Istituzioni di Algebra e Geometria

Prova scritta di Algebra

25 Giugno 2020

Istruzioni.

- Scegliete i 3 esercizi che vi piacciono di più tra i 5 proposti qui sotto.
- Risolvete i 3 esercizi scelti: ognuno vale 10 punti, per un massimo di 30 punti. Scrivete esplicitamente quali esercizi avete scelto: correggerò SOLO quei 3.
- Scrivete la soluzione degli esercizi in maniera chiara e ordinata e MOTIVANDO OGNI RISPOSTA.
- Durante la prova non si possono utilizzare fogli personali, appunti, libri, calcolatrici.
- Alla fine della prova seguite le istruzioni e caricate il vostro elaborato. Poi, ENTRO 10 MINUTI dalla fine della prova, allegate una foto o una scannerizzazione della stessa prova tramite portale della didattica, caricandola su "consegna elaborati".

→ vedi sotto

1. (a) Siano X, Y, G tre insiemi e si considerino

$$G^Y = \{f \mid f : Y \to G\}, \quad G^X = \{g \mid g : X \to G\};$$

infine, sia fissata un'applicazione suriettiva $\alpha : X \to Y$. Si definisca quindi l'applicazione

$$\begin{aligned} \chi : G^Y &\to G^X \\ f &\mapsto f \circ \alpha. \end{aligned}$$

Dimostrare che χ è un'applicazione iniettiva.

(b) Supponiamo adesso che G sia un gruppo moltiplicativo. Date $g, h \in G^X$ definiamo

$$\begin{aligned} gh\colon X &\to G \\ a &\mapsto g(a)h(a). \end{aligned}$$

Verificare che G^X con tale operazione è un gruppo.

(c) Nelle ipotesi del punto (b) qui sopra, verificare che G^X è abeliano se e solo se G è abeliano.

→ queste 2 parti sono l'esercizio #4 foglio 2

(a) χ é iniettiva:

siano $f_1, f_2 \in G^Y$ t.c. $\chi(f_1) = \chi(f_2)$

$\iff f_1 \circ \alpha = f_2 \circ \alpha$ come elementi di G^X

sia $y \in Y$ qualsiasi, allora per la suriettività di α, $\exists\ x \in X$ t.c. $y = \alpha(x)$

$$\implies f_1(y) = f_1(\alpha(x)) = (f_1 \circ \alpha)(x)$$
$$= (f_2 \circ \alpha)(x) = f_2(\alpha(x)) = f_2(y)$$

cioé $f_1 = f_2$ ✓

→ vedi sotto

2. Nel gruppo simmetrico S_8 si considerino le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 & 8 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 2 & 5 & 1 & 8 & 7 \end{pmatrix}.$$

(a) Decomporre $\alpha\beta$ in un prodotto di cicli disgiunti.

(b) Calcolare $\operatorname{sgn}(\alpha\beta)$ e $\operatorname{ord}(\alpha\beta)$.

(c) Esistono cicli in S_8 di ordine 12?

→ questo è l'esercizio # 11 foglio 5

3. Sia A un anello commutativo con unità e I un suo ideale. Il radicale di I è

$$\sqrt{I} = \{ \ a \in A \mid \exists \ n \in \mathbb{N} \text{ tale che } a^n \in I \ \}.$$

(a) Verificare che $I \subseteq \sqrt{I}$.

(b) Dimostrare che se $a \in \sqrt{I}$ allora esiste $N \in \mathbb{Z}$ tale che $a^m \in I$ per ogni $m \geq N$.

(c) Verificare che se $a, b \in \sqrt{I}$ allora anche $-a$ e $a + b$ sono in $\sqrt{I}$, e dedurre che $\sqrt{I}$ è un ideale.

→ questo è uguale all'esercizio # 11 foglio 6

4. Siano dati i gruppi $G = \mathbb{Z}_3 \times \mathbb{Z}_4$ e $H = \mathbb{Z}_2 \times \mathbb{Z}_6$.

(a) Esiste un isomorfismo dei gruppi additivi G e H?

(b) Elencare gli elementi dei gruppi moltiplicativi G^* e H^*.

(c) Esiste un isomorfismo dei gruppi moltiplicativi G^* e H^*?

vedi sotto anche se questo esercizio è
→ praticamente uguale al # 5 foglio 7

5. Si consideri il polinomio $p(x) = x^2 + x - 2 \in \mathbb{Q}[x]$ e sia $I = (p(x))$.

(a) Verificare che I non è né massimale, né primo.

(b) Determinare due ideali distinti J' e J'' contenenti I e tali che $J' + J'' = \mathbb{Q}[x]$.

(c) Calcolare gli zero–divisori di $\mathbb{Q}[x]/I$.

② (a) Calcolo $\alpha\beta$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 2 & 5 & 1 & 8 & 7 \\ 4 & 2 & 1 & 5 & 3 & 7 & 8 & 6 \end{pmatrix} \begin{array}{l} \circlearrowright \beta \\ \circlearrowright \alpha \end{array}$$

$$\Longrightarrow \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 1 & 5 & 3 & 7 & 8 & 6 \end{pmatrix}$$

$$= \underbrace{(1\,4\,5\,3)}_{\sigma_1}\underbrace{(6\,7\,8)}_{\sigma_2}$$

(b) $\text{ord}(\alpha\beta) = \text{mcm}(\text{ord}(\sigma_1), \text{ord}(\sigma_2)) = \text{mcm}(4,3) = 12$

Per calcolare il segno decompongo i cicli σ_1 e σ_2 in trasposizioni:

$\sigma_1 = (1\,4\,5\,3) = (1\,3)(1\,5)(1\,4)$

$\Longrightarrow \text{sgn}(\sigma_1) = -1$ (σ_1 é dispari)

$\sigma_2 = (6\,7\,8) = (6\,8)(6\,7)$

$\Longrightarrow \text{sgn}(\sigma_2) = 1$ (σ_2 é pari)

In totale,

$\text{sgn}(\alpha\beta) = \text{sgn}(\sigma_1\sigma_2) = \text{sgn}(\sigma_1)\,\text{sgn}(\sigma_2) = -1$

(c) Ovviamente no, l'ordine di un ciclo corrisponde alla sua lunghezza, e in S_8 ci sono cicli di lunghezza massima 8.

(5)

$\mathbb{Q}$ campo $\Longrightarrow \mathbb{Q}[x]$ PID

(a) $I=(p(x))$ é primo $\Longleftrightarrow$ é massimale

$\Longleftrightarrow p(x)$ é irriducibile

ma $p(x)=(x-1)(x+2)$ ✓

(b) Definisco $J'=(x-1)$ e $J''=(x+2)$

chiaramente $J'\neq J''$; inoltre

$$p(x)=(x-1)(x+2)\in J' \Longrightarrow I\subseteq J'$$

$$p(x)=(x-1)(x+2)\in J'' \Longrightarrow I\subseteq J''$$

Resta da dim. $J'+J''=\mathbb{Q}[x]$:

per questo basta dim. che $1\in J'+J''$; ponendo

$$1=\alpha(x-1)+\beta(x+2) \rightsquigarrow \begin{cases}\alpha=-\frac{1}{3}\\ \beta=\frac{1}{3}\end{cases}$$

cioé $1=-\underbrace{\frac{1}{3}(x-1)}_{\in J'}+\underbrace{\frac{1}{3}(x+2)}_{\in J''}\in J'+J''$

$$\Longrightarrow J'+J''=\mathbb{Q}[x] \quad ✓$$

(c) Gli zero-divisori in $\mathbb{Q}[x]/I$ sono le classi laterali

$f(x)+I\neq I=0_{\mathbb{Q}[x]/I}$ t.c. $\exists\ g(x)+I\neq I$ e

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

$\Longleftrightarrow f(x)\in\mathbb{Q}[x]$ é t.c. $f(x)\notin I$, ma $\exists\ g(x)\in\mathbb{Q}[x]$, $g(x)\notin I$ e $f(x)g(x)\in I$

$\Longleftrightarrow f(x)$ e $g(x)$ non sono multipli di $p(x)$, ma il prodotto sí.

$\Longrightarrow$ gli zero-divisori sono $\alpha(x-1)+I$ e $\beta(x+2)+I$ con $\alpha,\beta\in\mathbb{Q}$.

Istituzioni di Algebra e Geometria

Prova scritta di Algebra

10 Luglio 2020

Istruzioni.

- Scegliete i 3 esercizi che vi piacciono di più tra i 5 proposti qui sotto.
- Risolvete i 3 esercizi scelti: ognuno vale 10 punti, per un massimo di 30 punti. Scrivete esplicitamente quali esercizi avete scelto: correggerò SOLO quei 3.
- Scrivete la soluzione degli esercizi in maniera chiara e ordinata e MOTIVANDO OGNI RISPOSTA.
- Durante la prova non si possono utilizzare fogli personali, appunti, libri, calcolatrici.
- Alla fine della prova mostrate i fogli che avete scritto alla webcam, prima di chiudere tutto. Poi, ENTRO 10 MINUTI dalla fine della prova, allegate una foto o una scannerizzazione della stessa prova tramite portale della didattica, caricandola su "consegna elaborati".

→ queste 2 parti sono l'esercizio #9 foglio 2

1. Sia G un gruppo. Si ricordi che il centro di G è il sottoinsieme

$$Z(G) = \{ \, x \in G \mid gx = xg \; \forall \, g \in G \, \}.$$

   (a) Dimostrare che $Z(G)$ è un sottogruppo di G.
   (b) Dimostrare che $Z(G) = G$ se e solo se G è abeliano.
   (c) Determinare il centro del gruppo simmetrico $Z(S_n)$, per $n \geq 3$.

→ questa invece è l'esercizio #15 foglio 3

2. Sia $\alpha = 3 + i\sqrt{3} \in \mathbb{C}$.

   (a) Dimostrare che α è algebrico su $\mathbb{Q}$ e trovarne il polinomio minimo $p(x)$.
   (b) Spiegare perché $K = \mathbb{Q}[\alpha]$ è un campo, estensione algebrica di $\mathbb{Q}$ di dimensione 2.
   (c) Dimostrare perché K non può essere un'estensione di $\mathbb{R}$.

→ questo è identico all'esercizio #6 foglio 8, comq. vedi sotto

② (a) $\alpha \notin \mathbb{Q} \Longrightarrow$ il polinomio minimo ha grado almeno 2.

$\alpha = 3 + i\sqrt{3}$
$\alpha - 3 = i\sqrt{3}$
$\alpha^2 - 6\alpha + 9 = -3$
$\alpha^2 - 6\alpha + 12 = 0$

$\rightsquigarrow p(x) = x^2 - 6x + 12 \in \mathbb{Q}[x]$ ha α come radice
$\rightsquigarrow p(x)$ é il polinomio minimo di α su $\mathbb{Q}$.

(b) $K = \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ perché α é algebrico, come dimostrato nel punto (a), quindi K é un campo, estensione semplice di $\mathbb{Q}$ con α.
Inoltre $\dim_{\mathbb{Q}}(K) = [K : \mathbb{Q}] = \deg(p(x)) = 2$, il grado del polinomio minimo di α.

(c) K é contenuto nell'insieme degli elementi algebrici su $\mathbb{Q}$, che $\underbrace{\text{é numerabile}}$, quindi non puó contenere $\mathbb{R}$.

questo segue dal fatto che l'insieme dei polinomi a coefficienti razionali é numerabile, e ogni polinomio ha un numero finito di soluzioni.
Quindi gli elementi algebrici su $\mathbb{Q}$ sono una unione numerabile di insiemi finiti, che é numerabile.

→ questo è molto simile all'esercizio #5 foglio 6
la soluzione è cmq sotto

3. Si consideri il gruppo $\mathbb{Z}_{12}^*$ degli elementi invertibili di $\mathbb{Z}_{12}$, con l'usuale moltiplicazione indotta da $\mathbb{Z}$.

   (a) Elencare gli elementi di $\mathbb{Z}_{12}^*$ e scriverne la tabella di moltiplicazione.

   (b) Stabilire se il gruppo $\mathbb{Z}_{12}^*$ è isomorfo al gruppo additivo $\mathbb{Z}_2 \times \mathbb{Z}_2$, e in caso di risposta positiva scrivere esplicitamente un tale isomorfismo.

   (c) Stabilire se il gruppo $\mathbb{Z}_{12}^*$ è isomorfo al gruppo additivo $\mathbb{Z}_4$, e in caso di risposta positiva scrivere esplicitamente un tale isomorfismo.

→ vedi sotto

4. Sull'insieme $A = \mathbb{Z} \times \mathbb{Z}^*$ si definisca la relazione $\sim$ ponendo, per ogni $(a, b), (c, d) \in A$:

$$(a, b) \sim (c, d) \quad \text{se} \quad ad^2 - b^2c = 0.$$

   (a) Dimostrare che $\sim$ è una relazione di equivalenza.

   (b) Dimostrare che l'insieme quoziente $A/_\sim$ è un insieme infinito.
   (Suggerimento: se per assurdo $A/_\sim = \{[(a_1, b_1)]_\sim, \ldots, [(a_n, b_n)]_\sim\}$, allora ...)

   (c) Stabilire se la funzione

$$\begin{aligned} A/_\sim &\to \mathbb{C} \\ [(a,b)]_\sim &\mapsto a + ib \end{aligned}$$

   è ben definita.

→ vedi sotto

5. Si consideri la permutazione di S_6

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

   (a) Scrivere σ come prodotto di cicli disgiunti, e se ne calcoli il segno.

   (b) Calcolare quanti elementi contiene il sottogruppo $< \sigma >$ di S_6.

   (c) Data la permutazione

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix},$$

   calcolare i prodotti $\sigma\tau$ e $\tau\sigma$.

③ (a) $\bar{x} \in \mathbb{Z}_{12}$ è invertibile $\Longleftrightarrow$ MCD$(x, 12) = 1$

$\Longrightarrow \mathbb{Z}_{12}^* = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$

Tabella di moltiplicazione:

	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\overline{11}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\overline{11}$	$\bar{1}$	$\bar{5}$
$\overline{11}$	$\overline{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

(b) Chiaramente $|\mathbb{Z}_{12}^*| = |\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$

Dalla tabella sopra osserviamo che tutti gli elementi di $\mathbb{Z}_{12}^*$ hanno ordine 2, tranne $\bar{1}$ che ha ordine 1.
Lo stesso vale per gli elementi del gruppo additivo

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$$

L'isomorfismo cercato è

$$\begin{aligned} \varphi : \mathbb{Z}_{12}^* &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \bar{1} &\longmapsto (\bar{0}, \bar{0}) \\ \bar{5} &\longmapsto (\bar{1}, \bar{0}) \\ \bar{7} &\longmapsto (\bar{0}, \bar{1}) \\ \overline{11} &\longmapsto (\bar{1}, \bar{1}) \end{aligned}$$

Vale che:

$$\varphi(\bar{5} \cdot \bar{7}) = \varphi(\overline{11}) = (\bar{1}, \bar{1}) = (\bar{1}, \bar{0}) + (\bar{0}, \bar{1}) = \varphi(\bar{5}) + \varphi(\bar{7})$$

etc...

(in un esame dovete controllarle tutte ☺)

(c) Il gruppo additivo $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ contiene elementi di ordine maggiore di 2, ad esempio ord$(\bar{1}) = 4 \Longrightarrow \mathbb{Z}_{12}^* \not\cong \mathbb{Z}_4$.

(4) N.B. $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

(a) la relazione $\sim$ è:

riflessiva: $(a,b) \sim (a,b)$ perché $ab^2 - b^2a = 0$ ✓

simmetrica: $(a,b) \sim (c,d) \iff ad^2 - b^2c = 0$
$\iff cb^2 - d^2a = 0 \iff (c,d) \sim (a,b)$ ✓

transitiva: se $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$ allora

$ad^2 - b^2c = 0 \iff ad^2 = b^2c$

$cf^2 - d^2e = 0 \iff cf^2 = d^2e$

$\implies a\cancel{d^2}\cancel{c}f^2 = b^2\cancel{c}\cancel{d^2}e$

$af^2 = b^2e$, cioè $(a,b) \sim (e,f)$ ✓

(b) se per assurdo $A/_\sim$ fosse finito, diciamo $|A/_\sim| = n$, esisterebbero n coppie $(a_i, b_i) \in \mathbb{Z} \times \mathbb{Z}^*$ tali che

$$A/_\sim = \{[(a_1,b_1)]_\sim, [(a_2,b_2)]_\sim, \dots, [(a_n,b_n)]_\sim\}$$

Per trovare una contraddizione è sufficiente prendere una coppia $(c,d) \in \mathbb{Z} \times \mathbb{Z}^*$ tale che

$$cb_i^2 \neq d^2a_i \quad \forall i = 1 \dots n \quad ✓$$

(c) la funzione $f: A/_\sim \longrightarrow \mathbb{C}$
$$[(a,b)]_\sim \longmapsto a + ib$$

<u>non</u> è ben definita: ad esempio, $(1,2) \sim (4,4)$ ma ovviamente $1 + 2i \neq 4 + 4i$.

5

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix} = \underbrace{(1\,4)}_{\alpha}\underbrace{(2\,6\,3)}_{\beta}$

$\operatorname{sgn}(\alpha) = -1$

$\beta = (2\,6\,3) = (2\,3)(2\,6) \Longrightarrow \operatorname{sgn}(\beta) = 1$

$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta) = -1$

(b) $|\langle\sigma\rangle| = \operatorname{ord}(\sigma) = \operatorname{mcm}(\operatorname{ord}(\alpha), \operatorname{ord}(\beta)) = \operatorname{mcm}(2,3) = 6$

(c) $\sigma\tau = \begin{array}{cl} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 4 & 6 \\ 6 & 4 & 5 & 2 & 1 & 3 \end{pmatrix} & \begin{array}{l} \tau \\ \sigma \end{array} \end{array}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 1 & 3 \end{pmatrix} \left(= (1\,6\,3\,5)(2\,4) \right)$

$\tau\sigma = \begin{array}{cl} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \\ 3 & 6 & 1 & 2 & 4 & 5 \end{pmatrix} & \begin{array}{l} \sigma \\ \tau \end{array} \end{array}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 2 & 4 & 5 \end{pmatrix} \left(= (1\,3)(2\,6\,5\,4) \right)$

Istituzioni di Algebra e Geometria

Prova scritta di Algebra

15 Settembre 2020

Istruzioni.

- Scegliete i 3 esercizi che vi piacciono di più tra i 5 proposti qui sotto.
- Risolvete i 3 esercizi scelti: ognuno vale 10 punti, per un massimo di 30 punti. Scrivete esplicitamente quali esercizi avete scelto: correggerò SOLO quei 3.
- Scrivete la soluzione degli esercizi in maniera chiara e ordinata e MOTIVANDO OGNI RISPOSTA.
- Durante la prova non si possono utilizzare fogli personali, appunti, libri, calcolatrici.
- Alla fine della prova mostrate i fogli che avete scritto alla webcam, prima di chiudere tutto. Poi, ENTRO 10 MINUTI dalla fine della prova, allegate una foto o una scannerizzazione della stessa prova tramite portale della didattica, caricandola su "consegna elaborati".

→ vedi sotto

1. Sia $f(x) = x^3 + x^2 + 2 \in \mathbb{Z}[x]$. Si consideri la sua riduzione modulo p: $\overline{f}(x) \in \mathbb{Z}_p[x]$.
   (a) Dimostrare che per $p = 3$ il polinomio $\overline{f}(x) \in \mathbb{Z}_3[x]$ è irriducibile su $\mathbb{Z}_3$.
   (b) Dimostrare che per $p = 5$ il polinomio $\overline{f}(x) \in \mathbb{Z}_5[x]$ è irriducibile su $\mathbb{Z}_5$.
   (c) Dimostrare che invece $\overline{f}(x) \in \mathbb{Z}_7[x]$ è riducibile e trovarne i fattori irriducibili.

→ vedi sotto

2. Sia $k \in \mathbb{Z}$ un intero fissato, e si consideri l'insieme

$$A_k = \left\{ \begin{pmatrix} x & yk \\ y & x \end{pmatrix} \;\middle|\; x, y \in \mathbb{Q} \right\}.$$

   (a) Dimostrare che A_k è un sottoanello dell'anello $M(2, \mathbb{Q})$ delle matrici 2×2 a coefficienti in $\mathbb{Q}$ per ogni intero k.
   (b) Dimostrare che A_k è commutativo per ogni intero k.
   (c) Dimostrare che A_k è un dominio d'integrità se e solo se k non è un quadrato in $\mathbb{Z}$.

① Un polinomio di grado 3 è irriducibile su $A \iff$ non ha radici in A.

(a) Mostriamo che $\overline{f}(x)$ non ha radici in $\mathbb{Z}_3$:

$$\overline{f}(\overline{0}) = \overline{2} \neq \overline{0}$$
$$\overline{f}(\overline{1}) = \overline{1}^3 + \overline{1}^2 + \overline{2} = \overline{1} \neq \overline{0}$$
$$\overline{f}(\overline{2}) = \overline{2}^3 + \overline{2}^2 + \overline{2} = \overline{2} = \overline{0} \quad ✓$$

(b) Mostriamo che $\overline{f}(x)$ non ha radici in $\mathbb{Z}_5$:

$$\overline{f}(\overline{0}) = \overline{2} \neq \overline{0} \qquad \overline{f}(\overline{3}) = \overline{3} \neq \overline{0}$$
$$\overline{f}(\overline{1}) = \overline{4} \neq \overline{0} \qquad \overline{f}(\overline{4}) = \overline{2} \neq \overline{0} \quad ✓$$
$$\overline{f}(\overline{2}) = \overline{4} \neq \overline{0}$$

(c) Invece su $\mathbb{Z}_7$:

$$\overline{f}(\overline{0}) = \overline{2} \neq 0 \qquad \overline{f}(\overline{4}) = \overline{5}$$
$$\overline{f}(\overline{1}) = \overline{4} \qquad \overline{f}(\overline{5}) = \overline{5}$$
$$\longrightarrow \overline{f}(\overline{2}) = \overline{0} \quad (\overline{2} \text{ è radice}) \qquad \overline{f}(\overline{6}) = \overline{2}$$
$$\overline{f}(\overline{3}) = \overline{3}$$

$\Longrightarrow$ per Ruffini, $x - \overline{2}$ è un fattore di $x^3 + x^2 + \overline{2}$

Dividendo troviamo

$$x^3 + x^2 + \overline{2} = (x - \overline{2})(x^2 + \overline{3}x + \overline{6})$$

che è la scomposizione in fattori irriducibili, perché $\overline{g}(x) = x^2 + \overline{3}x + \overline{6}$ non ha radici:

$$\overline{g}(\overline{0}) = \overline{6} \qquad \overline{g}(\overline{4}) = \overline{6}$$
$$\overline{g}(\overline{1}) = \overline{3} \qquad \overline{g}(\overline{5}) = \overline{4}$$
$$\overline{g}(\overline{2}) = \overline{2} \qquad \overline{g}(\overline{6}) = \overline{4}$$
$$\overline{g}(\overline{3}) = \overline{3}$$

② (a) $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A_k$; A_k é un sottogruppo additivo: siano $\begin{pmatrix} x_1 & y_1 k \\ y_1 & x_1 \end{pmatrix}$ e $\begin{pmatrix} x_2 & y_2 k \\ y_2 & x_2 \end{pmatrix} \in A_k$, allora:

$$\begin{pmatrix} x_1 & y_1 k \\ y_1 & x_1 \end{pmatrix} - \begin{pmatrix} x_2 & y_2 k \\ y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 & (y_1 - y_2)k \\ y_1 - y_2 & x_1 - x_2 \end{pmatrix} \in A_k \quad \checkmark$$

Inoltre:

$$\begin{pmatrix} x_1 & y_1 k \\ y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & y_2 k \\ y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 x_2 + y_1 y_2 k & (x_1 y_2 + y_1 x_2)k \\ x_1 y_2 + x_2 y_1 & x_1 x_2 + y_1 y_2 k \end{pmatrix} \in A_k \quad \checkmark$$

(b) É sufficiente osservare che la formula del prodotto scritta nella parte (a) é completamente simmetrica rispetto agli indici ✓

(c) A_k é un dominio di integrità

$\Longleftrightarrow \nexists$ divisori dello zero, cioé $\nexists$

$$\begin{pmatrix} x_1 & y_1 k \\ y_1 & x_1 \end{pmatrix}, \begin{pmatrix} x_2 & y_2 k \\ y_2 & x_2 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ tali che}$$

$$\begin{pmatrix} x_1 & y_1 k \\ y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & y_2 k \\ y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 x_2 + y_1 y_2 k & (x_1 y_2 + y_1 x_2)k \\ x_1 y_2 + x_2 y_1 & x_1 x_2 + y_1 y_2 k \end{pmatrix} \overset{*}{=} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Se $k=0$, chiaramente A_0 non é un dominio di integrità, infatti:

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

Supponiamo $k \neq 0$.

($\Longrightarrow$) Se k é un quadrato in $\mathbb{Z}$, le 2 matrici $\begin{pmatrix} \sqrt{k} & k \\ 1 & \sqrt{k} \end{pmatrix}$ e $\begin{pmatrix} \sqrt{k} & -k \\ -1 & \sqrt{k} \end{pmatrix}$ sono divisori dello zero, quindi A_k non é un dominio di integrità:

$$\begin{pmatrix} \sqrt{k} & k \\ 1 & \sqrt{k} \end{pmatrix} \begin{pmatrix} \sqrt{k} & -k \\ -1 & \sqrt{k} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

($\Leftarrow$) Viceversa, se A_K ha divisori dello zero, dalla relazione $\textcircled{*}$ troviamo

$$\begin{cases} K y_1 y_2 + x_1 x_2 = 0 \\ x_1 y_2 + x_2 y_1 = 0 \end{cases}$$

supponiamo $y_1, y_2 \neq 0$:

$$\frac{x_1}{y_1} = -\frac{x_2}{y_2} \Longrightarrow K = -\frac{x_1 x_2}{y_1 y_2} = \left(\frac{x_1}{y_1}\right)^2 \text{ è un quadrato.}$$

se y_1 o $y_2 = 0$, troviamo una contraddizione.

→ questo esercizio è una variante dell'es. #9 foglio 2, che vi avevo proposto a lezione l'8/11/2023

3. Si ricordi che $A_n \leq S_n$ è il sottogruppo delle permutazioni pari del gruppo simmetrico S_n.

   (a) Sia $\sigma \in A_n$, con $n \geq 4$, tale che $\sigma(a) = b \neq a$: dimostrare che se $c, d \notin \{ a, b \}$ con $c \neq d$ allora dato il ciclo $\tau = (b\,c\,d)$ si ha che $\sigma\tau \neq \tau\sigma$.

   (b) Si ricordi che il centro di un gruppo G è il sottogruppo

   $$Z(G) = \{ x \in G \mid gx = xg \ \forall\, g \in G \}.$$

   Dimostrare che $Z(A_n) = \{ 1 \}$ per $n \geq 4$.

   (c) Determinare $Z(A_3)$.

→ questo è praticamente uguale all'esercizio #9 foglio 7, vedi sotto

4. Si consideri il polinomio $p(x) = x^2 - 2 \in \mathbb{Z}[x]$ e sia $I = (p(x))$ l'ideale generato da $p(x)$.

   (a) Dimostrare che I è un ideale primo.

   (b) Verificare che I non è massimale, trovando un ideale massimale J contenente I.

   (c) È vero o falso che tutti gli elementi non nulli di $\mathbb{Z}[x]/I$ sono invertibili? Perché?

→ queste 2 parti sono l'esercizio #18 foglio 4

5. Siano G e G' gruppi e sia $\varphi \in \mathrm{Hom}(G, G')$ un omomorfismo.

   (a) Dimostrare che se $K' \lhd G'$ è un sottogruppo normale, allora $\varphi^{-1}(K') \lhd G$ è un sottogruppo normale.

   (b) Dimostrare che se $H \leq G$ è un sottogruppo, allora $\varphi(H) \leq G'$ è un sottogruppo.

   (c) Dimostrare che se $K \lhd G$ è un sottogruppo normale e φ è un epimorfismo, allora $\varphi(K) \lhd G'$ è sottogruppo normale. Cosa non funzionerebbe se φ non fosse suriettivo?

→ questo lo abbiamo fatto a lezione il 30/10/2023

④ (a) I è primo perché $p(x)$ è irriducibile:
se $p(x) \mid f(x)g(x)$, necessariamente o $p \mid f$ oppure $p \mid g$ ✓

(b) Definiamo $J = (2, x)$ e mostriamo che
$$I \subsetneq J \subsetneq \mathbb{Z}[x]$$
siccome $x^2 - 2 = (-1) \cdot 2 + x \cdot x$, $p(x) \in J \Rightarrow I \subseteq J$.
D'altra parte $x \in J$ ma $x \notin I$, quindi il contenimento è stretto.

Se $J = \mathbb{Z}[x]$, avremmo $1 \in J$, ed esisterebbero $a(x), b(x) \in \mathbb{Z}[x]$ t.c. $1 = a(x) \cdot 2 + b(x) \cdot x$.
In particolare per $x = 0$ avremmo
$$1 = a(0) \cdot 2 \quad \text{↯} \quad \text{perché } a(0) \in \mathbb{Z}.$$
Resta da mostrare che J è massimale.
Sia $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots \in \mathbb{Z}[x]$
e sia
$$r_f = \begin{cases} 0 & \text{se } a_0 \text{ è pari} \\ 1 & \text{se } a_0 \text{ è dispari} \end{cases}$$
Definiamo l'omomorfismo di anelli
$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2, \quad f \longmapsto \overline{r_f}$$
φ è suriettivo ($\varphi(0) = \overline{0}$ e $\varphi(1) = \overline{1}$), inoltre
$$\begin{aligned} Ker(\varphi) &= \{ f(x) \in \mathbb{Z}[x] \mid \text{il termine noto } a_0 \text{ è pari} \} \\ &= \{ f(x) \in \mathbb{Z}[x] \mid a_0 = 2k,\ k \in \mathbb{Z} \} \\ &= \{ f(x) \in \mathbb{Z}[x] \mid f(x) = 2 \cdot k + x \cdot f'(x) \} = J \end{aligned}$$
$\Rightarrow$ per il teo di omo di anelli:
$$\mathbb{Z}[x]/J \cong \mathbb{Z}_2 \text{ che è un campo} \Rightarrow J \text{ è massimale.}$$

(c) $\mathbb{Z}[x]/I$ campo $\Leftrightarrow I$ è max, ma questo è falso,
quindi $\mathbb{Z}[x]/I$ contiene elementi non nulli non invertibili.