TEST DI VERIFICA DI ALGEBRA 2

13 Novembre 2007 — generalità su gruppi e anelli

Testo con soluzioni

. . . . . .

N.B.: il simbolo *contrassegna gli esercizi un po' più complessi.*

1 — Per ogni insieme X non vuoto, definiamo *supporto* di una qualsiasi permutazione $\sigma \in \mathcal{S}(X)$ il sottoinsieme $supp\,(\sigma) := \big\{\, x \in X \,\big|\, \sigma(x) \neq x \,\big\}\ \big(\subseteq X\big)$. Definiamo poi

$$\mathcal{S}_0(X) := \big\{\, \sigma \in \mathcal{S}(X) \,\big|\, supp\,(\sigma) \text{ è sottoinsieme finito} \,\big\} \quad .$$

Si dimostri che $\mathcal{S}_0(X)$ è un sottogruppo normale del gruppo $\mathcal{S}(X)$.

Soluzione: Osserviamo che valgono le seguenti identità insiemistiche:

$$\textbf{(1)}\ supp\,(id_X) = \emptyset \qquad \textbf{(2)}\ supp\,\big(\sigma^{-1}\big) = supp\,(\sigma)$$
$$\textbf{(3)}\ supp\,(\sigma\circ\tau) \subseteq supp\,(\sigma) \bigcup supp\,(\tau) \qquad \textbf{(4)}\ supp\,\big(\tau\circ\sigma\circ\tau^{-1}\big) = \tau\big(supp\,(\sigma)\big)$$

per ogni $\sigma, \tau \in \mathcal{S}(X)$. Per dimostrarle, può essere utile osservare che

$$supp\,(\rho) = X \setminus X^{\rho}\,, \qquad \text{dove} \quad X^{\rho} := \big\{\, x \in X \,\big|\, \rho(x) = x \,\big\}\,, \quad \forall\ \rho \in \mathcal{S}(X)$$

dopo di che tali identità si dimostrano facilmente. Ne segue che

(a) $id_X \in \mathcal{S}_0(X)$, in virtù della **(1)**

(b) $\sigma \in \mathcal{S}_0(X) \implies \sigma^{-1} \in \mathcal{S}_0(X)$, in virtù della **(2)**

(c) $\sigma\,, \tau \in \mathcal{S}_0(X) \implies \sigma\circ\tau \in \mathcal{S}_0(X)$, in virtù della **(3)**

(d) $\sigma \in \mathcal{S}_0(X)\,, \tau \in \mathcal{S}(X) \implies \tau\circ\sigma\circ\tau^{-1} \in \mathcal{S}_0(X)$, in virtù della **(4)**, e del fatto che $\Big|\tau\big(supp\,(\sigma)\big)\Big| = \Big|supp\,(\sigma)\Big|$.

Le *(a)*, *(b)*, *(c)* e *(d)* provano che $\mathcal{S}_0(X)$ è un sottogruppo normale di $\mathcal{S}(X)$, q.e.d. □

2 — Sia A un anello, sia X un insieme, e sia A^X l'anello delle applicazioni da X in A. Per ogni $f \in A^X$ definiamo il sottoinsieme $supp(f) := \{ x \in X \mid f(x) \neq 0_A \} \ (\subseteq X)$, detto *supporto* di f. Definiamo poi

$$A_0^X := \{ f \in A^X \mid supp(f) \text{ è sottoinsieme finito} \} \quad .$$

Si dimostri che A_0^X è un ideale (bilatero) dell'anello A^X.

Soluzione: Osserviamo che valgono le seguenti identità insiemistiche:

$$\textbf{(1)}\ supp\big(0_{A^X}\big) = \emptyset \qquad \textbf{(2)}\ supp(-f) = supp(f)$$
$$\textbf{(3)}\ supp\big(f+\ell\big) \subseteq supp(f) \bigcup supp(\ell) \qquad \textbf{(4)}\ supp\big(f\cdot\ell\big) \subseteq supp(f) \bigcap supp(\ell)$$

per ogni $f, \ell \in A^X$. Per dimostrarle, può essere utile osservare che

$$supp(h) = X \setminus Ker(h)\ , \qquad \text{dove} \quad Ker(h) := \{ x \in X \mid h(x) = 0_A \}\ , \quad \forall\ h \in A^X$$

dopo di che tali identità si dimostrano facilmente. Ne segue che

(a) $0_{A^X} \in A_0^X$, per la **(1)**
(b) $h \in A_0^X \implies (-h) \in A_0^X$, per la **(2)**
(c) $h\,,\, k \in A_0^X \implies \big(h+k\big) \in A_0^X$, per la **(3)**
(d) $h \in A_0^X\,,\, k \in A^X \implies h\cdot k \in A_0^X\,,\, k\cdot h \in A_0^X$, per la **(4)**, usata due volte.

Le *(a)*, *(b)*, *(c)* e *(d)* provano che A_0^X è un ideale bilatero di A^X, q.e.d. □

3 — Dimostrare che gli anelli $\mathbb{Z}_{21}\Big/\big([7]_{21}\big)$ e $\mathbb{Z}_7$ sono isomorfi.

Soluzione: L'applicazione

$$\varphi\colon \mathbb{Z}_{21} \longrightarrow \mathbb{Z}_7\ , \quad [z]_{21} \mapsto \varphi\big([z]_{21}\big) := [z]_7 \qquad\qquad \forall\ [z]_{21} \in \mathbb{Z}_{21}$$

è ben definita, ed è un morfismo di anelli. Il Teorema Fondamentale di Omomorfismo per gli anelli allora assicura che φ induce un isomorfismo di anelli

$$\varphi_*\colon \mathbb{Z}_{21}\Big/Ker(\varphi) \xhookrightarrow{\cong} Im(\varphi)\ , \quad \big([z]_{21} + Ker(\varphi)\big) \mapsto \varphi_*\big([z]_{21} + Ker(\varphi)\big) := \varphi\big([z]_{21}\big)$$

Ma nel caso presente si ha $Ker(\varphi) = \big([7]_{21}\big)\ \Big(= \big\{[0]_{21}, [7]_{21}, [14]_{21}\big\}\Big)$ e $Im(\varphi) = \mathbb{Z}_7$. Pertanto φ_8 è un isomorfismo (di anelli) tra $\mathbb{Z}_{21}\Big/\big([7]_{21}\big)$ e $\mathbb{Z}_7$, i quali dunque sono isomorfi (come anelli). □

4 — Dimostrare che gli anelli $\mathbb{Z}_3$ e $\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x\,-\,[5]_{12}\,,\,[3]_{12}\big)$ sono isomorfi.

Soluzione: Il risultato si può ottenere mediante ripetute applicazioni del Teorema del Doppio Quoziente ($=:$ T.D.Q.), e del Teorema Fondamentale di Omomorfismo ($=:$ T.F.O.) per anelli. Infatti, il T.D.Q. ci dà

$$\begin{aligned}\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x\,-\,[5]_{12}\,,\,[3]_{12}\big)\;&\cong\\ \cong\;\Big(\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x\,-\,[5]_{12}\big)\Big)\Big/&\Big(\big([7]_{12}\,x\,-\,[5]_{12}\,,\,[3]_{12}\big)\Big/\big([7]_{12}\,x\,-\,[5]_{12}\big)\Big)\end{aligned}\tag{1}$$

Ora osserviamo che $\big([7]_{12}\,x\,-\,[5]_{12}\big)=\big(-\,[5]_{12}\,x\,-\,[5]_{12}\big)=\big(x+[1]_{12}\big)$, e inoltre

$$\big(ev_{-[1]_{12}}\big)_*:\;\mathbb{Z}_{12}[x]\Big/\big(x+[1]_{12}\big)\;\cong\;\mathbb{Z}_{12}\tag{2}$$

tramite l'unico isomorfismo $\big(ev_{-[1]_{12}}\big)_*$ indotto, in virtù del T.F.O., dal morfismo di anelli

$$ev_{-[1]_{12}}:\mathbb{Z}_{12}[x]\longrightarrow\mathbb{Z}_{12}\,,\quad p(x)\mapsto ev_{-[1]_{12}}\big(p(x)\big):=p\big(-[1]_{12}\big)\qquad\forall\;\;p(x)\in\mathbb{Z}_{12}[x]$$

L'ideale $\big([7]_{12}\,x\,-\,[5]_{12}\,,\,[3]_{12}\big)\Big/\big([7]_{12}\,x\,-\,[5]_{12}\big)$, nell'anello $\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x\,-\,[5]_{12}\big)$, ha per immagine, rispetto all'isomorfismo $\big(ev_{-[1]_{12}}\big)_*$ considerato in (2), l'ideale $\big([3]_{12}\big)$, nell'anello $\mathbb{Z}_{12}$. Pertanto, $\big(ev_{-[1]_{12}}\big)_*$ induce a sua volta un isomorfismo

$$\Big(\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x-[5]_{12}\big)\Big)\Big/\Big(\big([7]_{12}\,x-[5]_{12}\,,\,[3]_{12}\big)\Big/\big([7]_{12}\,x-[5]_{12}\big)\Big)\;\cong\;\mathbb{Z}_{12}\Big/\big([3]_{12}\big)\tag{3}$$

Adesso — applicando due volte il T.D.Q. — abbiamo

$$\Big(\mathbb{Z}_{12}\Big/\big([3]_{12}\big)\Big)\;\cong\;\Big(\mathbb{Z}\Big/12\,\mathbb{Z}\Big)\Big/\Big(3\,\mathbb{Z}\Big/12\,\mathbb{Z}\Big)\;\cong\;\mathbb{Z}\Big/3\,\mathbb{Z}\;=:\;\mathbb{Z}_3\tag{4}$$

Infine, mettendo insieme gli isomorfismi in (1), in (3) e in (4) otteniamo una catena di isomorfismi da $\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x-[5]_{12}\,,\,[3]_{12}\big)$ a $\mathbb{Z}_3$, la cui composizione è un isomorfismo tra questi due anelli: l'isomorfismo inverso va da $\mathbb{Z}_{12}[x]\Big/\big([7]_{12}\,x\,-\,[5]_{12}\,,\,[3]_{12}\big)$ a $\mathbb{Z}_3$, dunque questi due anelli sono isomorfi. □

5 — Determinare tutti gli ideali degli anelli $\mathbb{Z}_{63}$ e $\mathbb{Q}[x]\Big/\big(3\,x^2+13\,x-10\big)$, precisando quali tra questi ideali siano primi e quali massimali.

Soluzione: Dalla teoria generale sappiamo che:

(a) gli ideali di un anello quoziente $A\Big/I$ (come sono quelli in esame) sono tutte e sole le immagini $\pi(J)=J\Big/I$, dove indichiamo con $\pi\colon A\longrightarrow\!\!\!\!\!\rightarrow A\Big/I$ la proiezione canonica, degli ideali J di A che contengano l'ideale I. Pertanto abbiamo:

(b) in un anello commutativo unitario (come sono quelli in esame) R, un ideale K è primo, risp. massimale, se e soltanto se $R\Big/K$ è un dominio, risp. un campo.

(c) in un anello commutativo unitario R a ideali principali (cioè in cui ogni ideale sia principale, cioè del tipo $(r)=rR$), dati due ideali $I=(n)$ e $J=(d)$ si ha $I\subseteq J$ se e soltanto se $d\,\Big|\,n$, cioè d divide n (cioè n è multiplo di d).

Applichiamo queste idee ai due casi in esame:

per $\mathbb{Z}_{63}$: $A=\mathbb{Z}$, $I=63\,\mathbb{Z}\implies\mathbb{Z}$ è commutativo unitario a ideali principali, e quindi $d\,\mathbb{Z}=J\supseteq I=63\,\mathbb{Z}\iff d\,\Big|63$. Dalla fattorizzazione $63=3^2\cdot 7$ si ha

$$\begin{aligned}
&d\,\mathbb{Z}=J\supseteq I=63\,\mathbb{Z}\iff d\,\Big|63=3^2\,7\iff\\
&\iff d\in\big\{\pm1,\pm3,\pm7,\pm9,\pm21,\pm63\big\}\iff J\in\big\{\mathbb{Z},3\,\mathbb{Z},7\,\mathbb{Z},9\,\mathbb{Z},21\,\mathbb{Z},63\,\mathbb{Z}\big\}\iff\\
&\iff\pi(J)\in\Big\{\mathbb{Z}_{63}=\big([1]_{63}\big),\big([3]_{63}\big),\big([7]_{63}\big),\big([9]_{63}\big),\big([21]_{63}\big),\big([63]_{63}\big)=\big\{0_{\mathbb{Z}_{63}}\big\}\Big\}
\end{aligned}$$

e dunque gli ideali dell'anello $\mathbb{Z}_{63}$ sono tutti e soli

$$\mathbb{Z}_{63}=\big([1]_{63}\big)\,,\quad\big([3]_{63}\big)\,,\quad\big([7]_{63}\big)\,,\quad\big([9]_{63}\big)\,,\quad\big([21]_{63}\big)\,,\quad\big([63]_{63}\big)=\big\{0_{\mathbb{Z}_{63}}\big\}\tag{5}$$

tra i quali il primo e l'ultimo sono gli ideali banali di $\mathbb{Z}_{63}$. Ora, detto $K=\big([d]_{63}\big)$ uno degli ideali in (5), per $R=\mathbb{Z}_{63}$ si ha

$$R\Big/K\;=\;\mathbb{Z}_{63}\Big/\big([d]_{63}\big)\;=\;\Big(\mathbb{Z}\Big/63\,\mathbb{Z}\Big)\Big/\Big(\big(d\,\mathbb{Z}+63\,\mathbb{Z}\big)\Big/63\,\mathbb{Z}\Big)\;\cong\;\mathbb{Z}\Big/d\,\mathbb{Z}\;=:\;\mathbb{Z}_d\tag{6}$$

dove l'isomorfismo finale è dato dal Teorema del Doppio Quoziente (=: T.D.Q.). A questo punto ricordiamo che

$$\mathbb{Z}_d\text{ è un dominio}\iff d\text{ è primo}\iff\mathbb{Z}_d\text{ è un campo}\tag{7}$$

e quindi da (5), (6) e (7) possiamo concludere che gli ideali primi di $\mathbb{Z}_{63}$ sono $\big([3]_{63}\big)$ e $\big([7]_{63}\big)$, e parimenti gli ideali massimali di $\mathbb{Z}_{63}$ sono — ancora — $\big([3]_{63}\big)$ e $\big([7]_{63}\big)$.

per $\mathbb{Q}[x]\Big/\big(\,3\,x^2+13\,x-10\,\big)$: $\quad A=\mathbb{Q}[x]\,,\ \ I=\big(p(x)\big)\,,$ con $\ p(x):=3\,x^2+13\,x-10$
$\Longrightarrow$ $\mathbb{Q}[x]$ è commutativo unitario a ideali principali, e quindi

$$d(x)\,\mathbb{Q}[x]\ =\ J\ \supseteq\ I\ =\ p(x)\,\mathbb{Q}[x]\ \iff\ d(x)\,\Big|p(x)$$

Dalla fattorizzazione $\ p(x):=3\,x^2+13\,x-10=(3\,x-2)\cdot(x+5)\ $ si ha allora

$$\begin{aligned}
&d(x)\,\mathbb{Q}[x]\ =\ J\ \supseteq\ I\ =\ p(x)\,\mathbb{Q}[x]\ \iff\ d(x)\Big|\,p(x)=(3\,x-2)\,(x+5)\ \iff\\
&\iff\ d(x)\in\big\{\,c\,,\,c\,(3\,x-2)\,,c\,(x+5)\,,\,c\,p(x)\,\big\}_{c\in\mathbb{Q}\setminus\{0\}}\ \iff\\
&\iff\ J=\big(d(x)\big)\in\big\{\,(1)=\mathbb{Q}[x]\,,\,\big(3\,x-2\big)\,,\,\big(x+5\big)\,,\,\big(p(x)\big)=I\,\big\}\ \iff\\
&\iff\ \pi(J)\in\Big\{\big(\,\overline{1}\,\big)=\mathbb{Q}[x]\Big/\big(p(x)\big)\,,\,\big(\,\overline{3\,x-2}\,\big)\,,\,\big(\,\overline{x+5}\,\big)\,,\,\big(\,\overline{p(x)}\,\big)=\pi(I)=\big\{\overline{0}\big\}\Big\}
\end{aligned}$$

e dunque gli ideali dell'anello $\ R:=\mathbb{Q}[x]\Big/\big(p(x)\big)\ $ sono tutti e soli

$$R=\big(\,\overline{1}\,\big)\,,\qquad\big(3\,x-2\big)\,,\qquad\big(\,\overline{x+5}\,\big)\,,\qquad\big\{\overline{0}\big\}=\big\{0_R\big\}\tag{8}$$

tra i quali il primo e l'ultimo sono gli ideali banali di $\ R\,$. Detto poi $\ K=\big(\,\overline{d(x)}\,\big)\ $ uno degli ideali in (8), per il quoziente si ha

$$\begin{aligned}
R\Big/K\ \ &=\ \Big(\mathbb{Q}[x]\Big/\big(p(x)\big)\Big)\Big/\Big(\big(d(x)\,\mathbb{Q}[x]+p(x)\,\mathbb{Q}[x]\big)\Big/p(x)\,\mathbb{Q}[x]\Big)\ \ \cong\\
&\cong\ \mathbb{Q}[x]\Big/d(x)\,\mathbb{Q}[x]\ \ =\ \ \mathbb{Q}[x]\Big/\big(d(x)\big)
\end{aligned}\tag{9}$$

dove l'isomorfismo finale è dato dal T.D.Q. Ma adesso ricordiamo che, dato che $\mathbb{Q}[x]$ è anello dei polinomi in *una* variabile a coefficienti in un *campo*, abbiamo

$$\mathbb{Q}[x]\Big/\big(d(x)\big)\ \text{ è un dominio }\iff d(x)\text{ è irriducibile }\iff\mathbb{Q}[x]\Big/\big(d(x)\big)\ \text{ è un campo}\tag{10}$$

e quindi da (8), (9) e (10) possiamo concludere che gli ideali primi di $\ R:=\mathbb{Q}[x]\Big/\big(d(x)\big)\ $ sono $\ \big(3\,x-2\big)\ $ e $\ \big(\,\overline{x+5}\,\big)\,,$ e parimenti essi sono (tutti e soli) gli ideali massimali di $\ R\,.\ \ \square$

6 — Dimostrare che nell'anello $\mathbb{Z}[x]$ l'ideale $I := \big(x^2 - x + 3\,,\, x + 2\big)$ non è primo.

Soluzione: Dalla teoria generale sappiamo che I è primo se e soltanto se $\mathbb{Z}[x]\Big/I$ è un dominio. Ora abbiamo

$$\mathbb{Z}[x]\Big/I \;=\; \mathbb{Z}[x]\Big/\big(x^2{-}x{+}3\,,\,x{+}2\big) \overset{(a)}{\cong} \Big(\mathbb{Z}[x]\Big/\big(x{+}2\big)\Big)\Big/\Big(\big(x^2{-}x{+}3\,,\,x{+}2\big)\Big/\big(x{+}2\big)\Big) \overset{(b)}{\cong}$$
$$\overset{(b)}{\cong} \mathbb{Z}\Big/\big((-2)^2-(-2)+3\big) \;=\; \mathbb{Z}\Big/9\,\mathbb{Z} \;=:\; \mathbb{Z}_9$$

dove l'isomorfismo (a) è dato dal Teorema del Doppio Quoziente, mentre l'isomorfismo (b) invece è quello indotto, in forza del Teorema Fondamentale di Omomorfismo (per anelli), dal morfismo (di anelli)

$$ev_{-2}\colon \mathbb{Z}[x] \longrightarrow \mathbb{Z}\,, \quad p(x) \mapsto ev_{-2}\big(p(x)\big) := p\big(-2\big) \qquad\qquad \forall\; p(x) \in \mathbb{Z}[x]$$

Dunque abbiamo $\mathbb{Z}[x]\Big/I \cong \mathbb{Z}_9$, e — poiché 9 *non* è primo — l'anello $\mathbb{Z}_9$ *non* è un dominio, quindi non lo è $\mathbb{Z}[x]\Big/I$, e pertanto l'ideale I *non* è primo.

NOTA: è *sbagliato* invece l'approccio seguente: l'ideale $I := \big(x^2 - x + 3\,,\, x + 2\big)$ è generato dai due polinomi $\big(x^2 - x + 3\big)$ e $(x + 2)$, quindi (?) si calcola il M.C.D. di questi due polinomi, che chiamiamo $d(x)$, e si conclude (?) che $\mathbb{Z}[x]\Big/I$ è un dominio se e soltanto se $d(x)$ è irriducibile! In particolare, utilizzando l'algoritmo euclideo delle divisioni successive per calcolare tale M.C.D il risultato che si trova è 9: il problema ora è che $9 = \text{M.C.D.}\big(x^2 - x + 3\,,\, x + 2\big)$ genera l'ideale $(9) := 9\,\mathbb{Z}[x] = \big(9\,\mathbb{Z}\big)[x]$, e certamente $\big(9\,\mathbb{Z}\big)[x] \not\ni (x + 2)$. Dunque troviamo che $I \neq \big(9\,\mathbb{Z}\big)[x] = (9)$, e quindi anche

$$\mathbb{Z}[x]\Big/I \;\neq\; \mathbb{Z}[x]\Big/\big(\text{M.C.D.}\big(x^2 - x + 3\,,\, x + 2\big)\big)$$

per cui *non ha senso* considerare le proprietà dell'elemento $\text{M.C.D.}\big(x^2 - x + 3\,,\, x + 2\big)$.

Questo procedimento andrebbe bene, in generale, *soltanto se* al posto di $\mathbb{Z}[x]$ avessimo $\mathbb{K}[x]$, dove $\mathbb{K}$ fosse un campo. In particolare, se in $\mathbb{K}$ si ha $9 \neq 0$ allora 9 è invertibile, si ha $(9) = 9\,\mathbb{K}[x] = \mathbb{K}[x] = I$ e tutto torna...

N.B.: nondimeno, nel caso molto speciale in esame, questo procedimento — che in generale è sbagliato — potrebbe ancora avere un qualche senso, ammesso che lo si sappia "gestire". Infatti, poiché $(x + 2)$ *è un polinomio monico di grado 1, nel calcolare il M.C.D. come sopra troviamo esattamente il resto della divisione di* $\big(x^2 - x + 3\big)$ *per* $(x + 2)$, *e tale resto non è altri che* $ev_{-2}\big(x^2 - x + 3\big)$. *E però a questo punto uno concluderebbe che* $\mathbb{Z}[x]\Big/I \cong \mathbb{Z}[x]\Big/(9) \cong \mathbb{Z}_9[x]$, *il che è comunque* **sbagliato**!!! □

7 — Applicando la tecnica esposta nella dimostrazione del Teorema di Cayley, si costruisca un morfismo iniettivo del gruppo $\big(\,\mathbb{Z}_6\,;+\big)$ nel gruppo simmetrico $\big(\,\mathcal{S}_6\,;\circ\big)$.

Soluzione: Il Teorema di Cayley afferma che, per ogni gruppo G, l'applicazione

$$\lambda:\,G\longrightarrow\mathcal{S}(G)\,,\quad g\,\mapsto\lambda(g):\begin{pmatrix}G&\lhook\joinrel\longrightarrow\!\!\!\!\!\rightarrow&G\\ x&\mapsto\lambda(g)(x):=g\,x\end{pmatrix}$$

è un ben definito morfismo iniettivo del gruppo G nel gruppo simmetrico $\mathcal{S}(G)$, detto *rappresentazione regolare sinistra*. Similmente, esiste un analogo morfismo iniettivo, detto *rappresentazione regolare destra*, dato da

$$\lambda:\,G\longrightarrow\mathcal{S}(G)\,,\quad g\,\mapsto\rho(g):\begin{pmatrix}G&\lhook\joinrel\longrightarrow\!\!\!\!\!\rightarrow&G\\ x&\mapsto\rho(g)(x):=x\,g^{-1}\end{pmatrix}$$

Si noti che quando G è commutativo — come nel caso di $G=\mathbb{Z}_6$ — i due monomorfismi λ e ρ sono legati dalle semplici relazioni (tra loro equivalenti)

$$\lambda(g)\,=\,\rho\big(g^{-1}\big)\,=\,\rho(g)^{-1}\,,\quad\rho(g)\,=\,\lambda\big(g^{-1}\big)\,=\,\lambda(g)^{-1}\,,\qquad\forall\;\,g\in G$$

Applichiamo queste costruzioni al caso del gruppo $G:=\big(\,\mathbb{Z}_6\,;+\big)$. Per λ abbiamo

$$\lambda\big(\,[z]_6\,\big)\big(\,[x]_6\,\big)\,:=\,[z]_6+[x]_6\,=\,[z+x]_6\qquad\quad\forall\;\;[z]_6\in\mathbb{Z}_6\,,\;\;[x]_6\in\mathbb{Z}_6$$

mentre per ρ abbiamo

$$\rho\big(\,[z]_6\,\big)\big(\,[x]_6\,\big)\,:=\,[x]_6-[z]_6\,=\,[x-z]_6\qquad\quad\forall\;\;[z]_6\in\mathbb{Z}_6\,,\;\;[x]_6\in\mathbb{Z}_6$$

Indichiamo ora ogni elemento $[z]_6\in\mathbb{Z}_6$ con la notazione $[z]_6=\overline{z}$. Utilizzando la notazione standard per le permutazioni, scriviamo ogni σ in $\mathcal{S}(\mathbb{Z}_6)$ come prodotto di cicli disgiunti, in cui gli elementi coinvolti sono gli elementi di $\mathbb{Z}_6$ sui quali σ agisca in modo non banale. Allora i monomorfismi λ e ρ sono descritti rispettivamente da

$$\lambda\big(\,\overline{0}\,\big)=id\;\;,\qquad\lambda\big(\,\overline{1}\,\big)=\big(\,\overline{0}\,,\,\overline{1}\,,\,\overline{2}\,,\,\overline{3}\,,\,\overline{4}\,,\,\overline{5}\,\big)\;\;,\qquad\lambda\big(\,\overline{2}\,\big)=\big(\,\overline{0}\,,\,\overline{2}\,,\,\overline{4}\,\big)\big(\,\overline{1}\,,\,\overline{3}\,,\,\overline{5}\,\big)$$
$$\lambda\big(\,\overline{3}\,\big)=\big(\,\overline{0}\,,\overline{3}\,\big)\big(\,\overline{1}\,,\overline{4}\,\big)\big(\,\overline{2}\,,\overline{5}\,\big)\,,\;\;\lambda\big(\,\overline{4}\,\big)=\big(\,\overline{0}\,,\,\overline{4}\,,\,\overline{2}\,\big)\big(\,\overline{1}\,,\,\overline{5}\,,\,\overline{3}\,\big)\,,\;\;\lambda\big(\,\overline{5}\,\big)=\big(\,\overline{0}\,,\,\overline{5}\,,\,\overline{4}\,,\,\overline{3}\,,\,\overline{2}\,,\,\overline{1}\,\big)$$

e da

$$\rho\big(\,\overline{0}\,\big)=id\;\;,\qquad\rho\big(\,\overline{1}\,\big)=\big(\,\overline{0}\,,\,\overline{5}\,,\,\overline{4}\,,\,\overline{3}\,,\,\overline{2}\,,\,\overline{1}\,\big)\;\;,\qquad\rho\big(\,\overline{2}\,\big)=\big(\,\overline{0}\,,\,\overline{4}\,,\,\overline{2}\,\big)\big(\,\overline{1}\,,\,\overline{5}\,,\,\overline{3}\,\big)$$
$$\rho\big(\,\overline{3}\,\big)=\big(\,\overline{0}\,,\overline{3}\,\big)\big(\,\overline{1}\,,\overline{4}\,\big)\big(\,\overline{2}\,,\overline{5}\,\big)\,,\;\;\rho\big(\,\overline{4}\,\big)=\big(\,\overline{0}\,,\,\overline{2}\,,\,\overline{4}\,\big)\,\big(\,\overline{1}\,,\,\overline{3}\,,\,\overline{5}\,\big)\,,\;\;\rho\big(\,\overline{5}\,\big)=\big(\,\overline{0}\,,\,\overline{1}\,,\,\overline{2}\,,\,\overline{3}\,,\,\overline{4}\,,\,\overline{5}\,\big)$$

N.B.: come svolgimento corretto dell'esercizio, sarebbe bastato descrivere anche soltanto uno tra i monomorfismi λ e ρ. □

8 — Sia G un gruppo, e sia $\psi : G \longrightarrow G$ un endomorfismo di G tale che $\psi^2 = \psi$. Dimostrare che $G \cong Im(\psi) \ltimes Ker(\psi)$, cioè G è (isomorfo a) il prodotto semidiretto dei suoi sottogruppi $Im(\psi)$ e $Ker(\psi)$.

Soluzione: Dalla teoria generale sappiamo che

$$Im(\psi) \leq G \quad , \qquad Ker(\psi) \trianglelefteq G \tag{11}$$

semplicemente perché ψ è un endomorfismo (di G). Inoltre, abbiamo anche

$$Im(\psi) \bigcap Ker(\psi) = \{e_G\} \quad ; \tag{12}$$

infatti, se $g \in Im(\psi) \bigcap Ker(\psi)$, allora esiste $\gamma \in G$ tale che $g = \psi(\gamma)$, e allora — poiché $\psi^2 = \psi$, per ipotesi — si ha anche

$$g = \psi(\gamma) = \psi^2(\gamma) = \psi\big(\psi(\gamma)\big) = \psi(g) = e_G$$

dato che $g \in Ker(\psi)$, e così $g = e_G$, q.e.d. Infine, si ha anche

$$Im(\psi) \cdot Ker(\psi) = G \quad ; \tag{13}$$

infatti, per ogni $g \in G$ si ha $g = \psi(g) \cdot \psi(g)^{-1} g$, con $\psi(g) \in \psi(G) = Im(\psi)$ e $\psi(g)^{-1} g \in Ker(\psi)$, in quanto, per l'ipotesi $\psi^2 = \psi$, si ha

$$\psi\big(\psi(g)^{-1} g\big) = \psi\big(\psi(g)^{-1}\big)\, \psi(g) = \psi\big(\psi(g)\big)^{-1} \psi(g) = \big(\psi^2(g)\big)^{-1} \psi(g) = \psi(g)^{-1} \psi(g) = e_G$$

Ma allora, per risultati generali, (11), (12) e (13) danno $G \cong Im(\psi) \ltimes Ker(\psi)$. □

9 — Dimostrare che il gruppo $\big(\mathbb{C}^* ; \cdot\big)$ è (isomorfo a) il prodotto diretto dei suoi sottogruppi $\mathbb{R}_+$ e $S^1 := \big\{\, z \in \mathbb{C} \,\big|\, |z| = 1 \,\big\}$.

Soluzione: Presentiamo due metodi:

Primo metodo (diretto): È immediato dimostrare che $\mathbb{R}_+$ e S^1 sono sottogruppi di $\mathbb{C}^*$, ovviamente normali perché $\mathbb{C}^*$ è abeliano. Inoltre, si ha $\mathbb{R}_+ \bigcap S^1 = \{1\}$, l'elemento neutro di $\mathbb{C}^*$. Infine, si ha anche $\mathbb{C}^* = \mathbb{R}_+ \cdot S^1$: infatti, per ogni $z \in \mathbb{C}^*$ abbiamo $z = |z| \cdot |z|^{-1} z$, con $|z| \in \mathbb{R}_+$ e $|z|^{-1} z \in S^1$, in quanto $\big||z|^{-1} z\big| = |z|^{-1} |z| = 1$. Pertanto, per risultati generali possiamo concludere che $\mathbb{C} \cong \mathbb{R}_+ \times S^1$, q.e.d.

Secondo metodo (applicazione dell'esercizio 8): L'applicazione "modulo"

$$|\ | : \mathbb{C}^* \longrightarrow \mathbb{C}^* \,, \quad z \mapsto |z|$$

è un endomorfismo del gruppo $\big(\mathbb{C}^*\,;\cdot\big)$ tale che $|\,|^2 = |\,|$. Allora l'esercizio 8 assicura che $\mathbb{C}^* \cong Im\big(|\,|\big) \ltimes Ker\big(|\,|\big)$. Poiché però il gruppo $\mathbb{C}^*$ è abeliano, ogni suo sottogruppo è normale, e quindi possiamo dire più precisamente che $\mathbb{C}^* \cong Im\big(|\,|\big) \times Ker\big(|\,|\big)$, cioè il prodotto semidiretto in effetti è un prodotto diretto. Infine, dalle definizioni stesse abbiamo che $Im\big(|\,|\big) = \mathbb{R}_+$ e $Ker\big(|\,|\big) = S^1$, e pertanto si conclude che $\mathbb{C} \cong \mathbb{R}_+ \times S^1$, q.e.d. □

10 — Nel gruppo simmetrico su 7 elementi $\mathcal{S}_7$, si consideri la permutazione

$$\sigma := (4,5,6) \circ (5,6,7) \circ (6,7,1) \circ (1,2,3) \circ (2,3,4) \circ (3,4,5)$$

(a) Scrivere σ come prodotto di cicli disgiunti, e come prodotto di trasposizioni.
(b) Determinare la permutazione inversa σ^{-1}.
(c) Determinare la classe coniugata di σ.

<u>Soluzione</u>*:*

(a) Il calcolo dà $\sigma = (1,2,7)$ come fattorizzazione di σ in prodotto di cicli disgiunti.

(b) Dalle definizioni abbiamo

$$\begin{aligned}\sigma^{-1} \;&=\; \big((4,5,6) \circ (5,6,7) \circ (6,7,1) \circ (1,2,3) \circ (2,3,4) \circ (3,4,5)\big)^{-1} \;= \\ &=\; (3,4,5)^{-1} \circ (2,3,4)^{-1} \circ (1,2,3)^{-1} \circ (6,7,1)^{-1} \circ (5,6,7)^{-1} \circ (4,5,6)^{-1} \;= \\ &=\; (5,4,3) \circ (4,3,2) \circ (3,2,1) \circ (1,7,6) \circ (7,6,5) \circ (6,5,4) \;=\; (7,2,1)\end{aligned}$$

oppure utilizzando l'identità $\sigma = (1,2,7)$ troviamo subito $\sigma^{-1} = (1,2,7)^{-1} = (7,2,1)$.

(c) La teoria generale garantisce che la classe coniugata di σ è l'insieme di tutte le permutazioni in $\mathcal{S}_7$ che abbiano la stessa struttura ciclica di σ, cioè — nel caso in esame — l'insieme di tutti le permutazioni cicliche di lunghezza 3. □

11 — Indicando con $\mathcal{S}_n$ il gruppo simmetrico su n elementi, si dimostri che

$$\forall\ \sigma \in \mathcal{S}_n\ ,\ \exists\ \tau \in \mathcal{S}_n :\ \tau\,\sigma\,\tau^{-1} = \sigma^{-1}$$

<u>Soluzione</u>*:* Dalla teoria generale del gruppo simmetrico sappiamo che due permutazioni sono coniugate se e soltanto se hanno la stessa struttura ciclica. Ora, per ogni $\sigma \in \mathcal{S}_n$ si ha sempre che σ e σ^{-1} hanno la stessa struttura ciclica, e quindi sono coniugate. Ma questo vuol dire esattamente che esiste $\tau \in \mathcal{S}_n$ tale che $\tau\,\sigma\,\tau^{-1} = \sigma^{-1}$, q.e.d. □

12 — Sia G un gruppo, e per ogni $x \in G$ indichiamo con $[x]_\kappa$ la classe coniugata dell'elemento x. Sia poi

$$H := \left\{ h \in G \,\middle|\, \left|[h]_\kappa\right| \in \mathbb{N} \right\}$$

il sottoinsieme di tutti gli elementi di G la cui classe coniugata sia finita.

Dimostrare che H è sottogruppo normale di G.

Soluzione: Per cominciare, si ha che $\left|[e_G]_\kappa\right| = \left|\{e_G\}\right| = 1 \in \mathbb{N}$, e quindi

$$e_G \in H \quad . \tag{14}$$

Inoltre, per ogni $h \in G$ si ha

$$\left[h^{-1}\right]_\kappa = \left\{ g\,h^{-1}g^{-1} \,\middle|\, g \in G \right\} = \left\{ \left(g\,h\,g^{-1}\right)^{-1} \,\middle|\, g \in G \right\} = \left\{ k \in G \,\middle|\, k^{-1} \in [h]_\kappa \right\}$$

da cui otteniamo

$$\left|\left[h^{-1}\right]_\kappa\right| = \left|\left\{ k \in G \,\middle|\, k^{-1} \in [h]_\kappa \right\}\right| = \left|[h]_\kappa\right|$$

per cui in particolare per $h \in H$ si ha

$$h \in H \implies \left|[h]_\kappa\right| \in \mathbb{N} \implies \left|\left[h^{-1}\right]_\kappa\right| = \left|[h]_\kappa\right| \in \mathbb{N} \implies h^{-1} \in H \quad . \tag{15}$$

Infine, per ogni $h, k \in G$ si ha

$$\begin{aligned}[h\,k]_\kappa = \left\{ g\,h\,k\,g^{-1} \,\middle|\, g \in G \right\} = \left\{ g\,h\,g^{-1} \cdot g\,k\,g^{-1} \,\middle|\, g \in G \right\} \subseteq \\ \subseteq \left\{ \gamma\,h\,\gamma^{-1} \,\middle|\, \gamma \in G \right\} \cdot \left\{ \eta\,k\,\eta^{-1} \,\middle|\, \eta \in G \right\} = [h]_\kappa \cdot [k]_\kappa\end{aligned}$$

da cui otteniamo

$$\left|[h\,k]_\kappa\right| \leq \left|[h]_\kappa \cdot [k]_\kappa\right| \leq \left|[h]_\kappa\right| \cdot \left|[k]_\kappa\right|$$

perciò se in particolare $h, k \in H$ allora si ha

$$h, k \in H \implies \left|[h]_\kappa\right|, \left|[k]_\kappa\right| \in \mathbb{N} \implies \left|[h\,k]_\kappa\right| \leq \left|[h]_\kappa\right| \cdot \left|[k]_\kappa\right| \in \mathbb{N} \implies h\,k \in H \tag{16}$$

Dalle (14), (15) e (16) ricaviamo che H è un sottogruppo di G.

Per la normalità, osserviamo che per ogni $g, h \in G$ si ha $\left[g\,h\,g^{-1}\right]_\kappa = [h]_\kappa$, e quindi $\left|\left[g\,h\,g^{-1}\right]_\kappa\right| = \left|[h]_\kappa\right|$, perciò nel caso che $h \in H$ si ha anche

$$hk \in H \implies \left|[h]_\kappa\right| \in \mathbb{N} \implies \left|\left[g\,h\,g^{-1}\right]_\kappa\right| = \left|[h]_\kappa\right| \in \mathbb{N} \implies g\,h\,g^{-1} \in H \qquad \forall\ g \in G$$

che significa appunto che il sottogruppo H è normale (in G). $\square$

13 — Sia V_4 il gruppo di Klein, cioè l'insieme $\{e, i, j, k\}$ con tabella moltiplicativa

$$ij = k = ji\,, \qquad jk = i = kj\,, \qquad ki = j = ik$$
$$i^2 = j^2 = k^2 = e^2 = e\,, \quad ei = i = ie\,, \quad ej = j = je\,, \quad ek = k = ke$$

Si dimostri che il gruppo $Aut_{\mathcal{G}}(V_4)$ degli automorfismi del gruppo V_4 è isomorfo al gruppo simmetrico $\mathcal{S}\big(\{i, j, k\}\big)$, dando un isomorfismo esplicito $Aut_{\mathcal{G}}(V_4) \xrightarrow{\cong} \mathcal{S}\big(\{i, j, k\}\big)$.

Soluzione: Sia $\varphi \in Aut_{\mathcal{G}}(V_4)$ un qualunque automorfismo del gruppo V_4. In particolare avremo $\varphi(e) = e$, perché e è l'elemento neutro di V_4. Pertanto φ sarà univocamente determinato dalla sua restrizione al sottoinsieme $\{i, j, k\}$ $\big(\subsetneq V_4\big)$, che indicheremo con la notazione $\varphi\big|_{\{i,j,k\}}$. Osserviamo poi che, dato che φ è biiettiva (in particolare, è iniettiva) e $\varphi(e) = e$, si ha anche $\varphi\big(\{i, j, k\}\big) = \{i, j, k\}$, quindi la restrizione $\varphi\big|_{\{i,j,k\}}$ è una permutazione di $\{i, j, k\}$. Pertanto, l'applicazione

$$Aut_{\mathcal{G}}(V_4) \lhook\joinrel\longrightarrow \mathcal{S}\big(\{i, j, k\}\big)\ , \qquad \varphi \mapsto \varphi\big|_{\{i,j,k\}} \tag{17}$$

è ben definita — nel senso che ha effettivamente immagine in $\mathcal{S}\big(\{i, j, k\}\big)$ — ed inoltre è iniettiva perché, come già osservato, ogni $\varphi \in Aut_{\mathcal{G}}(V_4)$ è univocamente determinato dalla sua restrizione $\varphi\big|_{\{i,j,k\}}$.

È immediato verificare che l'applicazione in (17) è anche un (mono)morfismo di gruppi; infine, è immediato anche verificare — direttamente — che essa è anche suriettiva. Pertanto, tale applicazione è un isomorfismo, esattamente del tipo richiesto. □

14 — Calcolare il gruppo $Aut_{\mathcal{G}}\big(\mathbb{Z}_8\big)$ degli automorfismi del gruppo $\big(\mathbb{Z}_8\,;+\big)$, descrivendolo come insieme (di applicazioni) e precisandone la tabella moltiplicativa.

Soluzione: In generale sappiamo che per ogni $n \in \mathbb{Z}$ esiste un isomorfismo di gruppi

$$\Psi\ :\ \big(Aut_{\mathcal{G}}(\mathbb{Z}_n)\,;\circ\big) \xrightarrow{\cong} \big(U(\mathbb{Z}_n)\,;\cdot\big)\ , \qquad \varphi \mapsto \varphi\big(\overline{1}\big) \tag{18}$$

Pertanto, applicando tale risultato al caso $n = 8$, dobbiamo soltanto calcolare il gruppo $\big(U(\mathbb{Z}_8)\,;\cdot\big)$ — in particolare, la sua tabella moltiplicativa — e dalla sua descrizione ricavarne una del gruppo $\big(Aut_{\mathcal{G}}(\mathbb{Z}_8)\,;\circ\big)$ tramite l'isomorfismo inverso Ψ^{-1}.

Ora, sappiamo che

$$U(\mathbb{Z}_8) \,=\, \big\{\,\overline{z}\;\big|\,\text{M.C.D.}(z, 8) = 1\,\big\} \,=\, \big\{\,\overline{1}\,,\,\overline{3}\,,\overline{5}\,,\overline{7}\,\big\} \tag{19}$$

e da questo è immediato scrivere la tabella moltiplicativa di $U(\mathbb{Z}_8)$, nella quale gli unici prodotti non banali sono

$$\overline{3}\cdot\overline{5} = \overline{7}\quad , \qquad \overline{5}\cdot\overline{7} = \overline{3}\quad , \qquad \overline{7}\cdot\overline{3} = \overline{5}\quad ; \tag{20}$$

tenuto conto che $U(\mathbb{Z}_8)$ è commutativo, e che $\overline{1}$ ne è l'elemento neutro, tanto basta a determinare completamente la suddetta tabella moltiplicativa.

Ora, se utilizziamo la notazione

$$\varphi_{\overline{z}} := \Psi^{-1}\big(\overline{z}\big) \qquad \forall\ \overline{z} \in U(\mathbb{Z}_8) \tag{21}$$

la (18) ci dà $Aut_{\mathcal{G}}(\mathbb{Z}_8) = \big\{\, \varphi_{\overline{1}}\,,\, \varphi_{\overline{3}}\,,\, \varphi_{\overline{5}}\,,\, \varphi_{\overline{7}} \,\big\}$, dove

$$\varphi_{\overline{z}}\big(\,\overline{\zeta}\,\big) := \overline{\zeta\, z} \qquad\qquad \forall\ \ \overline{z} \in U(\mathbb{Z}_8)\ ,\ \ \overline{\zeta} \in \mathbb{Z}_8$$

e questo descrive completamente tutti gli elementi di $Aut_{\mathcal{G}}(\mathbb{Z}_8)$, come applicazioni. Inoltre, la tabella moltiplicativa del gruppo $\big(\, Aut_{\mathcal{G}}(\mathbb{Z}_8)\,;\,\circ\,\big)$ si ottiene direttamente da quella di $\big(\, U(\mathbb{Z}_8)\,;\,\cdot\,\big)$, attraverso la (20) e la (21), ricordando che Ψ^{-1} è un (iso)morfismo, per cui abbiamo $\varphi_{\overline{z_1}\,\cdot\,\overline{z_2}} = \varphi_{\overline{z_1}} \circ \varphi_{\overline{z_2}}$. In particolare, i soli prodotti non ovvi in $Aut_{\mathcal{G}}(\mathbb{Z}_8)$ sono

$$\varphi_{\overline{3}} \circ \varphi_{\overline{5}} \,=\, \varphi_{\overline{7}} \quad , \qquad \varphi_{\overline{5}} \circ \varphi_{\overline{7}} \,=\, \varphi_{\overline{3}} \quad , \qquad \varphi_{\overline{7}} \circ \varphi_{\overline{3}} \,=\, \varphi_{\overline{5}} \quad . \qquad \square$$