ALGEBRA 1 PB-Z
VIII. 11 V 2012

Esercizio 1. Siano $\mathrm{F}(\mathbb{R},\mathbb{R})$ l'insieme delle funzioni reali di una variabile reale e $\mathrm{I}_0(\mathbb{R},\mathbb{R}) \subseteq \mathrm{F}(\mathbb{R},\mathbb{R})$ l'insieme delle funzioni che si annullano nel punto $0 \in \mathbb{R}$.

Si mostri che l'insieme $\mathrm{F}(\mathbb{R},\mathbb{R})$, se dotato delle usuali operazioni di somma e prodotto tra funzioni, è un anello commutativo unitario e che $\mathrm{I}_0(\mathbb{R},\mathbb{R})$ è un ideale bilatero di $\mathrm{F}(\mathbb{R},\mathbb{R})$.

Soluzione. L'insieme $\mathrm{F}(\mathbb{R},\mathbb{R})$, dotato delle usuali operazioni di somma e prodotto tra funzioni, è un anello commutativo unitario, perché tale è il codominio, $\mathbb{R}$, di ogni suo elemento.

$\mathrm{F}(\mathbb{R},\mathbb{R})$ è un anello commutativo; quindi, ogni suo ideale sinistro è un ideale destro (dunque, bilatero) e ogni suo ideale destro è un ideale sinistro (dunque, bilatero).

Il sottoinsieme $\{0\}$ di $\mathbb{R}$ un ideale (bilatero) dell'anello commutativo unitario $\mathbb{R}$ ([1]); quindi, $\mathrm{I}_0(\mathbb{R},\mathbb{R})$ è un ideale (bilatero) di $\mathrm{F}(\mathbb{R},\mathbb{R})$.

[1] Qui, come poco sopra, stiamo considerando $\mathbb{R}$ come codominio degli elementi di $\mathrm{I}_0(\mathbb{R},\mathbb{R})$.

Esercizio 2. Sia $(G, \cdot)$ un gruppo.

Si mostri che un sottoinsieme $X \subseteq G$ di G è un sottogruppo di G se e solo se è non vuoto e verifica la condizione

$$\diamond \quad x_1,\ x_2 \in X \ \Rightarrow\ x_1 x_2^{-1} \in X.$$

Soluzione. Per definizione, un **sottogruppo di** $(G, \cdot)$ è un sottoinsieme non vuoto X di G che, rispetto all'operazione binaria $\cdot$ definita su G, costituisce un gruppo. Quindi, un sottoinsieme X di G è un sottogruppo di $(G, \cdot)$ se e solo se è chiuso per l'operazione " $\cdot$ ", contiene l'elemento neutro di $(G, \cdot)$, contiene l'inverso di ogni suo elemento.

Dimostriamo, ora, il risultato enunciato nel testo dell'esercizio.

se...
Sia X un sottoinsieme non vuoto di G che verifica la condizione $\diamond$. Allora, X contiene l'elemento neutro e di $(G, \cdot)$; infatti, poiché è non vuoto, X contiene almeno un elemento $\tilde{x} \in X$; quindi, scegliendo $x_1 = \tilde{x}$ e $x_2 = \tilde{x}$, grazie alla condizione $\diamond$, abbiamo che $e = \tilde{x}\tilde{x}^{-1} = x_1 x_2^{-1}$ è un elemento di G. Inoltre, X contiene l'inverso di ogni suo elemento x; infatti, scegliendo $x_1 = e$ ([2]) e $x_2 = x$, grazie alla condizione $\diamond$, abbiamo che $x^{-1} = ex^{-1} = x_1 x_2^{-1}$ è un elemento di G. Infine, X è chiuso per l'operazione " $\cdot$ "; infatti, dati comunque x_1 e x_2 elementi di X, da quanto appena mostrato, X contiene x_1^{-1} e x_2^{-1} e, quindi, grazie alla condizione $\diamond$ i prodotti $x_1 x_1^{-1} = e$, $x_1 x_2^{-1}$, $x_1 x_1$, $x_1 x_2$, $x_2 x_1^{-1}$, $x_2 x_2^{-1} = e$, $x_2 x_1$, $x_2 x_2$, $x_1^{-1} x_1^{-1}$, $x_1^{-1} x_2^{-1}$, $x_1^{-1} x_1 = e$, $x_1^{-1} x_2$, $x_2^{-1} x_1^{-1}$, $x_2^{-1} x_2^{-1}$, $x_2^{-1} x_1$, $x_2^{-1} x_2$; dunque, in particolare, contiene il prodotto $x_1 x_2$.

...e solo se
Sia $X \subseteq G$ un sottogruppo di G e siano x_1, x_2 elementi di X. Allora, essendo $(X, \cdot)$ un sottogruppo di $(G, \cdot)$, il sottoinsieme X di G contiene gli elementi x_1^{-1}, x_2^{-1} e, quindi, i prodotti $x_1 x_2$, $x_2 x_1$, $x_1^{-1} x_2$, $x_2^{-1} x_1, x_1 x_2^{-1}$, $x_2 x_1^{-1}$, $x_1^{-1} x_2^{-1}$, $x_2^{-1} x_1^{-1}$; dunque, in particolare, X contiene $x_1 x_2^{-1}$. Infine, X è non vuoto, perché contiene almeno un elemento (ad esempio, contiene l'elemento neutro di $(G, \cdot)$).

[2] Come abbiamo appena visto, X contiene l'elemento neutro e di $(G, \cdot)$.

Esercizio 3. Siano $(G,\cdot)$ un gruppo e $S \leq G$ un sottogruppo di G.

I. Si mostri che le relazioni ϱ_{sn} e ϱ_{ds} definite da

$$\forall x_1, x_2 \in G \quad x_1 \varrho_{\mathrm{sn}} x_2 \Leftrightarrow x_1^{-1} x_2 \in S$$

e, rispettivamente,

$$\forall x_1, x_2 \in G \quad x_1 \varrho_{\mathrm{ds}} x_2 \Leftrightarrow x_1 x_2^{-1} \in S$$

sono di equivalenza e che le partizioni di G ad esse associate sono $\{xS\}_{x\in G}$ e, rispettivamente, $\{Sx\}_{x\in G}$.

II. Si mostri che tutte le classi laterali sinistre (destre) hanno la medesima potenza e che essa è uguale alla potenza di S considerato come insieme ([3]).

III. Dedurre il seguente teorema ([4]) ([5]).

Teorema (Lagrange). Sia G un gruppo finito. Allora l'ordine di un sottogruppo S di G è necessariamente un divisore dell'ordine di G.

Merita attenzione il fatto che il "Viceversa" in generale, non è vero.

Soluzione. Sia $e \in G$ l'elemento neutro del gruppo $(G,\cdot)$.

I.
Le relazioni ϱ_{sn} e ϱ_{ds} sono riflessive; infatti, contenendo S l'elemento neutro di $(G,\cdot)$, abbiamo che per ogni $x \in G$, è sempre vero che $S \ni e = x^{-1}x$ e, rispettivamente, che $S \ni e = xx^{-1}$; quindi, è sempre vero che $x \varrho_{\mathrm{sn}} x$ e, rispettivamente, che $x \varrho_{\mathrm{ds}} x$.

Le relazioni ϱ_{sn} e ϱ_{ds} sono simmetriche; infatti, se $x_1, x_2 \in G$ son tali che $x_1 \varrho_{\mathrm{sn}} x_2$ oppure $x_1 \varrho_{\mathrm{ds}} x_2$; ossia, se son tali che $x_1^{-1}x_2 \in S$ oppure $x_1 x_2^{-1} \in S$; allora, contenendo S l'inverso di ogni suo elemento, abbiamo che $S \ni x_2^{-1}x_1 = (x_1^{-1}x_2)^{-1}$ oppure, $S \ni x_2 x_1^{-1} = (x_1 x_2^{-1})^{-1}$; ossia, abbiamo che $x_2 \varrho_{\mathrm{sn}} x_1$ oppure, $x_2 \varrho_{\mathrm{ds}} x_1$.

Le relazioni ϱ_{sn} e ϱ_{ds} sono transitive; infatti, se $x_1, x_2, x_3 \in G$ son tali che $x_1 \varrho_{\mathrm{sn}} x_2$ e $x_2 \varrho_{\mathrm{sn}} x_3$ oppure $x_1 \varrho_{\mathrm{ds}} x_2$ e $x_2 \varrho_{\mathrm{ds}} x_3$; ossia, se son tali che $x_1^{-1}x_2 \in S$ e $x_2^{-1}x_3 \in S$ oppure $x_1 x_2^{-1} \in S$ e $x_2 x_3^{-1} \in S$; allora, essendo S chiuso rispetto al prodotto, abbiamo che $S \ni x_1^{-1}x_3 = x_1^{-1}x_2x_2^{-1}x_3$ oppure $S \ni x_1 x_3^{-1} = x_1 x_2^{-1} x_2 x_3^{-1}$.

Le partizioni di G associate a ϱ_{sn} e, rispettivamente, ϱ_{ds} sono $\{xS\}_{x\in G}$ e, rispettivamente, $\{Sx\}_{x\in G}$. Infatti, $x_1, x_2 \in G$ son tali che $x_1 \varrho_{\mathrm{sn}} x_2$ oppure $x_1 \varrho_{\mathrm{ds}} x_2$ se e solo se esiste un elemento $s_{\mathrm{sn}} \in S$ oppure un elemento s_{ds} tale che $x_1^{-1}x_2 = s_{\mathrm{sn}}$ oppure $x_1 x_2^{-1} = s_{\mathrm{ds}}$; ossia, se e solo se esiste un elemento $s_{\mathrm{sn}} \in S$ oppure un elemento s_{ds} tale che $x_2 = x_1 s_{\mathrm{sn}}$ oppure $x_1 = s_{\mathrm{ds}} x_2$; ossia se e solo se $x_2 S = x_1 s_{\mathrm{sn}} S$ oppure $Sx_1 = S s_{\mathrm{ds}} x_2$; ossia, S essendo chiuso per l'operazione " $\cdot$ ", se e solo se $x_2 S = x_1 S$ oppure $Sx_1 = Sx_2$.

---

[3] *Sugg.:* ...per ogni $x \in G$, le applicazioni $\mathrm{S}_x, \mathrm{D}_x : G \to G$ definite da $y \mapsto \mathrm{S}_x(y) = xy$ e, rispettivamente, $y \mapsto \mathrm{D}_x(y) = yx$ sono biunivoche...

[4] *Def.:* L'**ordine** di un gruppo $(G,\cdot)$ è la cardinalità di G considerato come insieme. Abitualmente l'ordine G è denotato $|G|$.

[5] *Sugg.:* Si scriva $|G| = |S| \cdot |G/\varrho_{\mathrm{sn}}|$ e $|G| = |S| \cdot |G/\varrho_{\mathrm{ds}}|$

II.
Mostriamo che per ogni fissato $x \in G$ le applicazioni $\mathrm{S}_x : G \to G$ e $\mathrm{D}_x : G \to G$ definite da $y \mapsto \mathrm{S}_x(y) = xy$ e, rispettivamente, $y \mapsto \mathrm{D}_x(y) = yx$ son ben definite e biunivoche.

Che esse siano ben definite e iniettive segue dalla seguente catena di equivalenze; per ogni $y_1, y_2 \in G$ abbiamo

$$y_1 = y_2 \;\Leftrightarrow\; xy_1 = xy_2 \;\Leftrightarrow\; \mathrm{S}_x(y_1) = \mathrm{S}_x(y_2)$$

e

$$y_1 = y_2 \;\Leftrightarrow\; y_1x = y_2x \;\Leftrightarrow\; \mathrm{D}_x(y_1) = \mathrm{D}_x(y_2)$$

Che esse sian suriettive segue dalla seguente considerazione; per ogni $y \in G$ gli elementi $z_{\mathrm{sn}} = x^{-1}y \in G$ e $z_{\mathrm{ds}} = yx^{-1} \in G$, ottenuti risolvendo in $(G, \cdot)$ le equazioni e $\mathrm{S}_x(\mathrm{Z}_{\mathrm{sn}}) = x\mathrm{Z}_{\mathrm{sn}} = y$, rispettivamente, $\mathrm{D}_x(\mathrm{Z}_{\mathrm{ds}}) = \mathrm{Z}_{\mathrm{ds}}x = y$, sono preimmagini di $y \in G$ secondo S_x e, rispettivamente, D_x.

Per ogni fissato $x \in G$, le classi laterali xS e Sx altro non sono che le immagini di S secondo le applicazioni biunivoche S_x e, rispettivamente, D_x. Ne segue che, per ogni fissato $x \in G$, gli insiemi xS e, rispettivamente, Sx hanno la stessa potenza dell'insieme S; ossia, abbiamo $|xS| = |S|$ e, rispettivamente, $|Sx| = |S|$.

III.
L'insieme G, che, per ipotesi, è finito, è ripartito, secondo ϱ_{sn} e, rispettivamente, ϱ_{ds}, in un numero finito di classi. Gli insiemi di tali classi di equivalenza sono G/ϱ_{sn} e, rispettivamente, G/ϱ_{ds}; così, la loro potenza è finita e uguale a $|G/\varrho_{\mathrm{sn}}|$ e, rispettivamente $|G/\varrho_{\mathrm{ds}}|$. Ora, dal punto II. segue che tutte le classi di equivalenza modulo ϱ_{sn} e ϱ_{ds} sono equipotenti e che la loro potenza è la stessa di S. Quindi, $|G| = |G/\varrho_{\mathrm{sn}}| \cdot |S|$ e rispettivamente, $|G| = |G/\varrho_{\mathrm{ds}}| \cdot |S|$. Ne segue che $|S|$ divide l'ordine di G.

Esercizio 4. Siano $(G,\cdot)$ un gruppo ciclico e $g \in G$ un generatore di G ([6]).

Si mostri che ogni sottogruppo $S \leq G$ è ciclico.

Soluzione. Osserviamo, preliminarmente, che ogni elemento x di un gruppo ciclico $(G,\cdot)$ è del tipo $x = g^z$, con $g \in G$ generatore di $(G,\cdot)$ e $z \in \mathbb{Z}$ un intero opportuno.

Sia, ora, $S \leq G$ un sottogruppo del gruppo ciclico $(G,\cdot)$.

caso banale.
Se $S \leq G$ è banale, allora S è ciclico. Infatti, se $S = \{1_{(G,\cdot)}\}$, allora $S = \langle 0\rangle$; se, invece, $S = G$, allora S è ciclico perché, per ipotesi, tale è G.

caso non banale.
Se $S \leq G$ è non banale, allora è ciclico. Premettiamo alcune osservazioni. Innanzi tutto, essendo non banale, S contiene almeno un elemento $s \in S$ tale che $s \neq 1_{(G,\cdot)}$. Inoltre, S essendo un gruppo, anche l'inverso $s^{-1} \in G$ di $s \in S$ è un elemento di S. Infine, considerato un generatore $g \in G$ di $(G,\cdot)$, abbiamo che, se $s = g^z$, allora $s^{-1} = g^{-z}$, con $z \in \mathbb{Z} \setminus \{0\}$, essendo entrambi s e s^{-1} diversi da $1_{(G,\cdot)}$. Per cui, almeno uno tra gli interi z e $-z$ è positivo. Ora, detto $n \in \mathbb{N} \setminus \{0\}$ il minimo naturale positivo tale che g^n appartenga a S, mostreremo che $S = \langle g^n\rangle$. A tal fine, mostreremo le due inclusioni $S \supseteq \langle g^n\rangle$ e $S \subseteq \langle g^n\rangle$.

La prima inclusione, $S \supseteq \langle g^n\rangle$, segue dal fatto che S, essendo un gruppo, contiene tutte le potenze di ogni suo elemento (dunque, in particolare, tutte le potenze di $g^n \in S$).

La seconda inclusione, $S \subseteq \langle g^n\rangle$, è una conseguenza della seguente osservazione. Sia $x \in S$ un qualsivoglia elemento di S. Poiché $S \subseteq G$ e $(G,\cdot)$ è ciclico, esiste $m \in \mathbb{Z}$ tale che $x = g^m$. Tra i sottoprodotti della divisione di $m\mathbb{Z}$ per $n \in \mathbb{N} \subseteq \mathbb{Z}$ troviamo due interi q e r tali che $m = nq + r$ e $0 \leq r < n$. Quindi, da

$$S \ni x = g^m = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r$$

otteniamo che

$$g^r = g^m (g^n)^{(-q)}$$

è un elemento di S, essendo $(g^n)^q$, in quanto potenza di $g^n \in S$, un elemento di S ([7]) ed essendo, per ipotesi, $g^m = x$ un elemento di S.

Allora, per la minimalità di n, il naturale r deve necessariamente essere nullo; ossia, $r = 0$. Quindi, da $g^m = (g^n)^q g^r$, abbiamo $x = g^m = (g^n)^q$; così che g^m è un elemento di $\langle g^n\rangle$.

---

[6] *Def.:* Un gruppo $(G,\cdot)$ è **ciclico** sse esiste un elemento $g \in G$ (detto **generatore** di G) tale che G è uguale all'insieme delle potenze con esponente intero di g; ossia, sse esiste $g \in G$ tale che $G = \{g^n,\ n \in \mathbb{Z}\}$. Notazioni abituali per un gruppo ciclico G generato da $g \in G$ sono $G = \langle g\rangle$ oppure $G = (g)$.

[7] In effetti, poco sopra abbiam mostrato che $\langle g^n\rangle \subseteq S$.

Esercizio 5. Siano $(G,\cdot)$ un gruppo ciclico finito, $g \in G$ un generatore di G e $n = |G|$ l'ordine di G.

I. Si mostri che, per ogni $s \in \{1,...,n\}$, l'ordine di g^s è uguale a $n/(n,s)$ ([8]), che $\langle g^s\rangle = \langle g^{(n,s)}\rangle$ e che l'elemento $g^s \in G$ genera G se e solo se $(n,s) = 1$ ([9]).

II. Si mostri per ogni $h \in \{1,...,n\}$ tale che $h|n$ esiste uno e un solo sottogruppo di G di ordine h ([10]).

Soluzione. Nell'esibire la mia soluzione, userò alcune delle affermazioni scritte a proposito dell'esercizio 4.

Innanzi tutto, osserviamo che, poiché $(G,\cdot)$ è ciclico e di ordine finito n, se $g \in G$ è un generatore di $(G,\cdot)$, allora $g^n = 1_(G,\cdot)$ ([11]). Conseguenza immediata di quanto appena detto è che possiamo scrivere $G = \{g,\ ...,\ g^{n-1},\ g^n = 1_{(G,\cdot)}\}$.

I.
Sia $\sigma \in \mathbb{N}$ il minimo naturale tale che $(g^s)^\sigma = 1_{(G,\cdot)}$. Per mostrare che σ, l'ordine di g^s, è uguale a $n/(n,s)$, osserviamo innanzi tutto che

$$(g^s)^{(n/(n,s))} = (g^n)^{s/(n,s)} = (1_{(G,\cdot)})^{s/(n,s)} = 1_{(G,\cdot)}$$

Quindi, $\sigma \mid n/(n,s)$.

Ora, sia $m \in \mathbb{N}$ tale che $(g^s)^m = 1_{(G,\cdot)}$; allora $n \mid sm$. Quindi,

$$\frac{n}{(n,s)} \mid \frac{s}{(n,s)}m$$

e, poiché $(\frac{n}{(n,s)}, \frac{s}{(n,s)}) = 1$, allora $\frac{n}{(n,s)} \mid m$. In particolare, $\frac{n}{(n,s)} \mid \sigma$.

Pertanto, $\frac{n}{(n,s)} = \sigma$, perché entrambi sono naturali.

Porcediamo, mostrando che $\langle g^s\rangle = \langle g^{(n,s)}\rangle$. Innanzi tutto, osserviamo che, da quanto appena visto, segue che i sottogruppi $\langle g^s\rangle$ e $\langle g^{(n,s)}\rangle$ hanno entrambi ordine $n/(n,s)$. Poi, dato che $(n,s) \mid s$, possiamo scrivere $g^s = (g^{(n,s)})^{(s/(n,s))}$; così che g^s è un elemento di $\langle g^{(n,s)}\rangle$. Dunque, $\langle g^s\rangle \subseteq \langle g^{(n,s)}\rangle$. Quindi, $\langle g^s\rangle$ e $\langle g^{(n,s)}\rangle$ sono uguali, in quanto equipotenti.

Ora, per far vedere che $g^s \in G$ genera G se e solo se $(n,s) = 1$, basta considerare quanto appena mostrato. Infatti, $n/(n,s) = |\langle g^s\rangle| = |G| = n$ se e solo se $(n,s) = 1$.

II.
Da quanto mostrato nella prima parte del punto I., il sottogruppo $\langle g^{n/h}\rangle$ ha potenza

---

[8] L'ordine di un elemento x di un gruppo $(G,\cdot)$ è il minimo naturale $o(x) \in \mathbb{N}$ tale che $x^{o(x)} = 1_{(G,\cdot)}$

[9] *Not.:* Dati due interi $a_1, a_2 \in \mathbb{Z}$, denotiamo con (a_1,a_2) l'unico massimo comun divisore positivo di a_1 e a_2. Dato un elemento $x \in G$, denotiamo con $\langle x\rangle$ il sottogruppo ciclico di G generato da x.

[10] *Sugg.:* Si consideri il sottogruppo $\langle g^{n/h}\rangle$ ...

[11] Lo si dimostri mostrando che, detto $\nu \in \mathbb{N}$ il minimo naturale tale che $g^\nu = 1_{(G,\cdot)}$, allora $n = \nu$; a tal fine, basta mostrare che entrambe le ipotesi $n \lneq \nu$ e $n \gneq \nu$ porterebbero a delle tesi in contraddizione con le assunzioni fatte.

h. D'altra parte, se $S \leq G$ è un sottogruppo di $(G, \cdot)$ di ordine h, allora, per quanto mostrato nell'esercizio 4, S è un gruppo ciclico, generato da un elemento x di ordine h. Tale x, essendo $(G, \cdot)$ ciclico, è necessariamente della forma $x = g^s$. Ora, per quanto visto nella prima parte del punto I., abbiamo $h = n/(n, s)$. Dunque, $(n, s) = n/h$ e, quindi, per quanto visto nella seconda parte del punto I.,

$$S = \langle x \rangle = \langle g^s \rangle = \langle g^{(n,s)} \rangle = \langle g^{n/h} \rangle.$$

Esercizio 6. Determinare il numero di relazioni di equivalenza su $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ e stabilire quante di esse sono compatibili con l'operazione di somma ([12]), ([13]).

Soluzione. Utilizziamo la formula

$$\mathrm{eq}_n = \sum_{k=0}^{n-1} \binom{n-1}{k} \mathrm{eq}_k; \quad \mathrm{eq}_0 = 1,$$

eq_n essendo la cardinalità dell'insieme delle relazioni di equivalenza definite su un insieme finito di potenza n.

Innanzi tutto, da $\mathrm{eq}_0 = 1$, abbiamo $\mathrm{eq}_1 = 1$ e, quindi, $\mathrm{eq}_2 = 1 + 1 = 2$. Così, $\mathrm{eq}_3 = 1 + 2 \cdot 1 + 2 = 3$ e, infine, $\mathrm{eq}_4 = 1 + 3 \cdot 1 + 3 \cdot 2 + 1 \cdot 5 = 15$.

Quindi, le relazioni di equivalenza definite sull'insieme di quattro elementi $\mathbb{Z}_4$ sono in numero di 15.

Stabilire quante siano le relazioni di equivalenza compatibili con l'operazione di somma è equivalente a stabilire quanti siano i sottogruppi normali del gruppo $(\mathbb{Z}_4, +)$. Ora, poiché $(\mathbb{Z}_4, +)$ è commutativo, ogni suo sottogruppo è normale. Quindi, per rispondere alla domanda, non ci resta che contare quanti sono i sottogruppi, banali e non banali, di $(\mathbb{Z}_4, +)$. A tal fine, poiché $(\mathbb{Z}_4, +)$ è ciclico e finito, utilizziamo i risultati enunciati nell'esercizio 5; in particolare, 4 essendo l'ordine di $(\mathbb{Z}_4, +)$, utilizziamo la seguente versione dell'enunciato del punto II. dell'esercizio 5.: per ogni $h \in \{1, ..., 4\}$ tale che $h|4$ esiste uno e un solo sottogruppo di $(\mathbb{Z}_4, +)$ di ordine h. Così, i divisori (anche banali) di 4 essendo in numero di 3 (essi sono 1, 2 e 4), troviamo che le relazioni di equivalenza definite su $\mathbb{Z}_4$ e compatibili con l'operazione di somma sono in numero di 3.

Faccio notare, infine, che il sottogruppo associato al divisore 1 di 4 è $\{\bar{0}\}$, sottogruppo banale di ordine 1; il sottogruppo associato al divisore 2 di 4 è $\{\bar{0},\ \bar{2}\}$, sottogruppo non banale di ordine 2; il sottogruppo associato al divisore 4 di 4 è $\{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3}\} = \mathbb{Z}_4$, sottogruppo banale di ordine 4.

---

[12] *Sugg.:* Si mostri che $\mathbb{Z}_4$ è ciclico

[13] *Sempl.:* Per ogni $n \in \mathbb{N}$, si denoti con eq_n la cardinalità dell'insieme delle relazioni di equivalenza definite su un insieme di cardinalità n. Per il calcolo di può rivelarsi utile la seguente formula $\mathrm{eq}_n = \sum_{k=0}^{n-1} \binom{n-1}{k} \mathrm{eq}_k$, $\mathrm{eq}_0 = 1$.

Esercizio 7. Si studi la riducibilità in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$, $\mathbb{Z}[X]$ dei seguenti polinomi a coefficienti interi

$$\begin{aligned} A(X) &= X^4 + 2X^2 + 2 \\ R(X) &= 3X^8 + 3X + 2 \\ P(X) &= X^4 + 2X^3 + 2X^2 + 5X + 2 \\ E(X) &= X^4 + X^2 + 1 \end{aligned}$$

Soluzione.

A(X)
Il grado del polinomio A(X) è quattro. Quindi, e in $\mathbb{C}[X]$, e in $\mathbb{R}[X]$, il polinomio A(X) è riducibile. D'altra parte, A(X) è irriducibile e in $\mathbb{Q}[X]$, e in $\mathbb{Z}[X]$. A tal fine, per il teorema di Gauß, è sufficiente mostrare l'irriducibilità di A(X) in $\mathbb{Z}[X]$. Questa può esser dimostrata riducendo A(X) modulo 3 ([14]). Infatti, grazie a una verifica diretta, è possibile mostrare che $A_3(X) = X^4 + \bar{2}X^2 + \bar{2}$, la riduzione modulo 3 di A(X), non si decompone come prodotto di un fattore di grado 1 per uno di grado 3, né come prodotto di due fattori di grado 2. Così, dall'irriducibilità di $A_3(X)$ in $\mathbb{Z}_3[X]$, abbiamo quella di A(X) in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$.

R(X)
Il grado del polinomio R(X) è otto. Quindi, e in $\mathbb{C}[X]$, e in $\mathbb{R}[X]$, il polinomio R(X) è riducibile. D'altra parte, R(X) è irriducibile e in $\mathbb{Q}[X]$, e in $\mathbb{Z}[X]$. A tal fine, per il teorema di Gauß, è sufficiente mostrare l'irriducibilità di R(X) in $\mathbb{Z}[X]$. Questa può esser dimostrata utilizzando uno dei criterî di Eisenstein. Infatti, detti $r_0, \ldots, r_8$ i coefficienti di R(X) (così che $R(X) = \sum_{h=0}^{8} r_h X^h$), osserviamo che il numero primo $p = 3$ è tale da dividere $r_8, \ldots, r_1$, tale da non dividere r_0 e tale che $p^2 = 9$ non divida r_8. Quindi, R(X) è irriducibile in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$.

P(X)
Il grado del polinomio P(X) è quattro. Quindi, e in $\mathbb{C}[X]$, e in $\mathbb{R}[X]$, il polinomio P(X) è riducibile. Ora, grazie al criterio di selezione delle eventuali radici razionali e a una verifica diretta, è possibile vedere che il polinomio P(X) ammette la radice razionale $\alpha = -2$. Quindi, P(X) è riducibile e in $\mathbb{Q}[X]$ ('ché ammette una radice razionale) e, per il teorema di Gauß, in $\mathbb{Z}[X]$.

E(X)
Il grado del polinomio E(X) è quattro. Quindi, e in $\mathbb{C}[X]$, e in $\mathbb{R}[X]$, il polinomio E(X) è riducibile. Mostreremo, ora, che E(X) è riducibile in $\mathbb{Q}[X]$ e, quindi, per il teorema di Gauß, in $\mathbb{Z}[X]$. Innanzi tutto, osserviamo che il criterio di selezione delle eventuali radici razionali non ci è d'aiuto; infatti, gli unici razionali candidati ad esser radici di E(X) sono 1 e -1, che, evidentemente, non son radici di E(X). Ne segue che E(X) non ha fattori di grado 1 in $\mathbb{Q}[X]$. Quindi, E(X) è riducibile in $\mathbb{Q}[X]$ se e solo se è decomponibile nel prodotto di due fattori di grado 2. Supponiamo, allora, che esistano $M(X) = m_2X^2 + m_1X + m_0$ e $U(X) = u_2X^2 + u_1X + u_0$ tali che

$$E(X) = M(X)U(X)$$

[14] La riduzione di A(X) modulo 2 è $A_2(X) = X^4$, che è evidentemente riducibile.

Allora, eseguendo la moltiplicazione tra M(X) e U(X) e uguagliando i coefficienti dei termini dello stesso grado di E(X) e di M(X)U(X), otteniamo

$$\begin{array}{rcl} m_2u_2 & = & 1 \\ m_2u_1 + m_1u_2 & = & 0 \\ m_2u_0 + m_1u_1 + m_0u_2 & = & 1 \\ m_1u_0 + m_0u_1 & = & 0 \\ m_0u_0 & = & 1 \end{array}$$

Il sistema così ottenuto è compatibile; infatti, ammette la seguente soluzione

$$(m_2,\ m_1,\ m_0;\ u_2,\ u_1,\ u_0) = (1,\ 1,\ 1;\ 1,\ -1,\ 1) \in \mathbb{Q}^{3+3}$$

Quindi, i polinomi M(X) e U(X), la cui esistenza era stata solamente ipotizzata, esistono realmente; essi sono $M(X) = X^2 + X + 1$ e $M(X) = X^2 - X + 1$. Dunque, essendo in $\mathbb{Q}[X]$ lecito scrivere $E(X) = M(X)U(X)$, il polinomio E(X) è riducibile e in $\mathbb{Q}[X]$. Infine, grazie il teorema di Gauß, abbiamo che il polinomio E(X) è riducibile anche in $\mathbb{Z}[X]$.