{R/J}{I/J} \longrightarrow R/I$$

Dim. $\widetilde{\Phi} : R/J \longrightarrow R/I$, $\widetilde{\Phi}(r + J) = r + I$ omomorfismo suriettivo di anelli.
$\ker(\widetilde{(\Phi)}) = I/J$. Per la Proposizione 3.9 $\widetilde{\Phi_*} = \Phi$ è un isomorfismo di anelli.

CVD

Definizione 4.16. Siano $I, J \lhd R$. I si dice *coprimo* a J se $I + J = R$.

Osservazioni. $R = \mathbb{Z}$, $I = n\cdot\mathbb{Z}$, $J = m\cdot\mathbb{Z}$. I e J sono coprimi se e solo se n e m sono coprimi (cioè $\mathrm{MCD}(n, m) = 1$).

Teorema 4.15 (Cinese dei Resti)**.** *Sia R un anello e siano $I_1, \cdots, I_n \lhd R$ due a due coprimi.*
Sia $\Pi_i : R \longrightarrow R/I_i$ la proiezione canonica. Allora

$$\Pi : R \longrightarrow \bigoplus_{i=1}^{n} R/I_i,\ \Pi(r) = (\Pi_1(r), \cdots, \Pi_n(r)),\ r \in R$$

è suriettivo e

$$\ker(\Pi) = \bigcap_{i=1}^{n} I_i$$

Dim. $\ker(\Pi) = \cap I_i$.
Basta dimostrare la suriettività.
Sia

$$J_i = \bigcap_{k=1,\, k\neq i}^{n} I_k$$

Allora $J_i \lhd R$.

- I_k e J_k sono coprimi
  Sappiamo che I_k e I_j sono coprimi se $j \neq k$, cioè $I_k + J_k = R$.
  $\Longrightarrow \exists\, a_j \in I_k,\ b_j \in I_j$ t.c. $1 = a_j + b_j$ (k è fissato)

$$1 = \prod_{j=1,\, j\neq k}^{n} (a_j + b_j) = a + b_1 \cdots b_n$$

$$a \in I_k$$

$$b_1 \cdots b_n \in I_1 \cdots I_{k-1} \cdot I_{k+1} \cdots I_n \leq I_1 \cap \cdots \cap I_{k-1} \cap I_{k+1} \cdots \cap I_n = J_k$$

$$\Longrightarrow a + b_1 \cdots b_n = a + b,\ a \in I_k,\ b \in J_k$$

$$\Longrightarrow 1 \in I_k + J_k \Longrightarrow I_k + J_k = R$$

- Allora esistono elementi $d_k \in I_k$, $e_k \in J_k$ t.c. $1 = e_k + d_k$
- $$\Pi_i(e_k) = \begin{cases} 1_{R/I_k} & \text{per } i = k \\ 0_{R/I_k} & \text{per } i \neq k \end{cases}$$

  $$\Pi_k(1_R) = \Pi_k(e_k) + \Pi_k(d_k) = 1_{R/I_k} \quad (I_k = \ker(\Pi_k))$$

  $$\text{se } i \neq k,\ e_k \in J_k = \bigcap_{j=1,\, j \neq k}^{n} I_j \subseteq I_i = \ker(\Pi_i)$$

- Siano $a_1, \cdots, a_n \in R$

  $$\underline{a} = (a_1 + I_1, \cdots, a_n + I_n) \in \bigoplus_{j=1}^{n} R/I_j$$

  $$\Pi_k(a_k) = \underline{a}_k$$

  Cerchiamo $y \in R$ t.c. $\Pi(y) = a$. Sia

  $$y = \sum_{j=1}^{n} e_j \cdot a_j$$

  $$\Pi_k(y) = \Pi_k\left(\sum_{j=1}^{n} e_j \cdot a_j\right) = \sum_{j=1}^{n} \Pi_k(e_j) \cdot \Pi_k(a_j) = \Pi_k(e_k) \cdot \Pi_k(a_k) = \underline{a}_k$$

  $$\Longrightarrow \Pi(y) = \underline{a}$$

CVD

Corollario 4.16. *Sia $R = \mathbb{Z}$ e siano $n_1, \cdots, n_n \in \mathbb{N}$ due a due coprimi. Siano $a_1, \cdots, a_n \in \mathbb{Z}$.*

(a) $\exists\, m \in \mathbb{Z}$ *t.c.* $m \equiv a_k \bmod n_k \quad (\Longleftrightarrow n_k \,|\, (m - a_k))$

(b) Sia $S \subseteq \mathbb{Z}$, $S = \{t \in \mathbb{Z} \mid t \equiv a_k \bmod n_k,\ k = 1, \cdots, n\}$
Allora $S = m + r \cdot \mathbb{Z}$, $r = \operatorname{mcm}(n_1, \cdots, n_n)$

Dim.

(a) $I_k = R{\cdot}n_k \quad (I_k \text{ e } I_j \text{ sono coprimi se } k \neq j)$

$$\Pi_k : R \longrightarrow R/I_k, \quad \Pi : R \longrightarrow \bigoplus_{k=1}^{n} R/I_k$$

$\underline{a} = (a_1 + I_1, \cdots, a_n + I_n)$
Sia $m \in \mathbb{Z}$, $\Pi(m) = \underline{a}$
$\Longrightarrow m{\cdot}a_k \in I_k = n_k{\cdot}\mathbb{Z} \Longleftrightarrow n_k \,\big|\, (m - a_k)$

(b) $S = \{t \in \mathbb{Z} \mid \Pi(t) = \underline{a}\} = m + \ker(\Pi)$

$$\ker(\Pi) = \bigcap_{k=1}^{n} I_k = \bigcap_{k=1}^{n} \mathbb{Z}{\cdot}n_k = \mathbb{Z}{\cdot}\mathrm{mcm}(n_1, \cdots, n_n)$$

$\mathrm{mcm}(n_1, \cdots, n_n) = n_1 \cdot\cdots\cdot n_n$

4.9 La decomposizione in numeri primi

Proposizione 4.17. *Sia $z \in \mathbb{Z} \setminus \{0\}$.*

- *$\exists\, u_z \in Z^*$ e numeri interi non negativi $\mathcal{E}_p^{(z)} \in \mathbb{N}_0$ t.c.*
  $\forall\, p \in P$ (insieme dei numeri primi) t.c.

$$z = u_z{\cdot}\prod_{p \in P} p^{\mathcal{E}_p}$$

- *Sia $S_z = \{p \in P \mid \mathcal{E}_p(z) > 0\}$. Allora $|S_z| < +\infty$*
- *u_z, $\mathcal{E}_p$, $p \in P$ sono univocamente determinati.*

Dim. Poiché $\mathbb{Z} = \mathbb{N} \overset{\circ}{\cup} -\mathbb{N}$, basta dimostrare la proposizione per $z \in \mathbb{N}$.
Procediamo per induzione.

$$z = 1,\ \mathcal{E}_p(1) = 0 \Longrightarrow 1 = 1{\cdot}\prod p^{\mathcal{E}_p(1)}$$

Siano $\mathcal{E}'_p(1)$, $p \in P$ altri numeri in $\mathbb{N}_0$ t.c.

$$1 = \prod_{p \in P} p^{\mathcal{E}'_p} \quad (S' = \{p \in P \mid \mathcal{E}'_p > 0\} \text{ finito }) \Longrightarrow 1 = \prod_{p \in S'} p^{\mathcal{E}'_p}$$

Basta dimostrare che $S' = \varnothing$.
Supponiamo per assurdo che $S' \neq \varnothing$.

$$\Longrightarrow 1 = \prod_{p \in S'} p^{\mathcal{E}'_p} \Longrightarrow \exists\, q \in S' \text{ t.c. } q \,\Big|\, \prod_{p \in S'} p^{\mathcal{E}'_p} \wedge q \nmid 1, \text{ assurdo}$$

$\Longrightarrow$ affermazione vera per $z = 1$.
Sia l'affermazione vera per tutti $k \in \mathbb{N}$, $k < z$, $z > 1$.

$$\Longrightarrow \exists\, q \in P \text{ t.c. } q \,|\, z \quad (\mathbb{Z}{\cdot}z \leq q{\cdot}\mathbb{Z},\ q \in P)$$

$w = \frac{z}{q} \in \mathbb{N}$ e l'affermazione è vera per w.

$$w = \prod_{p \in P} p^{\mathcal{E}_p(w)},\ S_w = \{p \in P \mid \mathcal{E}_p(w) > 0\} \text{ è finito },\ \mathcal{E}_p(w) \text{ sono univoci}$$

$$z = q^{\mathcal{E}_q(w)+1} \cdot \prod_{p \in P,\, p \neq q} p^{\mathcal{E}_p(w)},\ S_z = \{q\} \cup S_w \text{ è finito}$$

$$\mathcal{E}_p(z) = \mathcal{E}_p(w),\ p \neq q$$

$$\mathcal{E}_q(z) = \mathcal{E}_q(w) + 1$$

Siano $\mathcal{E}'_p \in N_0$ t.c.

$$z = \prod_{p \in P} p^{\mathcal{E}'_p},\ S' = \{p \in P \mid \mathcal{E}'_p > 0\} \text{ è finito}$$

$$z = \prod_{p \in S'} p^{\mathcal{E}'_p},\ q \,\big|\, z \Longrightarrow q \in S'$$

$$\Longrightarrow \frac{z}{q} = q^{\mathcal{E}'_q - 1} \cdot \prod_{p \in S',\, p \neq q} p^{\mathcal{E}'_p} \Longrightarrow w = \frac{z}{q} \Longrightarrow \mathcal{E}'_p = \mathcal{E}_p(w),\ \forall\, p \in P \setminus \{0\}$$

$$\mathcal{E}'_q - 1 = \mathcal{E}_q(w)$$

$$\mathcal{E}'_q = \mathcal{E}_q(w) + 1 = \mathcal{E}_q(z)$$

CVD

Corollario 4.18. *Siano*

$$m = u_m \cdot \prod_{p \in P} p^{\mathcal{E}_p(m)},\ n = u_n \cdot \prod_{p \in P} p^{\mathcal{E}_p(n)} \quad (m,\, n \neq 0)$$

- $$\mathrm{MCD}(m,n) = \prod_{p \in P} p^{\min\{\mathcal{E}_p(m), \mathcal{E}_p(n)\}}$$

  $$\mathrm{mcm}(m,n) = \prod_{p \in P} p^{\max\{\mathcal{E}_p(m), \mathcal{E}_p(n)\}}$$

- $$\mathrm{MCD}(m,n) = 1 \Longleftrightarrow S_m \cap S_n = \varnothing$$

Dim. Ovvio! $(d \,|\, m \Longleftrightarrow \mathcal{E}_p(d) \leq \mathcal{E}_p(m),\ \forall\, p \in P)$

CVD

Definizione 4.17. Sia $\mathbb{K}$ un campo.

- $M(x) = \{f \in \mathbb{K}[x] \mid f \text{ monico}\}$
  Sia
  $$f = \sum_{i=0}^{n} a_i \cdot x^i,\ n = \operatorname{grad}(f)$$
  f si dice *monico* se a_n (direttore) $= 1$
  $\Longrightarrow \forall\, f \in \mathbb{K}[x],\ f \neq 0,\ \exists\, a_f \in \mathbb{K}[x]^* = K^*$ t.c. $f \cdot a_f^{-1} \in M(x)$

- $\operatorname{MIrr}(x) = \{f \in \mathbb{K}[x] \mid f \text{ monico e irriducibile }, f \neq 1\}$
  $f \in \operatorname{MIrr}(x)$ t.c. $f = g \cdot h,\ g, h \in M[x] \Longrightarrow g = 1 \vee h = 1$

Proposizione 4.19. *Sia $f \in \mathbb{K}[x] \setminus \{0\}$. Allora $\exists\, \mathcal{E}_m(f) \in \mathbb{N}_0$, $m \in \operatorname{MIrr}(x)$, $a_f \in \mathbb{K}[x]^* = \mathbb{K}^*$ t.c.*

$$f = a_f \cdot \prod_{m \in \operatorname{MIrr}(x)} m^{\mathcal{E}_m(f)}, \quad S_f = \{m \in \operatorname{MIrr}(x) \mid \mathcal{E}_m(f) > 0\} \text{ è finito}$$

e questa decomposione è unica.

Dim. Come prima.

CVD

Capitolo 5

Moduli

Definizione 5.1. Sia $(R, +, \cdot)$ un anello. Un gruppo abeliano $(M, \oplus)$ dotato di una mappa $\bullet : R \times M \longrightarrow M$ si dice un *R-modulo (di sinistra)* se $\forall\, r, s \in R; \forall\, m, n \in M$

(a) $(r + s) \bullet (m \oplus n) = (r \bullet m) \oplus (s \bullet m) \oplus (r \bullet n) \oplus (s \bullet n)$

(b) $r \bullet (s \bullet m) = (r \cdot s) \bullet m$

(c) $1_R \bullet m = m$

Osservazioni. Le condizioni (b) e (c) fanno di $\bullet$ un'azione di gruppo di R su M

Esempi 5.1.

1. Siano $(S, +, \cdot)$ un anello e R un suo sottoanello; allora S è canonicamente un R-modulo mediante la mappa $\bullet := \cdot$ (esattamente il prodotto dell'anello).

2. Siano $(R, +, \cdot)$ un anello e I un suo ideale; allora I è canonicamente un R-modulo mediante la mappa $\bullet := \cdot$.

3. Siano $(\mathbb{K}, +, \cdot)$ un campo, $R = \mathbb{K}[T]$, M un $\mathbb{K}$-spazio vettoriale e $\alpha \in \mathrm{End}_{\mathbb{K}}(M)$. Allora M è un R-modulo mediante l'azione
$$\text{per } f = \sum_{i=0}^{N} a_i T^i \in R \text{ e } m \in M, \qquad f \bullet m = \Big(\sum_{i=0}^{N} a_i \alpha^i \Big)(m) \tag{5.1}$$
(la composizione di endomorfismi è un endomorfismo). Infatti (a) è chiaramente soddisfatta per le proprietà dei polinomi e perché α è un'applicazione lineare; per (b),
$$(f \cdot g) \bullet m = \Big(\sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j T^{i+j} \Big) \bullet m = \Big(\sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j \alpha^{i+j} \Big)(m) =$$
$$= \sum_{i=0}^{N} \sum_{j=0}^{M} \Big(a_i b_j \alpha^{i+j}(m) \Big) = f \bullet \Big(\sum_{j=0}^{M} b_j \alpha^j(m) \Big) = f \bullet (g \bullet m);$$

(c) è ovvia

4. Viceversa, sia M un $\mathbb{K}[T]$-modulo mediante la mappa $\bullet$. Allora in primo luogo M è canonicamente un $\mathbb{K}$-spazio vettoriale; se è anche $dim_{\mathbb{K}}(M) < \infty$, allora la funzione indotta da $\bullet$

$$\begin{aligned} \alpha : M &\longrightarrow M \\ \alpha(m) &= T \bullet m \end{aligned}$$

appartiene a $\mathrm{End}_{\mathbb{K}}(M)$. Infatti, $\forall\, h,k \in \mathbb{K}, \forall\, m,n \in M$ è

$$\begin{aligned} \alpha(h \bullet m \oplus k \bullet n) &= T \bullet (h \bullet m \oplus k \bullet n) = (T \cdot h) \bullet m \oplus (T \cdot k) \bullet n \\ &= (h \cdot T) \bullet m \oplus (k \cdot T) \bullet n = h \bullet \alpha(m) \oplus k \bullet \alpha(n) \end{aligned}$$

Definizione 5.2. Siano $(R,+,\cdot)$ un anello e $(M,\oplus)$ un R-modulo. $(N,\oplus)$ si dice *R-sottomodulo di M* se

(a) $(M,\oplus) \leq (N,\oplus)$

(b) $\forall\, r \in R, \forall\, n \in N,\ r \bullet n \in N$, proprietà che al solito modo indicheremo con $R \bullet N \subseteq N$

Notazione. Nel seguito, trattando di moduli, riserveremo la scrittura $N \leq M$ per indicare che N è sottomodulo di M, mentre se vogliamo riferirci alle sole strutture di gruppo dei due insiemi, indicheremo esplicitamente $(N,\oplus) \leq (M,\oplus)$ (N è sottogruppo di M).

Inoltre, salvo diversa indicazione, $\bullet$ indicherà sempre la mappa di struttura di modulo, anche quando non esplicitamente dichiarato.

Definizione 5.3. Siano$(R,+,\cdot)$ un anello e $(M,\oplus)$ un R-modulo. M si dice *R-modulo di torsione* se $\forall\, m \in M,\ \exists\, r_m \in R \setminus \{0\}$ t.c. $r_m \bullet m = 0$

Proposizione 5.1. *Siano $(R,+,\cdot)$ un anello e $(M,\oplus)$ un R-modulo. Allora*

(a) $\forall$ famiglia $\{M_i\}_{i=1}^k$ di R-sottomoduli di M, $\sum_{i=1}^k M_i \leq M$

(b) $\forall\, m \in M,\ R \bullet m \leq M$

Dim.

(a) Per induzione su k. Se $k = 2$, $M_1 \oplus M_2 = \{m_1 \oplus m_2 \in M \mid m_1 \in M_1 \wedge m_2 \in M_2\}$. Quindi preso $r \in R, r \bullet (m_1 \oplus m_2) = (r \bullet m_1) \oplus (r \bullet m_2) \in M_1 \oplus M_2$. Il passo induttivo è ovvio: se la tesi è vera per $k = n-1$ e si considera la famiglia $\{M_i\}_{i=1}^n$, basta porre $M_{n-1} \oplus M_n := \widetilde{M}$ per poter applicare l'ipotesi induttiva.

(b) $(R \bullet m, \oplus) \leq (M, \oplus)$ (l'elemento neutro è $0 = 0 \bullet m$, l'opposto di $r \bullet m$ è $(-r) \bullet m$), eredita la commutatività e $\forall\, r \bullet m \in R \bullet m, \forall\, s \in R,\ s \bullet (r \bullet m) = (s \cdot r) \bullet m \in R \bullet m$.

CVD

Definizione 5.4. Siano $(R, +, \cdot)$ un anello e $(M, \oplus)$ un R-modulo. M si dice *finitamente generato* se $\exists\, \{m_i\}_{i=1}^n \in M$ t.c. $M = R \bullet m_1 \oplus \cdots \oplus R \bullet m_n$

Definizione 5.5. Siano $(R, +, \cdot)$ un anello e $(M, \oplus)$ un R-modulo. Si definiscono l'annullatore di $m \in M$ in R come

$$\mathrm{Ann}_{\mathbb{R}}(m) = \{r \in R \mid r \bullet m = 0\}$$

e l'annullatore globale di M come

$$\mathrm{Ann}_{\mathbb{R}}(M) = \{r \in R \mid \forall\, m \in M,\ r \bullet m = 0\}$$

Osservazioni.

1. $\mathrm{Ann}_{\mathbb{R}}(m)$ è un *ideale di sinistra* di R, cioè è un suo sottogruppo abeliano e $R \cdot \mathrm{Ann}_{\mathbb{R}}(m) \subseteq \mathrm{Ann}_{\mathbb{R}}(m)$; perciò, se R è commutativo, $\mathrm{Ann}_{\mathbb{R}}(m) \lhd R$.

2. $\mathrm{Ann}_{\mathbb{R}}(M) = \bigcap_{m \in M} \mathrm{Ann}_{\mathbb{R}}(m)$. Inoltre, che R sia o meno commutativo, $\mathrm{Ann}_{\mathbb{R}}(M) \lhd R$.

Proposizione 5.2. *Siano $(\mathbb{K}, +, \cdot)$ un campo, $R = \mathbb{K}[T]$ e $(M, \oplus)$ un R-modulo finitamente generato. Allora sono equivalenti*

(i) M è un R-modulo di torsione

(ii) $\mathrm{Ann}_{\mathbb{R}}(M) \neq \{0\}$

(iii) $\dim_{\mathbb{K}}(M) < \infty$

Dim. M è finitamente generato, il che significa

$$\Longrightarrow\ \exists\, m_1, \ldots, m_k \text{ t.c. } M = r \bullet m_1 \oplus \cdots \oplus R \bullet m_k;$$

ora, ovviamente è $\mathrm{Ann}_R(M) \subseteq \bigcap_{i=1}^k \mathrm{Ann}_R(m_i)$, ma vale anche l'inclusione

opposta:

$$\text{siano } m = \sum_{i=1}^{k} r_i \bullet m_i, \qquad r \in \bigcap_{i=1}^{k} \mathrm{Ann}_R(m_i)$$

$$\Downarrow$$

$$\begin{aligned} r \bullet m &= \sum_{i=1}^{k} r \bullet (r_i \bullet m_i) \\ &= \sum_{i=1}^{k} (r \cdot r_i) \bullet m_i = \sum_{i=1}^{k} (r_i \cdot r) \bullet m_i \qquad (R \text{ è commutativo}) \\ &= \sum_{i=1}^{k} r_i \bullet (r \bullet m_i) = 0. \end{aligned}$$

Abbiamo cioè ottenuto

$$\mathrm{Ann}_R(M) = \bigcap_{i=1}^{k} \mathrm{Ann}_R(m_i) \tag{5.2}$$

(i)$\Longrightarrow$(ii): Se M è di torsione $\Longrightarrow$ $\forall\, i = 1, \ldots, k$, $\mathrm{Ann}_R(m_i) \neq \{0\}$; sappiamo che R è un dominio principale e che gli annullatori sono suoi ideali, ragion per cui

$$\begin{aligned} &\forall\, i = 1, \ldots, k,\ \exists\, f_i \in R \setminus \{0\} \text{ t.c. } \mathrm{Ann}_R(m_i) = R \cdot f_i \Longrightarrow \\ \Longrightarrow \qquad &\textstyle\bigcap_{i=1}^{k} \mathrm{Ann}_R(m_i) = \bigcap_{i=1}^{k} R \cdot f_i = R \cdot \mathrm{mcm}(f_i) \neq \{0\} \end{aligned} \qquad \square$$

(ii)$\Longrightarrow$(iii): Per (ii) $\exists\, f \in R \setminus \{0\}$ t.c. $\mathrm{Ann}_R(M) = R \cdot f$; inoltre, sfruttando la (5.2), possiamo trovare, come abbiamo fatto sopra, certi polinomi

$$\{f_i\}_{i=1}^{k} \subseteq R \setminus \{0\} \text{ t.c. } \mathrm{Ann}_R(m_i) = R \cdot f_i$$

(nessun $\mathrm{Ann}_R(m_i)$ può essere vuoto). Consideriamo ora la famiglia di mappe $\{\varphi_i\}_{i=1}^{k}$ definite da

$$\begin{aligned} \varphi_i : R &\longrightarrow R \bullet m_i \\ \varphi_i(r) &= r \bullet m_i \end{aligned}$$

si verifica immediatamente che esse sono $\mathbb{K}$-lineari e suriettive e che $\ker(\varphi_i) = \mathrm{Ann}_R(m_i)$, da cui

$$\begin{aligned} \dim_{\mathbb{K}}(R \bullet m_i) &= \dim_{\mathbb{K}}(R/\ker(\varphi_i)) = \\ \dim_{\mathbb{K}}(R/\mathrm{Ann}_R(m_i)) &= \dim_{\mathbb{K}}(R/R \cdot f_i) = \\ \mathrm{grad}(f_i) &\leq \mathrm{grad}(f). \end{aligned}$$

(f dev'essere esattamente il $\mathrm{mcm}(f_i)$). Ma allora

$$\dim_{\mathbb{K}}(M) \leq \sum_{i=1}^{k} \dim_{\mathbb{K}}(R \bullet m_i) \leq k \,\mathrm{grad}(f) < \infty \quad \square$$

(iii)$\Longrightarrow$(i): Sia $m \in M$ qualunque; la mappa

$$\begin{aligned} \varphi_m : R &\longrightarrow M \\ \varphi_m(r) &= r \bullet m \end{aligned}$$

è $\mathbb{K}$-lineare, da cui segue che

$$\mathrm{im}(\varphi_m) = R/\ker(\varphi_m) \qquad \text{(come spazi vettoriali)}$$

$$\text{ma } \ker(\varphi_m) = \mathrm{Ann}_R(m) \implies \mathrm{Ann}_R(m) \neq \{0\}$$

perché $\dim_{\mathbb{K}}(R) = \infty$, mentre l'immagine è un sottospazio vettoriale di uno spazio finito-dimensionale. □

CVD

Definizione 5.6. Siano $(R, +, \cdot)$ un anello, $(M, \oplus)$ e $(N, \otimes)$ due R-moduli mediante $\bullet$ e $\diamond$ rispettivamente. Un omomorfismo di gruppi $\varphi : M \longrightarrow N$ si dice *omomorfismo di R-moduli* se $\forall\, r \in R, \forall\, m \in M,\ \varphi(r \bullet m) = r \diamond \varphi(m)$.

Un omomorfismo di R-moduli biunivoco si dice *isomorfismo* di R-moduli.

Proposizione 5.3. *Siano $(R, +, \cdot)$ un anello e $(M, \oplus)$, $(N, \otimes)$ due R-moduli mediante le mappe $\bullet$ e $\diamond$ rispettivamente. Allora*

(a) Se $P \leq M$, $\implies$ M/P è un R-modulo (quoziente canonico) dove si ponga $r \bullet (m + P) := r \bullet m + P$ (si userà per semplicita lo stesso simbolo per le due mappe di R-modulo su M e su M/P).

(b) La proiezione canonica $\pi : M \longrightarrow M/P$ è omomorfismo di R-moduli.

(c) Se $\varphi : M \longrightarrow N$ è un omomorfismo di R-moduli, $\implies$ $\mathrm{im}(\varphi)$ e $\ker(\varphi)$ sono R-moduli e $\exists\, \varphi_* : M/\ker(\varphi) \longrightarrow \mathrm{im}(\varphi)$ isomorfismo di R-moduli.

(d) Se $P, Q \leq M \implies P \oplus Q \leq M$ e $(P \oplus Q)/Q \simeq P/(P \cap Q)$.

(e) Se $P, Q \leq M \wedge P \subseteq Q \implies (M/P)/(Q/P) \simeq M/Q$.

Dim.

(a) Ovvia.

(b) Anche.

(c) Dati $m \in \ker(\varphi), r \in R$ qualunque,

$$\varphi(r \bullet m) = r \diamond \varphi(m) = 0 \implies r \bullet m \in \ker(\varphi).$$

Siano $n \in \mathrm{im}(\varphi), r \in R$ qualunque:

$$\exists\, m \in M \text{ t.c. } \varphi(m) = n \implies r \diamond n = r \diamond \varphi(m) = \varphi(r \bullet m) \in \mathrm{im}(\varphi).$$

Il resto segue dalle proprietà dei gruppi abeliani *(analogo del primo teorema dell'omomorfismo)*.

(d) $P \oplus Q$ e $P \cap Q$ sono gruppi abeliani; siano allora $p \in P, q \in Q, r \in R$ qualsiasi:

$$r \bullet (p \oplus q) = (r \bullet p) \oplus (r \bullet q) \in P \oplus Q;$$

per $m \in P \cap Q, r \in R$ qualsiasi,

$$r \bullet m \in P \ \wedge \ r \bullet m \in Q \implies r \bullet m \in P \cap Q;$$

così $P \oplus Q$ e $P \cap Q$ sono R-sottomoduli. Ma allora per (b) la proiezione canonica $\pi_Q : M \longrightarrow M/Q$ è omomorfismo di R-moduli e il resto segue da (c) e dalle proprietà dei gruppi abeliani *(analogo del secondo teorema dell'omomorfismo).*

(e) $Q/P = \mathrm{im}(\pi_P|_Q)$ (proiezione canonica su P ristretta a Q), quindi è un R-modulo. La mappa

$$\begin{array}{rcl} \tau : M/P & \longrightarrow & M/Q \\ \tau(m) \oplus P & = & m \oplus Q \end{array}$$

è omomorfismo di R-moduli: infatti, $\forall\, r \in R, \forall\, m \in M$,

$$\tau(r \bullet (m \oplus P)) = \tau\Big((r \bullet m) \oplus P\Big) = (r \bullet m) \oplus Q = r \bullet \tau(m \oplus P);$$

la tesi segue da (c) e dalle proprietà dei gruppi abeliani *(analogo del terzo teorema dell'omomorfismo).*

CVD

5.1 Sottomoduli invarianti

Sappiamo dal Teorema cinese dei resti (4.15) che se $(R, +, \cdot)$ è un anello, $I_1, \ldots, I_n \lhd R$ sono 2 a 2 coprimi e le mappe $\pi_k : R \longrightarrow R/I_k$ per $k = 1, \ldots, n$ sono le proiezioni al quoziente (che sono omomorfismi di anelli), si trovano elementi

$$e_1, \ldots, e_n \in R \text{ t.c. } \pi_k(e_j) = \delta_{kj} + I_k.$$

Siano

$$\begin{array}{ll} \pi : R \longrightarrow \displaystyle\sum_{k=1}^{n} (R/I_k) & \text{la proiezione canonica } \pi(r) = \Big(\pi_1(r), \ldots, \pi_n(r)\Big) \\ I = \displaystyle\bigcap_{k=1}^{n} I_k = \ker(\pi) & \\ \overline{R} = R/I & \\ \overline{e_k} = e_k + I & \text{per } k = 1, \ldots, n \end{array}$$

allora valgono le relazioni

$$\overline{e_i}\cdot\overline{e_j} = \delta_{ij}\cdot\overline{e_j} \tag{5.3}$$

$$\sum_{k=1}^{n} \overline{e}_k = 1_{\overline{R}} \tag{5.4}$$

infatti, nella notazione del Teorema cinese dei resti,

$$e_i \in J_i \lhd R \ \wedge\ e_j \in J_j \lhd R \implies$$
$$\implies e_i\cdot e_j \in J_i \cap J_j = \bigcap_{k=1}^{n} I_k = \ker(\pi);$$

$$\pi_k\Big((\sum_{i=1}^{n} e_i) - 1\Big) = \Big(\sum_{i=1}^{n} \pi_k(e_i)\Big) - \pi_k(1)$$
$$= \pi_k(e_k) - \pi_k(1) = \pi_k(e_k - 1) = \pi_k(-d_k) = 0 \implies$$
$$\implies \Big((\sum_{i=1}^{n} e_i) - 1\Big) \in \bigcap_{k=1}^{n} \ker(\pi_k) = \bigcap_{k=1}^{n} I_k = \ker(\pi)$$

Ciò ci consente di dimostrare facilmente la

Proposizione 5.4. *Siano $(R,+,\cdot)$ un anello commutativo, $(M,\oplus)$ un R-modulo e $\{I_k\}_{k=1}^{n}$ una famiglia di ideali 2 a 2 coprimi di R tale che*

$$I \coloneqq \bigcap_{k=1}^{n} I_k \subseteq \mathrm{Ann}_R(M).$$

Allora, detto $\overline{R} \coloneqq R/I$, M è canonicamente un $\overline{R}$-modulo, dove

$$(r+I)\bullet m = r\bullet m$$

(al solito indichiamo la mappa di modulo rispetto a un quoziente canonico con lo stesso simbolo usato per quella rispetto all'anello d'origine); inoltre, nella notazione sopraindicata, gli $M_k \coloneqq \overline{e_k}\bullet M$ con $k = 1,\dots,n$ sono $\overline{R}$-sottomoduli di M in somma diretta, generano M e sono invarianti rispetto all'azione del proprio $\overline{e_k}$.

Dim. $\bullet$ è ben definita rispetto al passaggio al quoziente:

$$\forall\, r \in R, \forall\, m \in M, \forall\, i \in I \subseteq \mathrm{Ann}_R(M),$$
$$(r+i)\bullet m = r\bullet m \oplus i\bullet m = r\bullet m \oplus 0_M = r\bullet m;$$

Verifichiamo le 3 proprietà della def. 5.1 per elementi generici di R e M:

$$\text{(a):}\quad \Big((r+I)+(s+I)\Big)\bullet(m\oplus n) = \Big((r+s)+I\Big)\bullet(m\oplus n)$$
$$= \quad (r+s)\bullet(m\oplus n) = r\bullet m \oplus s\bullet m \oplus r\bullet n \oplus s\bullet n$$
$$= \quad (r+I)\bullet m \oplus (s+I)\bullet m \oplus (r+I)\bullet n \oplus (s+I)\bullet n$$

$$\text{(b):}\quad (r+I)\bullet\Big((s+I)\bullet m\Big) = (r+I)\bullet(s\bullet m)$$
$$= \quad r\bullet(s\bullet m) = (r\cdot s)\bullet m = \Big((r+I)\cdot(s+I)\Big)\bullet m$$

$$\text{(c):}\quad (1+I)\bullet m = 1\bullet m = m$$

Passiamo agli M_k, cercando in primo luogo di caratterizzarli: sia $n = \overline{e_k}\bullet m \in M_k \implies$

$$\overline{e_k}\bullet n = \overline{e_k}\bullet(\overline{e_k}\bullet m) = \overline{e_k}\bullet m = n \quad \text{in virtù della (5.3);}$$

viceversa, è banale che se $\overline{e_k}\bullet m = m \implies m \in M_k$; abbiamo perciò verificato che

$$\forall\, k = 1,\dots,n,\ M_k = \{m\in M \mid \overline{e_k}\bullet m = m\} \tag{5.5}$$

e questo già conferma che $\forall\, k = 1,\dots,n,\ M_k$ è invariante rispetto a $\overline{e_k}$. Siano ora $m,n \in M_k$ qualsiasi:

$$\overline{e_k}\bullet\Big(m\oplus(-n)\Big) = e_k\bullet\Big(m\oplus(-n)\Big)$$
$$= (e_k\bullet m)\oplus\Big(e_k\bullet(-n)\Big) = m\oplus(-n) \implies$$
$$\implies \quad m\oplus(-n)\in M_k \implies (M_k,\oplus)\le(M,\oplus)$$

(senza richiedere la commutatività di R arriviamo fin qui); infine,

$$\forall\, r\in R, \forall\, m\in M_k,\ \overline{e_k}\bullet(r\bullet m) = e_k\bullet(r\bullet m)$$
$$= (e_k\cdot r)\bullet m = (r\cdot e_k)\bullet m = r\bullet(\overline{e_k}\bullet m) = r\bullet m;$$

ma allora gli M_k sono $\overline{R}$-sottomoduli di M, come voluto.

Manca da dimostrare che sono in somma diretta e generano tutto M. se per certi indici $i\neq j, \exists\, m\in M_i\cap M_j \implies$

$$m = \overline{e_i}\bullet m \wedge m = \overline{e_j}\bullet m = \overline{e_j}\bullet(\overline{e_i}\bullet m) = (\overline{e_j}\cdot\overline{e_i})\bullet m = 0_R\bullet m = 0_M$$

grazie ancora alla (5.3), o, in altre parole,

$$\forall\, i\neq j,\ i,j\in\{1,2,\dots,n\},\ M_i\cap M_j = \{0_M\}.$$

Per la (5.4), qualunque sia $m\in M$, si può scrivere

$$m = 1_R\bullet m = (\sum_{k=1}^{n}\overline{e_k})\bullet m = \sum_{k=1}^{n}(\overline{e_k}\bullet m)\in\sum_{k=1}^{n}M_k$$

che conduce direttamente a

$$M = \sum_{k=1}^{n}M_k$$

CVD

La proposizione appena dimostrata indica una via per studiare i sottospazi vettoriali invarianti rispetto ad applicazioni lineari (autospazi) sfruttando l'equivalenza fra $\mathbb{K}$-spazi vettoriali e $\mathbb{K}[T]$-moduli mostrata negli esempi 5.1. Vediamo come.

Definizione 5.7. Siano $(\mathbb{K}, +, \cdot)$ un campo, $(V, \oplus)$ un $\mathbb{K}$-spazio vettoriale di dimensione finita e $\alpha \in \mathrm{End}(V)$. Per $g \in \mathbb{K}[T] \setminus \{0\}$ chiameremo *autospazio generalizzato relativo a* g il sottospazio vettoriale

$$V_g = \{v \in V \mid g(\alpha)(v) = 0\};$$

per $m \in MIrr_{\mathbb{K}}[T]$ si definisce *m-componente di Fitting di* (V, α) il sottospazio vettoriale

$$Fit_m(V) = \{v \in V \mid \exists\, k \in \mathbb{N} \text{ t.c. } m^k(\alpha)(v) = 0$$

Notazione. Se $g = \sum_{i=0}^{n} a_i T^i$, come sopra $g(\alpha) := \sum_{i=0}^{n} a_i \alpha^i$ con $\alpha^0 = id_V$.

Esempi 5.2.

1. Nelle ipotesi della definizione precedente, per $g \in \mathbb{K}[T]^*$, vale

   $$g(\alpha)(v) = 0 \iff v = 0 \text{ quindi } V_g = \{0\} \quad (g(\alpha) = a_0 \cdot id_V);$$

   per $g = T - \lambda$ con $\lambda \in \mathbb{K}$,

   $$V_g = \{v \in V \mid \big(\alpha - \lambda \cdot id_V\big)(v) = 0\},$$

   ovvero l'autospazio in senso stretto (se non contiene il solo 0) relativo all' autovalore λ, noto dal corso di Algebra Lineare.

2. Si vede subito che $V_g = \ker\big(g(\alpha)\big)$.

3. $Fit_m(V) = \bigcup_{k \in \mathbb{N}} V_{m^k}$. Sia $d = \dim_{\mathbb{K}}(V)$; allora $Fit_m(V) = V_{m^d}$. Infatti, chiaramente valgono le inclusioni

   $$\forall\, k \in \mathbb{N},\ V_{m^k} \subseteq V_{m^{k+1}};$$

   inoltre, se per un certo $n \in \mathbb{N}$, $V_{m^n} = V_{m^{n+1}}$, vale

   $$\forall\, k \in \mathbb{N},\ V_{m^{n+k}} = V_{m^{n+k+1}},$$

come si ricava facilmente dal Teorema del rango:

$$
\begin{aligned}
& V_{m^n} = V_{m^{n+1}} \implies \ker\big(m^n(\alpha)\big) = \ker\big(m^{n+1}(\alpha)\big) \implies \\
\implies \quad & \operatorname{im}\big(m^{n+1}(\alpha)\big) = m(\alpha)\Big(\operatorname{im}\big(m^n(\alpha)\big)\Big) = \operatorname{im}\big(m^n(\alpha)\big) \implies \\
\implies \quad & m(\alpha)|_{\operatorname{im}\left(m^n(\alpha)\right)} \text{ è isomorfismo di spazi vettoriali} \implies \\
\implies \quad & \operatorname{im}\big(m^{n+2}(\alpha)\big) = m(\alpha)\Big(\operatorname{im}\big(m^{n+1}(\alpha)\big)\Big) = \\
& = m(\alpha)\Big(\operatorname{im}\big(m^n(\alpha)\big)\Big) = \operatorname{im}\big(m^n(\alpha)\big) \implies \\
\implies \quad & V_{m^{n+2}} = \ker\big(m^{n+2}(\alpha)\big) = \ker\big(m^n(\alpha)\big) = V_{m^n}
\end{aligned}
$$

e così via per induzione. La catena ascendente di sottospazi vettoriali $\{V_{m^k}\}_{k\in\mathbb{N}}$ ha cioè un elemento massimale rispetto all'inclusione, ed esso può essere al più V_{m^d} in quanto il rango delle applicazioni lineari $\{m^k(\alpha)\}_{k\in\mathbb{N}}$ varia in maniera monotona strettamente decrescente fra d e 0 (non necessariamente raggiungendo gli estremi) finché non si stabilizza divenendo costante.

Osservazioni. La mappa

$$
\begin{aligned}
\varphi : \mathbb{K}[T] &\longrightarrow \operatorname{End}_{\mathbb{K}}(V) \\
\varphi(g) &= g(\alpha)
\end{aligned}
\tag{5.6}
$$

con $\alpha \in \operatorname{End}_{\mathbb{K}}(V)$ fissato è un omomorfismo di anelli. Sappiamo che $\dim_{\mathbb{K}}(\mathbb{K}[T]) = \infty$, $\dim_{\mathbb{K}}(\operatorname{End}(V)) = \dim_{\mathbb{K}}(V)^2 < \infty$, quindi

$$
\begin{aligned}
& \ker(\varphi) \lhd \mathbb{K}[T] \ \wedge\ \ker(\varphi) \neq \{0\} \implies \\
\implies \quad & \exists\, f \in Mon[T] \text{ t.c. } \ker(\varphi) = \mathbb{K}[T]\cdot f
\end{aligned}
$$

(f è univocamente determinato)

Definizione 5.8. In queste ipotesi, f si dice il *polinomio minimo* di α e si indica con $min_{\alpha,V}$, o più semplicemente min_α.

Proposizione 5.5. *Siano* $(\mathbb{K}, +, \cdot)$ *un campo,* $(V, \oplus)$ *un* $\mathbb{K}$*-spazio vettoriale di dimensione finita,* $\alpha \in \operatorname{End}(V)$*,* $f = min_\alpha = m_1^{\varepsilon_1}\cdot\ldots\cdot m_n^{\varepsilon_n}$ *con gli* $m_i \in MIrr[T]$*. Allora*

$$
\begin{aligned}
& V = \sum_{i=1}^{n} Fit_{m_i}(V), \text{ la somma è diretta e} \\
& \forall\, i = 1, \ldots, n,\ \alpha\Big(Fit_{m_i}(V)\Big) \subseteq Fit_{m_i}(V)
\end{aligned}
$$

Dim. Sia φ l'omomorfismo di anelli definito nella precedente osservazione; V è un $\mathbb{K}[T]$-modulo mediante $g \bullet v = \varphi(g)(v)$.
Poiché $\ker(\varphi) = \mathbb{K}[T]\cdot f$, posto

$$R := \mathbb{K}[T]/(\mathbb{K}[T]\cdot f),$$

per la proposizione 5.4 V è canonicamente un R-modulo mediante

$$\Big(g + (\mathbb{K}[T]\cdot f)\Big) \bullet v = g \bullet v.$$

Siano

$$I_j := \mathbb{K}[T]\cdot m_j^{\varepsilon_j} \text{ per } j = 1, \dots, n \implies$$

$\implies$ gli I_j sono 2 a 2 coprimi perché per loro definizione

$$m_i \neq m_k \implies I_i + I_k = \mathbb{K}[T]\cdot \mathrm{MCD}(m_i^{\varepsilon_i}\,;\, m_k^{\varepsilon_k}) = \mathbb{K}[T]\cdot 1 = \mathbb{K}[T];$$

ancora per definizione,

$$\mathrm{mcm}(m_1^{\varepsilon_1}\,;\dots;\, m_n^{\varepsilon_n}) = f \implies \bigcap_{j=1}^{n} I_j = \mathbb{K}[T]\cdot f.$$

Siamo esattamente nella situazione espressa all'inizio della sezione: usando la medesima notazione troviamo la famiglia $\{V_j\}_n^{j=1}$ t.c.

$$V = \sum_{j=1}^{n} V_j, \text{ la somma è diretta e}$$
$$\forall\, i = 1, \dots, n,\ \alpha(V_j) \subseteq V_j;$$

l'idea è quindi di mostrare che

$$\forall\, j = 1, \dots, n,\ V_j = Fit_{m_j}(V). \tag{5.7}$$

Sia $v \in V_j$, cioè $e_j \bullet v = v \implies$

$$m_j^{\varepsilon_j}(\alpha)(v) = m_j^{\varepsilon_j} \bullet v = m_j^{\varepsilon_j} \bullet (e_j \bullet v) = (m_j^{\varepsilon_j}\cdot e_j) \bullet v = 0,$$

dove l'ultima uguaglianza sussiste perché per costruzione

$$e_j \in \bigcap_{k=1,\, k\neq j}^{n} I_k \ \wedge\ m_j^{\varepsilon_j} \in I_j \implies e_j\cdot m_j^{\varepsilon_j} \in \mathbb{K}[T]\cdot f;$$

con ciò abbiamo ottenuto che

$$\forall\, j = 1, \dots, n,\ V_j \subseteq Fit_{m_j}(V)$$

Viceversa, sia $w \in Fit_{m_j}(V)$: poiché i V_k generano tutto V, si può scrivere

$$w = w_0 + w_1 \text{ con } w_0 \in V_j,\ w_1 \in \sum_{k=1,\, k\neq j}^{n} V_k.$$

Per assurdo sia $w_1 \neq 0$.

$$w_1 = w - w_0 \in Fit_{m_j}(V) \qquad (V_j \subseteq Fit_{m_j}(V)) \qquad \Longrightarrow$$
$$\Longrightarrow \quad \exists\, N_j \in \mathbb{N} \text{ t.c. } m_j^{N_j} \bullet w_1 = 0 \implies m_j^{N_j} \in \mathrm{Ann}_{\mathbb{K}[T]}(w_1);$$

d'altra parte, è anche, per definizione di w_1,

$$\mathrm{mcm}(m_k^{\varepsilon_k} \mid k \neq j) := d \in \mathrm{Ann}_{\mathbb{K}[T]}(w_1),$$

ragion per cui necessariamente

$$\mathrm{MCD}(d;\, m_j^{N_j}) = 1 \in \mathrm{Ann}_{\mathbb{K}[T]}(w_1)$$

cioè $1 \bullet w_1 = 0 \implies w_1 = 0$ e abbiamo la contraddizione.
Dunque $w_1 = 0$, che significa

$$\forall\, j = 1, \ldots, n,\ V_j \supseteq Fit_{m_j}(V)$$

e la (5.7) è dimostrata.

CVD

Abbiamo raggiunto il nostro scopo: è effettivamente possibile scomporre uno spazio vettoriale in una somma diretta di sottospazi invarianti rispetto a un qualunque endomorfismo prefissato.

Il legame riscontrato fra polinomi ed applicazioni lineari suggerisce di riflettere sulla fattorizzazione di particolari polinomi per ricavare un metodo pratico di scomposizione degli spazi vettoriali: si approderà alla fine a una particolare rappresentazione matriciale degli endomorfismi, nota come *forma canonica di Jordan*.

5.2 Forma canonica di Jordan (cenni)

Parti della materia trattata in questa sezione esulano dagli scopi del presente corso di Algebra, sebbene siano ad essi connesse; pertanto, saranno trattate in maniera non approfondita e di alcuni enunciati in esse contenuti saranno omesse le dimostrazioni. In ogni caso, la bibliografia fornisce le indicazioni per eventuali approfondimenti (si veda in particolare [1], [5]).

Premettiamo velocemente alcuni concetti relativi alla fattorizzazione dei polinomi.

5.2.1 Campi algebricamente chiusi

Definizione 5.9. Un campo $(\mathbb{K}, +, \cdot)$ si dice *algebricamente chiuso* se

$$\forall\, f \in \mathbb{K}[T] \text{ t.c. } \mathrm{grad}(f) \geq 1,\ \exists\, \lambda \in \mathbb{K} \text{ t.c. } f(\lambda) = 0$$

(cioè f ha una radice in $\mathbb{K}$).

Esempi 5.3.

1. $\mathbb{R}$ non è algebricamente chiuso perché $f = T^2 + 1$ ha grado 2 ma non ha radici in $\mathbb{R}$; Lo stesso polinomio ammette in $\mathbb{C}$ le due radici $\pm i$.

Ecco due notevoli proprietà le cui dimostrazioni saranno omesse necessitando di strumenti sviluppati nei successivi corsi di Algebra:

Teorema 5.6 (**fondamentale dell'algebra – Gauss**)**.** $\mathbb{C}$ *con le usuali operazioni è algebricamente chiuso.*

Teorema 5.7. *Ogni campo è sottocampo di un campo algebricamente chiuso.*

Una caratterizzazione di somma utilità per i campi algebricamente chiusi è quella espressa dalla

Proposizione 5.8. *Un campo* $(\mathbb{K}, +, \cdot)$ *è algebricamente chiuso se e solo se* $\forall\, f \in \mathbb{K}[T] \setminus \{0\}$*, si decompone in fattori di grado* 1*, più precisamente*

$$\exists\, a_f \in \mathbb{K}^*;\ \lambda_1, \dots, \lambda_n \in \mathbb{K};\ m_1, \dots, m_n \in \mathbb{N} \setminus \{0\}\ \textit{t.c.}\ f = a_f \cdot \prod_{i=1}^{n} (T - \lambda_i)^{m_i}$$

Dim. L'implicazione '$\Longleftarrow$' è palese.

Mostriamo che vale anche '$\Longrightarrow$' per induzione su $k = \operatorname{grad}(f)$. Se $k = 1$ non c'è alcunché da dimostrare; sia ora la tesi valida per ogni $\widetilde{f} \in \mathbb{K}[T]$ tale che $\operatorname{grad}(\widetilde{f}) < k$ con $k > 1$: per definizione di campo algebricamente chiuso,

$$\exists\, \lambda \in \mathbb{K} \text{ t.c. } f(\lambda) = \Longrightarrow\ (T - \lambda) | f$$

(considerato l'omomorfismo di anelli

$$\begin{array}{rcl} \varphi_\lambda : \mathbb{K}[T] & \longrightarrow & \mathbb{K} \\ \varphi_\lambda(g) & = & g(\lambda), \end{array}$$

si ha $\ker(\varphi_\lambda) = \mathbb{K}[T] \cdot (T - \lambda)$) perciò

$$\exists\, f' \in \mathbb{K}[T] \text{ t.c. } f = (T - \lambda) \cdot f'$$

con $\operatorname{grad}(f') = \operatorname{grad}(f) - 1$, ma allora a f' si può applicare l'ipotesi di induzione in modo che

$$f' = a \cdot \prod_{i=1}^{k-1} (T - \lambda_i)^{m_i} \text{ per certi } a \in \mathbb{K}^*;\ \lambda_i \in \mathbb{K};\ m_i \in \mathbb{N} \setminus \{0\}\ \Longrightarrow$$

$$\Longrightarrow\ f = a \cdot \prod_{i=1}^{k-1} (T - \lambda_i)^{m_i} \cdot (T - \lambda)$$

e il passo induttivo è completo.

CVD

Osservazioni. $(\mathbb{K}, +, \cdot)$ campo algebricamente chiuso $\implies$ $MIrr[T] = \{(T-\lambda) \mid \lambda \in \mathbb{K}\}$.

5.2.2 Scomposizione del polinomio minimo

Vediamo come la discussione precedente possa applicarsi al polinomio minimo associato a un endomorfismo.

Siano $(\mathbb{K}, +, \cdot)$ un campo algebricamente chiuso, $(V, \oplus)$ un $|K$-spazio vettoriale di dimensione finita e $\alpha \in \mathrm{End}(V)$ fissata, con polinomio minimo f; sappiamo che possiamo scomporre

$$f = (T-\lambda_1)^{\varepsilon_1} \cdot \ldots \cdot (T-\lambda_n)^{\varepsilon_n}$$

con i λ_i a 2 a 2 distinti. Ricordiamo allora la proposizione 5.5:

$$Fit_{(T-\lambda_i)}(V) = \ker\left((\alpha - \lambda_i \cdot id_V)^{\varepsilon_i}\right)$$

e, avendo ricavato, secondo la ormai abituale notazione, gli

$$\overline{e_i} = e_i + I_i \text{ con } I_i = \mathbb{K}[T] \cdot (T-\lambda_i)^{\varepsilon_i},$$

risulta

$$Fit_{(T-\lambda_i)}(V) = M_i \text{ e } \forall\, m \in M_i,\ (T-\lambda_i)^{\varepsilon_i} \bullet m = (T-\lambda_i)^{\varepsilon_i} \bullet (e_i \bullet m) = 0,$$

dunque $\forall\, i = 1, \ldots, n,\ I_i \leq \mathrm{Ann}^{\mathbb{K}[T]}(M_i)$.

Proposizione 5.9. *Siano $(\mathbb{K}; +, \cdot)$ un campo algebricamente chiuso, $(V, \oplus)$ un $\mathbb{K}$-spazio vettoriale di dimensione finita e $\alpha \in \mathrm{End}(V)$.*
α è diagonalizzabile se e solo se $min_\alpha = \prod_{i=1}^{n}(T-\lambda_i)$ con i λ_i a 2 a 2 distinti (cioè, nelle ipotesi all'inizio della presente sottosezione, se e solo se $\varepsilon_1 = \cdots = \varepsilon_n = 1$).

Dim. Per '$\Longrightarrow$': siano $\lambda_1, \ldots, \lambda_k$ gli autovalori di α e

$$V_{\lambda_1} := V_{(T-\lambda_1)}, \ldots, V_{\lambda_k} := V_{(T-\lambda_k)}$$

gli autospazi corrispondenti; allora $f := \prod_{i=1}^{k}(T-\lambda_i)$ si annulla su α (v. formula (5.6)), perciò deve essere $min_\alpha | f$, dove f si decompone in fattori di primo grado tutti distinti; questo implica che $min_\alpha = f$, che ha la forma cercata.

Passiamo a '$\Longleftarrow$': se nell'espressione di min_α $\varepsilon_1 = \cdots = \varepsilon_n = 1$, segue che

$$\forall\, i = 1, \ldots, n,\ Fit_{(T-\lambda_i)}(V) = \ker(\alpha - \lambda_i \cdot id_V) = V_{\lambda_i}$$

e per la proposizione 5.5 posiamo concludere che V possiede una base di autovettori per α.

Sfortunatamente non tutti gli endomorfismi sono diagonalizzabili; l'ideale sarebbe trovare una generalizzazione del concetto di diagonalizzabilità valida in condizioni più generali e che mantenga caratteristiche di semplicità nella rappresentazione matriciale. Il problema si riduce a trovare una base opportuna (dipendente da α) per $\mathrm{End}(V)$.

A questo scopo, osserviamo innanzi tutto che, per ogni autovalore λ, con molteplicità algebrica ε, detti

$$\begin{aligned} V_n &:= \ker\left((\alpha - id_V \cdot \lambda)^n\right) \\ V_{k,n} &:= (\alpha - id_V \cdot \lambda)^{n-k}(V_n) \end{aligned}$$

vale la catena di inclusioni:

$$\begin{array}{ccccccccccc} V_1 & \geq & V_{1,2} & \geq \cdots \geq & V_{1,n} & \geq \cdots \geq & V_{1,\varepsilon-1} & \geq & V_{1,\varepsilon} \\ \wedge\,| & & \wedge\,| & \ldots & \wedge\,| & \ldots & \wedge\,| & & \\ V_2 & \geq & V_{2,3} & \geq \cdots \geq & V_{2,n} & \geq \cdots \geq & V_{2,\varepsilon} & & \\ \wedge\,| & & \wedge\,| & & & & & & \\ \vdots & & \vdots & & & & & & \\ \wedge\,| & & \wedge\,| & & & & & & \\ V_{\varepsilon-1} & \geq & V_{\varepsilon-1,\varepsilon} & & & & & & \\ \wedge\,| & & & & & & & & \\ V_\varepsilon & & & & & & & & \end{array}$$

Supponiamo poi che esista una catena di vettori $\mathcal{B} = \{v_1, \ldots, v_l\} \subseteq V$ linearmente indipendenti tali che

$$\begin{aligned} \alpha(v_1) &= \lambda \cdot v_1 \\ \alpha(v_i) &= \lambda \cdot v_i + v_{i-1} \qquad \text{per } i = 2, \ldots, l; \end{aligned}$$

in tal caso la matrice quadrata che rappresenta la restrizione di α allo $\mathrm{span}\{v_1, \ldots, v_l\}$ rispetto alla base $\mathcal{B}$ è nella forma

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

Definizione 5.10. Una matrice in questa forma si chiama *blocco di Jordan* di ordine l relativo all'autovalore λ, una catena di vettori della forma suddetta è una *catena di Jordan* e una base di V interamente costituita da catene di Jordan 2 a 2 disgiunte (ovviamente, in generale riferite a tutti i vari autovalori dell'endomorfismo) si dice *base di Jordan* per α.

Esempi 5.4.

1. Se β è un endomorfismo diagonalizzabile di V, ogni base di autovettori per β è una base di Jordan costituita da catene di lunghezza 1.

2. Sia $V = \mathbb{R}^3$ con base canonica $\mathcal{C}$ e sia $\alpha \in \mathrm{End}(V)$ tale che

$$M_{\mathcal{C}}^{\mathcal{C}}(\alpha) = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

   I primi 2 vettori $e_1, e_2 \in \mathcal{C}$ costituiscono una catena di Jordan di lunghezza 2, mentre il terzo è una catena di lunghezza 1 a sé stante; si calcola agilmente che

$$\begin{array}{rclcrcl} V_1 & = & \mathrm{span}\{e_1,\, e_3\} & & V_{1,\,2} & = & \mathrm{span}\{e_1\} \\ V_2 & = & \mathrm{span}\{e_1,\, e_2,\, e_3\} & & & & \end{array}$$

3. Sia $V = \mathbb{R}^3$ con base canonica $\mathcal{C}$ e sia $\beta \in \mathrm{End}(V)$ tale che

$$M_{\mathcal{C}}^{\mathcal{C}}(\beta) = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$

   In questo caso la base è costituita da un'unica catena di Jordan di lunghezza 3; qui

$$\begin{array}{ccc} V_1 = \mathrm{span}\{e_1\} & V_{1,\,2} = \mathrm{span}\{e_1\} & V_{1,\,3} = \mathrm{span}\{e_1\} \\ V_2 = \mathrm{span}\{e_1,\, e_2\} & V_{2,\,3} = \mathrm{span}\{e_1,\, e_2\} & \\ V_3 = \mathrm{span}\{e_1,\, e_2,\, e_3\} & & \end{array}$$

L'esistenza di una base di Jordan per un endomorfismo è una proprietà estremamente generale: si può dimostrare che

Teorema 5.10. *Siano* $(\mathbb{K}; +, \cdot)$ *un campo,* $(V, \oplus)$ *un* $\mathbb{K}$*-spazio vettoriale di dimensione finita e* $\alpha \in \mathrm{End}(V)$.
Se α *ha tutti gli autovalori in* $\mathbb{K}$*, allora ammette una base di Jordan.*

In particolare, le ipotesi del teorema sono verificate se $\mathbb{K}$ è algebricamente chiuso. Ma questo ancora non esaurisce le proprietà notevoli delle basi di Jordan: posta

Definizione 5.11. Nelle ipotesi precedenti, se $\mathcal{B}$ è una base di Jordan per α, allora la matrice

$$M_{\mathcal{B}}^{\mathcal{B}}(\alpha)$$

(che come abbiamo visto ha la diagonale occupata dagli autovalori di α, la fila obliqua sovrastante costituita solo da 0 o 1 e tutte le altre entrate nulle) si chiama *forma canonica di Jordan* di α.

si ottiene che la forma canonica di Jordan di un endomorfismo, se esiste, è univocamente determinata a meno di permutazioni nell'ordine dei suoi blocchi di Jordan.

Concludiamo con un riassunto delle virtù della forma canonica di Jordan per un endomorfismo α:

- *induce una decomposizione dello spazio vettoriale di riferimento in sottospazi invarianti rispetto ad* α (tali infatti sono gli span di ciascuna catena di Jordan);
- *esiste sotto condizioni molto generali*;
- *è essenzialmente unica, a prescindere dalla base in cui è rappresentata*;
- soprattutto *è comoda da manipolare* (spesso non esiste altro motivo che la semplicità d'uso per esercitare la propria preferenza fra oggetti equivalenti !! ;-)

Bibliografia

[1] Marco Abate. *Geometria*. Mc Graw-Hill, 1996.

[2] Siegfried Bosch. *Algebra*. Springer, 2003.

[3] Serge Lang. *Algebra Lineare*. Bollati Boringhieri, 1985.

[4] Garrett Birkhoff Saunders Mac Lane. *Algebra*. Mursia, 1999.

[5] Edoardo Sernesi. *Geometria vol.1*. Bollati Boringhieri, 2000.