Appunti di Aritmetica

Ludovico Piazza

Anno Accademico 2019-2020

1 Aritmetica

Assioma del buon ordinamento o principio del minimo.
Ogni sotto insieme non vuoto di $\mathbb{N}$ ammette un minimo, cioè:

$$\forall S \subseteq \mathbb{N},\ S \neq \emptyset,\ \exists m_0 \in S \mid m_0 \leq s, \forall s \in S.$$

2 Teoria dei Gruppi

Proposizione 2.1. ***Condizioni di un sottogruppo***
Sia $H \subset G, H \neq \varnothing$. Allora $H < G$ se e solo se:

1. $\forall a, b \in H, ab \in H$; *(chiusura rispetto all'operazione)*
2. $\forall a \in H, a^{-1} \in H$. *(esistenza dell'inverso)*

Proposizione 2.2. ***Intersezione di sottogruppi***
$\forall H, K < G,\ H \cap K < G$.
Osservazione: $H \cup K$ non è necessariamente un sottogruppo di G.

2.1 Gruppi Ciclici

Proposizione 2.3. $\forall x \in G, \langle x \rangle < G$.

Teorema 2.1. ***Sottogruppi di gruppi ciclici***
Ogni sottogruppo di un gruppo ciclico è ciclico.

2.1.1 Il gruppo $\mathbb{Z}/n\mathbb{Z}$

Osservazione 2.3.1. *Ogni* $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$.

Proposizione 2.4. $\forall [a]_n \in \mathbb{Z}/n\mathbb{Z}$ *(NdS è il gruppo con +) si ha:*

$$\mathrm{ord}([a]_n) = \frac{n}{(a,n)}.$$

Corollario 2.4.1. $\forall [a]_n, d = \mathrm{ord}[a]_n$ *si ha che* $d|n$.
Più in particolare $\forall d|n$ *esistono esattamente* $\Phi(d)$ *elementi di ordine* d.

Corollario 2.4.2. *Sia* $H < \mathbb{Z}/n\mathbb{Z}$, $|H| = d \Rightarrow d|n$. *Inoltre* $\forall d|n$ *esiste un solo sottogruppo* H *di ordine* d, *cioè* $H = \langle [\frac{n}{d}]_n \rangle$.

Corollario 2.4.3. $\forall n \in \mathbb{N}, n = \sum_{d|n} \Phi(d)$

2.2 Omomorfismi

Proposizione 2.5. *Dato $f : G \to G'$ omomorfismo:*

1. $f(e) = e'$; *(identità)*
2. $f(x^{-1}) = (f(x))^{-1}$; *(inverso)*
3. $H < G \Rightarrow f(H) < G'$, $K < G' \Rightarrow f^{-1}(K) < G$; *(sottogruppi in sottogruppi)*
4. Im $f < G'$ $\quad e \quad$ Ker $f < G$ *(immagine e nucleo)*
5. f *iniettiva* $\Leftrightarrow$ Ker $f = e$. *(iniettività)*

Proposizione 2.6. ***Ordine dell'immagine***
$\forall x \in G$ *si ha* ord $f(x) \mid$ ord x.
Inoltre $\forall x,\ f$ *iniettiva* $\Leftrightarrow$ ord $f(x) =$ ord x.

Teorema 2.2. ***Sottogruppi di gruppi ciclici***
Sia G un gruppo ciclico allora:

1. *Se G è infinito, $G \cong \mathbb{Z}$;*
2. *Se $|G| = n$, $G \cong \mathbb{Z}/n\mathbb{Z}$.*

2.3 Prodotto diretto

Proposizione 2.7. ***Ordine degli elementi***
ord $(x, y) = [\text{ord } x, \text{ord } y]$.

Teorema 2.3. ***III Forma del Teorema Cinese del Resto***
$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \ \cong\ \mathbb{Z}/nm\mathbb{Z} \ \Leftrightarrow\ (m, n) = 1$.

Corollario 2.7.1. *Siano $n, m \geq 2,\ (n, m) = 1$, allora:*

$$(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/nm\mathbb{Z})^*.$$

2.4 Classi laterali e gruppi normali

Dato $H < G$ definiamo la relazione $\sim_H$ in maniera tale che

$$x \sim_H y \ \Leftrightarrow\ y^{-1}x \in H.$$

$\sim_H$ è una **relazione d'equivalenza**.
Le classi di equivalenza di $\sim_H$ sono **classi laterali sinistre**.

Osservazione 2.7.1. *Se $G = \mathbb{Z}$ e $H = n\mathbb{Z}$ allora $G/\sim_H \ \cong\ \mathbb{Z}/n\mathbb{Z}$.*

Teorema 2.4. ***Teorema di Lagrange***
Dato $H < G$, allora: $|H| \ \mid\ |G|$.

Corollario 2.7.2.

1. $\forall x \in G, \quad \text{ord } x \ \mid\ |G|$;
2. $\forall x \in G, \quad x^{|G|} = e.$ *(generalizzazione del teorema di Eulero)*

Corollario 2.7.3. ***Gruppi di ordine primo***
Sia G un gruppo e $|G| = p$ con p primo, allora G è ciclico e in particolare: $G \cong \mathbb{Z}/p\mathbb{Z}$.

2.5 Sottogruppi Normali e Gruppo Quoziente

Il sottogruppo H si dice normale in G se e solo se

$$\forall x \in G: \ H < G, \ xH = Hx$$

e si scrive $H \triangleleft G$.

Osservazione 2.7.2. ***Definizione equivalente di normalità***
$H \triangleleft G \ \Leftrightarrow \ \forall x \in G: \ xHx^{-1} \subset H.$

Proposizione 2.8. ***Particolarita del nucleo di un omomorfismo***
Dato $f : G \to G'$ omomorfismo:

1. $\mathrm{Ker} f \trianglelefteq G$: *(normalità del nucleo)*
2. $\forall x, y \in G$: *(= img., = classe laterale $\sim_{\mathrm{Ker} f}$)*
   $f(x) = f(y) \Leftrightarrow x \cdot \mathrm{Ker} f = y \cdot \mathrm{Ker} f$;
3. $\forall z \in \mathrm{Im} f$: *(classi laterali $\sim_{\mathrm{Ker} f}$ come controimmagini)*
   $z = f(x) \ \Rightarrow \ f^{-1}(z) = x \cdot \mathrm{Ker} f.$

Se $N \trianglelefteq G$ posso definire una struttura di gruppo su G/N.
G/N è un **gruppo quoziente**. $\mathbb{Z}/n\mathbb{Z}$ è il gruppo quoziente rispetto a $\mathbb{Z}$.

Proposizione 2.9. ***Nucleo della proiezione al gruppo quoziente***
Data la proiezione $\pi_n : G \to G/N, \ x \to xN$

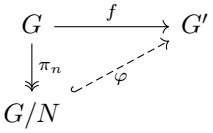
$$\mathrm{Ker}\pi_n = N.$$

Corollario 2.9.1. ***Corrispondenza tra sottogruppi normali e nuclei di omomorfismi***
I sottogruppi normali di G sono tutti e soli i nuclei degli omomorfismi definiti su G.

2.5.1 Teoremi di omomorfismi e conseguenze

Teorema 2.5. ***I Teorema di Omomorfismo***
$f : G \to G'$ omomorfismo di gruppi e $N \trianglelefteq G, N \subset \mathrm{Ker} f$ allora:

$\exists$ omomorfismo $\varphi : G/N \to G'$ tale che $f = \varphi \circ \pi_n$.



Commento: ogni omomorfismo si può fattorizzare in un omomorfismo surgettivo (π) ed uno iniettivo (φ).

Corollario 2.9.2. ***Immagine e nucleo di φ***
$\mathrm{Im}\varphi = \mathrm{Im} f$ *(infatti se f è surgettiva, φ è un isomorfismo)*
$\mathrm{Ker}\varphi = \mathrm{Ker} f/N$

Teorema 2.6. ***II Teorema di Omomorfismo***
Dato G gruppo, $H, K \trianglelefteq G$, $H \subseteq H$:

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

Teorema 2.7. ***III Teorema di Omomorfismo***
Siano $H, K \trianglelefteq G$ allora:

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

Teorema 2.8. ***Teorema di Corrispondenza tra sottogruppi***
Dati G gruppo, $N \trianglelefteq G$, $\pi_n : G \to G/N$ proiezione π_n induce una corrispondenza biunivoca tra i ***sottogruppi di G/N*** *e i* ***sottogruppi di G che contengono N****.*

*Inoltre, questa biezione conserva l'****indice di sottogruppo*** *e la* ***normalità*** *per ogni elemento.*