Appunti Aritmetica

APPUNTI DEL CORSO DI ARITMETICA TENUTO
DALLA PROF. DEL CORSO E DAL PROF. LOMBARDO

Diego Monaco
d.monaco2@studenti.unipi.it

Anno Accademico 2021-22

Premessa

Il seguente scritto è una mia rielaborazione delle note del corso di Aritmetica tenuto dalla professoressa Del Corso e dal professor Lombardo nell'anno accademico 2021-22, **le note non sono state revisionate dai suddetti prof**, nella stesura ho seguito l'ordine degli argomenti trattati dalla prof. Del Corso, partendo tuttavia dalla trattazione dei gruppi. In appendice, invece, vi sono complementi vari (per lo più a carattere teorico) tratti dalle lezioni del prof. Lombardo. Chiunque volesse aiutarmi a migliorare questi appunti può farlo segnalando eventuali errori e/o imprecisioni alla mia mail.

Ringraziamenti

Un ringraziamento a tutti coloro che mi hanno aiutato a trovare errori e che hanno dato consigli riguardo la stesura in particolare: Federico Allegri, Luca Milanese, Pietro Crovetto.

Indice

§1 Gruppi

§1.1 Definizione di gruppo

Definizione 1.1. Si dice che l'insieme non vuoto G è un **gruppo** $(G, \star)$ rispetto all'operazione $\star : G \times G \to G$ se:

- $\star$ è **associativa**: $a \star (b \star c) = (a \star b) \star c$, $\forall a, b, c \in G$.
- esiste $\exists e \in G$ l'**elemento neutro** tale che: $e \star a = a \star e$, $\forall a \in G$.
- esiste $\exists a^{-1} \in G$ l'**inverso** di ogni elemento del gruppo: $a \star a^{-1} = a^{-1} \star a$, $\forall a \in G$.

Definizione 1.2. Un gruppo si dice **abeliano** se $\star$ è **commutativa**: $a \star b = b \star a, \forall a, b \in G$.

Osservazione 1.3 — Per verificare che $(G, \star)$ è un gruppo occorre mostrare anche che $\star : G \times G \to G$, cioè che G è chiuso rispetto all'operazione $\star$:

$$\forall g_1, g_2 \in G \implies g_1 \star g_2 \in G$$

Esempio 1.4

- $\mathbb{K}$ campo $(\mathbb{K}, +, \cdot) \implies (\mathbb{K}, +)$ è un gruppo abeliano. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$, sono gruppi abeliani rispetto al $+$, mentre $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Z}/p\mathbb{Z}^*$ lo sono rispetto al $\cdot$.
- $(\mathbb{Z}, +)$ è un gruppo, $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo, $(\mathbb{Z}^*, \cdot) = \{\pm 1\}$ è un gruppo, $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ è un gruppo.
- $C_n = \{z \in \mathbb{C}^* | z^n = 1\}$, $(C_n, \cdot)$ è il gruppo delle radici n-esime dell'unità.
- Dato un insieme X, definiamo $S(X) = \{f : X \to X | f \text{ bigettiva}\}$ insieme delle permutazioni di X, $(S(X), \circ)$ è un gruppo[a].

[a] In generale $S(X)$ non è abeliano, infatti per $|X| \geqslant 3$ non è mai abeliano.

Esempio 1.5

Provare che $(C_n, \cdot)$ e $(S(X), \circ)$ sono gruppi rispetto alle relative operazioni.

Iniziamo con $(C_n, \cdot)$:

Soluzione. Per verificare che è un gruppo rispetto all'operazione $\cdot$, ci basta verificare una per una tutte le proprietà richieste dalla definizione:

(a) Chiusura: $\forall z, w \in \mathbb{C}^*$, ovvero $z^n = 1$ e $w^n = 1$, si ha $z \cdot w \in \mathbb{C}^*$:

$$(zw)^n = \underbrace{(zw) \dots (zw)}_{n-volte} = {}^{1} z^n w^n = 1 \cdot 1 = 1$$

da cui segue che $z \cdot w \in C_n$.

(b) Associatività: Poiché $\mathbb{C}^*$ è associativo, a maggior ragione $C_n \subset \mathbb{C}^*$ è associativo.

[1] Per quest'uguaglianza abbiamo utilizzato la commutatività dimostrata successivamente.

(c) Elemento Neutro: Per le proprietà delle potenze, poiché $1 \in \mathbb{C}^*$ e $1^n = 1$, segue che $1 \in C_n$.

(d) Inverso: Poiché $z \in C_n \implies z \in \mathbb{C}^*$ e $z^n = 1$, per le proprietà di gruppo $z^{-1} \in \mathbb{C}^*$, da quelle delle potenze segue invece che $z^{-1} \in C_n$, in quanto:

$$(z^{-1})^n = z^{-n} = (z^n)^{-1} = 1^{-1} = 1$$

pertanto $z^{-1} \in C_n, \forall z \in \mathbb{C}^*$.

(e) Commutatività: Segue dalla commutatività di $\mathbb{C}^*$, come nel punto (b).

□

Osservazione 1.6 (Proprietà dei numeri complessi) — Dalla teoria dei complessi segue che $|C_n| = n$, consideriamo $w_0 \in \mathbb{C}^*$ e $X = \{z \in \mathbb{C}^* | z^n = w_0\}$, sappiamo che $|X| = n$, se $w_0 \neq 0$, $(X, \cdot)$ è un gruppo se e solo se $w_0 = 1$.

Analogamente per $(S(X), \circ)$:

Soluzione. Per verificare che è un gruppo rispetto all'operazione $\circ$, ci basta verificare una per una tutte le proprietà richieste dalla definizione:

(a) Chiusura: $\forall f, g \in S(X)$ si ha $f \circ g \in S(X)$:

$$X \xrightarrow{f} X \xrightarrow{g} X \qquad (f \circ g : X \to X)$$

(b) Associatività: per verificare che $\forall f, g, h \in S(X)$: $f \circ (g \circ h) = (f \circ g) \circ h$, basta mostrare:

$$(f \circ (g \circ h))(x) = f((g \circ h))(x) = f(g(h(x)))$$
$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

dove si è seguita la regola di composizione delle funzioni da destra verso sinistra.

(c) Elemento Neutro: Se $X \neq \emptyset$, allora $(X \ni)\, id : X \longrightarrow X : x \longmapsto x$, la funzione id prende il nome di identità ed è l'elemento neutro rispetto a $\circ$.

(d) Inverso: Per le proprietà delle funzioni bigettive una funzione è bigettiva se e solo se ammette inversa e tale inversa è bigettiva a sua volta: $\forall f \in S(X)$, $\exists f^{-1} \in S(X)$ tale che $f \circ f^{-1} = id$.

□

Osservazione 1.7 (Gruppo Simmetrico) — Se $|X| = n$, allora $S(X) = S_n$ con $|S_n| = n!$, in quanto in questo caso S_n rappresenta l'insieme di tutte le permutazioni di $\{1, 2, \ldots, n\}$, esso è detto **gruppo simmetrico** su n.

Esempio 1.8 (S_3)

Consideriamo S_3 un gruppo non abeliano con 6 elementi. Definiamo due applicazioni σ e τ in S_3:

$$\sigma = \begin{matrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 1 \end{matrix} \quad \text{e} \quad \tau = \begin{matrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{matrix}$$

Come si osserva $\sigma \circ \tau \neq \tau \circ \sigma$, infatti: $\sigma \circ \tau(1) = \sigma(2) = 3$, mentre $\tau \circ \sigma(1) = \tau(2) = 1$. Oltre σ e τ in S_3 c'è anche l'identità id, che associa ogni elemento a se stesso, e le quattro funzioni composte che si possono ottenere:

$$\sigma^2 = \begin{matrix} 1 & \mapsto & 3 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 2 \end{matrix} \qquad \sigma \circ \tau = \begin{matrix} 1 & \mapsto & 3 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \end{matrix} \qquad \tau \circ \sigma^{a} = \begin{matrix} 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \end{matrix}$$

Pertanto, il gruppo simmetrico su 3 elementi è: $S_3 = \{id, \sigma, \tau, \sigma^2, \sigma \circ \tau, \tau \circ \sigma\}$.

[a] Che è uguale a $\sigma^2 \circ \tau$.

Teorema 1.9 (Proprietà Di Gruppo)

Sia $(G, \cdot)$ un gruppo allora:

(1) L'elemento neutro di G è unico.

(2) $\forall g \in G$ l'inverso di g è unico.

(3) $\forall g \in G$: $(g^{-1})^{-1} = g$.

(4) $\forall g, h \in G$: $(gh)^{-1} = h^{-1}g^{-1}$.

(5) Valgono le leggi di cancellazione a sinistra, $ab = ac \implies b = c$, ed a destra, $ba = ca \implies b = c$, $\forall a, b, c \in G$.

Dimostrazione. Dimostriamo una per volta le affermazioni del teorema:

(1) Supponiamo per assurdo che esistano due elementi neutri, siano $e_1, e_2 \in G$, possiamo scrivere:

$$e_1 = e_1 \cdot e_2 = e_2 \cdot e_1 = e_2$$

Dove abbiamo prima considerato e_2 elemento neutro e poi e_1, da ciò segue: $e_1 = e_2$.

(2) Siano a e b due inversi di $x \in G$, possiamo scrivere:

$$a = a \cdot e = a \cdot (x \cdot b) = (a \cdot x) \cdot b = e \cdot b = b$$

Come prima si vede che $a = b$.

(3) Sia $g \in G$ per mostrare che $(g^{-1})^{-1} = g$, basta far vedere che g ha le proprietà dell'inverso di g^{-1}, ovvero

$$g \cdot g^{-1} = g^{-1} \cdot g = e$$

che è vero, in quanto g^{-1} è l'inverso di g per definizione e per il punto (2) appena dimostrato, esso è unico.

(4) Come prima, per mostrare che $(gh)^{-1} = h^{-1}g^{-1}$, basta far vedere che $h^{-1}g^{-1}$ si comporta come l'inverso di gh:

$$h^{-1}g^{-1}gh = h^{-1}eh = e$$

$$ghh^{-1}g^{-1} = geg^{-1} = e$$

(5) Dimostriamo separatamente le due leggi di cancellazione, iniziando da quella a sinistra $ab = ac \implies b = c$, $\forall a, b, c \in G$:

$$b = eb = (a^{-1} \cdot a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1} \cdot a)c = ec = c$$

Pertanto: $ab = ac \implies b = c$. Dimostriamo analogamente la cancellazione a destra $ba = ca \implies b = c$, $\forall a, b, c \in G$:

$$b = be = b(a \cdot a^{-1}) = (ba)a^{-1} = (ca)a^{-1} = c(a \cdot a^{-1}) = ce = c$$

da cui: $ba = ca \implies b = c$.

□

Definizione 1.10. Dato un gruppo $(G, \star)$ ed un suo sottoinsieme $H \subseteq G$, con $H \neq \emptyset$, H si dice **sottogruppo** di G, $H \leqslant G$, se $(H, \star_H)$ è un gruppo.[2]

Esempio 1.11 (Sottogruppi Banali)
Dato un gruppo G, G ed $\{e\}$ sono sottogruppi di G.

I sottogruppi non banali di un gruppo sono detti **sottogruppi propri**.

Teorema 1.12 (Sottogruppo Di Un Gruppo)
Dato un gruppo $(G, \cdot)$ e un suo sottoinsieme $H \subseteq G$, $H \neq \emptyset$, H è un sottogruppo di G ($H \leqslant G$), se e solo se:

(1) H è chiuso rispetto a $\cdot$, $\forall h_1, h_2 \in H \implies h_1 \cdot h_2 \in H$.

(2) $\forall h \in H$ esiste $h^{-1} \in H$, tale che $h \cdot h^{-1} = h^{-1} \cdot h = e$.

Dimostrazione. Per dimostrare il teorema dobbiamo provare sia la *condizione necessaria* che la *condizione sufficiente*. La condizione necessaria del teorema è banalmente sempre verificata, poiché un sottogruppo gode delle stesse proprietà di un gruppo, pertanto sarà sempre chiuso per l'operazione ed ogni suo elemento avrà inverso nel sottogruppo. Ci resta da verificare la condizione sufficiente del teorema, ovvero, se sono valide (1) e (2), allora H è un gruppo. La via più semplice per mostrare che H è un gruppo è verificare le proprietà richieste per la definizione di gruppo, ovvero in questo caso: l'esistenza dell'elemento neutro e l'associatività.

(a) Associatività: Poiché $H \subseteq G$, essendo G un gruppo tutti i suoi elementi godranno della proprietà associativa, pertanto anche tutti quelli contenuti in H.

(b) Elemento Neutro: Se $H \neq \emptyset$, $\forall h \in H$, $\exists h^{-1} \in H \implies e = hh^{-1} \in H$, pertanto $e \in H$.

[2] $\star_H : H \times H \longrightarrow H$, cioè se H è un gruppo con l'operazione indotta da G.

Avendo provato che tutte le ipotesi sono soddisfatte, H è un gruppo, pertanto anche la condizione sufficiente del teorema è vera e quindi l'enunciato è verificato. □

Osservazione 1.13 ($\mathbb{N}$ e $\mathbb{Z}$) — $(\mathbb{N}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$ per il quale vale la (1) ma non la (2).

Esempio 1.14 (Sottogruppi)

- $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.
- $C_n < \mathbb{C}^*$.
- $\mathbb{Z}/n\mathbb{Z}^* \not< \mathbb{Z}/n\mathbb{Z}$ poiché sono gruppi rispetto ad operazioni diverse.
- Detto $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$, l'insieme dei multipli di n è un sottogruppo di $\mathbb{Z} \implies n\mathbb{Z} \leqslant \mathbb{Z}, \forall n \in \mathbb{N}$.

Proviamo che $(n\mathbb{Z}, +)$ è un gruppo.

Soluzione. Come in precedenza ci basta mostrare che soddisfa le proprietà di gruppo:

(a) Chiusura: $\forall nh, nk \in n\mathbb{Z}, nh + nk \in n\mathbb{Z}$, si vede facilmente che:

$$nk + nh = n\underbrace{(h + k)}_{\in\mathbb{Z}} \in n\mathbb{Z}$$

(b) Associatività: Come di consueto, essendo $n\mathbb{Z} \subseteq \mathbb{Z}$ e $\mathbb{Z}$ associativo, lo sarà anche $n\mathbb{Z}$.

(c) Elemento Neutro: Poiché $n|0 \implies 0 \in n\mathbb{Z}$ e $n \cdot 0 = 0 \cdot n, \forall n \in N$, 0 è l'elemento neutro di $n\mathbb{Z}$.

(d) Inverso: Sia $x \in n\mathbb{Z}$, allora $x = nk$, $k \in \mathbb{Z}$, allora possiamo scrivere$(-x) = n(-k)$, con $(-k)$ inverso di $k \in \mathbb{Z} \implies (-x) = n(-k) \in n\mathbb{Z}$, ovvero esiste sempre l'inverso di x in $n\mathbb{Z}$.

□

Osservazione 1.15 — Osserviamo due proprietà importanti:

- $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m|n$.
- $n\mathbb{Z} = m\mathbb{Z} \iff n|m \wedge n|m \implies n = \pm m$.

Corollario 1.16 (Unione Ed Intersezione Di Sottogruppi)
Dato un gruppo G e due sottogruppi $H, K \leqslant G$:

- $H \cap K \leqslant G$.
- $H \cup K \leqslant G$ se e solo se $H \subseteq K$ oppure $K \subseteq H$.

Definizione 1.17. Sia G un gruppo, diciamo **centro** del gruppo G l'insieme $Z(G) = \{g \in G | gx = xg, \forall x \in G\}$.

Teorema 1.18 (Proprietà Del Centro Di Un Gruppo)
Sia G un gruppo e sia $Z(G)$ il suo centro, vale:

(1) $Z(G) \leqslant G$.

(2) $Z(G) = G$ se e solo se G è abeliano.

Dimostrazione. Dimostriamo separatamente le due affermazioni.

(1) Utilizzando il teorema del sottogruppo visto in precedenza, possiamo dimostrare la prima affermazione del teorema provando che $Z(G)$ è chiuso per l'operazione e che ogni suo elemento ammette inverso.

(a) Chiusura:$\forall g_1, g_2 \in Z(G) \implies g_1 \cdot g_2 \in Z(G)$, consideriamo $g_1, g_2 \in Z(G)$, $g_1 x = x g_1$ e $g_2 x = x g_2$, si ha che $g_1 g_2 \in G$, poiché G è un gruppo. Consideriamo

$$(g_1 g_2)x = g_1(g_2 x) = g_1(x g_2) = (g_1 x)g_2 = (x g_1)g_2 = x(g_1 g_2)$$

$\forall x \in G$, da cui $g_1 g_2 \in Z(G)$.

(b) Inverso: Si deve dimostrare che $\forall g \in Z(G)$, $g^{-1} \in Z(G)$ (g^{-1} esiste sempre poiché G è un gruppo), deve essere $g^{-1}x = xg^{-1}$, $\forall x \in G$. Sappiamo che:

$$gx = xg$$

Moltiplichiamo per g^{-1} a sinistra:

$$g^{-1}gx = g^{-1}xg$$

$$x = g^{-1}xg$$

Moltiplichiamo per g^{-1} a destra:

$$xg^{-1} = g^{-1}xgg^{-1}$$

$$xg^{-1} = g^{-1}x$$

Ovvero $g^{-1} \in Z(G)$.

Avendo verificato (a) e (b), segue che $Z(G)$ è un sottogruppo di G.

(2) La *condizione necessaria* del teorema è vera banalmente, poiché se G è abeliano, per definizione ogni suo elemento commuta, pertanto appartiene a $Z(G)$. Per provare la *condizione sufficiente*, ovvero $G = Z(G) \implies G$ abeliano, basta osservare che $Z(G)$ è abeliano per sua definizione: $\forall g, h \in Z(G)$ si ha $gh = hg$, pertanto lo è anche G.

□

§1.2 Sottogruppi generati

Definizione 1.19. Sia G un gruppo e $x \in G$ definiamo **sottogruppo generato** da x in G l'insieme: $\langle x \rangle = \{x^k\}_{k\in\mathbb{Z}}$.

Di fatto si tratta dell'insieme delle potenze di x, per il quale valgono le usuali proprietà delle potenze.

Teorema 1.20 (Proprietà Di Un Sottogruppo Generato)
Sia G un gruppo, $x \in G$, e $\langle x \rangle$ il generato da x in G:

(1) $\langle x \rangle$ è un sottogruppo di G.

(2) $\langle x \rangle$ è abeliano.

Dimostrazione. Dimostriamo nell'ordine le tesi:

(1) Per dimostrare che $\langle x \rangle$ è un sottogruppo di G basta dimostrare che valgono le ipotesi del teorema del sottogruppo, tuttavia, essendo che gli esponenti delle potenze di x appartengono a $\mathbb{Z}$, se $\langle x \rangle \neq \emptyset$, segue subito che: $\forall x^n, x^m \in \langle x \rangle$, $x^n x^m = \underbrace{x^{n+m}}_{n+m\in\mathbb{Z}} \in \langle x \rangle$; e che $\forall x^n \in \langle x \rangle$, $\exists g^{-n} \in \langle x \rangle$.
Soddisfatte le ipotesi, segue pertanto che $\langle x \rangle$ è un gruppo.

(2) Analogamente a quanto visto sopra, essendo gli esponenti delle potenze in $\mathbb{Z}$, si osserva che:

$$\forall x^n, x^m \in \langle x \rangle\,, \qquad x^n x^m = x^{n+m} = x^{m+n} = x^m x^n$$

Pertanto $\langle x \rangle$ è un gruppo abeliano.

□

Esempio 1.21
Sia S_3 il gruppo simmetrico su 3 elementi, consideriamo:

$$\langle \sigma \rangle = \{id, \sigma, \sigma^2\} \qquad \langle \tau \rangle = \{id, \tau\}$$

Osservazione 1.22 — Se G è un gruppo finito, allora $\langle x \rangle$ è finito. Tuttavia, anche se G fosse infinito, $\langle x \rangle$ potrebbe essere finito. Ad esempio se $G = \mathbb{Z}$ e $x = 0$:

$$\langle 0 \rangle = \{k \cdot 0\}_{k\in\mathbb{Z}} = \{0\}$$

Mentre per $n \in \mathbb{Z}$, si ha:

$$\langle n \rangle = \{kn\}_{k\in\mathbb{Z}} = n\mathbb{Z}$$

che non è finito $|\langle n \rangle| = +\infty$.

Esempio 1.23

Preso $G = \mathbb{C}^*$, consideriamo la radice n-esima di 1, ovvero:

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

Il sottogruppo $\langle\zeta_n\rangle = \left\{\zeta_n^k\right\}_{k\in\mathbb{Z}}$ è composto da tutte le radici n-esime di 1, che sono al più n.

Osservazione 1.24 — Si osserva che:

- se $\langle x\rangle$ è finito, allora esiste $h > k$ tale che $x^h = x^k \implies x^{h-k} = e$, pertanto ci sono al più $h-k$ potenze di x distinte, poiché se $x^h = x^k$ le potenze di x si ripetono ciclicamente.
- se $|\langle x\rangle| = +\infty$ allora tutte le potenze di x sono distinte.

Definizione 1.25. Sia G un gruppo e $x \in G$ si definisce **ordine di un elemento** del gruppo, $\mathrm{ord}_G(x)$, il minimo intero positivo n (se esiste) per cui $x^n = e$. Se invece $x^n \neq e$ per ogni n positivo, diciamo che x ha ordine infinito.

$$\mathrm{ord}_G(x) = \min\left\{k > 0 | x^k = e\right\}$$

se:

$$\left\{k > 0 | x^k = e\right\} = \emptyset$$

allora $\mathrm{ord}_G(x) = +\infty$.

Esempio 1.26

- $\mathrm{ord}_{\mathbb{C}^*}(\zeta_n) = n$.
- $\mathrm{ord}_{\mathbb{Z}}(7) = +\infty$.

Teorema 1.27 (Ordine E Sottogruppo Generato)

Sia G un gruppo, $x \in G$ e $\mathrm{ord}(x) = d < +\infty$, allora:

(1) $\langle x\rangle = \left\{e, x, x^2, \ldots, x^{d-1}\right\}$, ovvero l'ordine del sottogruppo $\langle x\rangle$, generato da x in G, è uguale all'ordine di x ($|\langle x\rangle| = d$).

(2) $x^n = e \iff d|n$.

Dimostrazione. Proviamo separatamente le due affermazioni del teorema.

(1) Vogliamo dimostrare che $|\langle x\rangle| = d$, possiamo farlo dimostrando la doppia inclusione dell'insieme considerato con $\left\{e, x, x^2, \ldots, x^{d-1}\right\}$, mostrando che gli insiemi coincidono.

- Supponiamo che esistano due interi a e b, con (WLOG)[3] $d > a > b$, tali che $x^a = x^b$, per tali interi si avrebbe:

$$x^{a-b} = e \qquad \text{con} \quad 0 < a - b < d$$

ma ciò non è possibile, perché $d = \min\left\{k > 0 | x^k = e\right\}$, pertanto tutte le potenze $\left\{e, x, x^2, \dots, x^{d-1}\right\}$ sono distinte per costruzione, infatti, avendo definito come d l'ordine di x in G tutte le potenze tra 0 e $d-1$ devono necessariamente essere distinte, altrimenti d non sarebbe minimo (come già visto nell'Osservazione 1.24). Da ciò segue ovviamente che $\left\{e, x, x^2, \dots, x^{d-1}\right\} \subseteq \langle x \rangle \implies |\langle x \rangle| \geq d$. Abbiamo quindi dimostrato che, considerando un insieme di d potenze distinte esso è contenuto nel sottogruppo generato da x (fatto appunto da potenze distinte[4]), da cui segue la prima relazione sulla cardinalità di $\langle x \rangle$.

- Sia $x^n \in \langle x \rangle$ $(n \in \mathbb{Z})$ un qualunque elemento di $\langle x \rangle$, dividiamo n per d ottenendo $n = qd + r$ con $0 \leq r < d$, possiamo scrivere:

$$x^n = (\underbrace{x^d}_{=e})^q x^r = x^r \implies x^n = x^r \in \left\{e, x, x^2, \dots, x^{d-1}\right\}$$

ovvero $\langle x \rangle \subseteq \left\{e, x, x^2, \dots, x^{d-1}\right\} \implies |\langle x \rangle| \leq d$. Abbiamo mostrato che preso un generico elemento di $\langle x \rangle$ esso sia anche un elemento di $\left\{e, x, x^2, \dots, x^{d-1}\right\}$, da cui la seconda relazione sulla cardinalità di $\langle x \rangle$.

Da ciò segue, essendo la disuguaglianza una relazione antisimmetrica, che $|\langle x \rangle| = d$.

(2) Vogliamo dimostrare che $x^n = e \iff d|n$, per farlo dobbiamo provare separatamente la *condizione necessaria* (la freccia verso destra) e *condizione sufficiente* (la freccia verso sinistra).

- Mostriamo che $x^n = e \implies d|n$, per farlo dividiamo n per d, $n = qd + r$ con $0 \leq r < d$, poiché:

$$x^n = (\underbrace{x^d}_{=e})^q x^r = x^r = e \implies r = 0$$

ovvero $d|n$. Pertanto, supposto che $x^n = e$, dividendo n per d otteniamo sempre resto nullo nella divisione, in quanto $x^r = e$, con $r < d = \text{ord}(x)$ è possibile solo se $r = 0$.

- Proviamo il viceversa $d|n \implies x^n = e$, in tal caso basta osservare che $n = qd$, segue:

$$x^n = (\underbrace{x^d}_{=e})^q = e$$

Quindi, essendo n un multiplo dell'ordine di x si osserva facilmente, attraverso le proprietà delle potenze, che $x^n = e$.

□

[3] Without Loss of Generality, "Senza Perdita di Generalità", ovvero, essendo il caso $a < b < d$ identico al caso $b < a < d$ non è necessario che anche esso venga dimostrato, pertanto facendo questa assunzione di simmetria nella dimostrazione, ci basta dimostrare solo un caso essendo tutti gli altri di dimostrazione analoga.

[4] Come visto nell'osservazione 1.24, essendo $\langle x \rangle$ finito, ad un certo punto le potenze ciclano e quindi gli elementi si ripetono e sono tutti distinti.

Esempio 1.28

Se, ad esempio, avessimo $x^{100000} \equiv 1 \pmod 7$, con $x \in \mathbb{Z}/7\mathbb{Z}^*$, per il Teorema di Eulero si ha:

$$x^{\phi(7)} \equiv 1 \pmod 7 \implies {}^{a} \operatorname{ord}(x) | \phi(7) = 6$$

Inoltre:

$$x^{100000} \equiv 1 \pmod 7 \implies \operatorname{ord}(x) | 100000$$

Da cui $\operatorname{ord}(x) | (6, 100000) = 2$, cioè l'ordine di x è proprio 2[b]:

$$x^{100000} \equiv 1 \pmod 7 \iff x^2 \equiv 1 \pmod 7 \iff x \equiv \pm 1 \pmod 7$$

[a] Per quanto dimostrato nel punto (2) del Teorema 1.27.
[b] In realtà potrebbe essere anche $\operatorname{ord}(x) = 1$ ed in tal caso $x = \overline{1}$, ma da $x^2 \equiv 1 \pmod 7$ otteniamo anche questo valore.

Osservazione 1.29 — Se $\operatorname{ord}(x) = +\infty$, allora $|\langle x \rangle| = +\infty$.

§1.3 Gruppi ciclici

Definizione 1.30. Un gruppo G si dice **ciclico** se esiste $x \in G$ tale che $G = \langle x \rangle$. In tal caso x prende il nome di **generatore** di G.

Esempio 1.31

- $\mathbb{Z}$ è ciclico, infatti: $\mathbb{Z} = \langle 1 \rangle = \{k \cdot 1\}_{k\in\mathbb{Z}} = \{k\}_{k\in\mathbb{Z}}$. Nel caso di $\mathbb{Z}$, ± 1 sono gli unici generatori possibili.
- $\mathbb{R}$ non è ciclico.
- $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle = \{k[1]_n\}_{k\in\mathbb{Z}} = \{[k]_n\}_{k\in\mathbb{Z}}$.
- $\mathbb{Z}/8\mathbb{Z}^*$ non è ciclico, infatti $\mathbb{Z}/8\mathbb{Z}^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, non contiene alcun elemento di ordine 4 (l'ordine del gruppo), che quindi possa generare tutti suoi elementi.
- Siano p e q primi distinti, $\mathbb{Z}/pq\mathbb{Z}^*$ non è mai ciclico. Infatti, essendo $\phi(pq) = (p-1)(q-1)$, si può mostrare che $x^{\frac{(p-1)(q-1)}{2}} \equiv 1 \pmod{pq}$, $\forall x \in \mathbb{Z}$.

Esercizio 1.32. Provare che $\mathbb{Z}/11\mathbb{Z}^*$ è ciclico.

Soluzione. Per provare che $\mathbb{Z}/11\mathbb{Z}^*$ è ciclico basta trovare un elemento $x \in \mathbb{Z}/11\mathbb{Z}^*$ tale che $\text{ord}(x) = \phi(11) = 10$. Per il Teorema di Eulero sappiamo che: $x^{\phi(11)} \equiv 1 \pmod{11} \implies \text{ord}(x) | 10$, ovvero $\text{ord}(x) \in \div(10) = \{1, 2, 5, 10\}$. Si trova facilmente che:

$$2^5 \equiv -1 \pmod{11} \implies 2^{10} \equiv 1 \pmod{11} \implies \text{ord}(\overline{2}) = 10 \implies \mathbb{Z}/11\mathbb{Z}^* = \langle \overline{2} \rangle$$

□

Teorema 1.33 (Sottogruppo Di Un Gruppo Ciclico)
Ogni sottogruppo di un gruppo ciclico è ciclico.

Dimostrazione. Sia G un gruppo ciclico, ovvero tale che esiste g in G per cui $G = \langle g \rangle$, e sia H un sottogruppo di G ($H \leqslant G$), distinguiamo due casi

- Se $H = \{e\}$ allora $H = \langle e \rangle$.
- Se $\{e\} \subsetneq H$, allora esiste $h \in H$ ($h \neq e$) tale che $h = g^k$ ($k \in \mathbb{Z}$), inoltre, poiché H è un sottogruppo di G, segue che $g^k, g^{-k} \in H$, in tal caso posso prendere $k > 0$ e definire un insieme S:
$$S = \{m > 0 | g^m \in H\}$$
se $S \neq \emptyset$, si ha $S \subset \mathbb{N}$ e per il Principio del Minimo S ammette elemento minimo, sia esso m_0 (per quanto appena visto $g^{m_0} \in H$). Sia g^n un generico elemento di H, dividendo n per m_0, si ha: $n = qm_0 + r$ con $0 \leq r < m_0$, segue:
$$g^n = g^{m_0 q + r} = (g^{m_0})^q g^r$$
quindi:
$$g^r = (g^{m_0})^{-q} g^n$$

Poiché $g^{m_0} \in H$ per costruzione, così sarà anche il suo inverso (ricordiamo che per ipotesi $H \leqslant G$) $(g^{m_0})^{-1} \in H$. Per la proprietà di chiusura di H segue che $(g^{m_0})^{-q} g^n \in H \implies g^r \in H \implies r \in S$, tuttavia $r < m_0$ e m_0 è stato definito come il minimo di S, pertanto segue che $r = 0$, ovvero $m_0 | n$.
Pertanto $h = g^n = (g^{m_0})^q$, si conclude che un qualsiasi elemento $h = g^n$ di H è un potenza di g^{m_0}, quindi, segue dalla definizione che $H = \langle g^{m_0} \rangle$ è ciclico.

□

Osservazione 1.34 (Sottogruppi Di $\mathbb{Z}$) — Come già osservato i sottogruppi di $\mathbb{Z}$ sono tutti del tipo $n\mathbb{Z}$, $n \in \mathbb{Z}$, inoltre $n\mathbb{Z} = m\mathbb{Z} \iff m = \pm n$. Per quanto appena visto $\mathbb{Z}$ è un gruppo ciclico ($\mathbb{Z} = \langle 1 \rangle$) dunque ogni suo sottogruppo sarà ciclico a sua volta ($n\mathbb{Z}$ ciclico $\forall n \in \mathbb{Z}$), infatti si che $n\mathbb{Z} \leq \mathbb{Z} \implies n\mathbb{Z} = \langle n \rangle$ [a]
Inoltre:

$$n\mathbb{Z} = m\mathbb{Z} \iff \langle n \rangle = \langle m \rangle \iff n\mathbb{Z} \subset m\mathbb{Z} \wedge m\mathbb{Z} \subset n\mathbb{Z}$$

[a] Ricordiamo di star utilizzando la notazione esponenziale per la somma, rispetto alla quale $\mathbb{Z}$ e $n\mathbb{Z}$ sono gruppi, pertanto $\langle n \rangle = \{kn\}_{k \in \mathbb{Z}}$.

Esercizio 1.35. Dimostrare che $n\mathbb{Z} \subseteq m\mathbb{Z}$ se e solo se $m | n$.

Soluzione. Dimostriamo separatamente condizione necessaria e sufficiente:

- Proviamo che $n\mathbb{Z} \subseteq m\mathbb{Z} \implies m | n$, si osserva che se prendiamo $n \in m\mathbb{Z} \implies n = hm$ (per $h \in \mathbb{Z}$), pertanto n multiplo di $m \implies m | n$.
- Proviamo che $m | n \implies n\mathbb{Z} \subseteq m\mathbb{Z}$, se $m | n \implies n = mk$ (con $k \in \mathbb{Z}$), da cui $n \in m\mathbb{Z}$, se $x \in n\mathbb{Z} \implies x = nz$ (con $z \in \mathbb{Z}$), da cui $x = nz = m(kz) \implies x \in m\mathbb{Z} \implies n\mathbb{Z} \subseteq m\mathbb{Z}$.

□

Osservazione 1.36 (Il Gruppo $\mathbb{Z}/n\mathbb{Z}$) — È un gruppo ciclico $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$, con $\operatorname{ord}(\overline{1}) = n$. Per $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ si ha $\operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}}(\overline{a}) = \min\{k > 0 | k\overline{a} = \overline{0}\}$. Per determinare l'ordine devo risolvere la congruenza:

$$xa \equiv 0 \pmod{n}$$

Sia $d = (a, n)$, allora $a = a_1 d$ e $n = n_1 d$, da cui $(a_1, n_1) = 1$, pertanto:

$$a_1 dx \equiv 0 \pmod{n_1 d} \implies a_1 x \equiv 0 \pmod{n_1} \implies x \equiv 0 \pmod{n_1}$$

La minima soluzione positiva è:

$$x = n_1 = \frac{n}{(a, n)} \quad \text{(Ottenuta per } k = 1\text{)}$$

In generale vale quindi:

$$\boxed{\operatorname{ord}_n(\overline{a}) = \frac{n}{(a, n)}}$$

In particolare $\operatorname{ord}(\overline{a}) | n$.

Esempio 1.37 ($\mathbb{Z}/20\mathbb{Z}$)

Il gruppo $\mathbb{Z}/20\mathbb{Z}$ ha ordine $20 = 2^2 \cdot 5$. Pertanto l'ordine di un suo elemento random $\overline{a} \in div(20) = \{1, 2, 4, 5, 10, 20\}$, in generale:

$$\text{ord}(\overline{a}) = \frac{n}{(a,n)} = \frac{20}{(a,20)}$$

Pertanto, abbiamo:

- $\text{ord}(\overline{a}) = 1 \iff (a,20) = 20 \implies \overline{a} = \overline{0}$, ovvero $\phi(1)$ elementi di ordine 1.
- $\text{ord}(\overline{a}) = 2 \iff (a,20) = 10$[a] $\implies \overline{a} = \overline{10}$, ovvero $\phi(2)$ elementi di ordine 2.
- $\text{ord}(\overline{a}) = 4 \iff (a,20) = 5 \implies \overline{a} = \{\overline{5}, \overline{15}\}$, ovvero $\phi(4)$ di ordine 4.
- $\text{ord}(\overline{a}) = 5 \iff (a,20) = 4 \implies \overline{a} = \{\overline{4}, \overline{8}, \overline{12}, \overline{16}\}$, ovvero $\phi(5)$ di ordine 5.
- $\text{ord}(\overline{a}) = 10 \iff (a,20) = 2 \implies \overline{a} = \{\overline{2}, \overline{6}, \overline{14}, \overline{18}\}$, ovvero $\phi(10)$ di ordine 10.
- $\text{ord}(\overline{a}) = 20$[b] $\iff (a,20) = 1 \implies \overline{a} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$, ovvero proprio $\phi(20)$ di ordine 20.

[a] A questo punto il problema diventa combinatorio, infatti in tutti i casi, per contare gli a che vanno bene per il calcolo dell'M.C.D., basterà contare i multipli dell'M.C.D. minori di 20 e poi aggiungere/sottrarre i multipli dell'M.C.D. e degli altri fattori di 20 non comuni ad a.
[b] Ovvero $\overline{a}$ è un generatore di $\mathbb{Z}/20\mathbb{Z}$.

Corollario 1.38

(1) $\forall \overline{a} \in \mathbb{Z}/n\mathbb{Z}$: $\text{ord}(\overline{a}) | n$.[a]

(2) $\overline{a}$ genera $\mathbb{Z}/n\mathbb{Z} \iff (a,n) = 1$, ovvero $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$, quindi $\mathbb{Z}/n\mathbb{Z}$ ha $\phi(n)$ generatori.

(3) $\forall d | n$ in $\mathbb{Z}/n\mathbb{Z}$ ci sono esattamente $\phi(d)$ elementi di ordine d.[b] [c]

[a] Come vedremo è una conseguenza del Teorema Di Lagrange.
[b] Questo risultato è vero per un qualsiasi gruppo ciclico finito G.
[c] Quindi in un gruppo ciclico di ordine $n < +\infty$ ci sono esattamente $\phi(n)$ generatori.

Dimostrazione. Proviamo l'affermazione (3). Consideriamo una classe $\overline{a}$ generica, sia $\text{ord}(\overline{a}) = \frac{n}{(a,n)} = d$ ovvero $(a,n) = \frac{n}{d}$ da cui:

$$a = \frac{n}{d}k \text{[5]} \qquad \text{dove deve essere} \qquad (k,d) = 1$$

Poiché:

$$(a,n) = \left(\frac{n}{d}k, n\right) = n\left(\frac{k}{d}, 1\right) = \frac{n}{d}(k,d) = \frac{n}{d} \implies (k,d) = 1$$

Osserviamo che:

$$0 \leq a < n \text{[6]} \implies 0 \leq \frac{n}{d}k < n \implies 0 \leq \frac{k}{d} < 1 \implies 0 \leq k < d$$

[5] Per la proprietà fondamentale dell'M.C.D.
[6] Ricordiamo che $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, pertanto $\overline{0} \leq \overline{a} \leq \overline{n-1}$.

Pertanto il numero di k tali che $0 \leq k < d$ e $(k,d) = 1$ è proprio $\phi(d)$ (quindi possiamo scrivere $\phi(d)$ classi $\overline{a} \in \mathbb{Z}/20\mathbb{Z}$ distinte, aventi ordine d). □

Corollario 1.39

$$\sum_{d|n} \phi(d) = n$$

Dimostrazione. Sia $n = |\mathbb{Z}/n\mathbb{Z}|$, si osserva che:

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n}{}^{\cdot} X_d \quad \text{con } X_d = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | \operatorname{ord}(\overline{a}) = d\}$$

Ovvero $\mathbb{Z}/n\mathbb{Z}$ è l'unione di tutti gli insiemi che contengono gli elementi di $\mathbb{Z}/n\mathbb{Z}$ divisi per ordine. Segue:

$$n = \sum_{d|n} |X_d|$$

Ma per quanto visto $|X_d| = \phi(d)$, pertanto:

$$n = \sum_{d|n} \phi(d)$$

Ovvero la tesi. □

Osservazione 1.40 (Sottogruppi Di $\mathbb{Z}/n\mathbb{Z}$) — Dal teorema dei gruppi ciclici segue subito che i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono a loro volta ciclici, in particolare sia $H \leqslant \mathbb{Z}/n\mathbb{Z}$, allora $H = \langle \overline{a} \rangle$ e per quanto visto l'ordine di un sottogruppo generato da un elemento di un gruppo è proprio l'ordine dell'elemento nel gruppo $|H| = \operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}}(\overline{a})$. Inoltre, segue dal Corollario 1.38 precedente che ci sono sottogruppi di ordine d se e solo se $d|n$.

Teorema 1.41 (Sottogruppi Di $\mathbb{Z}/n\mathbb{Z}$)

Il gruppo $\mathbb{Z}/n\mathbb{Z}$ ha un unico sottogruppo di ordine d tale che $d|n$.

Dimostrazione. Sia $H \leqslant \mathbb{Z}/n\mathbb{Z}$, con $H = \langle \overline{a} \rangle$, allora, unendo quanto visto nell'osservazione sopra all'ultimo corollario, $|H| = \operatorname{ord}(\overline{a}) = d|n$. Consideriamo:

$$H_d = \left\{ \overline{0}, \frac{\overline{n}}{d}, 2\frac{\overline{n}}{d}, \dots, (d-1)\frac{\overline{n}}{d}, \right\} = \left\langle \frac{\overline{n}}{d} \right\rangle$$ [7] [8]

H_d contiene tutti gli elementi di ordine d[9] $\left(\frac{\overline{n}}{d}k \text{ e } (k,d) = 1\right)$, pertanto, ogni sottogruppo di ordine d coincide con H_d. □

[7] Si osserva subito che tutti gli elementi di H_d sono contenuti in $\left\langle \frac{n}{d} \right\rangle = \left\{k(\frac{n}{d})\right\}_{k \in \mathbb{Z}}$, inoltre i due insiemi hanno la stessa cardinalità (e come già visto in precedenza sono composti da elementi distinti, per la minimalità di di), pertanto coincidono.

[8] Per quanto visto nell'osservazione degli ordini in $\mathbb{Z}/n\mathbb{Z}$, si vede che $\frac{n}{d} = (a,n)$, quindi H_d è composto da elementi ottenuti come $\overline{(a,n)}k$ con $0 \leq k < d$.

[9] Moltiplicando ogni elemento di H_d per $\overline{d}$ si ottiene $\overline{n}k = \overline{0}$.

§1.4 Omomorfismi

Definizione 1.42. Siano $(G, \star)$ e $(G', \star')$ due gruppi, l'applicazione $f : G \longrightarrow G'$ è un **omomorfismo** di gruppi se:

$$f(x \star y) = f(x) \star' f(y) \qquad \forall x, y \in G$$

Esempio 1.43 (Omomorfismi Di Gruppi)

- Siano G e G' gruppi, l'applicazione $f : G \longrightarrow G' : x \longmapsto e'$ è un omomorfismo di gruppi, infatti:
$$f(\underbrace{x \star y}_{\in G}) = f(z) = e'$$
$$f(x) \star' f(y) = e' \star' e' = e'$$
- $id : G \longrightarrow G : x \longmapsto x$.
- $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : a \longmapsto \overline{a}$. Poiché
$$\pi(a + b) = \overline{a + b} = {}^{a}\overline{a} + \overline{b} = \pi(a) + \pi(b)$$
- $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \cdot) : x \longmapsto e^x$. Si verifica facilmente che:
$$\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x) \cdot \varphi(y)$$

.

[a] L'uguaglianza è giustificata dalla definizione di addizione tra classi.

Esercizio 1.44. Verificare che $\pi_{m,n} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} : [a]_n \longmapsto [a]_m$ è un omomorfismo di gruppi.

Soluzione. Osserviamo che la funzione è ben definita, in quanto cambiando rappresentati alle classi il risultato non varia. A questo punto, per le proprietà delle classi di resto, segue banalmente che la classe modulo m della somma di due interi modulo n è uguale alla somma delle classi modulo m degli interi modulo n:

$$\pi_{n,m}([a]_n + [b]_n) = \pi_{n,m}([a]_n) + \pi_{n,m}([b]_n) \qquad \forall [a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$$

□

Definizione 1.45. Dati G, H gruppi, ed un omomorfismo tra loro $f : G \longrightarrow H$, si definisce **nucleo** dell'omomorfismo f, l'immagine inversa del sottogruppo banale $\{e_H\}$, ovvero:

$$\ker f = \{g \in G | f(g) = e_H\} = f^{-1}(e_H)$$

Teorema 1.46 (Proprietà Degli Omomorfismi)
Sia $f : G \longrightarrow G'$ un omomorfismo tra gruppi, allora valgono le seguenti:

(1) $f(e) = e'$.

(2) $f(x^{-1}) = (f(x))^{-1}$, $\forall x \in G$.

(3) $\forall H \leqslant G$, $f(H) \leqslant G'$. In particolare $f(G) \leqslant G'$.

(4) $\forall K \leqslant G'$, $f^{-1}(K) \leqslant G$. In particolare $\ker f = f^{-1}(\{e'\}) \leqslant G$.

(5) f è iniettivo se e solo se $\ker f = \{e\}$.

(6) Se f è bigettiva, allora f^{-1} è un omomorfismo.

Dimostrazione. Proviamo singolarmente le proprietà:

(1) Si osserva che $f(e) = f(e \cdot e) = f(e) \cdot' f(e) \implies f(e) = f(e) \cdot' f(e)$, dove applicando la legge di cancellazione a sinistra dei gruppi, si ottiene $f(e) = e'$. [10] [11]

(2) Per dimostrare la tesi basta osservare che $e' = f(e) = f(g \cdot g^{-1}) = f(g) \cdot' f(g^{-1})$ e dunque per definizione di $(f(g))^{-1}$ in G' otteniamo $(f(g))^{-1} = f(g^{-1})$.

(3) Per provare che $f(H) \leqslant G'$ è sufficiente verificare le ipotesi del teorema sui sottogruppi precedentemente dimostrato:

   (a) Per prima cosa, mostriamo che l'insieme $f(H)$ è chiuso rispetto all'operazione $\cdot'$ (ristretta a $f(H)$[12]), dobbiamo ciè mostrare che $\forall f(h_1), f(h_2) \in f(H)$ si ha $f(h_1) \cdot' (h_2) \in f(H)$. Ci basta osservare che dalla proprietà fondamentale di omomorfismo segue:

$$f(h_1) \cdot' f(h_2) = f(\underbrace{h_1 \cdot h_2}_{\in H}) \implies f(h_1 \cdot h_2) \in f(H) \implies f(h_1) \cdot' f(h_2) \in f(H)$$

   (b) Ci rimane da mostrare che $\forall f(h) \in f(H)$, $\exists f^{-1}(h) \in f(H)$. Osserviamo che poiché H è un sottogruppo di G, allora $\forall h \in H$, $\exists h^{-1} \in H$ tale che $f(h^{-1}) \in f(H)$, e per quanto visto nella (2), segue che $f(h^{-1}) = f^{-1}(h)$.

(4) Per prima cosa osserviamo che $f^{-1}(K) = \{x \in G | f(x) \in K\}$, per provare che $f^{-1}(K) \leqslant G$ utilizziamo il teorema dei sottogruppi:

   (a) Proviamo che $\forall x, y \in f^{-1}(K)$ si ha $xy \in f^{-1}(K)$. Se $x, y \in f^{-1}(K) \implies f(x), f(y) \in K (\leqslant G')$, da cui $f(x) \cdot' f(y) \in K$, ma per la proprietà di omomorfismo $f(x) \cdot' f(y) = f(xy) \implies f(xy) \in K \implies xy \in f^{-1}(K)$.

   (b) Ci resta da dimostrare che $\forall x \in f^{-1}(K)$, $\exists x^{-1} \in f^{-1}(K)$. Se $x \in f^{-1}(K) \implies f(x) \in K (K \leqslant G')$, da cui $f^{-1}(x) = f(x^{-1}) \in K$, pertanto $x^{-1} \in f^{-1}(K)$ (l'esistenza di x^{-1} in G è assicurata dal fatto che G sia un gruppo).

(5) Proviamo entrambe le condizioni:

[10] Alternativamente la dimostrazione si può fare considerando un elemento $g \in G$ e notando che $f(g) = f(g \cdot e) = f(g) \cdot' f(e) \implies f(g) = f(g) \cdot' f(e)$, ripetendo anche a sinistra si osserva che $f(e)$ si comporta come l'elemento neutro di G', pertanto $f(e) = e'$.

[11] La tesi di questa dimostrazione ci permette di affermare che il nucleo di un omomorfismo non è mai vuoto, infatti contiene sempre almeno e.

[12] $\cdot' : f(H) \times f(H) \longrightarrow f(H)$

(a) Mostriamo che se f è iniettivo, allora $\ker f = \{e\}$. Se f è iniettivo, per definizione esiste un unico elemento $x \in G$ tale che $f(x) = e'$ e per quanto visto nella (1) deve essere che $x = e$, pertanto:

$$\ker f = \{x \in G | f(x) = e'\} = \{e\}$$

.

(b) Ora proviamo che se $\ker f = \{e\}$, allora f è iniettivo. Supponiamo che esistano $x, y \in G$ tali che $f(x) = f(y)$ (ovvero f non iniettivo), per la proprietà di omomorfismo che $f(x) \cdot' f^{-1}(y) = e' \implies f(x) \cdot' f(y^{-1}) = e'$, ma si osserva che $f(x) \cdot' f(y^{-1}) = f(x \cdot y^{-1})$, dove si era posto per ipotesi che $\ker f = \{e\}$, pertanto $xy^{-1} = e \implies x = y$ (moltiplicando a destra per y). Pertanto f è iniettivo per definizione.

(6) Per provare che f^{-1} è un omomorfismo è sufficiente verificare la definizione, ovvero: $f^{-1}(f(g_1) \cdot' f(g_2)) = f^{-1}(f(g_1)) \cdot f^{-1}(f(g_2))$, $\forall g_1, g_2 \in G$ (dove per l'ipotesi di bigettività di f sappiamo che $\mathrm{Im} f = G'$, quindi ogni elemento di G' si può scrivere come $f(g)$ per $g \in G$). Si osserva che:

$$f^{-1}(\underbrace{f(g_1) \cdot' f(g_2)}_{=f(g_1 \cdot g_2)}) = \underbrace{f^{-1}(f(g_1))}_{=g_1} \cdot \underbrace{f^{-1}(f(g_2))}_{=g_2}$$

$$f^{-1}(f(g_1 \cdot g_2)) = g_1 \cdot g_2 \implies g_1 \cdot g_2 = g_1 \cdot g_2 \quad \forall g_1, g_2 \in G$$

Ovvero la definizione di omomorfismo per f^{-1} è verificata per ogni elemento di G (e quindi di G' per l'ipotesi di bigettività).

□

Teorema 1.47 (Ordini Ed Omomorfismi)

Sia $f : G \longrightarrow G'$ un omomorfismo tra gruppi, allora vale che:

- $\mathrm{ord}(f(x)) | \mathrm{ord}(x)$, $\forall x \in G$.[a]
- f è iniettivo se e solo se $\mathrm{ord}(f(x)) = \mathrm{ord}(x)$, $\forall x \in G$.

[a] Si considera convenzionalmente, in questo caso, che $n | +\infty$, $\forall n \in \mathbb{N}$.

Dimostrazione. Proviamo singolarmente le proprietà:

(1) Sia $\mathrm{ord}(x) = d < +\infty$, quindi $x^d = e$, si nota che:

$$f^d(x) = \underbrace{f(x) \cdot' \ldots \cdot' f(x)}_{d-volte} = f(\underbrace{x \cdot \ldots \cdot x}_{d-volte}) = f(x^d) = f(e) = e'$$

quindi per il (2) del Teorema 1.27, segue che, poiché $f^d(x) = e'$, $\mathrm{ord}(f(x)) | \mathrm{ord}(x) (= d)$. Se $\mathrm{ord}(x) = +\infty$ non c'è bisogno di dimostrare nulla.

(2) Dimostriamo separatamente le due condizioni:

(a) Proviamo che se $\mathrm{ord}(f(x)) = \mathrm{ord}(x)$, allora f è iniettivo. Sfruttando il punto (5) del Teorema 1.46, ci basta dimostrare che se $\mathrm{ord}(f(x)) = \mathrm{ord}(x)$, allora $\ker f = \{e\}$ [13] . Sia $x \in \ker f$, si ha che $f(x) = e'$, allora $\mathrm{ord}(f(x)) = 1 \implies \mathrm{ord}(x) = 1$ (per ipotesi), allora $x = e$, pertanto $\ker f = \{e\} \iff f$ è iniettivo.

[13] Per quanto visto in precedenza, stiamo dimostrando una tesi equivalente a quella data.

(b) Dimostriamo ora che se f è iniettivo, allora $\operatorname{ord}(f(x)) = \operatorname{ord}(x)$. Se $\operatorname{ord}(f(x)) = +\infty \implies \operatorname{ord}(f(x)) | \operatorname{ord}(x) \implies \operatorname{ord}(x) = +\infty$.
Sia $\operatorname{ord}(f(x)) = n < +\infty$, allora $f^n(x) = e'$, inoltre $f^n(x) = f(x^n) = e'$, poiché, per ipotesi, f è iniettivo, $\ker f = \{e\} \implies x^n = e$, ma per il Teorema 1.27 ciò significa che $\operatorname{ord}(x) | n = \operatorname{ord}(f(x))$. Infine, unendo il risultato appena trovato con il punto (1) del teorema appena dimostrato, si ha:

$$\operatorname{ord}(x) | \operatorname{ord}(f(x)) \wedge \operatorname{ord}(f(x)) | \operatorname{ord}(x) \iff \operatorname{ord}(f(x)) = \operatorname{ord}(x)$$

□

Definizione 1.48. Si definisce **isomorfismo** un omomorfismo bigettivo tra due gruppi, $G \xrightarrow[\sim]{} G'$. Due gruppi si dicono **isomorfi** se esiste un isomorfismo tra loro, e si indica in questo modo:

$$G \cong G'$$

Osservazione 1.49 (Indistinguibilità Algebrica Di Gruppi Isomorfi) — Gruppi isomorfi sono tra loro "indistinguibili" per le proprietà di gruppo. Infatti:

- Hanno la stessa cardinalità (poiché esiste una bigezione tra i due insiemi di sostegno).
- Hanno elementi degli stessi ordini (perché se f è iniettivo, per quanto visto nel Teorema 1.47, x ed $f(x)$ hanno lo stesso ordine; inoltre, poiché f è surgettiva (quindi i due insiemi hanno la stessa cardinalità), tutti gli elementi x hanno immagine $f(x)$, con cardinalità uguale e quindi tutti gli ordini del gruppo di partenza rimangono invariati nel gruppo di arrivo).
- Gruppi isomorfi hanno gli "stessi" sottogruppi:

$$\{H \leqslant G\} \longleftrightarrow \{K \leqslant G'\}$$

$$H \xrightarrow{\varphi} f(H)$$

$$f^{-1}(K) \xleftarrow{\psi} K$$

$$\varphi \circ \psi(K) = K \quad f \circ f^{-1}(K) = K$$

$$\psi \circ \varphi(H) = H \quad \underbrace{f \circ f^{-1}(H)}_{id_G(H)} = H$$

Esempio 1.50

Consideriamo $C_n = \{z \in \mathbb{C}^* | z^n = 1\}$, per quanto visto $C_n < \mathbb{C}^*$, $|C_n| = n$ e $C_n = \langle \zeta_n \rangle$. Definiamo l'applicazione:

$$\overline{a} \longrightarrow \zeta_n^a$$

Si osserva facilmente che la funzione è sia surgettiva che iniettiva, pertanto bigettiva[a]. Quindi l'applicazione così definita è un omomorfismo, pertanto:

$$C_n \cong \mathbb{Z}/n\mathbb{Z}$$

[a] Data l'equipotenza dei due insiemi, sarebbe bastata una sola delle due condizioni per arrivare alla bigettività.

Teorema 1.51 (Isomorfismo Dei Gruppi Ciclici)
Sia G un gruppo ciclico, $G = \langle g \rangle$, allora:

(1) Se $|G| = +\infty$, allora $G \cong \mathbb{Z}$.

(2) Se $|G| = n$, allora $G \cong \mathbb{Z}/n\mathbb{Z}$.

Dimostrazione. Per dimostrare che G è isomorfo rispettivamente a $\mathbb{Z}$ o $\mathbb{Z}/n\mathbb{Z}$, ci basta trovare almeno un isomorfismo tra i due gruppi considerati.

(1) Consideriamo l'applicazione $\varphi : \mathbb{Z} \longrightarrow G : k \longmapsto g^k$[14],Osserviamo che usiamo proprio il generatore del gruppo come base, ciò servirà a rendere l'applicazione surgettiva. e proviamo che è un isomorfismo. Per farlo dobbiamo provare che è un omomorfismo bigettivo:

- Per provare che $\varphi : \mathbb{Z} \longrightarrow G$ è un omomorfismo ci basta usare le usuali proprietà delle potenze:
$$\varphi(k+h) = g^{k+h} = g^k g^h = \varphi(k)\varphi(h) \quad \forall k, h \in \mathbb{Z}$$
- Per provare che φ è bigettiva, dobbiamo dimostrare che è sia iniettiva che suriettiva. Per vedere che è iniettiva, ci basta osservare che essendo G un gruppo ciclico di cardinalità infinita gli elementi non si ripetono ciclicamente, allora:
$$g^k \neq g^h \quad \forall k, h \in \mathbb{Z} : k \neq h$$
Ovvero $\varphi(k) = \varphi(h) \iff h = k \implies \varphi$ iniettiva. Si osserva poi che $\mathrm{Im}\varphi = \{g^k\}_{k\in\mathbb{Z}} = \langle g \rangle = G$, ovvero $\mathrm{Im}\varphi = \mathrm{Cod}\varphi$, quindi φ è surgettiva. Possiamo concludere allora che φ è una bigezione.

(2) Analogamente al caso precedente, per provare che l'applicazione $\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G : \overline{a} \longmapsto g^a$ è un isomorfismo, dobbiamo provare che è un omomorfismo bigettivo, inoltre, poiché in questo caso l'applicazione è definita su $\mathbb{Z}/n\mathbb{Z}$, dobbiamo anche verificarne la buona definizione[15]:

- Se $\overline{a} = \overline{b} \implies g^a = g^b$, ma $\overline{a} = \overline{b} \iff a \equiv b \pmod{n} \iff b = a + hn$ con $h \in \mathbb{Z}$, quindi:
$$g^a = g^b = (\underbrace{g^n}_{=e})^h g^a \text{[16]} = g^a \quad \forall h \in \mathbb{Z}$$
Quindi il valore della funzione resta invariato per qualunque scelta del rappresentante, pertanto, φ è ben definita.
- Per vedere che φ è un omomorfismo, basta fare un'analoga osservazione a quella fatta nel caso (1):
$$\varphi(\overline{a} + \overline{b}) = g^{a+b} = g^a g^b = \varphi(\overline{a})\varphi(\overline{b}) \quad \forall \overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$$

[14].
[15] Il problema risiede dal fatto che gli elementi di $\mathbb{Z}/n\mathbb{Z}$ sono classi di resto modulo n, per le quali non esiste un unico rappresentante, pertanto bisogna verificare, affinché la funzione sia ben definita, che cambiando rappresentante della classe di resto, il risultato della funzione non cambi.
[16] Poiché $|G| = n$ e $G = \langle g \rangle \implies \mathrm{ord}(g) = n$.

- Poiché, per ipotesi $|G| = n = |\mathbb{Z}/n\mathbb{Z}|$ (con $n < +\infty$), ovvero i due insiemi hanno la stessa cardinalità ci basta verificare una sola tra iniettività e surgettività. Verifichiamo che φ è suriettiva, per farlo, osserviamo che $\mathrm{Im}\varphi = \{g^0, g^1, \dots, g^{n-1}\} = \langle g \rangle = G$. Pertanto φ è bigettiva.

□

Osservazione 1.52 (Conosciamo Tutto Dei Gruppi Ciclici) —

- Se $|G| = \langle x \rangle$ e $|G| = +\infty$:
  (1) Tutti i suoi elementi diversi da e hanno ordine $+\infty$.
  (2) Sia $H \leqslant G \implies H = \langle g^h \rangle$, per qualche h. Inoltre:

$$\{n\mathbb{Z} \leqslant \mathbb{Z}\}_{n\in\mathbb{N}} \longleftrightarrow \{H \leqslant G\}$$

$$\varphi(h\mathbb{Z}) = \left\langle g^h \right\rangle = H \qquad \text{ovvero} \qquad \varphi(hk) = (g^h)^k$$

  Ovvero ogni sotto gruppo di G è ciclico ed esiste sempre una bigezione (un isomorfismo quindi) φ che mette in corrispondenza questo sottogruppo con $h\mathbb{Z}$ e tale che l'immagine di $h\mathbb{Z}$ sia proprio il sottogruppo ciclico H. Quindi tutti i sottogruppi di G sono algebricamente equivalenti a quelli di $\mathbb{Z}$ ed in corrispondenza biunivoca con loro (quindi isomorfi). In questo caso l'immagine di $h\mathbb{Z}$ è il sottogruppo (ciclico) generato da g^h, ovvero $\langle g^n \rangle = \left\{(g^h)^k\right\}_{k\in\mathbb{Z}}$.

- Se $|G| = \langle x \rangle$ e $|G| = n$:
  (1) G ha $\phi(d)$ elementi di ordine d, $\forall d|n$ (non ci sono elementi di ordine h se $h \nmid n$).
  (2) Ha un unico sottogruppo di ordine d, $\forall d|n$ (Se $H \leqslant G$ e $H = \langle g \rangle$, allora $(\mathrm{ord}(g) =)|H| \mid |G|$). Inoltre, per $d \mid n$ in $\mathbb{Z}/n\mathbb{Z}$ il sottogruppo di ordine d:

$$H_d = \left\langle \overline{\frac{n}{d}} \right\rangle = \left\{ \frac{n}{d}k \right\}_{k=0,1,\dots,d-1} \xrightarrow[\sim]{\varphi} \left\langle g^{\frac{n}{d}} \right\rangle \text{ [a]}$$

[a] In entrambi i casi le bigezioni usate, sono quelle trovate nel Teorema 1.51, che ci assicurano sempre l'isomorfismo dei gruppi.

Esempio 1.53

Consideriamo $\mathbb{Z}/n\mathbb{Z} \cong C_n = \left\langle e^{\frac{2\pi i}{n}} \right\rangle$: Sia $n = 100$ chi è il sottogruppo di ordine 20 di C_{100}?

Quello generato da $\left\langle \left(e^{\frac{2\pi i}{100}}\right)^{\frac{100}{20}} \right\rangle = \left\langle e^{\frac{10\pi i}{100}} \right\rangle$. Infatti i sottogruppi di C_n sono isomorfi a quelli di $\mathbb{Z}/n\mathbb{Z}$ e in $\mathbb{Z}/n\mathbb{Z}$, per quanto visto nel Teorema 1.41, il sottogruppo di ordine 20 è dato da $\left\langle \overline{\frac{100}{20}} \right\rangle$, quindi, come abbiamo appena visto nell'Osservazione 1.52, il corrispettivo in C_n sarà : $\varphi\left(\left\langle \overline{\frac{100}{20}} \right\rangle\right) = \left\langle \left(e^{\frac{2\pi i}{100}}\right)^{\frac{100}{20}} \right\rangle$.

Esempio 1.54

Chi sono gli elementi di ordine n di C_n?
So che sono $\phi(n)$ e sono le immagini degli elementi di ordine n in $\mathbb{Z}/n\mathbb{Z}$. Ovvero:

$$\underbrace{\{\overline{a} | (a,n) = 1\}}_{\text{elementi di ordine } n \text{ in } \mathbb{Z}/n\mathbb{Z}} \xrightarrow{\varphi} \{g^a \mid (a,n) = 1\}$$

Ovvero:

$$\left\{ e^{\frac{2\pi i}{n} a} \;\middle|\; (a,n) = 1 \right\}$$

Osservazione 1.55 (Ovvia) — Ogni gruppo ciclico è abeliano. Il viceversa è, in generale, falso, ad esempio: $\mathbb{Z}/8\mathbb{Z}^*$ non è ciclico.

§1.5 Prodotto diretto di gruppi

Definizione 1.56. Siano $(G_1, \star_1)$ e $(G_2, \star_2)$ gruppi, consideriamo il prodotto cartesiano $G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$ e definiamo su di esso l'operazione:

$$(a, b) * (c, d) = (a \star_1 c, b \star_2 d)$$

L'insieme $G_1 \times G_2$ con l'operazione $*$ si dice **prodotto diretto** di gruppi.

Teorema 1.57 (Prodotto Diretto Di Gruppi)
Siano G_1 e G_2 due gruppi, vale:

(1) Il prodotto diretto di due gruppi G_1 e G_2 è un gruppo $(G_1 \times G_2, *)$.

(2) $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

(3) $\text{ord}(x, y) = [\text{ord}_{G_1}(x), \text{ord}_{G_2}(y)]$.

Dimostrazione. Proviamo le tre affermazioni:

(1) Per dimostrare che $(G_1 \times G_2, *)$ è un gruppo basta verificare singolarmente le quattro proprietà richieste dalla definizione di gruppo:

(a) Chiusura: Vogliamo dimostrare che $\forall (a, b), (c, d) \in G_1 \times G_2$ si ha $(a, b) * (c, d) \in G_1 \times G_2$, segue dalla definizione di prodotto di gruppi che:

$$(a, b) * (c, d) = (\underbrace{a \star_1 c}_{\in G_1}, \underbrace{b \star_2 d}_{\in G_2})$$

quindi dalla definizione di prodotto cartesiano segue la tesi:

$$(a \star_1 c, b \star_2 d) \in G_1 \times G_2 \qquad \forall (a, b), (c, d) \in G_1 \times G_2$$

(b) Associatività: Devo mostrare che: $\forall (a, b), (c, d), (e, f) \in G_1 \times G_2$ vale:

$$((a, b) * (c, d)) * (e, f) = (a, b) * ((c, d) * (e, f))$$

Segue dall'associatività di G_1 e G_2 che $\forall (a, b), (c, d), (e, f) \in G_1 \times G_2$:

$$\begin{aligned}((a, b) * (c, d)) * (e, f) &= (a \star_1 c, b \star_2 d) * (e, f) = \\ &= ((a \star_1 c) \star_1 e, (b \star_2 d) \star_2 f) = (a \star_1 (c \star_1 e), b \star_2 (d \star_2 f)) = \\ &= (a, b) * ((c, d) * (e, f))\end{aligned}$$

(c) Elemento Neutro: Poiché G_1 e G_2 sono gruppi è facile riconoscere che l'elemento $(e_1, e_2) \in G_1 \times G_2$ è proprio l'elemento neutro del gruppo prodotto, infatti:

$$\begin{aligned}(a, b) * (e_1, e_2) &= (a \star_1 e_1, b \star_2 e_2) = \\ = (e_1 \star_1 a, e_2 \star_2 b) &= (e_1, e_2) * (a, b) = (a, b) \qquad \forall (a, b) \in G_1 \times G_2\end{aligned}$$

(d) Inverso: Come nel caso precedente, poiché G_1 e G_2 sono gruppi si ha che $\forall (a, b) \in G_1 \times G_2$ esiste $(a^{-1}, b^{-1}) \in G_1 \times G_2$ tale che:

$$\begin{aligned}(a, b) * (a^{-1}, b^{-1}) &= (a \star_1 a^{-1}, b \star_2 b^{-1}) = \\ &= (a^{-1} \star_1 a, b^{-1} \star_2 b) = (a^{-1}, b^{-1}) * (a, b) = (e_1, e_2)\end{aligned}$$

(2) Sia $(x, y) \in Z(G_1 \times G_2)$, allora $\forall (g_1, g_2) \in G_1 \times G_2$ deve essere:

$$(x, y) * (g_1, g_2) = (g_1, g_2) * (x, y)$$

ovvero:

$$(x \star_1 g_1, y \star_2 g_2) = (g_1 \star_1 x, g_2 \star_2 y)$$

l'uguaglianza tra due coppie di elementi in un prodotto cartesiano è vera se e solo se:

$$x \star_1 g_1 = g_1 \star_1 x \qquad \forall g_1 \in G_1$$

$$y \star_2 g_2 = g_2 \star_2 y \qquad \forall g_2 \in G_2$$

Che sono contemporaneamente vere se e solo se:

$$x \in Z(G_1) \wedge y \in Z(G_2)$$

Quindi le coppie che appartengono a $Z(G_1 \times G_2)$ sono quelle in cui $x \in Z(G_1) \subseteq G_1$ e $y \in Z(G_2) \subseteq G_2$, ovvero le coppie appartenenti al prodotto cartesiano del centro dei due gruppi: $(x, y) \in Z(G_1) \times Z(G_2)$, da cui la tesi.

(3) Siano $m = \text{ord}_{G_1}(x)$, $n = \text{ord}_{G_2}(y)$ e $d = \text{ord}_{G_1 \times G_2}(x, y)$, vogliamo dimostrare che $d = [m, n]$. Per farlo, mostriamo che $d \mid [m, n]$, $[m, n] \mid d$ e sfruttiamo l'antisimmetria della divisibilità:

(a) Osserviamo che $(x, y)^{[m,n]} = (x^{[m,n]}, y^{[m,n]}) = (e_1, e_2)$ (poiché l'm.c.m. dei due ordini è multiplo di entrambi e quindi vale il Teorema 1.27), inoltre, sempre per il Teorema 1.27, si conclude che $d \mid [m, n]$.

(b) Adesso, osserviamo che $(x, y)^d = (x^d, y^d) = (e_1, e_2)$, quindi analogamente:

$$x^d = e_1 \iff m \mid d$$

$$y^d = e_2 \iff n \mid d$$

ma, da una nota proprietà dell'm.c.m.:

$$m \mid d \wedge n \mid d \iff [m, n] \mid d$$

.

Possiamo concludere che $d = [m, n]$, ovvero: $\text{ord}(x, y) = [\text{ord}_{G_1}(x), \text{ord}_{G_2}(y)]$.

□

Esempio 1.58 (Prodotto Diretto Di Gruppi)
Consideriamo i due gruppi $(\mathbb{Z}/3\mathbb{Z}, +)$ e $(\mathbb{Z}/2\mathbb{Z}, +)$, il prodotto diretto è dato da:

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$$

su di esso è definita l'operazione $+$:

$$(2,0) + (2,1) = (1,1)$$

Analizziamo ora gli ordini degli elementi[a]:

$$\begin{aligned} \operatorname{ord}(0,0) &= 1 & \operatorname{ord}(1,1) &= 6 \\ \operatorname{ord}(0,1) &= 2 & \operatorname{ord}(2,0) &= 3 \\ \operatorname{ord}(1,0) &= 3 & \operatorname{ord}(2,1) &= 6 \end{aligned}$$

Osserviamo che $|\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 6$, quindi $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ è ciclico in quanto ha elementi di ordine 6. In particolare si osserva per il Teorema 1.51 che:

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

[a] Possiamo riferirci agli ordini dei singoli elementi usando la relazione trovata nell'Osservazione 1.36.

Esempio 1.59 (Altri Esempi Di Prodotti Diretti)

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,1), (1,0), (1,1)\}$, il cui ordine è 4. Poiché non c'è alcun elemento di ordine 4, il gruppo non è ciclico. Tuttavia si verifica che $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z}^*$.
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ non è un gruppo ciclico.

Esercizio 1.60. Verificare che $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z}^*$.

Soluzione. Poiché i due insiemi hanno la stessa cardinalità, ci basta trovare una mappa che sia surgettiva o iniettiva. Consideriamo:

$$\varphi : \mathbb{Z}/8\mathbb{Z}^* \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : \begin{cases} 1 \longmapsto (0,0) \\ 3 \longmapsto (1,0) \\ 5 \longmapsto (0,1) \\ 7 \longmapsto (1,1) \end{cases}$$

Si osserva subito che è sia iniettiva che surgettiva, inoltre, per verifica diretta si vede che φ è un omomorfismo, pertanto φ è un isomorfismo di gruppi $\implies \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z}^*$.[17] Un'ulteriore conferma della correttezza è data dal fatto che, eccetto gli elementi neutri (associati tra loro), tutti gli altri elementi dei due gruppi hanno ordine 2, e ciò è coerente col fatto che in un isomorfismo gli ordini degli elementi di partenza e di arrivo siano uguali. □

[17] Per completezza, andrebbe verificata anche la buona definizione della funzione data, ma essendo banale è stata omessa (per verificarla basta cambiare rappresentante in ognuna delle quattro corrispondenze e poi procedere per verifica diretta).

Teorema 1.61 (Teorema Cinese Del Resto (III Forma))
Consideriamo $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$, vale:

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \iff (m,n) = 1$$

Dimostrazione. Sia $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, con $|G| = mn$. Per dimostrare che $G \cong \mathbb{Z}/mn\mathbb{Z}$ osserviamo, ricordando il Teorema 1.51, che ci basta mostrare che G è ciclico, ovvero $\exists g \in G$ tale che $\text{ord}(g) = |G| = mn$. Consideriamo un elemento $(\overline{x}, \overline{y})$, con $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ e $\overline{y} \in \mathbb{Z}/m\mathbb{Z}$, sappiamo che:

$$(\overline{x}, \overline{y}) = [\text{ord}(\overline{x}), \text{ord}(\overline{y})]$$

dove per l'Osservazione 1.36, possiamo scrivere:

$$[\text{ord}(\overline{x}), \text{ord}(\overline{y})] = \left[\frac{m}{(m,x)}, \frac{n}{(n,y)}\right] \leq [m,n] = \frac{mn}{(m,n)}$$

- Se $(m,n) > 1 \implies [m,n] < mn$[18] $\implies [\text{ord}(\overline{x}), \text{ord}(\overline{y})] < mn$ allora G non è ciclico perché non ha elementi di ordine mn.
- Se $(m,n) = 1$, allora $[m,n] = mn$, e si osserva che $\text{ord}(\overline{1}, \overline{1}) = [\text{ord}(\overline{1}), \text{ord}(\overline{1})] = [m,n] = \frac{mn}{(m,n)} = mn$, quindi $(\overline{1}, \overline{1})$ è un generatore di $G \implies G$ ciclico. Essendo quindi $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ciclico, esso è isomorfo a $\mathbb{Z}/mn\mathbb{Z}$ per il Teorema 1.51 e la prima parte della tesi è dimostrata.

Per completare la dimostrazione, dobbiamo provare l'implicazione opposta, ovvero $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \implies (m,n) = 1$. Per quanto appena visto, l'ipotesi di isomorfismo implica che $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è ciclico, ovvero esiste un elemento di ordine mn, ma se l'ordine di un elemento è definito come:

$$\text{ord}(x,y) = \left[\frac{m}{(m,x)}, \frac{n}{(n,y)}\right]$$

allora, detto $(\widetilde{x}, \widetilde{y})$ un generatore di G segue:

$$\text{ord}(\widetilde{x}, \widetilde{y}) = \left[\frac{m}{(m,\widetilde{x})}, \frac{n}{(n,\widetilde{y})}\right] = mn \leq [m,n] = \frac{mn}{(m,n)}$$

da cui:

$$mn \leq \frac{mn}{(m,n)} \implies (m,n) \leq 1 \implies (m,n) = 1$$

Pertanto la tesi è dimostrata. [19] □

Osservazione 1.62 (Dimostrazione Alternativa) — Come dimostrato per il Teorema Cinese Del Resto (II Forma), sappiamo che la mappa:

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} : [a]_{mn} \longmapsto ([a]_m, [a]_n)$$

è bigettiva se e solo se $(m,n) = 1$. A questo punto possiamo facilmente verificare che φ è un omomorfismo ed ottenere l'isomorfismo tra due gruppi, ovvero lo stesso

[18] Ricordiamo la nota relazione: $(m,n) \cdot [m,n] = mn$.
[19] Bastava anche dire che essendoci un elemento di ordine mn, e poiché l'ordine deve avere valore massimo $[m,n]$, allora l'unica possibilità è che sia $(m,n) = 1$.

risultato del Teorema 1.60 (TCR III Forma):

$$\varphi([a+b]_{mn}) = \varphi([a]_{mn}) + \varphi([b]_{mn}) \qquad \forall [a]_{mn}, [b]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$$

Quindi:

$$([a+b]_m, [a+b]_n) = ([a]_m, [a]_n) + ([b]_m, [b]_n)$$

Dove per la somma di elementi di un prodotto cartesiano si ha:

$$([a]_m, [a]_n) + ([b]_m, [b]_n) = ([a]_m + [b]_m, [a]_n + [b]_n)$$

ed infine per la definizione di somma tra classi di resto:

$$([a]_m + [b]_m, [a]_n + [b]_n) = ([a+b]_m, [a+b]_n)$$

Pertanto φ è un omomorfismo e quindi un isomorfismo.

Corollario 1.63

Consideriamo $\mathbb{Z}/m\mathbb{Z}^*$ e $\mathbb{Z}/n\mathbb{Z}^*$, vale:[a]

$$\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^* \cong \mathbb{Z}/mn\mathbb{Z}^* \iff (m,n) = 1$$

[a] Ricordiamo che $\mathbb{Z}/n\mathbb{Z}^*$ è un gruppo ciclico se e solo se $n = 2, 4, p^k, 2p^k$, con p primo dispari e $k > 0$.

Dimostrazione. Ricordando il corollario analogo del TCR (II Forma), sappiamo che l'applicazione $\varphi^* : \mathbb{Z}/mn\mathbb{Z}^* \longrightarrow \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^* : [a]_{mn} \longmapsto ([a]_m, [a]_n)$ è bigettiva se e solo se $(m,n) = 1$. Per verificare che φ^* è un omomorfismo, invece, si può procedere in maniera analoga a quanto fatto nell'Osservazione 1.61:

$$\varphi([ab]_{mn}) = \varphi([a]_{mn}) \cdot \varphi([b]_{mn}) \qquad \forall [a]_{mn}, [b]_{mn} \in \mathbb{Z}/mn\mathbb{Z}^*$$

Quindi:

$$([ab]_m, [ab]_n) = ([a]_m, [a]_n) \cdot ([b]_m, [b]_n)$$

Dove per il prodotto di elementi di un prodotto cartesiano si ha:

$$([a]_m, [a]_n) \cdot ([b]_m, [b]_n) = ([a]_m \cdot [b]_m, [a]_n \cdot [b]_n)$$

ed infine per la definizione di prodotto tra classi di resto ci dà l'omomorfismo:

$$([a]_m \cdot [b]_m, [a]_n \cdot [b]_n) = ([ab]_m, [ab]_n)$$

Pertanto φ è un omomorfismo e quindi un isomorfismo. □

Osservazione 1.64 — Siano p, q primi dispari, con $p \neq q$, allora $\mathbb{Z}/pq\mathbb{Z}^*$ non è ciclico.

$$\mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/pq\mathbb{Z}^*{}^{a}$$

Per dimostrare che non è ciclico basta osservare che non ha alcune proprietà dei gruppi ciclici. Ad esempio, possiamo osservare che il gruppo ha 3 elementi di ordine 2, mentre un gruppo ciclico ha $\phi(2)$ elementi di ordine 2, se $2 \mid |G|$ e 0 altrimenti. Si osserva:

$$|\mathbb{Z}/pq\mathbb{Z}^*| = \underbrace{(p-1)(q-1)}_{\text{pari } \implies 2||\mathbb{Z}/pq\mathbb{Z}^*| \implies \phi(2) \text{ elementi di ordine 2}}$$

Ma: $(\overline{-1}, \overline{1}), (\overline{1}, \overline{-1}), (\overline{-1}, \overline{-1})$ hanno tutti ordine 2, pertanto $\mathbb{Z}/pq\mathbb{Z}^*$ non è ciclico.

[a] $\mathbb{Z}/p\mathbb{Z}^*$ e $\mathbb{Z}/q\mathbb{Z}^*$ sono ciclici, mentre il loro prodotto diretto non lo è necessariamente, e come stiamo per vedere ciò è coerente col fatto che $\mathbb{Z}/pq\mathbb{Z}^*$ non sia ciclico.

§1.6 Classi laterali e teorema di Lagrange

Definizione 1.65. Sia G un gruppo e sia $H \leqslant G$. Definiamo la **relazione sinistra** modulo H come una relazione su G, ponendo $x \sim_H y$ se:

$$y^{-1}x \in H$$

e si indica con:

$$x \equiv y \pmod{H}$$

Osservazione 1.66 ($\sim_H$) — La relazione sinistra modulo H è una relazione di equivalenza su G, infatti è:

- (Riflessiva) $x \sim_H x$, $\forall x \in G$, infatti $x^{-1}x = e \in H$ (Poiché $H \leqslant G$).
- (Simmetrica) $x \sim_H y \implies y \sim_H x$, $\forall x, y \in G$, infatti $y^{-1}x \in H \implies x^{-1}y = (y^{-1}x)^{-1} \in H \implies y \sim_H x$.
- (Transitiva) $x \sim_H y$, $y \sim_H z \implies x \sim_H z$, $\forall x, y, z \in H$. Infatti: se $y^{-1}x \in H$ e $z^{-1}y \in H$, poiché H è un gruppo, allora:

  $$(z^{-1}y)(y^{-1}x) \in H \implies z^{-1}x \in H$$

  Ne segue che la relazione di equivalenza (congruenza) modulo H definisce delle classi di equivalenza che danno origine ad una partizione di G:

  $$[x]_H = \{y \in G | x \sim_H y\} = \{y \in G | y^{-1}x \in H\} = \{y \in G | x^{-1}y \in H\} =$$

  $$= {}^{a} \{y \in G | y \in xH\} = xH = \{xh | h \in H\}$$

  Dove xH prende il nome di **classe laterale sinistra** di H.

[a] Dove si è moltiplicato per x entrambi i lati a sinistra di $x^{-1}y \in H$.

Esempio 1.67 (Relazione Sinistra Modulo H)
Consideriamo $G = \mathbb{Z}$ e $n\mathbb{Z} = H \leqslant G$. Essendo $\mathbb{Z}$ un gruppo rispetto alla somma, possiamo riscrivere la relazione sinistra modulo H in notazione additiva:

$$x \equiv y \pmod{H} \iff y^{-1}x \in H$$

ovvero:

$$x \equiv y \pmod{n\mathbb{Z}} \iff (-y) + x \in H (= n\mathbb{Z})$$

da cui:

$$(-y) + x \in H (= n\mathbb{Z}) \iff n \mid x - y \iff x \equiv y \pmod{n}$$

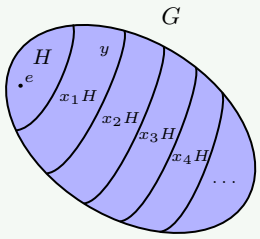
e quindi:

$$[x]_H = y + n\mathbb{Z} \qquad \text{con} \quad y \in \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

Osservazione 1.68 — Sia $H \leqslant G$ e sia definita su G una relazione sinistra modulo H $\sim_H$. Detto $\mathcal{R}$ l'insieme dei rappresentati per le classi di equivalenza determinate da $\sim_H$ su G, possiamo scrivere:

$$G = \bigcup_{x\in\mathcal{R}}^{\cdot} [x]_H = \bigcup_{x\in\mathcal{R}}^{\cdot} xH$$

ovvero G è unione delle sue classi laterali modulo H:



Dove $x_1H = yH$, poiché $y \in x_1H = yH$, perché $y \in x_1H$ e $y \in yH$ $(y = y \cdot e(\in H))$, quindi $y \in x_1H \cap yH \implies x_1H = yH$, perché sono classi di equivalenza, ergo o sono disgiunte o coincidono.

Teorema 1.69 (Teorema Di Lagrange)
Sia G un gruppo finito e $H \leqslant G$, allora l'ordine del sottogruppo divide l'ordine del gruppo: $|H| \mid |G|$.

Dimostrazione. Sia $|G| = n$, allora:

$$n = |G| = \left|\bigcup_{x\in\mathcal{R}}^{\cdot} xH\right| = \sum_{x\in\mathcal{R}} |xH|$$

Possiamo osservare che $|xH| = |H|$, $\forall x \in G$, ovvero tutte le classi laterali sinistre di H hanno la medesima cardinalità di quest'ultimo, infatti possiamo definire un'applicazione $\varphi : H \longrightarrow xH : h \longmapsto xh$ e mostrare che essa è bigettiva.
La surgettività è ovvia, poiché: $\mathrm{Im}(\varphi) = \{xh\}_{h\in\mathbb{Z}} = xH = \mathrm{Cod}(\varphi)$. Per provare l'iniettività basta mostrare che $\varphi(h_1) = \varphi(h_2) \iff h_1 = h_2$, ovvero: $xh_1 = xh_2 \implies h_1 = h_2$ (dove nell'ultimo passaggio abbiamo cancellato a sinistra). Allora:

$$|G| = \sum_{x\in\mathcal{R}} |xH| = \sum_{x\in\mathcal{R}} |H| = |H| \cdot |\mathcal{R}|$$

quindi la tesi:

$$|G| = |H| \cdot |\mathcal{R}|^{[20]} \implies |H| \mid |G|$$

□

[20] Come vedremo questa relazione ci permette anche di trovare il numero di classi laterali di H.

Osservazione 1.70 (Inverso Del Teorema Di Lagrange) — Come già osservato nel Teorema 1.41, nel caso particolare di $\mathbb{Z}/n\mathbb{Z}$, possiamo osservare che in generale vale anche per tutti i gruppi ciclici finiti il viceversa del teorema di Lagrange, ovvero: $\forall d \mid |G|, \exists! H \leqslant G : |H| = d$.
Per $\mathbb{Z}$ o $|n\mathbb{Z}| = +\infty$ il Teorema di Lagrange non ci dice nulla.

Esempio 1.71

Consideriamo $\mathbb{Z}/n\mathbb{Z}$, ogni sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ è ciclico, quindi $H \leqslant \mathbb{Z}/n\mathbb{Z} \implies H = \langle \overline{k} \rangle$, con $|H| = |\langle \overline{k} \rangle| = \text{ord}(\overline{k})$. Per Lagrange sappiamo quindi che $\text{ord}(\overline{k}) \mid n$, inoltre, per quanto visto nell'Osservazione 1.36 sappiamo anche che:

$$|H| = \text{ord}(\overline{k}) = \frac{n}{(n,k)} \implies \text{ord}(\overline{k}) \mid n$$

che è coerente col Teorema Di Langrage.

Corollario 1.72 (Ordini E Lagrange)

Sia G un gruppo finito:

(1) $\text{ord}(x) \mid |G|, \forall x \in G$.[a]

(2) $x^{|G|} = e, \forall x \in G$.

[a] Ciò generalizza il punto (1) del Corollario 1.38.

Dimostrazione. Le dimostrazioni seguono facilmente da teoremi precedentemente trattati:

(1) Dal punto (1) del Teorema 1.27 sappiamo che $\text{ord}(x) = |\langle x \rangle| (\leqslant G)$, e per il Teorema Di Lagrange: $\text{ord}(x) \mid |G|$.

(2) Per quanto appena visto nel punto (1) l'ordine di un elemento nel gruppo divide l'ordine del gruppo, quindi quest'ultimo è multiplo dell'ordine e per il Teorema 1.27, segue che $x^{|G|} = e$.

□

Corollario 1.73 (Teorema Di Eulero)

Siano $a, m \in \mathbb{Z}$, $m \geq 2$ e $(a, m) = 1$, allora:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Dimostrazione. Per dimostrare l'affermazione è sufficiente considerare come gruppo $G = \mathbb{Z}/m\mathbb{Z}^*$, ricordando che i suoi elementi sono tutte le classi imvertibili modulo m, sappiamo che $|G| = \phi(m)$ e quindi, per quanto appena visto nel Corollario 1.71, segue immediatamente la tesi:

$$x^{|G|} \equiv x^{\phi(m)} \equiv 1 \pmod{m}$$

□

Corollario 1.74 (Gruppi Di Ordine Primo)
Ogni gruppo di ordine p, con p primo, è ciclico e quindi isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Dimostrazione. Sia $|G| = p$, con p primo ($\implies$ $p \geq 2$ $\implies$ G contiene almeno un altro elemento oltre quello neutro), allora per il Corollario 1.71 segue che per $x \in G, x \neq e_G$, $\implies$ $\text{ord}(x) \mid |G| = p$, ma poiché x non può avere ordine 1 (essendo diverso dall'elemento neutro), allora $\text{ord}(x) = p \implies \langle x \rangle = G \implies G$ ciclico.
Per concludere ci basta applicare direttamente il Teorema 1.51 e segue la tesi:

$$G \cong \mathbb{Z}/p\mathbb{Z}$$

□

Definizione 1.75. Sia G un gruppo e sia $H \leqslant G$. Definiamo la **relazione destra** modulo H come una relazione su G, ponendo $x_H \sim y$ se:

$$xy^{-1} \in H$$

e si indica con:

$$y \equiv x \pmod{H}$$

Osservazione 1.76 ($_H\sim$) — La relazione destra modulo H, identicamente a quanto già visto nell'Osservazione 1.65, è una relazione di equivalenza su G. Pertanto possiamo definire analogamente le classi di equivalenza determinate su G da questa relazione:

$$_H[x] = \{y \in G | y_H \sim x\} = \left\{y \in G | y^{-1}x \in H\right\} = \left\{y \in G | yx^{-1} \in H\right\} =$$

$$= \{y \in G | y \in Hx\} = Hx = \{hx | h \in H\}$$

Dove Hx prende il nome di **classe laterale destra** di H.

Esempio 1.77 (Relazione Destra Modulo H)
Consideriamo $G = \mathbb{Z}$ e $n\mathbb{Z} = H \leqslant G$. Essendo $\mathbb{Z}$ un gruppo rispetto alla somma, possiamo riscrivere la relazione sinistra modulo H in notazione additiva:

$$y \equiv x \pmod{H} \iff xy^{-1} \in H$$

ovvero:

$$y \equiv x \pmod{n\mathbb{Z}} \iff x + (-y) \in H(= n\mathbb{Z})$$

da cui:

$$x + (-y) \in H(= n\mathbb{Z}) \iff n \mid y - x \iff y \equiv x \pmod{n}$$

e quindi:

$$_H[x] = n\mathbb{Z} + y \qquad \text{con} \quad y = \overline{0}, \overline{1}, \ldots, \overline{n-1}$$

Osservazione 1.78 (Classi Laterali In $\mathbb{Z}$) — Considerando ora le relazioni $\sim_H$ e ${}_H\sim$ definite sul gruppo $(\mathbb{Z},+)$, esse inducono una partizione del gruppo $\mathbb{Z}$ sul quale sono definite, dividendo il gruppo rispettivamente in classi laterali sinistre e destre, che si possono indicare così:

- classi laterali sinistre: $x+n\mathbb{Z}=\{x+nz\}_{z\in\mathbb{Z}}$.
- classi laterali destre: $n\mathbb{Z}+x=\{nz+x\}_{z\in\mathbb{Z}}$.[a]

Dato che $\mathbb{Z}$ è abeliano le due espressioni sono uguali: $x+n\mathbb{Z}=n\mathbb{Z}+x$, $\forall x\in G$, ovvero tutte le classi sinistre e destre corrispondenti sono a due a due coincidenti.

[a] Solo la classe $n\mathbb{Z}$ (con $x=e$) è un sottogruppo di $\mathbb{Z}$, in quanto è l'unica che contiene l'elemento neutro.

Osservazione 1.79 (Classi Laterali In Un Gruppo Abeliano) — Possiamo generalizzare la precedente osservazione come segue: se G è abeliano, allora $xH=Hx$, $\forall x\in G$, ovvero le classi laterali destre e sinistre del sottogruppo H, rispetto ad ogni elemento di G, sono uguali.

Esempio 1.80 (Classi Laterali Di S_3)

Consideriamo $G=S_3=\{id,\sigma,\sigma^2,\tau,\sigma\circ\tau,\sigma^2\circ\tau\}$, il gruppo delle permutazioni su 3 elementi, visto già nell'Esempio 1.8. Osserviamo preliminarmente che:

- $\sigma\neq\sigma^2$, perché altrimenti si avrebbe $\sigma=id$.
- $\sigma\neq\tau$, ciò è ovvio per definizione.
- $\sigma\neq\sigma\circ\tau$, perché altrimenti si avrebbe $\tau=id$.
- $\tau\neq\sigma\circ\tau$, perché altrimenti si avrebbe $\sigma=id$.

Consideriamo il sottogruppo di G generato da τ, ovvero $H=\langle\tau\rangle=\{id,\tau\}$[a][b], e calcoliamone la classe laterale destra e sinistra rispetto a σ (possiamo ottenere classi laterali diverse soltanto prendendo elementi al di fuori dell'insieme):

$$\sigma H=\{\sigma\circ id,\sigma\circ\tau\}=\{\sigma,\sigma\circ\tau\}$$

$$H\sigma=\{id\circ\sigma,\tau\circ\sigma\}=\{\sigma,\tau\circ\sigma\}=^{c}\{\sigma,\sigma^2\circ\tau\}$$

Come osservato sopra $\sigma\circ\tau\neq\sigma^2\circ\tau$, pertanto $\sigma H\neq H\sigma$, quindi le classi laterali sinistra e destra di H rispetto a σ sono diverse. Poiché $|G|=3!=6$ e $|H|=2$, possiamo ottenere in tutto 3 classi laterali per questo sottogruppo, l'ultima è quella ottenuta con σ^2:

$$\sigma^2H=\{\sigma^2\circ id,\sigma^2\circ\tau\}=\{\sigma^2,\sigma^2\circ\tau\}$$

$$H\sigma^2=\{id\circ\sigma^2,\tau\circ\sigma^2\}$$

[a] Ricordando che $\mathrm{ord}_{S_3}(\tau)=2$.
[b] H è già la classe laterale rispetto a id e τ ($\tau H=\{\mathrm{id},\tau\}=H\tau$), infatti un elemento in una classe è anche suo rappresentate, trattandosi di classi di equivalenza
[c] $\tau\circ\sigma=(12)(123)=(1)(23)=(23)=(132)(12)=\sigma^2\circ\tau$.

Esempio 1.81 (Classi Laterali Di Un Sottogruppo Di S_3)
Consideriamo ancora $G = S_3 = \{id, \sigma, \sigma^2, \tau, \sigma \circ \tau, \sigma^2 \circ \tau\}$, il gruppo delle permutazioni su 3 elementi, questa volta analizziamo il sottogruppo $K = \langle \sigma \rangle = \{id, \sigma, \sigma^2\} \leqslant G$. Poiché $|G| = 3! = 6$ e $|K| = 3$, possiamo ottenere in tutto 2 classi laterali per questo sottogruppo, quindi le uniche classi laterali possibili sono quelle generate con τ:

$$\tau K = \{\tau \circ id, \tau \circ \sigma, \tau \circ \sigma^2\}$$

$$K\tau = \{id \circ \tau, \sigma \circ \tau, \sigma^2 \circ \tau\} = \{\tau, \tau \circ \sigma^2, \tau \circ \sigma\}$$

Quindi le classi laterali sinistre e destre di K rispetto a τ coincidono.

Osservazione 1.82 — Le classi laterali di un sottogruppo possono coincidere anche se il gruppo non è abeliano.

§1.7 Sottogruppi normali

Definizione 1.83. Sia G un gruppo e $H \leqslant G$, se $gH = Hg$, $\forall g \in G$, H si dice **sottogruppo normale** di G e si indica con:

$$H \trianglelefteq G$$

Osservazione 1.84 — Osserviamo che:

(1) Se G è abeliano tutti i sottogruppi sono normali.

(2) In S_3 $\langle\sigma\rangle$ è normale, mentre $\langle\tau\rangle$ non è normale.

(3) $H \trianglelefteq G \iff gH = Hg \iff gHg^{-1} = H$, $\forall g \in G$. (In realtà vedremo che basta $gHg^{-1} \subseteq H$, $\forall g \in G$).

Teorema 1.85 (Sottogruppo Normale)
Siano G un gruppo ed $H \leqslant G$, allora: $H \trianglelefteq G \iff gHg^{-1} \subseteq H$, $\forall g \in G$.

Dimostrazione. Per dimostrare il teorema dobbiamo provare entrambe le implicazioni:

(a) Per dimostrare che se $H \trianglelefteq G$, allora $gHg^{-1} \subseteq H$, $\forall g \in G$, ci basta osservare che:

$$H \trianglelefteq G \implies gH = Hg \qquad \forall g \in G$$

da cui:

$$gH = Hg \implies gHg^{-1} = H \implies gHg^{-1} \subseteq H \qquad \forall g \in G$$

(b) Ci resta da dimostrare che se $gHg^{-1} \subseteq H$, $\forall g \in G$, allora $H \trianglelefteq G$, per farlo osserviamo che il primo contenimento vale per ogni elemento di G, anche per gli inversi:

$$gHg^{-1} \subseteq H \implies g^{-1}H(g^{-1})^{-1} \subseteq H \qquad \forall g \in G$$

quindi $g^{-1}Hg \subseteq H$, moltiplicando poi per g e g^{-1} segue:

$$g^{-1}Hg \subseteq H \implies Hg \subseteq gH \implies H \subseteq gHg^{-1} \qquad \forall g \in G$$

Avendo provato entrambi i contenimenti, per l'antisimmetria della relazione di contenimento, segue:

$$gHg^{-1} \subseteq H \wedge H \subseteq gHg^{-1} \iff gHg^{-1} = H \iff gH = Hg \qquad \forall g \in G$$

che per definizione è la tesi $H \trianglelefteq G$.

□

Osservazione 1.86 — Osserviamo che $gH = Hg$ è una condizione più debole di $gh = hg$, $\forall h \in H$, in quanto la condizione $gH = Hg$ può essere espressa come: $\forall h \in H$, $\exists h' \in H$ tale che $gh = h'g$, dove se $h = h'$, allora $h \in Z(G)$. In altre parole la prima condizione ci assicura l'esistenza di un elemento di H per cui la classe laterale destra è uguale alla sinistra, ma tale elemento non è necessariamente uguale a quello rispetto a cui si considera la classe laterale sinistra di H (e viceversa). Quindi la prima affermazione può essere vera anche se G non è abeliano (da cui l'Osservazione 1.81).

Ad esempio per $\langle\sigma\rangle \leqslant S_3$, si ha:

$$\tau\langle\sigma\rangle = \{\tau\circ id, \tau\circ\sigma, \tau\circ\sigma^2\}$$

$$\langle\sigma\rangle\tau = \{id\circ\tau, \sigma\circ\tau, \sigma^2\circ\tau\}$$

dove, come abbiamo visto $\tau\circ\sigma \neq \sigma\circ\tau$, ma allo stesso tempo $\tau\langle\sigma\rangle = \langle\sigma\rangle\tau$.

Esercizio 1.87. Sia G un gruppo, provare che i seguenti sottogruppi di G sono normali:

(1) $\{e\}$

(2) $Z(G)$

(3) G

Soluzione. Mostriamo uno per uno che i sottogruppi considerati sono normali:

(1) Nel caso del sottogruppo proprio $\{e\}$ possiamo mostrare che è normale sia applicando la definizione, che per il teorema appena dimostrato. Nel primo caso ci basta osservare che:
$$g\{e\} = \{e\}g \implies \{g\} = \{g\} \qquad \forall g \in G$$
che è sempre vera perché e è l'elemento neutro di G. Nel secondo caso basta osservare che:
$$g\{e\}g^{-1} = \{g\}g^{-1} = \{gg^{-1}\} = \{e\} \subseteq \{e\} \qquad \forall g \in G$$
da cui, di nuovo, la tesi $\{e\} \trianglelefteq G$.

(2) Abbiamo visto (Teorema 1.18) che $Z(G)$ è il sottogruppo degli elementi di G che commutano, quindi vale:
$$gZ(G) = gZ(G) \qquad \forall g \in G$$
che è esattamente la definizione di sottogruppo normale, dunque $Z(G) \trianglelefteq G$.

(3) Possiamo applicare il teorema appena dimostrato al sottogruppo proprio G ed osservare:
$$gGg^{-1} = \{\underbrace{gg'}_{\in G}|g' \in G\}g^{-1} = \{\underbrace{gg'g^{-1}}_{\in G}|g' \in G\} \subseteq G \qquad \forall g \in G$$
da cui la tesi $G \trianglelefteq G$.

□

Definizione 1.88. Sia G un gruppo e H un suo sottogruppo normale, definiamo **indice** di H in G il numero di classi laterali di H in G.

$$[G : H]$$

Osservazione 1.89 — Come abbiamo visto per il Teorema Di Lagrange esiste una bigezione $\varphi : H \xrightarrow[\sim]{} xH$, da cui $|H| = |xH|$, $\forall x \in G$, e, seguendo la dimostrazione, si osserva che la cardinalità dell'insieme dei rappresentanti $|\mathcal{R}|$ rappresenta il

numero di classi laterali di H in G[a], da cui:

$$[G : H] = \frac{|G|}{|H|}$$

Tale risultato, tuttavia, è valido solo nel caso di gruppi finiti, infatti come già visto nell'Osservazione 1.22, un sottogruppo di un gruppo infinito può avere sia ordine finito che infinito, mentre, nel caso di un gruppo finito l'ordine del sottogruppo deve necessariamente essere finito.[b]

[a] Potrebbe anche essere $|\mathcal{R}| = +\infty$ e quindi $[G : H] = +\infty$
[b] Nel caso generale (quindi anche quando abbiamo un gruppo ed un suo sottogruppo di ordine infinito) è necessario fare ricorso ai Numeri Cardinali.

Esercizio 1.90. Proponiamo due esercizi che ci permettono di fare utili osservazioni sull'indice appena introdotto:

(1) Dimostrare che $\#\{gH|g \in G\} = \#\{Hg|g \in G\}$, ovvero ci sono tante classi laterali sinistre quante destre di un sottogruppo.[a] [b]

(2) Dimostrare che ogni sottogruppo di indice 2 è normale.

[a] Questo esercizio ci permetterà di estendere la definizione di indice di un sottogruppo al caso generico di numero delle classi laterali.
[b] Per vedere un esempio si veda Classi laterali destre e sinistre.

Soluzione. Proviamo separatamente le due affermazioni:

(1) Per dimostrare che i due insiemi sono equipollenti ci basta trovare un'applicazione tra i due, che sia ben definita e bigettiva. Definiamo la funzione:

$$\varphi : \{gH|g \in G\} \longrightarrow \{Hg|g \in G\} : gH \longmapsto Hg^{-1}$$

(a) Dobbiamo verificare in primis la buona definizione dell'applicazione[21], consideriamo $g_1, g_2 \in G$, tali che $g_1H = g_2H$, ovvero $g_2^{-1}g_1 \in H$ (oppure $g_1^{-1}g_2 \in H$), affinché φ sia ben definita dobbiamo verificare che:

$$g_1H = g_2H \implies \varphi(g_1H) = \varphi(g_2H)$$

ovvero:

$$Hg_1^{-1} = Hg_2^{-1}$$

da cui $Hg_2^{-1}g_1 = H \implies g_2^{-1}g_1 \in H$ (oppure $Hg_1^{-1}g_2 = H \implies Hg_1^{-1}g_2 \in H$), ovvero la stessa relazione iniziale (che è equivalente logicamente al fatto che le due classi laterali sono uguali)[22], dunque, cambiando i rappresentanti delle classi laterali di partenza il risultato dell'applicazione non varia $\implies \varphi$ è ben definita.[23]

[21] Ricordiamo che le classi laterali di un sottogruppo sono classi di equivalenza, quindi hanno più di un solo rappresentante, pertanto quando si definisce un'applicazione tra di esse va verificata la buona definizione di quest'ultima.
[22] Invece, se ad esempio avessimo scelto come applicazione $\varphi : gH \longmapsto Hg$, per $g_1H = g_2H \iff g_2^{-1}g_1 \in H(g_1^{-1}g_2 \in H)$, avremmo ottenuto $g_2g_1^{-1} \in H(g_1g_2^{-1} \in H)$, quindi rappresentanti uguali avrebbero prodotto risultati diversi, non verificando la buona definizione.
[23] Se avessimo definito φ diversamente avremmo avuto due relazioni diverse tra g_1 e g_2 nel dominio e nell'immagine, e quindi vi sarebbero stato un problema di buona definizione.

(b) Per vedere φ è una bigezione, è sufficiente torvare un'inversa alla funzione data, e questa è banalmente:

$$\varphi^{-1} : \{Hg | g \in G\} \longrightarrow \{gH | g \in G\} : Hg \longmapsto g^{-1}H$$

ciò è equivalente a dire che φ è una bigezione.

(2) Siano G un gruppo e H un suo sottogruppo, tali per cui $[G : H] = 2$, in tal caso ci sono solo due classi laterali possibili, sia $s \in G \setminus H$, allora le uniche classi laterali possibili sono H, sH, oppure H, Hs. In tal caso, la prima classe laterale è sempre H stesso, pertanto $sH = Hs = G \setminus H$, $\forall s \in G \setminus H$. Inoltre, poiché $Hh = hH$[24], $\forall h \in H$, segue dunque che $gH = Hg$, $\forall g \in G$, quindi $H \trianglelefteq G$.

□

Teorema 1.91 (Sottogruppi Normali Ed Omomorfismi)
Siano G, G' due gruppi e $f : G \longrightarrow G'$ un omomorfismo tra loro, allora:

(1) $\ker f \trianglelefteq G$.

(2) $f(x) = f(y) \iff x \ker f = y \ker f$, $\forall x, y \in G$.[a]

(3) Sia $x \in G$ e $z = f(x)$, allora $f^{-1}(z) = x \ker f$.[b][c]

[a] In altre parole tutti gli elementi di una classe laterale del nucleo vanno in uno stesso elemento attraverso f (come accade per le classi di congruenza), quindi $x \ker f = y \ker f \implies x = yt$, $y \in \ker f$, ovvero, poiché x e y sono nella stessa classe laterale modulo $\ker f$, l'uno si può ottenere dall'altro per un elemento del nucleo, dunque $y^{-1}x \in \ker f \implies x \equiv y \pmod{\ker f}$.
[b] In pratica è l'inverso del punto (2).
[c] Per quanto visto nell'Teorema Di Lagrange segue allora che le controimmagini dell'omomorfismo hanno tutte la medesima cardinalità di $\ker f$.

Dimostrazione. Dimostriamo separatamente le affermazioni:

(1) Possiamo applicare il Teorema 1.84 per provare che il sottogruppo $\ker f$ è normale in G, dobbiamo dimostrare:

$$g \ker f g^{-1} \subseteq \ker f \qquad \forall g \in G$$

ovvero che, dato $t \in \ker f$:

$$gtg^{-1} \in \ker f \qquad \forall g \in G$$

poiché f è un omomorfismo si ha:

$$f(gtg^{-1}) = f(gt)f(g^{-1}) = f(g)f(t)f(g^{-1})$$

dove essendo $t \in \ker f \implies f(t) = e'$, segue:

$$f(gtg^{-1}) = f(g)f(g^{-1}) = f(g)f^{-1}(g) = e'$$

quindi $f(gtg^{-1}) = e'$, ovvero $gtg^{-1} \in \ker f \implies g \ker f g^{-1} \subseteq \ker f$, da cui la tesi.

[24] In quanto moltiplicando per un qualunque elemento del gruppo il prodotto deve essere ancora interno al gruppo, quindi in entrambi i casi si ottengono di nuovo tutti gli elementi di H, $Hh = hH = h$, $\forall h \in H$.

(2) Mostriamo che le due affermazioni sono logicamente equivalenti:

$$f(x) = f(y) \iff f^{-1}(y)f(x) = e' \iff f(y^{-1}x) = e' \qquad \forall x, y \in G$$

ovvero:

$$y^{-1}x \in \ker f \iff x \in y \ker f \qquad \forall x, y \in G$$

ma, essendo le classi laterali classi di equivalenza, allora x e y sono nella stessa classe laterale, pertanto:

$$x \in y \ker f \iff x \ker f = y \ker f \qquad \forall x, y \in G$$

pertanto le due affermazioni sono equivalenti.

(3) Sia $z = f(x)$, con $x \in G$, osserviamo che $f^{-1}(z) = \{y \in G | f(y) = z\}$, allora $f^{-1}(z) = \{y \in G | f(y) = f(x)\}$, ma per il punto (2) appena dimostrato questo insieme è la classe laterale di x modulo $\ker f$: $f^{-1}(z) = x \ker f$, ovvero la tesi.

□

§1.8 Gruppo quoziente

Definizione 1.92. Sia G un gruppo ed $N \trianglelefteq G$, l'insieme quoziente rispetto ad una delle due relazioni laterali G/N si dice **gruppo quoziente**:

$$G/N = \{gN | g \in G\}$$ [25] [26]

Se $N \trianglelefteq G$ posso considerare su G/N una struttura di gruppo indotta da G. Posso definire un'operazione tra classi laterali nel seguente modo:

$$g_1N \cdot g_2N = g_1g_2N$$

dove, essendo $g_1g_2 \in G$, g_1g_2N è ancora una classe laterale di G modulo N.

Lemma 1.93
L'operazione di prodotto tra classi laterali è ben definita.

Dimostrazione. Per verificare il lemma è sufficiente mostrare che se $x_1N = g_1N$ e $x_2N = g_2N$, allora $x_1x_2N = g_1g_2N$. Possiamo osservare che $x_1 = g_1s$ $(s \in N)$ e $x_2 = g_2t$ $(t \in N)$[27], dunque:

$$x_1x_2 = (g_1s)(g_2t) = g_1(sg_2)t = {}^{28}g_1g_2\underbrace{wt}_{\in N} \in g_1g_2N \implies x_1x_2 \in g_1g_2N$$

da cui $x_1x_2N = g_1g_2N$. □

Teorema 1.94
Dati un gruppo G e $N \trianglelefteq G$, il gruppo quoziente tra G ed N è un gruppo con l'operazione di prodotto tra classi laterali: $\left(G/N, \cdot\right)$.

Dimostrazione. Per dimostrare che G/N è un gruppo, dobbiamo verificare le quattro proprietà richieste dalla definizione di gruppo:

(a) Chiusura: Basta osservare che:

$$g_1N \cdot g_2N = \underbrace{g_1g_2}_{\in G}N \qquad \forall g_1, g_2 \in G$$

essendo $G/N = \{gH | g \in G\}$ la tesi è dimostrata.

(b) Associatività: Vogliamo dimostrare che $g_1N \cdot (g_2N \cdot g_3N) = (g_1N \cdot g_2N) \cdot g_3N$, $\forall g_1, g_2, g_3 \in G$, ci basta osservare che:

$$g_1N \cdot (g_2N \cdot g_3N) = (g_1N \cdot g_2N) \cdot g_3N \implies g_1N \cdot g_2g_3N = g_1g_2N \cdot g_3N$$

da cui:

$$g_1g_2g_3N = g_1g_2g_3N \qquad \forall g_1, g_2, g_3 \in G$$

si conclude che la tesi è vera.

[25] Poiché $N \trianglelefteq G$ è indifferente definire il gruppo quoziente con i laterali sinistri o destri.
[26] L'insieme esiste anche se N non è normale in G.
[27] Infatti se $xN = gN$, allora per $h \in N$, $x = gh \implies x = ghN \implies x = g(hN) = gN$.
[28] Poiché $N \trianglelefteq G$, allora le classi laterale sinistra e destra di ogni elemento modulo N coincidono, pertanto $Ng_2 = g_2N$, quindi esiste $w \in N$ tale che $sg_2 = g_2w$.

(c) Elemento Neutro: Poiché G è un gruppo, sia e il suo elemento neutro, allora $eN(=N)$ è l'elemento neutro del gruppo quoziente ${}^{G}\!/_{N}$, infatti:

$$eN \cdot gN = gN \cdot eN = gN \qquad \forall g \in G$$

pertanto $\left({}^{G}\!/_{N}, \cdot\right)$ è dotato di elemento neutro.

(d) Inverso: L'esistenza dell'inverso segue subito dal fatto che G sia un gruppo, infatti data gN, esiste sempre $g^{-1}N$ tale che:

$$g^{-1}N \cdot gN = gN \cdot g^{-1}N = eN \qquad \forall g \in G$$

□

Esempio 1.95 ($\mathbb{Z}/n\mathbb{Z}$)
Se prendiamo $G = \mathbb{Z}$ e $N = n\mathbb{Z}$, entrambi abeliani, segue che:

$${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \{[\overline{a}]_n\}$$

dove $\overline{a} = a + n\mathbb{Z}$, con $\overline{a} = \overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Teorema 1.96 (Omomorfismo Di Proiezione Al Quoziente)
Sia G un gruppo e $N \trianglelefteq G$, la mappa:

$$\pi_N : G \longrightarrow {}^{G}\!/_{N} : x \longmapsto xN$$

è un omomorfismo di gruppi surgettivo.

Dimostrazione. Possiamo verificare in maniera diretta che π_N è un omomorfismo:

$$\pi_N(xy) = xyN = xN \cdot yN = \pi_N(x) \cdot \pi_N(y) \qquad \forall x, y \in G$$

dove l'uguaglianza $xyN = xN \cdot yN$ è vera, poiché, come abbiamo visto ${}^{G}\!/_{N}$ è un gruppo rispetto al prodotto di classi laterali. Osserviamo, infine, che: $\mathrm{Im}\pi_N = \{xN\}_{x\in G} = {}^{G}\!/_{N} = \mathrm{Cod}(\pi_N)$, pertanto π_N è surgettivo. □

Osservazione 1.97 ($\ker \pi_N$) — Osserviamo che:

$$\ker \pi_N = \{x \in G | \pi_N(x) = xN = eN = N\} = \{x \in G | x \in N\} = N$$

Infatti, possiamo ottenere $\ker \pi_N = N$ anche con i contenimenti. Sia $n \in N$, allora:

$$\pi_N(n) = nN = N \implies N \subseteq \ker \pi_N$$

dove abbiamo usato il fatto che $n \in N$, e viceversa, sia $x \in \ker \pi_N$, allora

$$\pi_N(x) = xN = N \implies \ker \pi_N \subseteq N$$

Corollario 1.98

I sottogruppi normali di G[a] sono tutti e soli i nuclei degli omomorfismi definiti su G (dom $f = G$).[b] O, equivalentemente, un sottogruppo di G è normale se e solo se è il nucleo di un omomorfismo.

[a] Ricordiamo che in un gruppo rispetto ad una relazione c'è un solo sottogruppo (che può essere normale), mentre le restanti classi laterali sono soltanto insiemi.
[b] Generalizza l'Osservazione 1.96 ad ogni omomorfismo.

Dimostrazione. Per dimostrare il teorema dobbiamo provare entrambe le implicazioni:

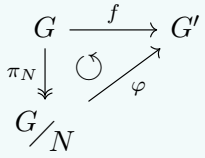
(a) Se $N \trianglelefteq G$, allora $N = \ker \pi_N$, ovvero N è sempre il nucleo della proiezione al quoziente (che può essere sempre definito per ipotesi), quindi tutti i sottogruppi normali sono nuclei di omomorfismi.

(b) Viceversa, se $f : G \longrightarrow G'$, allora per quanto visto nel Teorema 1.90, tutti i nuclei di omomorfismi sono sottogruppi normali, $\ker f \trianglelefteq G$.

Avendo provato entrambe le implicazioni, ovvero che un sottogruppo normale è sempre il nucleo di un omomorfismo (la proiezione al quoziente) e che il nucleo di un omomorfismo è sempre un sottogruppo normale in G, il teorema è dimostrato. □

§1.9 Teoremi di omomorfismo

Teorema 1.99 (Primo Teorema Di Omomorfismo)
Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi, sia $N \trianglelefteq G$ e $N \subseteq \ker f$, allora esiste ed è unico l'omomorfismo: $\varphi : {}^{G}\!/_{N} \longrightarrow G'$ che fa commutare il seguente diagramma:



ovvero $f = \varphi \circ \pi_N$, inoltre, $\mathrm{Im}\varphi = \mathrm{Im}f$ e $\ker \varphi = {}^{\ker f}\!/_{N}$.

Dimostrazione. Per dimostrare il teorema dobbiamo in primis dimostrare l'esistenza e l'unicità dell'applicazione φ: affinché il diagramma sia commutativo deve valere che $f = \varphi \circ \pi_N$, ovvero:

$$f(x) = \varphi \circ \pi_N(x) = \varphi(\pi_N(x)) = \varphi(xN) \qquad \forall x \in G$$

pertanto abbiamo costruito l'applicazione:

$$\varphi : {}^{G}\!/_{N} \longrightarrow G' : xN \longmapsto f(x)$$

da tale definizione osserviamo pertanto che φ esiste è unica (poiché deve sempre valere la relazione di commutatività del diagramma[29]). Poiché abbiamo definito la funzione su un insieme quoziente (e quindi mediante classi di equivalenza), essa è definita in termini di un suo rappresentante, per verificare che la definizione sia ben posta, e che quindi la funzione esista, dobbiamo verificarne la buona definizione. Consideriamo $xN = yN$ (ovvero $x \in yN$), allora deve essere $\varphi(xN) = f(x)$ e $\varphi(yN) = f(y)$, e per verificare la buona definizione deve valere:

$$\varphi(xN) = \varphi(yN) \implies f(x) = f(y)$$

per quanto visto nel Teorema 1.90 $f(x) = f(y) \iff x \ker f = y \ker f \iff x \in y \ker f$. Per ipotesi sappiamo che $xN = yN \implies x \in yN$, tuttavia, sempre per ipotesi $yN \subseteq y \ker f \implies x \in y \ker f \implies f(x) = f(y)$, poiché il risultato non varia cambiando rappresentante, abbiamo la buona definizione e di conseguenza la definizione dell'applicazione ha senso. Dobbiamo verificare che φ è un omomorfismo, per farlo possiamo usare il fatto che ${}^{G}\!/_{N}$ è un gruppo:

$$\varphi(xNyN) = \varphi(xN)\varphi(yN) \qquad \forall x, y \in G$$

da cui:[30]

$$\underbrace{\varphi(xyN)}_{=f(xy)} = f(x)f(y) = {}^{31}f(xy) \qquad \forall x, y \in G$$

quindi si conclude che φ è un omomorfismo. Ci restano da verificare le ultime due tesi:

[29] Cioè, affinché $\varphi \circ \pi_N = f$, poiché $x \overset{\pi_N}{\longmapsto} xN$, deve necessariamente essere che $xN \overset{\varphi}{\longmapsto} f(x)$.
[30] Dall'esistenza di φ, per la condizione imposta, segue che $f(x) = \varphi(x)$, $\forall x \in G$.
[31] Dove f è un omomorfismo per ipotesi.

- Per verificare che $\mathrm{Im}\varphi = \mathrm{Im}f$, osserviamo che:

$$\mathrm{Im}\varphi = \left\{\varphi(xN)\middle| xN \in {}^{G}\!/_{N}\right\} = \{f(x)|x \in G\} = \mathrm{Im}f$$

- Per quanto riguarda il nucleo di φ osserviamo:

$$\ker\varphi = \left\{xN \in {}^{G}\!/_{N}\middle|\varphi(xN) = e'\right\} = \left\{xN \in {}^{G}\!/_{N}\middle| f(x) = e'\right\} =$$

$$= \left\{xN \in {}^{G}\!/_{N}\middle| x \in \ker f\right\} \text{ [32]} = {}^{\ker f}\!/_{N}$$

□

Osservazione 1.100 ($N = \ker f$) — Nel caso particolare $N = \ker f$ il teorema ci dice:

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ {\scriptstyle \pi_{\ker f}}\downarrow & \circlearrowleft & \nearrow {\scriptstyle \varphi} \\ {}^{G}\!/_{\ker f} & & \end{array}$$

ovvero φ è un omomorfismo iniettivo, infatti $\ker\varphi = {}^{\ker f}\!/_{\ker f} = \{\ker f\}$ [a] $\cong \{e\}$, l'elemento neutro del gruppo ${}^{G}\!/_{\ker f}$, da cui, ricordando il punto (5) del Teorema 1.46, φ iniettivo.
Inoltre, ricordando che $\mathrm{Im}\varphi = \mathrm{Im}f \implies {}^{G}\!/_{\ker f} \cong \mathrm{Im}(f)$ [b], ogni omomorfismo può essere fattorizzato anche in questo modo:

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ {\scriptstyle \pi_{\ker f}}\downarrow & \circlearrowleft & \uparrow {\scriptstyle \varphi} \\ {}^{G}\!/_{\ker f} & \xrightarrow[\sim]{\overline{\varphi}} & \mathrm{Im}(f) \end{array}$$

[a] L'unica classe laterale di un gruppo quozientato per se stesso è il gruppo stesso, quindi ${}^{\ker f}\!/_{\ker f}$ è composto solo dal suo elemento neutro.
[b] Ciò è vero perché i due insiemi hanno la stessa cardinalità, esiste una applicazione iniettiva tra loro, e tale applicazione è un omomorfismo (in modo analogo a quanto visto nella dimostrazione del Primo Teorema Di Omomorfismo).

Osservazione 1.101 — Il Primo Teorema Di Omomorfismo asserisce quindi che ogni omomorfismo definito su un gruppo G si può fattorizzare in un omomorfismo surgettivo ($\pi_{\ker f}$) e una iniettivo (φ)

$$f(x) = \varphi \circ \pi_{\ker f}(x) \qquad \forall x \in G$$

[32] Sono le classi laterali xN con rappresentante x nel nucleo di f, essendo $N \subseteq \ker f$, quozientare $\ker f$ con N ci dà tutte le classi laterali modulo N di $\ker f$ (e quindi si stabilisce una partizione di $\ker f$ indott da N), con tutti i possibili rappresentanti in $\ker f$.

Teorema 1.102 (Secondo Teorema Di Omomorfismo)
Sia G un gruppo e $H, K \trianglelefteq G$, con $H \subseteq K$, allora:

$$\frac{G/H}{K/H} \cong G/K$$

Dimostrazione. Per dimostrare il teorema è sufficiente applicare due volte il Primo Teorema Di Omomorfismo, iniziamo considerando l'omomorfismo π_K, tale omomorfismo può essere fattorizzato considerando che $H \trianglelefteq G$, quindi:

$$\begin{array}{ccc} G & \xrightarrow{\pi_K} & G/K \\ {\scriptstyle \pi_H}\downarrow & \nearrow_{\varphi} & \\ G/H & & \end{array}$$

Dove $\mathrm{Im}\pi_K = \mathrm{Im}\varphi = G/K$, ovvero φ è surgettivo poiché lo è π_K, inoltre, $\ker\varphi = \ker\pi_{K/H} = K/H$. Riapplichiamo il Primo Teorema Di Omomorfismo alla mappa φ:

$$\begin{array}{ccc} G/H & \xrightarrow{\varphi} & G/K \\ {\scriptstyle \pi_{\ker\varphi}}\downarrow & \nearrow_{\overline{\varphi}} & \\ \frac{G/H}{K/H} & & \end{array}$$

dove abbiamo utilizzato come omomorfismo di proiezione del gruppo quello al nucleo del suo omomorfismo $\pi_{\ker\varphi} : G/H \twoheadrightarrow \frac{G/H}{\ker\varphi} = \frac{G/H}{K/H}$, da cui, come visto nell'Osservazione 1.99 $\overline{\varphi}$ è iniettivo, ma, come prima, $\mathrm{Im}\overline{\varphi} = G/K = \mathrm{Im}\varphi$, quindi $\overline{\varphi}$ è un isomorfismo tra gruppi (è un omomorfismo sempre per il Primo Teorema Di Omomorfismo), da cui la tesi:

$$\frac{G/H}{K/H} \cong G/K$$

□

Esempio 1.103 ($\mathbb{Z}$)
Consideriamo il gruppo $\mathbb{Z}$ e $m\mathbb{Z}, n\mathbb{Z} \trianglelefteq \mathbb{Z}$, con $m\mathbb{Z} \subseteq n\mathbb{Z}$ (ovvero $n \mid m$)[a], per il Secondo Teorema Di Omomorfismo si ha:

$$\frac{\mathbb{Z}/m\mathbb{Z}}{n\mathbb{Z}/m\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$$

[a] Come visto nell'Esercizio 1.35.

Corollario 1.104 (Quozienti Di Gruppi Ciclici)
Il gruppo quoziente di un gruppo ciclico è anch'esso ciclico.

Dimostrazione. Sia $G = \langle g \rangle$ un gruppo ciclico e $N \trianglelefteq G$ un suo sottogruppo normale (anch'esso ciclico, per quanto visto nel Teorema 1.33), vogliamo provare che $G/N = \langle gN \rangle$, con $g \in G$, ovvero che il gruppo quoziente è generato da una sua classe laterale. Per dimostrarlo possiamo utilizzare la doppia inclusione dei due insiemi:

- $\langle gN \rangle \subseteq G/N$ è banale, in quanto $gN \in G/N$ e G/N è un gruppo rispetto al prodotto di classi laterali.
- Per mostrare che $G/N \subseteq \langle gN \rangle$, osservo che per $xN \in G/N$, si ha $x \in G \implies x = g^k$ (con $k \in \mathbb{Z}$) in quanto G è ciclico per ipotesi, ma da ciò segue che: $x = g^k \implies g^k N = (gN)^k \in G/N$, pertanto segue $G/N \subseteq \langle gN \rangle$.

Dall'antisimmetria della relazione di inclusione segue la tesi: $\langle gN \rangle \subseteq G/N \wedge G/N \subseteq \langle gN \rangle \iff G/N = \langle gN \rangle$. □

Esercizio 1.105. Sia G un gruppo e $H, K \leqslant G$, allora HK[a] $\leqslant G$ se e solo se $HK = KH$[b]. In particolare questo è vero almeno se uno tra H e K è normale in G.

[a] Definiamo l'insieme HK **prodotto di sottogruppi** come l'insieme di tutti i prodotti hk, con $h \in H$ e $k \in K$.
[b] In tal caso la tesi $HK \leqslant G \iff HK = KH$ è anche equivalente logicamente a $KH \leqslant G$.

Soluzione. Per dimostrare l'affermazione proviamo:

- Proviamo che se $HK \leqslant G$, allora $HK = KH$, verifichiamo il duplice contenimento dei due insiemi:
  (a) Mostriamo che $\boxed{KH \subseteq HK}$, cioè che $kh \in HK$, $\forall k \in K, \forall h \in H$, osserviamo che possiamo scrivere $k = e \cdot k \in HK$ e $h = h \cdot e \in HK$, poiché HK è un sottogruppo, contiene il prodotto di tutti i suoi elementi, ed in particolare $kh \in HK$.
  (b) Viceversa, per mostrare $\boxed{HK \subseteq KH}$, bisogna verificare che $hk \in KH$, $\forall k \in K, \forall h \in H$, osserviamo che $h^{-1} = h^{-1} \cdot e \in HK$ e $k^{-1} = e \cdot h^{-1} \in HK$, quindi $k^{-1}h^{-1} \in HK \implies \exists h_2 \in H, \exists k_2 \in K$, tali che $k^{-1}h^{-1} = h_2 k_2$ ma per ipotesi HK è un sottogruppo, quindi è chiuso per inverso, pertanto $hk = k_2^{-1} h_2^{-1} \in KH$.
- Per dimostrare che se $KH = HK$, allora $HK \leqslant G$ (o $KH \leqslant G$) è sufficiente applicare il Teorema 1.12. Si osserva subito che se $hk \in HK$, allora $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK \implies (hk)^{-1} \in HK$, $\forall hk \in HK$, inoltre, presi $h_1 k_1$ e $h_2 k_2$ in HK, osserviamo che:

$$h_1 k_1 h_2 k_2 = h_1 \underbrace{(k_1 h_2)}_{=h_3 k_3} k_2 \overset{33}{=} h_1 h_3 k_3 k_2 = (h_1 h_3)(k_3 k_2) \in HK \qquad \forall h_1 k_1, h_2 k_2 \in HK$$

avendo verificato le ipotesi del teorema del sottogruppo segue che $HK = KH \implies HK \leqslant G$ e ciò completa la dimostrazione. Osserviamo che per definizione $KH =$

[33] Essendo per ipotesi $HK = KH$, segue che $\forall hk \in HK = KH$, $\exists k'h'$ tale che $hk = k'h'$.

HK equivale a $\{kH|k \in K\} = \{Hk|k \in K\}$, $\forall k \in K$, ma ciò coincide anche con la definizione di sottogruppo normale, pertanto la seconda condizione può anche essere espressa richiedendo che almeno uno dei due sottogruppi considerati sia normale.

□

Lemma 1.106 (Sottogruppi Normali Ed Omomorfismi)
Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi:

(1) Se $H \trianglelefteq G$ e f surgettiva, allora $f(H) \trianglelefteq G'$.

(2) Se $K \trianglelefteq G'$, allora $f^{-1}(K) \trianglelefteq G$.

Dimostrazione. Proviamo le tesi:

(1) Abbiamo già provato che $f(H) \leqslant G$ nel Teorema 1.46, per provare che $f(H)$ è normale in G', dobbiamo provare che $zf(H)z^{-1} \subseteq f(H)$ (seguendo quanto dimostrato nel Teorema 1.85), $\forall z \in G'$, ovvero:

$$zf(h)z^{-1} \in f(H) \qquad \forall z \in G'$$

dove, essendo f surgettiva, $\exists c \in G$ tale che $f(c) = z$, e seguendo la proprietà di omomorfismo possiamo scrivere:

$$zf(h)z^{-1} = f(c)f(h)f^{-1}(c) = f(\underbrace{chc^{-1}}_{\in H})^{34} \in f(H)$$

pertanto $f(H) \trianglelefteq G'$.

(2) Analogamente a quanto osservato prima, abbiamo già dimostrato che $f^{-1}(K) \leqslant G$ nel Teorema 1.46, inoltre, ricordiamo che per definizione $f^{-1}(K) = \{x \in G|f(x) \in K\}$. Per dimostrare la tesi dobbiamo mostrare che $gf^{-1}(K)g^{-1} \subseteq f^{-1}(K)$, $\forall g \in G$, ovvero $gkg^{-1} \in f^{-1}(K)$, $\forall g \in G$, possiamo considerare l'immagine dell'elemento:

$$f(gkg^{-1}) = \underbrace{f(g)f(k)f(g^{-1})}_{\in K} \implies gkg^{-1} \in f^{-1}(K) \qquad \forall g \in G$$

dove nell'ultimo passaggio abbiamo sfruttato il fatto che, essendo K normale in G', $aKa^{-1} = K$, $\forall a \in K$, e potendo definire le immagini di g e g^{-1} in G' la tesi è dimostrata.

□

[34] Dove abbiamo applicato la definizione di normalità in H

Teorema 1.107 (Terzo Teorema Di Omomorfismo)
Sia G un gruppo e siano $H, K \trianglelefteq G$, allora:

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

Dimostrazione. Per dimostrare il teorema possiamo applicare il Primo Teorema Di Omomorfismo cercando un'applicazione surgettiva $f : H \longrightarrow\!\!\!\!\!\rightarrow \frac{HK}{K}$, in modo tale da ottenere una bigezione se consideriamo la proiezione al quoziente modulo $\ker f$. Osserviamo che, poiché H e K sono normali in G, allora come visto nell'Esercizio 1.104 il loro prodotto è un sottogruppo di G, allora possiamo definire l'applicazione:

$$f : H \longrightarrow \frac{HK}{K} : h \longmapsto hK$$

Dove si è scelto di mandare h nella classe $hkK = hK$. Applicando il Primo Teorema Di Omomorfismo con $N = \ker f$, abbiamo la mappa:

$$\begin{array}{ccc} H & \xrightarrow{\ f\ } & \frac{HK}{K} \\ {\scriptstyle \pi_{\ker f}}\downarrow & \nearrow_{\varphi} & \\ H/_{\ker f} & & \end{array}$$

dove l'applicazione φ è bigettiva, in quanto $\mathrm{Im}\varphi = \mathrm{Im}f = \left\{ hkK \in {}^{HK}/_{K} \middle| h \in H \right\} = \frac{HK}{K}$, per provare ciò, osserviamo che $\mathrm{Im}f \subseteq \frac{HK}{K}$ è ovvio, quindi ci resta da verificare che $\frac{HK}{K} \subseteq \mathrm{Im}f = \{hk | h \in H\}$, ovvero che $hkK \in \frac{HK}{K}$, $h \in H$ e $k \in K$, ma $h \underbrace{kK}_{=K} = hK \in \varphi(h)$ (ovvero l'insieme dei rappresentati di ${}^{HK}/_{K}$ è semplicemente H, quindi hKè sempre immagine di qualche h), pertanto $\frac{HK}{K} \subseteq \mathrm{Im}f$, da ciò segue che $\mathrm{Im}f = \frac{HK}{K}$, ovvero f è surgettiva. Poiché si è scelto di quozientare per $\ker f$, il nucleo della nuova applicazione sarà banale: $\ker\varphi = {}^{\ker f}/_{\ker f} = \{\ker f\} \implies f$ iniettiva, e sempre per il Primo Teorema Di Omomorfismo tale applicazione sarà anche un omomorfismo. Abbiamo quindi dimostrato che:

$$\frac{H}{\ker f} \cong \frac{HK}{K}$$

Ci resta da mostrare che $\ker f = H \cap K$, osserviamo:

$$\ker f = \{h \in H | f(h) = hK = K\} = \{h \in H | h \in K\} = H \cap K$$

quindi la tesi:

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

□

§1.10 Teorema di corrispondenza dei sottogruppi

Teorema 1.108 (Teorema Di Corrispondenza Dei Sottogruppi)
Sia G un gruppo e $N \trianglelefteq G$, sia $\pi_N : G \longrightarrow {}^{G}\!/_{N}$ la proiezione al quoziente modulo N. La proiezione π_N induce una corrispondenza biunivoca tra i sottogruppi di ${}^{G}\!/_{N}$ e i sottogruppi di G che contengono N. Tale corrispondenza conserva la normalità e l'indice del sottogruppo.

Dimostrazione. Sia Y l'insieme dei sottogruppi di ${}^{G}\!/_{N}$, $Y = \left\{\mathcal{H} \leqslant {}^{G}\!/_{N}\right\}$, e X l'insieme dei sottogruppi di G che contengono N, $X = \{H \leqslant G | N \subseteq H\}$, vogliamo dimostrare che $\left\{\mathcal{H} \leq {}^{G}\!/_{N}\right\} \longleftrightarrow \{H \leq G | N \subseteq H\}$. Sia:

$$\alpha : X \longrightarrow Y : H \longmapsto \pi_N(H)$$

con $\pi_N(H) = {}^{H}\!/_{N}$, in quanto $\pi_N(H) = \{\pi_N(h) | h \in H\}$ [35] $= \{hN | h \in H\} = {}^{H}\!/_{N}$, ovvero α restituisce l'immagine insiemistica di un insieme (elemento di X) mediante π_N[36]. Definiamo inoltre:

$$\beta : Y \longrightarrow X : \mathcal{H} \longmapsto \pi_N^{-1}(\mathcal{H})$$

Con $\pi_N^{-1}(\mathcal{H}) = \{h \in H | \pi_N(h) = hN \in \mathcal{H}\}$ .Per dimostrare che esiste una corrispondenza biunivoca tra X ed Y, bisogna dimostrare che α e β sono l'una l'inversa dell'altra. Tuttavia, in quanto π_N è definita mediante classi laterali, bisognerà prima verificarne la buona definizione:

- α è ben definita: Per verificare ciò, basta ricordare il punto (3) del Teorema 1.46, quindi sia $H \leqslant G$, con $N \subseteq H$, allora $\pi_N(H) \leqslant {}^{G}\!/_{N}$, ovvero $\pi_N(H) = {}^{H}\!/_{N} \in Y$ (l'immagine di un sottogruppo, elemento di X, ci dà effettivamente un sottogruppo di ${}^{G}\!/_{N}$ e quindi un elemento di Y), poiché ${}^{H}\!/_{N}$ è un sottogruppo di ${}^{G}\!/_{N}$.
- β è ben definita: Per verificare ciò, ricordiamo il punto (4) del Teorema 1.46, quindi se $\mathcal{H} \leqslant {}^{G}\!/_{N}$, allora $\pi_N^{-1}(\mathcal{H}) \leqslant G$ (l'immagine di un sottogruppo, elemento di Y, ci dà effettivamente un sottogruppo di G e che quindi può essere un elemento di X), tuttavia, in questo caso, dobbiamo anche verificare anche che $N \subseteq \pi_N^{-1}(\mathcal{H})$, per fare ciò osserviamo che $N \in \mathcal{H}$ (poiché è l'elemento neutro del gruppo), ma per definizione di nucleo:

  $$\pi_N^{-1}(N) = \ker \pi_N \implies \ker \pi_N \subseteq \pi_N^{-1}(\mathcal{H})$$

  Ma, come visto nell'Osservazione 1.96 $\ker \pi_N = N \implies N \subseteq \pi_N(\mathcal{H}) \implies \pi_N^{-1}(\mathcal{H}) \in X$, e quindi è verificata anche la buona definizione di β.

Mostriamo che α e β sono l'una l'inversa dell'altra, iniziamo vedendo che $\alpha \circ \beta = \mathrm{id}_Y$:

$$\alpha \circ \beta(\mathcal{H}) = \pi_N \circ \pi_N^{-1}(\mathcal{H}) = \mathcal{H}$$

dove l'ultima uguaglianza è vera in quanto π_N è surgettiva[37], e come tale ammette inversa destra. Verifichiamo ora che $\beta \circ \alpha = \mathrm{id}_X$:

$$\beta \circ \alpha(H) = \pi_N^{-1} \circ \pi_N(H) = \pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}\left({}^{H}\!/_{N}\right) =$$

[35] Ovvero l'immagine di un insieme mediante una funzione.
[36] E gli elementi di tale immagine formano il gruppo quoziente ${}^{H}\!/_{N}$.
[37] Il fatto che ogni funzione surgettiva abbia un'inversa destra è equivalente all'Assioma Della Scelta.

$$= \left\{ h \in G \middle| \pi_N(h) = hN \in {}^{H}\!/_{N} \right\} = \{h \in G | h \in H\} = H$$

Per verificare che tale applicazione conservi la normalità, dobbiamo mostrare che $H \trianglelefteq G \iff \pi_N(H) = {}^{H}\!/_{N} \trianglelefteq {}^{G}\!/_{N}$, ciò segue immediatamente dal Lemma 1.105, infatti π_N è surgettiva dunque, se $H \in X$:

$$H \trianglelefteq G \implies \pi_N(H) \trianglelefteq {}^{G}\!/_{N}$$

e dato $\mathcal{H} \in Y$:

$$\mathcal{H} \trianglelefteq {}^{G}\!/_{N} \implies \pi_N^{-1}(\mathcal{H}) \trianglelefteq G$$

pertanto $H \trianglelefteq G \implies \pi_N(H) = {}^{H}\!/_{N} \trianglelefteq {}^{G}\!/_{N}$ e $\mathcal{H} \trianglelefteq {}^{G}\!/_{N} \implies \pi_N^{-1}(\mathcal{H}) \trianglelefteq G$.
Ci resta da verificare che la corrispondenza definita preservi l'indice del sottogruppo, ovvero che per $H \in X$:

$$[G : H] = \left[{}^{G}\!/_{N} : \pi_N(H) \right] = \left[{}^{G}\!/_{N} : {}^{H}\!/_{N} \right]$$

ricordando che gli elementi di ${}^{G}\!/_{N}$ sono le classi laterali di G modulo N, per dimostrare la tesi si deve far vedere che:

$$xH = yH \iff xN\left({}^{H}\!/_{N}\right) = yN\left({}^{H}\!/_{N}\right)$$

ovvero che due classi laterali di G modulo H sono uguali se e solo se lo sono anche le corrispettive classi laterale di ${}^{G}\!/_{N}$ modulo ${}^{H}\!/_{N}$, si osserva che:

$$xN\left({}^{H}\!/_{N}\right) = \{xNhN | h \in H\} = \{xhN | h \in H\}$$

e analogamente:

$$yN\left({}^{H}\!/_{N}\right) = \{yNhN | h \in H\} = \{yhN | h \in H\}$$

dove abbiamo usato il fatto che N sia normale per poter giustificare le ultime due uguaglianze. Quindi possiamo scrivere equivalentemente che deve essere:

$$xH = yH \iff \{xhN | h \in H\} = \{yhN | h \in H\}$$

inoltre, $xH = yH \iff y \in xH \implies y = xh_0$, $h_0 \in H$, da cui si ottiene che:

$$\{yhN | h \in H\} = \{x \underbrace{h_0 h}_{h_0 H = H} N | h \in H\} = \{xhN | h \in H\} = xN\left({}^{H}\!/_{N}\right)$$

nel terz'ultimo passaggio i prodotti sono tutti in H e quindi ci danno tutti gli altri elementi di H, pertanto si riottiene la definizione di $xN\left({}^{H}\!/_{N}\right)$,ciò dimostra l'ultima parte della tesi: $xH = yH \iff xN\left({}^{H}\!/_{N}\right) = yN\left({}^{H}\!/_{N}\right)$. □

Esempio 1.109
Sia $G = \mathbb{Z}$ e $N = n\mathbb{Z}$, da cui ${}^{G}\!/_{N} = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, per il Teorema di Corrispondenza si ha:

$$X = \{m\mathbb{Z} \subseteq \mathbb{Z} | n\mathbb{Z} \subset m\mathbb{Z}^{a}\} \longleftrightarrow \left\{K \leqslant {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right\} = Y$$

tale che:

$$\pi_{n\mathbb{Z}} : m\mathbb{Z} \longmapsto {}^{m\mathbb{Z}}\!/_{n\mathbb{Z}}{}^{b}$$

Questo ci dice che i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono tanti quante le proiezioni degli $m\mathbb{Z}$, con $m \mid n$ e sono del tipo $\pi_{n\mathbb{Z}}(m\mathbb{Z}) = {}^{m\mathbb{Z}}\!/_{n\mathbb{Z}}$ (dove $m \mid n$). Inoltre, il teorema di corrispondeza preserva anche l'indice del sottogruppo:

$$m = [\mathbb{Z} : m\mathbb{Z}] = \left[{}^{\mathbb{Z}}\!/_{n\mathbb{Z}} : {}^{m\mathbb{Z}}\!/_{n\mathbb{Z}}\right]$$

dove m rappresenta il numero di classi laterali di $\mathbb{Z}$ modulo $m\mathbb{Z}$ ed è uguale a quello delle classi laterali di $\mathbb{Z}/n\mathbb{Z}$ modulo $m\mathbb{Z}/n\mathbb{Z}$. In questo caso particolare, tuttavia, lo sapevamo già perché avevamo già contato i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ (infatti vale l'inverso di Lagrange, pertanto c'è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ per ogni $m \mid n$, del tipo $m\mathbb{Z}/n\mathbb{Z}$ e, che, come visto ne Teorema 1.41, ha esattamente ordine n/m), ricordando il Corollario 1.104, possiamo affermare che considerato un sottogruppo $m\mathbb{Z}/n\mathbb{Z} \leqslant \mathbb{Z}/n\mathbb{Z}$ si ha che (ricordando anche che il sottogruppo di ogni gruppo ciclico è ciclico):

$${}^{m\mathbb{Z}}\!/_{n\mathbb{Z}} = \langle \overline{m} \rangle \qquad \text{con} \qquad \operatorname{ord}(\overline{m}) = \frac{n}{(n,m)}$$

ma $m \mid n$ per ipotesi, quindi:

$$\operatorname{ord}(\overline{m}) = \frac{n}{m} = \left|{}^{m\mathbb{Z}}\!/_{n\mathbb{Z}}\right|$$

[a] Ovvero $m \mid n$, come visto nell'Esercizio 1.35.
[b] $\pi_{n\mathbb{Z}} : a(\in m\mathbb{Z}) \longmapsto [a]_n$.

Osservazione 1.110 — Se $N \trianglelefteq G$, allora $[G : N] = \left|{}^{G}\!/_{N}\right|$.

§2 Anelli

§2.1 Definizione di anello

Definizione 2.1. Un insieme non vuoto A si dice **anello** $(A, +, \cdot)$ se:

- $(A, +)$ è un gruppo abeliano.
- $\cdot$ è associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in A$.
- $\cdot$ è **distributivo** rispetto al $+$: $a \cdot (b+c) = a \cdot b + a \cdot c$ ed anche $(b+c) \cdot a = b \cdot a + c \cdot a$, $\forall a, b, c \in A$.

Definizione 2.2. Un anello $(A, +, \cdot)$ si dice **commutativo** se $\cdot$ è commutativo: $a \cdot b = b \cdot a$, $\forall a, b \in A$.

Definizione 2.3. Un anello $(A, +, \cdot)$ si dice **identitario** (o anello **con identità**) se esiste $1 \in A$: $a \cdot 1 = 1 \cdot a = a$, $\forall a \in A$.

Esempio 2.4 (Esempi Di Anello)

- $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ sono anelli commutativi con identità.
- $(m\mathbb{Z}, +, \cdot)$ è un anello commutativo con identità.
- $M_{n \times m}(\mathbb{R})$ è un anello commutativo con identità, $\forall n > 1$.

Definizione 2.5. Dato un anello A ed un suo elemento $x \in A$, x si dice **invertibile** in A se esiste $y \in A$ tale che:

$$x \cdot y = y \cdot x = 1$$

ovvero y è l'inverso di x, $y = x^{-1}$.

Definizione 2.6. Dato un anello con identità $(A, +, \cdot)$, possiamo definire l'insieme degli **elementi invertibili**:

$$A^* = \{x \in A | x \text{ è invertibile}\}$$

Esempio 2.7 (Insieme Degli Elementi Invertibili Di Un Anello)

- $\mathbb{Z}^* = \{\pm 1\}$.
- $\mathbb{Z}/m\mathbb{Z}^* = \{\overline{a} | (a, m) = 1\}$.[a]
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

[a] Ricordiamo che $ab \equiv 1 \pmod{n} \iff ab + nk = 1$, $k \in \mathbb{Z}$, che ha soluzioni intere (b, k) se e solo se $\gcd(a, n) \mid 1 \implies \gcd(a, n) = 1$.

Definizione 2.8. Dato un anello A ed un suo elemento $x \in A$, diciamo che x è un **divisore di zero** se esiste $y \in A$, con $y \neq 0$, tale che:

$$x \cdot y = y \cdot x = 0$$

Esempio 2.9

- In $\mathbb{Z}$ l'unico divisore di zero è 0.
- In $\mathbb{Z}/6\mathbb{Z}$ $\overline{2}$ è un divisore di zero, infatti: $\overline{2} \cdot \overline{3} = \overline{0}$.

Indichiamo con $D(A)$ l'insieme dei divisori di zero di un anello.

Definizione 2.10. Si definisce **dominio d'integrità** un anello commutativo con unità $(A, +, \cdot)$ in cui l'unico divisore di zero è 0:

$$D(A) = \{0\}$$

Definizione 2.11. Un anello commutativo con unità $(K, +, \cdot)$ si dice **campo** se:

$$K^* = K \setminus \{0\}$$

ovvero $(K, +)$ è un gruppo abeliano rispetto alla somma e $(K^*, \cdot)$ è un gruppo abeliano rispetto al prodotto.

Teorema 2.12 (Proprietà Degli Anelli)
Sia A un anello commutativo con unità, allora:

(1) $a \cdot 0 = 0 \cdot a = 0$, $\forall a \in A$.

(2) $(A^*, \cdot)$ è un gruppo (abeliano se A è commutativo).

(3) $D(A) \cap A^* = \emptyset$.

(4) Se A è un dominio di integrità valgono la legge di annullamento del prodotto e le leggi di cancellazione per la moltiplicazione (per ogni elemento diverso da 0).

Dimostrazione. Proviamo singolarmente le proprietà:

(1) Per dimostrare la tesi basta osservare, essendo lo 0 l'elemento neutro di $+$:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \qquad \forall a \in A$$

cancellando a destra $a \cdot 0$, poiché $(A, +)$ è un gruppo si ottiene:

$$a \cdot 0 = 0 \qquad \forall a \in A$$

analogamente si può mostrare l'affermazione a sinistra:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \qquad \forall a \in A$$

e cancellando a sinistra

$$0 \cdot a = 0 \qquad \forall a \in A$$

pertanto $a \cdot 0 = 0 \cdot a = 0$, $\forall a \in A$.

(2) Per provare che $(A^*, \cdot)$ è un gruppo, è sufficiente verificare le proprietà richieste dalla definizione:

(a) Chiusura: osserviamo che $\forall x, y \in A^*$, allora $\exists x^{-1}y^{-1} \in A$, pertanto $xy \in A^*$, poiché $y^{-1}x^{-1} \in A^*$.

(b) Associatività: poiché $A \subseteq A^*$, allora, essendo A associativo rispetto al $\cdot$, allora anche gli elementi di un suo qualsiasi sottoinsieme saranno associativi tra loro.

(c) Elemento Neutro: $1 \in A$, infatti, l'inverso di 1 è se stesso, quindi 1 è invertibile.

(d) Inverso: Segue per la stessa definizione di A^* che ogni suo elemento debba avere inverso moltiplicativo nel gruppo, $\forall x \in A, \exists x^{-1} \in A$:

$$x \cdot x^{-1} = x^{-1} \cdot x = 1 \qquad \forall x \in A$$

(3) Supponiamo per assurdo che $D(A) \cap A^* \neq \emptyset$, e consideriamo $x \in D(A) \cap A^*$, poiché $x \in D(A)$, allora $\exists z \in A, z \neq 0$, tale per cui:

$$xz = zx = 0$$

d'altra parte, poiché $x \in A^*$, allora $\exists x^{-1}$ tal per cui:

$$xy = yx = 1$$

da cui segue:

$$(zx)y = z(xy) \implies 0 \cdot y = z \implies z = 0$$

ma ciò è assurdo, pertanto l'ipotesi $D(A) \cap A^*$ è vuoto.

(4) Se A è un dominio d'integrità, allora $D(A) = \{0\}$, pertanto, se:

$$ab = 0$$

se $a = 0$, allora la legge di annullamento del prodotto è rispettata, se $a \neq 0$ ci sono due possibilità: o $b = 0$, ed in tal caso la legge di annullamento del prodotto è ancora rispettata, oppure $b \neq 0$, in tal caso, tuttavia, A non è più un dominio di integrità, poiché $A \neq \{0\}$, ma ciò è assurdo, pertanto la legge di annullamento del prodotto è sempre valida in un dominio d'integrità.
Dalla validità della legge in un dominio di integrità, segue anche che in tale dominio valgono le leggi di cancellazione rispetto al $\cdot$, infatti:

$$ab = ac \implies ab - ac = 0 \implies a(b - c) = 0 \qquad \forall a, b, c \in A$$

dove se $a \neq 0$, per la legge di annullamento del prodotto segue $b - c = 0 \implies b = c$, ovvero la legge di cancellazione sinistra. Analogamente per quella destra:

$$ba = ca \implies ba - ca = 0 \implies (b - c)a = 0 \qquad \forall a, b, c \in A$$

da cui se $a \neq 0$, allora $b - c = 0 \implies b = c$, ovvero la legge di cancellazione destra.

□

Corollario 2.13

Ogni campo è un dominio d'integrità.

Dimostrazione. Per definizione, l'insieme $(K, +, \cdot)$ si dice campo se $K^* = K \setminus \{0\}$, ma per quanto appena visto nel punto (2) del Teorema 2.12, $D(K) \cap K^* = \emptyset$, allora $D(K) \subseteq \{0\}$, ma, d'altra parte $0 \in D(K)$, pertanto $D(K) = \{0\}$, quindi per definizione K è un dominio d'integrità. □

Corollario 2.14
Ogni dominio d'integrità finito è un campo.

Dimostrazione. Sia A, con $|A| < +\infty$, un dominio d'integrità, definiamo per ogni $x \in A$, con $x \neq 0$ l'applicazione:

$$\varphi_x : A \longrightarrow A : a \longmapsto ax$$

si verifica subito che φ_x è iniettiva, infatti $\varphi_x(a) = \varphi_x(b) \iff xa = xb$, per la Legge di cancellazione sinistra, allora $a = b$ ($\iff \varphi_x(a) = \varphi_x(b)$). Inoltre, essendo $|A| < +\infty$, allora φ_x è anche surgettiva, quindi bigettiva.
Essendo φ_x bigettiva, allora $1 \in \text{Im}\varphi_x$, pertanto, esiste $\varphi_x(a) = ax = 1$, allora x è invertibile in A, $\forall x \in A$[38], $x \neq 0$. Quindi per definizione A è un campo. □

Osservazione 2.15 — Se A non è finito, allora il Corollario 2.14 non vale. Ad esempio, se consideriamo $\mathbb{Z}$, che è un dominio d'integrità, si osserva che non è un campo, in quanto $\mathbb{Z}^* \neq \mathbb{Z} \setminus \{0\}$.

Osservazione 2.16 — Consideriamo $\mathbb{Z}/m\mathbb{Z}$, ed osserviamo che:

$$\mathbb{Z}/m\mathbb{Z}^* = \{\overline{a} | (a, m) = 1\} \qquad D(\mathbb{Z}/m\mathbb{Z}) = \{\overline{a} | (a, m) \neq 1\}$$

Se $(a, m) = d > 1$, allora $\overline{a}\overline{\frac{m}{d}} = \overline{0}$[a], quindi $\overline{a} \in D(\mathbb{Z}/m\mathbb{Z})$ e $\overline{\frac{m}{d}} \neq \overline{0}$, quindi tutti gli elementi di $\mathbb{Z}/m\mathbb{Z}$ appartengono ad uno dei due insiemi, pertanto $\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}^* \cup D(\mathbb{Z}/m\mathbb{Z})$. Questo fatto può essere generalizzato a qualsiasi anello come stiamo per vedere.

[a] Cioè $\overline{a}$ è un divisore di zero.

Corollario 2.17
Sia A un anello finito, allora $A = A^* \cup D(A)$.

Dimostrazione. Possiamo dimostrare il corollario verificando la doppia inclusione dei due insiemi considerati:

- $A^* \cup D(A) \subseteq A$ è ovvia, essendo A^* e $D(A)$ sottoinsiemi di A.
- Per mostrare che $A \subseteq A^* \cup D(A)$, osserviamo che, considerato $a \in A$, se $a \in D(A)$ il contenimento è verificato, se invece $a \notin D(A)$, allora φ_a[39] è iniettiva (poiché valgono le Leggi di cancellazione) e quindi surgettiva.[40] Seguendo lo stesso ragionamento utilizzato nella dimostrazione del Corollario 2.14 osserviamo che a è invertibile, ovvero $a \in A^* \implies A \subseteq A^* \cup D(A)$.

Per l'antisimmetria della relazione di inclusione segue la tesi $A = A^* \cup D(A)$. □

[38] Ovvero, possiamo definire l'applicazione per ogni elemento di A, ed avere sempre nella sua immagine 1, in tal modo, ogni elemento è invertibile.
[39] Definita analogamente a quanto fatto nella dimostrazione del Corollario 2.14.
[40] Ricordando che per ipotesi $|A| < +\infty$.

§2.2 Omomorfismo di anelli

Definizione 2.18. Dati due anelli con identità A e B, l'applicazione $\varphi : A \longrightarrow B$ si dice **omomorfismo** di anelli se:

- $\varphi(x +_A y) = \varphi(x) +_B \varphi(y)$, ovvero φ è un omomorfismo tra $(A, +_A)$ e $(B, +_B)$, $\forall x, y \in A$.
- $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$, $\forall x, y \in A$.
- $\varphi(1_A) = 1_B$.

§3 Polinomi

§3.1 Anello dei polinomi

Definizione 3.1. Dato un anello commutativo con unità si definisce **anello dei polinomi** nell'**indeterminata** x:

$$A[x] = \left\{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \middle| n \in \mathbb{N}, a_i \in A\right\}$$

Gli elementi di tale anello prendono il nome di **polinomi**.

Osservazione 3.2 (Somma Di Polinomi) — Abbiamo utilizzato gli anelli per formalizzare le proprietà usuali dei polinomi, ad esempio la somma. Dati:

$$f(x) = \sum_{i=0}^{n} a_ix^i \qquad \text{e} \qquad g(x) = \sum_{i=0}^{m} b_ix^i$$

osserviamo che:

$$f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i$$

dove le somme $a_i + b_i$[a][b] sono somme tra elementi dell'anello A

[a] In questo caso si considerano anche i coefficienti uguali a 0.
[b] Inoltre se $m < n$, allora $b_{m+1} = b_{m+2} = \ldots = b_n = 0$.

Osservazione 3.3 (Prodotto Di Polinomi) — Osserviamo la stessa cosa per il prodotto di polinomi:

$$f(x) \cdot g(x) = \sum_{i=0}^{m+n} \left(\sum_{j+k=i} a_jb_k \right) x^i$$

ovvero:

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1x + a_2x^2 + \ldots) \cdot (b_0 + b_1x + b_2x^2 + \ldots) = \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots \end{aligned}$$

Osservazione 3.4 (Polinomio Nullo) — Il polinomio $f(x) = 0$ prende il nome di **polinomio nullo**. Si considera tale polinomio privo di termini ed il suo grado, a differenza del polinomio costante, non è 0.[a][b]

[a] Il polinomio nullo è anche l'unico polinomio ad avere un numero infinito di radici.
[b] Il grafico del polinomio nullo coincide con l'asse delle x sul piano cartesiano.

Teorema 3.5 (Struttura Di Anello Dei Polinomi)
L'anello dei polinomi $(A[x], +, \cdot)$ è un anello commutativo con unità.

Dimostrazione. Per dimostrare il teorema dobbiamo dimostrare che $(A[x], +)$ è un gruppo abeliano e poi che $A[x]$ rispetto all'operazione $\cdot$ è: associativo, distributivo, possiede elemento neutro ed è commutativo. Per dimostrare la prima cosa possiamo sfruttare il fatto che A è un anello commutativo con unità e la definizione data nell'Osservazione 3.2 di somma tra polinomi per verificare le proprietà richieste dalla definizione:

(a) Chiusura: Vogliamo dimostrare che presi $f(x), g(x) \in A[x]$, allora $f(x)+g(x) \in A[x]$, per farlo ci basta osservare che per definizione:

$$f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} (\underbrace{a_i + b_i}_{\in A})x^i$$

ovvero, il nuovo polinomio definito dalla scrittura sopra ha i coefficienti in A, quindi è verificata l'appartenenza ad $A[x]$.

(b) Associatività: Mostriamo che:

$$f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) \qquad \forall f(x), g(x), h(x) \in A[x]$$

da cui, per la definizione di somma:

$$f(x) + \sum_{i=0}^{\max\{m,o\}} (g_i + h_i)x^i = \sum_{i=0}^{\max\{n,m\}} (f_i + g_i)x^i + h(x)$$

quindi:

$$\sum_{i=0}^{\max\{n,m,o\}} (f_i + (g_i + h_i))x^i = \sum_{i=0}^{\max\{n,m,o\}} ((f_i + g_i) + h_i)x^i$$

dove l'ultima uguaglianza è sempre vera, in quanto per ipotesi A è un anello.

(c) Elemento Neutro: Nell'Osservazione 3.4 abbiamo definito il polinomio nullo come $f(x) = 0$, come si osserva tale polinomio è l'elemento neutro rispetto alla somma di $A[x]$:

$$f(x) + g(x) = {}^{41} \sum_{i=0}^{m} (0 + g_i)x^i = \sum_{i=0}^{m} (g_i + 0)x^i = g(x) \qquad \forall g(x) \in A[x]$$

(d) Inverso: Segue dall'inverso additivo in A, infatti, per ogni $f(x) \in A[x]$, possiamo definire $-f(x)$ come:

$$-f(x) = \sum_{i=0}^{n} (-a_i)x^i$$

dove $-a_i$ esiste sempre in quanto A è un anello. Per tale polinomio si verifica che:

$$f(x) + (-f(x)) = \sum_{i=0}^{n} (a_i + (-a_i))x^i = \sum_{i=0}^{n} ((-a_i) + a_i)x^i =$$
$$= (-f(x)) + f(x) = 0 \qquad \forall f(x) \in A[x]$$

[41] Ricordiamo che $(0, n) = n$, $\forall n \in \mathbb{N}$.

(e) Commutatività: Segue sempre dalla definizione di somma e dal fatto che A sia un anello:

$$f(x)+g(x)=\sum_{i=0}^{\max\{n,m\}}(a_i+b_i)x^i=\sum_{i=0}^{\max\{n,m\}}(b_i+a_i)x^i=g(x)+f(x)$$

$\forall f(x),g(x)\in A[x]$.

Verifichiamo le proprietà mancanti su $\cdot$ per la definizione di anello commutativo con unità:

(a) Chiusura: Verifichiamo che per ogni $f(x),g(x)\in A[x]$, allora $f(x)\cdot g(x)\in A[x]$:

$$f(x)\cdot g(x)=\sum_{i=0}^{n+m}\left(\sum_{j+k=i}a_jb_k\right)x^i$$

dove $a_jb_k\in A$, in quanto A è un anello, pertanto $f(x)\cdot g(x)\in A[x]$.

(b) Associatività: Come nel caso precedente segue dalle proprietà di A:

$$\begin{aligned}f(x)\cdot(g(x)\cdot h(x))&=\sum_{i=0}^{n+m+o}\left(\sum_{j+k+l=i}a_j(b_kc_l)\right)x^i=\\&=\sum_{i=0}^{n+m+o}\left(\sum_{j+k+l=i}(a_jb_k)c_l\right)x^i=(f(x)\cdot g(x))\cdot h(x)\end{aligned}$$

$\forall f(x),g(x),h(x)\in A[x]$.

(c) Elemento Neutro: Definiamo il polinomio $e(x)=1$ elemento neutro rispetto al $\cdot$ di $A[x]$, infatti:

$$e(x)\cdot g(x)=\sum_{i=0}^{m}\left(\sum_{j+k=i}1\cdot b_k\right)x^i=\sum_{i=0}^{m}\left(\sum_{j+k=i}b_k\cdot 1\right)x^i=g(x)\cdot e(x)=g(x)$$

$\forall g(x)\in A[x]$.

(d) Distributività: Si osserva che:

$$\begin{aligned}&(f(x)+g(x))\cdot h(x)=\\&=\sum_{i=0}^{\max\{n,m\}+o}\left(\sum_{j+k=i}(a_j+b_j)c_k\right)x^i=\sum_{i=0}^{\max\{n,m\}+o}\left(\sum_{j+k=i}(a_jc_k+b_jc_k)\right)x^i=\\&=\sum_{i=0}^{\max\{n,m\}+o}\left(\sum_{j+k=i}a_jc_k\right)x^i+\sum_{i=0}^{\max\{n,m\}+o}\left(\sum_{j+k=i}b_jc_k\right)x^i=\\&=f(x)\cdot h(x)+g(x)\cdot h(x)\end{aligned}$$

$\forall f(x),g(x),h(x)\in A[x]$.

(e) Commutatività: Segue da quella in A:

$$f(x)\cdot g(x)=\sum_{i=0}^{m+n}\left(\sum_{j+k=i}a_jb_k\right)x^i=\sum_{i=0}^{m+n}\left(\sum_{j+k=i}b_ka_j\right)x^i=g(x)\cdot f(x)$$

$\forall f(x),g(x)\in A[x]$.

□

Definizione 3.6. Dato un polinomio $f(x)\in A[x]\setminus\{0\}$ definiamo il **grado del polinomio**, $\deg f(x)$ o $\partial f(x)$, come l'indice del coefficiente non nullo più grande, ovvero:

$$\deg f(x)=\max\{i\in\mathbb{N}|a_i\neq 0\}$$

Osservazione 3.7 — Non definiamo il grado del polinomio nullo.[a]

[a] In alcuni contesti matematici può essere utile, invece, definire il grado del polinomio nullo come $-\infty$.

Esempio 3.8

Consideriamo i due polinomi $f(x),g(x)\in\mathbb{Z}/6\mathbb{Z}[x]$, definiti come $f(x)=2x$ e $g(x)=3x^2$, osserviamo che:

$$\overline{2}x\cdot\overline{3}x^2=\overline{6}x^3=\overline{0}$$

Teorema 3.9 (Proprietà Del Grado Dei Polinomi)

Dati due polinomi $f(x),g(x)\in A[x]$, valgono le seguenti proprietà rispetto ai gradi:

(1) $\deg(f(x)+g(x))\leq\max\{\deg f(x),\deg g(x)\}$.

(2) Se A è un dominio d'integrità: $\deg(f(x)\cdot g(x))=\deg f(x)+\deg g(x)$.

Dimostrazione. Dimostriamo separatamente le affermazioni:

(1) Ci basta ricordare la definizione di somma di polinomi, infatti, detti $\deg f(x)=n$ e $\deg g(x)=m$:

$$f(x)+g(x)=\sum_{i=0}^{\max\{n,m\}}(a_i+b_i)x^i$$

da cui segue per definizione di grado che $\deg(f(x)+g(x))\leq\max\{n,m\}$.

(2) Siano $\deg f(x)=n$ e $\deg g(x)=m$, per definizione m ed n sono i massimi interi tali per cui $a_n\neq 0$ e $b_m\neq 0$, essendo per ipotesi $A[x]$ un dominio di integrità, allora $D(A[x])=\{0\}$, ovvero l'unico divisore di zero è 0, da ciò segue che per definizione di prodotto di polinomi si ha:

$$f(x)\cdot g(x)=\sum_{i=0}^{n+m}\left(\sum_{j+k=i}a_jb_k\right)x^i=a_nb_mx^{n+m}+\ldots+a_0b_0$$

con $a_nb_m\neq 0$, in quanto, come visto $a_n,b_m\neq 0$, pertanto $\deg(f(x)+g(x))=n+m$, da cui segue la tesi $\deg(f(x)\cdot g(x))=\deg f(x)+\deg g(x)$.

□

Corollario 3.10

Sia A un anello commutativo con unità, se A è un dominio di integrità, allora l'anello dei polinomi a coefficienti in A è a sua volta un dominio di integrità.

Dimostrazione. Siano $f(x), g(x) \in A[x] \setminus \{0\}$, e $\deg f(x) = n \geq 0$, $\deg g(x) = m \geq 0$, essendo $a_n, b_m \neq 0$, segue che $a_n b_m \neq 0$ poiché per ipotesi A un dominio di integrità, pertanto $f(x) \cdot g(x) \neq 0$ se $f(x), g(x) \neq 0 \implies A[x]$ è un dominio d'integrità. □

Corollario 3.11

Sia A un dominio di integrità, allora $(A[x])^* = A^*$.

Dimostrazione. Se A è un dominio di integrità per quanto visto nel corollario 3.10, allora anche $A[x]$ è un dominio di integrità, consideriamo dunque un elemento invertibile $f(x) \in (A[x])^*$, si ha che per definizione:

$$\forall f(x) \in (A[x])^*, \exists g(x) \in A[x] : f(x) \cdot g(x) = g(x) \cdot f(x) = 1$$

in tale situazione si ha $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x) = \deg(1) = 0 \implies \deg f(x) = \deg g(x) = 0$, da ciò segue che $f(x) \in A^*$, che dimostra la tesi (ovvero che tutti gli invertibili di $A[x]$ sono invertibili di A). □

Osservazione 3.12 — Se consideriamo i polinomi a coefficienti in un anello che non sia un dominio di integrità, ad esempio $\mathbb{Z}/4\mathbb{Z}[x]$, si osserva che:

$$(\overline{2}x + \overline{1})^2 = \overline{4}x^2 + \overline{4}x + \overline{1} = \overline{1}$$

dove appunto $(\overline{2}x + \overline{1})$ è l'inverso di se stesso, ma $(\overline{2}x + \overline{1}) \notin \mathbb{Z}/4\mathbb{Z}^*$.

§3.2 Polinomi a coefficienti in un campo

Sia K un campo, consideriamo i polinomi in $K[x]$.

Teorema 3.13 (Teorema Di Divisione Euclidea)
Siano $f(x), g(x) \in K[x]$, con $f(x) \neq 0$, allora esistono e sono unici $q(x), r(x) \in K[x]$ tali che:

$$g(x) = q(x)f(x) + r(x)$$

con $0 \leq \deg r(x) < \deg f(x)$.

Dimostrazione. Se $g(x) = 0$, allora si ha $q(x) = 0$, $f(x) = 0$ e $r(x) = 0$. Se $g(x) \neq 0$, usiamo l'induzione su $n = \deg g(x)$. Per $n = 0$, $g(x)$ è una costante, allora, se $\deg f(x) = 0$, segue che:

$$g(x) = f(x)\frac{g(x)}{f(x)}$$

se $\deg f(x) > 0$, allora:

$$g(x) = 0 \cdot f(x) + g(x) \qquad 0 \leq \deg g(x) < \deg f(x)$$

e ciò conclude il passo base. Supponiamo ora la tesi vera per ogni $k \in \{1, \dots, n-1\}$, e proviamola per $\deg g(x) = n$. Se $\deg f(x) = m > n$, allora:

$$g(x) = 0 \cdot f(x) + g(x) \qquad 0 \leq \deg g(x) < \deg f(x)$$

se $m \leq n$, allora, scriviamo $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{i=0}^{n} b_i x^i$, allora si può scrivere:

$$g_1(x) = g(x) - \frac{b_n}{a_m}x^{n-m}f(x)$$

in tal modo si cancella il coefficiente di testa di $g(x)$ e si ha $\deg g_1(x) < \deg g(x)$ in quanto vale l'ipotesi induttiva, pertanto:

$$g_1(x) = q_1(x)f(x) + r(x)$$

da cui:

$$g(x) = q_1(x)f(x) + r(x) + \frac{b_n}{a_m}x^{n-m}f(x) = \left(q_1(x) + \frac{b_n}{a_m}x^{n-m}\right)f(x) + r(x)$$

□

Teorema 3.14 (Teorema Di Ruffini)
Sia $f(x) \in K[x]$ e $\alpha \in K$, allora $f(\alpha) = 0$, con $\alpha \in K$, se e solo se $x - \alpha \mid f(x)$.

Dimostrazione. Per dimostrare il teorema proviamo entrambe le implicazioni:

- Proviamo che se $f(\alpha) = 0$, allora $x - \alpha \mid f(x)$. Effettuando la divisione euclidea appena vista si osserva che:

  $$f(x) = (x - \alpha)q(x) + r(x)$$

  con $0 \leq \deg r(x) < \deg(x - \alpha) = 1$, da ciò si può osservare che:

  $$f(\alpha) = 0 \implies r(\alpha) = 0 \implies x - \alpha \mid f(x)$$

- Vediamo che se $x-\alpha \mid f(x)$, allora $f(\alpha)=0$. Per ipotesi si ha che:
$$f(x)=(x-\alpha)q(x)$$
da cui segue subito che $f(\alpha)=0$ per la legge di annullamento del prodotto in un anello.

□

Presi $f(x), g(x) \in K[x]$ si può parlare di M.C.D. e questo può essere calcolato mediante l'Algoritmo di Euclide:
$$\{f(x), g(x)\} \xrightarrow{\text{A.E.}} d(x) = (f(x), g(x))$$
inoltre si possono determinare in tal modo anche i polinomi coefficienti per l'Identità di Bézout:
$$d(x) = a(x)f(x) + b(x)g(x)$$
per tale massimo comune divisore vale l'unicità a meno di costante moltiplicativa, infatti, supponendo che ve ne siano due $d(x), d_1(x)$ deve essere che:
$$d(x) \mid d_1(x) \implies d_1(x) = c(x)d(x)$$
ed anche:
$$d_1(x) \mid d(x) \implies d(x) = \gamma(x)d_1(x)$$
da cui:
$$d_1(x) = c(x)\gamma(x)d_1(x) \implies c(x)\gamma(x) = 1$$
ovvero $c(x)$ costante ($\deg c(x) = 0$), quindi tutti i possibili M.C.D. differiscono a meno di una costante moltiplicativa non nulla.

Definizione 3.15. Sia $f(x) \in K[x]$ un polinomio non costante, esso si dice **irriducibile** in $K[x]$ se si ha che $f(x) = g(x)h(x)$, con $g(x), h(x) \in K[x]$, $\deg g(x) = 0$ oppure $\deg h(x) = 0$.[42]

Definizione 3.16. Sia $f(x) \in K[x]$ un polinomio non costante, esso si dice **primo** in $K[x]$ se si ha che quando $f(x) \mid g(x)h(x)$, con $g(x), h(x) \in K[x]$, allora $f(x) \mid g(x)$ o $f(x) \mid h(x)$.

Proposizione 3.17
Dato $f(x) \in K[x]$, esso è irriducibile se e solo se è primo.

Dimostrazione. Proviamo le implicazioni separatamente:

- Mostriamo che se $p(x)$ è primo, allora è irriducibile, sia:
$$p(x) = a(x)b(x) \implies p(x) \mid a(x)b(x)$$
sfruttiamo l'ipotesi di primalità e supponiamo (WLOG) che $p(x) \mid a(x)$, allora $a(x) = p(x)u(x)$, da cui:
$$p(x) = p(x)u(x)b(x) \implies u(x)b(x) = 1 \implies \deg b(x) = 0 \implies b(x) \in K$$
pertanto $p(x)$ è irriducibile.

[42] In altre parole un polinomio è irriducibile in un campo quando non si può scomporre ulteriormente come prodotto di polinomi di quel campo, ma soltanto in un polinomio di grado uguale per una costante (polinomio di grado 0). Si osserva inoltre che i polinomi di grado 0 sono invertibili, e quindi, come visto, uno dei due fattori nel prodotto è invertibile in K.

- (Vale in UFD) Mostriamo che se $p(x)$ è irriducibile, allora è primo, sia:

$$p(x) \mid a(x)b(x)$$

se $p(x) \mid a(x) \implies p(x)$ è primo, se $p(x) \nmid a(x)$, allora, essendo $p(x)$ irriducibile segue che $(p(x), a(x)) = 1$, e per il Lemma di Euclide (per i polinomi), segue che $p(x) \mid b(x) \implies p(x)$ primo.

□

Teorema 3.18 (Teorema Di Fattorizzazione Unica)
Ogni polinomio di $K[x]$ non costante si fattorizza in modo unico come prodotto di polinomi irriducibili

Osservazione 3.19 — L'unicità si ha a meno dell'ordine dei dei fattori e di moltiplicazione per elementi invertibili, ad esempio $x^2 = \frac{1}{2}x \cdot 2x = \frac{1}{4}x \cdot 4x = x \cdot x$. Inoltre, il teorema vale in qualsiasi anello a fattorizzazione unica (UFD).

Corollario 3.20
Sia $f(x) \in K[x]$, con $f(x) \neq 0$, allora $f(x)$ ha al più $\deg f(x)$ radici in K, ciascuna contata con la propria molteplicità.

Dimostrazione. Per quanto visto nel Teorema di Ruffini, $\alpha \in K$ è radice di $f(x)$ se e solo se $x - \alpha \mid f(x)$, ciò unito al Teorema di Fattorizzazione Unica ci permette pertanto di scrivere:

$$f(x) = (x - \alpha_1)^{e_1}(x - \alpha_2)^{e_2} \dots (x - \alpha_r)^{e_r} g(x)$$

dove $g(x)$ è il prodotto (irriducibile) dei fattori di grado maggiore di 1. Da ciò, essendo $K[x]$ un campo (e quindi anche un dominio di integrità), segue che:

$$\deg f(x) = e_1 + e_2 + \dots + e_r + \deg g(x)$$

essendo che $\deg g(x) \geq 0$, cui segue la tesi $e_1 + e_2 + \dots + e_r \leq \deg f(x)$. □

§3.3 Fattorizzazione Di Polinomi In Un Campo

La trattazione del problema della fattorizzazione di polinomi può essere svolta adeguatamente in un campo, poiché in esso vale il Teorema di Fattorizzazione Unica.

§3.3.1 $\mathbb{C}[x]$

Teorema 3.21 (Teorema Fondamentale Dell'Algebra)
Ogni polinomio non costante in $\mathbb{C}[x]$ ammette almeno una radice in $\mathbb{C}$.

Corollario 3.22 (Polinomi Irriducibili in $\mathbb{C}[x]$)
Dato un polinomio $p(x) \in \mathbb{C}[x]$ esso è irriducibile in $\mathbb{C}[x]$ se e solo se $\deg p(x) = 1$.

Dimostrazione. Mostriamo le due implicazioni:

- Vediamo che i polinomi di grado 1 in $\mathbb{C}[x]$ sono irriducibili. In generale, in ogni campo $K[x]$, un polinomio $p(x)$ di grado 1 può essere fattorizzato come prodotto di due polinomi, $p(x) = f(x)g(x)$, dove, essendo ogni campo dominio di integrità, deve essere che $\deg p(x) = \deg f(x) + \deg g(x) = 1$, con $\deg f(x), \deg g(x) \geq 0$, pertanto $\deg f(x) = 0$ oppure $\deg g(x) = 0$, e quindi, $p(x)$ è irriducibile in $\mathbb{C}[x]$ per definizione.
- Sia $p(x)$ un polinomio irriducibile in $\mathbb{C}[x]$, supponiamo che $\deg p(x) = d > 1$. Per il Teorema Fondamentale dell'Algebra esso ammette almeno una radice $\alpha \in \mathbb{C}$, e per il Teorema di Ruffini deve essere che:

  $$x - \alpha \mid p(x)$$

  ovvero $p(x) = (x - \alpha)q(x)$, con $\deg q(x) = \deg p(x) - 1$, pertanto $\deg q(x) \geq 1$, inoltre, $\deg(x - \alpha) = 1 > 0$, allora $p(x)$ non è irriducibile, in quanto $(\mathbb{C}[x])^* = \mathbb{C}^*$ ma $q(x), (x - \alpha) \notin \mathbb{C}^*$, si giunti così ad un assurdo, pertanto deve essere che $\deg p(x) = 1$.

□

Corollario 3.23
Ogni polinomio non costante in $\mathbb{C}[x]$ si fattorizza come prodotto di polinomi di grado 1.

Dimostrazione. Per quanto visto nel Teorema Fondamentale dell'Algebra ogni polinomio $p(x)$ non costante ammette almeno una radice α in $\mathbb{C}$, per il Teorema di Ruffini tale polinomio può sempre essere riscritto come $p(x) = (x - \alpha)q(x)$, e l'operazione può essere ripetuta fino ad ottenere:

$$p(x) = (x - \alpha_1)^{e_1}(x - \alpha_2)^{e_2} \dots (x - \alpha_r)^{e_r}$$

infine, per il Corollario 3.21, tutti i polinomi $(x - \alpha_i)^{e_i}$ sono irriducibili in $\mathbb{C}[x]$ essendo di grado 1. Alternativamente basta osservare che, essendo $\mathbb{C}[x]$ un campo, vale il Teorema di Fattorizzazione Unica, ma per il Corollario 3.21 tutti i fattori irriducibili devono avere grado 1. □

Corollario 3.24
Ogni polinomio di $\mathbb{C}[x]$ ha tante radici (contate con molteplicità) quanto il suo grado.

Dimostrazione. Per quanto visto nel corollario precedente, ogni polinomio in $\mathbb{C}[x]$ può essere fattorizzato come:

$$p(x) = (x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\dots(x-\alpha_r)^{e_r}$$

da cui $\deg p(x) = e_1 + e_2 + \dots + e_r$, e ciò dimostra la tesi. □

Osservazione 3.25 — In $\mathbb{C}[x]$ abbiamo quindi risultati teorici "bellissimi" ma determinare le radici di un polinomio è in generale abbastanza difficile.

Esempio 3.26
Consideriamo il polinomio $x^n - a \in \mathbb{C}[x]$, in questo caso le radici sono note, in quanto sono le radici $n-$esime di a. Possiamo scrivere in forma polare:

$$a = \rho e^{i\theta}$$

$a \neq 0$. In questo caso si ha che:

$$\sqrt[n]{a} = \left\{ \sqrt[n]{\rho} e^{i\frac{\theta+2k\pi}{n}} \,\middle|\, k = 0,1,\dots,n-1 \right\} =$$

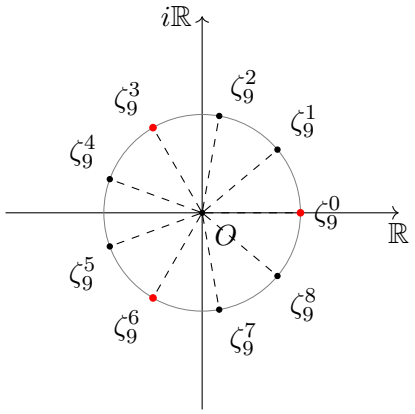
$$= \left\{ \sqrt[n]{\rho}\left(\cos\frac{\theta+2k\pi}{n} + i\sin\frac{\theta+2k\pi}{n}\right) \,\middle|\, k = 0,1,\dots,n-1 \right\}$$

Esercizio 3.27. Fattorizzare il polinomio $x^6 + x^3 + 1$ in $\mathbb{C}[x]$.

Soluzione. Osserviamo in primis che possiamo riscrivere il polinomio:

$$x^6 + x^3 + 1 = \frac{x^9 - 1}{x^3 - 1} = \frac{(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_9)}{(x-\beta_1)(x-\beta_2)(x-\beta_3)} = \frac{\prod_{i=0}^{8}(x-\zeta_9^i)}{\prod_{j=0}^{2}(x-\zeta_3^j)}$$

dove, essendo una divisione con resto nullo devono esistere n, m, k tali che: $\beta_1 = \alpha_n$, $\beta_2 = \alpha_m$, $\beta_3 = \alpha_k$. Le radici terze dell'unità possono quindi essere cancellate dalle radici none, poiché uguali, come si osserva:



pertanto si arriva all'espressione del polinomio di partenza come prodotto di polinomi di primo grado in $\mathbb{C}$:

$$x^6 + x^3 + 1 = (x - \zeta_9^1)(x - \zeta_9^2)(x - \zeta_9^4)(x - \zeta_9^5)(x - \zeta_9^7)(x - \zeta_9^8)$$

dove le radici none sono definite come $\{\zeta \in \mathbb{C} | \zeta^9 = 1\} = \langle \zeta_9 \rangle$.[43] □

§3.3.2 $\mathbb{R}[x]$

Un polinomio in $\mathbb{R}[x]$ è del tipo:

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

con $a_i \in \mathbb{R}$. Osserviamo preliminarmente che:

$$\mathbb{R} = \{z \in \mathbb{C} | z = \overline{z}\}$$

ovvero che i numeri reali sono il sottoinsieme dei complessi avente parte immaginaria nulla. Per tali numeri, come si osserva facilmente l'operazione di coniugato non ha effetto, quindi si ottiene che:

$$\overline{f(x)} = \sum_{i=0}^{n} \overline{a_i} x_i = \sum_{i=0}^{n} a_i x_i = f(x)$$

Per quanto visto nel Corollario 3.22 in $\mathbb{C}[x]$ $f(x)$ può essere completamente fattorizzato come prodotto di polinomi di primo grado:

$$f(x) = a_n(x - \alpha_1) \dots (x - \alpha_n)$$

con $\deg f(x) = n$, $\alpha_i \in \mathbb{C}$ e $a_n \in \mathbb{R}$. D'altra parte, posso considerare la fattorizzazione del coniugato del polinomio di partenza:

$$\overline{f(x)} = \overline{a_n}\overline{(x - \alpha_1)} \dots \overline{(x - \alpha_n)} = a_n(x - \overline{\alpha_1}) \dots (x - \overline{\alpha_n})$$

le due fattorizzazioni di $f(x)$ e $\overline{f(x)}$ sono vere e valide in $\mathbb{C}[x]$, ma dato che per ipotesi $f(x) \in \mathbb{R}[x]$, allora deve essere che $f(x) = \overline{f(x)}$, per il Teorema di Fattorizzazione Unica, le due scomposizioni viste devono essere la stessa cosa:

$$f(x) = \overline{f(x)} \implies (x - \alpha_1) \dots (x - \alpha_n) = (x - \overline{\alpha_1}) \dots (x - \overline{\alpha_n})$$

poiché nelle due fattorizzazioni non compaiono polinomi costanti, allora deve essere che $\forall i \in \{1, \dots, n\}$, $\exists j_i$ tale che $(x - \overline{\alpha_i}) = (x - \alpha_{j_i})$, distinguiamo due casi:

- $\underline{j_i = i}$: allora $\overline{\alpha_i} = \alpha_i$ se e solo se $\alpha_i \in \mathbb{R}$.
- $\underline{j_i \neq i}$: allora $(x - \alpha_i) \mid f(x)$ e $(x - \overline{\alpha_i}) \mid f(x)$, allora, essendo i polinomi distinti ed irriducibili in $\mathbb{C}[x]$ sono coprimi, segue che $(x - \alpha_i)(x - \overline{\alpha_i}) \mid f(x)$, in quanto $[(x - \alpha_i), (x - \overline{\alpha_i})] = (x - \alpha_i)(x - \overline{\alpha_i})$. Da ciò si ottiene che in $\mathbb{C}[x]$ si ha:

  $$f(x) = (x - \alpha_i)(x - \overline{\alpha_i})q(x)$$

  ma $(x - \alpha_i)(x - \overline{\alpha_i}) = x^2 - 2\mathrm{Re}(\alpha_i)x + |\alpha_i|^2 \in \mathbb{R}[x]$[44]. Abbiamo quindi una divisione tra polinomi a coefficienti reali, segue che $q(x) \in \mathbb{R}[x]$.

[43] Osserviamo che in questo caso abbiamo esattamente $\phi(9) = 6$ generatori, poiché $\langle \zeta_9 \rangle \cong \mathbb{Z}/9\mathbb{Z}$.

[44] Cosa che in realtà potevamo sapere più facilmente in quanto il coniugato di $(x - \alpha_i)(x - \overline{\alpha_i})$ è se stesso, pertanto è un polinomio a coefficienti reali.

Possiamo concludere che:

$$f(x) = \underbrace{(x-\alpha_1)\dots(x-\alpha_t)}_{\alpha_1,\dots,\alpha_t\in\mathbb{R}}\underbrace{[(x-\alpha_{t+1})(x-\overline{\alpha_{t+1}})]\dots[(x-\alpha_s)(x-\overline{\alpha_s})]}_{\in\mathbb{R}[x]}$$

ovvero:

Corollario 3.28

I polinomi irriducibili in $\mathbb{R}[x]$ sono quelli:

(1) di grado 1.

(2) di grado 2 con $\Delta < 0$.[a]

[a] In quanto avendo $\Delta < 0$ hanno due radici complesse coniugate.

Corollario 3.29

Ogni polinomio di $\mathbb{R}[x]$ si fattorizza in polinomi di grado 1 e di grado 2 con $\Delta < 0$.[a]

[a] Analogamente a quanto avviene in $\mathbb{C}[x]$ (Corollario 3.22), ciò segue dal corollario precedente e dal Teorema di Fattorizzazione Unica.

Esercizio 3.30. Fattorizzare x^4+1 in $\mathbb{R}[x]$.

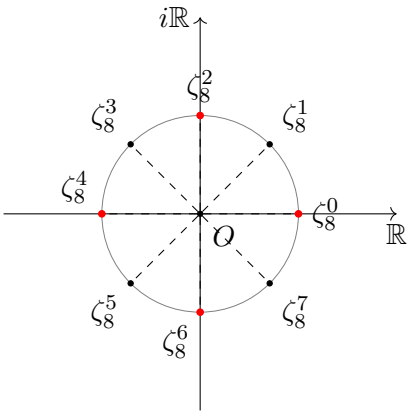
Soluzione. Possiamo procedere in due modi, il primo, osservando che:

$$x^4+1 = (x^2+1)^2 - 2x^2 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$$

che completa la fattorizzazione in quanto entrambi i polinomi a destra, avendo $\Delta < 0$, sono irriducibili in $\mathbb{R}[x]$. Alternativamente si può osservare che:

$$x^4+1 = \frac{x^8-1}{x^4-1} = \frac{\prod_{i=0}^{7}(x-\zeta_8^i)}{\prod_{j=0}^{3}(x-\zeta_4^j)}$$

e cancellando le radici quarte dell'unità, come si può osservare:



si ottiene che:

$$x^4+1 = (x-\zeta_8^1)(x-\zeta_8^3)(x-\zeta_8^5)(x-\zeta_8^7)$$

con $\zeta_8^7 = \overline{\zeta_8^1}$ e $\zeta_5 = \overline{\zeta_8^3}$, pertanto, osservando che:

$$\zeta_8^1 = \cos\left(\frac{2\pi}{8}\right) + i\sin\left(\frac{2\pi}{8}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$\zeta_8^3 = \cos\left(3\frac{2\pi}{8}\right) + i\sin\left(3\frac{2\pi}{8}\right) = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

e con qualche conto:

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

□

Osservazione 3.31 — Come si è visto, non avere radici non implica in generale l'irriducibilità in $\mathbb{R}[x]$, d'altra parte, ciò è vero per i polinomi di grado 2 (per quanto detto sulle radici complesse) e per i polinomi di grado 3, poiché in assenza di una radice non possono essere fattorizzati come prodotto di polinomi di grado 1 e 2 (e quindi poter essere ulteriormente riducibili).

§3.3.3 $\mathbb{Q}[x]$

Un polinomio in $\mathbb{Q}[x]$ è del tipo:

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

con $a_i \in \mathbb{Q}$. Osserviamo che, detto d l'm.c.m. dei denominatori, moltiplicando $f(x)$ per d, si ottiene $df(x) \in \mathbb{Z}[x]$.

Esempio 3.32
Sia:

$$f(x) = \frac{5}{4}x^2 + \frac{10}{3} \in \mathbb{Q}[x]$$

possiamo scrivere:

$$f(x) = \frac{5}{4}x^2 + \frac{10}{3} = \frac{1}{3}\left(\frac{15}{4}x^2 + 10\right) = \frac{1}{12}\left(15x^2 + 40\right) = \frac{5}{12}\left(3x^2 + 8\right)$$

Proposizione 3.33
Per ogni $f(x) \in \mathbb{Q}[x]$ esiste $\gamma \in \mathbb{Q}^*$ tale che $f(x) = \gamma f_1(x)$, con $f_1(x) \in \mathbb{Z}[x] (\subset \mathbb{Q}[x])$ e l'M.C.D. tra i coefficienti di $\gamma f_1(x)$ è 1.[a]

[a] Ovvero $f_1(x)$ primitivo.

Pertanto per ogni polinomio in $\mathbb{Q}[x]$ si può scrivere che:

$$f(x) = \gamma f_1(x) = \gamma \sum_{i=0}^{n} b_i x^i$$

con $b_i \in \mathbb{Z}$. Il problema della fattorizzazione di un polinomio in $\mathbb{Q}[x]$ si riduce quindi a quello della fattorizzazione di un polinomio in $\mathbb{Z}[x]$, in quanto, come visto, possiamo sempre ottenere un polinomio a coefficienti interi da uno a coefficienti razionali, e come vedremo nel prossimo paragrafo se tale polinomio è irriducibile in $\mathbb{Z}[x]$ lo è anche in $\mathbb{Q}[x]$.

§3.3.4 $\mathbb{Z}[x]$

Definizione 3.34. Dato un polinomio $f_1(x) \in \mathbb{Z}[x]$ si dice **contenuto** del polinomio in $\mathbb{Z}[x]$ l'M.C.D. dei suoi coefficienti:

$$c(f_1(x)) = (b_0, \dots, b_n)$$

Definizione 3.35. Dato un polinomio $f_1(x) \in \mathbb{Z}[x]$, se $c(f_1(x)) = 1$, allora il polinomio si dice **primitivo**.

Ovviamente ogni polinomio si può scrivere come:

$$f_2(x) = c(f_1(x))f_1(x)$$

Lemma 3.36 (Lemma Di Gauss)
Sia $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo, $f(x)$ è irriducibile in $\mathbb{Z}[x]$ se e solo se è irriducibile in $\mathbb{Q}[x]$.[a]

[a] Il lemma vale in qualsiasi anello a fattorizzazione unica (UFD).

Esempio 3.37
Possiamo ad esempio fattorizzare in $\mathbb{Q}[x]$:

$$(x^3 - x) = \frac{1}{2}\left(\frac{2}{7}x + \frac{2}{7}\right)(7x - 7)$$

ma posso fattorizzarlo anche in $\mathbb{Z}[x]$ per il Lemma di Gauss, essendo primitivo, possiamo riarrangiare le costanti razionali per ottenere 1 (e viceversa):

$$(x^3 - x) = x(x + 1)(x - 1)$$

A questo punto, non ci resta che esaminare l'irriducibilità dei polinomi in $\mathbb{Z}[x]$, questo problema può essere affrontato con l'utilizzo di tre tecniche: ricerca delle radici razionali, riduzione modulo un primo e criterio di Eisentein che ora vedremo in dettaglio.

Metodo Delle Radici Razionali

Teorema 3.38 (Teorema Delle Radici Razionali)
Sia $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio, allora ogni sua radice razionale è della forma α/β, con $\alpha, \beta \in \mathbb{Z}$, $(\alpha, \beta) = 1$, $\alpha \mid a_0$ e $\beta \mid a_n$.

Dimostrazione. Supponiamo che α/β sia una radice del polinomio $f(x) \in \mathbb{Z}[x]$, dobbiamo verificare che $\alpha \mid a_0$ e che $\beta \mid a_n$, osserviamo:

$$f\left(\frac{\alpha}{\beta}\right) = 0 \implies a_n\left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \ldots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 = 0$$

possiamo moltiplicare per β^n e portare l'ultimo termine a destra ottenendo:

$$a_n\alpha^n + a_{n-1}\beta\alpha^{n-1} + \ldots + a_1\beta^{n-1}\alpha = -a_0\beta^n$$

raccogliendo α al primo membro si ottiene:

$$\alpha(a_n\alpha^{n-1} + a_{n-1}\beta\alpha^{n-2} + \ldots + a_1\beta^{n-1}) = -a_0\beta^n$$

da cui, essendo per ipotesi $(\alpha, \beta) = 1$, segue la prima parte della tesi $\alpha \mid a_0$. Riprendendo la seconda espressione trovata, possiamo portare tutti i termini in β al secondo membro dell'equazione e raccogliere ottenendo:

$$-a_n\alpha^n = \beta(a_{n-1}\alpha^{n-1} + \ldots + a_1\beta^{n-2}\alpha + a_0\beta^{n-1})$$

a cui, essendo per ipotesi $(\alpha, \beta) = 1$, segue la seconda parte della tesi $\beta \mid a_n$. □

Il teorema appena visto ci permette quindi di ottenere tutte le potenziali radici razionali di $f(x)$, esse sono del tipo:

$$\left\{ \frac{\alpha}{\beta} \in \mathbb{Q} \middle| \alpha \mid a_0, \beta \mid a_n, (\alpha, \beta) = 1 \right\}$$

Osservazione 3.39 — Il teorema ci permette quindi di trovare tutte le potenziali radici razionali di un polinomio in $\mathbb{Z}[x]$, tuttavia, se nessuna di quelle determinate è una radice, allora tutte le sue radici (che esistono per il Teorema Fondamentale dell'Algebra) sono irrazionali o complesse. Al contrario, se sono state trovate esattamente $\deg f(x)$ radici razionali, allora il polinomio è completamente fattorizzabile in polinomi di primo grado irriducibili in $\mathbb{Z}[x]$ per il Teorema di Fattorizzazione Unica.

Riduzione Modulo Un Primo

Dato un primo p possiamo definire la proiezione al quoziente di polinomi come segue:

$$\pi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x] : f(x) \longmapsto \overline{f(x)}$$

dove si ha che:

$$\overline{f(x)} = \sum_{i=0}^{n} \overline{a_i} x^i$$

Come si osserva facilmente π_p è un omomorfismo di anelli, infatti $\pi_p(1) = \overline{1}$, $\pi_p(f(x) + g(x)) = \pi_p(f(x)) + \pi_p(g(x))$ e $\pi_p(f(x)g(x)) = \pi_p(f(x))\pi_p(g(x))$. Inoltre, se $p \nmid a_n$, allora $\deg(f(x)) = \deg(\pi_p(f(x)))$.

Teorema 3.40 (Irriducibilità Modulo Un Primo)
Dato un polinomio $f(x) \in \mathbb{Z}[x]$ riducibile in $\mathbb{Z}[x]$, allora per ogni primo p tale che $p \nmid a_n$, $\pi_p(f(x))$ è riducibile.

Dimostrazione. Se $f(x)$ è riducibile in $\mathbb{Z}[x]$ e $\deg(f(x)) = n$, allora si ha:

$$f(x) = g(x)h(x)$$

con $\deg(g(x)) = m$, $n > m \geq 1$, e di conseguenza $\deg(h(x)) = n - m$. Se $p \nmid a_n$, passando al quoziente modulo p il grado del polinomio si preserva, pertanto:

$$\pi_p(f(x)) = \pi_p(g(x))\pi_p(h(x))$$

con $\deg(\pi_p(f(x))) = n$, $\deg(\pi_p(g(x))) = m' \leq m$ e $\deg(\pi_p(h(x))) = d' \leq n - m$, da queste condizioni si ottiene che:

$$m' + d' \leq m + n - m \implies m' + d' \leq n$$

ma $n = m' + d'$, quindi i gradi dei due polinomi non possono ridursi (né ovviamente aumentare), pertanto $m' = m$ e $d' = n - m$, perciò $\pi_p(g(x))$ e $\pi_p(h(x))$ non sono costanti in $\mathbb{Z}/p\mathbb{Z}[x]$, dunque $\pi_p(f(x))$ è riducibile in $\mathbb{Z}/p\mathbb{Z}[x]$. □

Corollario 3.41 (Riduzione Modulo Un Primo)
Sia $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio primitivo, se esiste un primo $p \nmid a_n$ tale che $\pi_p(f(x))$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e per il Lemma di Gauss anche in $\mathbb{Q}[x]$).

Dimostrazione. Il corollario è la contronominale del Teorema 3.38. □

Osservazione 3.42 — Non è vero l'inverso del Teorema 3.38, cioè non è vero in generale che se $f(x)$ è irriducibile in $\mathbb{Z}[x]$ ($\mathbb{Q}[x]$) allora lo è anche in $\mathbb{Z}/p\mathbb{Z}[x]$. Un controesempio è $x^4 + 1$ che è irriducibile in $\mathbb{Z}[x]$, ma riducibile in $\mathbb{Z}/2\mathbb{Z}[x]$.

Esempio 3.43
Consideriamo il polinomio $x^2 + x + 1 \in \mathbb{Z}[x]$, essendo un polinomio di secondo grado, affinché sia irriducibile, è sufficiente verificare che non abbia radici, e ciò può essere fatto rapidamente per via diretta in $\mathbb{Z}/2\mathbb{Z}[x]$, infatti si ha:

$$\pi_2(x^2 + x + 1) = x^2 + x + \overline{1}$$

e si vede che né $\overline{0}$ né $\overline{1}$ sono radici del polinomio, pertanto esso è irriducibile in in $\mathbb{Z}/2\mathbb{Z}[x] \implies$ è irriducibile in $\mathbb{Z}[x]$ ($\mathbb{Q}[x]$).

Osservazione 3.44 (Polinomi Del Tipo $d_2x^2 + d_1x + d_0$) **—** Si osserva che, come appena fatto nell'esempio, si può verificare che in generale i polinomi in $\mathbb{Z}[x]$ della forma $d_2x^2 + d_1x + d_0$, con d_2, d_1, d_0 dispari e senza fattori comuni sono irriducibili in $\mathbb{Z}[x]$ ($\mathbb{Q}[x]$).

Criterio Di Eisenstein

Teorema 3.45 (Criterio Di Eisenstein)
Sia $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio primitivo e sia p un primo, se:

(i) $p \nmid a_n$.

(ii) $p \mid a_i$, $\forall i \in \{0, \ldots, n-1\}$.

(iii) $p^2 \nmid a_0$.

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ (e per il Lemma di Gauss anche in $\mathbb{Q}[x]$).

Dimostrazione. Supponiamo per assurdo che $f(x)$, con $\deg(f(x)) = n$ sia riducibile, allora:

$$f(x) = g(x)h(x)$$

con $\deg f(x) = m \geq 1$, $\deg(h(x)) = n - m \geq 1$. Possiamo applicare la proiezione al quoziente modulo p, e per le ipotesi si ha:

$$\overline{f(x)} = \overline{a_n} x^n (\neq \overline{0})$$

e inoltre:

$$\pi_p(f(x)) = \pi_p(g(x))\pi_p(h(x))$$

con:

$$\pi_p(g(x)) = \overline{b_m} x^m + \ldots + \overline{b_0} \qquad \text{e} \qquad \pi_p(h(x)) = \overline{c_{n-m}} x^{n-m} + \ldots + \overline{c_0}$$

Si ha che $\pi_p(f(x)) \in \mathbb{Z}/p\mathbb{Z}[x]$ (che è un campo), pertanto vale il Teorema di Fattorizzazione Unica, da ciò segue che $\pi_p(g(x))$ e $\pi_p(h(x))$ sono fattori del polinomio $\overline{a_n} x^n$, da cui segue, per la definizione di prodotto tra polinomi che:

$$\pi_p(g(x)) = \overline{b_m} x^m \qquad \text{e} \qquad \pi_p(h(x)) = \overline{c_{n-m}} x^{n-m}$$

ma da ciò segue che $b_0 \equiv c_0 \equiv 0 \pmod{p}$, da cui $a_0 \equiv b_0 c_0 \equiv 0 \pmod{p^2}$, ovvero $p^2 \mid a_0$, ma ciò è assurdo. □

Corollario 3.46 (Polinomi p-Eisensteiniani)
Per ogni naturale n esistono infiniti polinomi irriducibili di grado n in $\mathbb{Z}[x]$ ($\mathbb{Q}[x]$).

Dimostrazione. Per ogni n basta prendere un polinomio di p-Eisenstein, ovvero un polinomio che verifica sempre il Criterio di Eisenstein come:

$$x^n - p$$

che è irriducibile in $\mathbb{Z}[x]$ ($\mathbb{Q}[x]$), ed essendoci infiniti primi, possiamo trovare infiniti polinomi irriducibili di grado n. □

§3.4 Ideali

Definizione 3.47. Dato un anello unitario A, $I \subseteq A$ si dice **ideale** di A se:

- $I \trianglelefteq (A, +)$.
- I **assorbe** la moltiplicazione per elementi di A:

$$\forall a \in A, \forall x \in I, ax \in I$$

Se consideriamo l'insieme quoziente A/I, esso è un gruppo abeliano rispetto alla somma delle classi latrali (essendo I normale in A), infatti si ha:

$$(a + I) + (b + I) = (a + b) + I$$

inoltre, possiamo anche definire l'operazione di prodotto[45] che rende A/I un anello:

$$(a + I) \cdot (b + I) = ab + I$$

infine, se A è commutativo, anche A/I lo è, e se $1 \in A$, $1 + A$ è l'elemento neutro di A/I.

Osservazione 3.48 — Se A è abeliano e/o unitario anche A/I lo è, infatti, se A è unitario, allora esiste $(1 + I) \in A/I$, che come si verifica facilmente è l'elemento neutro. Inoltre, se A è abeliano, allora anche il prodotto di rappresentati di classi laterali di ideali lo è:

$$(a + I) \cdot (b + I) = ab + I = ba + I = (b + I) \cdot (a + I) \qquad \forall a, b \in A$$

Proposizione 3.49

Dato un anello A ed un suo ideale I, allora l'insieme quoziente tra l'anello e l'ideale è a sua volta un anello $\left(A/I, +, \cdot\right)$. [a]

[a] Commutativo se A commutativo, identitario se A identitario.

Dimostrazione. Essendo per ipotesi $I \trianglelefteq (A, +)$, segue che $\left(A/I, +\right)$ è un gruppo, ed è abeliano (in quanto A è un anello e quindi $(A, +)$ è abeliano). La chiusura per prodotto segue dalla definzione di prodotto tra classi laterali (vista sopra), mentre l'associatività del prodotto segue da quella in A:

$$\begin{aligned}((a + I)(b + I))(c + I) &= (ab + I)(c + I) = abc + I = \\ &= (a + I)(bc + I) = (a + I)((b + I)(c + I)) \qquad \forall (a + I), (b + I), (c + I) \in A/I\end{aligned}$$

infine, anche la distributività a destra e sinistra della somma rispetto al prodotto segue da quella in A:

$$(a + I) \cdot ((b + I) + (c + I)) = (a + I) \cdot ((b + c) + I) = (a(b + c) + I) = ((ab + ac) + I)$$

$$((a + I) + (b + I)) \cdot (c + I) = ((a + b) + I) \cdot (c + I) = ((a + b)c + I) = ((ac + bc) + I)$$

$\forall a, b, c \in A$. □

[45] Si verifica facilmente, tramite la proprietà di assorbimento, che tale operazione è ben definita.

Esempio 3.50
Sia $A = \mathbb{Z}$, allora $I = n\mathbb{Z}$, infatti, $mI \subseteq I$, $\forall m \in \mathbb{Z}$, o alternativamente $m \cdot n\mathbb{Z} \subseteq n\mathbb{Z}$, $\forall m \in \mathbb{Z}$.

Definizione 3.51. Dato l'anello dei polinomi a coefficienti nel campo K, $A = K[x]$, ed un suo elemento $f(x) \in K[x]$, definiamo **ideale generato** da $f(x)$:

$$(f(x)) = f(x)K[x] = \{f(x)a(x) | a(x) \in K[x]\}$$

Proposizione 3.52
Dato un anello di polinomi a coefficienti in un campo $K[x]$, ed un polinomio $f(x) \in K[x]$ irriducibile, allora l'ideale generato da $f(x)$ in $K[x]$ è un ideale.

Dimostrazione. Per dimostrare che $(f(x)) \trianglelefteq (K[x], +)$, basta osservare che $K[x]$ è un gruppo abeliano rispetto alla somma, pertanto tutti i suoi sottogruppi sono normali, quindi è sufficiente dimostrare che $(f(x)) \leqslant (K[x], +)$:

$$f(x)a(x) + f(x)b(x) = f(x)(\underbrace{a(x) + b(x)}_{\in K[x]}) \in (f(x)) \qquad \forall f(x)a(x), f(x)b(x) \in (f(x))$$

ed anche:

$$\forall a(x)f(x) \in (f(x)), \exists \underbrace{-(a(x))}_{\in K[x]} f(x) : a(x)f(x) + (-(a(x))f(x)) =$$
$$= (-(a(x))f(x)) + a(x)f(x) = 0$$

Infine, si osserva che:

$$g(x)a(x)f(x) = (g(x)a(x))f(x) \in (f(x)) \qquad \forall g(x) \in K[x], \forall a(x)f(x) \in (f(x))$$

□

Corollario 3.53
Dato un anello di polinomi a coefficienti in un campo $K[x]$ ed un polinomio del campo $f(x) \in K[x]$, allora l'insieme quoziente ottenuto dall'anello e dall'ideale generato nell'anello dal polinomio è un anello commutativo con identità $\left(\frac{K[x]}{(f(x))}, +, \cdot\right)$.

Dimostrazione. Per la Proposizione 3.52 sappiamo che $(f(x))$ è un ideale di $K[x]$, mentre per la Proposizione 3.49 sappiamo che $\frac{K[x]}{(f(x))}$ ha la struttura di anello, in particolare, poiché K è un campo, esso è un anello commutativo con unità, pertanto, come visto nell'Osservazione 3.48 segue che $\frac{K[x]}{(f(x))}$ è un anello commutativo con identità. □

Teorema 3.54

Considerato l'anello commutativo con identità $\left(\frac{K[x]}{(f(x))}, +, \cdot\right)$:

- esso è dato dai resti della divisione per $f(x)$, cioè dai polinomi $r(x)$, $\deg r(x) < \deg f(x)$[a].
- $\frac{K[x]}{(f(x))}$ è un K-spazio vettoriale, con $\dim_K \left(\frac{K[x]}{(f(x))}\right) = \deg(f(x))$ e base: $\{\overline{1}, \overline{x}, \dots, \overline{x}^{\deg f(x)-1}\}$.

[a] Che ovviamente comprendono anche il polinomio nullo nel caso in cui $f(x) \mid \overline{a(x)}$.

Dimostrazione. Per dimostrare che ogni classe $a(x) + (f(x))$ è rappresentata dal resto della divisione di $a(x)$ per $f(x)$ ci basta osservare che effettuando la divisione si ha:

$$a(x) = q(x)f(x) + r(x)$$

con $0 \leq \deg r(x) < f(x)$, da cui:

$$a(x) + (f(x)) = r(x) + q(x)f(x) + (f(x))$$

ma $q(x)f(x) \in (f(x))$ per definizione di ideale generato da $f(x)$, pertanto:

$$a(x) + (f(x)) = r(x) + (f(x))$$

Per la seconda affermazione osserviamo che:

$$\frac{K[x]}{(f(x))} = \left\{ \sum_{i=0}^{n-1} \overline{a_i x^i} + (f(x)) \middle| a_i \in K \right\}$$

ovvero, tutti gli elementi del quoziente sono le classi laterali dell'ideale generato che hanno appunto tutti i polinomi fino al grado $n-1$ come possibili rappresentati, da ciò segue che l'anello considerato è finitamente generato dall'insieme $\{\overline{1}, \overline{x}, \dots, \overline{x}^{\deg(f(x))-1}\}$ sul campo K:

$$\frac{K[x]}{(f(x))} = \left\langle \overline{1}, \overline{x}, \dots, \overline{x}^{\deg f(x)-1} \right\rangle_K$$

dove $\overline{1}, \overline{x}, \dots, \overline{x}^{\deg f(x)-1}$ sono linearmente indipendenti poiché i polinomi:

$$\sum_{i=0}^{n-1} \overline{a_i x^i}$$

sono resti di grado minore di n e quindi non possono fare $\overline{x}^n = \overline{0}$, quindi $\sum_{i=0}^{n-1} \overline{a_i x^i} = \overline{0} \iff a_i = 0, \forall i \in \{0, \dots, n-1\}$. Avendo dimostrato che $\{\overline{1}, \overline{x}, \dots, \overline{x}^{\deg f(x)-1}\}$ è una base del K-spazio vettoriale $\frac{K[x]}{(f(x))}$, segue che $\dim_K \left(\frac{K[x]}{(f(x))}\right) = \#\{\overline{1}, \overline{x}, \dots, \overline{x}^{\deg f(x)-1}\} = \deg f(x)$. □

Proposizione 3.55

Dato uno anello dei polinomi a coefficienti in un campo $K[x]$ e l'ideale generato da un polinomio dell'anello $(f(x))$, consideriamo una classe laterale dell'anello quotazione $\overline{a(x)} \in \frac{K[x]}{(f(x))}$:

(1) $\overline{a(x)}$ è invertibile se e solo se $(a(x), f(x)) = 1$.

(2) $\overline{a(x)}$ è un divisore di zero se e solo se $(a(x), f(x)) \neq 1$.

In particolare, ogni elemento dell'anello è o un divisore di zero o invertibile.[a]

[a] Poiché l'insieme $\frac{K[x]}{(f(x))}$ è finito, per quanto detto nel Teorema 3.54.

Dimostrazione. Dimostriamo le prime due tesi separatamente:

(1) Se $(a(x), f(x)) = 1$, vale il lemma di Bézout per i polinomi, ovvero $\exists \lambda(x), \mu(x) \in K[x]$ tali che:
$$a(x)\lambda(x) + f(x)\mu(x) = 1$$
o meglio, essendo i polinomi classi laterali modulo $(f(x))$:
$$\overline{a(x)}\,\overline{\lambda(x)} + \underbrace{\overline{f(x)}\,\overline{\mu(x)}}_{\in (f(x))} + (f(x)) = \overline{1} + (f(x)) \iff \overline{a(x)}\,\overline{\lambda(x)} + (f(x)) = \overline{1} + (f(x))$$
ma l'ultima uguaglianza è equivalente a $a(x)\lambda(x) \in \overline{1} + (f(x))$, che può essere riscritto anche come:
$$a(x)\lambda(x) \equiv 1 \pmod{(f(x))} \iff \overline{a(x)}\,\overline{\lambda(x)} = \overline{1}$$
dove l'ultima affermazione è equivalente al fatto che $\overline{a(x)}$ sia invertibile.

(2) Se $(a(x), f(x)) = d(x)$, con $\deg d(x) \geq 1$, allora $a(x) = a_1(x)d(x)$ e $f(x) = f_1(x)d(x)$, con $(a_1(x), f_1(x)) = 1$ e $\overline{a(x)}, \overline{f_1(x)} \neq \overline{0}$, si ha quindi che:
$$\overline{a(x)} \cdot \overline{f_1(x)} = \overline{a_1(x)}\,\underbrace{\overline{d(x)}\,\overline{f_1(x)}}_{=\overline{f(x)}=\overline{0}} = \overline{0}$$
pertanto $\overline{a(x)}$ è un divisore di zero di $\frac{K[x]}{(f(x))}$. Viceversa, se esiste $\overline{b(x)} \neq \overline{0}$ tale che $\overline{a(x)}\,\overline{b(x)} = \overline{0}$ allora $\overline{a(x)}$ non è invertibile $\implies (a(x), f(x)) \neq 1$, per quanto visto al punto precedente.

□

Osservazione 3.56 (Spazi Vettoriali) — Un gruppo abeliano $(V, +)$ si dice **spazio vettoriale** sul campo K se esiste un'appliazione:
$$K \times V \longrightarrow V : (\lambda, v) \longmapsto \lambda \cdot v$$
detta **prodotto scalare**, con le seguenti proprietà:

(i) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$, $\forall \lambda, \mu \in K$, $\forall v \in v$.

(ii) $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot$, $\forall \lambda \in K$, $\forall u, v \in v$.

(iii) $(\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v)$, $\forall \lambda, \mu \in K$, $\forall v \in V$.

(iv) $1 \cdot v = v$, $\forall v \in V$.

Osservazione 3.57 — Se A è un anello che contiene un campo K come sottoanello, con le operazioni di addizione di A come anello e l'operazione di moltiplicazione di A ristretta a $K \times A \longrightarrow A$, l'anello A è uno spazio vettoriale su K. In particolare, prendendo come anello $\frac{K[x]}{(f(x))}$, l'anello quoziente è uno spazio vettoriale sul campo K.

Corollario 3.58
$\frac{K[x]}{(f(x))}$ è un campo se e solo se $f(x)$ è irriducibile in $K[x]$.

Dimostrazione. Per dimostrare il teorema osserviamo che $\frac{K[x]}{(f(x))}$ è un campo se e solo se $\left(\frac{K[x]}{(f(x))}\right)^* = \frac{K[x]}{(f(x))} \setminus \{\overline{0}\}$, ovvero se $\forall \overline{a(x)} \in \frac{K[x]}{(f(x))}$, con $\overline{a(x)} \neq \overline{0}$, $\overline{a(x)}$ è invertibile, che per quanto visto nell'(1) del Teorema 3.54, equivale a $(a(x), f(x)) = 1$. L'ultima affermazione è equivalente al dire che:

$$(r(x), f(x)) = 1 \qquad \forall r(x) \in K[x] : \deg r(x) < \deg(x)$$

ovvero $f(x)$ non ha fattori in comune con nessun polinomio di $K[x]$ di grado minore, quindi con nessun polinimio dell'insieme $\frac{K[x]}{(f(x))}$, e ciò è equivalente al chiedere che $f(x)$ non possa essere scritto come prodtto di polinomi di grado > 0, ovvero equivale a dire che $f(x)$ è irriducibile in $K[x]$. □

Osservazione 3.59 — Si verifica facilmente che $\mathbb{Z}/p\mathbb{Z}$, con p primo, è un campo, d'ora in avanti si utilizzerà come notazione $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Esempio 3.60
Sia $K = \mathbb{F}_2$ e sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_2[x]$ di grado n. Il quoziente:

$$\frac{\mathbb{F}_2[x]}{(f(x))}$$

è un campo (ed allo stesso tempo uno spazio vettoriale di dimensione n), per quanto visto nel Teorema 3.54 gli elementi di tale campo sono rappresentabili con i polinomi di grado fino ad $n-1$ e coefficienti nell'anello $\mathbb{F}_2[x]$, pertanto il campo ha 2^n elementi, e come si vedrà è isomorfo a $\mathbb{F}_2^n$.

Esempio 3.61

Consideriamo ancora l'anello di polinomi $\mathbb{F}_2[x]$, come si verifica facilmente, poiché non ha radici, $f(x) = x^2 + x + 1$ è irriducibile, quindi il campo:

$$\frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}$$

ha esattamente 2^2 elementi, che sono $\{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$. Si osserva inoltre che:

$$\mathbb{F}_4 \cong \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}$$

Analogamente, preso $g(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ irriducibile, il campo:

$$\frac{\mathbb{F}_2[x]}{(x^3 + x + 1)}$$

ha esattamente 2^3 elementi.

§4 Estensioni Di Campi

§4.1 Estensioni ed estensioni algebriche

Definizione 4.1. Dati due campi K, F con $K \subseteq F$, F si dice **estensione** di K e si indica con:

$$F/K$$

Esempio 4.2 (Estensione Di Campi)
Vediamo alcuni esempi di estensioni di campo: $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{F}_4/\mathbb{F}_2$.

Definizione 4.3. Dato un campo K ed una sua estensione F, $\alpha \in F$ si dice **algebrico** su K se:

$$\exists f(x) \in K[x], f(x) \neq 0 : f(\alpha) = 0$$

Definizione 4.4. Dato un campo K ed una sua estensione F, $\alpha \in F$ si dice **trascendete** su K se non è algebrico, ovvero:

$$\nexists f(x) \in K[x], f(x) \neq 0 : f(\alpha) = 0$$

Esempio 4.5
Osserviamo che dato il campo $\mathbb{Q}$ e la sua estensione $\mathbb{R}$, allora $\sqrt{5} \in \mathbb{R}$ è algebrico su $\mathbb{Q}$, in quanto:

$$\exists (x^2 - 5) \in \mathbb{Q}[x] : f(\sqrt{5}) = 0$$

Viceversa, si dimostra che $\pi \in \mathbb{R}$ è trascendente su $\mathbb{Q}$[a] in quanto:

$$\nexists f(x) \in Q[x], f(x) \neq 0 : f(\pi) = 0$$

[a] Ciò è stato dimostrato nel 1882 dal matematico tedesco Ferdinand von Lindemann.

Osservazione 4.6 — Dato un polinomio a coefficienti in un campo $f(x) \in K[x] \setminus \{0\}$, se $\alpha \in F$ è algebrico su K, si ha che:

$$f(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$$

ovvero gli elementi $\{1, \alpha, \ldots, \alpha^n\}$ sono linearmente dipendenti su K, quindi ognuno di essi può essere espresso come combinazione lineare degli altri. Se invece $\alpha \in F$ è trascendete su K, si ha:

$$f(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0 \iff a_i = 0, \forall i \in \{0, \ldots, n\}, \forall f(x) \neq 0$$

ovvero gli elementi $\{1, \alpha, \ldots, \alpha^n\}$ sono linearmente indipendenti su K.

Definizione 4.7. Un'estensione F/K si dice **algebrica** se per ogni $\alpha \in F$, α è algebrico su K:

$$\forall \alpha \in F, \exists f(x) \in K[x], f(x) \neq 0 : f(\alpha) = 0$$

Esempio 4.8
$\mathbb{R}$ non è algebrico su $\mathbb{Q}$, poiché ad esempio, $\pi \in \mathbb{R}$ non è algebrico su $\mathbb{Q}$.

Definizione 4.9. Data un'estensione F/K e $\alpha \in F$, possiamo definire l'**omomorfismo di valutazione** di α su K:

$$\varphi_\alpha : K[x] \longrightarrow F : f(x) \longmapsto f(\alpha)(\in F)$$

L'immagine di tale omomorfismo è:

$$\varphi_\alpha(K[x]) = K[\alpha] = \{f(\alpha) | f(x) \in K[x]\}(\subseteq F)$$

Osservazione 4.10 — È chiaro che se K è un sottocampo di F, allora $K[x]$ è un sottoanello di $F[x]$, possiamo quindi valutare i polinomi di $K[x]$ anche negli elementi di F, in particolare, nel caso dell'omomorfismo di valutazione, è utile valutare $f(\alpha)$ in F, per non incorrere in problemi di calcolo, dovuti all'eventuale assenza di un elemento in K.

Possiamo considerare l'omomorfismo di valutazione ristretto a $K[\alpha](\subseteq F)$, tale omomorfismo per sua costruzione è surgettivo e pertanto vale il Primo Teorema Di Omomorfismo:

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi_\alpha} & K[\alpha](\subseteq F) \\ {\scriptstyle \pi_{\ker\varphi_\alpha}}\downarrow & \circlearrowleft \ \overset{\sim}{\nearrow}_{\overline{\varphi}} & \\ K[x]/_{\ker\varphi_\alpha} & & \end{array}$$

Dove appunto $\overline{\varphi}$ è un isomorfismo di anelli, in quanto, (le proprietà di omomorfismo tra gruppi sono già assicurate dal Primo Teorema Di Omomorfismo) si osserva che:

$$\overline{\varphi}(\overline{1}) = 1$$

e:

$$\overline{\varphi}(\overline{a(x)}\,\overline{b(x)}) = \overline{\varphi}(\pi(a(x))\pi(b(x))) = \overline{\varphi}(\pi(a(x)b(x))) =$$
$$= \varphi_\alpha(a(x)b(x)) = a(\alpha)b(\alpha) = \overline{\varphi}(\overline{a(x)})\overline{\varphi}(\overline{b(x)})$$

Quindi si ha che $K[x]/_{\ker\varphi_\alpha} \cong K[\alpha]$ come anelli. Si osserva poi che:

$$\ker\varphi_\alpha = \{f(x) \in K[x] | \varphi_\alpha(f(x)) = f(\alpha) = 0\}$$

ovvero, il nucleo dell'omomorfismo di valutazione (definito come la controimmagine dell'elemento neutro rispetto alla somma di $K[\alpha]$ $(\subseteq F)$), contiene tutti i polinomi che si annullano in α, ed ovviamente contiene sempre il polinomio nullo. Da quanto detto segue:

Corollario 4.11
Dato un'estensione F/K, si ha per $\alpha \in F$ che:

(1) α è trascendete su $K \iff \ker\varphi_\alpha = \{0\} \iff \varphi_\alpha$ è iniettivo $\iff K[x] \cong K[\alpha]$.[a]

(2) α è algebrico su $K \iff \ker\varphi_\alpha \neq \{0\} \iff \varphi_\alpha$ non è iniettivo.

[a] Ricordiamo che per il Primo Teorema Di Omomorfismo, scegliendo il nucleo come sottogruppo per cui quozientare si ha che $\overline{\varphi}$ è iniettivo, mentre se il nucleo è banale φ è iniettivo.

§4.2 Polinomi minimi

Sia $\mu_\alpha(x) \in \ker \varphi_\alpha$ un polinomio monico e di grado minimo tra i polinomi di $\ker \varphi_\alpha$, osserviamo che tale polinomio esiste, infatti detto:

$$S = \{\deg f(x) | f(x) \in \ker \varphi_\alpha \setminus \{0\}\} \subseteq \mathbb{N}$$

dove per quanto visto $S \neq \emptyset$ se α è algebrico su K, pertanto S ammette un minimo che chiamiamo $\deg \mu_\alpha(x)$.

Proposizione 4.12

Dato il polinomio $\mu_\alpha(x) \in \ker \varphi_\alpha$ monico e di grado minimo tra i polinomi di $\ker \varphi_\alpha$ si ha:

(1) $\mu_\alpha(x)$ è irriducibile in $K[x]$.

(2) $\ker \varphi_\alpha = (\mu_\alpha(x))$.

(3) $\mu_\alpha(x)$ è l'unico polinomio monico irriducibile nel nucleo dell'omomorfismo di valutazione che si annulla in α.

Dimostrazione. Verifichiamo le proposizioni singolarmente:

(1) Consideriamo il polinomio $\mu_\alpha(x) \in \ker \varphi_\alpha (\subseteq K[x])$ tale che $\mu_\alpha(\alpha) = 0$, se fosse che $\mu_\alpha(x) = a(x)b(x)$, con $a(x), b(x) \in K[x]$, allora:

$$0 = \mu_\alpha(\alpha) = a(\alpha)b(\alpha)$$

in $K[\alpha] (\subseteq F)$, ma per la legge di annullamento del prodotto[46] deve essere che $a(\alpha) = 0$ o $b(\alpha) = 0$ (ovvero $a(x) \in \ker \varphi_\alpha$ o $b(x) \in \ker \varphi_\alpha$), ma, $\mu_\alpha(x)$ ha grado minimo tra i polinomi di $K[x]$ che si annullano in α, ovvero (WLOG):

$$\deg a(x) \geq \deg \mu_\alpha(x)$$

poiché $\deg \mu_\alpha(x) = \deg a(x) + \deg b(x)$, l'unica possibilità è che $\deg a(x) = \deg \mu_\alpha(x)$ e $\deg b(x) = 0$ ovvero $\mu_\alpha(x)$ è irriducibile in $K[x]$.

(2) Definito l'ideale generato da $\mu_\alpha(x)$ in $K[x]$ come:

$$(\mu_\alpha(x)) = \mu_\alpha(x)K[x] = \{\mu_\alpha(x)a(x) | a(x) \in K[x]\}$$

segue che:

$$\varphi_\alpha(\mu_\alpha(x)a(x)) = \mu_\alpha(\alpha)a(\alpha) = 0$$

da cui $\mu_\alpha(x)a(x) \in \ker \varphi_\alpha$, pertanto $(\mu_\alpha(x)) \subseteq \ker \varphi_\alpha$. Sia $p(x) \in \ker \varphi_\alpha$, quindi $p(\alpha) = 0$ e $p(x) \in K[x]$, possiamo scrivere:

$$p(x) = q(x)\mu_\alpha(x) + r(x)$$

con $0 \leq \deg r(x) < \deg \mu_\alpha(x)$, segue che:

$$p(\alpha) = \underbrace{q(\alpha)\mu_\alpha(\alpha)}_{=0} + r(\alpha) = 0 \implies r(\alpha) = 0$$

$r(\alpha) = 0 \implies r(x) \in \ker \varphi_\alpha$, ma per la minimalità di $\deg \mu_\alpha(x)$ deve essere che $r(x) = 0$, da cui $\mu_\alpha(x) \mid p(x)$, da cui $p(x) \in (\mu_\alpha(x))$ e quindi $\ker \varphi_\alpha \subseteq (\mu_\alpha(x))$, ed infine la tesi $(\mu_\alpha(x)) = \ker \varphi_\alpha$.

[46] Vale poiché F è un campo e quindi un dominio di intergità.

(3) Sia $f(x) \in \ker \varphi_\alpha (\subseteq K[x])$ un polinomio monico, irriducibile, mostriamo che l'unica possibilità è che sia $f(x) = \mu_\alpha(x)$. Per quanto visto nel punto (2):

$$f(x) \in \mu_\alpha(x) \implies f(x) \in (\mu_\alpha(x)) \implies f(x) = a(x)\mu_\alpha(x)$$

se $f(x)$ è irriducibile, allora uno dei due fattori deve essere un invertibile in K, tuttavia, per il punto (1), $\mu_\alpha(x)$ è irriducibile in $K[x]$, pertanto $\deg \mu_\alpha(x) \geq 1 \implies \deg a(x) = 0$. Segue quindi:

$$f(x) = a\mu_\alpha(x)$$

ma sia $f(x)$ che $\mu_\alpha(x)$ sono per ipotesi monici, pertanto $a = 1$, segue la tesi:

$$f(x) = \mu_\alpha(x)$$

□

Abbiamo quindi dimostrato che se α è algebrico su $K[x]$ si ha che $\ker \varphi_\alpha \neq 0$ e $(\mu_\alpha(x)) = \ker \varphi_\alpha$, in particolare, l'unico polinomio monico, irriducibile in $K[x]$, e tale che $f(\alpha) = 0$, con $f(x) \in \ker \varphi_\alpha$ è $\mu_\alpha(x)$, ovvero il polinomio monico e di grado minimo in $\ker \varphi_\alpha$.

Definizione 4.13. Data un'estensione F/K e $\alpha \in F$ algebrico su K, definiamo **polinomio minimo** di α su K l'unico polinomio monico, irriducibile e che si annulla in α $(\in \ker \varphi_\alpha)$.

A questo punto sappiamo che il nucleo dell'omomorfismo di valutazione di α su $K[x]$ è proprio l'ideale generato dal polinomio minimo di α su $K[x]$.

Esempio 4.14
Presa l'estensione $\mathbb{R}/\mathbb{Q}$ e $\sqrt{5} \in \mathbb{R}$, è facile verificare che $\mu_{\sqrt{5}/\mathbb{Q}}(x) = x^2 - 5 \in \mathbb{Q}[x]$ è il polinomio minimo di $\sqrt{5}$ su $\mathbb{Q}$, infatti $\mu_{\sqrt{5}/\mathbb{Q}}(x)$ è monico, si annulla in $\sqrt{5}$, ed è irriducibile su $\mathbb{Q}[x]$, perché è esattamente un polinomio di p-Eisenstein (quindi irriducibile in $\mathbb{Z}[x]$ e per Lemma Di Gauss in $\mathbb{Q}[x]$).

Osservazione 4.15 — Per quanto appena visto $\mu_{\sqrt{5}/\mathbb{Q}}(x) = x^2 - 5 \in \mathbb{Q}[x]$ è irriducibile su quest'ultimo, quindi:

$$\frac{\mathbb{Q}[x]}{(x^2 - 5)}$$

è un campo, i cui elementi sono del tipo $\overline{f(x)} + (x^2 - 5)$, con $\deg f(x) < 2$. In particolare, per quanto visto, si ha che:

$$\begin{array}{ccc} \mathbb{Q}[x] & \xrightarrow{\varphi_\alpha} & \mathbb{Q}[\sqrt{5}] (\subseteq \mathbb{R}) \\ {\scriptstyle \pi_{\ker \varphi_{\sqrt{5}}}} \downarrow & \circlearrowleft & \nearrow_{\overline{\varphi}} \\ \mathbb{Q}[x]/(x^2 - 5) & & \end{array}$$

ovvero, l'immagine di $\mathbb{Q}[x]$ tramite l'omomorfismo di valutazione $\varphi_{\sqrt{5}}(\mathbb{Q}[x]) = \mathbb{Q}[\sqrt{5}]$ e:

$$\mathbb{Q}[\sqrt{5}] \cong \frac{\mathbb{Q}[x]}{(x^2 - 5)}$$

da cui segue che $\mathbb{Q}[\sqrt{5}]$ è un campo ed uno spazio vettoriale sul campo $\mathbb{Q}$. Ciò è vero in generale, data F/K e $\alpha \in F$ algebrico, sia $\mu_\alpha(x) \in K[x]$ il polinomio minimo di α su K, allora:

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi_\alpha} & K[\alpha](\subseteq F) \\ {\scriptstyle \pi_{(\mu_\alpha(x))}}\downarrow & \circlearrowleft & \nearrow_{\overline{\varphi}} \\ \frac{K[x]}{(\mu_\alpha(x))} & & \end{array}$$

e di nuovo:

$$K[\alpha] \cong \frac{K[x]}{(\mu_\alpha(x))}$$

con $\frac{K[x]}{(\mu_\alpha(x))}$ campo in quanto $\mu_\alpha(x)$ irriducibile su $K[x]$, e spazio vettoriale su $K[x]$, da ciò segue che $K[\alpha]$ è a sua volta un campo ed uno spazio vettoriale su K di $\dim_K(K[\alpha]) = \deg \mu_\alpha(x)$, con base $\{1, \alpha, \dots, \alpha^{\deg \mu_\alpha(x)-1}\}$.

Esempio 4.16

Consideriamo l'estensione di $\mathbb{Q}[\sqrt{5}]$ di $\mathbb{Q}$, essendo:

$$\mathbb{Q}[\sqrt{5}] \cong \frac{\mathbb{Q}[x]}{(x^2-5)}$$

si ha che $\mathbb{Q}[\sqrt{5}]$ è uno spazio vettoriale sul campo $\mathbb{Q}$ generato dalla base $\{1, \sqrt{5}\}$, pertanto gli elementi di $\mathbb{Q}[\sqrt{5}]$ hanno la seguente struttura:

$$\mathbb{Q}[\sqrt{5}] = \{a + b(1+\sqrt{5}) | a, b \in \mathbb{Q}\} = \{a + b\sqrt{5} | a, b \in \mathbb{Q}\}$$

consideriamo $1 + \sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ e vediamo che esso ammette inverso:

$$\frac{1}{1+\sqrt{5}} = -\frac{1}{4} + \frac{\sqrt{5}}{4}$$

Esempio 4.17

Consideriamo l'estensione di $\mathbb{Q}$:

$$\mathbb{Q}[\sqrt[3]{2}] \cong \frac{\mathbb{Q}[x]}{(x^3-2)}$$

esso è uno spazio vettoriali di base $\{1, \alpha, \alpha^2\}$ si ha che:

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}$$

preso $1 + 2\sqrt[3]{2} - \sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$ posso trovare l'inverso come:

$$(1 + 2\sqrt[3]{2} - \sqrt[3]{4})(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 1$$

da cui:

$$a - 2b + c + (2a + b - 8c)\sqrt[3]{2} + (a + 2b + c)\sqrt[3]{4} = 1$$

possiamo quindi determinare $a, b, c \in \mathbb{Q}$ risolvendo il sistema:

$$\begin{cases} a - 2b + c = 1 \\ 2a + b - 8c = 0 \\ a + 2b + c = 0 \end{cases}$$

che ci permette di determinare i coefficienti dell'inverso $a = \frac{17}{40}$, $b = -\frac{1}{4}$, $c = \frac{3}{40}$.

Osservazione 4.18 ($K(\alpha)$) — Consideriamo l'insieme di frazioni razionali a coefficienti in K:

$$K(x) = \left\{ \frac{f(x)}{g(x)} \middle| f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$

se α è algebrico su K, segue che $K[\alpha] = K(\alpha)$, infatti:

$$g(\alpha) \in K[\alpha] (\subseteq F), g(x) \neq 0 \implies \frac{1}{g(\alpha)} \in K[\alpha]$$

dove abbiamo sfruttato il fatto che $K[\alpha]$ sia un campo e quindi contenga l'inverso di ogni suo elemento, pertanto:

$$\forall f(\alpha) \in K[\alpha] : f(\alpha)\frac{1}{g(\alpha)} \in K[\alpha]$$

per le proprietà di chiusura del campo. Questa osservazione ci permette di usare in maniera indistinguibile le due notazioni $K[\alpha]$ e $K(\alpha)$ (entrambi sottoinsiemi di F) fintanto che α è algebrico su K.

§4.3 Estensioni semplici

Definizione 4.19. Sia F/K un'estensione di campi, definiamo **grado dell'estensione** di F/K come:

$$[F : K] = \dim_K F$$

Esempio 4.20
Abbiamo visto che se $\alpha \in F$ algebrico su K, si ha:

$$[K[\alpha] : K] = \dim_K K[\alpha] = \deg \mu_\alpha(x)$$

Definizione 4.21. Data l'estensione F/K, $\alpha \in F$ algebrico, chiamiamo l'estensione $K[\alpha]$ $(\subseteq F)$ **estensione semplice**.

Proposizione 4.22
Sia F/K un'estensione di campi, con $[F : K] < +\infty$, allora F è un'estensione algebrica di K.

Dimostrazione. Sia $[F : K] = n$ il grado dell'estensione e sia $\alpha \in F$, poiché F è un K-spazio vettoriale con $\dim_K F = n$, preso l'insieme $\{1, \alpha, \dots, \alpha^n\}$, contente $n + 1$ elementi di F. Per quanto detto[47], segue che gli elementi dell'insieme $\{1, \alpha, \dots, \alpha^n\}$ sono linearmente dipendenti, ovvero:

$$\exists a_0, \dots, a_n \in K : a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

con i coefficienti $a_0, \dots, a_n$ non tutti nulli, da quanto detto, segue (come anche già riportato nell'Osservazione 4.6) che esiste $f(x) \in K[x]$ con:

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

tale che $f(\alpha) = 0$, e questo ragionamento può essere ripetuto $\forall \alpha \in F$, pertanto F è un'estensione algebrica di K. □

Osservazione 4.23 — Abbiamo dimostrato che ogni estensione di grado finito è algebrica, il viceversa in generale è falso, quindi non ogni estensione algebrica ha grado finito.

Definizione 4.24. Date due estensioni L/F e F/K, si ha che $K \subseteq F \subseteq L$, ovvero L/K, in generale, una sequenza di estensioni prende il nome di **torre di estensioni**.

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

[47] Tralasciamo la dimostrazione di questo fatto di Algebra Lineare per brevità.

Teorema 4.25 (Teorema Dei Gradi Nelle Torri Di Estensioni)
Data una torre di estensioni $K \subseteq F \subseteq L$, con $[F : K] = n$ e $[L : F] = m$, allora $[L : K] = nm$.

$$\begin{array}{c} L \\ \Big| \, m \\ F \\ \Big| \, n \\ K \end{array} \quad nm$$

Dimostrazione. Per definizione sappiamo che $[F : K] = n$ ovvero F è un K-spazio vettoriale con $\dim_K F = n$, e ugualmente, $[L : F] = m$ ovvero L è un F-spazio vettoriale con $\dim_F L = m$, possiamo considerare allora una K-base di F, $\{v_1, \dots, v_n\}$, ed una F-base di L, $\{w_1, \dots, w_m\}$, per dimostrare la tesi, dobbiamo dimostrare che $\dim_K L = nm$, ovvero L ammette una K-base di cardinalità nm. Consideriamo l'insieme $\{v_i w_j\}_{i=1,\dots,n}^{j=1,\dots,m}$, come si osserva facilmente, esso ha cardinalità nm, dimostriamo quindi che tale insieme è una K-base di L, per fare ciò verifichiamo separatamente che gli elementi di $\{v_i w_j\}_{i=1,\dots,n}^{j=1,\dots,m}$ generano tutti gli elementi di L e che sono tra loro linearmente indipendenti:

- Sia $\alpha \in L$, poiché L è per ipotesi un F-spazio vettoriale, quindi $L = \langle w_1, \dots, w_m \rangle_F$, si ha che:
$$\alpha = \sum_{j=1}^{m} \lambda_j w_j \qquad\qquad \lambda_j \in F$$
d'altra parte, poiché F è un K-spazio vettoriale, quindi $F = \langle w_1, \dots, w_m \rangle_K$, si ha che:
$$\lambda_j = \sum_{i=1}^{n} a_{j_i} v_i \qquad\qquad a_{j_i} \in K$$
e sostituendo si ottiene:
$$\alpha = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{j_i} v_i \right) w_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{j_i} v_i w_j \qquad\qquad a_{j_i} \in K$$
e quindi l'insieme $\{v_i w_j\}_{i=1,\dots,n}^{j=1,\dots,m}$ genera L su K[48].

- Per dimostrare che l'insieme $\{v_i w_j\}_{i=1,\dots,n}^{j=1,\dots,m}$ è costituito da elementi linearmente indipendenti, è sufficiente mostrare che la somma:
$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{j_i} v_i w_j = 0$$
se e solo se sono nulli tutti i coefficienti a_{j_i}. Scriviamo esplicitamente la somma esterna:
$$\left(\sum_{i=1}^{n} a_{1_i} v_i \right) w_1 + \left(\sum_{i=1}^{n} a_{2_i} v_i \right) w_2 + \ldots + \left(\sum_{i=1}^{n} a_{m_i} v_i \right) w_m = 0$$

[48] Ovviamente tutti i prodotti $v_i w_j$ sono contenuti in L per le proprietà di campo e perché appartengono a sottocampi del campo considerato.

i prodotti $a_{j_i}v_i$, essendo $v_i \in F$ e $a_i \in K$, sono contenuti in F, pertanto, la somma appena scritta è una combinazione lineare dei w_j (della F-base di L), che sappiamo essere linearmente indipendenti su F (perché appunto sono una base di L), quindi la somma fa 0 se e solo se i coefficienti sono tutti nulli, ovvero:

$$\sum_{i=1}^{n} a_{1_i}v_i = \ldots = \sum_{i=1}^{n} a_{m_i}v_i = 0$$

essendo $\{v_1, \ldots, v_n\}$ una K-base di F, le singole somme $\sum_{i=1}^{n} a_{j_i}v_i$ sono nulle se e solo se $a_{j_i} = 0$, $\forall i \in \{1, \ldots, n\}$, quindi la somma iniziale è nulla se e solo se $a_{j_i} = 0$, $\forall i \in \{1, \ldots, n\}$, $\forall j \in \{1, \ldots, m\}$, quindi gli elementi di $\{v_i w_j\}_{i=1,\ldots,n}^{j=1,\ldots,m}$ sono linearmente indipendenti. □

Corollario 4.26
Data un'estensione F/K, con $\alpha \in F$, si ha che:

$$[K(\alpha) : K] \mid [F : K]$$

Dimostrazione. Per il teorema precedente, si può considerare la torre di estensioni $K \subseteq K(\alpha) \subseteq F$:

$$\begin{array}{c} F \\ | \\ K(\alpha) \\ | \\ K \end{array}$$

per tale torre, si ha che il grado dell'estensione F/K è dato da:

$$[F : K] = [F : K(\alpha)] \cdot [K(\alpha) : K]$$

da cui $[K(\alpha) : K] \mid [F : K]$. □

§4.4 Estensioni non semplici

Definizione 4.27. Sia F/K un'estensione, e siano $\alpha_1, \dots, \alpha_n \in F$ algebrici in K una **estensione non semplice** è:

$$K[\alpha_1, \dots, \alpha_n] = \{p(\alpha_1, \dots, \alpha_n) | p(x) \in K[x_1, \dots, x_n]\}$$

ovvero il sottoinsieme di F di tutte le valutazioni (mediante omomorfismo) degli elementi $\{\alpha_1, \dots, \alpha_n\}$ in tutti i polinomi di n ordinate ed a coefficienti nel campo K.

Proposizione 4.28
Data F/K un'estensione, e $\alpha_1, \dots, \alpha_n \in F$ algebrici, consideriamo l'estensione non semplice $K[\alpha_1, \dots, \alpha_n]$, allora:

(1) $K[\alpha_1, \dots, \alpha_n]$ è un campo.

(2) $K[\alpha_1, \dots, \alpha_n]$ è il più piccolo sottocampo di F che contiene K e $\alpha_1, \dots, \alpha_n$.

Dimostrazione. Dimostriamo i due punti della proposizione:

(1) Possiamo dimostrare questo punto per induzione su n, infatti, nel caso di $n = 1$, si ha $K[\alpha] = K(\alpha)$, che per quanto visto in precedenza è un campo. Supponiamo che $F_0 = K[\alpha_1, \dots, \alpha_{n-1}]$ sia un campo e proviamo che $K[\alpha_1, \dots, \alpha_n]$ lo è, osserviamo che $K[\alpha_1, \dots, \alpha_n]$, non è altro che la valutazione in α_n dei polinomi di $n-1$ indeterminate a coefficienti in $K[\alpha_1, \dots, \alpha_n]$:

$$K[\alpha_1, \dots, \alpha_n] = \varphi_{\alpha_n}(K[\alpha_1, \dots, \alpha_n][x]) = F_0[\alpha_n] = \{f(\alpha_n) | f(x) \in F_0[x]\}$$

dove il caso $n = 1$ ci assicura che $F_0[\alpha_n] = K[\alpha_1, \dots, \alpha_n]$ è un campo.

(2) Per dimostrare che $K[\alpha_1, \dots, \alpha_n]$ è il più piccolo sottocampo di F che contiene K e $\alpha_1, \dots, \alpha_n$, consideriamo tutti i campi M che contengono K e $\alpha_1, \dots, \alpha_n$, per dimostrare la tesi, dobbiamo provare che:[49]

$$K[\alpha_1, \dots, \alpha_n] = \bigcap_{\substack{K \subseteq M \subseteq F \\ \alpha_1, \dots, \alpha_n \in M}} M$$

Per verificare l'uguaglianza insiemistica verifichiamo la doppia inclusione, la prima è banale:

$$K[\alpha_1, \dots, \alpha_n] \supseteq \bigcap_{\substack{K \subseteq M \subseteq F \\ \alpha_1, \dots, \alpha_n \in M}} M$$

in quanto sappiamo che $K[\alpha_1, \dots, \alpha_n]$ è un sottocampo di F che contiene K e $\alpha_1, \dots, \alpha_n$ (quindi è uno dei termini considerati nell'intersezione), quindi l'intersezione è sempre contenuta in $K[\alpha_1, \dots, \alpha_n]$. Viceversa, $\forall M$, poiché M è un campo, tutte le espressioni del tipo $p(\alpha_1, \dots, \alpha_n)$, con $p(x) \in K[x_1, \dots, x_n]$ sono contenute in M (per le proprietà di chiusra del campo), ciò significa che:

$$K[\alpha_1, \dots, \alpha_n] \subseteq M, \forall M \implies K[\alpha_1, \dots, \alpha_n] \subseteq \bigcap_{\substack{K \subseteq M \subseteq F \\ \alpha_1, \dots, \alpha_n \in M}} M$$

[49] L'intersezione dei sottocampi con le proprietà richieste genera il più piccolo sottocampo (l'intersezione tra campi è un campo) che gode ancora della proprietà voluta (in questo caso contenere K e gli elementi $\alpha_1, \dots, \alpha_n$).

□

Osservazione 4.29 — Si può osservare che il grado dell'estensione $[K[\alpha,\beta]:K]$ è dato dal grado del polinomio minimo di β nel campo $K[\alpha]$ o ugualmente dal polinomio minimo di α a coefficienti nel campo $K[\beta]$:

$$[K[\alpha,\beta]:K] = \deg \underbrace{\mu_\alpha(x)}_{\in K[\beta]} = \deg \underbrace{\mu_\beta(x)}_{\in K[\alpha]}$$

Esercizio 4.30. Calcolare il polinomio minimo di $\sqrt[4]{x}$ su: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$.

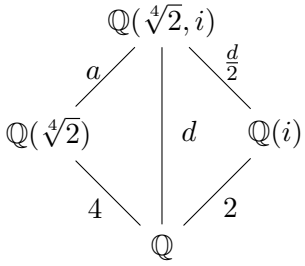
Soluzione. Vediamo caso per caso:

- In $\mathbb{R}$ si ha che $\sqrt[4]{2} \in \mathbb{R}$, pertanto si osserva facilmente che il polinomio minimo su $\mathbb{R}$ è:
$$\mu_{\sqrt[4]{2}/\mathbb{R}}(x) = x - \sqrt[4]{2}$$
che è irriducibile in $\mathbb{R}[x]$ in quanto di primo grado (come visto nella dimostrazione del Corollario 3.21 per ogni polinomio a coefficienti in un campo).

- In $\mathbb{Q}$ ovviamente si ha che $\sqrt[4]{2} \notin \mathbb{Q}$, si osserva che il polinomio $x^4 - 2$ si annulla in $\sqrt[4]{2} \in \mathbb{R}$, inoltre è irriducibile in $\mathbb{Z}[x]$ (per il Criterio Di Eisenstein) e di conseguenza lo è anche in $\mathbb{Q}[x]$ per il Lemma di Gauss, quindi:
$$\mu_{\sqrt[4]{2}/\mathbb{Q}}(x) = x^4 - 2$$

- Poiché $\mathbb{Q}(\sqrt{2})$ è un'estensione di $\mathbb{Q}$ si ha in generale che $\mu_{\alpha/\mathbb{Q}(\sqrt{2})}(x) \mid \mu_{\alpha/\mathbb{Q}}(x)$, fattorizzando $\mu_{\sqrt[4]{2}/\mathbb{Q}}(x) = x^4 - 2$ in $\mathbb{Q}(\sqrt{2})$ si ha che:
$$\mu_{\sqrt[4]{2}/\mathbb{Q}}(x) = x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$$
con $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$, quindi $x^4 - 2$ non è irriducibile in $\mathbb{Q}(\sqrt{2})$. Si osserva che $x^2 - \sqrt{2}$ è monico e si annulla in $\sqrt[4]{2}$, ma manca l'irriducibilità, tuttavia, utilizzando le estensioni semplici di $\mathbb{Q}$ (i cui gradi risultano semplici da determinare) ed il punto precedente si può studiare la torre di estensioni:
$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \ (= \mathbb{Q}(\sqrt{2})(\sqrt[4]{2})) \\ \Big(\begin{array}{c} \Big| \, m \\ \mathbb{Q}(\sqrt{2}) \\ \Big| \, 2 \end{array} \\ \mathbb{Q} \end{array} \quad 4$$
dove appunto, per il Teorema delle Torri, si ha che:
$$[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] \implies 4 = m \cdot 2$$
da cui si ricava appunto che $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})] = 2$, e quindi il polinomio minimo cercato è irriducibile se di grado 2, segue quindi:
$$\mu_{\alpha/\mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{2}$$

- Il campo $\mathbb{Q}(i)$ è un'estensione di grado 2, infatti $\mu_{i/\mathbb{Q}}(x) = x^2 + 1$, si ha quindi la seguente torre di estensioni:



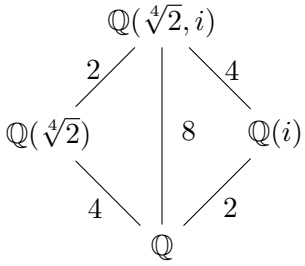
per il Teorema delle Torri, si ha che:

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}]$$

da ciò segue che $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = d/2$ e $a = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = d/4$. Si osserva che:

$$\mu_{\sqrt[4]{2}/\mathbb{Q}(i)}(x) \mid \mu_{\sqrt[4]{2}/\mathbb{Q}}(x) = x^4 - 2 \iff \deg \mu_{\sqrt[4]{2}/\mathbb{Q}(i)}(x) \leq 4$$

ma $\deg \mu_{\sqrt[4]{2}/\mathbb{Q}(i)}(x) = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = d/2$, da cui $d \leq 8$. Prima avevamo dimostrato che $4 \mid d$, pertanto, le uniche possibilità sono $d = 8$ e $d = 4$, da cui $d = 4 \iff a = 1$ e $d = 8 \iff a = 2$. In fine, si ottiene $a = 2$, in quanto $\mathbb{Q}(\sqrt[4]{2}, i) \neq \mathbb{Q}(\sqrt[4]{2})$, poiché $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, ma $i \notin \mathbb{R} \implies i \notin \mathbb{Q}(\sqrt[4]{2}) \implies a \neq 1 \implies a = 2$, da cui $d = 8$ e $d/2 = 4$. Possiamo completare la torre di estensioni:



Abbiamo quindi dimostrato che il grado dell'estensione $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)]$ è 4, quindi un polinomio di grado 4, monico in $\mathbb{Q}(i)[x]$ e che si annulli in $\sqrt[4]{2}$ è il polinomio minimo cercato, dunque, è facile vedere che:

$$\mu_{\sqrt[4]{2}/\mathbb{Q}(i)}(x) = x^4 - 2$$

□

Osservazione 4.31 — Nell'esercizio precedente abbiamo più volte usato il fatto che, data un'estensione non semplice $K \subseteq F \subseteq L$ e $\alpha \in F$ algebrico su K, si ha che:

$$\mu_{\alpha/L}(x) \mid \mu_{\alpha/K}(x)$$

ciò segue dal fatto che $\mu_{\alpha/K}(x) \in (\mu_{\alpha/L}(x))$.

§4.5 Chiusura algebrica

Definizione 4.32. Un campo L si dice **algebricamente chiuso** se ogni polinomio non costante di $L[x]$ ammette almeno una radice in L.

Osservazione 4.33 — Il Teorema Fondamentale dell'Algebra ci assicura che $\mathbb{C}$ è algebricamente chiuso.

Osservazione 4.34 — La definizione data è equivalente (come già visto in precedenza per il caso di $\mathbb{C}$) al fatto che ogni polinomio in $L[x]$ si può fattorizzare come prodotto di polinomi di grado 1. Da ciò segue anche che i polinomi irriducibili in $L[x]$ sono quelli di grado 1.

Definizione 4.35. Data un'estensione $\overline{K}/K$, $\overline{K}$ si dice **chiusura algebrica** di K se:

- $\overline{K}$ è algebricamente chiuso.
- $\overline{K}$ è algebrico (o un'estensione algebrica) su K.[50]

Esempio 4.36

Vediamo che:

(1) $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$, infatti $\mathbb{C}$ è algebricamente chiuso per il Teorema Fondamentale dell'Algebra, inoltre, $\mathbb{C}$ è algebrico su $\mathbb{R}$, infatti, l'unico elemento che $\mathbb{C}$ ha in più è i, ma per i si ha che:

$$\mu_{i/\mathbb{R}}(x) = x^2 + 1$$

da cui:

$$\mathbb{R}[i] \cong \frac{\mathbb{R}[x]}{(x^2+1)}$$

quindi $\mathbb{R}[i]$ è un campo ed un $\mathbb{R}$-spazio vettoriale di base $\{1, i\}$, da ciò segue che, posto $\mathbb{C} = \mathbb{R}[i]$, per la Proposizione 4.22 essendo l'estensione finita è anche algebrica, e quindi $\mathbb{C}$ è algebrico su $\mathbb{R}$.

(2) $\mathbb{C}$ non è la chiusura algebrica di $\mathbb{Q}$, poiché $\mathbb{C}$ non è algebrico su $\mathbb{Q}$.

Teorema 4.37 (Teorema Di Esistenza e Unicità della Chiusura Algebrica)

Ogni campo ammette una chiusura algebrica e questa è unica a meno di isomorfismo sul campo.

Date $\overline{K}$ e Ω chiusure algebriche di K, esiste ed è unico l'isomorfismo di anelli $\varphi : \overline{K} \longrightarrow \Omega$, tale che $\varphi_{|_K} = id$ (φ ristretta a K), e quindi lascia K invariato.

[50] Ricordiamo che ciò implica che tutti gli elementi di $\overline{K}$ sono algebrici su K, e quindi esiste almeno un polinomio in $K[x]$ di cui sono radici, ma, non essendo tutti gli elementi di $\overline{K}$ (che è algebricamente chiuso) anche elementi di K, non tutti i polinomi in $K[x]$ ammettono almeno una radice.

§4.6 Campi di spezzamento

Definizione 4.38. Dato un campo K e la sua chiusura algebrica $\overline{K}$, sia $f(x) \in K[x]$ un polinomio non costante, e siano $\alpha_1, \dots, \alpha_n \in \overline{K}$ le sue radici nella chiusura algebrica, si dice **campo di spezzamento** il campo $K(\alpha_1, \dots, \alpha_n)$ $(\subseteq \overline{K})$.

Osservazione 4.39 — Il campo di spezzamento di un polinomio $f(x) \in K[x]$ è quindi il più piccolo sottocampo della sua chiusura algebrica $\overline{K}$ che contiene tutte le radici di $f(x)$.

Esempio 4.40

Dato il polinomio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, trovare il suo campo di spezzamento significa trovare la più piccola estensione di $\mathbb{Q}$ che contiene tutte le sue radici nella chiusura algebrica $\overline{\mathbb{Q}}$, tali sono $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$, sia:

$$F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$$

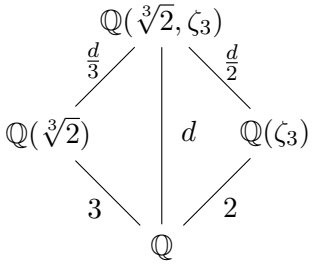
è facile verificare che $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Poiché $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ è un campo, è chiuso per prodotto e quindi contiene $\zeta_3\sqrt[3]{2}$ e $\zeta_3^2\sqrt[3]{2}$, quindi $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$; viceversa, poiché $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$ è un campo, contiene inversi e prodotti, quindi:

$$\zeta_3 = \zeta_3\sqrt[3]{2} \cdot \frac{1}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$$

da cui $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$.

Esercizio 4.41. Dato $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ estensione algebrica di $\mathbb{Q}$, dimostrare che $[F : \mathbb{Q}] = 6$.

Soluzione. Osserviamo che $\mu_{\sqrt[3]{2}(x)/\mathbb{Q}} = x^3 - 2$, che è irriducibile per Eisenstein, mentre si osserva che ζ_3 è radice del polinomio $x^2 + x + 1$, che non ha radici razionali, ed essendo di grado due è proprio il polinomio minimo di ζ_3, dunque si ha:



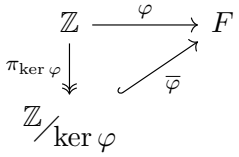
dunque si ha $6 \mid d$, inoltre, vale anche che $\mu_{\sqrt[3]{2}(x)/\mathbb{Q}(\zeta_3)} \mid \mu_{\sqrt[3]{2}(x)/\mathbb{Q}} \implies \frac{d}{2} \leq 3 \implies d \leq 6$ e quindi $d = 6$. □

§4.7 Caratteristica di un campo

Dato un campo F consideriamo l'omomorfismo di anelli:

$$\varphi : \mathbb{Z} \longrightarrow F : 1 \longmapsto 1_F : n \longmapsto \underbrace{1_F + \ldots + 1_F}_{n \text{ volte}}$$

Possiamo applicare il Primo Teorema Di Omomorfismo per fattorizzare l'omomorfismo come segue:



per quanto visto i nuclei degli omomorfismi sono tutti e soli i sottogruppi normali del gruppo di partenza, pertanto $\ker\varphi = n\mathbb{Z}$, $n \in \mathbb{Z}$, con $n \neq 1$ in quanto $\varphi(1) = 1_F \neq 0_F$, ovvero poiché la classe di 1 va nell'elemento neutro del prodotto in F, e non nell'elemento nullo, tale classe non starà nel nucleo dell'omomorfismo. Segue che o $n = 0$ oppure n è primo, in quanto, preso $n = hk$, $1 < h, k < n$, si ha che:

$$\varphi(n) = \varphi(h)\varphi(k) = 0_F$$

sarebbe quindi $\ker\varphi = n\mathbb{Z}$, ma in F vale la legge di annullamento del prodotto, quindi $\varphi(h) = 0_F$ o $\varphi(k) = 0_F$, ma ciò è assurdo, infatti, in tal caso si avrebbe h (o k) $\in n\mathbb{Z}$ ma $h, k < n$, quindi n non può essere un numero composto, ma soltanto un primo p che è divisibile soltanto per 1 (che può essere scartato in quanto $\varphi(1) = 1_F$) o per sé stesso. Segue quindi che:

$$\ker\varphi = \{0\}^{51} \qquad \text{o} \qquad \ker\varphi = p\mathbb{Z}$$

da cui:

$$\mathbb{Z}/\ker\varphi \cong \mathbb{Z} \qquad \text{o} \qquad \mathbb{Z}/\ker\varphi \cong \mathbb{Z}/p\mathbb{Z}$$

Definizione 4.42. Dato un campo K, e l'omomorfismo di anelli $\varphi : \mathbb{Z} \longrightarrow K$ definiamo **caratteristica** del campo $\operatorname{char} K$ come:

$$\operatorname{char} K = \begin{cases} 0 & \text{se } \ker\varphi = \mathbb{Z} \\ p & \text{se } \ker\varphi = p\mathbb{Z} \end{cases}$$

In altre parole la caratteristica di un campo è il minimo intero n (incluso lo 0) tale che:

$$n \cdot 1_F = 0_F$$

Osservazione 4.43 — Osserviamo che se $\operatorname{char} K = p$, allora $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$, mentre se $\operatorname{char} K = 0$, allora $\mathbb{Z} \hookrightarrow K$ e poiché K è un campo si ha che $\mathbb{Q} \hookrightarrow K$. Pertanto, i campi di caratteristica 0 sono quelli che contengono una copia isomorfa di $\mathbb{Q}$, mentre quelli di caratteristica p contengono una copia isomorfa di $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Per quanto detto segue che un campo finito ha necessariamente caratteristica p.

[51] Per essere precisi bisognerebbe considerare la classe di 0.

§5 Campi Finiti

§5.1 Definizione di campo finito

Definizione 5.1. Un campo di cardinalità finita si definisce **campo finito**.

Esempio 5.2
$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ è un campo finito, mentre $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{R}, \mathbb{C}, \mathbb{Q}(\zeta_4)$ sono campi di ordine infinito.

Osservazione 5.3 — Se F è un campo finito, quindi $|F| < +\infty$, si deve avere che $\operatorname{char} F = p$, in quanto se fosse $\operatorname{char} F = 0$, allora $\mathbb{Q} \subset F$, ma ciò è assurdo. Nel caso di $\operatorname{char} F = p$, si ha che $\mathbb{F}_p \subset F$.

Osservazione 5.4 — Se $f(x) \in \mathbb{F}_p[x]$ è irriducibile e $\deg f(x) = n$, allora:

$$F = \frac{\mathbb{F}_p[x]}{(f(x))}$$

ovvero F è un campo di caratteristica p e cardinalità p^n. Si ha quindi che $[F : \mathbb{F}_p] = \deg f(x) = n$, quindi F è un $\mathbb{F}_p$-spazio vettoriale di base $\{1, \overline{x}, \dots, \overline{x}^{n-1}\}$, ovvero gli elementi $a_0 + a_1 x + \dots + a_{n-1}$, con $a_i \in \mathbb{F}_p$, descrivono tutti gli elementi di F (una ed una sola volta, quindi ogni elemento di F ha scrittura univoca in tale rappresentazione). F come spazio vettoriale su $\mathbb{F}_p$ è isomorfo a $\mathbb{F}_p^n = (\mathbb{Z}/p\mathbb{Z})^n$ (che non è un campo, pertanto l'isomorfismo sussiste solo tra spazi vettoriali).

Esempio 5.5 (Campi non finiti di caratteristica p)
Per quanto detto, nulla ci vieta di non considerare anche campi di caratteristica p e cardinalità infinita, come ad esempio:

$$\mathbb{F}_p(x) = \left\{ \frac{f(x)}{g(x)} \middle| f(x), g(x) \in \mathbb{F}_p[x], g(x) \neq 0 \right\}$$

Osservazione 5.6 — Abbiamo visto che, dato un polinimio di grado n irriducibile in $\mathbb{F}_p[x]$, possiamo costurire un campo di p^n elementi, quindi, ad esempio, abbiamo:

$$\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}, \mathbb{F}_5$$

ma non possiamo avere $\mathbb{F}_6$, in quanto (come vedremo) non può essere ottenuto come quoziente.

Lemma 5.7 (Binomio Ingenuo)
Dato un campo K di caratteristica p, allora, per ogni x, y indeterminate, vale:

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} \qquad \forall n \in \mathbb{N}$$

Dimostrazione. Procediamo per induzione su n:

- Per $n = 1$ si ha che:
$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$$
ma si osserva che:
$$p \,\Big|\, \binom{p}{i} = \frac{p!}{i!(p-i)!} \qquad \forall i \in \{1, \dots, p-1\}$$
e quindi, in $\mathbb{F}_p$ rimangono solo i termini x^p e y^p. Si osserva infine che $p \nmid i|(p-i)!$, altrimenti si avrebbe uno 0 al denominatore.
- Assumiamo per ipotesi induttiva che il teorema sia vero per $1, \dots, n-1$ e dimostriamo che è vero per n:
$$(x+y)^{p^n} = \left((x+y)^{p^{n-1}}\right)^p = \left(x^{p^{n-1}} + y^{p^{n-1}}\right)^p = x^{p^n} + y^{p^n}$$
dove l'ultima uguaglianza segue dal caso base.

□

Osserviamo ora una proprietà fondamentale dei campi finiti:

Proposizione 5.8
Sia F un campo finito, allora $|F| = p^n$, con p primo e $n \geq 1$.

Dimostrazione. Preso F finito, allora $\operatorname{char} F = p$, ma quindi $\mathbb{F}_p \subset F$, da ciò segue che $[F : \mathbb{F}_p] = n < +\infty$, in quanto F ha soltanto un numero finito di elementi, quindi l'estensione è necessariamente algebrica (e la $\mathbb{F}_p$-base di F avrà cardinalità finita n). Ma essendo F un $\mathbb{F}_p$-spazio di dimensione n, allora è isomorfo come spazio vettoriale a $\mathbb{F}_p^n$, quindi, fissata $\{v_1, \dots, v_n\} \subset F$ come base, tutti gli elementi di F si posso esprimere come:

$$\sum a_i v_i \qquad a_i \in \mathbb{F}_p$$

e dalla base fissata segue l'isomorfismo tra spazi vettoriali:

$$F \longrightarrow \mathbb{F}_p^n : \sum a_i v_i \longmapsto (a_1, \dots, a_n)$$

da cui segue quindi che $|F| = |\mathbb{F}_p^n| = p^n$. □

Dal teorema appena dimostrato si può arrivare ad un risultato ancora più fondamentale e valido per tutte le chiusure algebriche:

Teorema 5.9

Per ogni p primo esiste ed è unico un campo con p^n elementi in ogni fissata chiusura algebrica di $\mathbb{F}_p$.

Dimostrazione. Data $\overline{\mathbb{F}_p}$ chiusra algebrica di $\mathbb{F}_p$, sia $F \subset \overline{\mathbb{F}_p}$ il campo con p^n elementi si deve avere $\mathbb{F}_p \subset F \subset \overline{\mathbb{F}_p}$, essendo F un campo si ha che $F^* = F \setminus \{0\}$, da cui $|F^*| = |F| - 1 = p^n - 1$, allora gli elementi diversi da 0 di questo campo devono essere radici del polinomio:

$$f(x) = x^{p^n-1} - 1 \in \overline{\mathbb{F}_p}[x]$$

in quanto per il (2) del Corollario 1.72, quindi:

$$\alpha^{p^n-1} = 1 \qquad \forall \alpha \in F^*$$

dunque, se il campo esiste, si ha che:

$$F \subset \{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n-1} - 1 = \alpha^{p^n} - \alpha = 0\}$$

come si osserva il polinomio $x^{p^n} - x$, di grado p^n, ha esattamente p^n radici in $\overline{\mathbb{F}_p}$, ciascuna contata con la propria molteplicità. Tuttavia il polinomio considerato non ha radici multiple, in quanto, la derivata è $f'(x) = p^n x^{p^n-1} - 1 = -1$ e da ciò segue che:

$$(f(x), -1) = 1$$

quindi il polinomio $f(x) = x^{p^n} - x$ ha esattamente p^n radici distinte in $\overline{\mathbb{F}_p}$ per il Criterio della Derivata. Da ciò segue che:

$$\#\{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n} - \alpha = 0\} = p^n$$

Quindi, l'insieme delle radici del polinomio considerato ha esattamente p^n radici in $\overline{\mathbb{F}_p}$ in quanto tutte distinte. Pertanto, o F è un campo ed è l'unico sottocampo di p^n elementi, quindi è esattamente $\{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n} - \alpha = 0\}$, o $\{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n} - \alpha = 0\}$ non ammette alcun sottocampo.
Se F non è un campo, allora $\overline{\mathbb{F}_p}$ non contiene campi di p^n elementi che quindi non esistono (in quanto, come visto, gli elementi di tale campo devono essere radici del polinomio scritto sopra, e quindi se tale insieme non è un campo non vi sono altri possibili campi con p^n elementi), mentre se F è un campo, abbiamo dimostrato come esso sia l'unico in $\overline{\mathbb{F}_p}$ con p^n elementi.[52]
Per completare la dimostrazione non ci resta altro che verificare che F sia un campo costituito da tutte la radici del polinomio $f(x) = x^{p^n} - x$ (e quindi ricadiamo nel secondo caso), per farlo ci basta osservare che deve essere $(F, +) \leqslant (\overline{\mathbb{F}_p}, +)$ e $(F^*, \cdot) \leqslant (\overline{\mathbb{F}_p}, \cdot)$:

(1) Si ha che $0, 1 \in F$, poiché $0^{p^n} = 0$ e $1^{p^n} = 1$.

(2) Presi $\alpha, \beta \in F$ si vuole dimostrare che $\alpha \pm \beta \in F$ (chiusura per somma ed inverso), quindi bisogna verificare che $(\alpha \pm \beta)^{p^n} - (\alpha \pm \beta) = 0$, ovvero $(\alpha \pm \beta)^{p^n} = (\alpha \pm \beta)$, e ciò segue dal Lemma del Binomio Ingenuo:

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta \implies \alpha + \beta \in F, \forall \alpha, \beta \in F$$

(l'ultima uguaglianza segue appunto dal fatto che α e β sono già elementi di F, e quindi $\alpha^{p^n} = \alpha$ e $\beta^{p^n} = \beta$).

[52] Abbiamo quindi supposto che un tale campo F esistesse e dedotto dalle ipotesi la sua struttura e la sua unicità, pertanto se tale insieme F è effettivamente un campo, allora vale tutto quello che abbiamo dimostrato.

(3) Presi $\alpha, \beta \in F$ deve essere che $\alpha\beta \in F$, ovvero $(\alpha\beta)^{p^n} - (\alpha\beta) = 0$, dunque $(\alpha\beta)^{p^n} = (\alpha\beta)$, poiché $\overline{\mathbb{F}_p}$ è commutativo segue:

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \implies \alpha\beta \in F, \forall \alpha, \beta \in F$$

(4) Preso $\beta \in F$, allora $\beta^{-1} \in F$, poiché $\beta \in F$ si ha:

$$\beta^{p^n} = \beta$$

considerato $(\beta)^{-1} \in \overline{\mathbb{F}_p}$, segue che:

$$(\beta^{-1})^{p^n} = \beta^{-p^n} = (\beta^{p^n})^{-1} = \beta^{-1}$$

quindi, per definizione di F, $\beta^{-1} \in F$, $\forall \beta \in F$.

□

Osservazione 5.10 — Indichiamo con $\mathbb{F}_{p^n}$ l'unico sottocampo di $\overline{\mathbb{F}_p}$ (per ogni p ed ogni n) con p^n elementi:

$$\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n} - \alpha = 0\}$$

In particolare essendo $(\mathbb{F}_p \subset)\mathbb{F}_{p^n}$ il campo avente per base (o campo generato da) le radici del polinomio $x^{p^n} - x$ (ed anche di $x^{p^n-1} - 1$, se si ricorda il fatto che lo 0 vi è sempre in $\mathbb{F}_{p^n}$ in quanto campo), esso il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$ $(x^{p^n-1} - 1)$[a].

[a] Ciò è ancora vero, perché $\mathbb{F}_{p^n}$ contiene lo 0.

§5.2 $\mathbb{F}_{p^n}$ come estensione di $\mathbb{F}_p$

Avendo dimostrato che per ogni p ed ogni n esiste un campo finito di cardinalità p^n, e che tutte le cardinatità di campi finiti sono del tipo p^n, a questo punto è lecito domandarsi se i campi del tipo:

$$\frac{\mathbb{F}_p[x]}{(f(x))}$$

con $f(x)$ irriducibile in $\mathbb{F}_p[x]$, con $\deg f(x) = n$, ovvero i campi costruiti come estensioni semplici, come visto in precedenza (aventi appunto esattamente p^n elementi), esauriscono tutti i campi, finiti, ovvero:

$$\mathbb{F}_{p^n} = \frac{\mathbb{F}_p[x]}{(f(x))} \qquad \forall p, \forall n \geq 1$$

se ciò fosse vero, l'ultimo teorema visto ci garantirebbe sempre l'esistenza di $\mathbb{F}_{p^n}$, e se appunto l'uguaglianza sopra fosse vera, ciò assicurerebbe conseguentemente l'esistenza di polinomi irriducibili di grado n in $\mathbb{F}_p[x]$, $\forall n \geq 1$, (come ad esempio accade in $\mathbb{Q}$ e $\mathbb{Z}$)[53], mentre ad esempio su $\mathbb{C}$ sono soltanto di grado 1 e su $\mathbb{R}$ di grado 1 e 2 (con $\Delta < 0$). La risposta alla domanda precedente, come vedremo, è affermativa.

Teorema 5.11 (Sottogruppo Finito Moltiplicativo Di Un Campo)
Ogni sottogruppo moltiplicativo finito di un campo è ciclico.

Dimostrazione. Sia K un campo, $G \leqslant K^*$ e $|G| = n < +\infty$, vogliamo dimostrare che G è ciclico, ovvero che ammette un elemento di ordine n. Si osserva che il polinomio:

$$f_d(x) = x^d - 1$$

per quanto visto, ha al più d radici in K, $\forall d \in \mathbb{N}$, e quindi ha al più d radici in $G(\subseteq K)$. Sia $d \mid n$, consideriamo l'insieme:

$$G_d = \{g \in G | g^d = 1\}$$[54]

segue che $|G_d| \leq d$ [55], infatti $f_d(x)$ ha al più d radici nel campo, e quindi al più d elementi che alla d fanno 1.
Diciamo $k_d = \#\{g \in G | \operatorname{ord}(g) = d\}$, se $d \nmid n$, allora $k_d = 0$ (in quanto non esistono elementi di tale ordine, per il Teorema di Lagrange), mentre se $d \mid n$, allora $k_d = 0$ oppure $k_d > 0$, ma nel secondo caso si ha che esiste almeno un elemento di ordine d, ovvero:

$$\exists g \in G : \operatorname{ord}(g) = d$$

allora si ha il sottogruppo $\langle g \rangle \leqslant G$, con $|\langle g \rangle| = d$, e tutti i suoi elementi elevati a d fanno l'identità, quindi:

$$\langle g \rangle \subseteq G_d$$

ciò significa che $|\langle g \rangle| = d \leq |G_d| \leq d \implies G_d = \langle g \rangle$, quindi se G ammette un elemento di ordine d, allora ha un unico sottogruppo di ordine d, $G_d(= \langle g \rangle)$, che è anche

[53] I polinomi Polinomi p-Eisensteiniani.
[54] Non è altro che il nucleo della mappa delle potenze d-esime di un gruppo in se stesso.
[55] Qui si fa uso dell'ipotesi di campo, nel fatto che non ci posso essere più elementi di un certo ordine rispetto all'ordine stesso (per quanto visto nel Corollario 3.20) e ciò fornisce il $\leq$ nella catena di disuguaglianze, in tal modo non vengono "sprecati elementi di un certo ordine", ad esempio in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, il polinomio $x^2 - 1$ ha tre radici, mentre ciò non può accadere in un campo per il corollario visto.

ciclico. Pertanto G o non ha elementi di ordine d, oppure sono tutti contenuti nell'unico sottogrupo ciclico G_d che li contiene, segue $k_d = \phi(d)$. Partizionando G in base all'ordine degli elementi si ha che:

$$n = |G| = \sum |G_d| = \sum_{d|n} k_d \leq \sum_{d|n} \phi(d) = n$$[56]

dove l'ultima uguaglianza è vera per il Corollario 1.39, e quindi la disuguaglianza nel mezzo è in realtà un uguaglianza:

$$\sum_{d|n} k_d = \sum_{d|n} \phi(d) = n$$

dall'uguaglianza segeue quindi che $\forall d \mid n$, $k_d = \phi(d)$, in particolare, $k_n = \phi(n) \geq 1$, quindi esiste $g \in G$ tale che $\text{ord}(g) = n \implies G$ ciclico. □

Esempio 5.12

Un esempio del teorema è già stato analizzato osservando i sottogruppi finiti di $\mathbb{C}^*$, ad esempio, se $G < \mathbb{C}^*$, con $|G| < +\infty$, allora:

$$G = \{\zeta \in \mathbb{C}^* | \zeta^n = 1\} = \langle \zeta_n \rangle = \mu_n$$

che appunto è un gruppo ciclico.

Corollario 5.13

$(\mathbb{F}_{p^n}^*, \cdot)$ è un gruppo ciclico, $\forall p$ primo, $\forall n \geq 1$.

Dimostrazione. Segue immediatamente dal Teorema 5.11, infatti $|\mathbb{F}_{p^n}^*| = p^n < +\infty$, dunque $(\mathbb{F}_{p^n}^*, \cdot) \leqslant \mathbb{F}_{p^n}$. □

Corollario 5.14

$\forall p$ primo, $\forall n \geq 1 : \mathbb{F}_{p^n}$ è un'estensione semplice di $\mathbb{F}_p$, ovvero esiste $\alpha \in \mathbb{F}_{p^n}$ tale che $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$.

Dimostrazione. Per quanto visto $\mathbb{F}_{p^n}^*$ è ciclico, quindi $\mathbb{F}_{p^n}^* = \langle \alpha \rangle$, $\alpha \in \mathbb{F}_{p^n}^*$, allora si ha che $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^n}$, ovvero si può considerare come **generatore dell'estensione**[57], un generatore del gruppo moltiplicativo $\mathbb{F}_{p^n}^*$.
Si osserva facilmente che $\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^n}$, poiché $\alpha \in \mathbb{F}_{p^n}$ e $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, viceversa, $\forall \beta \in \mathbb{F}_{p^n}$, si deve avere che $\beta \in \mathbb{F}_p[\alpha]$, se $\beta = 0$ è ovvio, se $\beta \neq 0$, allora β è invertibile $\beta \in \mathbb{F}_{p^n}^*$, ma per quanto visto è un gruppo ciclico, dunque $\beta \in \langle \alpha \rangle$, quindi $\beta = \alpha^k$, ma allora $\beta \in \mathbb{F}_p[\alpha]$, poiché in quest'ultimo, essendo un campo, ci sono tutte le potenze di α [58]. □

[56] $\leq$, poiché non sappiamo a priori se $k_d = 0$.
[57] Ovvero l'elemento che aggiungiamo al campo base per estenderlo.
[58] Si ricorda che $\mathbb{F}_{p^n}$ è un campo, quindi $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$

Osservazione 5.15 — Abbiamo visto che ogni generatore del gruppo moltiplicativo $(\mathbb{F}_p^* = \langle\alpha\rangle)$ è un generatore dell'estensione semplice $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$, il viceversa è falso, infatti, se $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$, non è detto che α generi $\mathbb{F}_p^*$.

A questo punto possiamo dare una risposta affermativa alla domanda che ci eravamo posti ad inizio paragrafo, ovvero esistono infiniti polinomi irriducibili di grado n a coefficienti in $\mathbb{F}_p$.

Corollario 5.16
$\forall p$ primo, $\forall n \geq 1 : \exists f(x) \in \mathbb{F}_p[x]$ irriducibile, con $\deg f(x) = n$.[a]

[a] E tali polinomi fissati p ed n si possono contare

Dimostrazione. Abbiamo visto che $\forall p$ primo, $\forall n \geq 1$, per quanto detto prima, si ha $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha] \cong \dfrac{\mathbb{F}_p[x]}{(\mu_\alpha(x))}$, con $\deg \mu_\alpha(x) = n$ e $\mu_\alpha(x)$ irriducibile in $\mathbb{F}_p[x]$ (essendo il polinomio minimo), poiché sappiamo che $\mathbb{F}_{p^n}$ è un'estensione semplice e $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Quindi i polinomi cercati sono tutti quelli minimi che generano le estensioni $\mathbb{F}_{p^n}$. □

Osservazione 5.17 — Consideraro $f(x) \in \mathbb{F}_p[x]$ irriducibile e di grado n, sia $\{\alpha_1, \ldots, \alpha_n\} \subset \overline{\mathbb{F}_p}$ l'insieme delle sue radici nella chiusrua algebrica di $\mathbb{F}_p$, consideriamo:

$$\mathbb{F}_p[\alpha_1] \cong \frac{\mathbb{F}_p[x]}{(f(x))}, \mathbb{F}_p[\alpha_2] \cong \frac{\mathbb{F}_p[x]}{(f(x))}, \ldots, \mathbb{F}_p[\alpha_n] \cong \frac{\mathbb{F}_p[x]}{(f(x))}$$

esse sono tutte estensioni di grado n (quindi campi con p^n elementi), in quanto si utilizzano radici del medsimo polinimio irriducibile per costruire le estensioni, quindi:

$$[\mathbb{F}_p[\alpha_i] : \mathbb{F}_p] = n \qquad \forall i \in \{1, \ldots, n\}$$

ma, per quanto visto nel Teorema 5.9 esiste ed è unico in $\overline{\mathbb{F}_p}$ un campo con p^n elementi, ma da ciò segue:

$$\mathbb{F}_p[\alpha_1] = \ldots = \mathbb{F}_p[\alpha_n]$$

e quindi, il campo di spezzamento di $f(x)$ è lo stesso per tutte le radici di un polinimio in $\mathbb{F}_p[x]$:

$$\mathbb{F}_p[\alpha_1, \ldots, \alpha_n] = \mathbb{F}_p[\alpha_i] = \mathbb{F}_{p^n} \qquad \forall i \in \{1, \ldots, n\}$$

ciò signifca che, aggiunta una sola radice del polinomio a $\mathbb{F}_p$ si ottiene direttamente il campo di spezzamento (cosa che non accade su $\mathbb{Q}$), inoltre, determinato il grado del campo di spezzamento (quindi quello di una singola estensione), si conosce il campo di spezzamento del polinomio che è sempre $\mathbb{F}_{p^n}$ (ovvero il campo delle radici del polinomio $x^{p^n} - x$).

§5.3 Sottocampi di $\mathbb{F}_{p^n}$

Osserviamo che non si può avere $\mathbb{F}_{3^2} \not\subset \mathbb{F}_{3^3}$, poiché $3 \nmid 2$, infatti vale la seguente:

Proposizione 5.18
Date due estensioni di $\mathbb{F}_p$, si ha $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ se e solo se $m \mid n$.

Dimostrazione. Proviamo le due implicazioni separatamente:

- Dimostriamo che se $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, allora $m \mid n$, per il Teorema Delle Torri si ha:

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = \underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]}_{=h}\underbrace{[\mathbb{F}_{p^m} : \mathbb{F}_p]}_{=m}$$

  da cui $n = hm \implies m \mid n$.

- Viceversa, supposto che $m \mid n$ (o anche $n = mh$, $h \in \mathbb{Z}$), proviamo che $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, o, essendo campi (quindi l'unico elemento che non è nei rispettivi gruppi moltiplicativi è lo 0), si può provare analogamente che $\mathbb{F}_{p^m}^* \subset \mathbb{F}_{p^n}^*$ (perché appunto lo 0 c'è comunque in entrambi). Si osserva che:

$$\mathbb{F}_{p^m}^* = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^m-1} = 1\} \qquad \text{e} \qquad \mathbb{F}_{p^n}^* = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^{p^n-1} = 1\}$$

  quindi, se $\alpha \in \mathbb{F}_{p^m}^*$, si deve avere (per il (2) del Corollario 1.72):

$$x^{p^m-1} = 1 \implies p^m - 1 \equiv 0 \pmod{p^m-1} \implies p^m \equiv 1 \pmod{p^m-1}$$

  da ciò, usando il fatto che $n = mh$, si ha:

$$p^n \equiv p^{mh} \equiv (p^m)^h \equiv 1^h \equiv 1 \pmod{p^m-1}$$

  da cui segue che $p^n \equiv 1 \pmod{p^m-1}$, ovvero $p^n - 1 \equiv 0 \pmod{p^m-1} \implies p^n - 1 = (p^m-1)\lambda$, $\lambda \in \mathbb{Z}$, quindi, riprendendo la relazione iniziale $\alpha^{p^m-1} = 1$ ed elevando a λ, segue $\alpha^{p^n-1} = 1$, pertanto $\alpha \in \mathbb{F}_{p^n}^*$, e quindi ogni elemento di $\mathbb{F}_{p^m}^*$ è anche elemento di $\mathbb{F}_{p^n}^*$ e ciò, unitamente al fatto che sono campi, verifica la tesi.

□

§5.4 Campi di spezzamento su $\mathbb{F}_p$

Teorema 5.19
Sia $f(x) \in \mathbb{F}_p[x]$ e sia $f(x) = f_1^{e_1}(x) \dots f_n^{e_n}$ la sua fattorizzazione in $\mathbb{F}_p[x]$, posto $\deg f_i(x) = d_i$, allora il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$, con $d = [d_1, \dots, d_r]$.

Dimostrazione. Sia $\mathbb{F}_{p^m}$ il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ (sappiamo per quanto visto che è di questo tipo, dato che è un'estesnione finita di $\mathbb{F}_p$, del tipo $\mathbb{F}_p(\gamma_1, \dots, \gamma_n)$), si vuole dimostrare che $m = d$. Sia γ_i una radice del polinomio $f_i(x)$ irriducibile su $\mathbb{F}_p[x]$, detto $d_i = \deg f_i(x)$, si ha che il campo di spezzamento di $f_i(x)$ è:

$$\mathbb{F}_p(\gamma_i) = \mathbb{F}_{p^{d_i}}$$

$\mathbb{F}_{p^m}$ è per definizione di campo di spezzamento la più piccola estensione di $\mathbb{F}_p$ che contiene tutte le radici di $f(x)$, quindi:

$$\mathbb{F}_{p^{d_i}} \subset \mathbb{F}_{p^m} \qquad \forall i \in \{1, \dots, n\}$$

da ciò (per la Proposizione 5.18) si ha che $d_i \mid m$, $\forall i \in \{1, \dots, n\}$, d'altra parte m è definito come il minimo intero tale per cui $\mathbb{F}_{p^m}$ contiene tutti gli $\mathbb{F}_{p^{d_i}}$, pertanto è proprio l'm.c.m.:

$$m = [d_1, \dots, d_n]$$

□

Osservazione 5.20 — Riguardo alla fattorizzazione dei polinomi in $\mathbb{F}_p[x]$, sappiamo che vale il criterio della derivata.

Corollario 5.21 (Polinomi irriducibili a coefficienti in $\mathbb{F}_p$)
Dato $f(x) \in \mathbb{F}_p[x]$ irriducibile, allora $f(x)$ ha radici multiple se e solo se $f'(x) = 0$.

Dimostrazione. Se $f(x)$ è irriducibile in $\mathbb{F}_p[x]$, allora non ha fattori propri, pertanto può avere solo raidci multiple, dunque se $f(x)$ ha radici multiple, allora $(f(x), f'(x)) \neq 1$ (per il Criterio Della Derivata), allora o $f(x) = 1$, ma non è possibile perché $f(x)$ ha fattori multipli, pertanto $(f(x), f'(x)) = f(x) \implies f(x) \mid f'(x)$, ma $\deg f'(x) \leq \deg f(x)$, pertanto l'unica possibilità è che $f'(x) = 0$. □

Osservazione 5.22 — Quanto detto non è vero se $\operatorname{char} K = 0$, infatti, in tal caso i polinomi irriducibili hanno radici distinte[a]. Se invece $\operatorname{char} K = p$, allora può succedere (tranne nel caso dei campi finiti), ad esempio per $K = \mathbb{F}_p(x)$, si considera l'anello dei polinomi $K[t]$ ed un suo elemento:

$$f(t) = t^p - x$$

si ha che:

$$f'(t) = pt^{p-1} = 0$$

allora $f(t)$ ha radici multiple:

$$(f(t), f'(t)) = f(t)$$

d'altra parte si verifica facilmente che $f(t)$ è irriducibile. Quindi se $\alpha \in \overline{K}$, e $f(\alpha) = 0$ da ciò segue che $\alpha^p = x$, quindi:

$$f(t) = t^p - \alpha^p = (t - \alpha)^p$$

[a] Per l'esattezza si dice che sono **separabili**.

Nei campi finiti non succede che un polinimio irriducibile abbia radici multiple, pioché vale:

Teorema 5.23
Sia $f(x) \in \mathbb{F}_p[x]$ e $f'(x) = 0$, allora $f(x) = (g(x))^p$, con $g(x) \in \mathbb{F}_p[x]$.

quindi i polinomi irriducibili non hanno mai derivata nulla, poiché quelli che la hanno sono potenze p-esime.

§5.5 Campo di spezzamento di $x^n - 1$ su $\mathbb{F}_p$

Chiamiamo $f_n(x) = x^n - 1 \in \mathbb{F}_p[x]$ il polinomio ciclotomico n-esimo a coefficienti in $\mathbb{F}_p$, sia $n = p^a m$, $m \in \mathbb{Z}$ e $(m, p) = 1$, da ciò, per il Lemma del Binomio Ingenuo, si ha che:

$$f_n(x) = x^n - 1 = x^{p^a m} - 1 = (x^m - 1)^{p^a}$$

da ciò possiamo sempre riportarci ad esponenti m con $(m, p) = 1$, quindi $p \nmid m$. Si cerca dunque di determinare il campo di spezzamento di $f_n(x)$, che per quanto detto, è uguale a quello di $f_m(x)$, sia $G_d = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^d - 1 = 0\}$ l'insieme delle radici d-esime di 1 nella chiusura algebrica del campo, allora:

Lemma 5.24
Considerato il gruppo G_n delle radici di f_n esso è uguale a quello delle radici di $f_m(x)$, $G_n = G_m$, inoltre è ciclico di ordine m.

Dimostrazione. La prima tesi segue da quanto appena detto, ovvero:

$$f_n(x) = (f_m(x))^{p^a}$$

Si osserva ora che, per quanto visto nel Teorema 5.11, essendo G_m finito e $G_m \leqslant \mathbb{F}_p^*$, allora G_m è ciclico. Infine, sappiamo che $|G_m| \leq m$ per il Corollario 3.20, e quindi ci basta dimostrare che le radici di $f_m(x)$ sono tutte distinte, per fare ciò utilizziamo il Criterio Della Derivata:

$$f'(x) = mx^{m-1} \neq 0$$

poiché $p \nmid m$, e quindi:

$$(f(x), f'(x)) = 1 \implies m \leq |G_m|$$

(dove si è osservato che $f'(x)$ ha solo 0 come radice, mentre $f(x)$ non lo ha come radice), dunque si può concludere $|G_m| = m$. □

Quindi il campo di spezzamento del polinomio $f_m(x) = x^m - 1$ è $\mathbb{F}_p[G_m]$, essendo G_m l'insieme delle radici. Come sappiamo deve essere:

$$(\mathbb{F}_p[G_n] =) \mathbb{F}_p[G_m] = \mathbb{F}_{p^k}$$

non ci resta che determinare k.

Lemma 5.25
$G_m \subset \mathbb{F}_{p^k}$ se e solo se $m \mid p^k - 1$.

Dimostrazione. Priviamo le due implicazioni:

- Dimostriamo che se $G_m \subset \mathbb{F}_{p^k}$, allora $|G_m| = m \mid p^k - 1$, ma ciò segue facilmente dal fatto che se $G_m \subset \mathbb{F}_{p^k}$, allora $G_m < \mathbb{F}_{p^k}^*$, e quindi il suo ordine divide quello del gruppo.
- Viceversa, se $m \mid p^k - 1$, allora $p^k - 1 = hm$, con $h \in \mathbb{Z}$, allora esiste $\alpha \in G_m$ tale che $g\alpha^m = 1 \implies \alpha^{p^k - 1} = \alpha^{mh} = 1^h = 1$ da cui $\alpha \in \mathbb{F}_{p^k}^*$.

□

Teorema 5.26 (Campo Di Spezzamento Di $x^n - 1$)

Dato il polinomio ciclotomico n-esimo $f_n(x) = x^n - 1 \in \mathbb{F}_p[x]$, e $n = p^a m$, con $(m, p) = 1$, il campo di spezzamento di $f_n(x)$ su $\mathbb{F}_p[x]$ è $\mathbb{F}_{p^k}$ con $k = \text{ord}_m(p)$.

Dimostrazione. Per detto nel Lemma 1 il campo di spezzamento di $x^n - 1$ è lo stesso di $x^m - 1$ ed è del tipo $\mathbb{F}_p[G_m] = \mathbb{F}_{p^k}$, d'altra parte, per il Lemma 2, sappiamo che $G_m \subset \mathbb{F}_{p^d} \iff m \mid p^d - 1$ (poiché come sappiamo, in un campo finito aggiunta una radice, vengono aggiunte anche tutte le altre al campo), k quindi è il minimo intero per il quale si ha $G_m \subset \mathbb{F}_{p^d}$:

$$k = \min\{d > 0 \text{ t.c. } m \mid p^d - 1\} = \min\{d > 0 \text{ t.c. } p^d \equiv 1 \pmod m\} = \text{ord}_m(p)$$

□

Esempio 5.27

Si vuole calcolare il campo di spezzamento di $f_7(x) = x^7 - 1$ su $\mathbb{F}_3$ e su $\mathbb{F}_{11}$. Iniziamo con $\mathbb{F}_3$, in tal caso si vuole trovare:

$$\text{ord}_7(3) = 6 \implies \mathbb{F}_{3^6}$$

il grado dell'estensione ci fornisce anche l'm.c.m. dei gradi della fattorizzazione in polinomi irriducibili di $f_7(x)$ su $\mathbb{F}_3$, infatti, essendo 6, quindi si può fattorizzare il polinimio su $\mathbb{F}_3$ come:

$$f_7(x) = x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

inoltre, il fatto che 6 sia l'm.c.m. dei gradi dei fattori irriducibili potrebbe suggeire un'altra possibile fattorizzazione del tipo $3 + 2 + 1$, ma come si osserva $f_7(x)$ non ha altre radici in $\mathbb{F}_3$, pertanto quella scritta è l'unica fattorizzazione possibile. Ugualmente in $\mathbb{F}_{11}$ basta determinare:

$$\text{ord}_7(11) = 3 \implies \mathbb{F}_{11^3}$$

dato il grado 3 le unica fattorizzazioni possibili nella forma dei gradi sono soltanto $3 + 3$ oppure $3 + 1 + 1 + 1$, ma la seconda non è possibile perché in $\mathbb{F}_{11}$ il polinomio non ha radici multiple.

Esempio 5.28

Studiare la fattorizzazione di $f_8(x) = x^8 - 1$ su $\mathbb{F}_p[x]$. Si osserva che per $p = 2$, si ha $2^3 = 8$ vale il Teorema del Binomio Ingenuo, dunque:

$$f_8(x) = x^8 - 1 = (x-1)^8$$

per $p \neq 2$, allora, per studiare la fattorizzazione si può utilizzare come visto il grado dell'estensione del campo di spezzamento su $\mathbb{F}_p$:

$$p^k \equiv 1 \pmod 8$$

ma tale congruenza ha soluzioni soltanto $k = 1, 2$ ($\mathbb{Z}/8\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), da ciò segue che i fattori irriducibili hanno grado 1 o 2, quindi:

$$f_8(x) = x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$$

da cui segue che $x^4 + 1$ è riducibile su $\mathbb{F}_p$ per ogni p. Quindi $x^4 + 1$ è irriducibile su $\mathbb{Q}$ ($\mathbb{Z}$), ma è riducibile modulo p per ogni p.

§A Complementi Sui Gruppi

§A.1 Numero di isomorfismi tra due gruppi

Esercizio A.1. Dimostrare che $\#\{f : \mathbb{Z}/18\mathbb{Z} \longrightarrow \mathbb{Z}/19\mathbb{Z}^* | f \text{ è un isomorfismo}\} = \#\{g \in \mathbb{Z}/19\mathbb{Z}^* | g \text{ è un generatore del gruppo}\}$.

Soluzione. Poiché un isomorfismo preserva gli ordini dei suoi elementi, Teorema 1.47, allora il generatore di $\mathbb{Z}/18\mathbb{Z}$ (ovvero $\overline{1}$) deve essere mandato dall'isomorfismo in $f(1)$, tale che $\text{ord}(f(1)) = 18$, ovvero ci sono 6 possibili scelte. Una volta stabilito dove mandare il generatore del gruppo, l'omomorfismo quindi f è completamente determinato, infatti, fissato $f(1)$ generatore, si ha:

$$f : \mathbb{Z}/18\mathbb{Z} \longrightarrow \mathbb{Z}/19\mathbb{Z}^* : \overline{k} \longmapsto \overline{f^k(1)}$$

dove si verifica facilmente che:

- f è un omomorfismo: infatti segue subito che, per le proprietà delle potenze si ha:

$$f(k_1 + k_2) = f^{k_1+k_2}(1) = f^{k_1}(1)f^{k_2}(1) = f(k_1) = f(k_2) \qquad \forall k_1, k_2 \in \mathbb{Z}/18\mathbb{Z}$$

- f è bigettivo: essendo gli insiemi della stessa cardinalità ci basta verificare che f è iniettivo, ovvero (per il (5) del Teorema 1.46) che il suo nucleo è banale:

$$\ker f = \{n \in \mathbb{Z}/18\mathbb{Z} | \underbrace{f(n)}_{=f^n(1)} = \overline{1}\} = \{n \in \mathbb{Z}/18\mathbb{Z} | f^n(1) \equiv 1 \pmod{19}\}$$

  dove $f(1)$ è un generatore, quindi il suo ordine moltiplicativo è 18, quindi per il Teorema Di Eulero:

$$\ker f = \{n \in \mathbb{Z}/18\mathbb{Z} | n \equiv 0 \pmod{18}\} = \{n \in \mathbb{Z}/18\mathbb{Z} | n = 18k, k \in \mathbb{Z}\} = \{\overline{0}\}$$

  quindi il nucleo è banale e l'omomorfismo bigettivo.

□

§A.2 Gruppo Abeliano

Esercizio A.2. Sia G un gruppo e sia $f : G \longrightarrow G : x \longmapsto x^2$. Dimostrare che f è un omomorfismo di gruppi se e solo se G è abeliano.

Soluzione. Per dimostrare la tesi vanno verificate entrambe le affermazioni:

- Verifichiamo che se f è un omomorfismo di gruppi, allora G è abeliano. Dall'ipotesi deve valere che:

$$f(xy) = f(x)f(y) \qquad \forall x, y \in G$$

  ovvero:

$$f(xy) = (xy)^2 = x^2y^2 \qquad \forall x, y \in G$$

  dove $(xy)^2 = xyxy$ e, applicando le leggi di cancellazione dei gruppi, segue:

$$xyxy = x^2y^2 \implies yxy = xy^2 \implies yx = xy \qquad \forall x, y \in G$$

  ovvero G è abeliano.

- Per provare che se G è abeliano, f è un omomorfismo, dobbiamo verificare che la proprietà di omomorfismo sia un'identità, ovvero:

$$f(xy) = f(x)f(y) \qquad \forall x, y \in G$$

da cui, di nuovo:

$$(xy)^2 = x^2y^2 \qquad \forall x, y \in G$$

dove, poiché G è abeliano per ipotesi, $(xy)^2 = xyxy = xxyy = x^2y^2$, $\forall x, y \in G$, che dimostra la tesi.[59]

□

Esercizio A.3. Sia G un gruppo tale per cui $g^2 = e$, $\forall g \in G$, dimostrare che G è abeliano.

Ad esempio $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oppure $\mathbb{Z}/8\mathbb{Z}^*$.

Soluzione. Possiamo considerare l'applicazione $f : G \longrightarrow G : g \longmapsto g^2 = e$, tale applicazione è un omomorfismo di gruppi, quindi, verifica l'ipotesi dell'Esercizio A.2, pertanto G è abeliano. □

§A.3 Descrizione di gruppi astratti

Proviamo a descrivere gruppi astratti in maniera puramente formale, iniziando con gruppi di ordine minore o uguale a 6.

Osservazione A.4 (Gruppo Di Ordine 1) — L'unico gruppo di ordine 1 che possiamo descrivere è $G = \{e\}$, ovvero il gruppo che contiene solo l'elemento neutro, e rispetto a cui non c'è nulla di rilevante da descrivere.

Osservazione A.5 (Gruppi Di Ordine $2, 3, 5$) — Nel caso in cui $|G| = 2, 3, 5$, sappiamo che per il Corollario 1.74 tutti i gruppi di questi ordini sono ciclici.

Proviamo a descrivere un gruppo G di ordine 4, mediante una **tavola di gruppo**. Elenchiamo in primis gli elementi del gruppo, $G = \{e, a, b, c\}$, poi studiamo il gruppo:[60]

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	a^2	ab	
b	b		b^2	
c	c			c^2

Riempite la riga e la colonna dell'elemento neutro, studiamo il prodotto $ab \in G$, esso deve essere uno dei quattro elementi $\{e, a, b, c\}$ contenuti nel gruppo, possiamo, tuttavia, subito escludere sia a che b, poiché: $ab = a \implies b = e$ e $ab = b \implies a = e$, ma ciò è assurdo.
Osserviamo che per il Teorema 1.72 l'ordine di ab deve dividere l'ordine del gruppo, pertanto abbiamo tre possibilità:

[59] La dimostrazione poteva anche essere strutturata usando direttamente delle equivalenze logiche per arrivare all'uguaglianza richiesta dalla tesi.
[60] Abbiamo scelto per convenzione di fare il prodotto colonna-riga per gli elementi.

- Se l'ordine di un elemento è 4, allora il sottogruppo generato da quell'elemento ha 4 elementi ed è proprio il gruppo $G \implies G$ ciclico, da cui $G \cong \mathbb{Z}/4\mathbb{Z}$, per il Teorema 1.51. Possiamo studiare in tal caso la nuova tavola di gruppo, supponiamo WLOG che l'elemento di ordine 4 sia a e scriviamo:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b		b^2	
c	c			c^2

  Dove $a^2 \neq e$, poiché in tal caso si avrebbe che $a = e \implies \text{ord}(a) = 2$, quindi a^2 può essere solo b o c, supponiamo sia b. A questo punto tutto è determinato, ad esempio $ab = aa^2 = a^3$, ma l'unica possibilità rimasta è che $a^3 = c$. Infine, $ac = aa^3 = a^4 = e$. Si osserva che nella riga appena scritta gli elementi compaiono una ed una sola volta[61], perché una riga contiene tutti gli elementi nella forma ax, infatti, se consideriamo l'applicazione $\varphi_a : G \longrightarrow G : x \longmapsto ax$, essa ha un'inversa $\varphi_{a^{-1}}$, quindi è una bigezione di un insieme in se stesso, pertanto è una permutazione, quindi l'immagine sarà una configurazione diversa degli stessi elementi di partenza. Ripetendo lo stesso ragionamento anche per le colonne possiamo ottenere la tavola di gruppo completa (e ricordando sempre che abbiamo posto $a^2 = b$), con le stesse regole del sudoku classico:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

- Se nessun elemento di G ha ordine 4, allora, visto che l'identità è l'unico elemento di ordine 1, tutti gli elementi di G devono avere ordine 2, da cui $a^2 = b^2 = c^2 = e$, inoltre per quanto visto nell'Esercizio A.3, il gruppo G è abeliano. Proviamo a scrivere la tavola di gruppo per questo caso, usando lo stesso procedimento del sudoku precedente:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

  Osserviamo che la tabella appena vista è quella di un gruppo abeliano di ordine 4 non ciclico, ma, noi conosciamo un altro gruppo di questo tipo e ordine che è $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(0,1),(1,0),(1,1)\}$. Proviamo a scrivere una bigezione tra i due gruppi:

$$\psi : G \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : \begin{cases} e \longmapsto (0,0) \\ a \longmapsto (1,0) \\ b \longmapsto (0,1) \\ c \longmapsto (1,1) \end{cases}$$

  Osserviamo che la tabella descrive esattamente il gruppo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

[61] Come nel gioco del Sudoku.

Abbiamo quindi visto che quindi non c'è alcun'altra possibilità per i gruppi di ordine 4, infatti o sono isomorfi a $\mathbb{Z}/4\mathbb{Z}$, oppure a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (o anche $\mathbb{Z}/8\mathbb{Z}^*$).
Proviamo ora a descrivere un gruppo G di ordine 6.

- Se G contiene un elemento di ordine 6, allora, analogamente a quanto visto sopra, per il Teorema 1.51, $G \cong \mathbb{Z}/6\mathbb{Z}$ (o anche $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).
- Se G contiene un elemento di ordine 3, allora in primis $\langle g \rangle \subseteq G$, consideriamo $h \in G \setminus \langle g \rangle$, allora per le proprietà di gruppo si deve avere che $G = \{e, g, g^2, h, hg, hg^2\}$, dove tutti gli elementi di G devono essere distinti. Infatti $hg^i \neq g^j$, altrimenti si avrebbe $h = g^{j-i}$ e quindi $h \in \langle g \rangle$, ma ciò è assurdo per ipotesi, inoltre, $hg^i \neq hg^j$, altrimenti si avrebbe $g^i = g^j$ con $i \neq j$, ma ciò è ancora assurdo. Osserviamo che risulta a questo punto semplice stabilire il risultato dei prodotti in un verso, ad esempio $hg \cdot g^2 = hg^3 = h$, ma non nel verso opposto, ad esempio $gh \neq e, g, g^2, h$, perché in ognuno di questi casi si giungerebbe ad un assurdo rispetto alle ipotesi fatte sul gruppo, ci restano hg e hg^2.
  (1) Se $gh = hg$, osserviamo preliminarmente che $h^2 \in \{e, g, g^2\}$, se $h^2 = g$, allora $h^3 = hh^2 = hg$, allora $\text{ord}(h) = 6$, pertanto G ciclico, ma ciò non è possibile per ipotesi. Analogo ragionamento per $h^2 = g^2$, quindi necessariamente $h^2 = e$. A questo punto possiamo osservare che $(gh)^2 = ghgh = g(gh)h$ per quanto supposto, quindi $(gh)^2 = g^2h^2 = g^2$, mentre $(gh)^3 = (gh)(gh)^2 = (gh)g^2h^2 = gh(gg)h^2 = g^3h^3 = eh = h$. A questo punto, per il Teorema di Lagrange abbiamo $\text{ord}(gh)||G| = 6$, ma abbiamo appena visto che $(gh)^2 = g^2$ e $(gh)^3 = h$, quindi l'ordine non è né 2 né 3, non può essere che $gh = e$ per quanto visto all'inizio, quindi $\text{ord}(gh) = 6$, ma ciò è assurdo, in quanto abbiamo supposto come ordine massimo 3 in G. Da ciò segue che $gh \neq hg$.
  (2) $gh = hg^2$ è l'unica possibilità rimasta, a questo punto possiamo scrivere la tabella del gruppo:

$\cdot$	e	g	g^2	h	hg	hg^2
e	e	g	g^2	h	hg	hg^2
g	g	g^2	e	hg^2	h	hg
g^2	g^2	e	g	hg	hg^2	h
h	h	hg	hg^2	e	g	g^2
hg	hg	hg^2	h	g^2	e	g
hg^2	hg^2	h	hg	g	g^2	e

  Abbiamo quindi visto che dato un gruppo di ordine 6, con un elemento di ordine massimo 3, la sua tavola di gruppo è fissata e coincide con quella appena vista. Un esempio di un gruppo di questo tipo è S_3. Possiamo allora cercare un isomorfismo tra S_3 ed il gruppo generico appena descritto, usando il fatto che gli isomorfismi preservano gli ordini degli elementi:

$$f : G \longrightarrow S_3 : \begin{cases} e \longmapsto id \\ g \longmapsto \sigma \\ g^2 \longmapsto \sigma^2 \\ h \longmapsto \tau \\ hg \longmapsto \tau \circ \sigma \\ hg^2 \longmapsto \tau \circ \sigma^2 \end{cases}$$

  Da qui si può verificare facilmente che f è anche un omomorfismo e che quindi è un isomorfismo.

- Se G contiene un elemento di ordine 2 come ordine massimo, allora $\forall g \in G$: $g^2 = e$, pertanto, come visto nell'Esercizio A.3, G è abeliano. Siano a, b due elementi distinti di $G \setminus \{e\}$ e consideriamo $H = \{e, a, b, ab\}$, voglio vedere se $H \leqslant G$, per verificarlo, ci basta dimostrare che è chiuso rispetto alla sua operazione, in questo caso si possono effettuare verifiche dirette, osserviamo che $a(ab) = a^2b = b$, inoltre $a^2 = b^2 = (ab)^2 = e$ [62], ci resta da valutare $b(ab) = (ab)b = a$, Pertanto H è un sottogruppo di G, privo di elementi di ordine 4, quindi si osserva facilmente che $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ma tutto ciò che abbiamo visto è assurdo poiché $4 \nmid 6$ ovvero $\#H \nmid \#G$:-).

§A.4 Classi laterali destre e sinistre

Abbiamo dimostrato nell'Esercizio 1.90 che il numero di classi laterali destre e sinistre modulo un sottogruppo è lo stesso. Vediamo ora un esempio concreto considerando come gruppo S_3, consideriamo il sottogruppo $H = \langle \tau \rangle = \langle (1,2) \rangle = \{id, \tau\}$, l'indice del sottogruppo (ovvero il numero di classi laterali), essendo S_3 finito è facilmente determinabile:

$$[S_3 : \langle \tau \rangle] = \frac{|S_3|}{|\langle \tau \rangle|} = \frac{3!}{2} = 3$$

A questo punto possiamo scrivere il gruppo quoziente delle classi laterali sinistre ${}^{S_3}\!/_{\langle \tau \rangle} = \left\{ \langle \tau \rangle, \sigma \langle \tau \rangle, \sigma^2 \langle \tau \rangle \right\}$, con:

$$\langle \tau \rangle = \{id, \tau\} = \{id, (1,2)\}$$
$$\sigma \langle \tau \rangle = \{\sigma, \sigma \circ \tau\} = \{(1,2,3), (1,3)\}$$
$$\sigma^2 \langle \tau \rangle = \{\sigma^2, \sigma^2 \circ \tau\} = \{(1,3,2), (2,3)\}$$

scriviamo le classi laterali destre partendo dal gruppo quoziente ${}^{S_3}\!/_{\langle \tau \rangle} = \left\{ \langle \tau \rangle, \langle \tau \rangle \sigma, \langle \tau \rangle \sigma^2 \right\}$, da cui:

$$\langle \tau \rangle = \{id, \tau\} = \{id, (1,2)\}$$
$$\langle \tau \rangle \sigma = \{\sigma, \tau \circ \sigma\}^{63} = \{(1,2,3), (2,3)\}$$
$$\langle \tau \rangle \sigma^2 = \{\sigma^2, \tau \circ \sigma^2\}^{64} = \{(1,3,2), (1,3)\}$$

nel cercare una bigezione tra classi laterali sinistre e destre, il nostro primo tentativo era stato provare $gH \longmapsto Hg$, in questo caso, ad esempio, avremmo avuto $\sigma \langle \tau \rangle \longmapsto \langle \tau \rangle \sigma$, ma, come si osserva che:

$$(1,3) \langle \tau \rangle \longmapsto \langle \tau \rangle (1,3)$$

dove $(1,3) \langle \tau \rangle = (1,2,3) \langle \tau \rangle$, da cui:

$$(1,2,3) \langle \tau \rangle \longmapsto \langle \tau \rangle (1,2,3)$$

ma $\langle \tau \rangle (1,2,3) = \langle \tau \rangle \sigma = \{(1,2,3), (2,3)\} \neq \{(1,2,3), (1,3)\} = \sigma \langle \tau \rangle$, quindi cambiando rappresentante abbiamo ottenuto due classi laterali diverse, pertanto il nostro tentativo di mandare $gH \longmapsto Hg$ è fallimentare a causa di un problema di buona definizione. Alternativamente, osserviamo che:

$$(1,3) \langle \tau \rangle \longmapsto \langle \tau \rangle (1,3)^{-1}$$

[62] Poiché G abeliano le verifiche sono vere in entrambi i sensi, quindi ci basta effettuarne la metà.
[63] $\tau \circ \sigma = \sigma^2 \circ \tau$.
[64] $\tau \circ \sigma^2 = \sigma \circ \tau$.

ma $(1,3)^{-1} = (1,3)$, d'altra parte $(1,3)\langle\tau\rangle = (1,2,3)\langle\tau\rangle$, e $(1,2,3)^{-1} = (1,3,2)$[65], pertanto data la corrispondenza:

$$(1,3)\langle\tau\rangle \longmapsto \langle\tau\rangle(1,3)^{-1} = \langle\tau\rangle(1,3)$$

come prima, $(1,2,3)\langle\tau\rangle = (1,3)\langle\tau\rangle$, da cui:

$$(1,2,3)\langle\tau\rangle \longmapsto \langle\tau\rangle(1,2,3)^{-1} = \langle\tau\rangle(1,3,2)$$

con $\langle\tau\rangle(1,3,2) = \langle\tau\rangle(1,3)$, ovvero, cambiando rappresentante abbiamo ottenuto la stessa classe in arrivo, pertanto la funzione è ben definita. Da qui si prosegue con la dimostrazione vista nell'Esercizio 1.90.

§A.5 Ordini degli elementi nel prodotto di gruppi

Esercizio A.6. Dato il gruppo $G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, contare gli elementi $(a,b,c) \in G$ di ordine 12.

Soluzione. Osserviamo in primis, come visto nel punto (3) del Teorema 1.57, per $g \in G$, $g = (a,b,c)$, si ha:

$$\mathrm{ord}(g) = [\mathrm{ord}_8(a), \mathrm{ord}_4(b), \mathrm{ord}_3(c)]$$

I possibili valori per ogni ordine sono dati dai divisori dell'ordine del gruppo, pertanto: $\mathrm{ord}_8(a) \in div(8) = \{1,2,4,8\}$, $\mathrm{ord}_4(b) \in div(4) = \{1,2,4\}, \mathrm{ord}_3(c) \in div(3) = \{1,3\}$. Affinché $\mathrm{ord}(g) = 12 = 2^2 \cdot 3$, deve essere necessariamente che $\mathrm{ord}_3(c) = 3$, pertanto $\mathrm{ord}_3(c)$ è fissato, e per tale ordine, sappiamo dal punto (3) del Corollario 1.38 che ci sono $\phi(3) = 2$ elementi di ordine 3 in $\mathbb{Z}/3\mathbb{Z}$ (ovvero due scelte per c), quindi ci resta da contare per quante coppie $(a,b) \in \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ si ha:

$$[\mathrm{ord}_8(a), \mathrm{ord}_4(b)] = 4$$

In questo caso è necessario che l'ordine di uno dei due sia sempre 4, inoltre, a non può mai avere ordine 8 in tali condizioni. Per effettuare il conteggio possiamo contare il numero di coppie il cui ordine divide 4 e sottrarre da questo il numero delle coppie il cui ordine divide 2 (ottenendo in tal modo esattamente le coppie il cui ordine è 4), quindi vogliamo eseguire il seguente conteggio:

$$\#\{g \in G \mid \mathrm{ord}(g) | 4\} - \#\{g \in G \mid \mathrm{ord}(g) | 2\}$$

osserviamo che $\mathrm{ord}(g) = [\mathrm{ord}_8(a), \mathrm{ord}_4(b)] \mid 4$, e ciò si ottiene in base alle proprietà dell'm.c.m., quando $\mathrm{ord}_8(a) \mid 4 \wedge \mathrm{ord}_4(b) \mid 4$, ovvero se e solo contemporaneamente (ricordando il (2) del Teorema 1.27) $a^4 = 4a \equiv 0 \pmod 8$ e $b^4 = 4b \equiv 0 \pmod 4$, il numero di soluzioni di ciascuna congruenza rappresenta il numero di elementi con la proprietà richiesta, oltretutto, le congruenze sono separate ed indipendenti, pertanto il numero di coppie con la proprietà richiesta sarà dato proprio dal prodotto del numero di soluzioni di entrambe. Osservando la prima si vede:

$$4a \equiv 0 \pmod 8 \implies a \equiv 0 \left(\mathrm{mod}\ \frac{8}{(4,8)}\right) \implies a \equiv 0 \pmod 2$$

quindi $a = 2k$, $k \in \mathbb{Z}$, e $a \in \mathbb{Z}/8\mathbb{Z}$ ovvero $0 \leq a < 8 \implies 0 \leq 2k < 8 \implies 0 \leq k < 4$, pertanto ci sono 4 soluzioni possibili (le classi di resto pari minori di 8). Analogamente si

[65] Poiché $\sigma \circ \sigma^2 = id$, allora $\sigma^{-1} = \sigma^2$.

trova che ci sono 4 scelte possibili per b (tutte le classi di resto vanno modulo 4 vanno bene). D'altronde le soluzioni richieste nel primo caso sono esattamente $\frac{8}{8/4} = 4$, ciò è vero in generale quando ci si domanda quante sono le soluzioni di $ax \equiv 0 \pmod{n}$ con $a \mid n$, infatti si ha che il numero richiesto è dato da $\frac{n}{x} = \frac{n}{n/d} = d$, questo fatto è vero in generale per tutti i gruppi ciclici[66]. Quindi dato un gruppo ciclico G, si ha che:

$$\#\{g \in G \mid \text{ord}(g) \mid d\} = d \qquad \text{per} \quad d \mid n$$

Alternativamente si può pensare che gli elementi il cui ordine divide d è dato da:

$$\sum_{e \mid d} \#\{g \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}(g) = e\}$$

ovvero, invece di metterli assieme, sommo il numero di elementi per ogni divisore dell'ordine, ma, ricordando il (3) del Teorema 1.38, sappiamo che il numero di elementi aventi ordine e è dato da $\phi(e)$, pertanto, ricordando anche il Corollario 1.39 si vede che:

$$\sum_{e \mid d} \#\{g \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}(g) = e\} = \sum_{e \mid d} \phi(e) = d$$

che conferma ancora il risultato precedente. A questo punto, ragionando in maniera analoga per contare gli elementi di $\{g \in G \mid \text{ord}(g) | 2\}$, quindi, $\text{ord}(g) | 2 \implies [\text{ord}_8(a), \text{ord}_4(b)] \mid 2 \implies \text{ord}_8(a) \mid 2 \wedge \text{ord}_4(b) \mid 2$, da cui ci basta contare il numero di classi soluzione per ciascuna congruenza e poi moltiplicare, ad esempio, nel primo caso si ha che $2a \equiv 0 \pmod{8}$ e per quanto appena visto abbiamo esattamente 2 classi di resto soluzione, analogamente per b. Possiamo quindi scrivere il conto finale:

$$4 \cdot 4 - 2 \cdot 2 = 12$$

e ciò conclude il problema. □

§A.6 Teorema Di Cauchy per $p = 2$

Teorema A.7 (Teorema Di Cauchy per $p = 2$)
Sia G un gruppo finito, con $|G|$ pari, allora esiste $g \in G$ tale che $\text{ord}(g) = 2$.

Dimostrazione. Un elemento di ordine 2 è tale per cui $g^2 = e$, con $g \neq e$, quindi $g = g^{-1}$. Definiamo la seguente relazione di equivalenza[67] $\sim$ in G:

$$g \sim h \iff g = h \quad \text{o} \quad g = h^{-1}$$

Possiamo considerare la partizione indotta su G da $\sim$, che accoppia gli elementi di G se sono uguali o se sono l'uno l'inverso dell'altro, le classi di equivalenza saranno quindi di due tipi: o la classe contiene un elemento ed il suo inverso, oppure contiene solo un elemento (in questo caso $g = h$, pertanto l'elemento coincide con il suo inverso), quindi abbiamo l'insieme quoziente:

$$G/\sim = \{\{e\}, \{g_1, g_1^{-1}\}, \dots, \{g_k, g_k^{-1}\}, \{h_1\}, \dots, \{h_s\}\}$$

[66] D'altra parte esiste sempre un isomorfismo con $\mathbb{Z}/n\mathbb{Z}$.
[67] Si può verificare facilmente in maniera diretta che tale relazione è di equivalenza.

da ciò, essendo G l'unione disgiunta di tutte le sue classi di equivalenza, possiamo osservare che:

$$|G| = 1 + 2k + s$$

ma $|G|$ è pari, quindi $|G| \equiv 0 \pmod 2 \implies |G| \equiv 1+2k+s \equiv 1+s \equiv 0 \pmod 2 \implies s$ dispari $\implies s \geq 1$[68], quindi c'è un numero positivo di elementi di ordine 2 (gli elementi h_i) che è la tesi.[69] □

§A.7 Sottogruppi dei gruppi finiti

Corollario A.8 (Sottogruppi di gruppi finiti)
Sia $(G, \cdot)$ un gruppo di ordine finito e $H \subseteq G$, con H chiuso rispetto all'operazione $\cdot_H$ indotta da G su H, allora $H \leqslant G$.

Dimostrazione. Per dimostrare il teorema ci basta far vedere che dalle ipotesi seguono le condizioni necessarie alla verifica del Teorema 1.12, ovvero ci basta verificare che ogni elemento di H ha inverso rispetto all'operazione $\cdot_H$ nell'insieme stesso. Visto che per ipotesi H è chiuso per l'operazione $\cdot_H$, e detto $|H| = n$, possiamo scrivere le potenze di H:

$$e, h, h^2, \dots, h^{n-1}, \underbrace{h^n}_{=e}$$

dove $h^n = e$ per il Corollario 1.72, quindi, usando le proprietà delle potenze segue che $h \cdot h^{n-1} = h^{n-1} \cdot h = e$, $\forall h \in H$, quindi per ogni elemento di H si può costruire un inverso come appena visto, pertanto il corollario è verificato. □

Osservazione A.9 ($\mathbb{N}$ e $\mathbb{Z}$) — L'ipotesi di finitezza richiesta nel corollario precedente è necessaria, ad esempio, per $G = \mathbb{Z}$ e $H = \mathbb{N}$, abbiamo un controesempio, infatti $\mathbb{N}$ è chiuso rispetto al $+$, ma non è un gruppo rispetto a quest'ultimo.

§A.8 Omomorfismi tra gruppi ciclici

Consideriamo prima due gruppi ciclici finiti, ad esempio $G_1 = \mathbb{Z}/m\mathbb{Z}$ e $G_2 = \mathbb{Z}/n\mathbb{Z}$ e studiamo l'insieme:

$$\mathrm{Hom}(G_1, G_2) = \{f : G_1 \longrightarrow G_2 | f \text{ omomorfismo}\}$$

Osservazione A.10 — Se $\varphi : G_1 \longrightarrow H$ è un omomorfismo, allora:

$$\varphi(\overline{1}) = h \implies \varphi(\overline{2}) = \varphi(\overline{1} + \overline{1}) = \varphi(\overline{1})\varphi(\overline{1}) = h^2$$

da cui:

$$\varphi(\overline{k}) = h^k$$ [a]

pertanto φ è completamente determinato da $\varphi(\overline{1})$.

[a] È la stessa cosa che osservare come in un omomorfismo valga: $f(x^n) = f^n(x)$.

[68] Ovviamente i numeri dispari non possono contenere 0
[69] In altre parole abbiamo dimostrato che G contiene necessariamente almeno un elemento di ordine 2.

L'osservazione appena fatta ci permette di dire che $\#\mathrm{Hom}(G_1, G_2) \leq n$, infatti, una volta determinata l'immagine del generatore tutte le altre immagini sono date, pertanto (anche in generale per un secondo gruppo finito non ciclico qualsiasi), il numero massimo possibile di omomorfismi sicuramnte non potrà superare l'ordine del gruppo di arrivo (e quindi il numero di scelte per l'immagine del generatore).

Osservazione A.11 (Omomorfismo all'elemento neutro) — Dati due gruppi G, H, l'applicazione $\varphi : G \longrightarrow H : g \longmapsto e_H$, $\forall g \in G$, che manda tutti gli elemento di G nell'elemento neutro di H è un omomorfismo, infatti;

$$\underbrace{\varphi(h+k)}_{=e_H} = \underbrace{\varphi(h)}_{=e_H}\underbrace{\varphi(k)}_{=e_H} \qquad \forall h, k \in G$$

Esempio A.12 (Caso $m = 3$, $n = 2$)

Proviamo a costruire l'omomorfismo $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, in tal caso, abbiamo solo due possibilità per mandare il generatore del gruppo di partenza ($[1]_3$) nel gruppo di arrivo. Nel primo caso proviamo a porre:

$$\varphi(\overline{1}) = \overline{1}$$

in tal caso, si avrebbe che:

$$\varphi(\overline{0}) = \varphi(\overline{1}+\overline{1}+\overline{1}) = \varphi(\overline{1}) + \varphi(\overline{1}) + \varphi(\overline{1}) = \overline{1}$$

ma $\mathrm{ord}_3(\overline{0}) = 1$, mentre $\mathrm{ord}_2(\overline{1}) = 2$, ma per il Teorema 1.47, ciò è assurdo poiché $\mathrm{ord}(f(x)) \nmid \mathrm{ord}(x) (2 \nmid 1)$, pertanto un tale omomorfismo non può esistere. Ponendo invece:

$$\varphi(\overline{1}) = \overline{0}$$

allora $\varphi(\overline{k}) = \overline{0}$, $\forall \overline{k} \in \mathbb{Z}/3\mathbb{Z}$, che è un omomorfismo come appena visto. Pertanto esiste un solo omomorfismo tra $\mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z}$.

A questo punto, possiamo trarre la conclusione del ragionamento per i gruppi ciclici finiti, infatti, abbiamo visto che l'omomorfismo $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ è completamente determinato da dove si manda la classe del generatore di $\mathbb{Z}/m\mathbb{Z}$ ($[1]_m$), e per il Teorema 1.47 deve essere che:

$$\mathrm{ord}(f([1]_m)) \mid \mathrm{ord}([1]_m) \implies \mathrm{ord}(f([1]_m)) \mid m$$

ma, allo stesso tempo, per il Corollario 1.72 deve essere che:

$$\mathrm{ord}(f([1]_m)) \mid \#\mathbb{Z}/n\mathbb{Z} \implies \mathrm{ord}(f([1]_m)) \mid n$$

ovvero $\mathrm{ord}(f([1]_m))$ è un divisore comune di m ed n, pertanto $\mathrm{ord}(f([1]_m)) \mid (m, n)$. Quindi, per determinare il numero di omomorfismi tra $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$, non ci resta che contare il numero di elementi il cui ordine divide (m, n) in $\mathbb{Z}/n\mathbb{Z}$, e, come visto nell'Esercizio A.6, posto $(m, n) = d$,ci basta applicare il il (2) del Teorema 1.27:

$$da \equiv 0 \pmod{n} \implies a = \frac{n}{d}k \,[70] \qquad (k \in \mathbb{Z})$$

[70] Osserviamo che $\dfrac{n}{(d,n)} = \dfrac{n}{((m,n),n)} = \dfrac{n}{(m,n)} = \dfrac{n}{d}$.

da cui, essendo $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, segue che:

$$0 \leq a < n \implies 0 \leq \frac{n}{d}k < n \implies 0 \leq k < d$$

ovvero ci sono esattamente $d = (m,n)$ possibili scelte per k (quindi valori di a), pertanto ci sono al massimo (m,n) omomorfismi tra $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z}$.[71] Viceversa, sia $h \in \mathbb{Z}/n\mathbb{Z}$ con $\text{ord}(h) \mid (m,n) = d$, allora affermo che la funzione:

$$\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : \overline{k} \longmapsto \overline{k \cdot h}$$

è ben definita(essendo definita su un'insieme quoziente) ed è appunto un omomorfismo. Per verificare la buona definizione ci basta prendere $k_2 \equiv k_1 \pmod{m}$, per cui $k_2 = mz + k_1$, $z \in \mathbb{Z}$, allora:

$$\varphi(k_1) = \varphi(mz + k_1) = \overline{mzh + k_1 h} = \overline{mzh} + \overline{k_1 h}$$

ma, essendo $\text{ord}(h) = d$, allora $dh \equiv 0 \pmod{n} \implies h \equiv 0 \left(\text{mod } \frac{n}{(m,n)}\right)$, ovvero h è un multiplo di $\dfrac{n}{(m,n)}$, quindi mh è multiplo di $\dfrac{mn}{(m,n)} = [m,n]$ (ovvero il prodotto è un multiplo di n), quindi $mh \equiv 0 \pmod{n}$, ergo:

$$\varphi(k_1) = \overline{k_1 h}$$

che verifica la buona definizione di φ. Alternativamente, potevamo verificare la buona definizione vedendo che, presi $k_1 \equiv k_2 \pmod{m}$, allora:

$$k_1 h \equiv k_2 h \pmod{n} \implies (k_1 - k_2)h \equiv 0 \pmod{n}$$

e per gli stessi motivi di prima, osservando che $k_1 - k_2 = mz$, $z \in \mathbb{Z}$, segue che il prodotto è multiplo di n e quindi la congruenza è verificata. Ci resta da dimostrare che φ è un omomorfismo, per farlo, consideriamo $k_1, k_2 \in \mathbb{Z}/m\mathbb{Z}$ e verifichiamo che:

$$\varphi(\overline{k}_1 + \overline{k}_2) = \underbrace{\varphi(\overline{k}_1)}_{=\overline{k_1 h}}\underbrace{\varphi(\overline{k}_2)}_{=\overline{k_2 h}} \qquad \forall k_1, k_2 \in \mathbb{Z}/m\mathbb{Z}$$

quindi:

$$\varphi(k_1 + k_2) = \overline{(k_1 + k_2)h} = \overline{k_1 h + k_2 h} = \overline{k_1 h} + \overline{k_2 h}$$

dove abbiamo usato le proprietà delle classi di resto modulo n, pertanto φ è un omomorfismo.

Si conclude quindi:

Proposizione A.13 (Omomorfismi tra gruppi ciclici finiti)

Dati due gruppi ciclici finiti G_1, G_2, di ordini rispettivamente m ed n, si ha che $|\text{Hom}(G_1, G_2)| = (m,n)$. [a]

[a] Abbiamo visto inoltre che tali omomorfismi sono costruiti in modo da mandare un generatore di G_1 in un elemento di G_2 di ordine (m,n).

[71] Abbiamo quindi visto come per un dato omomorfismo ci siano (m,n) elementi che soddisfano le condizioni richieste da quest'ultimo, ci resta da dimostrare che effettivamente per tutti gli (m,n) elementi l'omomorfismo funzioni.

Possiamo ancora vedere tutti gli altri casi di omomorfismi tra gruppi ciclici di cardinalità finita ed infinita, ricordando sempre che per il Teorema 1.51 possiamo utilizzare $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}$ come prototipi per tutti i gruppi ciclici. Quindi:

- Per $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$, osserviamo che vale ancora il ragionamento precedente, quindi un omomorfismo è completamente determinato da dove viene mandato il generatore del gruppo ciclico finito di partenza $[1]_n$, tale classe deve essere mandata in $f(\overline{1})$ tale che $\mathrm{ord}(f(\overline{1})) \mid \mathrm{ord}([1]_n) = n$, ma l'unico elemento di ordine finito in $\mathbb{Z}$ è 0 (e per questo si ha $\mathrm{ord}(0) = 1 \mid n$), pertanto l'unico omomorfismo possibile è quello banale che manda tutto nell'elemento neutro:
$$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z} : x \longmapsto 0 \qquad \forall x \in \mathbb{Z}$$
- Per $\mathrm{Hom}(\mathbb{Z}, H)$, con H gruppo ciclico qualsiasi, che può essere sia un gruppo ciclico di ordine finito che infinito, vale ancora il ragionamento precedente, quindi un omomorfismo è completamente determinato da dove viene mandato il generatore del gruppo ciclico di partenza ($\langle 1 \rangle = \mathbb{Z}$), tuttavia, in questo caso, basta fissare un elemento $h \in H$ e definire la funzione:[72]
$$f_h : \mathbb{Z} \longrightarrow H : n \longmapsto h^n$$
che è banalmente un omomorfismo per le proprietà delle potenze (ed avendo scelto un insieme di elementi e non di classi $\mathbb{Z}$ è sempre ben definita). Pertanto gli omomorfismi tra $\mathbb{Z}$ ed un gruppo ciclico qualsiasi sono in bigezione con il gruppo qualsiasi (quindi infiniti se il gruppo ha ordine infinito, n se il gruppo è finito):
$$\mathrm{Hom}(\mathbb{Z}, H) \xrightarrow[\sim]{} H$$

§A.9 Automorfismi

Definizione A.14. Sia G un gruppo, si definisce **automorfismo** ogni isomorfismo di G con se stesso.[73] Indichiamo con $\mathrm{Aut}(G)$ l'insieme degli automorfismi di G:
$$\mathrm{Aut}(G) = \left\{ f : G \xrightarrow[\sim]{} G \mid f \text{ omomorfismo} \right\}$$

Proposizione A.15 (Gruppo $\mathrm{Aut}(G)$)
Dato un gruppo G, l'insieme di tutti i suoi automorfismi è un gruppo con l'operazione di composizione $(\mathrm{Aut}(G), \circ)$.

Dimostrazione. Verifichiamo le usuali proprietà di gruppo:

(a) Chiusura: Verifichiamo che:
$$f \circ g(x) \in \mathrm{Aut}(G) \qquad \forall f(x), g(x) \in \mathrm{Aut}(G)$$
la composizione di due applicazioni bigettive è ancora bigettiva, inoltre essendo f, g due permutazioni si ha che $f \circ g : G \longrightarrow G$. Ci resta da verificare che $f \circ g$ sia anch'esso un omomorfismo, per farlo osserviamo che:
$$f \circ g(x + y) = f(g(x + y)) = f(g(x) + g(y)) = f(g(x)) + f(g(y)) \qquad \forall x, y \in G$$

[72] Ovviamente ciò segue dal mandare il generatore 1 in h, da cui appunto $n \longmapsto h^n$.
[73] Un automorfismo può anche essere definito come una permutazione di un insieme che è anche un omomorfismo.

(b) Associatività: La composizione di applicazioni è associativa, come visto per $(\xi(X), \circ)$ e preserva sia bigettività che omomorfismo.

(c) Elemento Neutro: L'applicazione $id \in \mathrm{Aut}(G)$ ed è un omomorfismo.

(d) Inverso: Per il (6) del Teorema 1.46, ogni applicazione bigettiva ammette inversa che a sua volta è un omomorfismo.

□

Analizziamo ora il gruppo degli automorfismi dei gruppi ciclici, quindi $\mathrm{Aut}(\mathbb{Z})$ e $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$:

Osservazione A.16 ($\mathrm{Aut}(\mathbb{Z})$) — Osserviamo che $\mathrm{Aut}(\mathbb{Z}) = \{\varphi : \mathbb{Z} \longrightarrow \mathbb{Z} | \varphi \text{ invertibile}\}$, inoltre, per quanto visto nel paragrafo A.8 un omomorfismo tra $\mathbb{Z}$ ed un gruppo qualsiasi è completamente determinato dal mandare n in h^n (avendo scelto di mandare $1 \longmapsto h$), quindi possiamo osservare che:

$$\mathrm{Aut}(\mathbb{Z}) = \{\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z} : 1 \longmapsto n | \varphi_n \text{ invertibile}\}$$

con $\varphi_n(h) = hn$[a], l'immagine dell'applicazione è data da:

$$\mathrm{Im}\varphi_n = \varphi_n(\mathbb{Z}) = \{\varphi_n(h) | h \in \mathbb{Z}\} = \{hn | h \in \mathbb{Z}\} = n\mathbb{Z}$$

per ipotesi φ_n è invertibile, quindi bigettiva, quindi surgettiva [b], ma $\mathbb{Z} = n\mathbb{Z} \iff n = \pm 1$, pertanto le uniche due applicazioni possibili sono l'identità id e l'applicazione che manda ogni elemento nel suo opposto (indicheremo quest'ultima per comodità con $-id$), quindi:

$$\mathrm{Aut}(\mathbb{Z}) = \{\pm id\}$$

dove si osserva che $\mathrm{Aut}(\mathbb{Z})$ è banalmente un gruppo ciclico[c], quindi:

$$\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

[a] Dove abbiamo utilizzato la notazione additiva perché ci troviamo in $\mathbb{Z}$ che è un gruppo abeliano.
[b] Ricordiamo che per definizione di automorfismo l'insieme di partenza e di arrivo devono coincidere, quindi l'applicazione deve essere surgettiva su $\mathbb{Z}$ stesso e non su una sua restrizione.
[c] Dove id è l'elemento neutro e $-id$ è l'unico elemento diverso da quello neutro, quindi necessariamente di ordine 2, per il quale $(-id)^2 = id$, quindi $\mathrm{Aut}(\mathbb{Z}) = \langle -id \rangle$.

Osservazione A.17 ($\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$) — Osserviamo che $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\varphi_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : \overline{x} \longmapsto \overline{ax}$[a]$ | \varphi_a \text{ invertibile}\}$, affinché φ_a sia invertibile deve essere bigettiva, ed essendo i gruppi finiti, ci basta che sia iniettiva, ovvero, per il (5) del Teorema 1.46, che $\ker \varphi_a = \{\overline{0}\}$. Studiamo il nucleo dell'omomorfismo:

$$\ker \varphi_a = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} | \varphi_a(\overline{x}) = ax \equiv 0 \pmod{n}\}$$

ovvero:

$$x \equiv 0 \pmod{\frac{n}{(a,n)}}$$

la congruenza ha esattamente (a, n) soluzioni in $\mathbb{Z}/n\mathbb{Z}$ (che rappresentano il nucleo dell'omomorfismo), affinché $\ker \varphi_a = \{\overline{0}\}$, quindi ci sia una sola soluzione, deve essere che: $\dfrac{n}{(a,n)} = n \implies (a, n) = 1$[b], quindi il nucleo è banale per tutti i valori

di $\overline{a}$ coprimi con n. Tuttavia, poiché in $\mathbb{Z}/n\mathbb{Z}$ tutti i numeri coprimi con n sono invertibili (e quindi appartengono a $\mathbb{Z}/n\mathbb{Z}^*$), sappiamo che per ogni a coprimo con n, $\exists b \in \mathbb{Z}/n\mathbb{Z}$ inverso di a:

$$ab \equiv 1 \pmod{n}$$

da cui si deduce che $\varphi_a^{-1} = \varphi_b$[c], ovvero che:

$$\varphi_b \circ \varphi_a(\overline{x}) = \varphi_b(\overline{ax}) = \overline{\underbrace{ba}_{=\overline{1}} x} \equiv x \pmod{n}$$

quindi $\varphi_a \circ \varphi_b = \varphi_b \circ \varphi_a = id$. A questo punto possiamo ottenere che:

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$$

per verificare ciò, cerchiamo un isomorfismo tra i due gruppi, ad esempio:

$$\psi : \mathbb{Z}/n\mathbb{Z}^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) : \overline{a} \longmapsto \varphi_a$$

verifichiamo che ψ è un isomorfismo, ovvero che è bigettiva ed è un omomorfismo.[d] Per la bigettività, si osserva che $|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = |\mathbb{Z}/n\mathbb{Z}^*| = \phi(n)$, e per quanto visto prima, se $(a, n) = 1$, allora φ_a è iniettiva, dunque biettiva. Per verificare la proprietà di omomorfismo bisogna verificare che:

$$\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{a}) \circ \psi(\overline{b}) \qquad \forall \overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}^*$$

essendo l'immagine di ψ calcolata in un elemento un insieme di funzioni, per dimostrare l'uguaglianza sopra, posso far vedere che:

$$\underbrace{\psi(\overline{a}\overline{b})(x)}_{=\varphi_{ab}(x)} = (\underbrace{\psi(\overline{a})}_{=\varphi_a} \circ \underbrace{\psi(\overline{b})}_{=\varphi_b})(x) \qquad \forall \overline{x} \in \mathbb{Z}/n\mathbb{Z}$$

da cui:

$$\varphi_{ab}(x) = (\varphi_a \circ \varphi_b)(x) \implies \overline{abx} = \varphi_a(\overline{bx}) = \overline{abx} \qquad \forall \overline{x} \in \mathbb{Z}/n\mathbb{Z}$$

Pertanto ψ è un isomorfismo e la proposizione è dimostrata.

[a] Come visto nel paragrafo A.8 un omomorfismo tra $\mathbb{Z}/n\mathbb{Z}$ ed un altro gruppo ciclico finito è completamente determinato dal mandare il generatore del gruppo $[1]_n$ in un elemento dell'altro gruppo di ordine (m, n), $[1]_n \longmapsto \overline{a} \implies \overline{k} \longmapsto \overline{a \cdot k}$.

[b] Infatti se $(a, n) = 1$, allora $0 \leq x < n \implies 0 \leq \frac{n}{(a,n)} k < n \implies 0 \leq k < (a, n) \implies 0 \leq k < 1$, quindi un solo valore possibile per k, e quindi una sola scelta per a, da cui una sola soluzione per la congruenza.

[c] Che prova subito che φ_a è invertibile e quindi è una bigezione.

[d] Andrebbe verificata anche la buona definizione.

§A.10 Sottogruppi ciclici di un gruppo

Sia G un gruppo, vogliamo contare i suoi sottogruppi (ciclici e finiti) di un dato ordine, indichiamo con $s_d(G)$ il numero dei sottogruppi ciclici di G di ordine d, o anche il numero di sottogruppi di G isomorfi a $\mathbb{Z}/d\mathbb{Z}$[74], sia $e_d(G)$ il numero di elementi di ordine d in G.

Proposizione A.18

Sia G un gruppo ciclico, il numero dei sottogruppi ciclici di G di ordine d è dato da:

$$s_d(G) = \frac{e_d(G)}{\phi(d)}$$

Dimostrazione. Come sappiamo, un buon modo di cercare sottogruppi di ordine d, è quello di considerare i sottogruppi generati da elementi di ordine d, consideriamo la funzione:

$$F_d : \{g \in G | \operatorname{ord}(g) = d\} \longrightarrow \{H \leqslant G | H = \langle h \rangle, h \in G\}^{75} : g \longmapsto \langle g \rangle$$

tale funzione è surgettiva, poiché se si considera un qualunque sottogruppo ciclico di ordine d ($H \cong \mathbb{Z}/d\mathbb{Z}$), esso deve avere necessariamente un generatore di ordine d, sia tale generatore h, allora $F_d(h) = H$. Alternativamente, si considera $H \cong \mathbb{Z}/d\mathbb{Z}$, infatti, possiamo fissare un isomorfismo tra i due gruppi ψ, prendendo $h = \psi^{-1}(\overline{1})$, ovvero prendendo il generatore di $\mathbb{Z}/d\mathbb{Z}$ e associandolo ad uno di H abbiamo trovato un isomorfismo tra i due gruppi. A questo punto, possiamo osservare come tale isomorfismo non è iniettivo e cercare di capire quanto non lo sia, ovvero, fissato H, vogliamo cercare la cardinalità dell'insieme:[76]

$$\{g \in G | F_d(g) = \langle g \rangle = H\}$$

vogliamo quindi contare il numero di generatori di $H \leqslant G$, ma essendo H un sottogruppo ciclico finito, possiamo applicare il (3) del Corollario 1.38 ed ottenere che il numero di generatori, ovvero elementi di ordine d, in H è dato da $\phi(d)$. A questo punto abbiamo una funzione F_d che è surgettiva ed in cui la controimmagine di ogni elemento ha cardinalità $\phi(d)$, pertanto si ha che:

$$\#\{g \in G | \operatorname{ord}(g) = d\} = \#\{H \leqslant G | H = \langle h \rangle, h \in G\} \cdot \phi(d)$$

ovvero:

$$e_d(G) = s_d(G) \cdot \phi(d)$$

che dimostra la tesi. □

Esercizio A.19. Contare i sottogruppi di $G = \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$ isomorfi a $\mathbb{Z}/8\mathbb{Z}$.

Soluzione. Per contare tali sottogruppi, per quanto abbiamo appena visto, è sufficiente contare gli elementi di ordine 8 di G e per il (3) del Teorema 1.57 sappiamo, posto $g = (a, b)$, che:

$$\operatorname{ord}(g) = [\operatorname{ord}_{16}(a), \operatorname{ord}_{32}(b)]$$

[74] Teorema 1.51.
[75] O anche i sottogruppi $H \cong \mathbb{Z}/d\mathbb{Z}$.
[76] Ciò è una conseguenza del fatto che data $f : X \longrightarrow Y$, si ha che $X = \bigcup_{y \in Y} f^{-1}(y)$, e quindi $|X| = \sum_{y \in Y} |f^{-1}(y)|$.

per contare il numero di elementi di ordine 8 ci basta contare il numero di elementi il cui ordine divide 8, e quindi per il (2) del Teorema 1.27 $8(a,b) = (\overline{0},\overline{0})$, e sottrarre per il numero di elementi il cui ordine divide 4:

$$e_8(G) = \#\left\{(a,b) \in \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z} \middle| \begin{cases} 8a \equiv 0 \,(\text{mod } 16) \\ 8b \equiv 0 \,(\text{mod } 32) \end{cases}\right\} - \#\left\{(a,b) \in \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z} \middle| \begin{cases} 4a \equiv 0 \,(\text{mod } 16) \\ 4b \equiv 0 \,(\text{mod } 32) \end{cases}\right\}$$

ovvero:

$$8 \cdot 8 - 4 \cdot 4 = 48$$

pertanto:

$$s_8(G) = \frac{e_8(G)}{\phi(8)} = \frac{48}{4} = 12$$

□

§A.11 Ordini in gruppi abeliani

Lemma A.20

Sia G un gruppo abeliano finito[a] e sia $\mathcal{O} = \{\text{ord}(g) | g \in G\}$, allora:

(1) Se $n \in \mathcal{O}$ e $d \mid n$, $d > 0$, allora $d \in \mathcal{O}$.

(2) Siano g_1 e g_2 elementi di ordini rispettivamente n_1 e n_2, con $(n_1, n_2) = 1$, allora $\text{ord}(g_1 + g_2) = n_1 \cdot n_2$.

(3) Se $n_1, n_2 \in \mathcal{O}$, allora $[n_1, n_2] \in \mathcal{O}$.

(4) $\max \mathcal{O} = \text{m.c.m.}\{\text{ord}(g) | g \in G\}$.

[a] L'ipotesi di finitezza non è necessaria, ma in questo caso semplifica le cose.

Dimostrazione. Dimostriamo singolarmente le proposizioni:

(1) Dato un elemento di ordine n, vogliamo trovarne uno di ordine d, per fare ciò ci basta considerare:

$$h = g^{\frac{n}{d}} \implies h^d = (g^{\frac{n}{d}})^d = g^n = e$$

pertanto, per il (2) del Teorema 1.27, $\text{ord}(h) | d$. Sia allora $\text{ord}(h) = k \implies h^k = e$ da cui:

$$h^k = (g^{\frac{n}{d}})^k = e$$

e, sempre per il Teorema 1.27, deve essere che:

$$\text{ord}(g) = n \,\Big|\, \frac{n}{d}k \iff d \mid k$$[77]

da cui $d = k = \text{ord}(h)$ che verifica la tesi, in quanto abbiamo un elemento di ordine d in G, ovvero $d \in \mathcal{O}$.

[77] In quanto $n \,\Big|\, \frac{n}{d}k \implies \frac{n}{d}k = nh$, $h \in \mathbb{Z}$, da cui $\frac{k}{d} = h \implies \frac{k}{d} \in \mathbb{Z}$, ovvero $d | k$.

(2) Osserviamo preliminarmente che:

$$\langle g_1 \rangle \cap \langle g_2 \rangle = K$$

dove $K \leqslant G$ in quanto intersezione di due sottogruppi da cui $K \leqslant \langle g_1 \rangle$, $K \leqslant \langle g_2 \rangle$, pertanto, per il Teorema di Lagrange, $\#K \mid n_1$ e $\#K \mid n_2$, pertanto $\#K \mid (n_1, n_2) = 1 \implies \#K = 1 \implies K = \{e\}$, quindi, se gli ordini di g_1 e g_2 sono coprimi, l'unica potenza che hanno in comune è l'identità. Per trovare l'ordine di $g_1 + g_2$, bisogna trovare gli esponenti h tali che $(g_1 + g_2)^h = e$, (da questo momento adotteremo la notazione moltiplicativa, nonostante il gruppo sia abeliano, per rendere più facile il ragionamento), ma:

$$(g_1 g_2)^h = \underbrace{(g_1 g_2) \dots (g_1 g_2)}_{h-\text{volte}}$$

dove, essendo per ipotesi G abeliano, possiamo riordinare gli esponenti ed ottenere:

$$(g_1 g_2)^h = g_1^h g_2^h$$

da cui, voler studiare:

$$g_1^h g_2^h = e \iff g_1^h = g_2^{-h}$$

ma ciò è vero se e solo se:

$$\begin{cases} g_1^h = e \\ g_2^{-h} = e \ (g_2^h = e) \end{cases}$$

che è vero se e solo se:

$$\begin{cases} n_1 \mid h \\ n_2 \mid h \end{cases}$$

da cui $[n_1, n_2] = n_1 n_2 \mid h$, cioè $\operatorname{ord}(g_1 g_2) = n_1 \cdot n_2$, in quanto l'ordine è minimo, quindi, poiché $(g_1 g_2)^{[n_1,n_2]} = g_1^{[n_1,n_2]} g_2^{[n_1,n_2]} = e$, ed $[n_1, n_2] \mid h$, allora $\operatorname{ord}(g_1 + g_2) = h = [n_1, n_2] = n_1 \cdot n_2$.

(3) Per dimostrare la tesi, ci basta trovare un elemento di ordine $[n_1, n_2]$, osserviamo che:

$$[n_1, n_2] = d_1 \cdot d_2 \qquad \text{con} \quad (d_1, d_2) = 1 \quad \text{e} \quad d_1 \mid n_1, d_2 \mid n_2$$ [78]

per il punto (1) esistono $g_1^{\frac{n_1}{d_1}}$ e $g_2^{\frac{n_2}{d_2}}$ in G di ordini rispettivamente d_1 e d_2, mentre per il punto (2) so che $\operatorname{ord}\left(g_1^{\frac{n_1}{d_1}} g_2^{\frac{n_2}{d_2}}\right) = d_1 \cdot d_2 = [n_1, n_2]$ che dimostra la tesi.

(4) Sia $M = \max \mathcal{O}$, allora $M \leq \text{m.c.m.}\{\operatorname{ord}(g) | g \in G\}$, poiché $M \in \mathcal{O}$, viceversa, se $n \in \mathcal{O}$, allora $[M, n] \in \mathcal{O}$ per il punto (3), ma, per quanto appena detto si osserva che: $M \leq [M, n] \leq M = \max \mathcal{O}$ ($\implies [M, n_i] = M$) quindi $n_i \mid M$, pertanto, M è multiplo di tutti gli altri ordini, quindi è proprio l'm.c.m.

□

Osservazione A.21 — Non è vero in generale che $\operatorname{ord}(g_1 g_2) = [\operatorname{ord}(g_1), \operatorname{ord}(g_2)]$. Ad esempio, per $G = \mathbb{Z}/3\mathbb{Z}^*$, presi $g_1 = g_2 = -1$ segue che $\operatorname{ord}(g_1) = \operatorname{ord}(g_2) = 2$, ma $\operatorname{ord}(g_1 g_2) = 1$.

[78] Seguendo il metodo di fattorizzazione classico per determinare l'm.c.m.

§A.11.1 $\mathbb{Z}/p\mathbb{Z}^*$

Teorema A.22
Sia p un numero primo, il gruppo $\mathbb{Z}/p\mathbb{Z}^*$ è ciclico.

Dimostrazione. Sia $\mathcal{O} = \{\text{ord}(x) | x \in \mathbb{Z}/p\mathbb{Z}^*\}$ e $M = \max \mathcal{O}$, per dimostrare che $\mathbb{Z}/p\mathbb{Z}^*$ è ciclico è necessario far vedere che $\phi(p) = p - 1 \in \mathcal{O}$, che si traduce nel dimostrare che $M = p - 1$. Osserviamo che per l'(1) del Corollario 1.72 segue che $\text{ord}(x) \mid p - 1$, $\forall x \in \mathbb{Z}/p\mathbb{Z}^*$, pertanto $M \leq p - 1$, inoltre, per il (4) del Lemma A.20, $\text{ord}(x) \mid M$, $\forall x \in \mathbb{Z}/p\mathbb{Z}^*$, segue quindi, essendo M multiplo comune a tutti gli ordini di elementi in $\mathbb{Z}/p\mathbb{Z}^*$, che:

$$x^M \equiv 1 \pmod{p} \qquad \forall x \in \mathbb{Z}/p\mathbb{Z}^*$$

Sia $f(x) = x^M - 1$, per quanto detto, vale che:

$$f(x) \equiv 0 \pmod{p} \qquad \forall x \in \mathbb{Z}/p\mathbb{Z}^*$$

il polinomio $f(x)$ ha almeno $p - 1$ radici, poiché M è l'm.c.m. di tutti gli ordini di elementi in $\mathbb{Z}/n\mathbb{Z}^*$, per il Teorema di Ruffini, il numero di radici di un polinomio è minore o uguale al suo grado, pertanto $p - 1 \leq \deg(f(x)) = M \implies p - 1 \leq M$, ciò completa la dimostrazione. □

§A.12 Gruppo infinito con elementi di ordine finito

Consideriamo il gruppo delle radici n esime dell'unità in $\mathbb{C}$:

$$\mu_n = \{\zeta \in \mathbb{C} | \zeta^n = 1\} \cong \mathbb{Z}/n\mathbb{Z}$$

i due gruppi sono isomorfi mediante l'isomorfismo:

$$(\mathbb{Z}/n\mathbb{Z} \ni)\overline{k} \longmapsto \exp\left(\frac{2\pi i}{n}k\right)(\in \mu_n)$$

consideriamo ora:

$$\mu_\infty = \bigcup_{n \geq 1} \mu_n$$

ovvero l'unione di tutti i gruppi μ_n, tale insieme è un gruppo con l'operazione di prodotto. Osserviamo che $\mu_\infty \leqslant \mathbb{C}^*$, quindi è sufficiente verificare che μ_∞ sia un sottogruppo, pertanto:

(1) Se $\zeta \in \mu_\infty$, allora esiste n tale che $\zeta \in \mu_n$ (che è un gruppo), pertanto, esiste $\zeta^{-1} \in \mu_n (\subset \mu_\infty) \implies \zeta^{-1} \in \mu_\infty$.

(2) Se $\zeta_1, \zeta_2 \in \mu_\infty$, allora esistono n_1, n_2 tali che $\zeta_1 \in \mu_{n_1}$ e $\zeta_2 \in \mu_{n_2}$, allora $(\zeta_1\zeta_2)^{n_1 n_2} = \zeta_1^{n_1 n_2}\zeta_2^{n_1 n_2} = 1 \cdot 1 = 1 \implies \zeta_1 \cdot \zeta_2 \in \mu_{n_1 \cdot n_2}$, ovvero $\zeta_1 \cdot \zeta_2 \in \mu_\infty$.

segue che $(\mu_\infty, \cdot)$ è un gruppo di ordine infinito, tuttavia ogni suo elemento ha ordine finito, infatti il gruppo è stato costruito come unione di gruppi finiti, e quindi tutti i suoi elementi hanno ordine finito: se $\zeta \in \mu_\infty \implies \exists n$ tale che $\zeta \in \mu_n$, da cui $\zeta^n = 1 \implies \text{ord}(\zeta) \mid n$ e quindi è finito.

§A.13 Gruppi con sottogruppi ciclici

Lemma A.23

Sia G un gruppo abeliano finito, $H < G$ ciclico. Supponiamo che:

(i) G/H ciclico;

(ii) $\left(\left|G/H\right|, |H|\right) = 1$;

allora G è ciclico.

Soluzione. Siano $m = |H|$ e $n = G/H$, essendo i gruppi ciclici per ipotesi, si ha $H \cong \mathbb{Z}/m\mathbb{Z}$ e $G/H \cong \mathbb{Z}/n\mathbb{Z}$. Consideriamo la proiezione modulo H:

$$\pi_H : G \longrightarrow G/H : g \longmapsto gH$$

essa è definita sempre (essendo G abeliano ogni suo sottogruppo è normale) ed è un omomorfismo surgettivo di gruppi. Poiché le classi laterali modulo H hanno tutte la medesima cardinalità si ha che $|G| = mn$ dunque per dimostrare che G è ciclico è sufficiente trovare un elemento di ordine mn, per ipotesi si ha che H è ciclico, quindi $H = \langle h \rangle$, con $h \in G$ e $\operatorname{ord}(h) = m$. D'altra parte si ha che G/H è ciclico, quindi contiene un elemento $xH (= \pi_H(x))$ di ordine n, per le proprietà di omomorfismo si ha che $n = \operatorname{ord}(\pi_H(x)) \mid \operatorname{ord}_G(x)$, pertanto $\operatorname{ord}(x) = nd$, $d \in \mathbb{Z}$. Per il (3) del Lemma A.20 sappiamo che l'insieme degli ordini di un gruppo abeliano è chiuso per l'operazione di m.c.m. (quindi l'm.c.m. di due ordini sarà ancora un ordine), si ha quindi che $[m, nd] \mid mn$ (per Lagrange) e per ipotesi, poiché $(n, m) = 1$, si ha che $mn \mid [m, nd] \implies [m, nd] = mn$, quindi esiste $g \in G$ di ordine mn. □

Osservazione A.24 — Osserviamo che le ipotesi fatte sono tutte strettamente necessarie per dimostrare che G è ciclico:

- Se G non è abeliano, ad esempio $G = S_3$, possiamo considerare $H = \langle \sigma \rangle$, si ha che $[S_3 : \langle \sigma \rangle] = 2 \implies \langle \sigma \rangle \trianglelefteq S_3$, quindi possiamo consderare il gruppo quoziente $S_3/\langle \sigma \rangle = \{\langle \sigma \rangle, \tau \langle \sigma \rangle\} = \{\langle \sigma \rangle, \langle \sigma \rangle \tau\} \cong \mathbb{Z}/2\mathbb{Z}$, tuttavia ovviamente S_3 non è ciclico, nonostante H e G/H siano ciclici e di ordini coprimi.
- Se H non è ciclico, consideriamo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ e $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \{\overline{0}\}$, quoziente ha tre elementi ($[G : H] = 3$) e quindi $G/H \cong \mathbb{Z}/3\mathbb{Z}$, gli ordini di H e G/H sono coprimi, ma nonostante ciò G non è ciclico (ad esempio per il Teorema Cinese del Resto).
- Se H e G/H non sono coprimi, ad esempio $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $H = \mathbb{Z}/2\mathbb{Z} \times \{\overline{0}\}$, si ha $G/H = \mathbb{Z}/2\mathbb{Z}$, ma G non è ciclico.

§A.13.1 $\mathbb{Z}/p^n\mathbb{Z}^*$

Teorema A.25
Il gruppo $\mathbb{Z}/p^n\mathbb{Z}^*$ è ciclico per ogni primo p dispari e per ogni $n \geq 1$.

Dimostrazione. Sappiamo che l'ordine modulo p^n di $(1+p)$ è p^{n-1}, ciò significa che il sottogruppo $H = \langle 1+p \rangle$ è ciclico di ordine p^{n-1}. Consideriamo l'insieme:

$$\widetilde{H} = \{x \in \mathbb{Z}/p^n\mathbb{Z}^* | x \equiv 1 \pmod{p}\} = {}^{79} \{x \in \mathbb{Z}/p^n\mathbb{Z} | x \equiv 1 \pmod{p}\}$$

da ciò si osserva che $|\widetilde{H}| = p^{n-1}$ (essendo una classe ogni p, su un totale di p^n classi). Si osserva che gli elementi di H sono congrui ad 1 modulo p pertanto $H \subseteq \widetilde{H}$, ma d'altra parte i due insiemi hanno la stessa cardinalità e quindi coincidono $\implies \widetilde{H}$ ciclico. Consideriamo:

$$f : \mathbb{Z}/p^n\mathbb{Z}^* \longrightarrow \mathbb{Z}/p\mathbb{Z}^* : [x]_{p^x} \longmapsto [x]_p$$

si osserva facilmente che (per le proprietà delle classi di resto) f è un omomorfismo, ed in particolare è surgettivo, infatti, se $[a]_p \in \mathbb{Z}/p\mathbb{Z}^*$, posso prendere $[a]_p = f([a]_{p^n})$, cioè posso sempre ridurre modulo p^n partendo da modulo p, e tale valore starà sempre in $\mathbb{Z}/p^n\mathbb{Z}^*$ e ciò è sempre valido per definizione di f. Osserviamo che:

$$\ker f = \{\overline{x} \in \mathbb{Z}/p^n\mathbb{Z}^* | f(\overline{x}) = [1]_p\} = \{x \in \mathbb{Z}/p^n\mathbb{Z}^* | x \equiv 1 \pmod{p}\} = H$$

per il Primo Teorema Di Omomorfismo segue:

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z}^* & \xrightarrow{f} & \mathbb{Z}/p\mathbb{Z}^* \\ {\scriptstyle \pi_{\ker f}}\downarrow & \circlearrowleft \quad \nearrow & \\ \dfrac{\mathbb{Z}/p^n\mathbb{Z}^*}{\langle 1+p \rangle} & & \end{array}$$

ovvero:

$$\frac{\mathbb{Z}/p^n\mathbb{Z}^*}{\langle 1+p \rangle} \cong \mathbb{Z}/p\mathbb{Z}^*$$

da cui $\frac{\mathbb{Z}/p^n\mathbb{Z}^*}{\langle 1+p \rangle}$ è ciclico. Si conclude che sono verificate le ipotesi del Lemma A.23: $\langle 1+p \rangle < \mathbb{Z}/p^n\mathbb{Z}^*$ è ciclico, $\frac{\mathbb{Z}/p^n\mathbb{Z}^*}{\langle 1+p \rangle}$ è ciclico, $\left(|\langle 1+p \rangle|, \left| \frac{\mathbb{Z}/p^n\mathbb{Z}^*}{\langle 1+p \rangle} \right| \right) = (p^{n-1}, p-1) = 1$, da ciò si conclude che $\mathbb{Z}/p^n\mathbb{Z}^*$ è ciclico. □

[79] Poiché $x \equiv 1 \pmod{p}$, allora è sempre coprimo con p^n.

§A.14 Numero di potenze modulo p^n

Esercizio A.26. Contare il numero delle potenze k-esime modulo p^n, ovvero:

$$\#\{x^k \in \mathbb{Z}/p^n\mathbb{Z}^* | x \in \mathbb{Z}/p^n\mathbb{Z}^*\}$$

Soluzione. Si vuole contare la cardinalità del seguente insieme:

$$\{x^k \in \mathbb{Z}/p^n\mathbb{Z}^* | x \in \mathbb{Z}/p^n\mathbb{Z}^*\}$$

per farlo consideriamo l'omomorfismo:

$$f_k : \mathbb{Z}/p^n\mathbb{Z}^* \longrightarrow \mathbb{Z}/p^n\mathbb{Z}^* : \overline{x} \longmapsto \overline{x^k}$$

per il Primo Teorema Di Omomorfismo si ha:

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z}^* & \xrightarrow{f_k} & \mathbb{Z}/p^n\mathbb{Z}^* \\ {\scriptstyle \pi_{\ker f}}\downarrow & \circlearrowleft & \uparrow \\ \dfrac{\mathbb{Z}/p^n\mathbb{Z}^*}{\ker f} & \xrightarrow[\sim]{} & \mathrm{Im} f_k \end{array}$$

come si osserva: $\mathrm{Im} f_k = \{x^k \in \mathbb{Z}/p^n\mathbb{Z}^* | x \in \mathbb{Z}/p^n\mathbb{Z}^*\}$, pertanto:

$$|\mathrm{Im} f_k| = \frac{|\mathbb{Z}/p^n\mathbb{Z}^*|}{|\ker f_k|} = \frac{\phi(p^n)}{|\ker f_k|}$$

siccome $\mathbb{Z}/p^n\mathbb{Z}^*$ è ciclico, allora $\mathbb{Z}/p^n\mathbb{Z}^* = \{g^0, g^2, \dots, g^{p^{n-1}(p-1)-1}\}$, a questo punto si osserva che:

$$\ker f_k = \{\overline{x} \in \mathbb{Z}/p^n\mathbb{Z}^* | f_k(\overline{x}) = x^k \equiv 1 \pmod p\}$$

quindi:

$$|\ker f_k| = \#\left\{g^i \in \mathbb{Z}/p^n\mathbb{Z}^* \middle| g^{ik} \equiv 1 \pmod p\right\}$$

da cui:

$$ik \equiv 0 \pmod{p^{n-1}(p-1)} \iff i \equiv 0 \left(\mathrm{mod}\ \frac{p^{n-1}(p-1)}{(k, p^{n-1}(p-1))}\right)$$

pertanto:

$$0 \le i < p^{n-1}(p-1) \iff 0 \le \frac{p^{n-1}(p-1)}{(k, p^{n-1}(p-1))} t < p^{n-1}(p-1) \qquad t \in \mathbb{Z}$$

da cui: $0 \le t < (k, p^{n-1}(p-1)) \implies (k, p^{n-1}(p-1))$ soluzioni, ed infine:

$$|\mathrm{Im} f_k| = \frac{p^{n-1}(p-1)}{(k, p^{n-1}(p-1))}$$

□

§A.15 Teorema Di Cauchy per gruppi abeliani

Teorema A.27 (Teorema Di Cauchy Per Gruppi Abeliani)
Sia G un gruppo abeliano finito e p un primo tale che $p \mid |G|$, allora esiste $g \in G$ tale che $\text{ord}(g) = p$.

Dimostrazione. Se $p \mid |G|$, allora $|G| = pn$, quindi si può provare la tesi per induzione su n . Se $n = 1$, $|G| = p$, pertanto, per il Corollario 1.74 G contiene un elemento di ordine p (ed è ciclico). Assumiamo ora la tesi vera $\forall i \in \{1, \dots, n\}$ e proviamola per $n + 1$, sia $h \in G \setminus \{e\}$, se:

- se $\text{ord}(h)$ è multiplo di p, allora per l'(1) del Lemma A.20, poiché $p \mid \text{ord}(h) \in \mathcal{O} \implies p \in \mathcal{O}$, quindi c'è un elemento di ordine p. Alternativamente, sappiamo che $|\langle h \rangle| \equiv 0 \pmod p$ ed è ciclico, quindi ha elementi di ogni ordine che divide il gruppo, ed in particolare, se $\text{ord}(h) = pt$, allora $\text{ord}(h^t) = p$.
- se $\text{ord}(h)$ non è multiplo di p, sia $H = \langle h \rangle$, osserviamo che $H \trianglelefteq G$ (essendo G abeliano) e quindi possiamo considerare G/H a sua volta abeliano e di ordine strettamente minore di $|G|$ $\left(\left|G/H\right| = \frac{|G|}{|H|}\right)$, si osserva inoltre che per ipotesi $p \mid |G|$ e $p \nmid |G|$, ovvero $p \mid \frac{|G|}{|H|}$. Si conclude quindi che il gruppo G/H verifica le ipotesi del teorema di Cauchy per un ordine strettamente più piccolo, quindi vale l'ipotesi induttiva:
$$\exists xH \in G/H : \text{ord}(xH) = p$$
possiamo considerare ora l'omomorfismo surgettivo di proiezione al quoziente modulo H
$$\pi_H : G \longrightarrow G/H : g \longmapsto gH$$
dalla surgettività di tale omomorfismo segue che $\exists x \in G : \pi_H(x) = xN$, dunque per le proprietà degli ordini in omomorfismi si ha:
$$\text{ord}((\pi_H(x))) \mid \text{ord}(x) \implies p \mid \text{ord}(x)$$
ed a questo punto siamo nel primo caso e la tesi è vera sempre per $n + 1 \implies$ la tesi è vera $\forall n \in \mathbb{N}$ per il Principio d'Induzione.

□

§A.16 Applicazioni del Teorema Di Corrispondenza

Esercizio A.28. Sia $G = \mathbb{Z} \times \mathbb{Z}$, trovare tutti i sottogruppi H di G tali che $[G : H] = 5$.

Soluzione. Osserviamo inizialmente che per ipotesi deve essere ${}^{G}\!/_{H} \cong \mathbb{Z}/5\mathbb{Z}$, ovvero che gli elementi di ${}^{G}\!/_{H}$ possono avere soltanto ordine 1 o 5 (ed in particolare ${}^{G}\!/_{H}$ è ciclico), ciò signifca che o $gH = H \iff g \in H (\implies 5g \in H)$[80], oppure $5(gH) = (5g)H = H \iff 5g \in H$, $\forall g \in G$, quindi per ipotesi deve essere sempre che $5G = \{5g | g \ \in G\} \subseteq H$, dove $5G = \{(5a, 5b) | a, b \in \mathbb{Z}\} = 5\mathbb{Z} \times 5\mathbb{Z}$. A questo punto, essendo $\mathbb{Z}$ abeliano, segue $K = 5\mathbb{Z} \times 5\mathbb{Z} \trianglelefteq G$, vale quindi il Teorema Di Corrispondenza Dei Sottogruppi:

$$\{H \leqslant G | K \subseteq H\} \longleftrightarrow \left\{\mathcal{H} \leqslant {}^{G}\!/_{K} \middle| \left[{}^{G}\!/_{K} : \mathcal{H}\right] = 5\right\}$$

dove ${}^{G}\!/_{K} = \dfrac{\mathbb{Z} \times \mathbb{Z}}{5\mathbb{Z} \times 5\mathbb{Z}} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$[81], dunque possiamo determinare i sottogruppi cercati, determinando i sottogruppi di $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ e poi prendendone la controimmagine. Quindi cerchiamo i sottogruppi di $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ di ordine 5 (che quindi sono ciclici), e come noto il loro numero è dato da:

$$s_5(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) = \frac{e_5(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})}{\phi(5)}$$

si osserva che in $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ tutti gli elementi hanno ordine 5 eccetto $(\overline{0}, \overline{0})$, quindi:

$$s_5(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) = \frac{25 - 1}{4} = 6$$

Osserviamo che i sottogruppi cercati sono: $\langle(\overline{1}, \overline{0})\rangle$, $\langle(\overline{1}, \overline{1})\rangle$,$\langle(\overline{1}, \overline{2})\rangle$, $\langle(\overline{1}, \overline{3})\rangle$, $\langle(\overline{1}, \overline{4})\rangle$, $\langle(\overline{1}, \overline{5})\rangle$, $\langle(\overline{0}, \overline{1})\rangle$, questi sottogruppi sono di ordine 5, e gli unici loro sottogruppi sono il gruppo banale e se stessi, poiché l'intersezione tra due sottogruppi è un sottogruppo, intersecando due di loro o coincidono o la loro intersezione è il sottogruppo banale, dunque, affinché tali sottogruppi siano tutti distinti (e quindi siano quelli che cerchiamo), è sufficiente controllare che le intersezioni a due a due siano tutte banali. Osserviamo che $\langle(\overline{0}, \overline{1})\rangle$ non contiene elementi della forma $(\overline{1}, \overline{x})$, quindi l'unica possibile Intersezione con gli altri è il sottogrupo banale, negli altri sottogruppi l'unico possibile elemento comune è della forma $(\overline{1}, \overline{x})$, ma al variare di $\overline{x}$ otteniamo il generatore di quel sottogruppo e le sue classi sono distinte da quelle di un altro generatore, pertanto tutti i sottogruppi sono distiniti e la loro intersezione è banale $\implies$ i sottogruppi trovati sono l'immagine di quelli richiesti all'inizio.[82] Non ci resta che prendere le controimmagini dei sottogruppi trovati, osserviamo preliminarmente che i sottogruppi possono essere riscritti mediante le congruenze, ad esempio;

$$\langle(\overline{1}, \overline{2})\rangle = \{(\overline{x}, \overline{y}) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} |\, y \equiv 2x \pmod 5\}$$

quindi $\langle(\overline{1}, \overline{2})\rangle = \langle(\overline{x}, \overline{2x})\rangle$. A questo punto i sottogruppi di partenza cercati si possono trovare ad esempio come:

$$\pi_K^{-1}(\langle(\overline{1}, \overline{3})\rangle) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | \pi_K((x, y)) \in \langle(\overline{1}, \overline{3})\rangle\} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} |\, y \equiv 3x \pmod 5\}$$

ed in generale $(G \geqslant)\{(x, y) \in \mathbb{Z} \times \mathbb{Z} |\, y \equiv kx \pmod 5\} \longleftrightarrow \langle(\overline{1}, \overline{k})\rangle$. □

[80] Per chiusra dell'operazione.
[81] Si dimostra che in generale $\frac{A \times B}{C \times D} \cong {}^{A}\!/_{C} \times {}^{B}\!/_{D}$.
[82] Il tipo di sottogruppi usati in questo caso è molto utlizzato per scrivere sottogruppi distinti di questo tipo in generale.

Osservazione A.29 — Si poteva osservare da subito che $5\mathbb{Z} \times \mathbb{Z} < \mathbb{Z} \times \mathbb{Z}$ e $\frac{\mathbb{Z}\times\mathbb{Z}}{5\mathbb{Z}\times\mathbb{Z}} \cong \mathbb{Z}/5\mathbb{Z} \times \{\overline{0}\}$, dunque $[\mathbb{Z} \times \mathbb{Z} : 5\mathbb{Z} \times \mathbb{Z}] = 5$ e analogamente $\mathbb{Z} \times 5\mathbb{Z} < \mathbb{Z} \times \mathbb{Z}$, con $[\mathbb{Z} \times \mathbb{Z} : \mathbb{Z} \times 5\mathbb{Z}] = 5$. Il primo sottogruppo corrisponde a $\langle(\overline{0}, \overline{1})\rangle$, mentre il secondo a $\langle(\overline{1}, \overline{0})\rangle$, e in generale:

$$\langle(\overline{x}, \overline{y})\rangle \longleftrightarrow (x + 5\mathbb{Z}) \times (y + 5\mathbb{Z})$$

§B Complementi Sui Polinomi

§B.1 Criterio della derivata

Teorema B.1 (Criterio della Drivata)
Sia K un campo, e $f(x) \in K[x]$, $f(x)$, allora $(f(x), f'(x)) \neq 1$ se e solo se $\exists \alpha \in \overline{K}$ tale che $f(x) = (x-\alpha)^2 g(x) \in \overline{K}[x]$.[a]

[a] Ovvero $f(x)$ ha una radice almeno doppia, eventualmente in un'estensione del campo.

Dimostrazione. Proviamo le due affermazioni provando le contronominali:

- Supponiamo che $(f(x), f'(x)) = 1$, e proviamo che $f(x)$ non ha radici doppie. Per Bézout si ha che:
$$f(x)a(x) + f'(x)b(x) = 1$$
se per assurdo $f(x) = (x-\alpha)^2 g(x)$, allora $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. Si osserva che $f'(\alpha) = f(\alpha) = 0$, sostituendo $x = \alpha$ nell'identità di Bézout si ha:
$$0 = f(\alpha)a(\alpha) + f'(\alpha)b(\alpha) = 1$$
ma ciò è assurdo, quindi $f(x)$ non ha radici doppie. Avendo dimostrato la contronominale della prima affermazione, anche tale affermazione sarà vera, quindi se $f(x)$ ha radici doppie, allora $(f(x), f'(x)) \neq 1$.

- Supponiamo che $f(x)$ non abbia radici multiple e proviamo che $(f(x), f'(x)) = 1$. Se per assurdo $(f(x), f'(x)) \neq 1$, quindi $(f(x), f'(x)) = a(x)$, con $\deg a(x) > 0$, allora su $\overline{K}$ abbiamo:
$$f(x) = a(x)g(x) \in \overline{K}[x] \qquad \text{e} \qquad f'(x) = a(x)h(x) \in \overline{K}[x]$$
e sempre nella chiusura algebrica $\exists \beta \in \overline{K} : a(\beta) = 0$, da cui per Ruffini $x - \beta \mid a(x) \mid f(x)$ e $x - \beta \mid a(x) \mid f'(x)$. Pertanto:
$$f(x) = (x-\beta)j(x) \qquad \text{e} \qquad f'(x) = j(x) + (x-\beta)j'(x)$$
da cui $0 = a(\beta)h(\beta) = f'(\beta) = j(\beta) \implies x - \beta \mid j(x)$, ed infine $f(x) = (x-\beta)^2 l(x)$, ovvero $f(x)$ ha una radice doppia, ma ciò è assurdo, quindi deve essere $(f(x), f'(x)) = 1$, da cui la contronominale: $(f(x), f'(x)) \neq 1 \implies f(x)$ ha radici multiple.

□

§C Complementi Sulle Estensioni Di Campi

§C.1 Estensioni Quadratiche

Teorema C.1
Sia K un campo con $\operatorname{char} K \neq 2$ ed ${}^{L}\!/_{K}$ con $[L:K]=2$. Allora esiste $\alpha \in K$ tale che $L = K(\sqrt{\alpha})$, ovvero tutte le estensioni quadratiche si ottengono estraendo una radice quadrata.

Dimostrazione. Sia $\beta \in L \setminus K$, dunuque $K \subseteq K(\beta) \subseteq L$, e si osserva che $K(\beta) = L$, infatti:

$$1 < [K(\beta):K] \leq 2$$

dove $1 < [K(\beta):K]$ poiché $\beta \notin K$ e quindi non esiste un polinomio di grado 1 in $K[x]$ che si possa annullare in β, e d'altra parte, $[K(\beta):K] \leq 2$, poiché $K(\beta) \subseteq L$ (ed L ha grado dell'estensione 2). Da ciò segue che $[K(\beta):K]=2$ e quindi $K(\beta)=L$.
A questo punto si osserva che β^2 non può essere linearmente indipendente rispetto a $\{1,\beta\}$, in quanto $\dim_K K(\beta) = 2$ e quindi:

$$c_2\beta^2 + c_1\beta + c_0 = 0$$

con almeno un $c_i \in K$ non tutti nulli. Osserviamo che $c_2 \neq 0$, in tal caso si avrebbe che:

$$c_1\beta + c_0 = 0$$

ma c_1 non può essere nullo, altrimenti si otterrebbe che $c_1 = 0$ e quindi la relazione iniziale non era davvero di indipendenza lineare, assurdo. Dunque si ha:

$$\beta = -\frac{c_0}{c_1} \in K$$

ma ciò va contro l'ipotesi di $\beta \in L \setminus K$. Pertanto $c_2 \neq 0$, da cui:

$$\beta^2 + \frac{c_1}{c_2}\beta + \frac{c_0}{c_2} = 0$$

da cui, completando il quadrato:

$$\beta^2 + \frac{c_1}{c_2}\beta + \frac{c_1^2}{4c_2^2} - \frac{c_1^2}{4c_2^2} + \frac{c_0}{c_2} = 0 \implies \left(\beta + \frac{c_1}{2c_2}\right)^2 - \frac{c_1^2}{4c_2^2} + \frac{c_0}{c_2} = 0$$

dove si è utilizzato il fatto che $\operatorname{char} K \neq 2$, altrimenti le frazioni col 2 al denominatore non potrebbero esistere. Detto $\gamma = \beta + \frac{c_1}{2c_2}$, si ha:

$$K(\gamma) = K(\beta) (= L)$$

e ciò segue dal fatto che γ e β differiscono per definizione soltanto per un elemento del campo base, inoltre:

$$\gamma^2 = \frac{c_1^2}{4c_2^2} - \frac{c_0}{c_2} \in K$$

quindi per ottenere L si è aggiunta la radice quadrata di γ. □

Teorema C.2 (Estensioni Quadratiche Uguali)
Sia K un campo, con $\operatorname{char} K \neq 2$, e siano $\alpha, \beta \in K^*$, allora $K(\sqrt{\alpha}) = K(\sqrt{\beta})$ se e solo se $\alpha\beta$ è un quadrato in K.[a]

[a] Il teorema è equivalente se $\frac{\alpha}{\beta}$ è un quadrato.

Dimostrazione. Proviamo separatamente le due frecce:

- Se $\alpha\beta = t^2 \in K$, allora:
$$K(\sqrt{\beta}) = K(\sqrt{t^2/\alpha}) = K(1/\sqrt{\alpha}) = K(\sqrt{\alpha})$$
- Se $K(\sqrt{\alpha}) = K(\sqrt{\beta})$, supponiamo che $[K(\sqrt{\alpha}) : K] = 2$, allora $\{1, \sqrt{\alpha}\}$ è una K-base dello spazio vettoriale $K(\sqrt{\alpha})$, infatti si verifica l'indipendenza lineare dell'espressione:
$$x \cdot 1 + y \cdot \sqrt{\alpha} = 0 \qquad x, y \in K$$
dove:
$$\text{se} \quad y = 0 \implies x = 0$$
$$\text{se} \quad y \neq 0 \implies \sqrt{\alpha} = -\frac{x}{y} \in K$$
ma α non è un quadrato in K, da ciò segue che 1 e $\sqrt{\alpha}$ sono linearmente indipendenti e quindi sono una base di $K(\sqrt{\alpha})$. Per ipotesi $K(\sqrt{\alpha}) = K(\sqrt{\beta}) \implies \sqrt{\beta} \in K(\sqrt{\alpha})$ e quindi:
$$\exists x, y \in K : \sqrt{\beta} = x + y\sqrt{\alpha} \implies \beta = x^2 + 2xy\sqrt{\alpha} + \alpha y^2 \in K$$
riscrivendo la seconda espressione si ottiene:
$$(x^2 + \alpha y^2 - \beta) \cdot 1 + (2xy) \cdot \sqrt{\alpha} = 0$$
per la lineare indipendenza deve essere:
$$\begin{cases} x^2 + \alpha y^2 - \beta = 0 \\ 2xy = 0 \end{cases}$$
In particolare siamo in un campo, quindi per $2xy = 0$ ci sono tre possibilità: $2 = 0$, ma ciò non è vero se $\operatorname{char} K \neq 2$, $x = 0$, $y = 0$. Allora:
  - Se $y = 0$ si ha che, sostituendo nella prima equazione, $x^2 = \beta$, ma ciò è assurdo, perché allora $K(\sqrt{\beta}) = K \neq K(\sqrt{\alpha})$, ma $[K(\sqrt{\alpha}) : K] = 2$, mentre $[K(\sqrt{\beta}) : K] = 1$.
  - Se $x = 0$, allora $\beta = \alpha y^2 \implies \alpha\beta = (\alpha y)^2 \in (K^2)^*$.

□

Osservazione C.3 — Se $\alpha \in (K^2)^*$, ovvero α è un quadrato, allora $K(\sqrt{\alpha}) = K$ (perché le radici di α stanno già in K), pertanto se $K(\sqrt{\beta}) = K(\sqrt{\alpha}) \implies K(\sqrt{\beta}) = K \implies \sqrt{\beta} \in K$, cioè anche $\beta \in (K^2)^*$, ed ovviamente $\alpha\beta \in (K^2)^*$.

§C.2 Lemma Dei Gradi Delle Estensioni

Lemma C.4

Dato un campo K e due sue estensioni $K(\alpha)$, $K(\beta)$ con $[K(\alpha) : K] = m$ e $[K(\beta) : K] = n$, allora:

- $[K(\alpha, \beta) : K] \leq mn$.
- Se $(m, n) = 1$, allora $[K(\alpha, \beta) : K] = mn$.

Dimostrazione. Per il calcolo del grado di $K(\alpha, \beta)$ su K si può usare il Teorema Delle Torri, con una qualunque delle due estensioni iniziali:

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\beta)] \cdot \underbrace{[K(\beta) : K]}_{=n}$$

si osserva che $[K(\alpha, \beta) : K(\beta)] = \deg \mu_{\alpha/K(\beta)}(x)$, invece, per ipotesi, sappiamo che esiste $\mu_{\alpha/K}(x)$, con $\deg \mu_{\alpha/K}(x) = m$, segue che $\mu_{\alpha/K}(x) \in K(\beta)[x]$, pertanto è divisibile per il polinomio minimo di α su questo campo che è una sua estensione:

$$\mu_{\alpha/K(\beta)}(x) \mid \mu_{\alpha/K}(x) \implies \deg \mu_{\alpha/K}(x) \leq m$$

ovvero $[K(\alpha, \beta) : K(\beta)] \leq m$, da cui $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\beta)] \cdot [K(\beta) : K] \leq mn$. Applicando il Teorema Delle Torri sia usando $K(\alpha)$ che $K(\beta)$ segue che:

$$[m, n] \mid [K(\alpha, \beta) : K] \implies [m, n] \leq [K(\alpha, \beta) : K]$$

essendo per ipotesi $(m, n) = 1 \implies [m, n] = mn \implies mn \leq [K(\alpha, \beta) : K]$, infine, per quanto visto nel primo punto $[K(\alpha, \beta) : K] \leq mn$ e quindi esattamente $[K(\alpha, \beta) : K] = mn$. □

Osservazione C.5 — In generale $[m, n] \mid [K(\alpha, \beta) : K]$ e quindi è sempre vero che $[m, n] \leq [K(\alpha, \beta) : K] \leq mn$.