Appunti delle esercitazioni di Lombardo

Ludovico Piazza

Anno Accademico 2019-2020

1 Aritmetica, combinatoria e congruenze

W.I.P.
...

2 Gruppi

2.1 Criterio per sottogruppi ($H \leq G$)

Se G infinito allora dobbiamo verificare che:

1. H non sia vuoto;
2. H sia chiuso per l'operazione;
3. $\forall h \in H : \exists h^{-1} \in H$.

Invece G finito $\Rightarrow$ il punto 3. è superfluo.

2.2 Sottogruppi prodotti da altri sottogruppi

Dati G e $H, K \leq H$ allora:

$$HK \leq G \Leftrightarrow HK = KH$$

2.3 Gruppi abeliani

$f : G \to G,\ g \to g^2$ omomorfismo $\Leftrightarrow G$ abeliano.

Corollario: $\forall g \in G : g^2 = \mathrm{id} \Leftrightarrow G$ abeliano.

2.4 Centro di $G_1 \times G_2$

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

2.5 Teorema di Cauchy (dimostrato per p=2 e gruppi abeliani)

Sia G un gruppo finito e p un primo tale che $p \mid |G|$. Allora $\exists g \in G : \text{ord}(g) = p$.

Più in particolare $p = 2 \Rightarrow \#\{g \in G \text{ di ordine } 2\} \equiv |G| + 1 \pmod 2$.

Lemma importante: $\frac{G}{Z(G)}$ ciclico $\Longrightarrow G$ abeliano.

2.6 Sottogruppi normali

Tutti i sottogruppi $H < G$ di indice 2, $Z(G) \trianglelefteq G$

2.7 Omomorfismi tra gruppi ciclici

- $\text{Hom}(\mathbb{Z}, G) \longleftrightarrow G$ bigezione di insiemi. Ogni omomorfismo, infatti, è esclusivamente determinato dal valore $f(1)$ ed esso può essere qualsiasi tra gli elementi di G.
- $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, Z) = \{f\} \qquad \text{con } \forall g \in \mathbb{Z}/n\mathbb{Z} : f(g) = 0.$
- $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{x \to ax : a \in \mathbb{Z}/m\mathbb{Z}, \quad a \equiv 0 \pmod{\frac{m}{(n,m)}}\}$. In totale sono (n, m) proprio come i possibili $a < n$ che risolvono la congruenza.

2.8 Automorfismi di G

- $\text{Aut}(\mathbb{Z}) = \{\text{id}, \ x \to -x\} \cong \mathbb{Z}/2\mathbb{Z}$
- $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$

2.9 Sottogruppi generati da un insieme S

1. $S = \{g\} \Longrightarrow \langle S \rangle = \langle g \rangle$
2. G abeliano $\Longrightarrow \langle S \rangle = \{g^n h^m \mid n, m \in \mathbb{Z}\}$
3. G non abeliano $\Longrightarrow \langle S \rangle = \{g^{n_1} h^{m_1} g^{n_2} h^{m_2} ... \ g^{n_r} h^{m_r} \mid n_i, m_i \in \mathbb{Z}, \ r \in \mathbb{N}\}$

2.10 Sottogruppi di $(\mathbb{Z}/p\mathbb{Z})^k$

Gli elementi di questo gruppo hanno ordine 1 o $p \Rightarrow$ i sottogruppi ciclici di ordine p sono:

$$\frac{p^k - 1}{\varphi(p)} = \frac{p^k - 1}{p - 1} = p^{k-1} + p^{k-2} + ... + 1.$$

Anche i sottogruppi (non ciclici) di ordine p^{k-1} sono $\frac{p^k - 1}{p-1}$.

2.11 Ciclicità e gruppo quoziente

Dati G abeliano, H ciclico e $\frac{G}{H}$ ciclico, $(\ |G| \ , \ |\frac{G}{H}| \ ) = 1 \Longrightarrow G$ è ciclico.

Lemma utile: dati $a, b \in G, \text{ord}(a) = m, \ \text{ord}(b) = n$ con $(m, n) = 1 \Longrightarrow \ \text{ord}(a+b) = mn$.

2.12 Ordini di elementi in un gruppo abeliano

Dati G un gruppo abeliano finito e $\mathcal{O} = \{\text{ord } x \mid x \in G\}$.

1. $n \in \mathcal{O}, \ d \mid n \Rightarrow d \in \mathcal{O}$
2. $m, n \in \mathcal{O} \Rightarrow \text{mcm}(m, n) \in \mathcal{O}$
3. $\max \mathcal{O} = \underset{m \in \mathcal{O}}{\text{mcm}} \ m$

2.13 $(\mathbb{Z}/p^k\mathbb{Z})^*$

Fatto importante: $(\mathbb{Z}/p\mathbb{Z})^*$ è ciclico.
Se p dispari e $k \geq 1$ allora $(\mathbb{Z}/p^k\mathbb{Z})^*$ è ciclico.

2.14 Congruenze $x^k \equiv 1 \ (\mod p^e \ )$

Se p dispari oppure $p = 2$ e $e \leq 2$ allora la congruenza ha $(k, \ \varphi(p^e))$ soluzioni.

3 Campi

3.1 Estensioni quadratiche

Dati F, K campi con char $\neq 2$ e $[F : K] = 2$ allora:

$$\exists \beta \in F : \ \beta^2 \in K, \ F = K(\beta).$$

(**Osservazione:** $\forall \gamma \in F \setminus K, \ K(\gamma) = F$.)

Più in particolare se considero $\mu_\beta(x) = x^2 + b_1 x + b_0$ allora $(\beta + \frac{b_1}{2})^2 \in K$
Fatto: $K(\sqrt{a}) = K(\sqrt{b}) \Leftrightarrow \exists c \in K^\times : b = a \cdot c^2$