

1 Esercizi di Algebra

1.1 Sistemi di Numerazione (esercizi svolti)

Esercizio 1.1 *Scrivere l'intero 121 nelle basi 8 e 5*

Svolgimento. Applicando iterativamente l'algoritmo di divisione euclidea per 8, si ha:

$$121 = 15 \cdot 8 + 1$$

$$15 = 1 \cdot 8 + 7$$

$$1 = 0 \cdot 8 + 1.$$

I resti ottenuti dalle divisioni costituiscono le cifre in base otto, lette dall'ultima alla prima, dell'intero:

$$(121)_{10} = (171)_8.$$

Infatti si ha $121 = 1 \cdot 8^2 + 7 \cdot 8^1 + 1 \cdot 8^0$. □

Allo stesso modo si procede per scrivere l'intero in base 5:

$$121 = 24 \cdot 5 + 1$$

$$24 = 4 \cdot 5 + 4$$

$$4 = 0 \cdot 5 + 4;$$

$$(121)_{10} = (441)_5.$$

Infatti si ha $121 = 4 \cdot 5^2 + 4 \cdot 5^1 + 1 \cdot 5^0$. □

Esercizio 1.2 *Scrivere l'intero 89 nelle basi 2 e 3*

Svolgimento. Come nell'esercizio precedente, otteniamo le cifre dell'intero nelle basi volute, applicando iterativamente l'algoritmo di divisione euclidea per 2 e per 3:

In base due:

$$89 = 44 \cdot 2 + 1$$

$$44 = 22 \cdot 2 + 0$$

$$22 = 11 \cdot 2 + 0$$

$$11 = 5 \cdot 2 + 1$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 0 \cdot 2 + 1$$

$$(89)_{10} = (1011001)_2.$$

$$\text{Infatti } 89 = 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0. \quad \square$$

In base tre:

$$89 = 29 \cdot 3 + 2$$

$$29 = 9 \cdot 3 + 2$$

$$9 = 3 \cdot 3 + 0$$

$$3 = 1 \cdot 3 + 0$$

$$1 = 0 \cdot 3 + 1$$

$$(89)_{10} = (10022)_3.$$

$$\text{Infatti } 89 = 1 \cdot 3^4 + 0 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0. \quad \square$$

1.2 Sistemi di Numerazione (esercizi proposti)

Esercizio 1.3 Verificare, utilizzando l'algoritmo di divisione euclidea, che

$$(75)_{10} = (300)_5 = (203)_6. \quad \square$$

Esercizio 1.4 Scrivere l'intero 100 nelle basi due, tre e quattro. □

Esercizio 1.5 Scrivere 35 in base 17 e scrivere 17 in base 2. □

1.3 Massimo Comun Divisore (esercizi svolti)

Esercizio 1.6 Trovare il massimo comun divisore di 444 e 100.

Svolgimento. Utilizzando l'algoritmo di Euclide si ha:

$$444 = 100 \cdot 4 + 44$$

$$100 = 44 \cdot 2 + 12$$

$$44 = 12 \cdot 3 + 8$$

$$12 = 8 \cdot 1 + 4$$

$$8 = 4 \cdot 2 + 0$$

L'ultimo resto non nullo é il massimo comun divisore.

$$MCD(444, 100) = 4$$

□

Esercizio 1.7 *Trovare il massimo comun divisore di 220 e 121 e scriverlo come combinazione lineare a coefficienti interi di 220 e 121.*

Svolgimento. Utilizzando l'algoritmo di Euclide si ha:

$$220 = 121 \cdot 1 + 99$$

$$121 = 99 \cdot 1 + 22$$

$$99 = 22 \cdot 4 + 11$$

$$22 = 11 \cdot 2 + 0$$

L'ultimo resto non nullo é il massimo comun divisore.

$$MCD(220, 121) = 11$$

Esplicitando i resti nei passaggi dell'algoritmo, si ricava:

$$99 = 220 - 121$$

$$22 = 121 - 99 = 121 - 220 + 121 = 2 \cdot 121 - 220$$

$$11 = 99 - 22 \cdot 4 = (220 - 121) - (2 \cdot 121 - 220) \cdot 4$$

$$11 = 220 - 121 - 8 \cdot 121 + 4 \cdot 220$$

$$11 = 5 \cdot 220 - 9 \cdot 121$$

il che verifica l' *identità di Bezout*

□

Esercizio 1.8 *Stabilire se l'equazione diofantea*

$$35x + 28y = 14$$

ammette soluzioni.

Svolgimento. Utilizziamo l'algoritmo di Euclide per calcolare $MCD(35,28)$:

$$35 = 28 \cdot 1 + 7$$

$$28 = 7 \cdot 4 + 0$$

L'ultimo resto non nullo é 7, quindi il massimo comun divisore divide 14, e l'equazione ammette soluzioni.

□

1.4 Massimo Comun Divisore (esercizi proposti)

Esercizio 1.9 Utilizzando l'algoritmo di Euclide, trovare il massimo comun divisore delle seguenti coppie di interi:

$$(680, 324)$$

$$(2240, 1024)$$

$$(1134, 525)$$

e verificare l'identità di Bezout per la prima delle tre coppie, scrivendo il massimo comun divisore come combinazione lineare intera di 680 e 324.

□

Esercizio 1.10 Dire, motivando la risposta, quali delle seguenti equazione diofantee ammettono soluzioni:

$$324x + 81y = 26$$

$$324x + 81y = 27$$

$$36x + 90y = 54$$

□

Esercizio 1.11 Calcolare il minimo comune multiplo delle seguenti coppie di interi:

$$(120, 32)$$

$$(222, 259)$$

Suggerimento. Utilizzare la formula

$$mcm(a, b) = \frac{a \cdot b}{MCD(a, b)}$$

□

1.5 Criteri di Divisibilit  (esercizi svolti e proposti)

Esercizio 1.12 *Dimostrare che un intero n   divisibile per 9 se e solo se la somma delle sue cifre decimali   un multiplo di 9.*

Svolgimento. Sia

$$n = 10^m r_m + 10^{(m-1)} r_{m-1} + \dots + 10r_1 + r_0$$

la scrittura decimale di n . Gli interi r_m, \dots, r_1, r_0 sono i resti delle divisioni per 10 di n e quindi le sue cifre decimali. Si ha

$$n - (r_m + \dots + r_0) = (10^m r_m + \dots + 10r_1 + r_0) - (r_m + \dots + r_1 + r_0) = (10^m - 1)r_m + \dots + (10 - 1)r_1$$

$$n - (r_m + \dots + r_0) = (99\dots9)r_m + \dots + 9r_1 = 9(11\dots1r_m + \dots + r_1);$$

il secondo membro dell'ultima uguaglianza   un multiplo di nove, e quindi

$$n \equiv (r_m + \dots + r_0) \pmod{9};$$

la classe dei resti modulo 9 di n coincide con la classe dei resti modulo 9 della somma delle sue cifre decimali, e questo prova il criterio di divisibilit  per 9. \square

Esercizio 1.13 *Dimostrare che un intero n   divisibile per 5 se e solo se l'ultima cifra decimale   0 oppure 5.*

Svolgimento. Usando la stessa notazione dell'esercizio precedente,   sufficiente dimostrare che le classi dei resti modulo 5 di n e di r_0 coincidono, e quindi n   divisibile per 5 se e solo se r_0   divisibile per 5 (le uniche possibilit , per un numero a una cifra, sono appunto 0 e 5).

$$n - r_0 = 10^m r_m + \dots + 10r_1 = 5(2^m 5^{(m-1)} r_m + \dots + 2r_1)$$

$$n \equiv r_0 \pmod{5}$$

\square

Esercizio 1.14 *Dimostrare che un intero   divisibile per 2 se e solo se l'ultima cifra   pari.*

Suggerimento. Procedere come nell'esercizio 1.13

Esercizio 1.15 *Dimostrare che un intero   divisibile per 3 se e solo se la somma delle sue cifre decimali   divisibile per 3.*

Suggerimento. Procedere come nell'esercizio 1.12

1.6 Esercizi Svolti sulle Classi di Resti

Esercizio 1.16 Sia $n = 2379876328939$. Trovare il resto, nella divisione per 4, di n e di n^2 .

Svolgimento. Poiché $n - 39 = 2379876328900$ è multiplo di 100, e quindi è anche multiplo di 4, risulta:

$$n \equiv 39 \equiv 3 \pmod{4}.$$

Inoltre, siccome n è dispari, possiamo scrivere $n = 2k + 1$ per un opportuno intero k .

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$

$$n^2 - 1 = 4(k^2 + k)$$

$$n^2 \equiv 1 \pmod{4}$$

□

Esercizio 1.17 Calcolare il resto, nella divisione per 10, di 3^{51} .

Svolgimento. Innanzitutto osserviamo che

$$3^4 = 81 \equiv 1 \pmod{10}$$

e quindi

$$3^{51} = 3^{48} \cdot 3^3 = (3^4)^{12} \cdot 3^3 = (81)^{12} \cdot 27$$

$(81)^{12}$ è congruo a $(1)^{12} = 1$ modulo 10:

$$3^{51} \equiv 27 \pmod{10}$$

$$3^{51} \equiv 7 \pmod{10}$$

□

1.7 Esercizi Proposti sulle Classi di Resti

Esercizio 1.18 Calcolare il resto, nella divisione per 5, di 22^8 .

Suggerimento. $22^8 = (2^8) \cdot (11^2)^4$.

□

Esercizio 1.19 Calcolare il resto, nella divisione per 7, di 711^{27}

1.8 Funzione di Eulero, Elementi Invertibili, Divisori dello Zero (esercizi svolti)

Esercizio 1.20 Calcolare $\Phi(9)$.

Svolgimento. Gli interi minori di 9 e coprimi con 9 sono 1,2,4,5,7,8. Quindi $\Phi(9) = 6$ □

Esercizio 1.21 Calcolare $\Phi(640)$.

Svolgimento. Usiamo la formula

$$\Phi(n) = \Phi(p_1^{s_1} \dots p_h^{s_h}) = (p_1 - 1) \dots (p_h - 1) \cdot (p_1^{s_1-1} \dots p_h^{s_h-1}).$$

(dove $p_1^{s_1} \dots p_h^{s_h}$ è la scomposizione in fattori primi dell'intero n)

$$\Phi(640) = \Phi(2^7 \cdot 5) = 1 \cdot 4 \cdot 2^6 \cdot 5^0 = 256.$$

□

Esercizio 1.22 Calcolare $|\mathcal{U}(30)|$, il numero di elementi invertibili di Z_{30}

Svolgimento. Ricordando che un elemento di Z_n è invertibile se e solo se non nullo e coprimo con n , si tratta di contare il numero di interi minori di 30 e coprimi con 30, quindi:

$$|\mathcal{U}(30)| = \Phi(30) = \Phi(2 \cdot 3 \cdot 5) = 1 \cdot 2 \cdot 4 = 8$$

□

Esercizio 1.23 Calcolare i divisori dello zero di Z_{25} .

Svolgimento. Ricordando che un elemento di Z_n è divisore dello zero se e solo se non è coprimo con n , il loro numero è di $n - \Phi(n)$. Nel nostro caso è possibile un calcolo esplicito di tutti gli elementi cercati:

$$\{5, 10, 15, 20, 25\}.$$

(tutti gli interi minori o uguali di 25 e non coprimi con 25) □

1.9 Funzione di Eulero, Elementi Invertibili, Divisori dello Zero (esercizi proposti)

Esercizio 1.24 Calcolare il valore della funzione di Eulero Φ per gli interi 15, 24, 19, 240, 330, 1000.

Suggerimento. Usare la formula 1.21

Esercizio 1.25 Dire quanti sono gli elementi invertibili in Z_{144} e quanti sono quelli in Z_{143} .

Esercizio 1.26 Scrivere tutti gli elementi di $\mathcal{U}(18)$ e di $\mathcal{U}(28)$.

Esercizio 1.27 Trovare i divisori dello zero in Z_{27}

1.10 Sistemi di Equazioni Congruenziali (esercizi svolti)

Esercizio 1.28 Utilizzando il teorema cinese del resto, risolvere il seguente sistema di equazioni congruenziali:

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 3 \pmod{5} \end{cases}$$

Svolgimento. Dopo aver osservato che $MCD(9, 5) = 1$ e che quindi é possibile applicare il teorema cinese del resto, una soluzione c é data dalla formula

$$c = c_2 \cdot 7 \cdot 5 + c_1 \cdot 3 \cdot 9$$

dove c_1 é un inverso di 5 modulo 9 e c_2 é un inverso di 9 modulo 5.

$$9c_2 \equiv 1 \pmod{5};$$

$$5c_1 \equiv 1 \pmod{9}.$$

Quindi

$$c_1 = 2$$

$$c_2 = 4$$

e una soluzione é data da

$$c = 4 \cdot 7 \cdot 5 + 2 \cdot 3 \cdot 9 = 70 + 108 = 178$$

Le soluzioni allora sono tutte e sole del tipo

$$x = 178 + n45, n \in \mathbb{Z}.$$

Ad esempio, si lascia per esercizio il verificare che -2 é soluzione del sistema dato. \square

Esercizio 1.29 Utilizzando il teorema cinese del resto, risolvere il seguente sistema di equazioni congruenziali:

$$\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 2 \pmod{5} \end{cases}$$

Svolgimento. Essendo $MCD(6, 5) = 1$ si procede, come nell'esercizio precedente, innanzitutto a trovare gli inversi di 6 modulo 5, e di 5 modulo 6 rispettivamente.

$$6c_2 \equiv 1 \pmod{5}, \quad c_2 = 1;$$

$$5c_1 \equiv 1 \pmod{6}, \quad c_1 = 5.$$

Una soluzione é data da

$$c = 4 \cdot 5 \cdot 5 + 1 \cdot 1 \cdot 6 = 100 + 12 = 112,$$

e tutte e sole le soluzioni sono del tipo $112 + n30$, quindi anche del tipo

$$x = 22 + 30n$$

(si lascia al lettore il compito di verificare quest'ultima affermazione) \square

Esercizio 1.30 Utilizzando il teorema cinese del resto, risolvere il seguente sistema di equazioni congruenziali:

$$\begin{cases} x \equiv 8 \pmod{5} \\ x \equiv 9 \pmod{6} \\ x \equiv 10 \pmod{7} \end{cases}$$

Svolgimento. Essendo $MCD(5, 6, 7) = 1$ si procede innanzitutto a trovare gli inversi di $6 \cdot 7$ modulo 5, di $5 \cdot 7$ modulo 6 e di $6 \cdot 7$ modulo 5:

$$42c_1 \equiv 1 \pmod{5}, \quad c_1 = 3;$$

$$35c_2 \equiv 1 \pmod{6}, \quad c_2 = -1;$$

$$30c_3 \equiv 1 \pmod{7}, \quad c_3 = 4.$$

Una soluzione é data dalla formula

$$c = 8 \cdot c_1 \cdot 6 \cdot 7 + 9 \cdot c_2 \cdot 5 \cdot 7 + 10 \cdot c_3 \cdot 5 \cdot 6 = 1893.$$

Poiché 1893 é congruo a 3 modulo $210 = 5 \cdot 6 \cdot 7$, le soluzioni del sistema sono tutte e sole del tipo

$$3 + n \cdot 210, \quad n \in \mathbb{Z}$$

\square

1.11 Sistemi di Equazioni Congruenziali (esercizi proposti)

Esercizio 1.31 Utilizzando il teorema cinese del resto, risolvere i seguenti sistemi di equazioni congruenziali:

$$\begin{cases} x \equiv 5 \pmod{10} \\ x \equiv 7 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 4 \pmod{5} \end{cases}$$

$$\begin{cases} x \equiv 8 \pmod{3} \\ x \equiv 3 \pmod{10} \\ x \equiv 9 \pmod{7} \end{cases}$$

\square

1.12 Esercizi sul piccolo teorema di Fermat

Esercizio 1.32 *Dimostrare che l'intero 111111 è divisibile per 7.*

Svolgimento. Applicando il piccolo teorema di Fermat al numero primo 7, si ha

$$7 \mid (10^7 - 10),$$

$$7 \mid (9999990),$$

$$7 \mid 9 \cdot 10 \cdot 111111,$$

e poiché 7 non divide 9 né 10, si ha che 7 divide 111111. □

Esercizio 1.33 *Dimostrare che ogni numero primo $p \neq 2, 3, 5$ divide $\underbrace{11\dots 1}_{p-1}$.*

Svolgimento. Applicando il piccolo teorema di Fermat come nell'esercizio precedente, si ha:

$$p \mid (10^p - 10),$$

$$p \mid \underbrace{(99\dots 90)}_{p-1},$$

$$p \mid 9 \cdot 10 \cdot \underbrace{11\dots 1}_{p-1},$$

e poiché per ipotesi p non divide 9 né 10, si ha che p divide $\underbrace{11\dots 1}_{p-1}$. □

1.13 Esercizi sulla notazione Additiva e Moltiplicativa

Esercizio 1.34 *Portare in forma additiva le seguenti espressioni moltiplicative:*

$$a^3b^2, \quad a^{-1}(b^2c^{-1})^2, \quad (x^3y^{-2})^{-1}z, \quad a^{-1}b^{-1}ab = 1$$

□

Esercizio 1.35 *Portare in forma moltiplicativa le seguenti espressioni additive:*

$$3a - b - c, \quad -x + 3y = 0, \quad -x - y + x + y, \quad 3(-2x + 6y)$$

□

1.14 Esercizi sull'Ordine di un elemento in un Gruppo

Esercizio 1.36 *Dimostrare che, per ogni elemento non nullo h nel gruppo additivo $(Z_n, +)$ degli interi modulo n , si ha $|h| = \frac{n}{MCD(n,h)}$.*

Svolgimento. Poniamo $k = \frac{n}{MCD(n,h)}$. Se n, h sono coprimi, allora $k = n$ e gli interi

$$h, 2h, \dots, (n-1)h$$

non sono multipli di n , perché h e' coprimo con n . Quindi il minimo multiplo di h che sia multiplo anche di n é hn , ovvero $|h| = n = k$, come volevamo.

Se invece $MCD(n, h) \neq 1$, si ha $n = kh$ e allora

$$h, 2h, \dots, (k-1)h$$

sono tutti interi minori di $n = kh$ e quindi non sono multipli di n , dunque ancora una volta il minimo multiplo di h che é multiplo di n (e quindi congruo a zero modulo n) é kh e quindi $|h| = k$. \square

Esercizio 1.37 *Calcolare $|3|$ in Z_6 , $|12|$ in Z_{18} e $|10|, |11|, |12|$ in Z_{30}*

\square

1.15 Esercizi svolti sui Morfismi

Esercizio 1.38 *Dire se l'applicazione*

$$f : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in (M_2(Z), +, \cdot) \rightarrow a \in (Z, +, \cdot)$$

é un morfismo di anelli.

Svolgimento. Siano $a, b, c, d, a', b', c', d'$ elementi di Z . Si ha:

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] = f\left[\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}\right] = a+a' = f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] + f\left[\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right].$$

Quindi f rispetta l'operazione di somma; d'altra parte si ha:

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] = f\left[\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\right] = aa'+bc' \neq aa' = f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \cdot f\left[\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right],$$

quindi f non rispetta l'operazione di prodotto, e pertanto non é un morfismo di anelli. \square

Esercizio 1.39 *Dire se l'applicazione*

$$f : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Q) \rightarrow a+d \in Q$$

é un morfismo di anelli.

Svolgimento. siano $a, b, c, d, a', b', c', d'$ elementi di \mathcal{Q} . Si procede alla verifica come nell'esercizio precedente.

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] = f\left[\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}\right] = a+a'+d+d' = a+d+a'+d' = f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) + f\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right),$$

quindi f rispetta l'operazione di somma, ma

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] = f\left[\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\right] = aa'+bc'+cb'+dd' \neq (a+d)(a'+d') = f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \cdot f\left[\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right]$$

non rispetta quella di prodotto, quindi non é un morfismo di anelli. \square

Esercizio 1.40 Sia G_n il gruppo delle radici n -me dell'unit  sul campo complesso \mathcal{C} . Gli elementi di G_n sono quindi della forma $x_m = \cos(2\pi \frac{m}{n}) + i \operatorname{sen}(2\pi \frac{m}{n})$; provare che l'applicazione

$$f : x_m \in (G_n, \cdot) \rightarrow m \in (\mathbb{Z}, +)$$

  un morfismo.

Svolgimento. Siano

$$x_{m_1} = \cos(2\pi \frac{m_1}{n}) + i \operatorname{sen}(2\pi \frac{m_1}{n})$$

$$x_{m_2} = \cos(2\pi \frac{m_2}{n}) + i \operatorname{sen}(2\pi \frac{m_2}{n})$$

due radici n -me di 1. Ricordiamo le formule di addizione di numeri complessi in forma trigonometrica: il modulo del prodotto   uguale al prodotto dei moduli (nel caso di radici dell'unit  il modulo   sempre 1) e l'argomento del prodotto   uguale alla somma degli argomenti. Pertanto si ha:

$$f(x_{m_1} \cdot x_{m_2}) = f[\cos(2\pi \frac{m_1}{n} + 2\pi \frac{m_2}{n}) + i \operatorname{sen}(2\pi \frac{m_1}{n} + 2\pi \frac{m_2}{n})] = f[\cos(2\pi \frac{m_1 + m_2}{n}) + i \operatorname{sen}(2\pi \frac{m_1 + m_2}{n})]$$

$$f(x_{m_1} \cdot x_{m_2}) = m_1 + m_2 = f(x_{m_1}) + f(x_{m_2}).$$

\square

1.16 Esercizi proposti sui Morfismi

Esercizio 1.41 Una radice n -ma dell'unit  sul campo complesso si dice primitiva se ha periodo n . Dimostrare che una radice n -ma dell'unit  nella forma

$$x_m = \cos(2\pi \frac{m}{n}) + i \operatorname{sen}(2\pi \frac{m}{n})$$

  primitiva se e solo se m   coprimo con n .

Suggerimento. G_n ha ordine n per il teorema fondamentale dell'algebra, quindi utilizzando il procedimento dell'esercizio 1.40 si può dimostrare che (G_n, \cdot) é isomorfo a $(Z_n, +)$. L'asserto segue allora dall'esercizio 1.36. \square

Esercizio 1.42 Verificare che l'applicazione determinante

$$\det : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Q) \rightarrow (ad - bc) \in Q$$

é un morfismo dei gruppi moltiplicativi. \square

Esercizio 1.43 Dire se e quali delle seguenti applicazioni sono morfismi di anelli:

$$f_1 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Q) \rightarrow c \in Q;$$

$$f_2 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Q) \rightarrow a + b + c + d \in Q;$$

$$f_3 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Q) \rightarrow 0 \in Q.$$

\square

Esercizio 1.44 Dimostrare che la funzione

$$f : x \in (R, +) \rightarrow 2^x \in (]0, +\infty[, \cdot)$$

é un isomorfismo di gruppi. \square

Esercizio 1.45 Dire se l'applicazione

$$f : a + ib \in (C, +, \cdot) \rightarrow a - ib \in (C, +, \cdot)$$

é un morfismo del gruppo additivo e/o di quello moltiplicativo dei numeri complessi \square

Esercizio 1.46 Sia (G, \cdot) un gruppo, e a un suo fissato elemento. Dire se e quali delle seguenti applicazioni sono morfismi di gruppo:

[traslazione sinistra]

$$f_1 : x \in G \rightarrow ax \in G$$

[coniugio]

$$f_2 : x \in G \rightarrow a^{-1}xa \in G$$

[commutatore]

$$f_3 : x \in G \rightarrow a^{-1}x^{-1}ax \in G$$

□

1.17 Legge di Cancellazione in un Gruppo (esercizi svolti)

Esercizio 1.47 Siano a, b, c elementi di un gruppo. Risolvere le seguenti equazioni in x :

$$axb = c, \quad a^{-1}xa = c \quad acxb = c$$

Soluzioni. $x = a^{-1}cb^{-1}$, $x = aca^{-1}$, $x = c^{-1}a^{-1}cb^{-1}$

□

Esercizio 1.48 Dimostrare che, in ogni gruppo G , le applicazioni

[Traslazione Sinistra di ampiezza a]

$$\tau_a^s : x \in G \rightarrow ax \in G$$

[Traslazione Destra di ampiezza a]

$$\tau_a^d : x \in G \rightarrow xa \in G$$

sono permutazioni di G

Svolgimento. Si consideri ad esempio la traslazione sinistra. Per ogni $x, y \in G$, si ha:

$$\tau_a^s(x) = \tau_a^s(y) \iff ax = ay \iff x = y$$

per la legge di cancellazione, quindi τ_a^s é iniettiva. Inoltre

$$\tau_a^s(a^{-1}x) = aa^{-1}x = x$$

quindi τ_a^s é anche suriettiva, quindi é biettiva e risulta dunque una permutazione di G .

□

Esercizio 1.49 Dimostrare che un gruppo G é abeliano se e solo se l'applicazione

$$f : a \in G \rightarrow a^2 \in G$$

é un morfismo.

Svolgimento. Per ogni coppia di elementi $a, b \in G$ si ha:

$$f(ab) = f(a)f(b) \iff (ab)^2 = a^2b^2 \iff abab = aabb \iff a(ba)b = a(ab)b \iff ba = ab$$

□

1.18 Legge di Cancellazione in un gruppo (esercizi proposti)

Esercizio 1.50 Siano a, b, c elementi di un gruppo. Risolvere le seguenti equazioni in x :

$$a^{-1}bxb = cab, \quad axa = bcb \quad abxc = 1$$

□

Esercizio 1.51 Dimostrare che un gruppo G è abeliano se e solo se l'applicazione

$$f : a \in G \rightarrow a^{-1} \in G$$

è un morfismo. In tal caso dimostrare che f è un isomorfismo.

□

Esercizio 1.52 Dimostrare che un gruppo G è abeliano se e solo se si ha $[a, b] = 1$ per ogni $a, b \in G$

Suggerimento. Il commutatore è definito da $[a, b] = a^{-1}b^{-1}ab$.

□

Esercizio 1.53 Dimostrare che un gruppo G è abeliano se e solo se la traslazione destra di ampiezza a coincide con la traslazione sinistra di ampiezza a per ogni $a \in G$

□

Esercizio 1.54 Dimostrare che la traslazione destra e quella sinistra di ampiezza a sono dei morfismi se e solo se $a = 1$

□

1.19 Gruppi Ciclici (esercizi svolti)

Esercizio 1.55 Dimostrare che ogni gruppo ciclico è abeliano

Svolgimento. Sia G un gruppo ciclico, con generatore g . Poiché ogni elemento di G è una potenza di g , scelti due qualsiasi elementi $a, b \in G$, esistono interi n, m (che supponiamo positivi) tali che $a = g^n$, $b = g^m$. Si ha:

$$ab = g^n g^m = \underbrace{g \cdot g \cdot \dots \cdot g}_n \cdot \underbrace{g \cdot g \cdot \dots \cdot g}_m = \underbrace{g \cdot g \cdot \dots \cdot g}_{n+m} = \underbrace{g \cdot g \cdot \dots \cdot g}_{m+n} = g^m g^n = ba$$

□

Esercizio 1.56 Sia G un gruppo privo di sottogruppi non banali (diversi da 1 e da G). Dimostrare che G è ciclico

Svolgimento. Il gruppo identico é ciclico per definizione, quindi possiamo supporre che G abbia un elemento non identico, $1 \neq g \in G$. Ebbene g é un generatore, infatti $\langle g \rangle \neq 1$ é un sottogruppo, e quindi per ipotesi coincide con G . \square

Esercizio 1.57 Sia $G = \langle g \rangle$ un gruppo ciclico. Dimostrare che $G = \{g^m, m \in \mathbb{Z}\}$ e che l'applicazione

$$f : g^m \in G \rightarrow m \in \mathbb{Z}$$

é un morfismo. \square

Svolgimento. La prima affermazione é lasciata come semplice esercizio di verifica. Per quanto riguarda la seconda, basta osservare che per ogni coppia di interi positivi m, k si ha:

$$f(g^m g^k) = f(\underbrace{g \dots g}_m \underbrace{g \dots g}_k) = f(\underbrace{g \dots g}_{(m+k)}) = f(g^{(m+k)}) = m + k = f(g^m) + f(g^k)$$

$$f(g^m g^{-k}) = f(\underbrace{g \dots g}_m \underbrace{g^{-1} \dots g^{-1}}_k) = f(\underbrace{g \dots g}_{(m-k)}) = f(g^{(m-k)}) = m - k = f(g^m) + f(g^{-k})$$

$$f(g^{-m} g^{-k}) = f(\underbrace{g^{-1} \dots g^{-1}}_m \underbrace{g^{-1} \dots g^{-1}}_k) = f(\underbrace{g^{-1} \dots g^{-1}}_{(m+k)}) = f(g^{(-m-k)}) = -m - k = f(g^{-m}) + f(g^{-k})$$

\square

Esercizio 1.58 Trovare tutti i generatori di Z_{24} .

Svolgimento. Basta calcolare tutti gli interi minori di 24 e coprimi con 24:

$$\{1, 5, 7, 11, 13, 17, 19, 23\}$$

\square

Esercizio 1.59 Dimostrare che il gruppo additivo dei numeri razionali $(\mathbb{Q}, +)$ non é ciclico.

Svolgimento. Se per assurdo $\mathbb{Q} = \langle \frac{n}{m} \rangle$ con n, m interi, allora possiamo supporre ovviamente $m \neq +1$ e $m \neq -1$. Per ipotesi di assurdo ogni razionale si scrive come multiplo di n/m e quindi in particolare esiste un intero k tale che

$$\frac{n}{m^2} = k \frac{n}{m}$$

$$\frac{1}{m} = k$$

ma $1/m$ non é un intero, quindi l'assurdo. \square

1.20 Gruppi Ciclici (esercizi proposti)

Esercizio 1.60 Dimostrare che i gruppi additivi $(\mathbb{Z}; +)$ e $(\mathbb{Z}_m; +)$ sono gruppi ciclici.

Suggerimento. 1 è un generatore

2

Esercizio 1.61 Trovare tutti i generatori di $\mathbb{Z}_{25}; \mathbb{Z}_{28}; \mathbb{Z}_{30}; \mathbb{Z}_{40}$

2

Esercizio 1.62 Calcolare h_2 in \mathbb{Z}_{10} e h_4 in \mathbb{Z}_{30}

Esercizio 1.63 Dimostrare che il gruppo delle radici n-me dell'unità è ciclico di ordine n e che le radici primitive sono i suoi generatori

Suggerimento. Utilizzare gli esercizi 1.40 e 1.41

2

Esercizio 1.64 Trovare un sottogruppo di ordine 10 in \mathbb{Z}_{30} e un sottogruppo di ordine 12 in \mathbb{Z}_{60} e in \mathbb{Z}_{24}

2

Esercizio 1.65 Scrivere in forma trigonometrica le radici primitive seste dell'unità in \mathbb{C}

2

Esercizio 1.66 Sia p un numero primo. Dimostrare che ogni elemento non nullo del gruppo ciclico \mathbb{Z}_p è un generatore

2

1.21 Esercizi svolti sui gruppi di permutazioni

Esercizio 1.67 Dire se le permutazioni

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}; \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$$

sono permutazioni disgiunte

Svolgimento. L'insieme degli elementi mossi (non fissati) da α è $\{1, 2\}$ mentre quello degli elementi mossi da γ è $\{2, 3, 4\}$. Questi due insiemi hanno l'elemento 2 in comune, quindi non sono disgiunti. Dunque

Svolgimento. Si tratta di verificare se $\sigma\tau = \tau\sigma$. si ha:

$$\sigma\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{bmatrix}$$

$$\tau\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{bmatrix}$$

quindi $\sigma\tau \neq \tau\sigma$: le permutazioni non commutano. \square

Esercizio 1.71 *Dimostrare che S_5 non é abeliano*

Svolgimento. Le due permutazioni dell'esercizio precedente sono elementi di S_5 che non commutano! \square

Esercizio 1.72 *Calcolare il segno delle seguenti permutazioni:*

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{bmatrix}; \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{bmatrix}$$

Svolgimento. Innanzitutto scriviamo σ e τ in notazione ciclica:

$$\sigma = (12)(345), \quad \tau = (1234)(56);$$

Ricordando che ogni ciclo di lunghezza k ha segno $(-1)^{(k-1)}$ e che il segno del prodotto di permutazioni é uguale al prodotto dei segni delle permutazioni, si ha:

$$\text{sgn}(\sigma) = (-1)(1) = -1, \quad \text{sgn}(\tau) = (-1)(-1) = 1.$$

σ é dispari, τ é pari. \square

1.22 Esercizi proposti sui gruppi di permutazioni

Esercizio 1.73 *Dimostrare che $|S_n| = n!$*

Esercizio 1.74 *Dire se le seguenti permutazioni sono disgiunte*

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

\square

Esercizio 1.75 *Decomporre in cicli disgiunti le seguenti permutazioni*

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 3 & 4 & 1 & 7 & 8 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 6 & 7 & 2 & 5 & 4 & 9 & 8 \end{bmatrix}$$

□

Esercizio 1.76 Calcolare gli ordini delle permutazioni dei due esercizi precedenti

Esercizio 1.77 Dire se le seguenti coppie di permutazioni commutano

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 1 & 5 \end{bmatrix}, \quad \tau_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 4 & 3 \end{bmatrix}$$

$$\sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{bmatrix}, \quad \tau_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{bmatrix}$$

e calcolarne gli ordini.

□

Esercizio 1.78 Dire quali delle seguenti permutazioni di S_6 appartengono al gruppo alterno A_6 :

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{bmatrix}$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{bmatrix}$$

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix}$$

Esercizio 1.79 Calcolare ordine e segno delle seguenti permutazioni:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 1 & 5 & 4 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 5 & 3 & 4 & 7 & 9 & 6 & 8 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 & 10 & 11 & 9 \end{bmatrix}$$

□

1.23 Altri esercizi sui Gruppi

Esercizio 1.80 Dire quali tra i gruppi D_6, D_{12}, D_{11} contengono un sottogruppo ciclico di ordine 6

Suggerimento. Considerare il sottogruppo delle rotazioni

□

Esercizio 1.81 Calcolare il centro del gruppo quadrimo di Klein V_4 e del gruppo dei quaternioni Q

□

Esercizio 1.82 Trovare almeno due gruppi non isomorfi di ordine 20

□

Esercizio 1.83 Dire se le seguenti affermazioni sono vere o false

- D_9 è isomorfo a Z_9
- D_9 è isomorfo a Z_{18}
- D_9 contiene un sottogruppo isomorfo a Z_9
- D_9 contiene un sottogruppo isomorfo a Z_{18}
- D_9 non contiene sottogruppi ciclici

□

1.24 Esercizi svolti sugli Ideali di un Anello

Esercizio 1.84 Si considerino, nell'anello degli interi Z , gli ideali $I = (32)$ e $J = (28)$. Calcolare $I \cap J$ e $I + J$

Svolgimento. Ricordando che, per ogni coppia di interi relativi m, n si ha

$$(m) \cap (n) = (\text{mcm}(m, n))$$

$$(m) + (n) = (\text{MCD}(m, n))$$

risulta

$$I \cap J = (224), \quad I + J = (4)$$

□

Esercizio 1.85 Dire se nell'anello Z tra i tre ideali $I = (30), J = (70), K = (5)$ ce ne è uno che contiene gli altri due, e calcolare l'ideale $I + J$.

Svolgimento. Ricordando che, per ogni coppia di interi relativi m, n si ha $(m) \subseteq (n)$ se e solo se n divide m , abbiamo

$$J \subseteq K, \quad I \subseteq K, \quad I + J = (10)$$

□

Esercizio 1.86 *Nell'anello $M_2(\mathbb{R})$ delle matrici quadrate di ordine 2 sui reali, dire se l'insieme*

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, a \in \mathbb{R} \right\}$$

è un ideale sinistro.

Svolgimento. Per ogni $a, b \in \mathbb{R}$ si ha:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix}$$

quindi la differenza di due elementi di H è ancora un elemento di H . Per ogni $x, y, z, t, a \in \mathbb{R}$, si ha:

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xa & 0 \\ za & 0 \end{pmatrix}$$

quindi il prodotto a sinistra di un elemento di H per un elemento di $M_2(\mathbb{R})$ non è necessariamente un elemento di H , quindi H non è un ideale sinistro. □

Esercizio 1.87 *Sia $A(\mathbb{R})$ l'anello delle funzioni reali di variabile reale, e sia $a \in \mathbb{R}$ fissato. Dire se l'insieme*

$$I(a) = \{f \in A(\mathbb{R}) : f(a) = 0\}$$

è un ideale.

Svolgimento. Per ogni $f, g \in I(a)$ e per ogni $\alpha \in A(\mathbb{R})$ si ha:

$$(f - g)(a) = f(a) - g(a) = 0 - 0 = 0$$

$$(f \cdot \alpha)(a) = (\alpha \cdot f)(a) = \alpha(a) \cdot f(a) = \alpha(a) \cdot 0 = 0$$

quindi la differenza di due elementi di $I(a)$ e il prodotto di un elemento di $I(a)$ per un elemento dell'anello sono ancora elementi di $I(a)$. Esso è pertanto un ideale. □

1.25 Esercizi proposti sugli Ideali di un Anello

Esercizio 1.88 *Si considerino, nell'anello degli interi \mathbb{Z} , gli ideali $I = (60)$ e $J = (48)$. Calcolare $I \cap J$ e $I + J$*

□

Esercizio 1.89 Dire quali dei seguenti ideali di Z sono ideali massimali:

$$I = (14), \quad J = (13), \quad K = (101)$$

□par

Esercizio 1.90 Nell'anello $M_2(Z)$ delle matrici quadrate di ordine 2 sugli interi, dire se l'insieme

$$H = \left\{ \begin{pmatrix} h & h \\ h & h \end{pmatrix}, h \in Z \right\}$$

è un ideale sinistro (destro).

□

Esercizio 1.91 Nell'anello $M_2(Q)$ delle matrici quadrate di ordine 2 sui razionali, dire se l'insieme

$$H = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, a, b \in Q \right\}$$

è un ideale sinistro (destro).

□

1.26 Algoritmo di Divisione Euclidea per Polinomi (esercizi svolti)

Esercizio 1.92 Calcolare il resto $r(x)$ e il quoziente $q(x)$ della divisione euclidea (in $Q[x]$) del polinomio $f(x) = 6x^3 + 2x - 1$ per il polinomio $g(x) = 2x^2 + x + 1$

Svolgimento. Innanzitutto dividiamo il termine di grado massimo di f per il termine di grado massimo di g , ottenendo il termine di grado massimo del quoziente, cioè $3x$. Moltiplicando $3x$ per $g(x)$ si ha

$$6x^3 + 3x^2 + 3x.$$

Operiamo ora con il polinomio

$$h(x) = f(x) - 6x^3 + x^2 + 3x = -3x^2 - x - 1;$$

dividendo, come prima, il suo termine di grado massimo per il termine di grado massimo di g , otteniamo $-3/2$, il termine successivo del quoziente. Moltiplichiamo ora $g(x)$ per $-3/2$ e otteniamo:

$$-3x^2 - (3/2)x - (3/2).$$

Il resto è dato allora da

$$r(x) = h(x) - (-3x^2 - (3/2)x - (3/2)) = (1/2)x + (1/2)$$

mentre il quoziente é

$$q(x) = 3x - (3/2);$$

e' lasciato per esercizio al lettore verificare che

$$f(x) = q(x) \cdot g(x) + r(x),$$

con $\deg(r) < \deg(g)$. □

Esercizio 1.93 Calcolare, per ogni $n > 0$, quoziente e resto della divisione euclidea in $Q[x]$ del polinomio $x^n - 1$ per il polinomio $x - 1$.

Svolgimento. Operiamo come nell'esercizio precedente: dalla prima divisione dei rispettivi termini di grado massimo, otteniamo il termine di grado massimo del quoziente, cioe' x^{n-1} . Moltiplicando x^{n-1} per $(x - 1)$ si ha $(x^n - x^{n-1})$. Sottraiamo quest'ultimo polinomio da $x^n - 1$ e otteniamo $x^{n-1} - 1$. Ripetendo l'operazione a partire da $x^{n-1} - 1$ e poi continuando in questo modo, i coefficienti del quoziente sono tutti uguali a uno, quindi il quoziente é

$$x^{n-1} + x^{n-2} + \dots + x + 1$$

e il resto é zero. Resta cosí dimostrata in particolare la formula

$$x^n - 1 = (x - 1) \cdot (x^{n-1} + x^{n-2} + \dots + x + 1)$$

□

Esercizio 1.94 Trovare il Massimo Comun Divisore monico dei polinomi

$$f = x^3 + 6x^2 + 11x + 6, \quad g = x^2 - 4$$

Svolgimento. Utilizziamo, in analogia a quanto fatto con la divisione di interi, l'algoritmo di Euclide. Operando le divisioni successive, si ha:

$$f = (x + 6)g + (15x + 30)$$

$$g = \left(\frac{1}{15}x - \frac{2}{15}\right)(15x + 30) + 0.$$

L'ultimo resto non nullo é $(15x+30)$, quindi esso é un massimo comun divisore di f, g . Per trovare il massimo comun divisore monico é sufficiente moltiplicare il polinomio cosi' trovato per l'inverso del suo termine direttore, quindi

$$d = \frac{1}{15}(15x + 30) = x + 2$$

é il massimo comun divisore monico cercato. □

1.27 Algoritmo di Divisione Euclidea per Polinomi (esercizi proposti)

Esercizio 1.95 Calcolare il resto e il quoziente della divisione euclidea (in $Q[x]$) delle seguenti coppie di polinomi:

$$\begin{aligned} x^4 + 3x^2 + 2x + 2, & \quad x^2 + x + 1 \\ x^3 + x^2 + 2x + 3, & \quad x - 3 \\ 5x^5 + 4x^4 - 2x - 2, & \quad 5x^4 - 1 \end{aligned}$$

□

Esercizio 1.96 Dimostrare che, per ogni base $a \geq 2$, risulta

$$\underbrace{(11\dots1)}_n)_a = \frac{a^n - 1}{a - 1}$$

Suggerimento. Utilizzare la formula 1.93

□

Esercizio 1.97 Trovare il Massimo Comun Divisore monico delle seguenti coppie di polinomi

$$\begin{aligned} x^3 + x - 10, & \quad x^2 - x + 10 \\ 3x^3 - 12x, & \quad 2x - 2 \end{aligned}$$

□

Esercizio 1.98 Scrivere nella forma di Bezout i massimi comun divisori dell'esercizio precedente.

□

1.28 Riducibilità e Radici di Polinomi (esercizi svolti)

Esercizio 1.99 Dire se il polinomio $f = x^2 - 4$ è riducibile o irriducibile su $Q[x]$

Svolgimento. f ha la radice $2 \in Q$ quindi, per il teorema di Ruffini, è divisibile per il polinomio $x - 2$ e pertanto è riducibile.

□

Esercizio 1.100 Dire se il polinomio $f = 5x^3 + 6x^2 + 10x + 2$ è riducibile o irriducibile su $Q[x]$

Svolgimento. Il numero primo 2 divide tutti i coefficienti di f tranne quello di grado massimo. Inoltre $2^2 = 4$ non divide il termine noto. Quindi f è irriducibile per il criterio di Eisenstein.

□

Esercizio 1.101 Dire quali fra i polinomi

$$f = x^4 + x^3 + x + 1$$

$$g = x^4 + x^3 + x^2 + x + 1$$

sono irriducibili in $\mathbb{Q}[x]$

Svolgimento. f é riducibile perche' ammette -1 come radice, pertanto il teorema di Ruffini assicura che é divisibile per $x + 1$. Invece g é irriducibile perché é il quinto polinomio ciclotomico. \square

Esercizio 1.102 Dire quali tra i seguenti polinomi hanno radici multiple in $\mathbb{Q}[x]$:

$$f = x^{11} - 11$$

$$g = 8x^8$$

$$h = x^4 + 4x^3 + 3x^2 + 6x + 12$$

Svolgimento. Poiché un polinomio ha una radice multipla c se e solo se c é anche radice del polinomio derivato, consideriamo i polinomi derivati

$$Df = 10x^{10}, \quad Dg = 64x^7, \quad Dh = 4x^3 + 12x^2 + 6x + 6.$$

Df ha solo la radice 0 , che non é radice di f . Quindi f é privo di radici multiple. Dg ha solo la radice 0 , che é anche radice di g . quindi g ha radici multiple (per la precisione ha la radice 0 con molteplicitá 8). Infine Dh é un polinomio irriducibile per il criterio di Eisenstein, quindi privo di radici in \mathbb{Q} . Di conseguenza h é privo di radici multiple. \square

Esercizio 1.103 Dire quali tra i polinomi

$$f = x^2 + x + 1$$

$$g = x^3 + x + 1$$

sono riducibili in $\mathbb{R}[x]$

Svolgimento. Il polinomio f é irriducibile, perché di secondo grado, con $\Delta < 0$. Il polinomio g invece é riducibile, come tutti i polinomi reali di grado ≥ 3 . \square

1.29 Riducibilitá e Radici di Polinomi (esercizi proposti)

Esercizio 1.104 Dire quali tra i seguenti polinomi sono riducibili in $\mathbb{Q}[x]$:

$$f_1 = 8x^4 + 49x^3 + 7x^2 + 28x + 21$$

$$f_2 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$f_3 = x^6 + x^5 + x^3 + x^2 + x + 1$$

$$f_4 = x^2 - 7$$

$$f_5 = x^7 - 1$$

□

Esercizio 1.105 Dire quali tra i seguenti polinomi hanno radici multiple in $Q[x]$:

$$f_1 = 18x^6$$

$$f_2 = 4x^2 + 4x + 1$$

$$f_3 = 2x^3 + 3x^2 + 2x + 2$$

$$f_4 = x^4 - 4$$

□

Esercizio 1.106 Sia K un campo. Stabilire se l'applicazione

$$D : f \in K[x] \rightarrow Df \in K[x]$$

che associa a ogni polinomio il suo derivato é un morfismo additivo e/o moltiplicativo.

□

Esercizio 1.107 Sia $f = ax^2 + bx + c$ un polinomio di secondo grado a coefficienti complessi. Dire perché f ha esattamente due radici c_1, c_2 e dimostrare che

$$c_1 + c_2 = \frac{-b}{a}, \quad c_1 \cdot c_2 = \frac{c}{a}$$

Suggerimento. Utilizzare il teorema fondamentale dell'algebra e scomporre f nel prodotto di polinomi di primo grado

□

Esercizio 1.108 Dire quali dei seguenti polinomi sono irriducibili in $R[x]$:

$$f_1 = x^2 - x + 1$$

$$f_2 = x^2 + x - 1$$

$$f_3 = 8x^4 + 7x^3 + 6x^2 + 5x + 4$$

□

1.30 Teorema di Lagrange e Sottogruppi Normali (esercizi svolti)

Esercizio 1.109 *Dimostrare che un gruppo di ordine p , dove p è un numero primo, è abeliano.*

Svolgimento. Sia G un gruppo di ordine p . Per il teorema di Lagrange, se H è un sottogruppo di G , il suo ordine deve essere un divisore di p . Siccome p è un numero primo, i suoi unici divisori sono quelli banali e allora gli unici sottogruppi di G sono quelli banali. L'asserto segue allora dagli esercizi 1.55 e 1.56. \square

Esercizio 1.110 *Sia G un gruppo finito, e siano H e K suoi sottogruppi. Sapendo che $|H| = 10$ e $|K| = 9$, dimostrare che $|G|$ è multiplo di 90 e calcolare il sottogruppo intersezione $H \cap K$.*

Svolgimento. Per il teorema di Lagrange, 9 divide $|G|$ e anche 10 divide $|G|$; di conseguenza anche 90 divide $|G|$. Sempre per il teorema di Lagrange, siccome $H \cap K$ è un sottogruppo sia di H che di K , il suo ordine divide $|H|$ e divide anche $|K|$, quindi $|H \cap K| = 1$ e pertanto l'intersezione coincide con il sottogruppo identico. \square

Esercizio 1.111 *Sia G un gruppo finito, che ha un unico sottogruppo H di ordine m . Dimostrare che H è un sottogruppo normale di G .*

Svolgimento. Sia a un qualsiasi elemento di G . L'insieme

$$a^{-1}Ha$$

è un sottogruppo di G , come il lettore può facilmente verificare. Inoltre l'applicazione

$$f : h \in H \rightarrow a^{-1}ha \in a^{-1}Ha$$

è una biezione, quindi risulta $|a^{-1}Ha| = |H| = m$. Poiché H è l'unico sottogruppo di ordine m , possiamo concludere che $a^{-1}Ha = H$ e cioè che H è normale. \square

Esercizio 1.112 *Il gruppo dei quaternioni Q è un gruppo di ordine 8, con un unico sottogruppo di ordine 2. Dimostrare che Q ha tutti i sottogruppi normali. (Si osservi che Q è un esempio di gruppo non abeliano con tutti i sottogruppi normali)*

Svolgimento. Per il teorema di Lagrange, tutti i sottogruppi di Q devono avere ordine 1,2,4 oppure 8. I sottogruppi di ordine 1 e 8 sono quelli banali, quindi normali. Il sottogruppo di ordine 2 è l'unico nel suo ordine, quindi è normale per l'esercizio precedente. I sottogruppi di ordine 4, infine, hanno indice 2 e quindi sono normali. \square

Esercizio 1.113 *Trovare un sottogruppo normale non banale del gruppo diedrale D_n per ogni $n \geq 3$.*

Suggerimento. Il sottogruppo delle rotazioni ha indice 2. \square

Esercizio 1.114 Sia $GL_2(\mathbb{R})$ il gruppo lineare delle matrici invertibili 2×2 sui reali. Dire se il sottogruppo

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad = 1 + bc \right\}$$

é normale in $GL_2(\mathbb{R})$.

Svolgimento. S é il sottogruppo delle matrici a determinante 1. Poiché l'applicazione

$$\delta : a \in GL_2(\mathbb{R}) \rightarrow \det(a) \in \mathbb{R}$$

é un morfismo, il lettore puo' verificare facilmente che $\text{Ker}\delta = S$ e quindi S é un sottogruppo normale.

□

1.31 Teorema di Lagrange e Sottogruppi Normali (esercizi proposti)

Esercizio 1.115 Sia G un gruppo finito di ordine ≤ 60 , e H, K suoi sottogruppi tali che $|H| = 20$ e $|K| = 3$. Calcolare $|G|$ e $|H \cap K|$.

□

Esercizio 1.116 Dire, motivando la risposta, quali dei seguenti gruppi sono semplici:

$$Z_{51}, \quad Z_{52}, \quad Z_{53}, \quad D_{54}, \quad S_{10}$$

Suggerimento. A_{10} é un sottogruppo di indice 2 di S_{10}

Esercizio 1.117 Si consideri il gruppo $U_2(\mathbb{Z})$ delle matrici 2×2 unitriangolari superiori a coefficienti interi:

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}.$$

Dire se il sottogruppo

$$H = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in \mathbb{Z} \right\}$$

é normale in G .

□

1.32 Esercizi Svolti sui Quozienti

Esercizio 1.118 Sia H un sottogruppo di ordine 4 in Z_{40} . Determinare tutti i sottogruppi non banali del gruppo quoziente Z_{40}/H .

Svolgimento. Poiché i quozienti di gruppi ciclici sono a loro volta ciclici, Z_{40}/H è ciclico di ordine 10, quindi i suoi sottogruppi non banali sono esattamente due, di ordini 2 e 5 rispettivamente. Tali sottogruppi devono essere necessariamente del tipo

$$K_1/H, \quad K_2/H$$

con K_1, K_2 sottogruppi di Z_{40} tali che:

$$|K_1/H| = 2, \quad |K_2/H| = 5.$$

Da ciò risulta:

$$\begin{aligned} |K_1| &= 8, & K_1 &= \langle 5 \rangle \\ |K_2| &= 20, & K_2 &= \langle 2 \rangle. \end{aligned}$$

I sottogruppi del quoziente cercati sono dunque

$$K_1/H = \langle 5 \rangle / \langle 10 \rangle$$

$$K_2/H = \langle 2 \rangle / \langle 10 \rangle.$$

□

Esercizio 1.119 Dire quali dei seguenti quozienti di anelli di polinomi risultano essere campi:

$$R[x]/(x^2 - 1)$$

$$Q[x]/(x^2 + 1)$$

$$R[x]/(x)$$

$$Z_3[x]/(x^2 + x + 1)$$

Svolgimento. Il polinomio $x^2 - 1$ è riducibile su $R[x]$, quindi $(x^2 - 1)$ non è un ideale massimale, e dunque $R[x]/(x^2 - 1)$ non è un campo. Al contrario, $x^2 + 1$ e x sono polinomi irriducibili sui campi Q e R , quindi $Q[x]/(x^2 + 1)$ e $R[x]/(x)$ sono campi. Infine, il polinomio $x^2 + x + 1$ è riducibile su $Z_3[x]$. Si ha infatti, riducendo i coefficienti modulo 3:

$$x^2 + x + 1 = x^2 + x - 2 = (x + 2)(x - 1) \in Z_3[x]$$

e quindi l'ultimo quoziente non può essere un campo. □

Esercizio 1.120 Dire se $Z/(7)$ è un campo.

Svolgimento. L'ideale (7) è massimale in Z perché 7 è un numero primo. Quindi $Z/(7)$ è un campo. □

1.33 Esercizi Proposti sui Quozienti

Esercizio 1.121 Sia $G = Z_{60}$, e sia H l'unico sottogruppo di G di ordine 2. Calcolare tutti i sottogruppi di G/H

□

Esercizio 1.122 Dire quali dei seguenti quozienti sono campi:

$$R[x]/(17x^4 + 4x^3 + 2x + 1), \quad Q[x]/(x^5 - 9x + 6), \quad C[x]/(x^2 + 1)$$

$$Q[x]/(x^3 + x^2 + x + 1), \quad Z/(8), \quad Z/(143), \quad Z_{30}/(10)$$

□

Esercizio 1.123 Dire se l'ideale $(x^2 + x + 1)$ è massimale in $Z_3[x]$; in caso di risposta negativa, trovare almeno un ideale massimale che lo contenga.

□

1.34 Elementi Algebrici

Esercizio 1.124 Dimostrare che gli elementi $\sqrt{2}$, i , $1 + \sqrt{3}$ sono algebrici su Q , trovando per ciascuno di essi un polinomio di cui è radice.

Svolgimento. Posto $a = \sqrt{2}$, si ottiene con semplici passaggi che

$$a^2 = 2, \quad a^2 - 2 = 0,$$

cioè a è radice del polinomio $x^2 - 2$. Con lo stesso procedimento si ottengono i polinomi $x^2 + 1$, che ammette come radice i , e $x^2 - 2x - 2$, che ammette come radice $1 + \sqrt{3}$

Esercizio 1.125 Dire quali tra i seguenti elementi sono algebrici su Q :

$$\sqrt{1 + \sqrt{2}}, \quad \sqrt[3]{4}, \quad 2\sqrt{2}, \quad 1 + \pi.$$

Degli elementi che risultano algebrici, determinare il polinomio minimo su Q .

Svolgimento. Posto $a = \sqrt{1 + \sqrt{2}}$, si ha:

$$a^2 = 1 + \sqrt{2}, \quad a^2 - 1 = \sqrt{2}$$

$$(a^2 - 1)^2 = 2, \quad a^4 - 2a^2 + 1 = 2;$$

otteniamo così che a è algebrico perché radice del polinomio $x^4 - 2x^2 - 1$, che è monico e ha il grado minimo possibile, quindi è il polinomio minimo di a . Con lo stesso procedimento si ottiene il polinomio minimo di $\sqrt[3]{4}$, $x^3 - 4$. L'elemento $2^{\sqrt{2}}$ invece è trascendente, perché potenza ad esponente irrazionale di un elemento algebrico. L'elemento $1 + \pi$, infine, non può essere algebrico: se fosse radice di un polinomio a coefficienti razionali f , allora π sarebbe radice del polinomio $f(x - 1)$, ma π è trascendente, quindi non può essere radice di alcun polinomio in $Q[x]$. Quindi anche $1 + \pi$ è trascendente. \square

Esercizio 1.126 Dire, motivando la risposta, quali tra i seguenti elementi sono algebrici su Q :

$$i/2, \quad \sqrt{(2)^3}, \quad 2^{\sqrt{3}}, \quad \sqrt{1 + \sqrt[3]{2}}$$

$$\sqrt{2} + \sqrt{3}, \quad \sqrt{e}, \quad i - \sqrt[3]{3}, \quad e^i$$

Di ciascun elemento che risulta algebrico, determinare almeno un polinomio che lo ammetta come radice. \square

Esercizio 1.127 Trovare i polinomi minimi di tutte le radici del polinomio

$$3x^3 - 2x^2 - 3x + 2$$

\square

1.35 Campo dei Quozienti e Sottoanello Fondamentale

Esercizio 1.128 Trovare il campo dei quozienti dei seguenti domini di integrità:

$$Z, \quad Q, \quad R, \quad Z_3$$

Suggerimento. Se K è un campo, $Q(K) = K$ \square

Esercizio 1.129 Trovare il sottoanello fondamentale e la caratteristica di $A = M_2(R)$

Svolgimento. Per definizione $E(A)$ è l'insieme dei multipli dell'unità di A , cioè della matrice identica di ordine 2:

$$E(A) = \left\{ \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}, n \in Z \right\}$$

che è isomorfo a Z , come il lettore può facilmente verificare, e quindi $\text{char} A = 0$. \square

Esercizio 1.130 Determinare la caratteristica dei seguenti anelli

$$R, \quad M_4(Q), \quad M_3(Z_3), \quad Z_5[x]$$

Svolgimento. In maniera del tutto simile all'esercizio precedente, é facile verificare che i sottoanelli fondamentali di R e di $M_4(Q)$ sono isomorfi a Z , e quindi la loro caratteristica é zero. Per quanto riguarda $M_3(Z_3)$, osserviamo che i suoi elementi sono le matrici a coefficienti interi modulo 3, quindi il sottoanello fondamentale é:

$$E(M_3(Z_3)) = \left\{ \begin{pmatrix} n & 0 & 0 \\ 0 & n & 0 \\ 0 & 0 & n \end{pmatrix}, n \in Z_3 \right\},$$

isomorfo a Z_3 . Per quanto riguarda $Z_5[x]$, osserviamo che i suoi elementi sono i polinomi a coefficienti interi modulo 5, quindi il sottoanello fondamentale é l'insieme dei multipli modulo 5 del polinomio costante 1:

$$E(Z_5[x]) = \{n \in Z_5\} \simeq Z_5.$$

In conclusione, $\text{char}(M_3(Z_3)) = 3$ e $\text{char}(Z_5[x]) = 5$. □

Esercizio 1.131 *Dire, motivando la risposta, se R può essere sottocampo fondamentale di qualche campo.*

Svolgimento. NO perché il sottocampo fondamentale di un campo può essere isomorfo solo a Q oppure a Z_c , con c numero primo. Non può quindi essere R . □

Esercizio 1.132 *Determinare la caratteristica dei seguenti anelli:*

$$M_3(Z_{11}), \quad Q[x], \quad M_5(Z), \quad C, \quad Z_7[x]$$

e determinare il sottocampo fondamentale di R

□

Esercizio 1.133 *Dire, motivando la risposta, se un anello di caratteristica 3 può essere infinito.*

Suggerimento. Considerare $Z_3[x]$. □

Esercizio 1.134 *Dire, motivando la risposta, se Z_6 può essere il sottocampo fondamentale di qualche campo.*