

# 1 Gruppi

## 1.1 Definizioni base

**Def** un *magma* è un insieme  $M$  in cui è definita una singola operazione binaria. L'unico assioma soddisfatto dall'operazione è quello di chiusura.

**Def** un magma associativo si dice *semigrupp*

**Esempio**  $(\mathbb{Z}^+, +)$ ,  $(\mathbb{N}, \times)$

**Def** un *monoide* è una terna  $(M, *, e)$  dove  $M$  è un insieme chiuso rispetto a  $*$  che è un'operazione associativa con elemento neutro  $e$ . Un monoide quindi è un semigrupp con elemento neutro

**Esempio**  $(\mathbb{Z}, \times)$

**Def** un *grupp* è una terna  $(G, *, 1)$  dove  $(G, *, 1)$  è un monoide in cui ogni elemento è invertibile

## 1.2 Sottogruppo normale

**Def:** Sia  $H$  sottogruppo di  $G$ ,  $H$  si dice normale

$H \triangleleft G$  se  $ghg^{-1} \in H \quad \forall g \in G, h \in H$

Esempio:  $K \triangleleft H \triangleleft G$  non è detto che  $K \triangleleft G$  (vd esempio wiki)

## 1.3 Gruppi abelianizzati e commutatori

**Def.**  $[g, h] := g^{-1}h^{-1}gh$  commutatore

$[H, K] = \{[h, k] : h \in H, k \in K\}$  per  $H, K \subset G$

**Def:** il gruppo  $[G, G]$  viene detto sottogruppo dei commutatori

**Oss.** un elemento di  $[G, G]$  non è per forza della forma  $[g, h]$

**Lemma:**  $[G, G] \triangleleft G$

**Oss.**  $G$  è abeliano  $\iff [G, G] = \{1\}$

**Lemma:** sia  $N$  un sottogruppo normale di  $G$ , allora

$G/N$  è abeliano  $\iff [G, G] \triangleleft N$  ovvero il sottogruppo dei commutatori

è il piu' piccolo sottogruppo normale di  $G$

$Ab(G) = G/[G, G]$  abelianizzato

$G \simeq G' \Rightarrow Ab(G) \simeq Ab(G')$  ma non viceversa

## 1.4 Gruppo risolubile

Def. Un gruppo  $G$  è detto risolubile se esiste una sequenza di sottogruppi

$$G = G_1 \supset G_2 \supset \dots \supset G_m = \{1\}$$

tale che

- $G_{k+1} \triangleleft G_k$
- $G_k/G_{k+1}$  è abeliano

Esempio:  $S_3$  è risolubile

Def: sia  $G$  un gruppo, poniamo

- $G^{(1)} = G$
- $G^{(k+1)} = [G^{(k)}, G^{(k)}]$

La serie

$$G = G^{(1)} \supset G^{(2)} \supset \dots \supset G^{(k)}$$

viene detta serie derivata.

Thm: sia  $G$  un gruppo. Allora  $G$  è risolubile  $\iff \exists m > 0$  t.c.  $G^{(m)} = \{1\}$

## 1.5 Gruppo ciclico

È un gruppo che può essere generato da un unico elemento.

Sia  $G$  ciclico. Se  $|G| = n$  finito allora  $G \simeq \mathbb{Z}/n\mathbb{Z}$  altrimenti  $G \simeq \mathbb{Z}$

$g^i$  genera  $\iff (i, n) = 1$

Oss. un gruppo ciclico è abeliano

**Prop.** Ogni sottogruppo ed ogni gruppo quoziente di un gruppo ciclico è ciclico.

$G = \{g^n : g \in \mathbb{Z}\}$  notazione moltiplicativa

$G = \{ng : n \in \mathbb{Z}\}$  notazione additiva

**Thm** ogni sottogruppo finito  $G$  del gruppo moltiplicativo di un campo  $E$  è ciclico.

**Prop** sia  $G$  un gruppo ciclico finito,  $a \in G$  allora

$x^n = a$  in  $G$  ha soluzioni  $\iff a^{\frac{|G|}{(n, |G|)}} = 1$

**Oss** se  $G$  è un gruppo finito e  $(n, |G|) = 1$  allora  $x^n = a$  ha soluzione in  $G$   
 $\forall a \in G$

### 1.5.1 Radici n-esime dell'unità

$R_n = \{\alpha \in \mathbb{C} : \alpha^n = 1\}$  radici n-esime dell'unità

Def n-esimo polinomio ciclotomico

$$\Phi_n = \prod_{\zeta \in RPU} (x - \zeta)$$

Lemma:

$$\prod_{d|n} \Phi_d = x^n - 1$$

Lemma:  $\Phi_n$  è un polinomio monico di  $\mathbb{Z}[X]$  e ha grado  $\varphi(n)$

Thm:  $\Phi_n$  è irriducibile in  $\mathbb{Q}[X]$

Def: sia  $F$  un campo e  $w \in F$  una radice primitiva  $n$ -esima dell'unità, allora  $F(w)/F$  è detta  $n$ -esima estensione ciclotomica di  $F$

Def: un'estensione di Galois  $E/F$  è detta ciclica se  $\text{Gal}(E/F)$  è un gruppo ciclico

## 1.6 Gruppo di torsione

Un gruppo di torsione o gruppo periodico è un gruppo in cui ogni elemento ha ordine finito. Tutti i gruppi finiti sono di torsione.

Il concetto di gruppo di torsione non va confuso con quello di gruppo ciclico:  $(\mathbb{Z}, +)$  è ciclico senza essere di torsione.

$\text{Tor}(G) = \{ g \in G : g^n = 1 \}$  notazione moltiplicativa

$\text{Tor}(G) = \{ g \in G : ng = 0 \}$  notazione additiva

Sia  $\varphi : G \rightarrow G'$  isomorfismo allora

$\varphi(\text{Tor}(G)) = \text{Tor}(G')$

## 1.7 Gruppo diedrale

Gli elementi base del gruppo sono le rotazioni del poligono pari all' $n$ -esima parte dell'angolo giro, e la riflessione attorno ad un asse di simmetria del poligono. Esistono in tutto  $n$  rotazioni possibili e  $n$  assi di simmetria per un poligono di  $n$  lati, per cui il gruppo diedrale corrispondente è formato da  $2n$  elementi.

Esempio: quadrato

$$\langle x, y | x^4 = y^2 = (xy)^2 = 1 \rangle$$

## 1.8 Esempi

### Gruppi comuni

$(\mathbb{Z}, +), (\mathbb{Q}^*, \times)$

$S_n$  gruppo delle permutazioni, non è abeliano

### Il gruppo simmetrico $S_n$

Sia  $S_n$  l'insieme di tutte le mappe biettive da

$$\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

$\pi \in S_n$  è detta permutazione di  $\{1, 2, \dots, n\}$

Oss.  $|S_n| = n!$

Lemma:  $S_n$  è generato da  $(1, 2), (1, 3), \dots, (1, n)$

Lemma:  $S_n$  è generato da  $(1, 2)$  e  $(1, 2, \dots, n)$

Def: una coppia  $(i, j)$  è detta inversione della permutazione  $\pi$  se  $\pi(i) > \pi(j)$ . Denotiamo con  $\varphi(n)$  il numero di inversioni di una permutazione.

Lemma:  $\varphi(\pi\sigma) = \varphi(\pi) + \varphi(\sigma) \pmod{2}$

Prop. in ogni rappresentazione di  $\pi$  come prodotto di 2-cicli, il numero di 2-cicli sarà sempre pari o sempre dispari.

Oss. il prodotto di due permutazioni pari è ancora pari e l'inverso di una permutazione pari è ancora pari.

Def: l'insieme delle permutazioni pari forma un sottogruppo di  $S_n$  detto gruppo alterno  $A_n$

Lemma:  $A_n$  è generato dai 3-cicli  $(i, j, k)$  per  $i, j, k$  distinti

Prop.  $A_n \triangleleft S_n$ ,  $S_n/A_n \simeq \{1, -1\}$ , segue che  $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$

Thm:  $[S_n, S_n] = A_n$

### Gruppo generale lineare

$GL_n(K)$  gruppo generale lineare: matrici invertibili di dimensione  $n$  a valori in  $K$

$SL_n(K)$  gruppo lineare speciale: sottogruppo delle matrici avente determinante uguale a 1

Oss. non sono commutativi per  $n > 1$

Oss.  $SL_n(K) \triangleleft GL_n(K)$  (sottogruppo normale, vd thm Binet)

$O_n(K) = \{A \in GL_n(K) | A^T A = A A^T = I\}$  gruppo ortogonale

$SO_n(K)$  gruppo ortogonale speciale (gruppo delle rotazioni dello spazio)

### Gruppo di Galois

Sia  $E/F$  estensione di campi

$Gal(E/F) = \{\sigma : E \rightarrow E : \sigma \text{ automorfismo t.c. } \sigma(a) = a \forall a \in F\}$

### Gruppo fondamentale

$\pi(X, x_0)$  è un gruppo rispetto al cammino prodotto di classi di equivalenza di cappi omotopi con punto base  $x_0$

$H_q(C) := Z_q(C)/B_q(C)$   $q$ -esimo gruppo di omologia

dove  $Z_q(C) := \ker \delta_q$  e  $B_q(C) := \text{Im} \delta_{q+1}$

## 2 Teoremi sui gruppi e congruenze

**Def.** funzione di Eulero  $\varphi(n) = \#U(\mathbb{Z}/n\mathbb{Z}) = \{a \in \mathbb{Z} : 0 \leq a < n, (a, n) = 1\}$

**Lemma:** se  $p$  è primo  $\varphi(p) = p - 1$

**Prop.**  $\varphi(p^k) = p^k - p^{k-1}$

**Thm.** se  $(m, n) = 1$  allora  $\varphi(mn) = \varphi(m)\varphi(n)$

**Prop.**  $\sum_{d|n} \varphi(d) = n$

### Teorema di Lagrange

Sia  $G$  un gruppo finito e  $H$  un suo sottogruppo,  $|G : H|$  l'indice di  $H$  in  $G$  (il numero di classi laterali di  $H$  in  $G$ ) allora  $|G| = |H||G : H|$

Corollario: il periodo di  $a \in G$  divide l'ordine di  $G$

### Teorema di Eulero Fermat

Se  $(a, n) = 1$  allora  $a^{\varphi(n)} \equiv 1 \pmod{n}$

### Piccolo teorema di Fermat

$a^p \equiv a \pmod{p}$

### Teorema di Wilson

$(p-1)! \equiv -1 \pmod{p}$

**Prop.** se  $p \equiv 1 \pmod{4}$  allora  $-1$  è un quadrato mod  $p$  ovvero  $\exists x$  t.c.  $x^2 \equiv -1 \pmod{p}$

**Prop.** se  $p = 2^n + 1$  è un primo allora  $3$  è una radice primitiva mod  $p$

## 2.1 Gruppo degli elementi invertibili

**Prop.**  $(1 + ap)^{p^{\beta-2}} \equiv 1 + ap^{p^{\beta-1}} \pmod{p^{\beta}}$

**Lemma:** sia  $p > 2$  primo e  $a$  un intero non multiplo di  $p$ .

Allora  $1 + ap$  ha ordine  $p^{\alpha-1} \pmod{p^{\alpha}}$

**Lemma:** se  $a$  non è multiplo di  $2$  la classe resto  $1 + 4a \pmod{2^{\alpha}}$  ha ordine  $2^{\alpha-2}$

Oss. è la versione del lemma precedente per  $p = 2$

**Prop** il gruppo  $U(\mathbb{Z}/p^{\alpha}\mathbb{Z})$  è ciclico per  $p > 2$  primo

**Teorema**  $U(\mathbb{Z}/m\mathbb{Z})$  è ciclico se e solo se  $m = 2, 4, p^k, 2p^k$

**Prop.** Supponiamo esista una radice primitiva mod  $m$  con  $(a, m) = 1$

Allora  $a$  è una potenza  $n$ -esima (cioè  $x^n \equiv a \pmod{m}$  ha soluzione)  $\iff$

$a^{\frac{\varphi(m)}{(n, \varphi(m))}} \equiv 1$

Oss. deriva dalla proposizione più generale sui gruppi ciclici

**Prop.** sia  $p > 2$  primo,  $p \nmid a, p \nmid n$ , se  $x^n \equiv a \pmod{p}$  è risolubile allora anche  $x^n \equiv a \pmod{p^e}$  è risolubile  $\forall e \geq 1$

## 2.2 Legge di reciprocità quadratica

**Def.** di resto quadratico e simbolo di Legendre

**Prop. di Eulero**  $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$

**Corollario**  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ ,  $\left(\frac{1}{p}\right) = 1$ ,  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

**Legge accessoria**

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}$$

cioè 1 se  $p \equiv \pm 1 \pmod{8}$ ,  $-1$  se  $p \equiv \pm 3 \pmod{8}$

**Teorema (Legge di reciprocità quadratica)**

$$\left(\frac{p}{q}\right) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

Che si può riformulare come:  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$  se  $p, q \equiv -1 \pmod{4}$ , 1 altrimenti

**Def** somma di Gauss

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$$

Oss di fatto è il prodotto fra un carattere moltiplicativo e uno additivo

**Lemma**

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$$

**Lemma** se  $p \nmid a$

$$\sum_{t=0}^{p-1} \zeta^{at} = 0$$

Oss sono riconducibili al caso più generale:

**Lemma**  $\sum_{g \in G} \chi(g) = 0$  se  $\chi$  non è il carattere banale

**Prop**  $g_a = \left(\frac{a}{p}\right) g_1$

**Prop**  $g_1^2 = (-1)^{\frac{p-1}{2}} p$

### 3 Numeri di Mersenne, Fermat e Carmichael

**Def**  $M_p = 2^p - 1$  è detto numero di Mersenne

**Def**  $F_n := 2^{2^n} + 1$  è detto numero di Fermat

**Def**  $p$  si dice *elite prime* se è una radice primitiva modulo tutti i primi di Fermat salvo un numero finito

**Teorema di Pepin**  $F_n$  è primo  $\iff 3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

#### 3.1 Divisori della forma $b^n \pm 1$

**Prop**  $b, n > 1$  interi. Se un primo  $p | b^n - 1$  allora o  $p | b^d - 1$  per un divisore proprio  $d$  di  $n$  o  $p \equiv 1 \pmod{n}$

**Prop**  $b, n > 1$  interi. Se un primo  $p > 2, p | b^n + 1$  allora o  $p | b^d + 1$  per un divisore proprio  $d$  di  $n$  con  $\frac{n}{d}$  dispari o  $p \equiv 1 \pmod{2n}$

**Prop** un divisore primo  $p$  di  $F_k$  con  $k > 1$  soddisfa  $p \equiv 1 \pmod{2^{k+2}}$

## 4 Anelli

### 4.1 The ring of integers

The rings of integers of number fields may be divided in several classes:

- Quelli che non sono PID e quindi non sono domini Euclidei come  $\mathbb{Q}[\sqrt{-5}]$
- Quelli che sono PID e non sono domini Euclidei come  $\mathbb{Q}[\sqrt{-19}]$
- Quelli che sono Euclidei ma non norm-Euclidean come  $\mathbb{Q}[\sqrt{69}]$
- Quelli che sono norm-Euclidean come gli interi di Gauss (gli interi di  $\mathbb{Q}[\sqrt{-1}]$ )

The norm-Euclidean quadratic fields have been fully classified, they are  $\mathbb{Q}[\sqrt{d}]$  where  $d$  is:

-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73

### 4.2 Gli interi algebrici

**Prop.** i numeri algebrici formano un campo

**Prop.** gli interi algebrici formano un anello

**Prop.** un numero complesso è un intero algebrico sse il suo polinomio minimo su  $\mathbb{Q}$  ha coefficienti interi.

**Thm** se  $D \equiv 2, 3 \pmod{4}$  allora  $\mathbb{Q}(\sqrt{D}) = \mathbb{Z}[\sqrt{D}]$

se  $D \equiv 1 \pmod{4}$  allora  $\mathbb{Q}(\sqrt{D}) = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$

### 4.3 Ideale

**Def.** sia  $A$  un anello,  $I \subset A$  si dice **ideale** di  $A$  se

- 1)  $I$  è sottogruppo di  $(A, +, \times)$
- 2)  $x \in I$  e  $a \in A$  allora  $ax, xa \in I$

**Def.** se un ideale è generato da un solo elemento diciamo che è principale

**Oss.** Un ideale che sia contemporaneamente destro e sinistro si dice ideale **bilatero**. Nel caso particolare in cui  $A$  sia un anello commutativo le nozioni date coincidono e parliamo semplicemente di ideale.

**Def.** un ideale si dice **proprio** se è un sottoinsieme proprio di  $A$  cioè non coincide con  $A$ .

**Def.** Un ideale proprio è un ideale **massimale** se non è contenuto strettamente in nessun altro ideale proprio

**Oss.** Gli ideali massimali sono pertanto caratterizzati dalla proprietà di essere contenuti solamente in due ideali: l'intero anello e l'ideale massimale stesso

**Def.** un ideale proprio è detto ideale **primo** se  $\forall ab \in I$  allora  $a$  o  $b$  appartengono a  $I$ . **Proprietà** L'anello quoziente  $A/I$  è un dominio  $\iff I$  è un ideale primo

L'anello quoziente  $A/I$  è un campo  $\iff I$  è un ideale massimale **Operazioni sugli ideali**  $I + J = \{a + b | a \in I, b \in J\}$

$IJ = \{a_1b_1 + \dots + a_nb_n | a_i \in I, b_i \in J, i = 1, \dots, n \text{ per } n = 1, 2, \dots\}$



Osservazioni:

$$IJ \subset I \cap J$$

$$I \cup J \subset I + J$$

$I \cap J$  è ancora un ideale mentre  $I \cup J$  non sempre

#### 4.4 Domini

Un dominio è un anello commutativo con unità in cui vale la legge di annullamento del prodotto

Su un dominio è definita una funzione Norma

**Oss.**  $\varepsilon$  è invertibile  $\implies N(\varepsilon) = 1$

se vale anche l'altra implicazione la norma si dice *speciale* **Dominio Euclideo**  
È un dominio dotato di una norma in cui è possibile fare la divisione con resto.

##### Definizione (1)

Un dominio  $R$  è euclideo se  $\exists d : R \rightarrow \mathbb{N}$  t.c.  $\forall a, b \in R, b \neq 0 \exists q, r \in R$  t.c.

$$a = bq + r$$

$$d(r) < d(b)$$

##### Definizione (2)

Come (1) però con  $d(a) \leq d(ab)$

Oss. dato un dominio euclideo  $R$  si dimostra che se ne può modificare la norma  $d$  in modo che soddisfi (2)

##### Definizione (3)

Come (1) però con  $d(ab) = d(a)d(b)$

##### Definizione (4)

Limitatamente a un number ring (anello degli interi algebrici) in un number field ci si può chiedere se vale (3) con  $d$  la norma ordinaria cioè  $N_{\mathbb{K}/\mathbb{Q}}$

Se questo vale si dice che  $R$  è *norm-Euclidean*

**Lemma:** la norma di un dominio euclideo è speciale

**Oss.** in un dominio euclideo primo = irriducibile

**Thm** ogni dominio euclideo è un PID

**Thm** ogni dominio euclideo è un UFD

#### 4.5 PID

A si dice PID (Principal ideal domain) se è un dominio in cui ogni ideale di  $A$  è principale.

**Thm** PID  $\implies$  UFD

**Def** un PID si dice **Noetheriano** se soddisfa la ACC (condizione sulle catene ascendenti) ovvero ogni catena ascendente di ideali

$$(a_1) \subseteq (a_2) \subseteq \dots$$

è stazionaria cioè esiste un indice  $k$  t.c.  $(a_k) = (a_{k+1}) = \dots$

**Esempio** PID che non è un dominio euclideo:  $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$

## 4.6 UFD

**Def.** un dominio si dice a fattorizzazione unica se ogni elemento non nullo e non invertibile di  $D$

1) si scrive come prodotto di irriducibili

2) i fattori irriducibili di due fattorizzazioni sono gli stessi con le stesse molteplicità e a meno di associati

**Esempio:** UFD che non è un PID

1)  $K[X, Y]$ : l'ideale generato da  $(x, y)$  non è principale

2)  $Z[X]$ : l'ideale generato da  $(2, x)$  non è principale

**Prop.** se  $D$  è un UFD  $\implies D[X]$  è un UFD

## 5 Campi

### 5.1 Norma e Traccia

**Def.** the (field) norm maps elements of a larger field into a subfield

Sia  $E/F$  un'estensione di Galois di grado finito, allora la norma e la traccia sono definite rispettivamente come

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$$

$$Tr(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$$

**Prop.** sia  $G = \text{Gal}(E/F)$ , e  $H = \{\sigma \in G | \sigma(\alpha) = \alpha\}$  lo stabilizzatore di  $\alpha$  e  $f = x^m + a_{m-1}x^{m-1} + \dots + a_0$  sia il polinomio minimo di  $\alpha$  su  $F$ . Allora:

$$N(\alpha) = (-1)^{|G|} a_0^{|H|}$$

$$Tr(\alpha) = -|H| a_{m-1}$$

### 5.2 Estensioni

Sia  $E/F$  un'estensione algebrica

**Estensione di Galois** sia  $E^G := \{a \in E | \sigma(a) = a \forall \sigma \in G\}$  dove  $G = \text{Gal}(E/F)$   
 $E^G = F$

**Estensione normale** se ogni polinomio irriducibile in  $F[X]$  che ha una radice in  $E$  ha tutte le radici in  $E$ .

**Estensione separabile** se il polinomio minimo di ogni  $\alpha \in F$  è separabile

**Estensione ciclotomica**  $E \supset F$  campo di spezzamento di  $x^n - 1$

**Estensione ciclica** se il suo gruppo di Galois è ciclico.

**Def** si dice *torre radicale* una successione di estensioni  $F = F_1 \subset F_2 \subset \dots \subset F_m$   
t.c.  $F_{i+1} = F_i(\alpha_i)$  con  $\alpha_i^{n_i} \in F_i$

**Estensione radicale** se esiste una torre radicale

$$F = F_1 \subset F_2 \subset \dots \subset F_m = E$$

## 6 Polinomi

### 6.1 Definizioni

**Polinomio minimo:**

$E \supset F, \alpha \in E, f \in F[X]$

$f$  monico e di grado minimo t.c.  $f(\alpha) = 0$

**Polinomio irriducibile:**

quando i suoi unici divisori sono 1 e lui stesso

**Polinomio separabile:**

Ogni fattore irriducibile ha radici distinte nel campo di spezzamento

**Polinomio ciclotomico:**

Il polinomio minimo di  $\zeta_n$  su  $\mathbb{Q}$  dove  $\zeta_n = e^{\frac{2\pi i}{n}}$

**Polinomio primitivo:**

$f \in \mathbb{Z}[X]$  si dice primitivo se il massimo comun divisore di tutti i coefficienti è 1.

**Polinomio caratteristico:**

$p_A(x) := \det(A - xI_n)$

dove  $A$  è una matrice quadrata di dimensione  $n$  a coefficienti in un campo  $\mathbb{K}$

### 6.2 Proposizioni e teoremi

**Lemma di Gauss:** il prodotto di due polinomi primitivi è primitivo.

**Corollario:** se un polinomio è irriducibile in  $\mathbb{Z}[X]$  allora è irriducibile anche in  $\mathbb{Q}[X]$

**Prop.** se  $p(x) \in \mathbb{Z}[X]$  e  $p(0), p(1)$  sono entrambi dispari  $\implies p(x)$  non ha soluzioni intere (p.31 libro)

## 7 Morfismi

**Def** un morfismo è un'applicazione  $f : A \rightarrow B$  che conserva le operazioni

**Isomorfismo** morfismo biiettivo

**Omomorfismo** morfismo tra due strutture algebriche dello stesso tipo

**Endomorfismo** è un omomorfismo con  $A = B$

**Automorfismo** è un endomorfismo biiettivo, ovvero un isomorfismo con  $A = B$

### 7.1 Esulando dall'algebra

**Omeomorfismo** è una funzione fra spazi topologici continua, biunivoca e con inversa continua

**Diffeomorfismo** è una funzione tra due varietà differenziabili con la proprietà di essere differenziabile, invertibile e di avere l'inversa differenziabile.