ALGEBRA 2 - ESERCIZI

Matteo Varbaro, studio 946

Sottogruppi (richiamo di teoria)

Sia $(G, *)$ un gruppo.

DEF.: $H \subseteq G$ è un **sottogruppo** di G se $(H, *)$ è un gruppo, cioè:

(i) $x, y \in H \Rightarrow x * y \in H$;

(ii) $y \in H \Rightarrow y^{-1} \in H$;

(iii) $e \in H$ (se $H \neq \emptyset$ questa è già implicata da (i) e (ii)).

LEMMA: Per $\emptyset \neq H \subseteq G$, sono equivalenti:

1. H è un sottogruppo di G;
2. per ogni $x, y \in H$, $x * y^{-1} \in H$.

OSS.: Perché la seconda proprietà implica che $y^{-1} \in H$? Se $y * y^{-1} = e \in H$, allora posso scegliere la coppia $e, y \in H$, da cui segue $e * y^{-1} = y^{-1} \in H$!

Sottogruppi

ESERCIZIO: Consideriamo il gruppo $(\mathbb{C}, +)$.

- L'insieme $H = \{z \in \mathbb{C} : |z| = 1\}$ è un sottogruppo di $\mathbb{C}$? No: infatti $1 \in H$, ma $1 + 1 = 2$, avendo norma $\sqrt{2}$, non sta in H.
- $H = \{z \in \mathbb{C} : \mathrm{Re}(z) = \mathrm{Im}(z)\}$ è un sottogruppo di $\mathbb{C}$?

  Vediamo: se $x, y \in H$, allora $\mathrm{Re}(x - y) = \mathrm{Re}(x) - \mathrm{Re}(y)$ e $\mathrm{Im}(x - y) = \mathrm{Im}(x) - \mathrm{Im}(y)$, quindi

  $$\mathrm{Re}(x - y) = \mathrm{Im}(x - y).$$

  Allora $x - y \in H$. Inoltre $0 \in H$, quindi $H \neq \emptyset$. Dunque si, H è un sottogruppo di $\mathbb{C}$.

Sottogruppi

ESERCIZIO: Consideriamo il gruppo $(\mathbb{C}^*, \cdot)$.

- L'insieme $H = \{z \in \mathbb{C}^* : |z| = 1\}$ è un sottogruppo di $\mathbb{C}^*$? Si:

$$x, y \in H \Rightarrow |x| = |y| = 1 \Rightarrow$$
$$|xy^{-1}| = |x||y^{-1}| = |x||y|^{-1} = 1 \Rightarrow xy^{-1} \in H$$

  Inoltre $1 \in H$, quindi $H \neq \emptyset$.

- $H = \{z \in \mathbb{C}^* : \mathrm{Re}(z) = \mathrm{Im}(z)\}$ è un sottogruppo di $\mathbb{C}^*$?
  No: $z = 1 + i \in H$, ma $z^2 = 2i$, quindi

$$\mathrm{Re}(z^2) = 0 \neq 2 = \mathrm{Im}(z^2).$$

  Siccome $z \in H$ ma $z^2 \notin H$, $(H, \cdot)$ non è un gruppo.

Sottogruppi

ESERCIZIO: Sia $G = \mathrm{GL}_2(\mathbb{Q})$. Quali dei seguenti insiemi sono sottogruppi di G:

1. $H = \{A \in G : \det(A) = 1\}$. Si, infatti:

$\forall\, A, B \in H,\ \det(AB^{-1}) = \det(A)\det(B)^{-1} = 1,$ dunque $AB^{-1} \in H$.

Inoltre $I_2 \in H$, quindi $H \neq \emptyset$.

2. $H = \{A = (a_{ij}) \in G : a_{ij} \in \mathbb{Z}\}$. No:

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in H,\ \text{ma } A^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \notin H.$$

Sottogruppi

3. $H = \{A = (a_{ij}) \in G : a_{ij} \in \mathbb{Z} \text{ e } \det(A) = +/-1\}$. Si, infatti:
   - $\forall\ A = (a_{ij}) \in H$,

     $$A^{-1} = \begin{pmatrix} a_{22}/\det(A) & -a_{12}/\det(A) \\ -a_{21}/\det(A) & a_{11}/\det(A) \end{pmatrix},$$

     dunque A^{-1} ha entrate in $\mathbb{Z}$. Inoltre

     $$\det(A^{-1}) = \det(A)^{-1} = +/-1,$$

     quindi $A^{-1} \in H$.
   - $\forall\ A, B \in H$, $\det(AB) = \det(A)\det(B) = +/-1$; inoltre AB ha entrate in $\mathbb{Z}$, quindi $AB \in H$.
   - $I_2 \in H$.

Sottogruppi

4. $H = \{A_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Q}\}$. Si, infatti:
   - $\forall\ A_x \in H,\ A_x^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = A_{-x} \in H.$
   - $\forall\ A_x, A_y \in H, A_x A_y = \begin{pmatrix} 1 & y+x \\ 0 & 1 \end{pmatrix} = A_{y+x} \in H.$
   - $I_2 = A_0 \in H.$

Si noti che, quindi, H è un sottogruppo **Abeliano** di $\mathrm{GL}_2(\mathbb{Q})$:

$$A_x A_y = A_{y+x} = A_{x+y} = A_y A_x \quad \forall\ x, y \in \mathbb{Q}.$$

Sottogruppi

5. $H = \{A \in G : A^2 = I_2\}$. No, si considerino:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.$$

Abbiamo che $A^2 = I_2$ e $B^2 = I_2$. Ma

$$AB = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix},$$

e $(AB)^2 = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix} \neq I_2$.

Sottogruppi

LEMMA: Sia $\emptyset \neq H \subseteq G$ tale che $\sharp H < \infty$. Sono equivalenti:

1. H è un sottogruppo di G;
2. per ogni $x, y \in H$, $x * y \in H$.

Dim.: (1) $\Rightarrow$ (2) $\checkmark$.

(2) implica che: $y \in H \Rightarrow y^n \in H \; \forall \; n \in \mathbb{N} \setminus \{0\}$. Siccome H è finito, allora esistono $m \neq n$ tali che $y^m = y^n$. Supponiamo $n > m$; abbiamo $\pi(y) | n - m$, dunque $e = y^{n-m} \in H$.

Dunque, per ogni $y \in H$, (2) $\Rightarrow y^{-1} = y^{n-m-1} \in H$. Allora:

$$\forall \; x, y \in H, \text{ poiché } y^{-1} \in H \Rightarrow x * y^{-1} \in H$$

Come abbiamo già ricordato, la parte rossa scritta sopra è equivalente a (1). $\square$

Periodo (richiamo di teoria)

DEF.: Il **periodo** di un elemento $g \in G$ è:

$$\pi(g) = \inf\{n \in \mathbb{N} \setminus \{0\} : g^n = e\}.$$

ESEMPI: 1. Sia $4 \in \mathbb{Z}_6$. Si noti che:

- $4 \neq 0$ in $\mathbb{Z}_6$;
- $4 + 4 = 2 \neq 0$ in $\mathbb{Z}_6$;
- $4 + 4 + 4 = 0$ in $\mathbb{Z}_6$.

Quindi $\pi(4) = 3$.

2. Se $4 \in \mathbb{Z}$, allora $4n \neq 0 \ \forall \ n \in \mathbb{N} \setminus \{0\}$. Quindi $\pi(4) = \infty$.

3. Sia $a \in \mathbb{Q}$, e $g = \begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$. Allora

$$g^2 = \begin{pmatrix} 1 & a - a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

dunque $\pi(g) = 2$.

Periodo (richiamo di teoria)

Sia G un gruppo, e $g \in G$ un suo elemento di periodo finito.

- $g^n = e \Leftrightarrow \pi(g) | n$.
- Più in generale, $g^n = g^m \Leftrightarrow \pi(g) | n - m$.
- $\forall\ h \in \mathrm{gp}(g),\ \pi(h) | \pi(g)$. Più precisamente,

$$\pi(g^k) = \pi(g) / \operatorname{MCD}(\pi(g), k).$$

Periodo

ESERCIZIO: Si considerino le matrici di $\mathrm{GL}_2(\mathbb{Q})$:

$$g = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Provare che: 1. $\pi(g) = 3$, 2. $\pi(h) = 2$, 3. $\pi(gh) = \pi(hg) = \infty$.

1. $g^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ e $g^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot g = I_2$. Quindi $\pi(g) = 3$.

2. Chiaramente $h^2 = I_2$, dunque $\pi(h) = 2$.

3. $gh = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Per provare che $\pi(gh) = \infty$, dobbiamo dimostrare che $(gh)^n \neq I_2 \ \ \forall\ n \in \mathbb{N} \setminus \{0\}$. Come fare?

Periodo

... Supponiamo che $x \in \mathrm{GL}_2(\mathbb{Q})$ sia una matrice della forma:

$$x = \begin{pmatrix} a & b \\ * & * \end{pmatrix},$$

con $a, b \in \mathbb{Q}$. Ricordando che $gh = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, si ha:

$$x(gh) = \begin{pmatrix} b & a+b \\ * & * \end{pmatrix}.$$

Quindi se b è strettamente positivo e $a \geq 0$, le 2 entrate della prima riga di $x(gh)$ saranno strettamente positive. Grazie a questa osservazione, $(gh)^n = \begin{pmatrix} * & f_n \\ * & * \end{pmatrix}$ con qualche $f_n > 0$. Dunque $\pi(gh) = \infty$. (Si può osservare che f_n è l'n-esimo numero di Fibonacci).

Periodo

... Rimane da dimostrare che $\pi(hg) = \infty$, dove

$$hg = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}.$$

Supponiamo per assurdo che esista $n \in \mathbb{N} \setminus \{0\}$ per cui $(hg)^n = I_2$:

$$\begin{aligned} gh = h^{-1}(hg)h \Rightarrow (gh)^n = (h^{-1}hgh)^n &= (h^{-1}hgh)(h^{-1}hgh)\cdots(h^{-1}hgh) \\ &= h^{-1}(hg)hh^{-1}(hg)hh^{-1}\cdots(hg)h = h^{-1}(hg)^n h = h^{-1}I_2 h = I_2. \end{aligned}$$

Questo è assurdo, perché avevamo visto che $\pi(gh) = \infty$. Quindi

$$\pi(hg) = \pi(gh) = \infty.$$

Periodo

ESERCIZIO: Siano x e y elementi di periodo finito di un gruppo G tali che $xy = yx$

- Dimostrare che $\pi(xy) | \operatorname{mcm}(\pi(x), \pi(y))$. Sia $m = \pi(x)$, $n = \pi(y)$ e $N = \operatorname{mcm}(m, n)$. Poiché $xy = yx$,

$$(xy)^N = (xy)(xy)\cdots(xy) = xyxy\cdots xy =$$
$$= x^N y^N = (x^m)^{n/\operatorname{MCD}(m,n)} (y^n)^{m/\operatorname{MCD}(m,n)} = e.$$

  Quindi $\pi(xy) | N$.

- Provare che $\operatorname{gp}(x) \cap \operatorname{gp}(y) = \{e\} \Rightarrow \pi(xy) = \operatorname{mcm}(\pi(x), \pi(y))$. Se $(xy)^M = x^M y^M = e$, significa che x^M e y^M sono inversi l'un dell'altro. Dunque x^M e y^M sono elementi di $\operatorname{gp}(x) \cap \operatorname{gp}(y) = \{e\}$. Perciò $x^M = y^M = e$, cosicché M è multiplo sia di m che di n, e dunque di $\operatorname{mcm}(m, n)$.

Periodo

- Provare che, se $\mathrm{MCD}(\pi(x), \pi(y)) = 1$, allora $\mathrm{gp}(x) \cap \mathrm{gp}(y) = \{e\}$. In particolare $\pi(xy) = \pi(x)\pi(y)$.
  - $a \in \mathrm{gp}(x) \Rightarrow \pi(a) | \pi(x) = m$;
  - $a \in \mathrm{gp}(y) \Rightarrow \pi(a) | \pi(y) = n$.

  Quindi $a \in \mathrm{gp}(x) \cap \mathrm{gp}(y) \Rightarrow \pi(a) | \mathrm{MCD}(m, n) = 1$. Dunque

  $$\mathrm{gp}(x) \cap \mathrm{gp}(y) = \{e\}.$$

  Per quanto visto prima dunque:

  $$\pi(xy) = \mathrm{mcm}(\pi(x), \pi(y)) = \pi(x)\pi(y).$$

OSS: Se $\mathrm{gp}(x) \cap \mathrm{gp}(y) \neq \{e\}$ $\pi(xy)$ può essere diverso da $\mathrm{mcm}(\pi(x), \pi(y))$: ad esempio si considerino $4, 6 \in \mathbb{Z}_{20}$ $(12 \in \mathrm{gp}(4) \cap \mathrm{gp}(6))$:

$$\pi(4) = 5,\ \pi(6) = 10, \quad \text{ma} \quad \pi(4+6) = 2 \neq 10 = \mathrm{mcm}(5, 10).$$

Periodo

ESERCIZIO: Calcolare il periodo della permutazione

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} \in S_5.$$

- $g^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} \neq 1.$
- $g^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \neq 1.$
- $g^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix} \neq 1.$
- $g^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \neq 1.$
- $g^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1.$

Quindi $\pi(g) = 6$.

Periodo

Nell'esercizio precedente, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} = (12) \cdot (543)$, e

$$\pi(g) = 6 = 2 \cdot 3 = \pi((12)) \cdot \pi((543))$$

LEMMA (visto a teoria): Ogni permutazione $\sigma \in S_n$ si scrive come prodotto di a_i-cicli τ_i disgiunti fra loro:

$$\sigma = \tau_1 \cdot \tau_2 \cdots \tau_k.$$

(Se richiediamo che $\tau_i \neq 1 \ \forall \ i = 1, \ldots, k$, tale scrittura è unica a meno dell'ordine).

ESERCIZIO: Sia $\sigma \in S_n$, e siano $\tau_1, \ldots, \tau_k$ degli a_i-cicli disgiunti fra loro il cui prodotto sia σ. Dimostrare che

$$\pi(\sigma) = \mathrm{mcm}(a_1, \ldots, a_k).$$

Periodo

... Ragioniamo per induzione su k:

se $k = 1$, $\sigma = \tau_1$ è un a_1-ciclo, quindi $\pi(\sigma) = a_1$.

Supponiamo per induzione che $\sigma' = \tau_1 \cdot \tau_2 \cdots \tau_{k-1}$ abbia periodo $\mathrm{mcm}(a_1, \ldots, a_{k-1})$. Si noti che:

- $\sigma = \sigma' \cdot \tau_k$;
- $\mathrm{gp}(\sigma') \cap \mathrm{gp}(\tau_k) = \{e\}$;
- $\sigma' \cdot \tau_k = \tau_k \cdot \sigma'$.

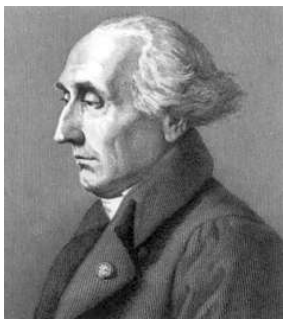
Come abbiamo visto, queste ipotesi ci permettono di dire che

$$\pi(\sigma) = \mathrm{mcm}(\pi(\sigma'), \pi(\tau_k)) = \mathrm{mcm}(\mathrm{mcm}(a_1, \ldots, a_{k-1}), a_k) = \mathrm{mcm}(a_1, \ldots, a_k).$$

Il teorema di Lagrange (richiamo di teoria)

DEF.: Sia G un gruppo finito, e $H \subseteq G$ un suo sottogruppo.
L'**indice** di H è definito come:

$$[G : H] := \sharp\{gH : g \in G\}.$$



Joseph-Luis Lagrange
(Torino, 25/1/1736 - Parigi, 10/4/1813)

TEOREMA: Se H è un sottogruppo di un gruppo finito G, allora:

$$|H| \cdot [G : H] = |G|.$$

Inoltre $[G : H] = \sharp\{Hg : g \in G\}$.

COROLLARIO: Se H è un sottogruppo di un gruppo finito G, allora $|H|$ divide $|G|$.

Normalità (richiamo di teoria)

DEF.: Un sottogruppo H di G si dice **normale** in G se

$$gH = Hg \ \forall \ g \in G.$$

OSS: $H \subseteq G$ è un sottogruppo normale in G se e solo se:

$$\forall \ g \in G, \ \forall \ h \in H \Rightarrow g^{-1}hg \in H.$$

Se $H \subseteq G$ è normale, allora ha senso considerare il gruppo quoziente G/H. Dalla definizione segue che $|G/H| = [G : H]$, dunque il teorema di Lagrange in questo caso dice che

$$|H| \cdot |G/H| = |G|$$

Normalità

ESERCIZIO: Sia $G = S_4$, $\tau = (1234) \in G$, e $H = \mathrm{gp}(\tau)$.

- Qual'è l'ordine di H? $|H| = \pi((1234)) = 4$.
- Qual'è l'indice di H? Per il teorema di Lagrange:

$$[G : H] = |G|/|H| = 24/4 = 6.$$

- H è normale? No:

$$H = \{\tau = (1234),\ \tau^2 = (13)(24),\ \tau^3 = (1432),\ \tau^4 = e\}.$$

Ma $(12)(1234)(12) = (1342) \notin H$.

Normalità

ESERCIZIO: Sia G un gruppo, e H un suo sottogruppo.

- Se G è Abeliano, H è normale? Si, perché:

$$g^{-1}hg = g^{-1}gh = h \in H \quad \forall\, g \in G,\ \forall\, h \in H.$$

- Se H è Abeliano, è normale? Non necessariamente, ad esempio $H = \mathrm{gp}(\tau)$ è Abeliano per ogni $\tau \in G$, ma nella slide precedente abbiamo visto che se $\tau = (1234) \in S_4$, $\mathrm{gp}(\tau)$ non è normale in $G = S_4$.
- Se H è normale e K è un altro sottogruppo normale di G, allora $H \cap K$ è un sottogruppo normale di G? Si, dati elementi di $g \in G$ e $h \in H \cap K$:

$$g^{-1}hg \in H \quad \text{e} \quad g^{-1}hg \in K \Rightarrow g^{-1}hg \in H \cap K$$

Omomorfismi (richiamo di teoria)

Se G e G' sono gruppi, una funzione $\phi : G \to G'$ si dice **omomorfismo** se:

$$\phi(gh) = \phi(g)\phi(h) \quad \forall\ g, h \in G.$$

Se ϕ è un omomorfismo:

- $\mathrm{Ker}(\phi)$ è un sottogruppo normale di G.
- $\mathrm{Im}(\phi)$ è un sottogruppo di G'.
- $\mathrm{Im}(\phi) \cong G/\mathrm{Ker}(\phi)$ (I TEOREMA DI ISOMORFISMO).

I sottogruppi normali di G sono tutti e soli i nuclei di omomorfismi che partono da G.

I sottogruppi di G sono tutti e soli le immagini di omomorfismi che arrivano a G.

Omomorfismi

ESERCIZIO: Sia G un gruppo, e $H = \{(g, g) : g \in G\} \subseteq G^2$.

- Dimostrare che H è normale in $G^2 \Leftrightarrow G$ è Abeliano.

  " $\Leftarrow$ " è ovvio. " $\Rightarrow$ " Se H è normale in G^2, allora

  $$x^{-1}(g, g)x \in H \quad \forall\, x \in G^2,\ (g, g) \in H.$$

  Per ogni $g, h \in G$, si scelga $x = (h, e)$. Allora

  $$x^{-1}(g, g)x = (h^{-1}, e)(g, g)(h, e) = (h^{-1}gh, g) \in H.$$

  Quindi $h^{-1}gh = g \Rightarrow gh = hg \Rightarrow G$ è Abeliano.
- Se G è Abeliano, si dimostri che $G^2/H \cong G$. .....

Omomorfismi

Si consideri la funzione:

$$\begin{array}{rcl} \phi : G^2 & \to & G \\ (x, y) & \mapsto & xy^{-1} \end{array}$$

- $\phi((x, y)(u, v)) = \phi((xu, yv)) = xu(yv)^{-1} = xuv^{-1}y^{-1} = xy^{-1}uv^{-1} = \phi((x, y))\phi((u, v))$. Quindi ϕ è un omomorfismo.
- ϕ è surgettivo: $\forall\ g \in G$, $\phi((g, e)) = g$.
- $(x, y) \in \mathrm{Ker}(\phi) \Leftrightarrow xy^{-1} = e \Leftrightarrow x = y$. Quindi $\mathrm{Ker}(\phi) = H$.

Allora, grazie al primo teorema di isomorfismo, deduciamo che

$$G^2/H \cong G.$$

Omomorfismi

ESERCIZIO: Fissato un gruppo G, dire quali delle seguenti funzioni $f : G \to G$ sono omomorfismi:

- $f(x) = x^{-1} \quad \forall\, x \in G$. No: $G = S_3$,

  $f((12)(13)) = f((132)) = (132)^{-1} = (123) \neq (12)(13) = f((12))f((13))$.

  Però è un omomorfismo se G è Abeliano:

  $$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y).$$

- Per $g \in G$ fissato, $f(x) = g^{-1}xg \quad \forall\, x \in G$. Si:

  $$f(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = f(x)f(y).$$

Omomorfismi

ESERCIZIO: Dire se esiste, eventualmente determinandolo, un omomorfismo di gruppi del tipo:

- iniettivo e non surgettivo da $\mathbb{Z}$ in $\mathbb{Z}$: si, per esempio $f(x) = 2x \ \ \forall\, x \in \mathbb{Z}$.
- surgettivo e non iniettivo da $\mathbb{Z}$ in $\mathbb{Z}$: no, se

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

è surgettivo, allora dal primo teorema di isomorfismo $\mathbb{Z} \cong \mathbb{Z}/\operatorname{Ker}(f)$, che è vero se e solo se $\operatorname{Ker}(f) = \{0\}$.

- non banale da $\mathbb{Z}_n$ in $\mathbb{Z}$: no, infatti se $f : \mathbb{Z}_n \to \mathbb{Z}$ è un omomorfismo allora:

$$nf(k) = f(nk) = f(0) = 0 \ \ \forall\, k \in \mathbb{Z}_n,$$

dunque $f(k) = 0$ per ogni $k \in \mathbb{Z}_n$.

Omomorfismi

- surgettivo da $\mathbb{Z}$ in S_4: no, infatti se $\mathbb{Z} \xrightarrow{f} S_4$ fosse surgettivo, allora $S_4 \cong \mathbb{Z}/\operatorname{Ker}(f)$; ma ciò è impossibile perché S_4 non è abeliano.
- iniettivo da $\mathbb{Z} \to \mathbb{Q}^*$: si, ad esempio

$$\begin{array}{rccc} f : \mathbb{Z} & \to & \mathbb{Q}^* \\ m & \to & 2^m \end{array}$$

- da $\mathbb{Z}$ in S_7 con nucleo $\operatorname{gp}(11)$: no, infatti se $\mathbb{Z} \xrightarrow{f} S_7$ fosse un tale omorfismo, avremmo che $\mathbb{Z}_{11} \cong \mathbb{Z}/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$ sarebbe un sottogruppo di S_7. Ciò contraddirrebbe Lagrange, perché 11 non divide $7! = |S_7|$.

Omomorfismi

- da $\mathbb{Z}$ in S_7 con nucleo $\mathrm{gp}(12)$: si, si consideri

$$\sigma = (123)(4567) \in S_7,$$

e si noti che $\pi(\sigma) = 12$. L'omomorfismo

$$\begin{array}{rcl} f : \mathbb{Z} & \to & S_7 \\ m & \to & \sigma^m \end{array}$$

è tale che $\mathrm{Ker}(f) = \mathrm{gp}(12)$.

- da $\mathbb{Z}$ in S_7 con nucleo $\mathrm{gp}(9)$? Rispondete per casa .....

Omomorfismi & periodo

Ricordiamo che, dato un omomorfismo di gruppi $f : G_1 \to G_2$, si ha:

- Per ogni $x \in G_1$, $\pi(f(x))|\pi(x)$:

$$(n = \pi(x) \Rightarrow f(x)^n = f(x^n) = f(e_{G_1}) = e_{G_2}).$$

- Se f è iniettivo, allora $\pi(f(x)) = \pi(x)\ \forall\ x \in G_1$:

$$(m < \pi(x) \Rightarrow f(x)^m = f(x^m) \underset{\mathrm{Ker}(f)=\{e_{G_1}\}}{\neq} e_{G_2}.$$

- Per ogni $n \in \mathbb{N} \setminus \{0\}$, esiste un elemento z di $\mathbb{C}^*$ di periodo n: basta considerare

$$z = \cos 2\pi/n + i \sin 2\pi/n.$$

Omomorfismi & periodo

OSS.: La funzione $f : \mathbb{C}^* \to \mathrm{GL}_2(\mathbb{R})$ definita come:

$$x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

è un omomorfismo di gruppi:

$$f(x+iy)f(s+it) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}\begin{pmatrix} s & t \\ -t & s \end{pmatrix} = \begin{pmatrix} xs-yt & xt+ys \\ -ys-xt & -yt+xs \end{pmatrix}$$
$$= f((xs-yt)+i(xt+ys)) = f((x+iy)(s+it)).$$

Si noti che f è iniettivo. Dunque per ogni $n \in \mathbb{N} \setminus \{0\}$, esiste un elemento A di $\mathrm{GL}_2(\mathbb{R})$ di periodo n. Si noti anche che

$$\det(f(x+iy)) = x^2 + y^2 = |x+iy|^2$$

Omomorfismi & periodo

ESERCIZIO: *Esiste un omomorfismo di gruppi ...*

(c) *... iniettivo da* $\mathbb{Z}_4$ *a* $\mathbb{C}^*$*?* Si, basta scegliere $z \in \mathbb{C}^*$ di periodo 4, e definire $f(\overline{k}) = z^k$.

(d) *... iniettivo da* $\mathbb{Z}_4$ *a* $\mathbb{C}$*?* No, poiché $\mathbb{C}$ non ha elementi di periodo 4.

(e) *... da* $\mathbb{Z}$ *a* $\mathrm{GL}_2(\mathbb{R})$ *con nucleo* $\mathrm{gp}(5)$*?* Si, basta scegliere $A \in \mathrm{GL}_2(\mathbb{R})$ di periodo 5, e definire $f(k) = A^k$.

(f) *... iniettivo da* $\mathbb{Z}^5$ *a* $\mathbb{Q}^*$*?* Si, ad esempio basta definire

$$f(a, b, c, d, e) = 2^a 3^b 5^c 7^d 11^e.$$

(Il fatto che f è iniettivo segue dalla fattorizzazione unica, e dal fatto che $2, 3, 5, 7, 11$ sono numeri primi).

Gruppi piccoli

DOMANDA: Qual'è il gruppo non Abeliano di ordine più piccolo possibile?

Nelle prossime slides dimostreremo che, se G non è Abeliano, allora $|G| \geq 6$. Inoltre, a meno di isomorfismo gli unici gruppi di ordine 6 sono:

$$\mathbb{Z}_6 \quad \text{e} \quad S_3.$$

Dunque S_3 è l'unico gruppo non Abeliano di ordine 6.

ESERCIZIO: Se G è un gruppo il cui ordine è un numero primo, allora è Abeliano.

Sia $e \neq g \in G$: allora, essendo $\mathrm{gp}(g)$ un sottogruppo di G, abbiamo che $\pi(g)$ divide $|G|$ per Lagrange. Ma

$$\pi(g) \neq 1 \ \ \& \ \ |G| \text{ numero primo } \Rightarrow \pi(g) = |G|,$$

da cui $G = \mathrm{gp}(g)$. Dunque G è Abeliano!

Gruppi piccoli

ESERCIZIO: Sia G un gruppo tale che $g^2 = e$ per ogni $g \in G$. Dimostrare che G è Abeliano.

Se $g, h \in G$, allora $(gh)(hg) = geg = gg = e$. Dunque

$$hg = (gh)^{-1}.$$

Ma per ipotesi $(gh)^2 = e$, quindi anche $gh = (gh)^{-1}$. Allora $hg = gh$ per ogni $g, h \in G$, quindi G è Abeliano.

ESERCIZIO: Dimostrare che:

$$|G| = 4 \Rightarrow G \text{ è Abeliano}$$

Se esiste $g \in G$ di periodo 4, allora $G = \mathrm{gp}(g)$ è Abeliano.

Altrimenti, siccome per il teorema di Lagrange $\pi(g)|4$ per ogni $g \in G$, abbiamo che $g^2 = e$ per ogni $g \in G$. Per quanto visto nell' esercizio precedente un tale gruppo G è Abeliano!

Gruppi piccoli

Ricapitolando, finora sappiamo che:

- $|G| = 1 \Rightarrow G$ è Abeliano (ovvio).
- $|G| \in \{2, 3, 5\} \Rightarrow G$ è Abeliano ($|G|$ è primo).
- $|G| = 4 \Rightarrow G$ è Abeliano.

Quindi se G non è Abeliano allora $|G| \geq 6$. D'altronde sappiamo che S_3 non è Abeliano e ha ordine 6 !

Ora proveremo che S_3 è l'unico gruppo non Abeliano di ordine 6: più in generale, proveremo che gli unici gruppi di ordine 6 sono:

$$S_3 \quad \text{e} \quad \mathbb{Z}_6.$$

Sia G un gruppo di ordine 6. Se esiste $g \in G$ di periodo 6, allora $G = \mathrm{gp}(g) = \mathbb{Z}_6$. Supponiamo che $\pi(g) \neq 6$ per ogni $g \in G$; per Lagrange $\pi(g) \in \{2, 3\}\ \forall\ e \neq g \in G$ ....

Gruppi piccoli

Supponiamo per assurdo che $g^2 = e \ \forall \ g \in G$: in tal caso G è Abeliano, e la sua tabella di moltiplicazione sarebbe:

$\cdot$	1	a	b	ab	...	...
1	1	a	b	ab	...	...
a	a	1	ab	b	...	...
b	b	ab	1	a	...	...
ab	ab	b	a	1	...	...
...	...	...	...	...	...	...
...	...	...	...	...	...	...

Notiamo che $\{1, a, b, ab\}$ sarebbe un sottogruppo di G di ordine 4. Ma questo contraddice il teorema di Lagrange, poiché 4 non divide $6 = |G|$. Dunque deve esistere $g \in G$ di periodo 3 .....

Gruppi piccoli

Supponiamo che a sia un elemento di G tale che $\pi(a) = 3$.
Siccome $H = \mathrm{gp}(a) = \{1, a, a^2\}$ ha indice

$$|G : H| = |G|/|H| = 6/3 = 2,$$

H è un sottogruppo normale di G. Quindi possiamo considerare il gruppo quoziente G/H di ordine 2. Poniamo

$$G = \{1, a, a^2, b, c, d\}.$$

Siccome $\overline{b}^2 = \overline{1}$ in G/H, allora $b^2 \in H$. Proviamo che $b^2 = 1$:

$$b^2 \neq 1 \Rightarrow b^2 \in \{a, a^2\} \text{ e } \pi(b) = 3.$$

Ma allora $b^3 = b(b^2) = 1$, quindi b è l'inverso di un elemento in $\{a, a^2\}$; ma a e a^2 sono l'uno inverso dell'altro, dunque $b = a$ oppure $b = a^2$. In ogni caso otterremmo un assurdo, quindi $b^2 = 1$.
Discorso analogo vale per c e d:

$$b^2 = c^2 = d^2 = 1.$$

Gruppi piccoli

Siamo pronti per costruire la tabella della moltiplicazione di G:

$\cdot$	1	a	a^2	b	ab	ba
1	1	a	a^2	b	ab	ba
a	a	a^2	1	ab	ba	b
a^2	a^2	1	a	ba	b	ab
b	b	ba	ab	1	a^2	a
ab	ab	b	ba	a	1	a^2
ba	ba	ab	b	a^2	a	1

$(a^2b)(ba) = 1 \quad \& \quad (a^2b)^2 = 1 \Rightarrow a^2b = ba$

Potete verificare che quella sopra è proprio la tabella moltiplicativa di S_3, scegliendo, per esempio:

$$a = (123) \quad \text{e} \quad b = (12).$$

Automorfismi (richiamo di teoria)

DEF.: Un **automorfismo** di un gruppo G è un isomorfismo da G in G. L'insieme degli automorfismi di G si denota con $\mathrm{Aut}(G)$, ed è un gruppo con la composizione come prodotto:

$$\phi * \psi = \phi \circ \psi \quad \forall\, \phi, \psi \in \mathrm{Aut}(G).$$

Dato $g \in G$, l'omomorfismo $T_g : G \to G$ definito da $T_g(x) = g^{-1}xg$ è un automorfismo.

DEF.: Un elemento del tipo T_g con $g \in G$ si dice **automorfismo interno** di un gruppo G. L'insieme degli automorfismi interni di G si denota con $\mathrm{Inn}(G)$, ed è un sottogruppo di $\mathrm{Aut}(G)$.

PROP.: $\mathrm{Inn}(G)$ è un sottogruppo normale di $\mathrm{Aut}(G)$. Inoltre, se $Z(G) = \{g \in G : gx = xg \ \forall\, x \in G\}$ è il **centro** di G (che è un sottogruppo normale in G), si ha:

$$\mathrm{Inn}(G) \cong G/Z(G).$$

Automorfismi

ESERCIZIO: Se $n \geq 3$, dimostrare che $Z(S_n) = \{e\}$.

$\forall\ e \neq \sigma \in S_n$, per provare che $\sigma \notin Z(S_n)$, dobbiamo esibire $\tau \in S_n$ tale che $\sigma\tau \neq \tau\sigma$:

$$\sigma \neq e \Rightarrow \exists\ i \neq j \in \{1, \ldots, n\} : \sigma(i) = j.$$

Siccome $n \geq 3$, $\exists\ k \in \{1, \ldots, n\} \setminus \{i, j\}$: consideriamo $\tau = (ik)$:

- $\sigma\tau(i) = \sigma(k) \neq j$.
- $\tau\sigma(i) = \tau(j) = j$.

Dunque $\sigma\tau \neq \tau\sigma$, cioè $\sigma \notin Z(S_n)$.

Automorfismi

ESERCIZIO: $\mathrm{Aut}(S_3) = S_3$. Sappiamo che $Z(S_3) = \{e\}$, quindi $\mathrm{Inn}(G) \cong S_3$. Dunque S_3 è un sottogruppo di $\mathrm{Aut}(G)$. In particolare $6 = |S_3|$ divide l'ordine di $\mathrm{Aut}(G)$.

Notiamo che, se ϕ è un automorfismo di un gruppo G, allora il periodo di g è uguale a quello di $\phi(g)$ per ogni $g \in G$. Denotando con A l'insieme di tutte le funzioni bigettive da S_3 in se stesso *che preservano il periodo*, dunque, $\mathrm{Aut}(S_3) \subseteq A$. Poiché S_3 ha esattamente 1 elemento di periodo 1, 3 di periodo 2 e 2 di periodo 3, A ha cardinalità $1! \cdot 3! \cdot 2! = 12$. Quindi

$$|\mathrm{Aut}(G)| \leq 12.$$

Dunque $\mathrm{Aut}(G)$ ha ordine 6 o 12...

Automorfismi

Consideriamo la bigezione di $\phi : S_3 \to S_3$ tale che:

- $\phi((12)) = (13)$;
- $\phi((13)) = (12)$;
- $\phi(\sigma) = \sigma \quad \forall\, \sigma \in S_3 \setminus \{(12), (13)\}$.

Si noti che $\phi \in A$, ma non sta in $\mathrm{Aut}(G)$ perché:

$$\phi((12))\phi((13)) = (13)(12) = (123) \neq (132) = \phi((132)) = \phi((12)(13)).$$

Allora $|\mathrm{Aut}(S_3)| < 12$, quindi $|\mathrm{Aut}(S_3)| = 6$ e $\mathrm{Aut}(S_3) \cong S_3$.

CURIOSITÀ: si può dimostrare che $\mathrm{Aut}(S_n) \cong S_n$ per ogni $n \neq 6$, e che S_6 è un sottogruppo di $\mathrm{Aut}(S_6)$ di indice 2.

Prodotti (richiamo di teoria)

Siano G_1 e G_2 gruppi, $H_1 \subseteq G_1$ e $H_2 \subseteq G_2$ sottogruppi $G = G_1 \times G_2$, e $H = H_1 \times H_2 \subseteq G$.

- H è normale in G se e solo se H_i è normale in G_i per ogni $i = 1, 2$.
- Se H è normale, $G/H \cong G_1/H_1 \times G_2/H_2$.

Non tutti i sottogruppi di G sono della forma $H_1 \times H_2$:

ESEMPIO: Sia $g = (g_1, g_2) \in G$ un elemento *di periodo infinito* e $H = \mathrm{gp}(g)$. Allora

$$\exists\, H_1 \subseteq G_1, H_2 \subseteq G_2 \ : \ H = H_1 \times H_2 \ \Leftrightarrow \ g_1 = e_{G_1} \ \text{ o } \ g_2 = e_{G_2}.$$

Infatti $\pi(g) = \infty \Leftrightarrow \pi(g_1) = \infty$ oppure $\pi(g_2) = \infty$. Supponiamo $\pi(g_1) = \infty$; se $H = H_1 \times H_2$, allora dovrebbe esistere $n \in \mathbb{Z}$ tale che $g^n = (g_1^n, g_2^n) = (e_{G_1}, g_2)$ (poiché $(e_{G_1}, g_2) \in H_1 \times H_2$). Ma $g_1^n = e_{G_1} \Rightarrow n = 0$, quindi l'unica possibilità è che $g_2 = g_2^0 = e_{G_2}$.

Prodotti

Siano G_1 e G_2 gruppi, $G = G_1 \times G_2$, e $g = (g_1, g_2) \in G$.

- *Dimostrare che* $\pi(g) = \mathrm{mcm}(\pi(g_1), \pi(g_2))$. Dato $n \in \mathbb{N} \setminus \{0\}$, chiamando $N = \mathrm{mcm}(\pi(g_1), \pi(g_2))$ abbiamo

$$g^n = e_G \Leftrightarrow (g_1^n, g_2^n) = (e_{G_1}, e_{G_2}) \Leftrightarrow \pi(g_1)|n \text{ e } \pi(g_2)|n \Leftrightarrow N|n$$

- *Se g ha periodo finito, dimostrare che esistono $H_1 \subseteq G_1, H_2 \subseteq G_2$ tali che $\mathrm{gp}(g) = H_1 \times H_2$ se e solo se $\mathrm{MCD}(\pi(g_1), \pi(g_2)) = 1$*. Se $g = (g_1, g_2) \in H_1 \times H_2$, allora $g_1 \in H_1$ e $g_2 \in H_2$. Dunque, se H_1 e H_2 esistono, allora $H_1 = \mathrm{gp}(g_1)$ e $H_2 = \mathrm{gp}(g_2)$. Allora abbiamo un inclusione di insiemi finiti

$$\mathrm{gp}(g) = \{(g_1^a, g_2^a) : a \in \mathbb{Z}\} \subseteq \{(g_1^b, g_2^c) : b, c \in \mathbb{Z}\} = \mathrm{gp}(g_1) \times \mathrm{gp}(g_2),$$

che è un'uguaglianza se e solo se $|\mathrm{gp}(g)| = |\mathrm{gp}(g_1) \times \mathrm{gp}(g_2)|$ se e solo se $\mathrm{mcm}(\pi(g_1), \pi(g_2)) = \pi(g_1)\pi(g_2)$.

Prodotti

ESERCIZIO: Sia G un gruppo, e H e H' due sottogruppi.

(i) *Se H è normale e $H' \cong H$, possiamo dedurre che H' è normale?* No, ad esempio si consideri $G = \mathbb{Z}_2 \times S_3$, $H = \mathrm{gp}((1, \mathrm{id}))$ e $H' = \mathrm{gp}((0, (12)))$. H e H' sono isomorfi perché entrambi hanno ordine 2, H è normale perché $H = \mathbb{Z}_2 \times \{\mathrm{id}\}$, ma H' non lo è perché $H' = \{0\} \times \mathrm{gp}((12))$.

(ii) *Provare che, se esiste $\phi \in \mathrm{Aut}(G)$ tale che $\phi(H) = H'$, allora H è normale se e solo se H' è normale. Inoltre, in tal caso $H \cong H'$ e, se H è normale, $G/H \cong G/H'$.*

$$\forall\, g \in G, h \in H,\ g^{-1}hg \in H \Leftrightarrow \phi(g^{-1}hg) \in \phi(H) \Leftrightarrow$$
$$\phi(g)^{-1}\phi(h)\phi(g) \in \phi(H) \Leftrightarrow (g')^{-1}h'g' \in H'\ \forall\, g' \in G, h' \in H'$$

...

Prodotti

(ii) ... Chiaramente $\phi|_H : H \to G$ è un omomorfismo di gruppi iniettivo, dunque $H \cong \phi(H) = H'$.

Inoltre, se H (e quindi H') è normale $\overline{\phi} : G \to G/H'$ è surgettivo, e $\mathrm{Ker}(\overline{\phi}) = \phi^{-1}(H') = H$. Per il I teorema di isomorfismo, dunque,

$$G/H = G/\mathrm{Ker}(\overline{\phi}) \cong G/H'.$$

(iii) *Se sia H che H' sono normali, e $H \cong H'$, possiamo dedurre che $G/H \cong G/H'$?* No, ad esempio sia $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, $H = \mathrm{gp}((2,0))$ e $H' = \mathrm{gp}((0,1))$. Essendo G Abeliano, sia H che H' sono normali. Inoltre $|H| = |H'| = 2 \Rightarrow H \cong H'$; ma

$$H = \mathrm{gp}(2) \times \{0\} \Rightarrow G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$H' = \{0\} \times \mathbb{Z}_2 \Rightarrow G/H' \cong \mathbb{Z}_4$$

Azioni (richiamo di teoria)

Sia G un gruppo e X un insieme. Un' applicazione

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

si dice **azione** di G su X se:

- $e \cdot x = x \quad \forall\, x \in X$;
- $(gh) \cdot x = g \cdot (h \cdot x) \quad \forall\, g, h \in G,\ x \in X$.

Ad un elemento $x \in X$ sono associati due oggetti:

- L'**orbita** di x, $O_x = \{g \cdot x : g \in G\} \subseteq X$;
- Lo **stabilizzatore** (anche detto **gruppo di isotropia**) di x, $C_x = \{g \in G : g \cdot x = x\} \subseteq G$.

Per ogni $x \in X$, C_x è un sottogruppo (non necessariamente normale) di G e

$$|C_x||O_x| = |G|.$$

Azioni

ESERCIZI Sia X l'insieme delle funzioni da $\mathbb{R}$ in $\mathbb{R}$, e $*_i : \mathbb{Z} \times X \to X$, $i = 1, 2$, definite come:

$$(n *_1 f)(x) = f(n + x)$$
$$(n *_2 f)(x) = f(x) + n$$

(a) $*_1$ *è un' azione di* X *su* $\mathbb{Z}$*?* Si:

- $\forall\, x \in \mathbb{R},\ (0 *_1 f)(x) = f(0 + x) = f(x) \Rightarrow 0 *_1 f = f$.
- $\forall\, x \in \mathbb{R},\ ((m + n) *_1 f)(x) = f(m + n + x) = (m *_1 f)(n + x) = n *_1 (m *_1 f)(x)$
  $\Rightarrow (n + m) *_1 f = (m + n) *_1 f = n *_1 (m *_1 f)$.

Determinare un elemento $f \in X$ *con orbita banale*. Bisogna trovare $f \in X$ tale che $n *_1 f = f\ \forall\ n \in \mathbb{Z}$, ovvero tale che

$$f(n + x) = f(x)\ \forall\ n \in \mathbb{Z}, x \in \mathbb{R}.$$

Una funzione del genere è, per esempio, $f(x) = \sin(2\pi x)$.

Azioni

Ricordiamo che $*_2 : \mathbb{Z} \times X \to X$, è definita come:

$$(n *_2 f)(x) = f(x) + n$$

(b) $*_2$ *è un' azione di* X *su* $\mathbb{Z}$*?* Si:

- $\forall\, x \in \mathbb{R},\ (0 *_2 f)(x) = f(x) + 0 = f(x) \Rightarrow 0 *_2 f = f$.
- $\forall\, x \in \mathbb{R},\ ((m+n) *_2 f)(x) = f(x) + m + n = (n *_2 (m *_2 f))(x)$ $\Rightarrow (n+m) *_2 f = (m+n) *_2 f = n *_2 (m *_2 f)$.

Determinare un elemento $g \in X$ *che non stia nell'orbita di* $f(x) = x^2$. Ad esempio si consideri $g(x) = x$; se esistesse $n \in \mathbb{Z}$ tale che $n *_2 f = g$, allora

$$x^2 + n = x \quad \forall\, x \in \mathbb{R}.$$

Questo è impossibile, perché $x^2 - x + n$ ha al più 2 radici.

Azioni

ESERCIZIO Sia $H = \left\{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \subset \mathrm{GL}_2(\mathbb{R})$.

(i) H è un sottogruppo di $\mathrm{GL}_2(\mathbb{R})$. *Esiste in H un elemento di periodo 4?* No: sia A un tale elemento. Siccome $A^4 = I_2$, si ha

$$\det(A)^4 = \det(A^4) = 1,$$

dunque $\det(A) \in \{+1, -1\}$. Se $\det(A) = 1$, allora

$$A = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} =: A_b.$$

È facile vedere che $A_b^4 = A_{4b}$, dunque $A_b^4 = I_2 \Leftrightarrow b = 0$; ciò non è possibile perché allora $A = I_2$ avrebbe periodo 1.

Se $\det(A) = -1$, allora $A = \begin{pmatrix} -1 & 0 \\ b & 1 \end{pmatrix}$. Allora avremmo

$$A^2 = \begin{pmatrix} 1 & 0 \\ -b + b & 1 \end{pmatrix} = I_2.$$

Allora il periodo di A sarebbe 2, che è una contraddizione.

Azioni

(ii) Si consideri l'azione $* : H \times \mathbb{R}^2 \to \mathbb{R}^2$ definita come:

$$A_{a,b} * (x, y) = (ax, bx + y), \; A_{a,b} = \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}.$$

Trovare la partizione di $\mathbb{R}^2$ *in orbite*. Si noti che, per $(x, y) \in \mathbb{R}^2$,

$$O_{(x,y)} = \{(ax, bx + y) : a, b \in \mathbb{R}, a \neq 0\}.$$

- Se $x \neq 0$, allora $O_{(x,y)} = \{(u, v) : u, v \in \mathbb{R}, u \neq 0\}$. Infatti se (u, v) sta nel secondo insieme, allora

$$(u, v) = (u/x \cdot x, (v - y)/x \cdot x + y) = A_{u/x,(v-y)/x} * (x, y).$$

- Se $x = 0$, allora $O_{(x,y)} = O_{(0,y)} = \{(0, y)\}$.

Dunque la partizione di $\mathbb{R}^2$ in orbite è:

$$\mathbb{R}^2 = O_{(1,0)} \cup \left(\bigcup_{y \in \mathbb{R}} O_{(0,y)} \right).$$

Azioni

ESERCIZIO: Sia $X = \{\text{polinomi in } n \text{ variabili a coefficienti interi}\}$ e $\rho : S_n \times X \to X$ l'applicazione definita come:

$$(\sigma, F(x_1, \ldots, x_n)) \mapsto \sigma \cdot F := F(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

- Calcolare $(13) \cdot F$ dove $F = x_1^2 + x_1 x_2^2 + x_3^3$:

$$(13) \cdot F = x_3^2 + x_3 x_2^2 + x_1^3.$$

- Dimostrare che ρ è un'azione:
  - ovviamente $e \cdot F = F \ \ \forall\, F \in X$;
  - $\forall\, \sigma, \tau \in S_n$, $F = F(x_1, \ldots, x_n) \in X$:

$$(\sigma\tau) \cdot F = F(x_{\sigma\tau(1)}, \ldots, x_{\sigma\tau(n)}) = \sigma \cdot F(x_{\tau(1)}, \ldots, x_{\tau(n)}) = \sigma \cdot (\tau \cdot F)$$

Azioni

Si consideri $F = \prod_{1 \le i < j \le n}(x_i - x_j)$.

- Dati $1 \le h < k \le n$, si calcoli $(hk) \cdot F$: siano

$$G = \prod_{\substack{i,j \in \{1,\dots,n\} \setminus \{h,k\} \\ i<j}} (x_i - x_j)$$

$$H = \prod_{1 \le i < h} (x_i - x_h)(x_i - x_k) \cdot \prod_{k < j \le n} (x_h - x_j)(x_k - x_j).$$

Si osservi che $(hk) \cdot G = G$, e

$$(hk) \cdot H = \prod_{1 \le i < h} (x_i - x_k)(x_i - x_h) \cdot \prod_{k < j \le n} (x_k - x_j)(x_h - x_j) = H.$$

Azioni

- ... Ora ci scriviamo F come

$$G \cdot H \cdot \prod_{h<j<k} (x_h - x_j)(x_j - x_k) \cdot (x_h - x_k)$$

Dunque $(hk) \cdot F$ sarà:

$$G \cdot H \cdot \prod_{h<j<k} (x_k - x_j)(x_j - x_h) \cdot (x_k - x_h) =$$

$$G \cdot H \cdot \prod_{h<j<k} (-1)(x_j - x_k)(-1)(x_h - x_j) \cdot (-1)(x_h - x_k) =$$

$$G \cdot H \cdot \prod_{h<j<k} (x_j - x_k)(x_h - x_j) \cdot (-1)(x_h - x_k) =$$

$$(-1) \cdot G \cdot H \cdot \prod_{h<j<k} (x_j - x_k)(x_h - x_j) \cdot (x_h - x_k) =$$

$$= -F$$

Azioni

- Dimostrare che lo stabilizzatore C_F di F è un sottogruppo di S_n di indice 2: Siccome $|C_F||O_F| = |S_n|$, basta provare che O_F ha cardinalità 2. In effetti possiamo vedere che

$$O_F = \{F, -F\}.$$

Ad esempio, questo si può vedere così: ogni $\sigma \in S_n$ si può scrivere come prodotto di scambi:

$$\sigma = \tau_1 \cdots \tau_k.$$

Nella slide precedente abbiamo visto che $\tau \cdot F = -F$ per ogni scambio τ, dunque

$$\sigma \cdot F = \tau_1 \cdot (\tau_2 \cdots (\tau_k \cdot F) \dots) = (-1)^k F.$$

Il gruppo alternante

Ricordiamo che $F = \prod_{1 \leq i < j \leq n}(x_i - x_j)$.

DEF.: Una permutazione $\sigma \in S_n$ è **pari** se $\sigma \cdot F = F$, **dispari** se $\sigma \cdot F = -F$.

OSS.: Come sappiamo, è possibile scrivere ogni permutazione $\sigma \in S_n$ come prodotto di scambi. Tale scrittura non è unica, ma dall'esercizio precedente possiamo dire che, se $\sigma = \tau_1 \cdots \tau_k$ per certi scambi τ_i, allora σ è pari se e solo se k è pari.

DEF.: Lo stabilizzatore di F, cioè il sottogruppo delle permutazioni pari di S_n, si chiama il **gruppo alternante**, e si denota con A_n.

OSS.: Avendo indice 2, A_n è un sottogruppo normale di S_n.

Il gruppo alternante

ESERCIZIO: sia $\tau \in S_n$ un k-ciclo. Dimostrare che τ è pari se e solo se k è dispari.

Scriviamo $\tau = (i_1\ i_2\ \cdots\ i_k)$ come prodotto di scambi come segue:

$$(i_1\ i_k)\cdots(i_1\ i_4)(i_1\ i_3)(i_1\ i_2) = \tau.$$

Abbiamo scritto τ come prodotto di $k-1$ scambi. Quindi τ è pari se e solo se $k-1$ è pari.

OSS.: Se $\sigma \in S_n$ si scrive come prodotto di a_i-cicli τ_i, $i = 1, \ldots, k$, allora σ è pari se e solo se $\sum_{i=1}^{k}(a_i - 1)$ è pari.

Infatti, dall'esercizio precedente ogni τ_i si può scrivere come prodotto di $(a_i - 1)$ scambi, dunque $\sigma = \tau_1 \cdots \tau_k$ si può scrivere come prodotto di $\sum_{i=1}^{k}(a_i - 1)$ scambi.

Il gruppo alternante

ESERCIZIO: Elencare gli elementi di A_4 e dire quali sono i loro periodi.

Ogni elemento di S_4 può essere scritto in maniera unica come prodotto di cicli disgiunti: dunque gli elementi di S_4 sono:

(i) id;

(ii) 2-cicli (6 elementi);

(iii) prodotti di 2-cicli disgiunti (3 elementi);

(iv) 3-cicli (8 elementi);

(v) 4-cicli (6 elementi).

Per l'osservazione della slide precedente, gli elementi di A_4 sono di tipo (i), (iii) o (iv). In particolare i periodi possibili sono 1, 2 o 3.

Il gruppo alternante

ESERCIZIO: Dimostrare che A_4 non ha sottogruppi di ordine 6.

Osserviamo che $|A_4| = 24/2 = 12$, dunque se $H \subseteq A_4$ fosse un sottogruppo di ordine 6, avendo indice 2 sarebbe normale. Dunque A_4/H sarebbe un gruppo di ordine 2. Allora $\overline{\sigma}^2 = e$ per ogni $\sigma \in A_4$, cioè

$$\sigma^2 \in H \quad \forall\, \sigma \in A_4.$$

Per quanto precedentemente dimostrato, ogni 3-ciclo di S_4 sta in A_4; e poiché se σ è un 3-ciclo allora $\sigma = \sigma^4 = (\sigma^2)^2$, **ogni 3-ciclo è un quadrato**. Dunque ogni 3-ciclo starebbe in H. In S_4 ci sono 8 3-cicli: $(123), (124), (134), (234)$ e i loro quadrati; allora H dovrebbe avere ordine almeno 9 (contenendo i 3-cicli e l'elemento neutro), e ciò è una contraddizione.

Non c'è una formula risolutiva per equazioni di 5° grado

Évariste Galois
(Bourg-La-Reine, 25/10/1811 -
Parigi, 31/5/1832)

Il gruppo alternante

ESERCIZIO: Dimostrare che A_5 non ha sottogruppi normali non banali.

Prima di tutto, osserviamo che in A_5 stanno i seguenti elementi:

- I 5-cicli di S_5, che sono $4! = 24$; essi hanno periodo 5;
- I 3-cicli di S_5, che sono $\binom{5}{3}2 = 20$; essi hanno periodo 3;
- I prodotti di 2-cicli disgiunti di S_5, che sono $5 \cdot 2 = 10$; essi hanno periodo 2.

Inoltre $|A_5| = 120/2 = 60$, dunque per Lagrange gli ordini possibili per un sottogruppo $H \neq \{\mathrm{id}\}$ sono $2, 3, 4, 5, 6, 10, 12, 15, 20, 30$. Inoltre se H è normale si può formare il quoziente A_5/H ...

Il gruppo alternante

- $|H| = 30 \Rightarrow |A_5/H| = 2$. Dunque ogni quadrato starebbe in H: ma ogni 5-ciclo σ è un quadrato ($\sigma = (\sigma^3)^2$) e ogni 3-ciclo σ è un quadrato pure ($\sigma = (\sigma^2)^2$). Dunque tutti i 5-cicli e i 3-cicli dovrebbero stare in H, ma $24 + 20 > 30$.
- $|H| = 20 \Rightarrow |A_5/H| = 3$. Dunque ogni cubo starebbe in H: ma ogni 5-ciclo σ è un cubo ($\sigma = (\sigma^2)^3$). Dunque tutti i 5-cicli dovrebbero stare in H, ma $24 > 20$.
- $|H| = 15 \Rightarrow |A_5/H| = 4$. Dunque ogni quarta potenza starebbe in H: ma ogni 5-ciclo σ è una quarta potenza ($\sigma = (\sigma^4)^4$). Dunque tutti i 5-cicli dovrebbero stare in H, ma $24 > 15$.
- $|H| = 12 \Rightarrow |A_5/H| = 5$. Dunque ogni quinta potenza starebbe in H: ma ogni 3-ciclo σ è una quinta potenza ($\sigma = (\sigma^2)^5$). Dunque tutti i 3-cicli dovrebbero stare in H, ma $20 > 12$.
- $|H| = 10 \Rightarrow |A_5/H| = 6$. Dunque ogni sesta potenza starebbe in H: ma ogni 5-ciclo σ è una sesta potenza ($\sigma = \sigma^6$). Dunque tutti i 5-cicli dovrebbero stare in H, ma $24 > 10$.

Il gruppo alternante

- $|H| = 6 \Rightarrow |A_5/H| = 10$. Dunque ogni decima potenza starebbe in H: ma ogni 3-ciclo σ è una decima potenza ($\sigma = (\sigma^{10})$. Dunque tutti i 3-cicli e dovrebbero stare in H, ma $20 > 6$.
- $|H| = 5 \Rightarrow |A_5/H| = 12$. Dunque ogni dodicesima potenza starebbe in H: ma ogni 5-ciclo σ è una dodicesima potenza ($\sigma = (\sigma^3)^{12}$). Dunque tutti i 5-cicli dovrebbero stare in H, ma $24 > 5$.
- $|H| = 4 \Rightarrow |A_5/H| = 15$. Dunque ogni quindicesima potenza starebbe in H: ma ogni prodotto di 2-cicli disgiunti σ è una quindicesima potenza ($\sigma = \sigma^{15}$). Dunque tutti i prodotti di 2-cicli disgiunti dovrebbero stare in H, ma $10 > 4$.
- $|H| = 3 \Rightarrow |A_5/H| = 20$. Dunque ogni ventesima potenza starebbe in H: ma ogni 3-ciclo σ è una ventesima potenza ($\sigma = (\sigma^2)^{20}$). Dunque tutti i 3-cicli dovrebbero stare in H, ma $20 > 3$.
- $|H| = 2 \Rightarrow H = \mathrm{gp}(\sigma)$ dove σ è un prodotto di 2-cicli disgiunti. Non è restrittivo assumere $\sigma = (12)(34)$: poiché

$$(123)\sigma(132) = (14)(23) \notin H = \mathrm{gp}(\sigma)$$

allora H non è normale in A_4.

Finita generazione per gruppi Abeliani

Se G è un gruppo Abeliano generato da $g_1, \ldots, g_n$, allora esiste un omomorfismo surgettivo

$$\begin{array}{rcl} \phi : \mathbb{Z}^n & \to & G \\ (a_1, \ldots, a_n) & \mapsto & g_1^{a_1} \cdots g_n^{a_n} \end{array}$$

In particolare, G è numerabile. Quindi gruppi Abeliani come $\mathbb{R}$ o $\mathbb{C}$ certamente non sono finitamente generati. Esistono gruppi Abeliani di cardinalità numerabile che non sono finitamente generati?

Finita generazione per gruppi Abeliani

ESERCIZIO: Dimostrare che $\mathbb{Q}$ è un gruppo Abeliano non finitamente generato.

Siano $x_1, \ldots, x_n \in \mathbb{Q}$ e $G = \mathrm{gp}(x_1, \ldots, x_n)$. Vogliamo provare che $G \subsetneq \mathbb{Q}$. L'elemento tipico di G è $x = \sum_{i=1}^{n} m_i x_i$ con $m_i \in \mathbb{Z}$. Se

$$x_i = a_i/b_i \ : \ a_i \in \mathbb{Z}, b_i \in \mathbb{Z} \setminus \{0\}, \ i = 1, \ldots, n,$$

quindi, $x = \sum_{i=1}^{n} m_i a_i / b_i = a/(b_1 \cdots b_n)$ dove $a = m_1 a_1 b_2 \cdots b_n + \ldots$ Scegliendo un qualunque intero non nullo k che non divide $b_1 \cdots b_n$, certamente $1/k$ non può essere uguale a $a/(b_1 \cdots b_n)$ per nessun intero a, (altrimenti $ka = b_1 \cdots b_n$). Dunque $1/k \in \mathbb{Q} \setminus G$.

Finita generazione per gruppi Abeliani

ESERCIZIO: Dimostrare che $\mathbb{Q}^*$ è un gruppo Abeliano non finitamente generato.

Siano $x_1, \ldots, x_n \in \mathbb{Q}^*$ e $G = \mathrm{gp}(x_1, \ldots, x_n)$. Vogliamo provare che $G \subsetneq \mathbb{Q}^*$. L'elemento tipico di G è $x = \prod_{i=1}^n x_i^{m_i}$ con $m_i \in \mathbb{Z}$. Se

$$x_i = a_i/b_i \ : \ a_i, b_i \in \mathbb{Z} \setminus \{0\}, \ i = 1, \ldots, n,$$

quindi, $x = \dfrac{a_1^{m_1} \cdots a_n^{m_n}}{b_1^{m_1} \cdots b_n^{m_n}}$.
Scegliendo un numero primo p che non divide $a_1 \cdots a_n b_1 \cdots b_n$, certamente p non può essere uguale a x, (altrimenti, se $I = \{i : m_i < 0\}$ e $J = \{j : m_j \geq 0\}$, avremmo

$$p \cdot \prod_{i \in I} a_i^{-m_i} \cdot \prod_{j \in J} b_j^{m_j} = \prod_{j \in J} a_j^{m_j} \cdot \prod_{i \in I} b_i^{-m_i}).$$

Dunque $p \in \mathbb{Q}^* \setminus G$.

Anelli

Anelli e prime proprietà

ESERCIZIO: Quali fra le seguenti operazioni danno una struttura di anello a $\mathbb{Z}$? ($+$ e $\cdot$ indicano l'usuale somma e prodotto):

- $(\mathbb{Z}, +, \cdot)$: si, perché $(\mathbb{Z}, +)$ è un gruppo Abeliano, e per ogni $a, b, c \in \mathbb{Z}$ si ha $(ab)c = a(bc)$ e $a(b + c) = ab + ac$.
- $(\mathbb{Z}, +, *)$ dove $a * b = a \ \forall \ a, b \in \mathbb{Z}$: no, ad esempio

$$1 * 2 = 1 \neq 2 = 1 * 1 + 1 * 1.$$

- $(\mathbb{Z}, \cdot, +)$. No perché $(\mathbb{Z}, \cdot)$ non è un gruppo: infatti l'elemento neutro sarebbe 1, ma allora 2 non ha l'inverso.
- $(\mathbb{Z}, +, *)$ con $a * b = a^b$: no, ad esempio:

$$(2 * 2) * 3 = 4^3 = 64 \neq 256 = 2^8 = 2 * (2 * 3).$$

Anelli e prime proprietà

- $(\mathbb{Z}, +, *)$ dove, fissato $k \in \mathbb{Z}$, $a * b = kab \ \forall \ a, b \in \mathbb{Z}$: si, perché $(\mathbb{Z}, +)$ è un gruppo Abeliano, e per ogni $a, b, c \in \mathbb{Z}$

$$(a * b) * c = kab * c = k^2abc = a * kbc = a * (b * c)$$
$$a * (b + c) = ka(b + c) = kab + kac = a * b + a * c$$

- $(\mathbb{Z}, +, +)$. No, fallisce la proprietà distributiva:

$$1 + (1 + 1) = 3 \neq 4 = (1 + 1) + (1 + 1).$$

Anelli e prime proprietà

ESERCIZIO: Sia $(\mathbb{Z}, +, *)$ un anello. Dimostrare che $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ è univocamente determinato dal valore di $1 * 1$.

Sia $1 * 1 = k$; allora, per ogni $a \in \mathbb{Z}$, grazie alla distributività si ha:

$$1 * b = 1 * (1 + 1 + \ldots + 1) = 1 * 1 + 1 * 1 + \ldots + 1 * 1 = bk.$$

Dato $a \in \mathbb{Z}$, dunque:

$$a * b = (1 + 1 + \ldots + 1) * b = 1 * b + 1 * b + \ldots + 1 * b = abk = kab.$$

Per quanto detto precedentemente, possiamo quindi concludere che i seguenti fatti sono equivalenti:

- $(\mathbb{Z}, +, *)$ un anello.
- Esiste $k \in \mathbb{Z}$ tale che $a * b = kab \quad \forall \quad a, b \in \mathbb{Z}$.

Inoltre $(\mathbb{Z}, +, *)$ è un anello unitario $\Leftrightarrow$ $k = \pm 1$ (verificare x casa).

Anelli e prime proprietà

ESERCIZIO: Sia A un anello commutativo e unitario e $a, b \in A$. Provare o confutare:

- *Se a è invertibile, allora ab è invertibile*. No, per esempio se $b = 0$ $ab = 0$ non è invertibile.
- *Se a è invertibile e $b \neq 0$, allora ab è invertibile*. No, per esempio se $A = \mathbb{Z}$, $a = 1$ e $b = 2$ allora $ab = 2$ non è invertibile.
- *Se a e b sono invertibili, allora ab è invertibile*. Si, perché $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aa^{-1} = 1$.
- *Se a è 0-divisore, allora ab è 0-divisore*. Si, infatti se $0 \neq c \in A$ è tale che $ac = 0$, allora $abc = acb = 0$.
- *Se a è nilpotente, allora ab è nilpotente*. Si, infatti se $n \in \mathbb{N}$ è tale che $a^n = 0$, allora $(ab)^n = a^n b^n = 0$.

Anelli e prime proprietà

- *Se a e b sono invertibili, allora $a+b$ è invertibile*. No, per esempio se $A=\mathbb{Z}$ e $a=b=1$, allora $a+b=2$ non è invertibile.
- *Se a e b sono 0-divisori, allora $a+b$ è uno 0-divisore*. No, per esempio se $A=\mathbb{Z}_6$, $a=\overline{4}$ e $b=\overline{3}$ allora $a+b=\overline{1}$ non è 0-divisore.
- *Se a e b sono nilpotenti, allora $a+b$ è nilpotente*. Si, infatti siano $m,n\in\mathbb{N}$ tali che $a^m=b^n=0$: allora

$$(a+b)^{m+n}=\sum_{i=0}^{m+n}\binom{m+n}{i}a^i b^{m+n-i}$$

$$=\sum_{i=0}^{m}\binom{m+n}{i}a^i b^n b^{m-i}+\sum_{i=m+1}^{m+n}\binom{m+n}{i}a^m a^{i-m}b^{m+n-i}$$

$$=\sum_{i=0}^{m}\binom{m+n}{i}a^i 0 b^{m-i}+\sum_{i=1}^{n}\binom{m+n}{i}0a^{i-m}b^{m+n-i}=0$$

Anelli e prime proprietà

ESERCIZIO: Provare o confutare:

(i) *Un sottoanello di un campo è un campo*. No, per esempio $\mathbb{Z}$, che non è un campo, è un sottoanello del campo $\mathbb{Q}$.

(ii) *Un sottoanello A di un dominio R è un dominio*. Si, perché $0_A = 0_R$. Quindi dati $a, b \in A \subseteq R$

$$a \neq 0_A, b \neq 0_A \Rightarrow a \neq 0_R, b \neq 0_R \Rightarrow ab \neq 0_R \Rightarrow ab \neq 0_A.$$

(iii) *Un sottoanello di un anello unitario è unitario*. No, ad esempio $2\mathbb{Z}$, che non è unitario, è un sottoanello dell'anello unitario $\mathbb{Z}$.

(iv) *Un sottoanello A di un anello ridotto R è ridotto*. Si, il ragionamento è analogo a quello fatto in (ii) perché $0_A = 0_R$.

(v) *Un sottoanello A di un anello commutativo R è commutativo*. Si, perchè la moltiplicazione in A è la stessa di quella in R.

Anelli e prime proprietà

(vi) *Se A è un sottoanello unitario di un anello unitario R, allora $1_A = 1_R$.* No, per esempio si consideri $R = \mathbb{Z}_6$, che è unitario con unità $\overline{1}$. Il sottoinsieme $A = \{\overline{0}, \overline{3}\}$ è un sottoanello unitario, ma $1_A = \overline{3}$.

(vii) *Se $\{0\} \neq A$ è un sottoanello unitario di un dominio unitario R, allora $1_A = 1_R$.* Si: sia $a \neq 0$ un elemento di A; $1_A a = a = 1_R a$, siccome R è un dominio, implica che $1_A = 1_R$.

(viii) *Se A è un sottoanello unitario di un anello unitario R, allora $U(A) = U(R) \cap A$.* No, si consideri lo stesso esempio in (vi).

(ix) *Se A è un sottoanello unitario di un anello unitario R tale che $1_A = 1_R$, allora $U(A) = U(R) \cap A$.* No, per esempio siano $A = \mathbb{Z}$ e $R = \mathbb{Q}$. Allora $U(A) = \{\pm 1\}$, $U(R) = \mathbb{Q}^*$ e $U(R) \cap A = \mathbb{Z}^*$.

(x) *Se R non è un campo ogni suo sottoanello non è un campo.* No, nell'esempio (vi) R non è un campo, ma A si.

Omomorfismi

ESERCIZIO: Quali fra i seguenti sono omomorfismi di anelli:

(i) $f : \mathbb{Z} \to \mathbb{Z}$ *definito da* $f(n) = 3n$. No, per esempio

$$f(1 \cdot 1) = f(1) = 3 \neq 9 = f(1) \cdot f(1).$$

(ii) $f : \mathbb{Z} \to \mathbb{R}$ *definito da* $f(n) = 2^n$. No, non è neppure un omomorfismo di gruppi:

$$f(0) = 1 \neq 0.$$

(iii) $f : M_{2,2}(\mathbb{R}) \to \mathbb{R}$ *definito da* $f(A) = \det(A)$. No, ad esempio siano

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & 0 \\ 0 & 1/2 \end{pmatrix}.$$

Allora $f(A) + f(B) = 1 - 1 = 0$ ma $f(A + B) = -3/2$.

Omomorfismi

(iv) $f : M_{2,2}(\mathbb{R}) \to \mathbb{R}$ *definito da* $f(A) = A_{1,1}$. No, ad esempio sia

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Allora $f(A)^2 = 0^2 = 0$ ma $f(A^2) = f(I_2) = 1$.

(v) $f : \mathbb{C} \to \mathbb{C}$ *definito da* $f(z) = \overline{z}$ *(coniugazione complessa)*. Si, perché $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ e $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

(vi) $f : \mathbb{R} \to \mathbb{C}$ *definito da* $f(x) = x + ix$. No, ad esempio $f(1^2) = f(1) = 1 + i \neq 2i = (1 + i)^2 = f(1)^2$.

(vii) $f : \mathbb{R} \to \mathbb{C}$ *definito da* $f(x) = ix$. No, ad esempio $f(1^2) = f(1) = i \neq -1 = i^2 = f(1)^2$.

(viii) $f : \mathbb{R} \to \mathbb{C}$ *definito da* $f(x) = x$. Si, perché $\mathbb{R}$ è un sottoanello di $\mathbb{C}$.

Omomorfismi

(ix) $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ *definito da* $f(\overline{x}) = 3\overline{x}$. Si, infatti f è un omomorfismo di gruppi e, per ogni $\overline{x}, \overline{y}$, si ha:

$$f(\overline{xy}) = 3\overline{xy} = 9\overline{xy} = f(\overline{x})f(\overline{y}).$$

(x) $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ *definito da* $f(\overline{x}) = 2\overline{x}$. No, ad esempio $f(\overline{1}^2) = f(\overline{1}) = \overline{2} \neq \overline{4} = f(\overline{1})^2$.

(xi) $f : \mathbb{Z}_2 \to \mathbb{Z}_6$ *definito da* $f(\overline{x}) = 3\overline{x}$. Si: per prima cosa bisogna vedere che f è ben definita: se $\overline{x} = \overline{y}$ in $\mathbb{Z}_2$ allora $x - y = 2n$ per qualche intero n; dunque $3x - 3y = 6n$, che implica $3\overline{x} = 3\overline{y}$ in $\mathbb{Z}_6$. Ora si procede come in (ix) per dire che f è omomorfismo di anelli.

Omomorfismi

ESERCIZIO: Siano A e B anelli, e $f : A \to B$ un omomorfismo di anelli. Provare o confutare:

(i) *Se A e B sono unitari, $f(1_A) = 1_B$.* No, per esempio si considerino $A = B = \mathbb{Z}_6$ e $f(\overline{x}) = 3\overline{x}$.

(ii) *Se A è unitario e f è surgettiva, allora B è unitario e $f(1_A) = 1_B$.* Si: dato $b \in B$, sia $a \in A$ tale che $f(a) = b$:

$$f(1_A)b = f(1_A)f(a) = f(1_A a) = f(a) = b.$$

Dunque B è unitario con elemento neutro $f(1_A)$.

Unità

ESERCIZIO: Sia A un anello, e $B \subseteq A$ un suo sottoanello tale che $1_B = 1_A$. Provare che:

- $U(B) \subseteq U(A)$:

$$b \in U(B) \Rightarrow \exists\ b' \in B : bb' = 1_B \underset{1_B = 1_A}{\Rightarrow}$$

$$\exists\ b' \in B : bb' = 1_A \underset{B \subseteq A}{\Rightarrow} \exists\ b' \in A : bb' = 1_A \Rightarrow b \in U(A).$$

- Se $U(A) \subseteq B$, allora $U(B) = U(A)$:

$$a \in U(A) \Rightarrow \exists\ a' \in A : aa' = 1_A \Rightarrow \exists\ a' \in U(A) : aa' = 1_A \underset{1_B = 1_A}{\Rightarrow}$$

$$\exists\ a' \in U(A) : aa' = 1_B \underset{U(A) \subseteq B}{\Rightarrow} \exists\ a' \in B : aa' = 1_B \Rightarrow a \in U(B).$$

- $b \in U(B) \Leftrightarrow b \in U(A)$ e $b^{-1} \in B$:

$$b \in U(B) \Leftrightarrow \exists\ b' \in B : bb' = 1_B \underset{1_B = 1_A}{\Leftrightarrow}$$

$$\exists\ b' \in B : bb' = 1_A \Leftrightarrow b \in U(A) \text{ e } b^{-1} = b' \in B.$$

Unità

ESERCIZIO: Siano A e B due anelli unitari, e $R = A \times B$ l'anello prodotto $((a,b)+(a',b') = (a+a', b+b')$ e $(a,b)(a',b') = (aa', bb'))$. Si provi:

(i) *R è unitario e* $1_R = (1_A, 1_B)$. Dato $r = (a,b) \in R$, si ha:

$$1_R r = (1_A a, 1_B b) = (a,b) = r.$$

(ii) $U(R) = U(A) \times U(B)$.

$$r = (a,b) \in U(R) \Leftrightarrow \exists\ r' = (a',b') \in R : rr' = 1_R$$
$$\Leftrightarrow (aa', bb') = (1_A, 1_B) \Leftrightarrow r = (a,b) \in U(A) \times U(B)$$

Unità

ESERCIZIO: Siano A e B due anelli unitari isomorfi tra loro (come anelli). Allora $U(A)$ e $U(B)$ sono isomorfi tra loro (come gruppi).

Sia $f : A \to B$ un isomorfismo di anelli. Allora, essendo f surgettivo, $f(1_A) = 1_B$. Sia $a \in U(A)$, e $a' \in A$ tale che $aa' = 1_A$:

$$f(a)f(a') = f(aa') = f(1_A) = 1_B.$$

Quindi $f(a) \in U(B)$. Dunque $f(U(A)) \subseteq U(B)$. Considerando l'inversa di f, allo stesso modo $f^{-1}(U(B)) \subseteq U(A)$, cioè (essendo f bigettiva) $U(B) \subseteq f(U(A))$. Quindi

$$f|_{U(A)} : U(A) \to U(B)$$

è una funzione bigettiva, e poiché $f(a_1a_2) = f(a_1)f(a_2)$ per ogni $a_1, a_2 \in U(A)$, $f|_{U(A)}$ è un isomorfismo di gruppi.

Unità

ESERCIZIO: Dato $n \in \mathbb{Z}$, si consideri la funzione di Eulero

$$\phi(n) = |U(\mathbb{Z}_n)| = |\{a \in \mathbb{N} : 1 \leq a < n : \mathrm{MCD}(a, n) = 1\}|.$$

Si dimostri che, se $\mathrm{MCD}(m, n) = 1$, *allora* $\phi(mn) = \phi(m)\phi(n)$.

Si consideri la funzione $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ definita come $f(a) = (\overline{a}, \overline{a})$: f è un omomorfismo di anelli, infatti:

- $f(a + b) = (\overline{a + b}, \overline{a + b}) = (\overline{a}, \overline{a}) + (\overline{b}, \overline{b}) = f(a) + f(b)$;
- $f(ab) = (\overline{ab}, \overline{ab}) = (\overline{a}, \overline{a}) \cdot (\overline{b}, \overline{b}) = f(a) \cdot f(b)$;

Siccome $\mathrm{MCD}(m, n) = 1$, f è surgettivo, inoltre $\mathrm{Ker}(f) = (mn)$. Infatti:

$$f(a) = 0 \Leftrightarrow (\overline{a}, \overline{a}) = 0 \text{ in } \mathbb{Z}_m \times \mathbb{Z}_n \Leftrightarrow m|a \text{ e } n|a \Leftrightarrow mn = \mathrm{mcm}(m, n)|a.$$

Per il I teorema di isomorfismo per anelli, quindi, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ come anelli. Dunque $U(\mathbb{Z}_{mn}) \cong U(\mathbb{Z}_m \times \mathbb{Z}_n)$ come gruppi. Essendo $U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$, si ha che

$$\phi(mn) = \phi(m)\phi(n)$$

L'anello delle serie formali

Dato un anello A, sia $A[[x]]$ l'insieme delle *serie formali a coefficienti in A*:

$$\sum_{n\in\mathbb{N}} a_n x^n.$$

Considerando somma e prodotto così definiti:

- se $f = \sum_{n\in\mathbb{N}} a_n x^n \in A[[x]]$ e $g = \sum_{n\in\mathbb{N}} b_n x^n \in A[[x]]$:

$$f + g = \sum_{n\in\mathbb{N}} (a_n + b_n) x^n \in A[[x]].$$

- se $f = \sum_{n\in\mathbb{N}} a_n x^n \in A[[x]]$ e $g = \sum_{n\in\mathbb{N}} b_n x^n \in A[[x]]$:

$$f \cdot g = \sum_{n\in\mathbb{N}} \sum_{\substack{i,j\in\mathbb{N} \\ i+j=n}} (a_i b_j) x^n \in A[[x]].$$

È facile verificare che $(A[[x]], +, \cdot)$ è un anello. Inoltre A è un sottoanello di $A[[x]]$. L'anello $A[[x]]$ è l' anello delle serie formali a coefficienti in A.

L'anello delle serie formali

ESERCIZIO: sia A un anello commutativo e unitario. Provare che:

- $A[[x]]$ *è commutativo e unitario, con* $1_{A[[x]]} = 1_A$: siano $f = \sum_{n\in\mathbb{N}} a_n x^n \in A[[x]]$ e $g = \sum_{n\in\mathbb{N}} b_n x^n \in A[[x]]$:

$$f \cdot g = \sum_{n\in\mathbb{N}} \sum_{\substack{i,j\in\mathbb{N} \\ i+j=n}} (a_i b_j) x^n = \sum_{n\in\mathbb{N}} \sum_{\substack{i,j\in\mathbb{N} \\ i+j=n}} (b_j a_i) x^n = g \cdot f,$$

$$1_A \cdot f = \sum_{n\in\mathbb{N}} 1_A a_n x^n = \sum_{n\in\mathbb{N}} a_n x^n = f.$$

- $1 - x$ *è un'unità di* $A[[x]]$. Se $f = \sum_{n\in\mathbb{N}} a_n x^n = \sum_{n\in\mathbb{N}} x^n \in A[[x]]$:

$$(1-x)\cdot f = 1 + \sum_{n\in\mathbb{N}\setminus\{0\}} (a_n - a_{n-1}) x^n = 1 + \sum_{n\in\mathbb{N}\setminus\{0\}} (1-1) x^n = 1 + 0 = 1.$$

L'anello delle serie formali

- *Provare che* $f = \sum_{n\in\mathbb{N}} a_n x^n \in U(A[[x]]) \Leftrightarrow a_0 \in U(A)$.
  - "$\Rightarrow$": sia $g = \sum_{n\in\mathbb{N}} b_n x^n \in A[[x]]$ tale che $f \cdot g = 1_{A[[x]]} = 1_A$. Allora $a_0 b_0 = 1_A$, cioè $a_0 \in U(A)$.
  - "$\Leftarrow$": siccome $a_0 \in U(A) \subseteq U(A[[x]])$,

$$f \in U(A[[x]]) \Leftrightarrow a_0^{-1} \cdot f \in U(A[[x]]).$$

Dunque possiamo supporre che $f = 1 - gx$, dove $g = \sum_{n\in\mathbb{N}} -a_{n+1}x^n$. Sia $h = \sum_{n\in\mathbb{N}} g^n x^n$. Allora

$$f \cdot h = 1 + \sum_{n\in\mathbb{N}\setminus\{0\}} (g^n - g g^{n-1})x^n = 1 + 0 = 1.$$

ATTENZIONE: a priori h potrebbe non stare in $A[[x]]$, perché un anello non è chiuso per somme infinite .....

L'anello delle serie formali

ESEMPIO. Si consideri $\mathbb{Q}[[x]]$: $1/n^2 \in \mathbb{Q}[[x]]$ per ogni $n \in \mathbb{N} \setminus \{0\}$, ma

$$\sum_{n \in \mathbb{N} \setminus \{0\}} 1/n^2 = \pi^2/6 \notin \mathbb{Q}[[x]].$$

Però $\sum_{n \in \mathbb{N} \setminus \{0\}} (1/n^2) x^n \in \mathbb{Q}[[x]]$ .....

In generale, se $f_n = \sum_{i \in \mathbb{N}} a_{i,n} x^i \in A[[x]]$, allora

$$\sum_{n \in \mathbb{N}} f_n x^n = \sum_{n \in \mathbb{N}} b_n x^n, \qquad \text{dove} \quad b_n = \sum_{i=0}^{n} a_{i,n-i} \in A.$$

sta in $A[[x]]$. Quindi nella precedente slide $h = \sum_{n \in \mathbb{N}} g^n x^n \in A[[x]]$.

L'anello delle serie formali

ESERCIZIO: sia A un anello commutativo e unitario. Provare che:

- *L'insieme* $\{f = \sum_{n\in\mathbb{N}\setminus\{0\}} a_n x^n : a_n \in A\}$ *è l'ideale di* $A[[x]]$ *generato da* x: Si ha che

$$(x) = \{x \cdot g : g = \sum_{n\in\mathbb{N}} b_n x^n \in A[[x]]\} =$$

$$\left\{\sum_{n\in\mathbb{N}} b_n x^{n+1} : b_n \in A\right\} \underset{a_n = b_{n-1}}{=} \left\{\sum_{n\in\mathbb{N}\setminus\{0\}} a_n x^n : a_n \in A\right\}$$

- $A[[x]]/(x) \cong A$: si consideri la funzione $\phi : A[[x]] \to A$ definita da $\sum_{n\in\mathbb{N}} a_n x^n \mapsto a_0$. Siano $f = \sum_{n\in\mathbb{N}} a_n x^n$ e $g = \sum_{n\in\mathbb{N}} b_n x^n$:

$$\phi(f+g) = \phi(\sum_{n\in\mathbb{N}}(a_n + b_n)x^n) = a_0 + b_0 = \phi(f) + \phi(g),$$

$$\phi(f \cdot g) = \phi(\sum_{n\in\mathbb{N}} \sum_{\substack{i,j\in\mathbb{N} \\ i+j=n}} (a_i b_j)x^n) = a_0 b_0 = \phi(f)\phi(g)$$

L'anello delle serie formali

- Quindi $\phi : A[[x]] \to A$ è un omomorfismo di anelli, ovviamente è surgettivo, e $\mathrm{Ker}(\phi) = (x)$. Quindi $A[[x]]/(x) \cong A$.
- (x) *è un ideale primo (massimale) di* $A[[x]]$ *se e solo se* A *è un dominio (campo)*: segue dal fatto che $A[[x]]/(x) \cong A$ e dalla caratterizzazione di ideali primi e massimali.
- *se* $A = K$ *è un campo, allora* (x) *è l'unico ideale massimale di* $K[[x]]$. Per assurdo sia $I \subseteq K[[x]]$ un ideale massimale diverso da (x). Si consideri $f \in I \setminus (x)$: allora $f = \sum_{n\in\mathbb{N}} a_n x^n$ con $a_0 \neq 0$, quindi $f \in U(K[[x]])$, dunque $I = K[[x]]$, contraddicendo il fatto che I è massimale.

Un anello commutativo e unitario con un unico ideale massimale si dice anello locale.

Vari

ESERCIZIO: Sia $A = \left\{ X \in M_2(\mathbb{R}) : X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a \in \mathbb{Q} \text{ e } c \in \mathbb{Z} \right\}$.

a) *Provare che A è un sottoanello di $M_2(\mathbb{R})$.* (Facile).

b) *A è commutativo? Unitario?* A non è commutativo, ad esempio:

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 4 & 5 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Ovviamente A è unitario, poiché $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$.

c) *$U(A)$ è Abeliano? Finito? Ci sono elementi di periodo 2 e/o 3?* Sia $X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in A$. Si noti che

$$X \in U(A) \Leftrightarrow X \in U(M_2(\mathbb{R})) \text{ e } X^{-1} \in A.$$

Allora $X \in U(A) \Leftrightarrow ac \neq 0$ e $\begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix} \in A$. Quindi

$$U(A) = \left\{ X \in M_2(\mathbb{R}) : X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a \in \mathbb{Q}^*, c = \pm 1 \right\}.$$

Vari

c) Quindi $U(A)$ non è Abeliano né finito. Ovviamente $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in U(A)$ ha periodo 2. Per provare che non ce ne sono di periodo 3, ad esempio si osservi che $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^3 = \begin{pmatrix} a^3 & * \\ 0 & c^3 \end{pmatrix}$, quindi se $X^3 = I_2$ per $X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ allora $a = c = 1$. Ma se

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3b \\ 0 & 1 \end{pmatrix} = I_2,$$

allora $b = 0$, quindi $X = I_2$ avrebbe periodo 1.

c) *Provare che A contiene un sottoanello isomorfo a* $\mathbb{Q} \times \mathbb{Z}$. Sia $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a \in \mathbb{Q}, c \in \mathbb{Z} \right\} \subseteq A$. È semplice vedere che la funzione $f : B \to \mathbb{Q} \times \mathbb{Z}$ definita da $\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mapsto (a, c)$ è un isomorfismo di anelli.

Vari

ESERCIZIO: Dato un anello A (non necessariamente commutativo né unitario) e $m > 1$ un numero naturale, provare che

$$\forall \ \ 0 \neq a \in A, \ \ a^m \neq 0 \Rightarrow A \text{ è ridotto.}$$

In particolare, $\forall \ \ 0 \neq a \in A, \ \ a^2 \neq 0 \Rightarrow A$ è ridotto.

Sia $0 \neq a \in A$. Innanzitutto vogliamo provare che $a^{m^k} \neq 0$ per ogni $k \in \mathbb{N}$. Per $k = 0$ è ovvio, e per $k = 1$ è vero per ipotesi. Quindi facciamo un' induzione su k. Se $k > 1$, $b = a^{m^{k-1}}$ è un elemento di A diverso da 0 per induzione. Dunque $b^m \neq 0$ per ipotesi. Quindi

$$a^{m^k} = a^{m^{k-1}m} = b^m \neq 0.$$

Adesso, sia $x \in A$, e $n \in \mathbb{N}$ tale che $x^n = 0$. Sia $k \in \mathbb{N}$ tale che $m^k \geq n$, e sia $s = m^k - n \in \mathbb{N}$. Allora

$$x^{m^k} = x^n x^s = 0x^s = 0.$$

Per quanto detto prima, allora $x = 0$. Cioè A è ridotto.

Vari

ESERCIZIO: Sta $A \subseteq M_2(\mathbb{Z})$ l'insieme delle matrici

$$\begin{pmatrix} a+b & b \\ 0 & a \end{pmatrix}, \ a, b \in \mathbb{Z}$$

- *Provare che A è un sottoanello commutativo di $M_2(\mathbb{Z})$.* Siano $X = \begin{pmatrix} a+b & b \\ 0 & a \end{pmatrix}$ e $Y = \begin{pmatrix} c+d & d \\ 0 & c \end{pmatrix}$:

$$X - Y = \begin{pmatrix} (a-c)+(b-d) & b-d \\ 0 & a-c \end{pmatrix} \Rightarrow A \text{ sottogruppo di } M_2(\mathbb{Z}) \ +$$

$$XY = \begin{pmatrix} ac+(ad+bc+bd) & ad+bc+bd \\ 0 & ac \end{pmatrix} = YX \Rightarrow A \text{ sottoanello commutativo di } M_2(\mathbb{Z})$$

- *A è un dominio?* No, ad esempio $\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- *A è ridotto?* Si, infatti

$$\begin{pmatrix} a+b & b \\ 0 & a \end{pmatrix}^2 = \begin{pmatrix} (a+b)^2 & 2ab+b^2 \\ 0 & a^2 \end{pmatrix} = 0 \Rightarrow \begin{pmatrix} a+b & b \\ 0 & a \end{pmatrix} = 0$$

Vari

ESERCIZIO: Sia G un gruppo, e H un suo sottogruppo normale. Dimostrare che, se G/H è Abeliano, allora ogni sottogruppo $K \subseteq G$ contenente H è normale.

Dobbiamo dimostrare che $\forall\ x \in K,\ g \in G \Rightarrow g^{-1}xg \in K$:

- se $x \in H$ allora $g^{-1}xg \in H \subseteq K$ ✓;
- altrimenti, in G/H abbiamo

$$\overline{g^{-1}xg} = \overline{g}^{-1}\overline{xg} \underset{G/H \text{ Abeliano}}{=} \overline{g}^{-1}\overline{gx} = \overline{x},$$

cioè $g^{-1}xgx^{-1} \in H$; allora $g^{-1}xg \in Hx \subseteq K$ ✓.

Vari

Sia $G \subseteq \mathrm{GL}_3(\mathbb{Z})$ il sottogruppo formato dagli elementi del tipo

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b, c \in \mathbb{Z}_3.$$

ESERCIZIO: *Provare che G è un gruppo non Abeliano di ordine 27.* Chiaramente $|G| = 27$; per vedere che non è Abeliano siano

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Allora $AB = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, mentre $BA = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ ...

Vari

Provare che $A^3 = I_3 \quad \forall A \in G$.

- $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$;
- $A^2 = \begin{pmatrix} 1 & 2a & b + ac + b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$;
- $A^3 = \begin{pmatrix} 1 & 3a & b + 2ac + b + ac + b \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = I_3$.

(quindi G è un gruppo non Abeliano in cui ogni elemento diverso dall'identità ha periodo 3, mentre ricordiamo che se tutti gli elementi di un gruppo hanno periodo 2 allora il gruppo deve essere Abeliano) ...

Vari

Si può vedere che $Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_3 \right\}$. *Provare che* $G/Z(G) \cong \mathbb{Z}_3^2$. Si consideri la funzione $\phi : G \to \mathbb{Z}_3^2$ definita da:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a, c).$$

Poiché $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a'+a & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix}$, ϕ è un omomorfismo. Chiaramente ϕ è surgettivo e il nucleo di ϕ è $Z(G)$, dunque $G/Z(G) \cong \mathbb{Z}_3^2$.

Vari

ESERCIZIO: Sia G un gruppo finito di ordine pari. Provare che esiste $g \in G$ di periodo 2.

Per assurdo, $g \neq g^{-1}\ \forall\ g \in G \setminus \{e\}$; allora

$$\bigcup_{g \in G \setminus \{e\}} \{g, g^{-1}\}$$

dovrebbe avere cardinalità pari, ma questo contraddice il fatto che $G \setminus \{e\}$ ha cardinalità dispari.

Vari

ESERCIZIO: Sia G un gruppo Abeliano, e $T(G)$ l'insieme degli elementi di G di periodo finito.

(a) *Provare che $T(G)$ è un sottogruppo di G*:

- $g \in T(G) \Rightarrow \exists\, n \in \mathbb{N} \setminus \{0\} : g^n = e \Rightarrow g^{-1} = g^{n-1} \Rightarrow (g^{-1})^n = (g^{n-1})^n = (g^n)^{n-1} = e^{n-1} = e \Rightarrow g^{-1} \in T(G)$;
- $g, h \in T(G) \Rightarrow \exists\, m, n \in \mathbb{N} \setminus \{0\} : g^m = e = h^n \Rightarrow g^{mn} = h^{mn} = e \Rightarrow (gh)^{mn} \underset{G \text{ Abeliano}}{=} g^{mn} h^{mn} = e \Rightarrow gh \in T(G)$.

(b) *Verificare che $T(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$*: Sia $g \in T(\mathbb{R}/\mathbb{Z})$, e $x \in \mathbb{R}$ un rappresentante della classe di g:

$$g \in T(\mathbb{R}/\mathbb{Z}) \Leftrightarrow \exists\, n \in \mathbb{N} \setminus \{0\} : ng = 0 \Leftrightarrow nx \in \mathbb{Z}$$
$$\Leftrightarrow \exists\, m \in \mathbb{Z} : nx = m \Leftrightarrow x = m/n \in \mathbb{Q} \Leftrightarrow g \in \mathbb{Q}/\mathbb{Z}.$$

Vari

ESERCIZIO: Sia G il sottogruppo di $\mathbb{C}^*$ generato da 2 e $1+i$.

(a) *Determinare $H \subseteq \mathbb{Z}^2$ tale che $G \cong \mathbb{Z}^2/H$.*

Siccome G è un gruppo Abeliano generato da 2 elementi, c'è un omomorfismo surgettivo di gruppi $f : \mathbb{Z}^2 \to G$:

$$f(m,n) = 2^m(i+1)^n.$$

Quindi per il I teorema di isomorfismo $G \cong \mathbb{Z}^2/\operatorname{Ker}(f)$, dunque $H = \operatorname{Ker}(f)$. Allora determiniamo $\operatorname{Ker}(f)$: $(m,n) \in \operatorname{Ker}(f) \Leftrightarrow (1+i)^n = 2^{-m}$. Scrivendo $1+i = \sqrt{2}(\cos \pi/4 + i \sin \pi/4)$,

$$(\sqrt{2})^n(\cos n\pi/4 + i \sin n\pi/4) = 2^{-m} \Leftrightarrow n = 8k \text{ e } m = -4k.$$

Quindi $H = \operatorname{gp}((-4,8))$.

Vari

(b) *Determinare* $T(G)$. Sfruttando l'isomorfismo $\overline{f} : \mathbb{Z}^2/H \to G$, $2^m(1+i)^n \in T(G) \Leftrightarrow (\overline{m}, \overline{n}) \in T(\mathbb{Z}^2/H) \Leftrightarrow k \cdot (m,n) \in H$ per qualche $k \in \mathbb{N} \setminus \{0\}$. Siccome $H = \mathrm{gp}((-4,8))$, quindi, devono esistere $h \in \mathbb{Z}, k \in \mathbb{N} \setminus \{0\}$ tali che

$$\begin{cases} km = -4h \\ kn = 8h \end{cases}$$

che è possibile se e solo se $n = -2m$. Allora

$$T(G) = \{2^m(1+i)^{-2m} : m \in \mathbb{Z}\} = \{1, i, -1, -i\}.$$

Vari

ESERCIZIO: Sia $Y = \{1, 2, \ldots, n\}$, X l'insieme delle parti di Y e $\rho : S_n \times X \to X$ l'applicazione definita come:

$$(\sigma, A) \mapsto \sigma \cdot A := \sigma(A) \ (= \{\sigma(i) : i \in A\}).$$

- *Dimostrare che ρ è un'azione*:
  - $\forall\ A \in X,\ \mathrm{id} \cdot A = \mathrm{id}(A) = A$;
  - $\forall\ \sigma, \tau \in S_n,\ A \in X,\ (\sigma\tau) \cdot A = \sigma\tau(A) = \sigma(\tau(A)) = \sigma \cdot (\tau \cdot A)$.
- *Calcolare una decomposizione di X in orbite*: Se $A \in X$ ha cardinalità k, $|\sigma(A)| = k$. Dunque $O_A \subseteq \{B \in X : |B| = k\}$. Per provare che questa è effettivamente un'uguaglianza, si scrivano $A = \{a_1, \ldots, a_k\}$ e $B = \{b_1, \ldots, b_k\}$, e si definisca, per esempio, $\sigma \in S_n$ come segue:

$$\sigma(i) = \begin{cases} i & \text{se } i \notin A \cup B \\ b_j & \text{se } i = a_j \\ a_j & \text{se } i = b_j \end{cases}$$

Vari

- ... Quindi, la decomposizione di X in orbite è la seguente:

$$X = O_{\emptyset} \cup O_{\{1\}} \cup O_{\{1,2\}} \ldots \cup O_{\{1,\ldots,n\}}.$$

- *Calcolare i gruppi di isotropia e i loro ordini*. Per $A \in X$, il gruppo di isotropia di A è

$$C_A = \{\sigma \in S_n : \sigma(A) = A\}.$$

Poiché $|C_A||O_A| = n!$, $|A| = k \Rightarrow |C_A| = \dfrac{n!}{\binom{n}{k}} = k!(n-k)!$.

Vari

ESERCIZIO: In S_7, si consideri la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 5 & 2 & 4 & 1 \end{pmatrix}.$$

- σ *sta in* A_7*?* Scrivendo σ come prodotto di cicli disgiunti, si ha

  $$\sigma = (137)(2645).$$

  Quindi $\sigma \notin A_7$ perché $(3-1)+(4-1) = 5$ è dispari.
- *Esiste un 2-ciclo* (ij) *tale che* $A_7 \cdot \sigma = A_7 \cdot (ij)$*?* Si, perchè A_7 ha indice 2 in S_7, dunque ha solo 2 classi laterali, A_7 e un altro insieme B. Siccome né σ né (ij) sta in A_7, allora $A_7 \cdot \sigma = A_7 \cdot (ij) = B$ (quindi qualunque 2-ciclo va bene).
- Sia $G = \mathrm{gp}(\sigma)$. *Esiste un omomorfismo non banale* $\phi : G \to \mathbb{Z}_7$*?* No, poiché $\pi(\phi(g))$ deve dividere $\pi(g) = 12$, ma in $\mathbb{Z}_7$ tutti gli elementi non banali hanno periodo 7.

Vari

ESERCIZIO: Sia G un gruppo tale che $G/Z(G)$ è ciclico. Provare che G è Abeliano.

Sia $g \in G$ tale che $G/Z(G) = \mathrm{gp}(\overline{g})$. Per ogni $x, y \in G$, esistono interi m, n tali che, in $G/Z(G)$,

$$\overline{x} = \overline{g}^{-m} \quad \text{e} \quad \overline{y} = \overline{g}^{-n}.$$

Dunque $xg^m \in Z(G)$ e $yg^n \in Z(G)$. Allora

$$xyg^{n+m} = xyg^n g^m = xg^m yg^n = yxg^m g^n = yxg^{m+n} = yxg^{n+m}$$

Concludiamo perché $(xy)g^{n+m} = (yx)g^{n+m} \Rightarrow xy = yx$.

Vari

ESERCIZIO: Sia $D_4 = \langle \tau, \sigma : \tau^2 = \sigma^4 = e,\ \tau\sigma = \sigma^3\tau \rangle$ il gruppo diedrale. Calcolare il centro di D_4.

Immergendo D_4 in S_4, possiamo assumere che $\sigma = (1234)$ e $\tau = (13)$. Gli elementi di D_4 (in questa immersione) sono:

- id;
- $\tau, \tau\sigma = (12)(34), \tau\sigma^2 = (24), \tau\sigma^3 = (14)(23), \sigma^2 = (13)(24)$;
- $\sigma, \sigma^3 = (1432)$.

Osserviamo che $\sigma^2 \in Z(D_4)$: infatti

$$(13)(13)(24) = (24) = (13)(24)(13)$$
$$(12)(34)(13)(24) = (14)(23) = (13)(24)(12)(34)$$
$$(24)(13)(24) = (13) = (13)(24)(24)$$
$$(14)(23)(13)(24) = (12)(34) = (13)(24)(14)(23)$$

Vari

Dunque $\mathrm{gp}(\tau^2) \subseteq Z(D_4)$. Tale inclusione è un'uguaglianza, altrimenti $|Z(D_4)| = 4$ e $D_4/Z(D_4)$, avendo ordine 2, sarebbe ciclico; questo contraddirrebbe il fatto che D_4 non è Abeliano. Quindi $\mathrm{gp}(\tau^2) = Z(D_4)$.

Provare che $D_4/Z(D_4) \cong \mathbb{Z}_2^2$. Basta osservare che $D_4/Z(D_4)$ ha ordine 4, e gli unici gruppi di ordine 4 sono $\mathbb{Z}_4$ e $\mathbb{Z}_2^2$. Ma $D_4/Z(D_4)$ non può essere ciclico perché D_4 non è Abeliano.

Ideali

ESERCIZIO: Sia A un anello commutativo unitario. Provare o confutare:

(i) *L'intersezione di ideali è un ideale.* Si, sia $\{I_i\}_{i\in U}$ una famiglia di ideali di A e $J = \bigcap_{i\in U} I_i$:

- $x, y \in J \Rightarrow x, y \in I_i \ \forall\ i \Rightarrow x + y \in I_i \ \forall\ i \Rightarrow x + y \in J$;
- $a \in A, x \in J \Rightarrow x \in I_i \ \forall\ i \Rightarrow ax \in I_i \ \forall\ i \Rightarrow ax \in J$.

(ii) *L'intersezione di ideali primi è un ideale primo.* No, ad esempio si considerino gli ideali primi (2) e (3) di $\mathbb{Z}$: si ha

$$(2) \cap (3) = (6),$$

e (6) non è un ideale primo. Per verificare l'uguaglianza in verde:

- $(2) \supseteq (6)$ e $(3) \supseteq (6) \Rightarrow (2) \cap (3) \supseteq (6)$;
- sia $n \in (2) \cap (3)$: allora esistono $h, k \in \mathbb{Z}$ tali che $2h = n = 3k$; allora, grazie alla fattorizzazione unica, esiste $s \in \mathbb{Z}$ tale che $h = 3s$ e $k = 2s$. Dunque $n = 6s \in (6)$, cioè $(2) \cap (3) \subseteq (6)$.

(iii) *L'intersezione di ideali radicali è un ideale radicale.* Si, sia $\{I_i\}_{i\in U}$ una famiglia di ideali radicali di A e $J = \bigcap_{i\in U} I_i$: se $x \in A, n \in \mathbb{N}$ è tale che $x^n \in J$, allora $x^n \in I_i \ \forall\ i$. Essendo ogni I_i è radicale, dunque $x \in I_i \ \forall\ i$; allora $x \in J$.

Ideali

ESERCIZIO: Sia A un anello commutativo unitario (ricordiamo che un ideale $I \subseteq A$ è proprio se $I \subsetneq A$, cioè se $1 \notin I$). Provare le seguenti:

(i) *Se $I \subseteq A$ è un ideale e $f \in A$, $\overline{f} \in A/I$ è invertibile se e solo se $I + (f)$ non è proprio*: $\overline{f} \in A/I$ è invertibile se e solo se esiste $g \in A$ tale che $\overline{f}\,\overline{g} = \overline{1}$ (in A/I) $\Leftrightarrow \exists\, g \in A : fg - 1 \in I \Leftrightarrow 1 \in I + (f)$.

(ii) *A è un campo se e solo se $\{0\}$ è il suo unico ideale proprio*.

- "$\Rightarrow$": sia I un ideale di A. Se $0 \neq x \in I$, poiché A è un campo, esiste $y \in A : xy = 1$; allora $1 \in I$. Quindi o $I = \{0\}$ o $I = A$.
- "$\Leftarrow$": sia $0 \neq x \in A$; poiché $(x) = A$, $1 \in (x)$. Cioè esiste $y \in A : xy = 1$. Quindi A è un campo.

Ideali

(iii) *A è un campo se e solo se $\{0\}$ è un ideale massimale*. Siccome $A \cong A/\{0\}$, A è un campo se e solo se $\{0\}$ è massimale.

(iv) *A è un dominio se e solo se $\{0\}$ è un ideale primo*. Siccome $A \cong A/\{0\}$, A è un dominio se e solo se $\{0\}$ è primo.

(v) *A è un anello ridotto se e solo se $\{0\}$ è un ideale radicale*. Siccome $A \cong A/\{0\}$, A è ridotto se e solo se $\{0\}$ è radicale.

Ideali

ESERCIZIO: Sia $\mathcal{F}$ l'anello delle funzioni da $\mathbb{R}$ in $\mathbb{R}$ con somma e moltiplicazione puntuali. Dato $f \in \mathcal{F}$, sia $\mathcal{Z}_f = \{x \in \mathbb{R} : f(x) = 0\} \subseteq \mathbb{R}$. Si provi che:

(i) $(f) = \{g \in \mathcal{F} : \mathcal{Z}_f \subseteq \mathcal{Z}_g\}$: sia $g \in \mathcal{F}$ tale che $\mathcal{Z}_f \subseteq \mathcal{Z}_g$, cioè $g(x) = 0$ per ogni $x \in \mathcal{Z}_f$, e si definisca $h \in \mathcal{F}$ come:

$$h(x) = \begin{cases} g(x)/f(x) & \text{se } x \notin \mathcal{Z}_f \\ 0 & \text{altrimenti} \end{cases}$$

Allora $g = fh \in (f)$. Quindi $\{g \in \mathcal{F} : \mathcal{Z}_f \subseteq \mathcal{Z}_g\} \subseteq (f)$. L'altra inclusione è chiara, perché $\forall\ h \in \mathcal{F}, \mathcal{Z}_f \subseteq \mathcal{Z}_{hf}$.

(ii) (f) *è proprio se e solo se* $\mathcal{Z}_f \neq \emptyset$. Abbiamo che $\{g \in \mathcal{F} : \mathcal{Z}_f \subseteq \mathcal{Z}_g\}$ è uguale a $\mathcal{F}$ se e solo se $\mathcal{Z}_f = \emptyset$, quindi si conclude da (i).

(iii) (f) *è primo se e solo se è massimale se e solo se* $|\mathcal{Z}_f| = 1$. Se $|\mathcal{Z}_f| > 1$, siano $x_1 \neq x_2$: $f(x_1) = f(x_2) = 0$, e si definiscano ...

Ideali

(iii) ... $g_1, g_2 \in \mathcal{F}$ come

$$g_1(x) = \begin{cases} f(x) & \text{se } x \neq x_1 \\ 1 & \text{se } x = x_1 \end{cases} \qquad g_2(x) = \begin{cases} 1 & \text{se } x \neq x_1 \\ 0 & \text{se } x = x_1 \end{cases}$$

Dunque, dato $x \in \mathbb{R}$, abbiamo:

- se $x \neq x_1$, $g_1(x) \cdot g_2(x) = f(x) \cdot 1 = f(x)$;
- se $x = x_1$, $g_1(x) \cdot g_2(x) = 1 \cdot 0 = 0 = f(x)$.

Dunque $f = g_1 g_2$, ma $g_1 \notin (f)$ poiché $x_1 \in \mathcal{Z}_f \setminus \mathcal{Z}_{g_1}$ e $g_2 \notin (f)$ poiché $x_2 \in \mathcal{Z}_f \setminus \mathcal{Z}_{g_2}$. Quindi (f) non è primo.

D'altra parte, se $|\mathcal{Z}_f| = 1$, sia $I \supsetneq (f)$ un ideale di $\mathcal{F}$. Allora esiste $g \in I$ tale che $\mathcal{Z}_f \not\subseteq \mathcal{Z}_g$, cioè tale che $\mathcal{Z}_f \cap \mathcal{Z}_g = \emptyset$ (siccome $|\mathcal{Z}_f| = 1$). Si noti che $|f| \in (f)$ (perché $\mathcal{Z}_{|f|} = \mathcal{Z}_f$) e $|g| \in (g)$ per la stessa ragione, quindi la funzione $h = |f| + |g|$ sta in $(f) + (g)$, dunque $h \in I$. Siccome $\mathcal{Z}_h = \emptyset$, si ha $\mathcal{F} = (h) \subseteq I$. Concludendo, I non è proprio, quindi (f) è massimale.

(iv) (f) è *radicale*. Siano $g \in \mathcal{F}, n \in \mathbb{N} : g^n \in (f)$; questo è il caso se e solo se $\mathcal{Z}_f \subseteq \mathcal{Z}_{g^n}$; poiché $\mathcal{Z}_g = \mathcal{Z}_{g^n}$, $g \in (f)$.

Ideali

(v) *Se $I \subseteq \mathcal{F}$ è un ideale finitamente generato, allora $I = (f)$ per qualche $f \in \mathcal{F}$.* Sia $I = (f_1, \dots, f_k)$. Poiché $\mathcal{Z}_{|f_i|} = \mathcal{Z}_{f_i}$, abbiamo che

$$|f_i| \in (f_i) \subseteq I.$$

Dunque $f := \sum_{i=1}^{k} |f_i| \in I$. Proviamo che $I = (f)$: poiché $f \in I$, ovviamente $(f) \subseteq I$. Per provare che $I \subseteq (f)$ basta provare che $f_i \in (f)\ \forall\ i = 1, \dots, k$. Questo è vero perché $\mathcal{Z}_f = \bigcap_{i=1}^{k} \mathcal{Z}_{f_i}$.

(vi) *Esistono ideali di $\mathcal{F}$ non principali?* Si: sia

$$I = \{f \in \mathcal{F} : \mathcal{Z}_f \supseteq [x, +\infty) \text{ per qualche } x \in \mathbb{R}\}.$$

È facile verificare che I è un ideale di $\mathcal{F}$. Per ogni $x \in \mathbb{R}$, si consideri la funzione f_x di $\mathcal{F}$ definita come:

$$f_x(y) = \begin{cases} 1 & \text{se } y < x \\ 0 & \text{se } y \geq x \end{cases}$$

Si noti che $\mathcal{Z}_{f_x} = [x, +\infty)$, dunque $f_x \in I$. Se esistesse $f \in \mathcal{F}$ tale che $I \subseteq (f)$, bisognerebbe avere che $\mathcal{Z}_f \subseteq \mathcal{Z}_{f_x} = [x, +\infty)$ per ogni $x \in \mathbb{R}$, cioè che $\mathcal{Z}_f = \emptyset$, cioè $(f) = \mathcal{F}$ ...

Ideali

(vi) ... Ma ciò è assurdo perché $\mathcal{Z}_1 \not\supseteq [x, +\infty)$ per alcun $x \in \mathbb{R}$, dunque $1 \notin I$. (In particolare, I non è finitamente generato).

(vii) *L'ideale I del punto precedente è massimale?* No: ad esempio, si coniderino

$$g_1(y) = \begin{cases} 0 & \text{se } y \geq 0 \text{ e } y \in \mathbb{Q} \\ 1 & \text{altrimenti} \end{cases} \qquad g_2(y) = \begin{cases} 0 & \text{se } y \geq 0 \text{ e } y \notin \mathbb{Q} \\ 1 & \text{altrimenti} \end{cases}$$

Si noti che $\mathcal{Z}_{g_1 g_2} = [0, +\infty)$, quindi $g_1 g_2 \in I$. ma $g_i \notin I$ poiché $\mathcal{Z}_{g_i} \not\supseteq [x, +\infty)$ per alcun $x \in \mathbb{R}$. Dunque I non è primo, e a maggior ragione neppure massimale.

D'ora in poi tutti gli anelli saranno commutativi e unitari.

Valutazioni

ESERCIZIO. Sia B un anello, e $A \subseteq B$ un sottoanello. Dato $b \in B$, si verifichi che la funzione $\mathrm{val}_b : A[x] \to B$ definita da

$$f = \sum_{i=0}^{n} a_i x^i \mapsto f(b) = \sum_{i=0}^{n} a_i b^i \in B$$

è un omomorfismo di anelli.

- $f, g \in A[x] \Rightarrow \mathrm{val}_b(f+g) = (f+g)(b) = f(b) + g(b) = \mathrm{val}_b(f) + \mathrm{val}_b(g)$;
- $f, g \in A[x] \Rightarrow \mathrm{val}_b(fg) = (fg)(b) = f(b)g(b) = \mathrm{val}_b(f)\,\mathrm{val}_b(g)$.

L'anello $\mathrm{Im}(\mathrm{val}_b)$ verrà denotato con $A[b]$.

Valutazioni

ESERCIZIO. Si consideri l'inclusione di anelli $\mathbb{Z} \subseteq \mathbb{C}$.

- *Provare che* $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$. Si consideri l'omomorfismo surgettivo $\mathrm{val}_i : \mathbb{Z}[x] \to \mathbb{Z}[i]$, e calcoliamone il nucleo:

$$f \in \mathbb{Z}[x] : f \in \mathrm{Ker}(\mathrm{val}_i) \Leftrightarrow f(i) = 0 \underset{f \in \mathbb{R}[x]}{\Leftrightarrow} f(-i) = 0.$$

  Dunque $f \in \mathrm{Ker}(\mathrm{val}_i) \Leftrightarrow (x-i)(x+i) | f$ (in $\mathbb{C}[x]$). Siccome $(x-i)(x+i) = x^2+1$, allora $\mathrm{Ker}(\mathrm{val}_i) = (x^2+1)$. Cioè

$$\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1).$$

- *Se* $n \in \mathbb{Z}$ *è tale che* $\sqrt{n} \notin \mathbb{Q}$, *provare che* $\mathbb{Z}[\sqrt{n}] \cong \mathbb{Z}[x]/(x^2-n)$. Come prima, si consideri $\mathrm{val}_{\sqrt{n}} : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{n}]$. Vogliamo provare che $\mathrm{Ker}(\mathrm{val}_{\sqrt{n}}) = (x^2-n)$, e per fare questo bisognerà provare, come prima, che $f(\sqrt{n}) = 0 \Leftrightarrow f(-\sqrt{n}) = 0 \ \ \forall\ f \in \mathbb{Z}[x]$.

Valutazioni

- A tal scopo, si noti che, se $g = \sum_{i=0}^{s} a_i x^{2i} \in \mathbb{Z}[x]$, allora

$$g(\sqrt{n}) = g(-\sqrt{n}) = \sum_{i=0}^{s} a_i n^i \in \mathbb{Z}.$$

Sia $f = \sum_{i=0}^{s} a_i x^i \in \mathbb{Z}[x]$, e scriviamo $f = g + xh$ dove

$$g = \sum_{j=0}^{\lfloor s/2 \rfloor} a_{2j} x^{2j}$$

$$h = \sum_{j=0}^{\lfloor s/2 \rfloor} a_{2j+1} x^{2j}$$

Quindi $f(\sqrt{n}) = g(\sqrt{n}) + \sqrt{n} \cdot h(\sqrt{n}) = a + \sqrt{n} \cdot b$ per qualche $a, b \in \mathbb{Z}$, e $f(-\sqrt{n}) = a - \sqrt{n} \cdot b$, dunque

$$f(\sqrt{n}) = 0 \Leftrightarrow f(-\sqrt{n}) = 0.$$

Isomorfismi canonici

ESERCIZIO: Dato un anello A, provare che:

- Per ogni $a \in A$, $A[X]/(X-a) \cong A$: Si consideri l'omomorfismo di anelli $\mathrm{val}_a : A[X] \to A$ (definito da $F \mapsto F(a)$). Si noti che val_a è surgettivo, poiché

$$\mathrm{val}_a(r) = r \quad \forall\ r \in A.$$

Dunque $A \cong A[X]/\operatorname{Ker}(\mathrm{val}_a)$. Vogliamo provare

$$\operatorname{Ker}(\mathrm{val}_a) = (X-a).$$

"$\supseteq$" è chiaro. Per "$\subseteq$", sia $F \in \operatorname{Ker}(\mathrm{val}_a)$; essendo $X-a$ monico, è possibile effettuare la divisione con resto di F per $X-a$:

$$F = (X-a)Q + r, \quad Q \in A[X], r \in A.$$

Ma $0 = F(a) = (a-a)Q(a) + r = r$, quindi $F = (X-a)Q$ appartiene a $(X-a)$.

Isomorfismi canonici

- Per ogni $a \in A$, $F_1, \ldots, F_r \in A[x]$,

$$A[X]/(X-a, F_1, \ldots, F_r) \cong A/(F_1(a), \ldots, F_r(a)) :$$

Per il secondo teorema di isomorfismo per anelli, se $I = (X-a)$ e $J = (X-a, F_1, \ldots, F_r)$ si ha:

$$A[X]/(X-a, F_1, \ldots, F_r) \cong \frac{A[X]/I}{J/I}.$$

Abbiamo già visto nella slide precedente che $A[X]/I \cong A$, quindi resta da dimostrare che $J/I = (F_1(a), \ldots, F_r(a))$. Questo è chiaro perché

$$J/I = \mathrm{val}_a(J) = (F_1(a), \ldots, F_r(a)).$$

Isomorfismi canonici

ESERCIZIO: Si calcoli $\mathbb{Z}[i]/(7+i)$.

Siccome $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$, si ha

$$\mathbb{Z}[i]/(7+i) \cong \frac{\mathbb{Z}[X]/(X^2+1)}{(X^2+1, 7+X)/(X^2+1)}.$$

Dal secondo teorema d' isomorfismo per anelli:

$$\frac{\mathbb{Z}[X]/(X^2+1)}{(X^2+1, 7+X)/(X^2+1)} \cong \mathbb{Z}[X]/(X^2+1, X+7).$$

Dall'esercizio precedente $\mathbb{Z}[X]/(X^2+1, X+7) \cong \mathbb{Z}/((-7)^2+1)$ $= \mathbb{Z}_{50}$. Dunque $\mathbb{Z}[i]/(7+i) \cong \mathbb{Z}_{50}$.

Si osservi che $N(7+i) = 50$, infatti si puó dimostrare che $|\mathbb{Z}[i]/(z)| = N(z)$ per ogni $z \in \mathbb{Z}[i]$.

Isomorfismi canonici

ESERCIZIO: Si consideri il sottoanello $A = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$ di $\mathbb{R}$.

a) *A è un dominio? Un campo?* Essendo un sottoanello di un dominio, A è un dominio. A non è un campo, ad esempio 2 non è invertibile:

$$2(a + b\sqrt{7}) = 2a + 2b\sqrt{7} = 1 \underset{a,b\in\mathbb{Z}}{\Rightarrow} \; b = 0, \; 2a = 1,$$

ma questo è impossibile ($a \in \mathbb{Z}$).

b) *Provare che $A \cong \mathbb{Z}[x]/(x^2 - 7)$.* Qualche lezione fa abbiamo dimostrato che $\mathbb{Z}[\sqrt{n}] \cong \mathbb{Z}[x]/(x^2 - n)$ per ogni $n \in \mathbb{Z}$ tale che $\sqrt{n} \notin \mathbb{Z}$. Poiché $A = \mathbb{Z}[\sqrt{7}]$, l'isomorfismo richiesto è un caso particolare.

c) *Sia $I = (1 + \sqrt{7}) \subseteq A$. Provare che $6 \in I$ e dire se I è primo.* Si noti che $6 = (1 + \sqrt{7})(-1 + \sqrt{7}) \in I$. Da uno degli isomorfismi canonici,

$$A/I \cong \mathbb{Z}[x]/(x^2 - 7, 1 + x) \cong \mathbb{Z}/((-1)^2 - 7) \cong \mathbb{Z}_6.$$

Poiché $\mathbb{Z}_6$ non è un dominio, I non è primo.

Isomorfismi canonici

ESERCIZIO: sia A un anello e $I \subseteq A$ un ideale:

- *Provare che* $I[x] = \{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0, \ldots, a_n \in I\}$ *è un ideale di* $A[x]$, *e che* $A[x]/I[x] \cong A/I[x]$: siano $f = \sum_{i=0}^{n} a_i x^i \in I[x]$, $g = \sum_{i=0}^{m} b_i x^i \in I[x]$ e $h = \sum_{i=0}^{s} c_i x^i \in A[x]$: allora

$$f + g = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)x^k \in I[x].$$

$$f \cdot h = \sum_{k=0}^{n+s} \sum_{\substack{i \in \{0,\ldots,n\} \\ j \in \{0,\ldots,s\} \\ i+j=k}} (a_i c_j)x^k \in I[x].$$

Dunque $I[x]$ è un ideale di $A[x]$.

Si consideri l'omomorfismo surgettivo di anelli $\phi : A[x] \to A/I[x]$ definito come $f = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \overline{a_i} x^i$. Chiaramente $\phi(f) = 0$ $\Leftrightarrow a_i \in I \ \forall \ i = 0, \ldots, n \Leftrightarrow f \in I[x]$. Dunque $\mathrm{Ker}(\phi) = I[x]$, quindi

$$A[x]/I[x] \cong A/I[x].$$

Isomorfismi canonici

- *Sia* $\tilde{I} = \{f = \sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0 \in I\}$. *Provare che* $\tilde{I}$ *è un ideale di* $A[x]$, *e che* $A[x]/\tilde{I} \cong A/I$: si noti che $\tilde{I} = \{f \in A[x] : f(0) \in I\}$:
  - $f, g \in \tilde{I} \Rightarrow (f+g)(0) = f(0) + g(0) \in I \Rightarrow f + g \in \tilde{I}$;
  - $f \in \tilde{I}, h \in A[x] \Rightarrow (fh)(0) = f(0)h(0) \in I \Rightarrow fh \in \tilde{I}$.

  Dunque $\tilde{I}$ è un ideale di $A[x]$.

  Si consideri l'omomorfismo surgettivo di anelli $\psi : A[x] \to A/I$ definito come $f \mapsto \overline{f(0)}$. Chiaramente $\psi(f) = 0 \Leftrightarrow f(0) \in I \Leftrightarrow f \in \tilde{I}$. Dunque $\mathrm{Ker}(\psi) = \tilde{I}$, quindi

$$A[x]/\tilde{I} \cong A/I.$$

Ripasso

Sia A un dominio d'integrità:

- dati $a, b \in A$, allora

$$(a) = (b) \Leftrightarrow \exists\, u \in U(A) : ua = b.$$

- dato $a \in A$, (a) ideale primo $\Rightarrow$ a irriducibile.
- se A è un UFD, dato $a \in A$, (a) ideale primo $\Leftrightarrow$ a irriducibile.
- A dominio euclideo $\Rightarrow$ A PID $\Rightarrow$ A UFD. Nessuna freccia può essere capovolta.

Gli interi di Gauss

Gli interi di Gauss sono gli elementi dell'anello $\mathbb{Z}[i]$.

Carl Friedrich Gauss
(Braunschweigh, 30/4/1777 -
Gottinga, 23/2/1855)

Essendo $\mathbb{Z}[i]$ un UFD (poiché è un PID), dato un elemento $z \in \mathbb{Z}[i]$

$$z \text{ è irriducibile } \Leftrightarrow (z) \text{ è un ideale primo.}$$

Quali sono gli interi di Gauss irriducibili?

Faremo una serie di esercizi che ci permetterà di rispondere a questa domanda. È utile ricordare che

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\} = \{z \in \mathbb{Z}[i] : N(z) = 1\}.$$

Gli interi di Gauss

All'interno dei prossimi esercizi risponderemo anche alla seguente domanda in teoria dei numeri:

Quali numeri primi > 2 sono una somma di due quadrati?

Vediamo: 3 no, $5 = 2^2 + 1^2$, 7 no, 11 no, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, 19 no, 23 no, $29 = 5^2 + 2^2$ .....

Da questi esempi sembrerebbe che un primo $p > 2$ è somma di due quadrati se e solo se $p = 1 \pmod 4$. Dimostreremo questo fatto non banale, e vedremo anche che la scrittura come somma di due quadrati è unica. *Tutto ciò non vale per numeri non primi*:

- $21 = 1 \pmod 4$, ma non è scrivibile in nessun modo come somma di due quadrati.
- $65 = 1 \pmod 4$, ma $65 = 8^2 + 1^2 = 7^2 + 4^2$.

Gli interi di Gauss

ESERCIZIO: Sia G un gruppo Abeliano finito, e $n = \max\{\pi(g) : g \in G\}$. Allora $\pi(g)|n$ per ogni $g \in G$ (equivalentemente $g^n = 1 \ \ \forall\, g \in G$).

(Se G non è Abeliano questo è falso: per esempio in S_3 il periodo massimo è 3, ma ci sono elementi di periodo 2).

Sia $x \in G$ tale che $\pi(x) = n$. Per assurdo $\exists\, g \in G : m = \pi(g) \nmid n$. Allora esiste un numero primo p e $a \in \mathbb{N}$ tale che p^a divide m ma non n. Sia

$$b = \max\{i \in \mathbb{N} : p^i | n\}.$$

Per quanto detto $b < a$. Si osservi che

$$\pi(x^{p^b}) = \frac{n}{\mathrm{MCD}(n, p^b)} = n/p^b \quad \text{e} \quad \pi(g^{m/p^a}) = \frac{m}{\mathrm{MCD}(m, m/p^a)} = p^a.$$

Quindi $\mathrm{MCD}(\pi(x^{p^b}), \pi(g^{m/p^a})) = 1$. Poiché x^{p^b} e g^{m/p^a} commutano:

$$\pi(x^{p^b} g^{m/p^a}) = \pi(x^{p^b}) \cdot \pi(g^{m/p^a}) = n/p^b \cdot p^a > n.$$

Ciò contraddice la massimalità di n.

Gli interi di Gauss

ESERCIZIO: Sia K un campo finito, e $G = U(K)$. Allora G è ciclico.

Sia $n = \max\{\pi(g) : g \in G\}$. Dall'esercizio precedente $g^n = 1$ per ogni $g \in G$, quindi

$$G \subseteq \{x \in K : x^n = 1\}.$$

Poiché un polinomio di grado n a coefficienti in un campo ha al più n radici, si ha

$$|\{x \in K : x^n = 1\}| \leq n.$$

Quindi $|G| \leq n$; se $x \in G$ è tale che $\pi(x) = n$, allora, $\mathrm{gp}(x) = G$.

ESEMPIO: se p è un numero primo, $U(\mathbb{Z}_p)$ è ciclico. Al contrario in

$$U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

nessun elemento ha periodo 4 ($\overline{1}^2 = \overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$.)

Gli interi di Gauss

ESERCIZIO: Sia $p > 2$ un numero primo. Provare che le seguenti tre affermazioni sono equivalenti:

(a) $\exists\, a, b \in \mathbb{Z}$: $p = a^2 + b^2$;

(b) $p = 1 \pmod 4$;

(c) p è riducibile in $\mathbb{Z}[i]$.

La strategia sarà di dimostrare $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

- $(a) \Rightarrow (b)$: avendo $p = a^2 + b^2$ in $\mathbb{Z}$, allora anche in $\mathbb{Z}_4$

$$\overline{p} = \overline{a^2 + b^2} = \overline{a^2} + \overline{b^2} = \overline{a}^2 + \overline{b}^2.$$

  D'altronde $\{x^2 : x \in \mathbb{Z}_4\} = \{\overline{0}, \overline{1}\}$. Dunque $\overline{a}^2 + \overline{b}^2 \in \{\overline{0}, \overline{1}, \overline{2}\}$; essendo p dispari, si ha $\overline{p} = \overline{1}$.

- $(c) \Rightarrow (a)$: siano $z_1, z_2 \in \mathbb{Z}[i]$ elementi non invertibili tali che $p = z_1 z_2$. Allora $p^2 = N(z_1)N(z_2)$. Poiché z_1 e z_2 non sono in $U(\mathbb{Z}[i])$, $N(z_1)$ e $N(z_2)$ sono interi > 1. L'unica possibilità, dunque, è che $N(z_1) = N(z_2) = p$, cioè che $p = a^2 + b^2$ dove $z_1 = a + ib$.

Gli interi di Gauss

- $(b) \Rightarrow (c)$ ($\overline{p} = \overline{1}$ in $\mathbb{Z}_4 \Rightarrow p$ riducibile in $\mathbb{Z}[i]$). Sia $a \in \mathbb{Z}$ tale che $p = 4a + 1$. Allora $|U(\mathbb{Z}_p)| = 4a$. Siccome $\mathbb{Z}_p$ è un campo finito, $U(\mathbb{Z}_p)$ è ciclico. Sia $x \in \mathbb{Z}$ tale che $\mathrm{gp}(\overline{x}) = U(\mathbb{Z}_p)$. Allora

$$x^{4a} - 1 = 0 \pmod{p}.$$

Allora $(\overline{x}^{2a} - \overline{1})(\overline{x}^{2a} + \overline{1}) = \overline{x}^{4a} - \overline{1} = \overline{0}$ in $\mathbb{Z}_p$. Avendo $\overline{x}$ periodo $4a$ in $U(\mathbb{Z}_p)$, $\overline{x}^{2a} - \overline{1} \neq \overline{0}$; essendo $\mathbb{Z}_p$ un dominio, allora

$$x^{2a} + 1 = 0 \pmod{p}.$$

Siano $z_1 = x^a + i$ e $z_2 = x^a - i$ in $\mathbb{Z}[i]$. Si ha che $z_1 z_2 = x^{2a} + 1$ sta in $(p) \subseteq \mathbb{Z}[i]$. Ma z_1 non sta in (p) (poiché $p(u + iv) = x^a + i$ implicherebbe $pv = 1$) e analogamente $z_2 \notin (p)$. Ma allora (p) non è primo, che poiché $\mathbb{Z}[i]$ è un UFD implica che p è riducibile.

Gli interi di Gauss

ESERCIZIO: Sia $z \in \mathbb{Z}[i]$ con parte reale e parte immaginaria non nulle. Provare che le seguenti due affermazioni sono equivalenti:

(a) $N(z)$ è un numero primo;

(b) z è irriducibile.

- $(a) \Rightarrow (b)$. Supponiamo che $z = z_1 z_2$ per $z_1, z_2 \in \mathbb{Z}[i]$. Allora $N(z) = N(z_1)N(z_2)$, che poiché $N(z)$ è un numero primo significa che una fra $N(z_1)$ e $N(z_2)$ è uguale a 1. Cioè uno fra z_1 e z_2 è invertibile in $\mathbb{Z}[i]$. Quindi z è irriducibile.
- $(b) \Rightarrow (a)$. Assumiamo per assurdo che $z\overline{z} = N(z)$ non sia primo; allora esistono r, s numeri interi maggiori di 1 tali che $z\overline{z} = rs$. Essendo z irriducibile, (z) è un ideale primo di $\mathbb{Z}[i]$; quindi uno fra r e s sta in (z) (siccome $rs \in (z)$). Possiamo supporre $r \in (z)$, cioè $r = zz_1$ per qualche $z_1 \in \mathbb{Z}[i]$. Quindi $z\overline{z} = zz_1 s$, cioè $\overline{z} = z_1 s$. Coniugando, $z = \overline{z}_1 s$. Ma z è irriducibile, e s è un intero maggiore di 1. Quindi z_1 è invertibile, ovvero $z_1 \in \{\pm 1, \pm i\}$. Allora l'uguaglianza in blu contraddice il fatto che sia la parte reale che quella immaginaria di z siano non nulle.

Gli interi di Gauss

ESERCIZIO: Gli elementi irriducibili in $\mathbb{Z}[i]$ sono esattamente:

(a) $p, -p, ip, -ip$ con $p \in \mathbb{N}$ un numero primo uguale a 3 modulo 4;

(b) $z \in \mathbb{Z}[i]$ con $N(z)$ numero primo di $\mathbb{N}$.

Se $z \in \mathbb{Z}[i]$ ha entrambe la parte reale e quella immaginaria non nulle, allora z è irriducibile se e solo se è di tipo (b). Altrimenti, $N(z)$ è un quadrato in $\mathbb{Z}$, quindi di certo z non è di tipo (b) (indipendentemente dal fatto che sia irriducibile o no). Poiché z è irriducibile se e solo se uz è irriducibile per ogni

$$u \in U(\mathbb{Z}[i]) = \{\pm 1, \pm i\},$$

possiamo assumere che $z = n$ sia un numero naturale. Di certo, se n non è un numero primo allora è riducibile anche in $\mathbb{Z}[i]$. D'altra parte abbiamo visto che se n è un primo > 2 allora n è riducibile se e solo se $n = 1 \pmod 4$. Inoltre, $n = 2$ è riducibile perché $2 = (1 + i)(1 - i)$. Allora n è irriducibile se e solo se è un numero primo uguale a 3 modulo 4.

Gli interi di Gauss

ESERCIZIO: Sia $p \in \mathbb{N}$ un numero primo tale che $p = a^2 + b^2$ per una coppia di numeri naturali a e b: provare che, se c e d sono numeri naturali tali che $p = c^2 + d^2$, allora

$$\{a, b\} = \{c, d\}.$$

Se $p = a^2 + b^2 = c^2 + d^2$, allora in $\mathbb{Z}[i]$ abbiamo:

$$p = z_1\overline{z}_1 = z_2\overline{z}_2, \quad \text{dove} \quad z_1 = a + bi \text{ e } z_2 = c + di.$$

Poiché $N(z_1) = N(\overline{z}_1) = N(z_2) = N(\overline{z}_2) = p$ è un numero primo, allora $z_1\overline{z}_1$ e $z_2\overline{z}_2$ sono due fattorizzazioni in irriducibili di p in $\mathbb{Z}[i]$. Essendo $\mathbb{Z}[i]$ un UFD, tali fattorizzazioni devono essere uguali a meno dell' ordine dei fattori e di moltiplicazione per elementi invertibili di $\mathbb{Z}[i]$, che significa proprio che $\{a, b\} = \{c, d\}$.

Gli interi di Gauss

Concludiamo osservando che un numero primo $p \in \mathbb{N}$ da luogo a:

- se $p = a^2 + b^2$, gli ideali primi $(a + bi), (a - bi) \subseteq \mathbb{Z}[i]$;
- se $p = 3 \pmod 4$, l'ideale primo $(p) \subseteq \mathbb{Z}[i]$.

Inoltre, poiché in un dominio A si ha $(a_1) = (a_2) \Leftrightarrow a_1 = ua_2$ per qualche $u \in U(A)$, e poiché $\mathbb{Z}[i]$ è un PID:

- quelli in verde sono tutti e soli gli ideali primi di $\mathbb{Z}[i]$;
- $(a + bi) = (a - bi) \Leftrightarrow a = b = 1$ $(1 + i = -i(1 - i))$, dunque tutti gli ideali in verde sono distinti a parte se $a = b = 1$.

MCD - Ripasso

Sia A un dominio. Dati due elementi non nulli $a, b \in A$, un elemento $x \in A$ si dice **massimo comun divisore** di a e b se:

- x divide sia a che b.
- Se $y \in A$ divide sia a che b, allora y divide x.

Potrebbe non esistere nessun massimo comun divisore. Se esiste non è unico, ma lo è a meno di moltiplicazione per invertibili:

$x_1 \in A$ e $x_2 \in A$ sono massimi comun divisori di a e $b \Leftrightarrow \exists\ u \in U(A) : x_1 = ux_2$.

Dunque denoteremo un massimo comun divisore di a e b con

$$\mathrm{MCD}(a, b).$$

- A UFD $\Rightarrow \forall\ a \neq 0 \neq b \in A\ \ \exists\ \mathrm{MCD}(a, b) \in A$.
- A PID $\Rightarrow (a, b) = (\mathrm{MCD}(a, b))\ \ \forall\ a, b \in A$.
- A dominio euclideo $\Rightarrow$ il massimo comun divisore si può calcolare algoritmicamente.

MCD

ESERCIZIO: Dato uno dei seguenti ideali $I \subseteq \mathbb{Z}[i]$, si decida se I è proprio, ed eventualmente se $\mathbb{Z}[i]/I$ è un campo, un dominio o meno.

- $I = (5+2i,\ 3-i)$. Si noti che $N(5+2i) = 29$ e $N(3-i) = 10$. Quindi, in $\mathbb{C} \supseteq \mathbb{Z}[i]$:

$$\frac{5+2i}{3-i} = \frac{(5+2i)(3+i)}{10} = \frac{13+11i}{10}.$$

L'intero di Gauss più vicino a $13/10 + 11/10i$ è $1+i$, e:

$$5+2i = (3-i)(1+i)+1.$$

Quindi $1 \in I$, cioè $I = \mathbb{Z}[i]$ non è proprio.

MCD

- $I = (7+i,\ 9+7i)$. Si noti che $N(7+i) = 50$ e $N(9+7i) = 130$. Quindi, in $\mathbb{C} \supseteq \mathbb{Z}[i]$:

$$\frac{9+7i}{7+i} = \frac{(9+7i)(7-i)}{50} = \frac{70+40i}{50}.$$

L'intero di Gauss più vicino a $7/5 + 4/5i$ è $1+i$, e:

$$(1).\ \ 9+7i = (7+i)(1+i)+3-i.$$

Siccome

$$(2).\ \ 7+i = (3-i)(2+i),$$

$\mathrm{MCD}(7+i, 9+7i) = 3-i$. Dunque $I = (3-i) \subseteq \mathbb{Z}[i]$ perché $\mathbb{Z}[i]$ è un PID. Poiché $N(3-i) = 10$ non è un numero primo, $3-i$ è riducibile per la caratterizzazione degli irriducibili di $\mathbb{Z}[i]$. Quindi I non è un ideale primo, dunque $\mathbb{Z}[i]/I$ non è un dominio, tantomeno non è un campo. Si osservi che i massimi comun divisori di $7+i$ e $9+7i$ sono anche $-3+i, 1+3i$ e $-1-3i$.

MCD

- $I = (6+3i,\ 3+14i)$. Si noti che $N(6+3i) = 45$ e $N(3+14i) = 205$. Quindi, in $\mathbb{C} \supseteq \mathbb{Z}[i]$:

$$\frac{3+14i}{6+3i} = \frac{(3+14i)(6-3i)}{45} = \frac{60+75i}{45}.$$

L'intero di Gauss più vicino a $60/45 + 75/45i$ è $1+2i$, e:

$$(1).\ \ 3+14i = (6+3i)(1+2i)+3-i.$$

Siccome $N(3-i) = 10$, in $\mathbb{C} \supseteq \mathbb{Z}[i]$ abbiamo:

$$\frac{6+3i}{3-i} = \frac{(6+3i)(3+i)}{10} = \frac{15+15i}{10}.$$

Gli interi di Gauss più vicini a $15/10 + 15/10i$ sono

$$\{1+i,\ 2+i,\ 1+2i,\ 2+2i\}\ .....$$

MCD

- ..... Considerando, ad esempio, $2+i$, si ha:

$$(2).\quad 6+3i=(3-i)(2+i)-1+2i.$$

Siccome

$$(3).\quad 3-i=(-1+2i)(-1-i),$$

deduciamo che $\mathrm{MCD}(3+14i,6+3i)=-1+2i$. Quindi, essendo $\mathbb{Z}[i]$ un PID:

$$I=(-1+2i)\subseteq\mathbb{Z}[i].$$

Poiché $N(-1+2i)=5$ è un numero primo, I è un ideale primo per la caratterizzazione degli irriducibili di $\mathbb{Z}[i]$. Essendo un ideale primo non nullo in un PID, I è massimale, dunque $\mathbb{Z}[i]/I$ è un campo, in particolare un dominio.

UFD

ESERCIZIO: Sia $A \subseteq \mathbb{Q}[x]$ il sottoanello

$$A = \{a_0 + a_2x^2 + a_3x^3 + \ldots + a_nx^n : a_i \in \mathbb{Q}\}.$$

- *Provare che* $U(A) = \mathbb{Q}^*$: L'uguaglianza segue dal fatto che $1_A = 1_{\mathbb{Q}[x]}$ e $\mathbb{Q}^* = U(\mathbb{Q}[x]) \subseteq A$.
- *Sia* $0 \neq h \in A$ *di grado 2 o 3. Provare che* h *è irriducibile in* A: siano $f, g \in A$ tali che $h = fg$. Se i gradi di f e di g fossero diversi da zero, allora sarebbero entrambi almeno 2; allora $fg \in \mathbb{Q}[x]$ sarebbe un polinomio di grado ≥ 4, che è assurdo. Allora uno fra f e g ha grado 0, cioè è invertibile. Dunque h è irriducibile.

UFD

Con le notazioni precedenti, si consideri $x^6 \in A$; questo elemento ha due fattorizzazioni in irriducibili:

- $x^6 = x^2 \cdot x^2 \cdot x^2$;
- $x^6 = x^3 \cdot x^3$.

In particolare A non è un UFD; x^6 ha addirittura due fattorizzazioni che usano un numero diverso di fattori.

UFD

ESERCIZIO: Sia $A = \{a + xg : a \in \mathbb{Q},\ g \in \mathbb{R}[x]\} \subset \mathbb{R}[x]$.

a) *Provare che A è un sottoanello di $\mathbb{R}[x]$*: Siano $a_1 + xg_1$ e $a_2 + xg_2$ elementi di A:

- $a_1 + xg_1 - (a_2 + xg_2) = (a_1 - a_2) + x(g_1 - g_2) \in A$.
- $(a_1 + xg_1)(a_2 + xg_2) = a_1a_2 + x(a_2g_1 + a_1g_2 + g_1g_2) \in A$.

Quindi A è un sottoanello di $\mathbb{R}[x]$.

b) *Determinare $U(A)$*. È facile vedere che

$$U(A) = U(\mathbb{R}[x]) \cap A = \mathbb{R}^* \cap A = \mathbb{Q}^*.$$

c) *Sia $P = \{f \in A : f(0) = 0\}$. Provare che P è un ideale di A, e studiarne le proprietà*. Che P è un ideale di A è chiaro. Si consideri l'omomorfismo di anelli $\phi : A \to \mathbb{Q}$ definito da $\phi(f) = f(0)$. Chiaramente ϕ è surgettivo ($\phi(a + gx) = a$), e $\mathrm{Ker}(\phi) = P$. Dunque $A/P \cong \mathbb{Q}$, in particolare P è massimale...

c) ... Vogliamo ora capire se $P \subset A$ è principale: Si noti che

$$P = \{xg : g \in \mathbb{R}[x]\} \subset A.$$

Sia $f = xg \in P$ tale che $(f) = P$. Siccome $x \in P$ e $\sqrt{2}x \in P$, dovrebbero esistere $p, q \in A$ tali che

$$x = pf = xpg, \quad \sqrt{2}x = qf = xqg,$$

da cui $pg = 1$ e $qg = \sqrt{2}$. Tali uguaglianze, valendo in A, valgono anche in $\mathbb{R}[x]$. Dunque p, q, g devono essere invertibili in $\mathbb{R}[x]$, cioè numeri reali non nulli. Allora

$$\sqrt{2} = q/p,$$

ma ciò è impossibile perché p e q, essendo elementi di grado 0 di A, stanno in $\mathbb{Q}$. Quindi P non è principale.

UFD

d) *Provare che x e $\sqrt{2}x$ sono irriducibili in A e non equivalenti in A.*
Poiché $U(A) = U(\mathbb{R}[x]) \cap A$, per ogni $f \in A$ si ha

$$f \text{ riducibile in } A \Rightarrow f \text{ riducibile in } \mathbb{R}[x].$$

Quindi x e $\sqrt{2}x$ sono irriducibili in A. Se fossero equivalenti in A, allora $(x) = (\sqrt{2}x)$ come ideali di A, che non è vero per un ragionamento analogo a quello fatto nella slide precedente. Dunque x e $\sqrt{2}x$ non sono equivalenti in A.

e) *A è un UFD?* No, infatti

$$2x^2 = x \cdot 2x = \sqrt{2}x \cdot \sqrt{2}x$$

sono 2 fattorizzazioni diverse in fattori irriducibili.

Caratteristica

ESERCIZIO: Sia A un anello di caratteristica $p > 0$, dove p è un numero primo. Provare che

$$\begin{aligned} F : A &\to A \\ a &\mapsto a^p \end{aligned}$$

è un omomorfismo di anelli.

Innanzitutto si noti che, per ogni $1 \leq i \leq p-1$,

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{i(i-1)(i-2)\cdots 1}$$

è diviso da p in $\mathbb{Z}$. Siano $a, b \in A$:

$$F(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = \binom{p}{0} b^p + \binom{p}{p} a^p = a^p + b^p = F(a) + F(b)$$

$$F(ab) = (ab)^p = a^p b^p = F(a)F(b)$$

$F : A \to A$ è chiamato l' omomorfismo di **Frobenius**.

Caratteristica

ESERCIZIO: Sia A un anello di caratteristica $p > 0$, dove p è un numero primo. Provare che A è ridotto se e solo se il Frobenius $F : A \to A$ è iniettivo.

- "$\Rightarrow$": $a \in \mathrm{Ker}(F) \Leftrightarrow F(a) = a^p = 0$; dunque ogni elemento di $\mathrm{Ker}(F)$ è nilpotente, quindi

$$A \text{ ridotto} \quad \Rightarrow \quad \mathrm{Ker}(F) = \{0\}.$$

- "$\Leftarrow$": F è iniettivo se e solo se $F(a) = a^p \neq 0 \ \forall \ 0 \neq a \in A$. Come visto qualche lezione fa, ciò implica che A è ridotto.

Caratteristica

Un campo K si dice **perfetto** se una delle due seguenti condizioni è soddisfatta:

- $\mathrm{char}(K) = 0$; oppure
- $\mathrm{char}(K) > 0$ e il Frobenius $F : K \to K$ è surgettivo.

OSS.: 1). Se K è algebricamente chiuso è perfetto. Infatti, se $\mathrm{char}(K) = p > 0$, per ogni $\lambda \in K$ il polinomio $x^p - \lambda \in K[x]$ ammette radici. Se α è una tale radice, allora $F(\alpha) = \alpha^p = \lambda$.

2). Se K è perfetto di caratteristica positiva, F è un isomorfismo: infatti $F : K \to K$ è anche iniettivo perché K, essendo un campo, è ridotto.

3). Se K è un campo finito, allora è perfetto. Si noti che la caratteristica di K deve essere per forza positiva. Essendo un campo ridotto, $F : K \to K$ è una funzione iniettiva da un insieme finito in se stesso, quindi è pure surgettiva.

Estensioni di campi - Ripasso

Siano $K \subseteq L$ due campi (tali che K è un sottoanello di L), e $\alpha \in L$. Consideriamo l'omomorfismo di valutazione $\mathrm{val}_\alpha : K[X] \to L$, ricordando che con $K[\alpha]$ intendiamo $\mathrm{Im}(\mathrm{val}_\alpha)$.

- α è algebrico su K se e solo se $\mathrm{Ker}(\mathrm{val}_\alpha) \neq (0)$;
- α è trascendente su K se e solo se $\mathrm{Ker}(\mathrm{val}_\alpha) = (0)$.

Siccome $K[X]/\mathrm{Ker}(\mathrm{val}_\alpha) \cong K[\alpha] \subseteq L$ è un dominio, $\mathrm{Ker}(\mathrm{val}_\alpha)$ è un ideale primo di $K[X]$. Se α è algebrico su K, essendo $K[X]$ un PID, $\mathrm{Ker}(\mathrm{val}_\alpha)$ è massimale, cioè $K[\alpha]$ è un campo. In tal caso, $\mathrm{Ker}(\mathrm{val}_\alpha) = (f)$ per un qualche polinomio monico $f \in K[X]$. Tale $f \in K[X]$ viene chiamato il polinomio minimo di α su K.

Estensioni di campi

ESERCIZIO: Provare che $\sqrt{2} \notin \mathbb{Q}[\sqrt[3]{2}]$.

Siano $K = \mathbb{Q}[\sqrt{2}]$ e $L = \mathbb{Q}[\sqrt[3]{2}]$. Si osservi che il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è

$$X^2 - 2 \in \mathbb{Q}[X],$$

mentre quello di $\sqrt[3]{2}$ è

$$X^3 - 2 \in \mathbb{Q}[X].$$

Quindi $[K : \mathbb{Q}] = 2$ e $[L : \mathbb{Q}] = 3$. Se $\sqrt{2}$ appartenesse a $\mathbb{Q}[\sqrt[3]{2}]$, allora avremmo $K \subseteq L$, e dunque

$$3 = [L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = [L : K] \cdot 2,$$

che è assurdo.

Estensioni di campi

ESERCIZIO: Provare che $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Siccome $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, abbiamo

$$\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3}].$$

D'altra parte, sia $u = \sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}] = K$; allora

$$(u-\sqrt{2})^2 = u^2 - 2u\sqrt{2} + 2 = 3,$$

da cui $\sqrt{2} = (u^2-1)/2u$ sta in K, poiché K è un campo. Quindi anche $\sqrt{3} = u - \sqrt{2} \in K$, dunque

$$\mathbb{Q}[\sqrt{2},\sqrt{3}] \subseteq K = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$$

Estensioni di campi

ESERCIZIO: Sia $t \geq 0$ un numero razionale e $\alpha = \sqrt{\sqrt{t} - 1}$.

a) *Provare che* α *è algebrico su* $\mathbb{Q}$: Si osservi che

$$\alpha^2 = \sqrt{t} - 1,$$

da cui $(\alpha^2 + 1)^2 = t$; quindi α è radice del polinomio

$$F_t = X^4 + 2X^2 + 1 - t \in \mathbb{Q}[X].$$

In particolare α è algebrico su $\mathbb{Q}$.

b) *Provare che* $\sqrt{t} \in \mathbb{Q}[\alpha]$. Siccome $\mathbb{Q}[\alpha]$ è un anello, $\mathbb{Q}[\alpha] \ni \alpha^2 = \sqrt{t} - 1$, quindi $\sqrt{t} = \alpha^2 + 1 \in \mathbb{Q}[\alpha]$.

c) *Esiste* t *tale che* $\alpha \in \mathbb{Q}[\sqrt{t}]$*?* Si, ad esempio si consideri $t = 25$. In questo caso

$$\alpha = 2 \in \mathbb{Q} = \mathbb{Q}[\sqrt{t}].$$

Estensioni di campi

d) *Se $\sqrt{t} \notin \mathbb{Q}$, si trovino i polinomi minimi di α su $\mathbb{Q}$ e su $\mathbb{Q}[\sqrt{t}]$:* abbiamo già visto che α è radice del polinomio

$$F_t = X^4 + 2X^2 + 1 - t \in \mathbb{Q}[X].$$

Per provare che F_t è il polinomio minimo di α su $\mathbb{Q}$, proviamo che $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$. Siccome

$$4 \geq [\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}[\sqrt{t}]] \cdot [\mathbb{Q}[\sqrt{t}] : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}[\sqrt{t}]] \cdot 2,$$

basterà dimostrare che $\alpha \notin \mathbb{Q}[\sqrt{t}]$. Se per assurdo $\alpha \in \mathbb{Q}[\sqrt{t}]$, allora esistono $a, b \in \mathbb{Q}$ tali che

$$\alpha = a + b\sqrt{t}.$$

Allora $\alpha^2 = a^2 + b^2 t + 2ab\sqrt{t}$, da cui $(1 - 2ab)\sqrt{t} = a^2 + b^2 t + 1$. Ciò è possibile solo se $1 - 2ab = 0$ e $a^2 + b^2 t + 1 = 0$; poiché $t \geq 0$, l'ultima uguaglianza è assurda.

Siccome α è radice di $G_t = X^2 - \sqrt{t} + 1 \in \mathbb{Q}[\sqrt{t}]$ e, per quanto detto, $[\mathbb{Q}[\alpha] : \mathbb{Q}[\sqrt{t}]] = 2$, G_t è il polinomio minimo di α su $\mathbb{Q}[\sqrt{t}]$.

Estensioni di campi

ESERCIZIO: Trovare il polinomio minimo di $\sqrt{2}+\sqrt{3}$ su $\mathbb{Q}$.

Sia $u = \sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}] = K$. Allora si ha

$$u^2 = 2+3+2\sqrt{6} \;\Leftrightarrow\; u^2-5 = 2\sqrt{6}$$
$$(u^2-5)^2 = 24 \;\Leftrightarrow\; u^4-10u^2+1 = 0$$

Dunque $\sqrt{2}+\sqrt{3}$ è una radice di $f = X^4-10X^2+1 \in \mathbb{Q}[X]$. Vogliamo provare che f è il polinomio minimo di u su $\mathbb{Q}$. A tale scopo basta provare che $[K:\mathbb{Q}] = 4$. Dall' esercizio precedente $K = \mathbb{Q}[\sqrt{2},\sqrt{3}]$, quindi

$$[K:\mathbb{Q}] = [K:\mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = [K:\mathbb{Q}[\sqrt{2}]] \cdot 2.$$

Dunque $[K:\mathbb{Q}]$ è un numero pari ≤ 4. Per provare che è 4 basta trovare 3 elementi di K linearmente indipendenti su $\mathbb{Q}$ ...

Estensioni di campi

... Si considerino $1, \sqrt{2}, \sqrt{3} \in K$ e $a, b, c \in \mathbb{Q}$ tali che

$$a \cdot 1 + b \cdot \sqrt{2} + c \cdot \sqrt{3} = 0.$$

Allora $a = -b\sqrt{2} - c\sqrt{3}$, da cui

$$(-b\sqrt{2} - c\sqrt{3})^2 = 2b^2 + 3c^2 + 2bc\sqrt{6} = a^2 \in \mathbb{Q}$$

Allora $bc\sqrt{6} \in \mathbb{Q}$, che è possibile solo se $bc = 0$. Dall'equazione in blu:

- $b = 0 \Rightarrow -c\sqrt{3} = a \in \mathbb{Q}$. Questo è possibile solo se $c = 0$. Quindi $0 = b = c = a$.
- $c = 0 \Rightarrow -b\sqrt{2} = a \in \mathbb{Q}$. Questo è possibile solo se $b = 0$. Quindi $0 = c = b = a$.

In definitiva $a = b = c = 0$, dunque $1, \sqrt{2}, \sqrt{3} \in K$ sono linearmente indipendenti su $\mathbb{Q}$. Allora, per quanto detto prima, $[K : \mathbb{Q}] = 4$.

Estensioni di campi

ESERCIZIO: Sia K un campo, e $f \in K[X]$ un polinomio di grado 2. Se α è una radice di f, provare che $K[\alpha]$ è il campo di spezzamento di f.

Sia $L = K[\alpha]$. Essendo $\alpha \in L$ una radice di f, in $L[X]$ si ha che

$$f = (X - \alpha)g.$$

Siccome f ha grado 2, g deve avere grado 1. Dunque abbiamo spezzato f in fattori lineari in $L[X]$. Inoltre, siccome un campo di spezzamento di $f \in K[X]$ deve contenere K e tutte le radici di f, allora deve contenere $K[\alpha]$. Dunque $K[\alpha]$ è il campo di spezzamento di $f \in K[X]$.

OSS.: Dall'esercizio precedente segue che $[L : K] \leq 2$ se L è il campo di spezzamento di un polinomio $f \in K[X]$ di grado 2.

In generale, si può dimostrare $[L : K] \leq n!$ se L è il campo di spezzamento di un polinomio $f \in K[X]$ di grado n.

Estensioni di campi

ESERCIZIO: Calcolare $[L : K]$ dove L è il campo di spezzamento del polinomio $f = X^3 + 2 \in K[X]$ dove:

- $K = \mathbb{Q}$: sia $\xi \in \mathbb{C}$ una radice diversa da -1 di $X^3 + 1$. Allora le radici di $X^3 + 2$ sono

$$-\sqrt[3]{2},\ \xi\sqrt[3]{2},\ \xi^2\sqrt[3]{2}.$$

Allora $L = \mathbb{Q}[\sqrt[3]{2}, \xi]$. Quindi $\mathbb{Q}[\sqrt[3]{2}] \subseteq L$, e $\mathbb{Q}[\xi] \subseteq L$. Dunque:

- Siccome il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $X^3 - 2$, $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. Quindi

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt[3]{2}]] \cdot [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt[3]{2}]] \cdot 3.$$

- Siccome $X^3 + 1 = (X + 1)(X^2 - X + 1)$, il polinomio minimo di ξ su $\mathbb{Q}$ è $X^2 - X + 1$, $[\mathbb{Q}[\xi] : \mathbb{Q}] = 2$. Quindi

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\xi]] \cdot [\mathbb{Q}[\xi] : \mathbb{Q}] = [L : \mathbb{Q}[\xi]] \cdot 2.$$

Allora $[L : \mathbb{Q}]$ è un multiplo di 6.

Estensioni di campi

- D'altra parte, siccome $\mathbb{Q}[\sqrt[3]{2}, \xi] = L$ e

$$[\mathbb{Q}[\sqrt[3]{2}, \xi] : \mathbb{Q}[\sqrt[3]{2}]] = [\mathbb{Q}[\sqrt[3]{2}][\xi] : \mathbb{Q}[\sqrt[3]{2}]] \leq [\mathbb{Q}[\xi] : \mathbb{Q}] = 2,$$

allora

$$[L : \mathbb{Q}] = [\mathbb{Q}[\sqrt[3]{2}, \xi] : \mathbb{Q}[\sqrt[3]{2}]] \cdot [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] \leq 2 \cdot 3.$$

Ne deduciamo che $[L : \mathbb{Q}] = 6$.

- $K = \mathbb{Z}_3$: in tal caso $f = X^3 - 2$ si spezza in fattori lineari già in $K[X]$, infatti se $F : K[X] \to K[X]$ è il Frobenius:

$$f = X^3 + 2 = F(X) + F(2) = F(X + 2) = (X + 2)^3.$$

Quindi $L = K$ in questo caso, cioè $[L : \mathbb{Z}_3] = 1$.

Estensioni di campi

- $K = \mathbb{Z}_5$: si osservi che $f(2) = 2^3 + 2 = 0$ in $\mathbb{Z}_5$, quindi in $\mathbb{Z}_5[X]$

$$f = X^3 + 2 = (X - 2)(X^2 + 2X + 4).$$

Dunque L è il campo di spezzamento di

$$g = X^2 + 2X + 4 \in \mathbb{Z}_5[X].$$

Si verifica che g non ha radici in $\mathbb{Z}_5$; dunque se α è una radice di g, allora $L = \mathbb{Z}_5[\alpha]$ e

$$[L : \mathbb{Z}_5] = 2.$$

Isomorfismi canonici

ESERCIZIO: Si consideri l' anello $A = \mathbb{Q}[X, Y]$. Il suo ideale $I = (X - Y^2, X^2 + 2XY + 2)$ è primo?

Si noti che $A = B[X]$ dove $B = \mathbb{Q}[Y]$. Per uno degli isomorfismi canonici

$$A/I \cong B/(Y^4 + 2Y^3 + 2).$$

Dunque I è un ideale primo di A se e solo se $(Y^4 + 2Y^3 + 2)$ è un ideale primo di $B = \mathbb{Q}[Y]$ se e solo se $Y^4 + 2Y^3 + 2$ è un polinomio irriducibile di $\mathbb{Q}[Y]$. Per il criterio di Eisenstein $Y^4 + 2Y^3 + 2$ è effettivamente un poliomio irriducibile di $\mathbb{Q}[Y]$, dunque $I \subseteq A$ è primo.

Isomorfismi canonici

ESERCIZIO: Si consideri l' anello $A = \mathbb{Z}[i][X]$. Si scelgano $n \in \mathbb{Z}$ tali che l'ideale $I = (X - i, X^2 + X + n)$ sia non radicale, radicale ma non primo e primo.

Per uno degli isomorfismi canonici

$$A/I \cong \mathbb{Z}[i]/(n - 1 + i).$$

Usando il fatto che $\mathbb{Z}[i] \cong \mathbb{Z}[Y]/(Y^2 + 1)$, il secondo teorema d'isomorfismo per anelli e di nuovo il medesimo isomorfismo canonico si ha:

$$\begin{aligned} \mathbb{Z}[i]/(n - 1 + i) &\cong \frac{\mathbb{Z}[Y]/(Y^2 + 1)}{(Y^2 + 1, Y + n - 1)/(Y^2 + 1)} \\ &\cong \mathbb{Z}[Y]/(Y + n - 1, Y^2 + 1) \cong \mathbb{Z}_{n^2 - 2n + 2} \end{aligned}$$

Dunque se, ad esempio, $n = 8$, I non è radicale (poiché $\mathbb{Z}_{50}$ non è ridotto); se $n = 4$, I è radicale ma non primo; se $n = 3$, I è primo.

Isomorfismi canonici

ESERCIZIO: Si consideri l'ideale $J = (X^2 + 1) \subseteq A = \mathbb{R}[X, Y]$. Dimostrare che A/J è un PID.

Si noti che $J = I[Y]$ dove $I = (X^2 + 1) \subseteq B = \mathbb{R}[X]$. Quindi, per uno degli isomorfismi canonici,

$$A/J = B[Y]/I[Y] \cong B/I[Y].$$

Ma $B/I = \mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$, quindi $A/J \cong \mathbb{C}[Y]$ che è un PID.

Estensioni di campi

ESERCIZIO: Sia $\alpha \in \mathbb{C}$ una radice di $f(X) = X^3 + 2X + 1 \in \mathbb{Q}[X]$.

(i) *Si provi che $f(X)$ è il polinomio minimo di α.* Bisogna provare che $f(X)$ è irriducibile su $\mathbb{Q}[X]$, e avendo $f(X)$ grado 3 ciò è equivalente a dimostrare che $f(X)$ non ha radici in $\mathbb{Q}$. Le possibili radici razionali di $f(X)$ sono 1 o -1, ma $f(1) = 4$ e $f(-1) = -2$. Dunque $f(X)$ è il polinomio minimo di α.

(ii) *Dopo aver osservato che $\beta = \alpha^2 + \alpha$ è algebrico su $\mathbb{Q}$, si calcoli* $[\mathbb{Q}(\beta] : \mathbb{Q}]$. β è algebrico su $\mathbb{Q}$ perché prodotto e somma di algebrici su $\mathbb{Q}$ è algebrico su $\mathbb{Q}$. Poiché $\mathbb{Q}[\alpha]$ è un sottoanello di $\mathbb{C}$, $\beta \in \mathbb{Q}[\alpha]$. Dunque $\mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha]$, e

$$3 = [\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}[\beta]] \cdot [\mathbb{Q}[\beta] : \mathbb{Q}].$$

Dunque $[\mathbb{Q}[\beta] : \mathbb{Q}]$ o è 1 o 3, ma non può essere 1 perché altrimenti $\beta \in \mathbb{Q}$ e α sarebbe radice di $X^2 + X - \beta \in \mathbb{Q}[X]$ che ha grado 2. Quindi $[\mathbb{Q}[\beta] : \mathbb{Q}] = 3$.

Estensioni di campi

ESERCIZIO: Siano K un campo, $L = K(t)$ (dove t è una variabile su K), e $F = X^2 - t \in L[X]$.

(i) *Si provi che F è irriducibile.* Avendo F grado 2, esso è irriducibile se e solo se non ha radici in L. Se $f(t)/g(t) \in L$ fosse una radice di F, $f(t)^2 = t \cdot g(t)^2$. Ciò è impossibile: siccome $g(t) \neq 0$, anche $f(t) \neq 0$; siano $f(t) = \sum_{i=d}^{e} a_i t^i$ e $g(t) = \sum_{i=m}^{n} b_i t^i$ con $a_d, b_m \neq 0$. Se $m \geq d$, l'uguaglianza in rosso direbbe che $a_d^2 = 0$ $(2d < 2m + 1)$; Se $m < d$, l'uguaglianza in rosso direbbe che $b_m^2 = 0$ $(2m + 1 < 2d)$. Dunque F è irriducibile.

(ii) *Se $K = \mathbb{Z}_2$, si fattorizzi F nel suo campo di spezzamento su L.* Avendo F grado 2, il suo campo di spezzamento su L è $L' = L[\sqrt{t}]$. Siccome la caratteristica di L' è 2, in $L'[X]$ si ha:

$$X^2 - t = (X - \sqrt{t})^2.$$

Ideali massimali

ESERCIZIO: Sia A un anello, e $x \in A$. Allora

$$x \in U(A) \Leftrightarrow x \text{ non è contenuto in alcun ideale massimale di } A.$$

Se $x \in U(A)$, allora $(x) = A$, quindi "$\Rightarrow$" è chiaro. Per il viceversa, supponiamo per assurdo che $x \notin U(A)$. Allora (x) sarebbe un ideale proprio di A, quindi il seguente insieme non è vuoto:

$$\mathcal{F} = \{I \text{ ideali propri contenenti } x\}$$

Ora abbiamo bisogno del lemma di Zorn, che ricordiamo:

Se X è un insieme non vuoto, parzialmente ordinato,
tale che ogni sua catena ammette un maggiorante in X,
allora X contiene almeno un elemento massimale.

Ideali massimali

... Abbiamo già osservato che $\mathcal{F}$ è un insieme non vuoto, inoltre è dotato dell'ordine parziale dato dall'inclusione. Una catena C di $\mathcal{F}$ è un insieme totalmente ordinato di ideali propri di A contenenti l'elemento x: quindi se I e J appartengono a C, o $I \subseteq J$ oppure $J \subseteq I$. Il che implica che

$$Y = \bigcup_{I \in C} I$$

è un ideale di A. Inoltre, Y è proprio e contiene x, dunque Y è un maggiorante di C in $\mathcal{F}$. Dunque $\mathcal{F}$ contiene almeno un elemento massimale M; tale M è un ideale massimale contenente x, una contraddizione.

Ideali massimali

ESERCIZIO: Sia A un anello, $x \in A$ un elemento nilpotente e $u \in U(A)$. Allora $x + u \in U(A)$.

Sia $J \subseteq A$ un qualunque ideale massimale, e $N \in \mathbb{N}$ tale che $x^N = 0$. Siccome $x^N = 0 \in J$, e J è radicale, x appartiene a J. Dunque x appartiene a tutti gli ideali massimali di A. Se per assurdo $x + u$ non fosse invertibile, allora dovrebbe appartenere a un ideale massimale $I \subseteq A$ per l'esercizio precedente. Ma per quanto appena detto anche $x \in I$, dunque $u = (x + u) - x$ apparterrebbe a I. Allora I non sarebbe proprio, che è assurdo.

Caratteristica

ESERCIZIO: Sia A un anello di caratteristica $n > 0$. Si provi che, se $x \in A$, allora $\pi(x)|n$ (si ricordi che A è un gruppo Abeliano).

Poiché A ha caratteristica n,

$$n \cdot 1_A = \underbrace{1_A + \ldots + 1_A}_{n \text{ volte}} = 0.$$

Dunque $n \cdot x = n \cdot (1_A x) = (n \cdot 1_A)x = 0x = 0$. Quindi $\pi(x)|n$.

Caratteristica

ESERCIZIO: Provare che non si può dare una struttura di campo a $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.

Se per assurdo si potesse, sia K un tale campo. Avendo cardinalità 16, K avrebbe caratteristica 2. Ma G ha elementi di periodo 4 (per esempio $(0, 0, 1)$) e ciò contraddice l'esercizio precedente.