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 *semigruppo*
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 semigruppo con elemento neutro
Esempio $(\mathbb{Z}, \times)$

Def un *gruppo* 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
$H \lhd G$ se $ghg^{-1} \in H \ \forall g \in G, h \in H$

Esempio: $K \lhd H \lhd G$ non è detto che $K \lhd G$ (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 delle forma $[g, h]$

Lemma: $[G, G] \lhd G$
Oss. G è abeliano $\iff$ $[G, G] = \{1\}$

Lemma: sia N un sottogruppo normale di G, allora
G/N è abeliano $\iff$ $[G, G] \lhd N$ 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

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

tale che
- $G_{k+1} \lhd G_k$
- 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
$$G = G^{(1)} \supset G^{(2)} \supset ... \supset G^{(k)}$$
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 puo' 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 gruppoo 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'unita'

R_n =$\{\alpha \in \mathbb{C} : \alpha^n = 1\}$ radici n-esime dell'unita'
Def n-esimo polinomio ciclotomico

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

Lemma:

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

Lemma: Φ_n è un polinomio monico di $\mathbb{Z}[X]$e ha grado $\varphi(n)$
Thm: Φ_n è irriducibile in $\mathbb{Q}[X]$
Def: sia F un campo e $w \in F$ una radici primitiva n-esima dell'unita',
allora $F(w)/F$ è detta n-esima estensione ciclotomica di F
Def: un'estensione di Galois E/F è detta ciclica
se $Gal(E/F)$ 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.

Tor(G) = { $g \in G : g^n = 1$ } notazione moltiplicativa
Tor(G) = { $g \in G : ng = 0$ } notazione additiva

Sia $\varphi : G \to G^{'}$ isomorfismo allora
$\varphi(Tor(G)) = Tor(G')$

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
$< x, y|x^4 = y^2 = (xy)^2 = 1 >$

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 biiettive da

$$\pi : \{1, 2, .., n\} \to \{1, 2, .., n\}$$

$\pi \in S_n$ è detta permutazione di $\{1, 2, .., n\}$
Oss. $|S_n| = n!$
Lemma: S_n è generato da $(1, 2), (1, 3), .., (1, n)$
Lemma: S_n è generato da $(1, 2)$ e $(1, 2, .., n)$

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

Lemma: $\varphi(\pi\sigma) = \varphi(\pi) + \varphi(\sigma) \bmod 2$
Prop. in ogni rappresentazione di π come prodotto di 2-cicli, il numero di 2-cicli sara' 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. $A_n \lhd S_n$, $S_n/A_n \simeq \{1, -1\}$, 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. $SL_n(K) \lhd GL_n(K)$ (sottogruppo normale, vd thm Binet)

$O_n(K)$ =$\{A \in GL_n(K) | A^T A = AA^T = I\}$ gruppo ortogonale
$SO_n(K)$ gruppo ortogonale speciale (gruppo delle rotazioni dello spazio)

Gruppo di Galois
Sia E/F estensione di campi
$Gal(E/F)$ =$\{\sigma : E \to E : \sigma$ 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 $B_q(C)$:=Imδ_{q+1}

2 Anelli

2.1 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

2.2 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 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 $\mathbb{Q}(\sqrt{D}) = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$

2.3 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** $I + J = \{a + b | a \in I, b \in J\}$
$IJ = \{a_1 b_1 + .. + a_n b_n | a_i \in I, b_i \in J, i = 1, .., n \text{ per } n = 1, 2, ..\}$

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

2.4 Domini

Un dominio è un anello commutativo con unità in cui vale la legge di annullamenteo del prodotto
Su un dominio è definita una funzione Norma
Oss. ε è invertibile $\implies N(\varepsilon) = 1$
se vale anche l'altra implicazione la norma di 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 $\exists d : R \to \mathbb{N}$ t.c. $\forall a, b, \in R, b \neq 0$ $\exists q, r, \in \mathbb{R}$ 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

2.5 PID

A si dice PID (Principal ideal domain) se è un dominio è 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

$$(a_1) \subseteq (a_2) \subseteq ...$$

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

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

2.6 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

3 Campi

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

$$N(\alpha) = (-1)^{|G|} a_o^{|H|}$$
$$Tr(\alpha) = -|H| a_{m-1}$$

3.2 Estensioni

Sia E/F un'estensione algebrica

Estensione di Galois sia $E^G := \{a \in E | \sigma(a) = a \forall \sigma \in G\}$ dove $G = Gal(E/F)$
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 $F = F_1 \subset F_2 \subset ... \subset F_m$ t.c. $F_{i+1} = F_i(\alpha_i)$ con $\alpha_i^{n_i} \in F_i$

Estensione radicale se esiste una torre radicale
$F = F_1 \subset F_2 \subset ... \subset F_m = E$

4 Polinomi

4.1 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 ζ_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 divisiore 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 $\mathbb{K}$

4.2 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)

5 Morfismi

Def un morfismo è un'applicazione $f : A \to B$ 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 $A = B$

5.1 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.