

# Tutorati di algebra 2

February 5, 2025

## 1 Tutorato 1

**Esercizio 1.** Sia  $\phi$  l'omomorfismo di gruppi

$$\phi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^3, e_1 \mapsto (10, 2, -14), e_2 \mapsto (-6, -2, 42)$$

e sia  $G$  il gruppo quoziente  $\mathbb{Z}^3 / \text{Im}(\phi)$ . Si calcoli il numero di sottogruppi di ordine 2 e di ordine 4 di  $G$ .

**Dimostrazione**

—

Given:

The homomorphism  $\phi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^3$  is defined by:

$$\phi(e_1) = \begin{pmatrix} 10 \\ 2 \\ -14 \end{pmatrix}, \quad \phi(e_2) = \begin{pmatrix} -6 \\ -2 \\ 42 \end{pmatrix}$$

Matrix Representation  $A$ :

$$A = \begin{pmatrix} 10 & -6 \\ 2 & -2 \\ -14 & 42 \end{pmatrix}$$

—

Objective:

Find invertible integer matrices  $P$  and  $Q$  such that  $D = PAQ$  is diagonal (Smith normal form), and write down the elementary matrices used at each step.

—

Swap  $R1$  and  $R2$ .

Elementary Matrix  $E_1$ :

$$E_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Updated Matrix  $A_1$ :

$$A_1 = E_1 A = \begin{pmatrix} 2 & -2 \\ 10 & -6 \\ -14 & 42 \end{pmatrix}$$

Step 2: Eliminate Entry Below Pivot in Column 1

Elementary Row Operation:

$$R_2 \leftarrow R_2 - 5R_1$$

Elementary Matrix  $E_2$ :

$$E_2 = \begin{pmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Updated Matrix  $A_2$ :

$$A_2 = E_2 A_1 = \begin{pmatrix} 2 & -2 \\ 0 & 4 \\ -14 & 42 \end{pmatrix}$$

Step 3: Eliminate Entry Below Pivot in Column 1

Elementary Row Operation:

$$R_3 \leftarrow R_3 + 7R_1$$

Elementary Matrix  $E_3$ :

$$E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 7 & 0 & 1 \end{pmatrix}$$

Updated Matrix  $A_3$ :

$$A_3 = E_3 A_2 = \begin{pmatrix} 2 & -2 \\ 0 & 4 \\ 0 & 28 \end{pmatrix}$$

Step 4: Eliminate Entry Below Pivot in Column 2

Elementary Row Operation:

$$R_3 \leftarrow R_3 - 7R_2$$

Elementary Matrix  $E_4$ :

$$E_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -7 & 1 \end{pmatrix}$$

Updated Matrix  $A_4$ :

$$A_4 = E_4 A_3 = \begin{pmatrix} 2 & -2 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}$$

—  
Step 5: Eliminate Off-Diagonal Entry in Position (1,2)

Elementary Column Operation:

$$C2 \leftarrow C2 + 1 \times C1$$

Elementary Matrix  $Q_1$ :

$$Q_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Updated Matrix  $D = A_4 Q_1$ :

$$D = A_4 Q_1 = \begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}$$

$$D = PAQ = \begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}$$

—  
By the Fundamental Theorem of Finitely Generated Abelian Groups,  $G$  is isomorphic to:

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$$

Sottogruppi di ordine 2 in  $G$ :

$$\{(a, b, c) \in G : 2a = 0 \pmod{2}, 2b = 0 \pmod{4}, 2c = 0\} \Rightarrow \{(0, 0, 0), (1, 0, 0), (0, 2, 0), (1, 2, 0)\}$$

$$|\langle (1, 0, 0), (0, 2, 0), (1, 2, 0) \rangle| = 3$$

Sottogruppi di ordine 4 in  $G$ :

$$\{(a, b, c) \in G : b \in \{1, 3\}, c = 0\}$$

$$\text{Generati da: } \{(0, 1, 0), (1, 1, 0), (1, 3, 0)\}$$

$$|\langle (0, 1, 0), (1, 1, 0), (1, 3, 0) \rangle| = 3$$

□

**Esercizio 2.** Trovare una base per il gruppo abeliano dato dalle soluzioni intere del sistema di equazioni  $x + 2y + 3z = 0, x + 4y + 9z = 0$ , e lo si descriva come prodotto di gruppi ciclici.

**Dimostrazione**

$$\left( \begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 1 & 4 & 9 & 0 \end{array} \right) \square \times (-1) \stackrel{?}{R_2 - R_1} \rightarrow R_2 \left( \begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & 2 & 6 & 0 \end{array} \right)$$

$$\begin{cases} x_1 + 2 \cdot x_2 + 3 \cdot x_3 = 0 \\ 2 \cdot x_2 + 6 \cdot x_3 = 0 \end{cases}$$

- Find the variable  $x_2$  from the equation 2 of the system (1):

$$2x_2 = -6x_3$$

$$x_2 = -3x_3$$

Find the variable  $x_1$  from the equation 1 of the system (1):

$$x_1 = -2x_2 - 3x_3 = -2 \cdot (-3x_3) - 3x_3 = 3x_3$$

$$x_1 = 3x_3$$

$$x_2 = -3x_3$$

$$x_3 = x_3$$

General Solution  $\bar{x} : X = \begin{pmatrix} 3x_3 \\ -3x_3 \\ x_3 \end{pmatrix}$  The solution set:  $\left\{ x_3 \cdot \begin{pmatrix} 3 \\ -3 \\ 1 \end{pmatrix} \right\}$

□

**Esercizio 3.** Si utilizzino operazioni elementari per righe e colonne nell'anello  $\mathbb{Z}[i]$  degli interi Gaussiani per diagonalizzare la matrice

$$\begin{bmatrix} 3 & 2+i \\ 2-i & 9 \end{bmatrix}$$

### Dimostrazione

Given Matrix:

$$A = \begin{pmatrix} 3 & 2+i \\ 2-i & 9 \end{pmatrix}$$

Objective:

Use elementary row and column operations over  $\mathbb{Z}[i]$  to diagonalize  $A$  (find its Smith normal form). We will:

- Use the element with the smallest norm as the pivot. - Apply the Euclidean algorithm in  $\mathbb{Z}[i]$ . - Provide all the elementary matrices used at each step.

Step 1: Compute Norms and Choose Pivot

Compute the norms of the elements:

$$- N(3) = 3^2 = 9 - N(2+i) = 2^2 + 1^2 = 5 - N(2-i) = 2^2 + (-1)^2 = 5 - N(9) = 9^2 = 81$$

Smallest Norm:  $N(2+i) = 5$

Action: Swap columns to bring  $2+i$  to position  $(1,1)$ .

Elementary Operation 1: Swap Columns 1 and 2

Elementary Column Matrix  $Q_1$ :

$$Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Updated Matrix  $A_1$ :

$$A_1 = AQ_1 = \begin{pmatrix} 2+i & 3 \\ 9 & 2-i \end{pmatrix}$$

Step 2: Eliminate Entry Below Pivot in Column 1

Objective: Use the Euclidean algorithm to find  $k \in \mathbb{Z}[i]$  such that:

$$9 = k(2+i) + r \quad \text{with} \quad N(r) < N(2+i)$$

Division in  $\mathbb{Z}[i]$ :

Compute  $k$  and  $r$ :

$$-k = 4 - 2i - r = -1$$

Verification:

$$(4-2i)(2+i) = 10 \implies 9 - 10 = -1$$

Elementary Row Operation:

$$R_2 \leftarrow R_2 - (4-2i)R_1$$

Elementary Row Matrix  $P_2$ :

$$P_2 = \begin{pmatrix} 1 & 0 \\ -(4-2i) & 1 \end{pmatrix}$$

Updated Matrix  $A_2$ :

$$A_2 = P_2 A_1 = \begin{pmatrix} 2+i & 3 \\ -1 & -10+5i \end{pmatrix}$$

Step 3: Swap Rows to Bring Smallest Norm Pivot to Position  $(1,1)$

Compute norms:

$$-N(-1) = 1 - N(2+i) = 5$$

Action: Swap rows to bring  $-1$  to position  $(1,1)$ .

Elementary Row Matrix  $P_1$ :

$$P_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Updated Matrix  $A_3$ :

$$A_3 = P_1 A_2 = \begin{pmatrix} -1 & -10 + 5i \\ 2 + i & 3 \end{pmatrix}$$

—  
Step 4: Eliminate Entry Below Pivot in Column 1

Compute  $k$ :

$$k = \frac{2+i}{-1} = -(2+i)$$

Elementary Row Operation:

$$R_2 \leftarrow R_2 - kR_1 = R_2 + (2+i)R_1$$

Elementary Row Matrix  $P_3$ :

$$P_3 = \begin{pmatrix} 1 & 0 \\ 2+i & 1 \end{pmatrix}$$

Compute Updated Row  $R_2$ :

$$R_2 = (2+i, 3) + (2+i)(-1, -10+5i) = (0, -22)$$

Updated Matrix  $A_4$ :

$$A_4 = P_3 A_3 = \begin{pmatrix} -1 & -10 + 5i \\ 0 & -22 \end{pmatrix}$$

—  
Step 5: Eliminate Entry Above Pivot in Column 2

Compute  $k$ :

$$k = \frac{-10+5i}{-1} = 10-5i$$

$$Q_2 = \begin{pmatrix} 1 & -(10-5i) \\ 0 & 1 \end{pmatrix}$$

Updated Matrix  $D$ :

$$D = A_4 Q_2 = \begin{pmatrix} -1 & 0 \\ 0 & -22 \end{pmatrix}$$

—  
Final Diagonal Matrix:

$$D = \begin{pmatrix} -1 & 0 \\ 0 & -22 \end{pmatrix}$$

For clarity, we can multiply rows or columns by  $-1$  (which is a unit in  $\mathbb{Z}[i]$ ) to get positive entries:

$$D' = \begin{pmatrix} 1 & 0 \\ 0 & 22 \end{pmatrix}$$

□

**Esercizio 4.** In  $G = \mathbb{R} \setminus \{-1\}$  si consideri l'operazione  $*$  definita da  $a * b = ab + a + b$  per ogni  $a, b \in G$ .

- (1) Dimostrare che  $(G, *)$  è un gruppo.
- (2) Dimostrare che  $H = \{h \in G \mid h > -1\}$  è un sottogruppo di  $(G, *)$ .
- (3) Il sottoinsieme  $K = \{k \in G \mid -2 < k \leq 0\}$  è un sottogruppo di  $(G, *)$ ?

**Dimostrazione**

□

**Esercizio 5.** Siano  $\frac{r}{s}, \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$  con  $MCD(r, s) = MCD(m, n) = 1$ . Dimostrare che nel gruppo  $(\mathbb{Q}, +)$  vale

$$\left\langle \frac{r}{s}, \frac{m}{n} \right\rangle = \left\langle \frac{MCD(r, m)}{\text{mcm}(s, n)} \right\rangle.$$

Se ne deduca che per ogni sottoinsieme finito  $X$  di  $(\mathbb{Q}, +)$  il sottogruppo  $\langle X \rangle$  è ciclico. Mostrare che  $(\mathbb{Q}, +)$  possiede sottogruppi propri non ciclici.

**Dimostrazione**

*Parte 1: Dimostrazione dell'uguaglianza dei sottogruppi*

Sia  $d = \text{mcm}(s, n)$ . Poiché  $s$  e  $n$  dividono  $d$ , possiamo scrivere:

$$\frac{r}{s} = \frac{r \cdot \frac{d}{s}}{d}, \quad \frac{m}{n} = \frac{m \cdot \frac{d}{n}}{d}.$$

Definiamo:

$$r' = r \cdot \frac{d}{s}, \quad m' = m \cdot \frac{d}{n}.$$

Notiamo che  $r'$  e  $m'$  sono interi.

Il sottogruppo generato da  $\frac{r}{s}$  e  $\frac{m}{n}$  è dato da:

$$\left\langle \frac{r}{s}, \frac{m}{n} \right\rangle = \left\{ k_1 \cdot \frac{r}{s} + k_2 \cdot \frac{m}{n} \mid k_1, k_2 \in \mathbb{Z} \right\}.$$

Sostituendo le espressioni trovate:

$$k_1 \cdot \frac{r}{s} + k_2 \cdot \frac{m}{n} = \frac{k_1 r' + k_2 m'}{d}.$$

Il numeratore  $N$  è una combinazione lineare intera di  $r'$  e  $m'$ :

$$N = k_1 r' + k_2 m'.$$

Notiamo che:

-  $\text{gcd}(r, s) = 1$  implica  $\text{gcd}(r, d/s) = 1$ , quindi  $\text{gcd}(r, r') = 1$ . - Analogamente,  $\text{gcd}(m, m') = 1$ .

Calcoliamo  $\text{gcd}(r', m')$ . Poiché  $r'$  e  $m'$  sono multipli di  $r$  e  $m$ , rispettivamente, e  $r$  e  $m$  possono avere un fattore comune  $g = \text{gcd}(r, m)$ , abbiamo:

$$\text{gcd}(r', m') = \text{gcd}\left(r \cdot \frac{d}{s}, m \cdot \frac{d}{n}\right) = \frac{d}{\text{mcm}(s, n)} \cdot \text{gcd}(r, m) = \frac{d}{d} \cdot g = g.$$

Quindi, il numeratore  $N$  è multiplo di  $g$ , e possiamo scrivere:

$$N = g \cdot \ell, \quad \ell \in \mathbb{Z}.$$

Pertanto, ogni elemento del sottogruppo è della forma:

$$\frac{N}{d} = \frac{g \cdot \ell}{d} = \ell \cdot \frac{g}{d}.$$

Abbiamo dimostrato che:

$$\left\langle \frac{r}{s}, \frac{m}{n} \right\rangle \subseteq \left\langle \frac{g}{d} \right\rangle = \left\langle \frac{\gcd(r, m)}{\text{mcm}(s, n)} \right\rangle.$$

*Parte 2: Dimostrazione dell'inclusione inversa*

Dobbiamo mostrare che  $\frac{g}{d}$  può essere espresso come combinazione lineare intera di  $\frac{r}{s}$  e  $\frac{m}{n}$ .

Consideriamo l'equazione diofantea:

$$ar' + bm' = g, \quad a, b \in \mathbb{Z}.$$

Poiché  $\gcd(r', m') = g$ , l'equazione ha soluzioni intere.

Sia  $(a_0, b_0)$  una soluzione particolare dell'equazione. Allora:

$$\frac{g}{d} = \frac{a_0 r' + b_0 m'}{d} = a_0 \cdot \frac{r}{s} + b_0 \cdot \frac{m}{n}.$$

Quindi:

$$\left\langle \frac{g}{d} \right\rangle \subseteq \left\langle \frac{r}{s}, \frac{m}{n} \right\rangle.$$

Unendo le due inclusioni, otteniamo:

$$\left\langle \frac{r}{s}, \frac{m}{n} \right\rangle = \left\langle \frac{\gcd(r, m)}{\text{mcm}(s, n)} \right\rangle.$$

*Deduzione: Ogni sottogruppo finitamente generato di  $(\mathbb{Q}, +)$  è ciclico*

Sia  $X = \left\{ \frac{r_1}{s_1}, \frac{r_2}{s_2}, \dots, \frac{r_k}{s_k} \right\} \subset \mathbb{Q}$  con  $\gcd(r_i, s_i) = 1$ .

Sia  $d = \text{mcm}(s_1, s_2, \dots, s_k)$ .

Per ogni  $i$ , scriviamo:

$$\frac{r_i}{s_i} = \frac{r_i \cdot \frac{d}{s_i}}{d}.$$

Definiamo  $r'_i = r_i \cdot \frac{d}{s_i}$ , che è un intero.

Calcoliamo  $g = \gcd(r'_1, r'_2, \dots, r'_k)$ .

Allora:

$$\langle X \rangle = \left\{ \frac{\sum_{i=1}^k k_i r'_i}{d} \mid k_i \in \mathbb{Z} \right\} = \left\{ \frac{g \cdot \ell}{d} \mid \ell \in \mathbb{Z} \right\} = \left\langle \frac{g}{d} \right\rangle.$$

Il sottogruppo  $\langle X \rangle$  è generato da  $\frac{a}{d}$ , quindi è ciclico.

*Constructing a Proper Non-Cyclic Subgroup of  $(\mathbb{Q}, +)$*

Example: Consider the subgroup  $H$  of  $(\mathbb{Q}, +)$  defined by:

$$H = \left\{ \frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0} \right\}$$

This subgroup consists of all rational numbers whose denominators (in lowest terms) are powers of 2. These are known as dyadic rationals .

Properties of the Subgroup  $H$

1.  $H$  is a Subgroup of  $(\mathbb{Q}, +)$

To show that  $H$  is a subgroup, we verify the subgroup criteria:

- Closure under addition:

Take any two elements  $\frac{a}{2^n}, \frac{b}{2^m} \in H$ . Their sum is:

$$\frac{a}{2^n} + \frac{b}{2^m} = \frac{a2^m + b2^n}{2^{n+m}} = \frac{c}{2^{n+m}}, \text{ where } c = a2^m + b2^n \in \mathbb{Z}$$

Since  $n + m \geq 0$  and  $c \in \mathbb{Z}$ , the sum is in  $H$ .

- Existence of inverses:

For any  $\frac{a}{2^n} \in H$ , its inverse is  $-\frac{a}{2^n} \in H$ , since  $-a \in \mathbb{Z}$ .

- Contains the identity element:

When  $a = 0$ ,  $\frac{0}{2^n} = 0 \in H$ .

2.  $H$  is a Proper Subgroup of  $(\mathbb{Q}, +)$

- Properness:

There exist rational numbers not in  $H$ . For example,  $\frac{1}{3} \notin H$ , since 3 is not a power of 2.

3.  $H$  is Not Cyclic

Suppose, for contradiction, that  $H$  is cyclic. Then there exists an element  $q \in H$  such that:

$$H = \langle q \rangle = \{nq \mid n \in \mathbb{Z}\}$$

Let  $q = \frac{a}{2^n}$  for some  $a \in \mathbb{Z}, n \geq 0$ . Then the elements generated by  $q$  are:

$$nq = n \cdot \frac{a}{2^n} = \frac{na}{2^n}$$

Key Observation:

- The denominators of all elements in  $\langle q \rangle$  are fixed at  $2^n$ . - However,  $H$  contains elements with denominators  $2^k$  for all  $k \geq 0$ .

*Contradiction:*

Consider the element  $\frac{1}{2^{n+1}} \in H$ . We need to determine if  $\frac{1}{2^{n+1}}$  can be expressed as  $nq$  for some  $n \in \mathbb{Z}$ :

$$nq = \frac{na}{2^n} = \frac{1}{2^{n+1}}$$

This implies:

$$na = \frac{1}{2}$$

But  $na$  is an integer, while  $\frac{1}{2}$  is not. Thus,  $\frac{1}{2^{n+1}}$  cannot be generated by  $q$ .

□