APPUNTI DI TEORIA DEI GRUPPI

Mario Mainardis

Indice

1 Richiami **9**
1.1 Alcuni risultati elementari 9
1.1.1 Definizioni 9
1.1.2 Sottogruppi, classi laterali e generatori 11
1.1.3 Esponente 13
1.1.4 Omomorfismi 14
1.1.5 Congruenze, quozienti e sottogruppi normali 16
1.2 Esercizi 19

2 Estensioni di gruppi e serie di sottogruppi **23**
2.1 La Legge Modulare di Dedekind 24
2.2 Estensioni 26
2.2.1 Estensioni spezzanti e complementi 26
2.2.2 Endomorfismi idempotenti e fattorizzazioni 27
2.3 Serie di composizione 28
2.4 Sottogruppi subnormali 29
2.5 Teorema di Jordan-Hölder 30
2.6 Esercizi 34

3 Gruppi abeliani finiti **37**
3.1 Decomposizione primaria 38
3.2 Decomposizione di un p-gruppo abeliano finito 40
3.3 Il reticolo dei sottogruppi di $C_{p^h} \times C_p$ 42
3.4 La struttura dei gruppi abeliani finiti 44
3.5 Esercizi 46

4 Gruppi liberi e presentazioni **49**
4.1 Gruppi liberi 49
4.1.1 Semigruppi e monoidi 49
4.1.2 Monoidi e gruppi finitamente generati 50
4.1.3 Esistenza di monoidi liberamente generati 51
4.1.4 Esistenza e unicità di gruppi liberamente generati 51
4.2 Presentazioni 53
4.3 Esercizi 56

5 Gruppi simmetrici **57**
5.1 Richiami . . . 57
5.2 Struttura normale dei gruppi simmetrici . . . 60
5.3 Esercizi . . . 62

6 Commutatori e interderivato **65**
6.1 Commutatori . . . 65
6.2 L'interderivato di due sottogruppi . . . 66
6.3 Esercizi . . . 69

7 Gruppi risolubili e gruppi nilpotenti **71**
7.1 Serie abeliane e gruppi risolubili . . . 72
7.1.1 La serie derivata . . . 72
7.2 Serie centrali e gruppi nilpotenti . . . 74
7.2.1 La serie centrale ascendente . . . 74
7.2.2 La serie centrale discendente . . . 76
7.3 La serie delle chiusure normali . . . 77
7.4 Esercizi . . . 79

8 Azioni di gruppi **81**
8.1 Azione di un gruppo su se stesso . . . 81
8.1.1 Azione di un gruppo sul suo supporto per moltiplicazione a destra . . . 82
8.1.2 Azione di un gruppo su se stesso per coniugio . . . 83
8.1.3 Azione per coniugio sulle sezioni normali . . . 85
8.1.4 Sottogruppi caratteristici . . . 85
8.1.5 Prodotti semidiretti . . . 88
8.1.6 Gruppi diedrali . . . 90
8.2 Azione di un gruppo su un insieme . . . 91
8.2.1 G-insiemi . . . 91
8.2.2 G-sottoinsiemi e orbite . . . 92
8.2.3 G-omomorfismi . . . 93
8.2.4 Quozienti di G-insiemi e Primo Teorema di Omomorfismo per G-insiemi . . . 93
8.2.5 Stabilizzatori puntuali e globali . . . 95
8.2.6 Punti fissi . . . 95
8.2.7 Orbite e stabilizzatori . . . 96
8.2.8 L'equazione delle orbite . . . 97
8.2.9 Azioni transitive e primitive . . . 98
8.2.10 Decomposizione di un'azione . . . 100
8.2.11 Decomposizione di un'azione non transitiva . . . 101
8.2.12 Azione trasposta e prodotti intrecciati . . . 102
8.2.13 Prodotto intrecciato di azioni . . . 103
8.2.14 Decomposizione di un'azione transitiva e non primitiva . . . 105
8.3 Esercizi . . . 108

9 I Teoremi di Sylow e di Schur-Zassenhaus **115**
9.1 Il Teorema di Sylow 116
9.1.1 Esistenza dei Sylow 116
9.1.2 Coniugio dei Sylow 118
9.2 Normalizzanti nei p-gruppi finiti 120
9.3 Caratterizzazione dei gruppi nilpotenti finiti 122
9.4 Il Teorema di Schur-Zassenhaus 123
9.5 Esercizi 129

10 Azioni di gruppi su gruppi **135**
10.1 L'architettura di un gruppo finito 135
10.1.1 *cc*-sottogruppi 136
10.1.2 Il Teorema di Fitting 136
10.1.3 Il Teorema di Bender-Fitting 139
10.1.4 Sottogruppi critici 144
10.1.5 Esercizi 145
10.2 Azioni coprime e azioni unipotenti 146
10.2.1 Azione coprima 149
10.2.2 Controllo dell'azione coprima 151
10.2.3 Azioni sulle serie 153
10.2.4 Azione coprima su un gruppo abeliano 156
10.3 Esercizi 160

11 Gruppi lineari **161**
11.1 Azioni di GL(V) e SL(V) 162
11.1.1 Alcune azioni di $GL(V)$ e $SL(V)$ 164
11.2 Trasvezioni e Sottogruppi Radice 168
11.3 Il criterio di Iwasawa e semplicità di PSL(V) 174
11.3.1 Il criterio di Iwasawa 174
11.3.2 Semplicità di $PSL(V)$ 175
11.4 Sottogruppi parabolici in $GL(V)$ e in $SL(V)$ 176
11.4.1 Il radicale unipotente 178
11.4.2 La Decomposizione di Levi 180
11.4.3 Azione sul radicale di un parabolico massimale 184
11.4.4 Il reticolo dei sottogruppi contenenti un Borel 186
11.4.5 Sottogruppi parabolici in $PGL(V)$ e $PSL(V)$ 187
11.4.6 Caratteristica Locale e Teorema di Borel-Tits per $PSL(V)$ 188
11.5 Decomposizione di Bruhat *da fare* 191
11.6 Elementi di ordine coprimo con la caratteristica 191
11.6.1 Potenze irriducibili di cicli di Singer I 192
11.6.2 Cenni di rappresentazioni di anelli 193
11.6.3 Potenze irriducibili di cicli di Singer II 198
11.6.4 Automorfismi coprimi di uno spazio vettoriale 198
11.6.5 Automorfismi di GL(V) DA FARE 203
11.7 Esercizi 203

12 Forme bilineari e isometrie **205**
12.1 Forme bilineari 205
12.1.1 Forme bilineari riflessive 207
12.1.2 Forme bilineari alternanti 209
12.2 Isometrie 211
12.2.1 Il Lemma di Witt per gli spazi simplettici 215

13 Gruppi Simplettici **219**
13.1 Il Gruppo Simplettico 219
13.2 Conseguenze del Lemma di Witt 220
13.3 La geometria simplettica 222
13.3.1 Bandiere e telai simplettici 223
13.4 Sottogruppi parabolici di $Sp(V)$ 226
13.5 Sottogruppi radice simplettici 230
13.5.1 Gruppi di radici lunghe e trasvezioni simplettiche 231
13.5.2 Gruppi di radici corte 233
13.6 Semplicità di $PSp(V)$ 234
13.7 La Decomposizione di Levi nei parabolici di $Sp(V)$ 236
13.8 Azione sul radicale di un parabolico massimale di $Sp(V)$ 236
13.9 Il reticolo dei sottogruppi contenenti un Borel in $Sp(V)$ 236
13.10Sottogruppi parabolici di $PSp(V)$ 236
13.11Teorema di Borel-Tits per $PSp(V)$ 236
13.12Esercizi 237

14 Sistemi di Tits **239**
14.1 Sistemi di Tits 239
14.1.1 Sistemi di Tits per i gruppi lineari 240
14.1.2 Sistemi di Tits per i gruppi simplettici 244
14.2 Gruppi di Weyl 244
14.2.1 Gruppi di riflessioni 244
14.2.2 Gruppi di Coxeter 247
14.2.3 Gruppi di Coxeter di rango 2 e gruppi diedrali 250
14.3 Esercizi 253

15 Analisi locale **255**
15.1 Introduzione 255
15.2 Transfer e fusione 256
15.2.1 Trasversali 256
15.2.2 Transfer 258
15.2.3 Il Sottogruppo focale 260
15.2.4 Proprietà locali della fusione 261
15.2.5 Controllo locale della p-nilpotenza 266
15.3 La Fattorizzazione di Thompson 269
15.3.1 Moduli p-riducibili e quadratici 269
15.3.2 Il Sottogruppo di Thompson 274
15.4 Il Criterio di p-nilpotenza di Thompson 276

15.5 Azione senza punti fissi 278
15.5.1 Gruppi di Frobenius 278
15.5.2 Dimostrazione del Teorema di Thompson 280
15.6 Esercizi 282

A Strutture e loro automorfismi **285**
A.1 Strutture algebrico-relazionali 285
A.2 Endomorfismi ed automorfismi di strutture 286
A.3 Il gruppo degli automorfismi di una struttura 287
A.3.1 Il gruppo degli automorfismi di un gruppo ciclico 287
A.3.2 Il gruppo degli automorfismi di un p-gruppo abeliano elementare 289
A.4 Grafi e geometrie 289
A.4.1 Grafi 289
A.4.2 Le geometrie di Tits 290
A.4.3 La geometria proiettiva e lo spazio delle bandiere 291
A.5 Esercizi 296

Capitolo 1

Richiami

In questo capitolo riassumiamo brevemente le principali definizioni e risultati che dovrebbero essere noti dal corso di Algebra. Le dimostrazioni sono lasciate per esercizio.

1.1 Alcuni risultati elementari

1.1.1 Definizioni

Sia X un'insieme, un'**operazione** su X è un'applicazione

$$\sigma: X \times X \to X.$$

Se a e b sono elementi di X, l'immagine tramite σ della coppia (a,b) si dice **prodotto** di a e b e si indica con $a\sigma b$ o, più semplicemente, con ab. Per indicare le operazioni useremo di solito i simboli $\cdot, *$.

Un **gruppo** è una terna $(G, \cdot, e)$, dove G è un insieme (detto **supporto** del gruppo), $\cdot$ è un'operazione su G ed e è un elemento di G che verificano le seguenti proprietà:

GA1 l'operazione $\cdot$ è **associativa** , cioè per ogni a, b e c in G, risulta

$$a \cdot (b \cdot c) = (a \cdot b) \cdot (c);$$

GA2 per ogni a in G risulta

$$e \cdot a = a \cdot e = a;$$

GA3 per ogni elemento a di G esiste un elemento x in G tale che

$$a \cdot x = x \cdot a = e$$

L'elemento e si dice **identià** (o **elemento neutro** del gruppo $(G, \cdot, e)$.

Lemma 1.1.1 *Se $(G, \cdot, e)$ è un gruppo e $a \in G$, allora esiste un unico elemento $x \in G$ tale che $xa = ax = e$*

Se a e x sono come nel Lemma 1.1.1, x si dice **inverso** di a e si indica con a^{-1}. Attenzione l'inverso del prodotto di due elementi a e b di G è il prodotto degli inversi presi nell'ordine inverso:

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Come ha osservato H. Weyl, questo si sperimenta ogni giorno: quando ci si veste, prima si mettono i calzetti e poi le scarpe, quando ci si spoglia, prima si tolgono le scarpe e poi si tolgono i calzetti [31].

ESEMPI

1. Se $\mathbf{Z}$ è l'insieme dei numeri interi, la terna $(\mathbf{Z}, +, 0)$ è un gruppo.

2. Sia X un insieme, S_X l'insieme di tutte le **permutazioni** di X (cioè delle applicazioni biiettive da X in X). Sia $\circ$ la composizione di applicazioni e id_X l'applicazione identica. Allora la terna $(S_X, \circ, id_X)$ è un gruppo e si dice **gruppo simmetrico** sull'insieme X o **gruppo delle permutazioni** dell'insieme X. Se n è un intero positivo e X è l'insieme $\{1, \ldots, n\}$ dei numeri interi compresi tra 1 e n, indicheremo S_X semplicemente con S_n.

3. Siano $(A, \cdot_A, e_A)$ e $(B, \cdot_B, e_B)$ due gruppi e sia $A \times B$ il prodotto diretto degli insiemi A e B. Su $A \times B$ definiamo un'operazione nel modo seguente: sia
$$\cdot_{A\times B} \colon (A \times B) \times (A \times B) \to A \times B$$
definita, per ogni (a_1, b_1) e (a_2, b_2) in $A \times B$, da
$$(a_1, b_1) \cdot_{A\times B} (a_2, b_2) := (a_1 \cdot_A a_2, b_1 \cdot_B b_2).$$
Allora la tripla $(A \times B, \cdot_{A\times B}(e_a, e_b)$ è un gruppo e si chiama **prodotto diretto esterno** dei gruppi A e B.

Quando non è necessario specificare l'operazione $\cdot$ e l'identità e, si scrive semplicemente G al posto di $(G, \cdot, e)$, 1 o 1_G al posto di e e, se a e b sono elementi di G, si indica il loro prodotto $a \cdot b$ con ab.

Se G è un gruppo, la cardinalità dell'insieme G si indica con $|G|$ e si dice **ordine** di G. Un gruppo si dice **finito** se il suo ordine è un numero naturale.

Se x è un elemento di G, definiamo $x^0 := 1$ e, per induzione,

$$x^n := x \cdot x^{n-1}$$

per ogni $n \in \mathbf{N} \setminus \{\mathbf{0}\}$. Se z è un intero negativo poniamo

$$x^z := (x^{-z})^{-1}.$$

Questa notazione è compatibile con quella usata per definire l'inverso e valgono le "regole delle potenze": per ogni $n, m \in \mathbf{Z}$ ed $x, y \in G$,

$$x^{n+m} = x^n x^m \text{ e } (xy)^{-1} = y^{-1}x^{-1}.$$

Un gruppo X si dice **abeliano** o **commutativo** se per ogni x, y in X risulta

$$xy = yx.$$

In tal caso, per ogni $n \in \mathbf{N}$, vale anche:

$$(xy)^n = x^n y^n$$

$\mathbf{Z}$ è un gruppo abeliano, S_X, se $|X| > 2$, non è abeliano.

Se G è un gruppo abeliano, a volte è comodo usare la **notazione additiva**: in tal caso l'operazione di gruppo si indica con il simbolo $+$ e non si omette, l'elemento neutro si indica con il simbolo 0 e, per ogni $z \in \mathbf{Z}$ ed ogni $x \in G$ si scrive zx al posto di x^z.

1.1.2 Sottogruppi, classi laterali e generatori

Se $(G, \cdot, e)$ è un gruppo, un **sottogruppo** di G è un sottoinsieme non vuoto H di G tale che per ogni a, b in H l'elemento ab^{-1} sia ancora in H. Si osservi che, se H è un sottogruppo di $(G, \cdot, e)$, deve esistere un elemento h in H e quindi anche $e = hh^{-1}$ è un elemento di H. Ne segue che la tripla $(H, \cdot_{|_{H\times H}}, e)$ è ancora un gruppo. Per indicare che H è un sottogruppo di G scriveremo $H \leq G$ ($H < G$ se $H \leq G$ e $H \neq G$). Ovviamente $\{1\}$ e G sono sottogruppi di G. I sottogruppi di G diversi da $\{1\}$ e G si dicono **propri**. Un sottogruppo proprio H di G tale che gli unici sottogruppi di G contenenti H sono H e G si dice **massimale**. Se H è un sottogruppo massimale di un gruppo G scriveremo $H <_{max} G$.

Esempi

1. Per ogni $n \in \mathbf{N}$, l'insieme $n\mathbf{Z} = \{nz \mid z \in \mathbf{Z}\}$ è un sottogruppo di $\mathbf{Z}$.

2. Se Y è un sottoinsieme dell'insieme X, allora gli insiemi

   $$C_{S_X}(Y) := \{\sigma | \sigma \in S_X \text{ e } \forall y \in Y\, y^\sigma = y\}$$

   e

   $$N_{S_X}(Y) := \{\sigma | \sigma \in S_X \text{ e } \forall y \in Y\, y^\sigma \in Y\}$$

   sono sottogruppi di S_X con $C_{S_X}(Y) \leq N_{S_X}(Y)$.

3. Se G è un gruppo, l'insieme

   $$Z(G) := \{z \in G | zg = gz \text{ per ogni } g \in G\}$$

   è un sottogruppo di G e si chiama **centro** di G.

Se H è un sottogruppo di un gruppo G e $g \in G$, il sottoinsieme Hg, definito da

$$Hg = \{hg | h \in H\},$$

si dice **classe laterale destra di H in G di rappresentante** g. Analogamente l'insieme

$$gH = \{gh | h \in H\}$$

si dice **classe laterale sinistra di H in G di rappresentante** g.

Proposizione 1.1.2 *Sia G un gruppo ed $H \leq G$. Ogni classe laterale di H in G ha la stessa cardinalità di H.*

Indicheremo l'insieme delle classi laterali destre di H in G con G/H.

Proposizione 1.1.3 *Se G ed H sono come nella proposizione precedente, G/H è una partizione di G.*

La cardinalità di G/H si dice **indice** di H in G e si indica con

$$|G : H|.$$

In particolare, dalla Proposizione 1.1.2 e dalla Proposizione 1.1.3, si ottiene immediatamente il seguente risultato.

Teorema 1.1.4 (Teorema di Lagrange, versione classica) *Sia G un gruppo ed H un suo sottogruppo. Se G oppure $|H|$ e $|G : H|$ sono finiti, allora*

$$|G| = |G : H||H|$$

Proposizione 1.1.5 *Se H e K sono sottogruppi di un gruppo G allora $H \cap K$ è un sottogruppo di G.*

Si osservi che, in generale, l'unione di due sottogruppi non è mai un sottogruppo, tranne il caso in cui i due sottogruppi sono contenuti uno dentro l'altro (Esercizio 1.2.4).

Se S è un sottoinsieme di G l'intersezione $\langle S \rangle$ di tutti i sottogruppi di G contenenti S è un sottogruppo di G che si dice **sottogruppo generato da** S. Si vede immediatamente che $\langle S \rangle$ è il più piccolo (per inclusione) sottogruppo di G contenente l'insieme S. In particolare se $G = \langle S \rangle$ diremo che S è un **sistema di generatori** di G, oppure che G è **generato** da S (o dagli elementi di S). Un gruppo generato da un solo elemento si dice **ciclico**.

Proposizione 1.1.6 *Se G è ciclico generato dall'elemento x, allora*

$$G = \{x^z | z \in \mathbf{Z}\}.$$

Indichiamo con $\mathcal{L}(G)$ l'insieme di tutti i sottogruppi di G. Se H e K sono sottogruppi di G, $\langle H, K \rangle$ è il più piccolo (per inclusione) sottogruppo di G contenente H e K e $H \cap K$ è il più grande sottogruppo di G contenuto sia in H

che in K. Quindi, come insieme parzialmente ordinato, $\mathcal{L}(G)$ è un reticolo e, per questo motivo, viene anche chiamato **reticolo dei sottogruppi** di G. Anche se il reticolo dei sottogruppi di un gruppo, in generale, non determina il gruppo a meno di isomorfismi (ad esempio, se C_3 è gruppo ciclico di ordine 3 e S_3 è il gruppo delle permutazioni dell'insieme $\{1,2,3\}$, allora $\mathcal{L}(C_3 \times C_3)$ è isomorfo, come insieme parzialmente ordinato, a $\mathcal{L}(S_3)$), la struttura reticolare di $\mathcal{L}(G)$ può fornire interessanti informazioni sul gruppo G. Il testo di riferimento sui reticoli di gruppi è la monografia [25].

Se H e K sono sottogruppi di G, con il simbolo HK indichiamo il seguente insieme:

$$HK = \{hk \mid h \in H, k \in K\}.$$

HK è chiaramente contenuto in $\langle H, K\rangle$ ma in generale non coincide con $\langle H, K\rangle$. Vale infatti il seguente risultato.

Proposizione 1.1.7 *Siano H e K sottogruppi di un gruppo G. Allora $HK = KH$ se e solo se $\langle H, K\rangle = HK$.*

Il risyltato seguente è l'analogo per i gruppi del Teorema di Grassmann sulla dimensioni dei sottospazi di uno spazio vettoriale.

Proposizione 1.1.8 *Se H e K sono sottogruppi finiti di un gruppo G, allora*

$$|HK||H \cap K| = |H||K|.$$

1.1.3 Esponente

Il minimo intero strettamente positivo k tale che $x^k = 1$ si dice **periodo** o **ordine** dell'elemento x, se tale intero esiste, altrimenti si dice che x ha **periodo (ordine) infinito**. Un elemento di ordine 2 si dice **involuzione**. Un gruppo in cui ogni elemento ha periodo finito si dice di **torsione**.

Lemma 1.1.9 *Se g ha ordine finito n e k è un intero tale che $g^k = 1$, allora n divide k.*

Dimostrazione. Facciamo la divisione con resto di k per n:

$$k = nq + r \text{ con } q \in \mathbf{Z} \text{ e } 0 \leq r < n.$$

Da questo segue che

$$1 = g^k = g^{nq+r} = (g^n)^q g^r = 1g^r = g^r,$$

da cui segue che $r = 0$ per la minimalità di n. ∎ Un gruppo G si dice **di esponente finito** se esistono interi k tali che, per ogni $g \in G$, $g^k = 1$. In tal caso il minimo di questi interi si chiama **esponente** di G. Se per ogni intero positivo k esiste un elemento g di G tale che $g^k \neq 1$ diremo che G ha esponente infinito. Si osservi che esistono gruppi di torsione con esponente infinito. Dalla definizione di esponente segue immediatamente il seguente

Lemma 1.1.10 *Se G è di esponente finito, $exp(G)$ è il minimo comune multiplo degli ordini degli elementi di G.*

Per il Lemma 1.1.9, segue immediatamente che

Corollario 1.1.11 *Se G ha esponente finito n e k è un intero tale che $g^k = 1$ per ogni $g \in G$, allora n divide k.*

In particolare, se $|G|$ è finito, per il Teorema di Lagrange, $|\langle g \rangle|$ divide $|G|$ per ogni $g \in G$, quindi:

Lemma 1.1.12 *Se G è finito, $exp(G)$ è finito e divide $|G|$.*

In generale non è detto che l'esponente di un gruppo coincida con il suo ordine, ad esempio, se G è il gruppo di Klein, il suo ordine è 4, mentre il suo esponente è 2. Abbiamo visto però che nei gruppi ciclici questo è vero e dimostreremo, alla fine di questa sezione, che questa proprietà caratterizza i gruppi ciclici. Vediamo ora il comportamento dell'esponente dei sottogruppi e dei quozienti:

Lemma 1.1.13 *Sia G di esponente finito.*

1. *Se H è un sottogruppo di G, H è di esponente finito e $exp(H)$ divide $exp(G)$.*
2. *Se N è un sottogruppo normale di G. Allora G/N è di esponente finito e $exp(G/N)$ divide $exp(G)$.*

DIMOSTRAZIONE. Sia $n = exp(G)$, quindi $x^n = 1$ per ogni $x \in G$. Per il Corollario 1.1.11, basta provare che, per ogni $h \in H \cap G/N$, $h^n = 1$. Questo segue immediatamente se $h \in H$, perché $H \leq G$, mentre, se $H \in G/N$, segue perché $(xN)^n = (x^n)N = 1N = 1_{G/N}$. ∎

Anche in questo caso osserviamo che non è affatto detto che, con le notazioni del lemma precedente, l'esponente di H, o di G/N, sia un divisore proprio dell'esponente di G. E questo neppure nel caso in cui H sia un sottogruppo proprio o N sia diverso da $\{1\}$: ad esempio se G è di nuovo il gruppo di Klein, ogni suo sottogruppo di ordine 2 ha esponente 2 ed il quoziente di G su un suo sottogruppo di ordine 2 ha ancora esponente 2.

1.1.4 Omomorfismi

Se G^* è un altro gruppo, un **omomorfismo** tra G e G^* è un'applicazione $\phi: G \to G^*$ tale che per ogni a, b in G risulta

$$(ab)^\phi = a^\phi b^\phi.$$

Un omomorfismo iniettivo si dice **monomorfismo**, un omomorfismo suriettivo si dice **epimorfismo** ed un omomorfismo biiettivo si dice **isomorfismo**. Due gruppi si dicono **isomorfi** se esiste un isomorfismo tra di loro. Un omomorfismo da un gruppo G in se stesso si dice **endomorfismo**, un'endomorfismo biiettivo si dice **automorfismo**. ESEMPI

1. L'applicazione $exp: \mathbf{R} \to \mathbf{R}^{>0}$ definita per ogni $x \in \mathbf{R}$ da $x^{exp} = e^x$ è un omomorfismo dal gruppo $(\mathbf{R}, +, 0)$ al gruppo $(\mathbf{R}^{>0}, \cdot, 1)$.

2. Se n è un intero, la mltiplicazione per n è un endomorfismo di $\mathbf{Z}$ in $\mathbf{Z}$.

3. Se Y è un sottoinsieme di X la restrizione a Y,

$$|_Y : N_{S_X}(Y) \to S_Y$$

definita, per ogni $\sigma \in N_{S_X}(Y)$ da

$$\sigma \mapsto \sigma_{|_Y},$$

è un omomorfismo di gruppi.

4. Se G è un gruppo e $a \in G$, l'applicazione

$$\gamma_a : G \to G$$

definita, per ogni $g \in G$, da

$$g \mapsto a^{-1}ga$$

è un automorfismo di G. L'elemento $a^{-1}ga$ si indica con g^a e si chiama **coniugato di** g **tramite** a. Due elementi h e g di G (o due sottoinsiemi H e L di G), tali che $h = g^a$ ($H = L^a := \{l^a | l \in L\}$) per qualche a in G, si dicono **coniugati** in G.

5. L'insieme degli automorfismi di G si indica con $Aut(G)$. La tripla $(Aut(G), \circ, id)$, dove $\circ$ è la composizione di applicazioni e id è l'applicazione identica su G, è un gruppo.

6. Se G è un gruppo, l'applicazione

$$\gamma : G \to Aut(G)$$

definita, per ogni $a \in G$ da

$$a \mapsto \gamma_a$$

è un omomorfismo di gruppi.

L'insieme $\{g \in G | g^\phi = 1_{G^*}\}$ è un sottogruppo di G. Si chiama **nucleo** di ϕ e si indica con $\ker(\phi)$.

Esempi Siano X, Y $|_Y$, G e γ come sopra, allora

1. $\ker(|_Y) = C_{S_X}(Y)$.

2. $\ker(\gamma) = Z(G)$.

Proposizione 1.1.14 *Sia $\phi : G \to G^*$ un omomorfismo di gruppi. Allora ϕ è iniettivo se e solo se* $\ker(\phi) = \{1\}$.

Proposizione 1.1.15 *Siano G ed H gruppi, R un sottoinsieme di G tale che $G = \langle R \rangle$ e sia $\phi: R \to H$ un'applicazione. Allora esiste al più un omomorfismo di gruppi $\overline{\phi}: G \to H$ tale che $\overline{\phi}|_R = \phi$.*

DIMOSTRAZIONE. Supponiamo che $\phi_1: G \to H$ e $\phi_2: G \to H$ siano omomorfismi di gruppi tali che $\phi_i|_R = \phi$ e sia T l'insieme

$$\{g \in G | g^{\phi_1} = g^{\phi_2}\}$$

Si vede facilmente che T è un sottogruppo di G che contiene R. Poiché $G = \langle R \rangle$, segue che $G = T$, da cui $\phi_1 = \phi_2$. ∎

Osserviamo che non è detto che in generale l'applicazione $\overline{\phi}$ esista: per esempio l'applicazione da $\{1, 0\} \to \mathbf{Z}$ che associa 1 a 1 e 0 a -1 non si può estendere ad alcun omomorfismo di gruppi da $\mathbf{Z}$ in se stesso.

1.1.5 Congruenze, quozienti e sottogruppi normali

Sia $G = (G, \cdot, 1)$ un gruppo. Una relazione d'equivalenza $\sim$ su G si dice **congruenza** se, per ogni a, a', b, b' in G

$$\left.\begin{array}{l} a \sim a' \\ b \sim b' \end{array}\right\} \Rightarrow ab \sim a'b'$$

ESEMPIO Se $\phi: G \to \overline{G}$ è un omomorfismo di gruppi, allora la relazione $\sim_\phi$ definita, per ogni $a, a' \in G$ da $a \sim_\phi a'$ se e solo se $a^\phi = (a')\phi$ è una congruenza su G. $\sim_\phi$ è la congruenza su G **associata** all'omomorfismo ϕ.

Se $\sim$ è una congruenza su un gruppo G, l'insieme quoziente $G/\sim$ eredita da G una struttura di gruppo $(G/\sim, \cdot_\sim, [1]_\sim)$, dove, indicando per ogni $a \in G$ con $[a]_\sim$ la classe di equivalenza di a, l'operazione $\cdot_\sim$ è (ben) definita da

$$[a]_\sim \cdot_\sim [b]_\sim = [ab]_\sim.$$

Le congruenze su un gruppo G si possono classificare facilmente, infatti, se $\sim$ è una congruenza su G, la classe $[1]_\sim$ è un sottogruppo **normale** di G, cioè un sottogruppo N di G tale che, per ogni $a \in G$ ed ogni $g \in N$, $g^a \in N$. Viceversa, se N è un sottogruppo normale di G la relazione $\sim_N$, definita, per ogni a e b in G, da

$$a \sim_N b \text{ se e solo se } ab^{-1} \in N,$$

è una congruenza su N tale che $N = [1]_{\sim_N}$. In altre parole,

Lemma 1.1.16 *Per ogni gruppo G le applicazioni*

$$N \mapsto \sim_N \text{ e } \sim \mapsto [1]_\sim \tag{1.1}$$

sono biiezioni una inversa dell'altra tra l'insieme dei sottogruppi normali di G l'insieme delle congruenze su G. Inoltre se $g \in G$, $[g]_{\sim_N} = Ng$ e se $h \in G$, $NgNh = Ngh$.

Osserviamo che, se H è un sottogruppo di un gruppo G, ma non è normale in G, *allora* $\sim_H$ è ancora una relazione di equivalenza su G, ma non una congruenza e quindi non è possibile definire un'operazione sull'insieme quoziente $G/\sim_H$ (vedi Esercizio 5.3.5.9)). Vedremo più avanti, però, che $\sim_H$ è una congruenza per una struttura (quella di G-insieme) più debole di quella di gruppo.

Proposizione 1.1.17 *Sia G un gruppo, N un sottogruppo di G. Allora le seguenti affermazioni sono equivalenti:*

1. *N è normale in G;*
2. *per ogni $g \in G$ $Ng = gN$.*

Per indicare che N è un sottogruppo normale di G scriveremo $N \trianglelefteq G$.

Se H e K sono sottogruppi di un gruppo G, diremo che K **normalizza** H se $H \trianglelefteq \langle H, K\rangle$. Si osservi che un sottogruppo N di G è normale in G se e solo se è normalizzato da G.

Si noti che se K normalizza N, allora $NK = KN$ per ogni sottogruppo K di G. In particolare, per la Proposizione 1.1.7, NK è un sottogruppo di G.

Esempi

1. Il nucleo di un omomorfismo di gruppiè un sottogruppo normale del dominio.
2. Il centro di un gruppo G è un sottogruppo normale di G.
3. Se Y è un sottoinsieme di un insieme X, $C_{S_X}(Y)$ è un sottogruppo normale di $N_{S_X}(Y)$.
4. Il sottogruppo di S_3 generato dall'elemento che scambia 1 con 2 e lascia fisso 3 non è un sottogruppo normale di S_3.

Se N è un sottogruppo normale di un gruppo G, si scrive semplicemente G/N al posto di $G/\sim_N$ ed il gruppo G/N si dice **gruppo quoziente di G modulo** (**su**) N. L'applicazione

$$\begin{aligned} \pi\colon \quad & G \to G/N \\ & g \mapsto Ng \end{aligned}$$

è un omomorfismo suriettivo e si chiama **proiezione canonica di G su G/N** il cui nucleo coincide con N. Questo chiude il cerchio, infatti:

1. ogni equivalenza associata ad un'omomorfismo che ha per dominio un gruppo G è una congruenza;
2. ogni congruenza su G è del tipo $\sim_N$ dove N è un sottogruppo normale di G;

3. ogni sottogruppo normale N di G è il nucleo di un omomorfismo (la proiezione canonica π di G su G/N).

Teorema 1.1.18 (Primo Teorema di Omomorfismo) *Sia $\phi: G \to G^*$ un omomorfismo di gruppi e $K = \ker \phi$. Allora*

1. *$K \trianglelefteq G$;*
2. *se π è la proiezione canonica di G su G/K, esiste un unico omomorfismo $\overline{\phi}: G/K \to G^*$ tale che per ogni $g \in G$ si abbia $g^{\pi\overline{\phi}} = g^{\phi}$ (cioè $\pi\overline{\phi} = \phi$);*
3. *$\overline{\phi}$ è iniettivo;*
4. *$\overline{\phi}$ è biiettivo se e solo se ϕ è suriettivo.*

Teorema 1.1.19 (Teorema di Corrispondenza) *Sia $\phi: G \to H$ un omomorfismo di gruppi e $K = \ker \phi$. Sia $\mathcal{L}$ il reticolo dei sottogruppi di G contenenti K e $\mathcal{L}'$ il reticolo dei sottogruppi di H che sono contenuti in G^{ϕ}. Allora l'applicazione, che ad ogni $H \in \mathcal{L}$ associa $H^{\phi} = \{h^{\phi} \mid h \in H\}$, è un isomorfismo di reticoli tra $\mathcal{L}$ e $\mathcal{L}'$. Inoltre, se $N \in \mathcal{L}$ e $N \trianglelefteq G$, allora $N^{\phi} \trianglelefteq G^{\phi}$.*

Consideriamo il caso in cui H sia il quoziente G/N del gruppo G modulo un sottogruppo normale N e ϕ sia la proiezione canonica. Dal Teorema di Corrispondenza si ottiene che esiste un isomorfismo tra l'intervallo dei sottogruppi di G contenenti N ed il reticolo dei sottogruppi di G/N, inoltre tale isomorfismo manda sottogruppi normali in sottogruppi normali.

Se N è un sottogruppo normale proprio, cioè $\{1\} < N < G$, allora N e G/N sono due gruppi il cui ordine è minore di quello di G e quindi, in teoria, più facili da studiare. Teoremi come quello di corrispondenza permettono di ottenere, dalle informazioni su questi gruppi più piccoli, delle informazioni su tutto G. Ad esempio se G/N contiene un sottogruppo normale proprio T, per il teorema di corrispondenza, la sua antiimmagine $T^{\pi^{-1}}$ tramite la proiezione canonica π di G su G/N è un sottogruppo normale proprio di G contenente propriamente N.

Applichiamo ora il Teorema di Corrispondenza per classificare tutti i sottogruppi di un gruppo ciclico. Sia C un gruppo ciclico e sia c un suo generatore. Consideriamo l'applicazione

$$\begin{aligned} \zeta: \quad & \mathbf{Z} \to C \\ & z \mapsto c^z. \end{aligned}$$

Si verifica immediatamente che ζ è un omomorfismo suriettivo di gruppi dal gruppo additivo degli interi nel gruppo C. Se C è ciclico infinito, il nucleo di ζ è $\{0\}$ e quindi C è isomorfo a $\mathbf{Z}$. Se C è finito, allora il nucleo di ζ è $|C|\mathbf{Z}$. Quindi, per il Primo Teorema di Omomorfismo, o $C \cong \mathbf{Z}$, oppure $|C|$ è finito ed è isomorfo a $\mathbf{Z}/|C|\mathbf{Z}$. Supponiamo ora che C sia finito. Per il Teorema di Corrispondenza, i sottogruppi di C sono in corrispondenza biunivoca con i sottogruppi di $\mathbf{Z}$ che contengono il sottogruppo $|C|\mathbf{Z}$. Questi sono tutti e soli i

sottogruppi del tipo $m\mathbf{Z}$, dove m divide $|C|$. Osserviamo che $m\mathbf{Z}$ è generato da m e quindi il sottogruppo di C corrispondente a $m\mathbf{Z}$ è generato da m^ζ, cioè da c^m. Osserviamo inoltre che se t è un intero primo con $|C|$, allora esistono degli interi r e s tali che $r|C| + st = 1$. Tenendo presente che $c^{|C|} = 1$, segue che, per ogni t primo con $|C|$ e per ogni intero m,

$$c^m = c^{m(r|C|+st)} = c^{mr|C|}c^{mst} = c^{mst} \in \langle c^{mt}\rangle.$$

Poiché, ovviamente, $c^{mt} \in \langle c^m\rangle$, otteniamo $\langle c^m\rangle = \langle c^{tm}\rangle$, per ogni intero t primo con $|C|$. Riassumendo,

Proposizione 1.1.20 (Teorema di Struttura dei Gruppi Ciclici) *Sia C un gruppo ciclico generato dall'elemento c, allora*

1. *se C è infinito, C è isomorfo a $\mathbf{Z}$ ed i suoi sottogruppi sono tutti e soli del tipo $\langle c^m\rangle$ dove $m \in \mathbf{Z}$;*
2. *se C è finito C è isomorfo a $\mathbf{Z}/|C|\mathbf{Z}$ ed i suoi sottogruppi sono tutti e soli del tipo $\langle c^m\rangle$ dove m divide $|C|$, inoltre per ogni intero t primo con $|C|$, $\langle c^m\rangle = \langle c^{tm}\rangle$;*
3. *in particolare, se $|C| = p^k$ dove p è un numero primo e k è un numero naturale, allora i sottogruppi di C sono tutti e soli del tipo $\langle c^{p^h}\rangle$ dove h è un numero naturale minore di k, quindi l'insieme dei sottogruppi ordinato per inclusione è una catena di lunghezza $k+1$. Inoltre, per ogni numero naturale h ed ogni numero intero t non divisibile per p, $\langle c^{p^h}\rangle = \langle c^{tp^h}\rangle$.*

1.2 Esercizi

Esercizio 1.2.1 *Sia G un gruppo, T un insieme e G^T l'insieme di tutte le funzioni da T a G. Per ogni $f_1, f_2 \in G^T$ sia $f_1 \cdot f_2$ la funzione da T a G definita, per ogni $t \in T$, da*

$$(f_1 \cdot f_2)(t) = (f_1(t))(f_2(t)).$$

$f_1 \cdot f_2$ si dice **prodotto puntuale** *delle funzioni f_1 e f_2.*

1. *Si provi che G^T con il prodotto puntuale è un gruppo.*
2. *Si provi che se T è finito di ordine n, allora G^T è isomorfo al gruppo*

$$\underbrace{G \times G \times \ldots \times G}_{n-volte}.$$

Esercizio 1.2.2 *Siano C_h e C_k due gruppi ciclici di ordine ripettivamente h e k. Si provi che il prodotto diretto $C_h \times C_k$ è ciclico se e solo se h e k sono coprimi.*

Esercizio 1.2.3 *Sia G un gruppo di esponente t e sia N un sottogruppo normale di G. Si provi che l'esponente di G/N è minore od uguale a t.*

Esercizio 1.2.4 *Siano H e K sottogruppi di un gruppo G. Si provi che $H \cup K$ è un sottogruppo di G se e solo se $H \subset K$ oppure $K \subset H$.*

Esercizio 1.2.5 *Sia G un gruppo*

1. *Si provi che l'intersezione di una famiglia qualsiasi di sottogruppi di G è ancora un sottogruppo di G.*

2. *Si provi che l'intersezione di una famiglia qualsiasi di sottogruppi normali di G è ancora un sottogruppo normale di G.*

3. *Si deduca da 1) che l'insieme $\mathcal{L}(G)$ dei sottogruppi di G ordinato per inclusione è un reticolo di G avente G come elemento massimo e $\{1\}$ come minimo.*

4. *Si deduca da 2) che l'insieme $\mathcal{N}(G)$ dei sottogruppi normali di G ordinato per inclusione è un sottoreticolo di $\mathcal{L}(G)$ avente G come elemento massimo e $\{1\}$ come minimo.*

Esercizio 1.2.6 *Si provi che il centro di un gruppo G è un sottogruppo normale di G.*

Esercizio 1.2.7 *In un gruppo abeliano tutti i sottogruppi sono normali.*

Esercizio 1.2.8 *Sia G un gruppo ed H un suo sottogruppo. Sia R un insieme di generatori di H. Si provi che H è normale in G se e solo se per ogni $g \in G$ ed ogni $r \in R$ risulta*

$$r^g \in H.$$

Esercizio 1.2.9 *Sia G un gruppo ed H un suo sottogruppo. Sia S un insieme di generatori di G. Si provi che H è normale in G se e solo se per ogni $s \in S$ ed ogni $h \in H$ risulta*

$$h^s \in H.$$

Un sottogruppo H di un gruppo G si dice **quasinormale** in G se e solo se per ogni altro sottogruppo K di G risulta

$$HK = KH.$$

Esercizio 1.2.10 *(Ore) Si provi che un sottogruppo massimale di un gruppo G è normale se e solo se è quasinormale.*

Esercizio 1.2.11 *(Ore) Sia G un gruppo e H, K due suoi sottogruppi tali che $G = HK$. Si provi che per ogni $g \in G \setminus H$ $Hg \cap K \neq \emptyset$.*

Esercizio 1.2.12 *Sia G un gruppo, H un suo sottogruppo e siano*

$$N_G(H) = \{g | g \in G \text{ e } H^g = H\}$$

e

$$C_G(H) = \{g | g \in G \text{ e } g^{-1}hg = h \, \forall h \in H\}.$$

Dimostrare che

1. *$N_G(H)$ e $C_G(H)$ sono sottogruppi di G;*
2. *$C_G(H) \trianglelefteq N_G(H)$;*
3. *$C_G(H) \cap H = Z(H)$;*
4. *$H \trianglelefteq N_G(H)$;*
5. *$H \trianglelefteq G$ se e solo se $G = N_G(H)$;*

Il sottogruppo $N_G(H)$ si dice **normalizzante** *di H in G. Il sottogruppo $C_G(H)$ si dice* **centralizzante** *di H in G e, se g è un elemento di $C_G(H)$, diremo che g* **centralizza** *H.*

Esercizio 1.2.13 *Siano a e b due elementi di un gruppo G con $ab = ba$ e $\langle a \rangle \cap \langle b \rangle = \{1\}$. Si provi che se a ha ordine r e b ha ordine s allora l'ordine di ab è il minimo comune multiplo di a e di b.*

Esercizio 1.2.14 *Si provi che se G è un gruppo finito di ordine pari, allora G contiene un'involuzione (suggerimento: se ogni elemento non identico di un gruppo G è diverso dal suo inverso, G conterrebbe un numero dispari di elementi).*

Capitolo 2

Estensioni di gruppi e serie di sottogruppi

Sia G un gruppo ed N un sottogruppo normale di G. Nel primo capitolo abbiamo ricordato due risultati, il Teorema di Lagrange ed il Teorema di Corrispondenza, che permettevano di ottenere informazioni su G dalla struttura di N e di G/N. Questo è il problema centrale della teoria delle estensioni. Ed è un problema del tutto naturale: spesso abbiamo maggiori informazioni su N e G/N che su tutto G (per esempio nel caso di dimostrazioni per induzione sui gruppi finiti con ipotesi che si ereditano ai quozienti ed ai sottogruppi normali).

La teoria delle estensioni porta naturalmente allo studio delle serie di sottogruppi: supponiamo di trovare dei sottogruppi normali in N e G/N. Allora possiamo ripetere lo stesso ragionamento con N e G/N e così via. Per il teorema di corrispondenza otteniamo in questo modo una serie (cioè un insieme totalmente ordinato)

$$N_0 = G \geq N_1 \geq N_2 \geq \ldots \geq N_k = \{1\}$$

di sottogruppi di G ciascuno normale dentro il precedente. Se il gruppo è finito (ma questo vale anche una situazione più generale, come vedremo) questo procedimento termina dopo un numero finito di passi. Si ottiene così quella che si dice una serie di composizione. Con l'aumentare del numero dei sottogruppi che compongono una serie, da un lato si semplifica la struttura dei gruppi quoziente

$$N_i/N_{i+1}$$

e questo è bene, dall'altra però le difficoltà nell'applicare la teoria delle estensioni aumentano esponenzialmente, per cui la strategia di studiare un gruppo attraverso le serie di composizione si è rivelata finora di difficile applicazione. Strategie più efficaci verranno introdotte nei capitoli sulle azioni di gruppo.

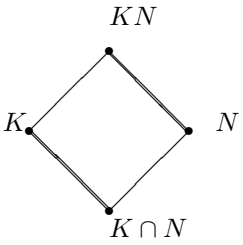
La prima sezione di questo capitolo introduce due strumenti fondamentali: il Secondo Teorema di Omomorfismo e la Legge Modulare di Dedekind. Questi due risultati permettono di determinare degli isomorfismi tra fattori di serie

subnormali distinte e saranno usati costantemente in seguito. In particolare, la dimostrazione del Teorema di Jordan Hölder è una classica applicazione del Secondo Teorema di Omomorfismo. La legge Modulare di Dedekind verrà usata nella generalizzazione al caso non abeliano del Teorema di Schur-Zassenhaus.

2.1 La Legge Modulare di Dedekind

Teorema 2.1.1 *Sia G un gruppo. N e K sottogruppi di G con N normale in G. Allora*

1. *KN è un sottogruppo di G;*
2. *$K \cap N$ è un sottogruppo normale di K*
3. *$KN/N \cong K/(K \cap N)$* (Secondo teorema di omomorfismo).



Dimostrazione. I punti 1. e 2. sono lasciati come esercizio. Dimostriamo il punto 3. utilizzando il Primo Teorema di Omomorfismo. Sia

$$\phi\colon K \to G/N$$

l'applicazione definita dalla posizione

$$k \mapsto kN$$

per ogni $k \in K$. Osserviamo che ϕ si ottiene restringendo a K il dominio della proiezione canonica di G su G/N. In particolare ϕ è un omomorfismo. Inoltre la sua immagine è KN/N. Infatti ogni elemento di KN è del tipo kh con $k \in K$ e $h \in N$, inoltre per ogni $h \in N$ ed ogni $k \in K$ risulta $khN = kN$, quindi

$$KN/N = \{khN | k \in K, h \in N\} = \{kN | k \in K, \} = K^{\phi}.$$

Mostriamo ora che $\ker \phi = K \cap N$. Sia $k \in N \cap K$, allora $k^{\phi} = kN = N$, quindi $K \cap N \subseteq \ker \phi$; viceversa se $k \in \ker \phi$, allora $N = k^{\phi} = kN$ e quindi $k \in \ker \phi \cap N \subseteq K \cap N$. Per il primo teorema di omomorfismo risulta

$$K/(K \cap N) = K/\ker \phi \cong KN/N.$$

■

Il Secondo Teorema di Omomorfismo permette di ottenere, dalla struttura di N e K, informazioni sulla struttura del sottogruppo generato da N e da K. Questo avviene, ad esempio, nei seguenti due corollari. Si osservi però che se N non è normale (o, più precisamente, se KN non è un sottogruppo), la struttura di $\langle K, N\rangle$ non è affatto controllata dalle strutture di N e di K: per esempio, il gruppo diedrale di ordine infinito D_∞ costruito nell'Esercizio 8.3.17 ha ordine infinito ed è generato da due sottogruppi H e K di ordine 2.

Corollario 2.1.2 *Nelle ipotesi del teorema precedente, N è un sottogruppo normale massimale in KN se e solo se $K \cap N$ è un sottogruppo normale massimale di K.*

DIMOSTRAZIONE. Esercizio. ∎

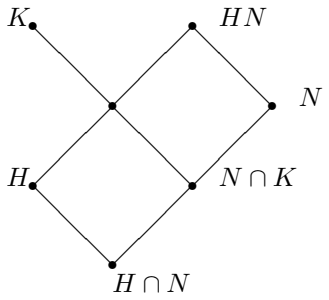
Corollario 2.1.3 *Nelle ipotesi del Teorema 2.1.1 risulta*

$$|KN| = |K||N||K \cap N|^{-1}$$

DIMOSTRAZIONE. Esercizio (usare il Teorema di Lagrange). ∎

Teorema 2.1.4 (LEGGE MODULARE DI DEDEKIND) *Sia N un sottogruppo normale di un gruppo G e siano H e K due sottogruppi di G con $H \leq K$. Allora*

$$(HN) \cap K = H(N \cap K).$$



DIMOSTRAZIONE. Chiaramente $H(N \cap K)$ è contenuto in HN e K, quindi

$$(HN) \cap K \geq H(N \cap K).$$

Viceversa se $hn \in (HN) \cap K$, con $h \in H$ e $n \in N$, allora, posto $k = hn$ risulta

$$n = h^{-1}k \in N \cap K,$$

da cui segue l'inclusione opposta. ∎

2.2 Estensioni

Siano N, G e H gruppi. Diremo che G è un'**estensione** di N con H se G contiene un sottogruppo normale $\overline{N}$ tale che

$$\overline{N} \cong N \text{ e } G/\overline{N} \cong H.$$

Come abbiamo già accennato, il problema delle estensioni di gruppo è quello di studiare quali informazioni sul gruppo G si possono ottenere dalla coppia (N, H) Osserviamo, però, che, in generale, la coppia (N, H) non individua in modo unico il gruppo G: ci sono essenzialmente due situazioni critiche in cui G non è individuato dalla coppia (N, H) ed i seguenti sono gli esempi più semplici di queste due situazioni.

ESEMPIO 1. $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ e $\mathbf{Z}/4\mathbf{Z}$ sono due estensioni non isomorfe di $\mathbf{Z}/2\mathbf{Z}$ con $\mathbf{Z}/2\mathbf{Z}$ (entrambi i gruppi hanno un sottogruppo normale isomorfo a $\mathbf{Z}/2\mathbf{Z}$ ed il quoziente modulo questo sottogruppo è isomorfo a $\mathbf{Z}/2\mathbf{Z}$).

ESEMPIO 2 S_3 (il gruppo simmetrico sull'insieme $\{1, 2, 3\}$) e $\mathbf{Z}/6\mathbf{Z}$ sono due estensioni non isomorfe di $\mathbf{Z}/3\mathbf{Z}$ con $\mathbf{Z}/2\mathbf{Z}$ (come sopra, entrambi i gruppi hanno un sottogruppo normale isomorfo a $\mathbf{Z}/3\mathbf{Z}$ ed il quoziente modulo questo sottogruppo è isomorfo a $\mathbf{Z}/2\mathbf{Z}$).

2.2.1 Estensioni spezzanti e complementi

Sia G un'estensione del gruppo $\overline{N}$ per un gruppo $\overline{K}$ e sia, come nella sezione precedente, N un sottogruppo normale di G tale che

$$\overline{N} \cong N \text{ e } G/N \cong \overline{K}.$$

Se G possiede un sottogruppo K tale che

$$NK = G \text{ e } N \cap K = \{1\}, \tag{2.1}$$

allora G si dice estensione **spezzante** di $\overline{N}$ con $\overline{K}$ o che G si **fattorizza come prodotto semidiretto interno** del sottogruppo N con il sottogruppo K. Si osservi che, dal Secondo Teorema di Omomorfismo, segue che

$$K \cong G/N \cong \overline{K}.$$

Se G è un gruppo ed N è un suo sottogruppo (non necessariamente normale), un **complemento** di N in G è un sottogruppo K che verifica le condizioni (2.1). In particolare se N è un sottogruppo normale di G, G è un'estensione spezzante di N con G/N se e solo se N ha un complemento in G.

Si osservi che in generale il complemento non è unico: nell'esempio 1 della sezione precedente gli insieme $A := \{(a, 0)|a \in \mathbf{Z}/2\mathbf{Z}\}$, $B := \{(0, b)|b \in \mathbf{Z}/2\mathbf{Z}\}$ e $D := \{(a, a)|a \in \mathbf{Z}/2\mathbf{Z}\}$ sono sottogruppi di $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ed A ha

sia B che D come complementi. Inoltre non sempre esistono complementi, sempre nell'esempio 1 della sezione precedente il sottogruppo $2\mathbf{Z}/4\mathbf{Z}$ non ha complementi.

Vedremo in seguito, con i prodotti semidiretti, che tutte le estensioni spezzanti di un gruppo $\overline{N}$ per un gruppo $\overline{H}$ possono venire, in pratica, determinate quando si conoscono il gruppo $Aut(\overline{N})$ degli automorfismi di $\overline{N}$ e gli omomorfismi di $\overline{H}$ in $Aut(\overline{N})$. Studiare le estensioni non spezzanti è molto più difficile, in questo corso mostreremo solo che se $\overline{N}$ e $\overline{H}$ sono finiti ed hanno ordine coprimo, allora ogni estensione di $\overline{N}$ per $\overline{H}$ è spezzante. Questo è una parte del Teorema di Schur-Zassenhaus, di importanza fondamentale nella teoria dei gruppi finiti.

2.2.2 Endomorfismi idempotenti e fattorizzazioni

Vediamo ora come le fattorizzazioni di un gruppo G come prodotto semidiretto di due suoi sottogruppi corrispondono ad endomorfismi **idempotenti** di G, cioè a quegli endomorfismi π di G tali che

$$\pi\pi = \pi.$$

Proposizione 2.2.1 *Sia G un gruppo.*

1. *Se π è un endomorfismo idempotente di G, allora*

$$G = \ker(\pi)G^{\pi} \ \ e \ \ \ker(\pi) \cap G^{\pi} = \{1\}.$$

2. *Viceversa, se G è il prodotto di due sottogruppi N ed K con $N \trianglelefteq G$, e $K \cap N = \{1\}$, allora esiste un endomorfismo idempotente π di G tale che $N = \ker(\pi)$ e $K = G^{\pi}$.*

Dimostrazione. Sia π un endomorfismo idempotente di G. Se $t \in \ker(\pi) \cap G^{\pi}$, allora $t = h^{\pi}$ per qualche $h \in G$. Poiché π è idempotente, segue che

$$t = h^{\pi} = h^{\pi\pi} = t^{\pi} = 1,$$

da cui $\ker(\pi) \cap G^{\pi} = \{1\}$. Inoltre, per ogni $g \in G$, risulta

$$g = (g(g^{\pi})^{-1})(g^{\pi})$$

e $g(g^{\pi})^{-1} \in ker(\pi)$, infatti

$$(g(g^{\pi})^{-1})^{\pi} = g^{\pi}((g^{\pi})^{-1})^{\pi} = g^{\pi}((g^{\pi})^{\pi})^{-1} = g^{\pi}(g^{\pi})^{-1} = 1,$$

da cui la tesi.

Viceversa, se G è il prodotto di due suoi sottogruppi K e N con N normale in G e $K \cap N = \{1\}$, allora ogni elemento g di G si scrive in modo unico come prodotto di un elemento k_g di K e di un elemento n_g di N. L'applicazione

$$\begin{array}{rccc} \tau\colon & G & \to & G \\ & g & \mapsto & k_g \end{array}$$

è un endomorfismo idempotente di G il nucleo e la cui immagine coincidono con N e K rispettivamente. Chiameremo tale endomorfismo **proiezione** di G su K associata alla decomposizione di G come prodotto semidiretto dei sottogruppi K e N. Chiaramente la restrizione di π al sottogruppo K coincide con l'applicazione identica di K. ■.

2.3 Serie di composizione

Sia G un gruppo e supponiamo che N_1 sia un sottogruppo **normale massimale** di G, cioè $N_1 \trianglelefteq G$ e se $N_1 \leq M \leq G$ con $M \trianglelefteq G$, allora $M = N_1$ o $M = G$. Per il teorema di corrispondenza il gruppo quoziente G/N_1 non possiede sottogruppi normali propri. Un gruppo non identico privo di sottogruppi normali propri si dice **semplice**. Abbiamo così dimostrato il seguente risultato:

Lemma 2.3.1 *Se N è un sottogruppo normale massimale di un gruppo G, allora il gruppo quoziente G/N è semplice.*

Sia ora N_2 un sottogruppo normale massimale di N_1. Allora, per il lemma precedente anche il gruppo quoziente N_1/N_2 è semplice (si osservi che in generale non è vero che N_2 sia ancora normale in G (Esercizio 5.3.5)).

Se il gruppo G è finito, esiste un intero positivo l tale che, procedendo in questo modo, dopo l passi si ottiene una catena di sottogruppi

$$N_0 > N_1 > \cdots > N_l \tag{2.2}$$

tali che, per ogni $i \in \{0, ..., l-1\}$, tali che

1. $N_0 = G$ e $N_l = \{1\}$;
2. $N_{i+1} \trianglelefteq N_i$ e
3. i gruppi quoziente N_i/N_{i+1} sono semplici e non triviali.

Una catena di sottogruppi che verifica le condizioni 1. e 2. si dice **serie subnormale** del gruppo G, una serie subnormale che verifica anche la condizione 3. si dice **serie di composizione** del gruppo G. Il numero l si dice **lunghezza della serie**.

Più in generale, se N e H sono sottogruppi di di G con $N \leq H$ ed esiste una catena di sottogruppi

$$N_0 = H > N_1 > \cdots > N_r = N \tag{2.3}$$

tali che, per ogni $i \in \{0, ..., r-1\}$, $N_{i+1} \trianglelefteq N_i$, diremo che N è un sottogruppo **subnormale** di H e la serie si dice **serie subnormale tra H e N**. Il minimo delle lunghezze delle serie subnormali tra N e H si dice **difetto di subnormalità** di N in H. In particolare N è normale in H se e solo se ha difetto di subnormalità in H uguale a 1. Una serie subnormale tra H e N che verifica

anche la condizione 3. si dice **serie di composizione da H a N**. Se $H = G$ diremo semplicemente che N è subnormale. Date due serie subnormali tra H e N

$$\mathcal{H}\colon H_0 = H > H_1 > \cdots > H_l = N$$

e

$$\mathcal{K}\colon K_0 = H > K_1 > \cdots > K_m = N$$

di un gruppo G, diremo che $\mathcal{H}$ **contiene** la (è un **raffinamento** della) serie $\mathcal{K}$ se $\{K_i | i = 1, ..., m\} \subseteq \{H_i | i = 1, ..., l\}$.

Abbiamo dimostrato che ogni gruppo finito possiede una serie di composizione. In generale non è vero che un gruppo infinito possieda serie di composizione. Ad esempio, il gruppo additivo dei numeri interi è privo di sottogruppi minimali (e quindi privo di serie di composizione). Nell'Esercizio 2.6.10 viene dato un esempio di un gruppo infinito abeliano privo di sottogruppi massimali.

I gruppi quoziente N_i/N_{i+1} si dicono **fattori della serie**. Nel caso di una serie di composizione essi si dicono **fattori di composizione**. Più avanti vedremo che i fattori di composizione dipendono solo dal gruppo G e non dalla serie di composizione. Essi costituiscono gli atomi di cui è costituito il gruppo G. Per questo motivo un problema centrale nella teoria dei gruppi finiti è stato quello di determinare i gruppi semplici. La Classificazione dei Gruppi Semplici Finiti (CSFG) è stata finalmente raggiunta negli anni '80. Per la sua enorme complessità, la dimostrazione di questo teorema è unica in matematica. Per questo motivo è tutt'ora in corso un processo di revisione il cui scopo è di riorganizzare ed eventualmente semplificare questa dimostrazione. Molto facile è invece determinare quali sono i gruppi semplici abeliani. Si ha infatti il seguente risultato.

Proposizione 2.3.2 *Se G è un gruppo semplice abeliano, allora il suo ordine è un numero primo p e G è isomorfo a $\mathbf{Z}/p\mathbf{Z}$.*

DIMOSTRAZIONE. Sia $x \in G$, $x \neq 1$. Allora $\langle x \rangle$ è un sottogruppo di G ed è normale perché G è abeliano (Esercizio 1.2.7). Dunque $G = \langle x \rangle$ perché G è semplice. Ne segue che G è ciclico e quindi per la Proposizione 1.1.20 isomorfo ad un quoziente di $\mathbf{Z}$. Poiché $\mathbf{Z}$ possiede sottogruppi propri e $\mathbf{Z}_n$ non ha sottogruppi propri se e solo se n è un numero primo, segue la tesi. ∎

I gruppi alterni A_n con $n \geq 5$ sono semplici; daremo più avanti una dimostrazione di ciò. Questi costituiscono una delle due famiglie infinite di gruppi semplici finiti. L'altra famiglia è costituita dai gruppi di tipo Lie che sono dei particolari gruppi di matrici. Oltre ai gruppi appartenenti a queste due famiglie ci sono 26 gruppi semplici detti sporadici.

2.4 Sottogruppi subnormali

Nel paragrafo precedente abbiamo dato la definizione di sottogruppo subnormale. La proprietà principale della subnormalità è che, a differenza della normalità,

questa è una relazione transitiva nell'insieme dei sottogruppi di un gruppo. La subnormalità è una condizione più debole della normalità; si vede immediatamente che un sottogruppo normale è subnormale mentre in generale il viceversa non è vero (Esercizio 5.3.5). Vale però il seguente risultato (la dimostrazione è facile e viene lasciata per esercizio).

Lemma 2.4.1 *Sia G un gruppo. Allora*

1. *un sottogruppo subnormale di un sottogruppo subnormale di G è subnormale in G (essere subnormale in è una relazione transitiva);*
2. *un sottogruppo subnormale massimale di G è normale;*
3. *un sottogruppo normale massimale di G è anche subnormale massimale.*

Nel gruppo simmetrico S_3 il sottogruppo generato dalla trasposizione $(1, 2)$ è massimale (ha indice 3) ma non è normale quindi non è subnormale.

Si vede facilmente (Esercizio 2.6.11) che un epimorfismo di gruppi manda sottogruppi subnormali del dominio in sottogruppi subnormali dell'immagine. In particolare, se H è un sottogruppo normale ed N è un sottogruppo subnormale di un gruppo G, per il Teorema di Corrispondenza HN è un sottogruppo subnormale di G. Supponiamo ora che H sia normale massimale e non contenga N. Allora, HN è un sottogruppo subnormale di G che contiene propriamente H. Per il punto 2. del Lemma 2.4.1, HN coincide con G. Per il secondo teorema di omomorfismo,

$$G/H = HN/H \cong N/H \cap N$$

poiché H è normale massimale in G, G/H e $N/H \cap N$ sono gruppi semplici e quindi $H \cap N$ è normale massimale in N. Abbiamo così dimostrato il seguente risultato

Lemma 2.4.2 *Sia N un sottogruppo subnormale di un gruppo G ed H un sottogruppo normale massimale di G non contenente N. Allora $N \cap H$ è un sottogruppo normale massimale di N.*

Osserviamo che se N non è subnormale il lemma in generale non è più vero. Ad esempio il gruppo alterno A_5, come abbiamo già detto, è semplice e quindi $\{1\}$ è un sottogruppo normale massimale di A_5. D'altra parte A_5 contiene un sottogruppo isomorfo a S_3 (Esercizio 2.6.14). Se N è questo sottogruppo, allora N ha ordine 6 e possiede un sottogruppo normale di ordine 3. Ne segue che $\{1\} = \{1\} \cap N$ non è normale massimale in N.

2.5 Teorema di Jordan-Hölder

Osserviamo che un gruppo può avere diversi sottogruppi massimali normali e quindi può avere diverse serie di composizione, l'esempio più semplice è il gruppo $\mathbf{Z}_6$. G possiede esattamente due sottogruppi propri: $2\mathbf{Z}_6$ e $3\mathbf{Z}_6$ che sono massimali, minimali e normali. Quindi G possiede le due serie di composizione

$$\mathbf{Z}_6 > 2\mathbf{Z}_6 > \{1\}$$

e

$$\mathbf{Z}_6 > 3\mathbf{Z}_6 > \{1\}.$$

Si osservi che entrambe le serie hanno la medesima lunghezza (cioè 2), inoltre

$$\mathbf{Z}_6/2\mathbf{Z}_6 \cong 3\mathbf{Z}_6$$

e

$$\mathbf{Z}_6/3\mathbf{Z}_6 \cong 2\mathbf{Z}_6,$$

cioè i fattori di composizione sono a due a due isomorfi. Questo fatto vale in generale. Più precisamente definiamo una relazione d'equivalenza tra le serie subnormali da un gruppo G ad un suo sottogruppo subnormale N nel modo seguente:
se

$$\mathcal{R}\colon R_0 = G > R_1 > \cdots > R_l = N$$

e

$$\mathcal{S}\colon S_0 = G > S_1 > \cdots > S_m = N$$

sono due serie subnormali da G a N allora diremo che sono **equivalenti** se sono soddisfatte le seguenti condizioni

1. $l = m$
2. esiste una permutazione σ di $0, ..., l-1$ tale che

$$R_i/R_{i+1} \cong S_{i^\sigma}/S_{i^\sigma+1}.$$

Teorema 2.5.1 (Teorema di Jordan-Hölder) *Sia G un gruppo. Se G possiede una serie di composizione, allora tutte le serie di composizione sono tra loro equivalenti*

In questi appunti non faremo uso del teorema di Jordan-Hölder. Si è voluto comunque includere questo risultato e la sua dimostrazione perchè in questa vengono applicati molti dei risultati finora ottenuti.

Premettiamo alla dimostrazione del teorema di Jordan-Hölder i seguenti lemmi. I primi due dovrebbero essere, a questo punto, evidenti e la dimostrazione viene lasciata per esercizio.

Lemma 2.5.2 *Sia G un gruppo ed N un suo sottogruppo subnormale. Siano*

$$G_0 = G > G_1 > ... > G_r = N \tag{2.4}$$

una serie subnormale da G a N e

$$N_0 = N > N_1 > ... > N_t = \{1\} \tag{2.5}$$

una serie subnormale di N. Allora la serie

$$G_0 = G > G_1 > ... > G_r = N_0 = N > N_1 > ... > N_t = \{1\} \tag{2.6}$$

è una serie subnormale di G. Inoltre se le serie (2.4) e (2.5) sono di composizione, anche la (2.6) è di composizione.

Lemma 2.5.3 *Sia G un gruppo ed N un suo sottogruppo subnormale. Siano*

$$G_0 = G > G_1 > ... > G_r = N \tag{2.7}$$

e

$$H_0 = G > H_1 > ... > H_r = N \tag{2.8}$$

due serie subnormali equivalenti da G a N e

$$G_r = N > G_{r+1} > ... > G_t = \{1\} \tag{2.9}$$

e

$$H_r = N > H_{r+1} > ... > H_t = \{1\} \tag{2.10}$$

due serie subnormali equivalenti di N. Allora le serie

$$G_0 > G_1 > ... > G_t \tag{2.11}$$

e

$$H_0 > H_1 > ... > H_t \tag{2.12}$$

sono due serie subnormali equivalenti di G.

Lemma 2.5.4 *Sia G un gruppo con una serie di composizione $\mathcal{G}$ di lunghezza r e sia H un sottogruppo normale massimale di G. Allora G ha una serie di composizione equivalente alla $\mathcal{G}$ il cui primo termine è H.*

DIMOSTRAZIONE. Sia $\mathcal{G}$ la serie

$$G_0 = G > G_1 > ... > G_r = \{1\} \tag{2.13}$$

e sia t il più grande intero tale che $G_t \not\leq H$. Allora per ogni $0 < i \leq t$ risulta

$$G_{i-1} = G_i(G_{i-1} \cap H) \text{ e } G_i \cap H = G_i \cap (G_{i-1} \cap H). \tag{2.14}$$

Infatti, per il Lemma 2.4.2, essendo H normale massimale in G e G_{i-1} subnormale in G, $G_{i-1} \cap H$ è normale massimale in G_{i-1}. Per il Lemma 2.4.1, essendo $G_i \trianglelefteq G_{i-1}$ e $G_i \not\leq G_{i-1} \cap H$, risulta $G_{i-1} = G_i(G_{i-1} \cap H)$. La seconda uguaglianza è ovvia, essendo $G_i \leq G_{i-1}$. Per il Secondo Teorema di Omomorfismo, otteniamo dalla (2.14)

$$\begin{aligned} G_{i-1}/G_i &= G_i(G_{i-1} \cap H)/G_i \cong (G_{i-1} \cap H)/(G_i \cap (G_{i-1} \cap H)) \\ &= (G_{i-1} \cap H)/(G_i \cap H), \end{aligned}$$

cioè

$$G_{i-1}/G_i \cong (G_{i-1} \cap H)/(G_i \cap H) \tag{2.15}$$

Infine, ancora per il Secondo Teorema di Omomorfismo,

$$\begin{aligned} G_{i-1}/(G_{i-1} \cap H) &= G_i(G_{i-1} \cap H)/(G_{i-1} \cap H) \cong G_i/(G_i \cap (G_{i-1} \cap H)) \\ &= G_i/G_i \cap H. \end{aligned}$$

Poiché ciò vale per ogni $0 < i \leq t$, si ottiene

$$G_i/(G_i \cap H) \cong G_{i-1}/(G_{i-1} \cap H) \cong \ldots \cong G_0/(G_0 \cap H) = G/H. \tag{2.16}$$

Osserviamo che $G_{t+1} \leq (G_t \cap H)$. D'altra parte, poichè G_{t+1} è normale massimale in G_t e $(G_t \cap H)$ è un sottogruppo normale proprio di G_t risulta $G_{t+1} = G_t \cap H$.

Consideriamo ora la serie

$$H_0 = G > H_1 > \ldots > H_{t+1}$$

dove $H_i = G_{i-1} \cap H$ per ogni $0 < i \leq t+1$ (in particolare si osservi che $H_1 = H$ e $H_{t+1} = G_{t+1}$). Sia σ la permutazione di $\{0, 1, \ldots, t\}$ che manda i in $i+1$ per $0 \leq i < t$ e t in 0. Per le (2.15) e (2.16) risulta $G_i/G_{i+1} \cong H_{i^\sigma}/H_{i^\sigma+1}$ per ogni $0 \leq i \leq t+1$ e quindi questa serie è equivalente alla serie

$$G_0 > G_1 > \ldots > G_{t+1}.$$

Per il Lemma 2.5.3 la serie

$$H_0 = G > H_1 = H > \ldots > H_{t+1} = G_{t+1} > G_{t+2} > \ldots > G_r = \{1\}$$

è equivalente alla serie $\mathcal{G}$ ed $H_1 = H$. ■

Dimostriamo ora il Teorema di Jordan-Hölder. Siano

$$G_0 = G > G_1 > ... > G_r = \{1\} \tag{2.17}$$

e

$$H_0 = G > H_1 > ... > H_s = \{1\} \tag{2.18}$$

due serie di composizione del gruppo G. Dimostriamo, per induzione su r che sono equivalenti. Se $r = 1$, il gruppo G è semplice ed il risultato è immediato. Sia $r > 1$. Per il Lemma 2.5.4 esiste una serie di composizione

$$K_0 = G > K_1 = H_1 > ... > K_r = \{1\} \tag{2.19}$$

equivalente alla serie (2.17). Per ipotesi induttiva le serie

$$K_1 = H_1 > ... > K_r = \{1\}$$

e

$$H_1 > ... > H_s = \{1\}$$

sono equivalenti essendo serie di composizione del gruppo H_1. Quindi, per il Lemma 2.5.3, le serie (2.19) e (2.18) sono equivalenti. Per la transitività dell'equivalenza, anche la (2.17) e la (2.18) sono equivalenti.

2.6 Esercizi

Esercizio 2.6.1 *Sia G il prodotto di due suoi sottogruppi N ed K. Si provi che $N \cap K = \{1\}$ se e solo se ogni elemento di G si può scrivere in modo unico come prodotto di un elemento di N e di un elemento di K.*

Esercizio 2.6.2 *Sia G un gruppo abeliano di ordine nk con n, k interi naturali di ordine coprimo. Si provi che G è estensione spezzante di un gruppo N in cui ogni elemento ha ordine che divide n con un gruppo K in cui ogni elemento ha ordine che divide k.*

Esercizio 2.6.3 *Con le ipotesi e le notazioni dell'esercizio precedente, si provi che $|N| = n$ e $|K| = k$.*

Esercizio 2.6.4 *Si provi che se G è un gruppo ciclico finito ed N è un sottogruppo di G, allora N ha un complemento se e solo se $|N|$ è coprimo con $|G : N|$.*

Esercizio 2.6.5 *Sia V un gruppo abeliano finito in cui ogni ogni elemento ha ordine p. Si provi che ogni sottogruppo possiede un complemento e che tale complemento non è unico.*

Esercizio 2.6.6 *Sia G un gruppo, N un sottogruppo normale di G e K un complemento di N in G. Si provi che, per ogni $n \in N$, anche K^n è un complemento di N in G.*

Esercizio 2.6.7 *Sia G un gruppo, N un sottogruppo normale di G e K un complemento di N in G. Si provi che se K è l'unico complemento di N in G allora $K \trianglelefteq G$.*

In alcuni testi viene data la seguente definizione di estensione. Siano N e H gruppi, un gruppo G si dice **estensione** di N con H se esistono due omomorfismi $\iota\colon N \to G$ e $\pi\colon G \to H$ tali che

1. ι è iniettivo;
2. π è suriettivo;
3. $N^\iota = ker(\pi)$.

Inoltre G si dice **spezzante** se esiste un omomorfismo

$$\delta\colon H \to G$$

tale che

$$h^{\delta\pi} = h$$

per ogni $h \in H$.

Esercizio 2.6.8 *Si provi che queste definizioni di estensione ed estensione spezzante sono equivalenti a quelle che abbiamo date.*

Esercizio 2.6.9 *Sia G un gruppo finito. Si provi che ogni serie subnormale di G è contenuta in una serie di composizione.*

Esercizio 2.6.10 *Sia p un numero primo indichiamo con $\mathbf{Z}_{p^\infty}$ l'insieme dei numeri complessi z tali che $z^{p^n} = 1$ per qualche $n \in N$.*

1. *Si dimostri che $\mathbf{Z}_{p^\infty}$ è un sottogruppo del gruppo moltiplicativo dei numeri complessi;*
2. *Si dimostri che gli unici sottogruppi di $\mathbf{Z}_{p^\infty}$ sono i sottogruppi*

$$\mathbf{Z}_{p^k} = \{z | z \in \mathbf{C}, z^{p^k} = 1\}$$

   al variare di k in $\mathbf{N}$.

3. *Si dimostri che $\mathcal{L}(\mathbf{Z}_{p^\infty})$ è totalmente ordinato e non ha elementi massimali.*

Esercizio 2.6.11 *Sia $\phi: G \to H$ un omomorfismo suriettivo di gruppi. Si provi che se N è un sottogruppo subnormale di G, allora N^ϕ è un sottogruppo subnormale di G^ϕ.*

Esercizio 2.6.12 *Sia G un gruppo con una serie di composizione. Siano H_1 e K_1 sottogruppi normali massimali di G. H un sottogruppo normale massimale di H_1 e K un sottogruppo normale massimale di K_1. Si provi che $\langle H, K\rangle$ è un sottogruppo subnormale di G.* (Suggerimento: per induzione sulla lunghezza di una serie di composizione di G. Se $\langle HK\rangle$ è contenuto in H_1 oppure in K_1 la tesi segue per induzione. Altrimenti $G = HK_1 = H_1K$. Ne segue che per ogni $g \in G$ esistono $h \in H, h_1 \in H_1, k \in K$ e $k_1 \in K_1$ tali che $g = h_1k = k_1h$. Si deduca da ciò che $\langle H^g K^g\rangle \subseteq \langle H, K\rangle$).

Esercizio 2.6.13 *Si provi che se G è un gruppo con una serie di composizione e H, K sono sottogruppi subnormali di G, allora anche $H \cap K$ e $\langle H, K\rangle$ sono subnormali in G.*(Suggerimento: per $H \cap K$ si consideri una serie subnormale da G a H e la serie da H a $H \cap K$ che si ottiene intersecando con H i sottogruppi di una serie subnormale da G a K. Per $\langle H, K\rangle$ si considerino due serie di composizione da G a H e da G a K e, per induzione sulla somma delle loro lunghezze, ci si riduca alla situazione dell'esercizio precedente).

Esercizio 2.6.14 *Si provi che per ogni $n > 3$ il gruppo alterno A_n contiene un sottogruppo isomorfo al gruppo simmetrico S_{n-2}* (suggerimento: si consideri l'insieme delle permutazioni del tipo $\sigma\rho$ ove σ lascia fissi $n-1$ ed n e ρ è la permutazione identica oppure la permutazione $(n-1, n)$ a seconda che σ sia di segno pari o dispari).

Esercizio 2.6.15 *Sia $\phi: G \to H$ un omomorfismo suriettivo di gruppi.*

1. *Si dimostri che se* $G_0 = G > G_1 > \ldots > G_r = \{1_G\}$ *è una serie subnormale di* G *allora la serie* $G_0^\phi = H \geq G_1^\phi \geq \ldots \geq G_r^\phi = \{1_H\}$ *è una serie subnormale di* H.

2. *Si provi che, per ogni* $O \leq i < r$, *se il gruppo* G_i/G_{i-1} *è semplice, allora il gruppo* G_i^ϕ/G_{i-1}^ϕ *è semplice oppure identico.*

3. *si dimostri che se* G *possiede una serie di composizione, allora anche* H *possiede una serie di composizione.*

Esercizio 2.6.16 *Sia* G *un gruppo con una serie di composizione ed* N *un suo sottogruppo normale.*

1. *Si provi che esiste una serie di composizione di* G *contenente la serie* $G > N > \{1\}$.

2. *Si dimostri che ogni serie subnormale di* G *è contenuta in una serie di composizione* (suggerimento: si trovi una serie di composizione da G a N con il teorema di corrispondenza e l'esercizio precedente, si trovi poi una serie di composizione di N in modo analogo alla dimostrazione del lemma 2.5.4).

Capitolo 3

Gruppi abeliani finiti

In questo capitolo vogliamo studiare la struttura dei gruppi abeliani finiti. Esempi di gruppi abeliani sono il gruppo additivo dei numeri interi ed i suoi quozienti. Questi, come si è detto nel primo capitolo, sono tutti gruppi ciclici e, viceversa, ogni gruppo ciclico è isomorfo ad uno di questi. Osserviamo poi che la somma diretta di gruppi abeliani è ancora un gruppo abeliano. Quindi, in particolare, ogni somma diretta di gruppi ciclici finiti è un gruppo abeliano finito. Nelle pagine seguenti dimostreremo il viceversa, cioè che ogni gruppo abeliano finito è somma diretta di gruppi ciclici. Questo è spesso noto anche come il Teorema di Frobenius-Stickelberger. La dimostrazione è divisa in due parti: nella prima mostreremo che un gruppo abeliano finito è somma diretta di gruppi **primari**, gruppi cioè in cui ogni elemento ha ordine una potenza dello stesso numero primo; nella seconda parte mostreremo che ogni gruppo primario è, a sua volta, somma diretta di gruppi ciclici. Il seguente risultato dovrebbe essere noto dal corso di Algebra (si dimostra comunque facilmente per induzione su $|n|$).

Lemma 3.0.17 *Sia G un gruppo, a e b elementi di G e m, n numeri interi allora:*

1. $a^{m+n} = a^m \cdot a^n$;
2. *se G è abeliano, allora $(ab)^n = a^n b^n$.*

Dovrebbe essere ormai evidente come informazioni sulla struttura di $\mathbf{Z}$ e dei suoi quozienti siano fondamentali per lo studio dei gruppi abeliani finiti. In particolare sarà utile il seguente risultato noto dal corso di Algebra.

Lemma 3.0.18 *Siano $n_1, \ldots, n_h$ numeri interi non tutti nulli e sia d un loro massimo comun divisore. Allora esistono degli interi $x_1, \ldots, x_h$ tali che*

$$d = \sum_{i=1}^{h} n_i x_i$$

Come è uso indicheremo il massimo comun divisore positivo tra m ed n con il simbolo (m, n).

Ricordiamo che, se p è un numero primo, un gruppo P si dice **p-primario** o **p-gruppo**, se ogni elemento di P ha ordine una potenza di p.

Corollario 3.0.19 *Se P è un p-gruppo abeliano finito, allora $|P|$ è una potenza di p.*

DIMOSTRAZIONE. Proviamo la tesi per induzione sull'ordine di P. Se $|P| = 1$ non c'è nulla da dimostrare perché $1 = p^0$. Supponiamo che $|P| > 1$. Sia $g \in P$, $g \neq 1$ e $N = \langle g \rangle$. Se $N = G$, allora $|G| = |N| = exp(N)$ per quanto osservato sull'esponente dei gruppi ciclici. Per il Lemma 1.1.13 N e G/N sono p-gruppi finiti. Inoltre, poiché N un sottogruppo proprio non identico di G, N e G/N hanno ordine strettamente minore di $|G|$, quindi, per ipotesi induttiva, hanno ordine una potenza di p. Per il teorema di Lagrange $|G| = |G/N||N|$ e quindi $|G|$ è una potenza di p. ∎

Questo risultato è vero in generale per ogni p-gruppo finito, non necessariamente abeliano, ma la dimostrazione è più difficile e si vedrà in seguito come conseguenza dei Teoremi di Sylow.

Lemma 3.0.20 *Siano A e B due gruppi di esponente rispettivamente h e k. Allora $exp(A \times B)$ è il minimo comune multiplo di h e k.*

DIMOSTRAZIONE. Sia d il minimo comune multiplo di h e k. Allora $d = hd_1$ e $d = kd_2$ con d_1, d_2 in $\mathbf{Z}$. Ne segue che, per ogni $(a, b) \in A \times B$ con $a \in A$ e $b \in B$, risulta

$$(a, b)^d = (a^d, b^d) = (a^{hd_1}, b^{kd_2}) = (1, 1),$$

dunque $exp(A \times B) \leq d$. D'altra parte, per il Lemma 1.1.13, h e k dividono $exp(A \times B)$, da cui la tesi. ∎

3.1 Decomposizione primaria

In questa sezione sia A un gruppo abeliano di esponente finito n. Se t è un intero, indichiamo con A^t l'insieme $\{a^t | a \in A\}$.

Lemma 3.1.1 *Siano t, h e k interi con h e k coprimi e $n = hk$.*

1. *A^t è un sottogruppo di A.*
2. *$exp(A^t) = n/d$ dove d è il massimo comun divisore tra t e n.*
3. *$A = A^h A^k$ e $A^h \cap A^k = \{1\}$ (dunque $A = A^h \times A^k$).*
4. *A^k è l'insieme degli elementi di A che hanno ordine che divide h.*

DIMOSTRAZIONE. La prima affermazione segue immediatamente dalle, regole delle potenze, tenuto conto che A è abeliano. Sia $l = exp(A^t)$ e siano $\overline{n} = n/d$ e $\overline{t} = t/d$. Poiché d è il massimo comun divisore tra n e t, $\overline{n}$ e $\overline{t}$ sono coprimi. Proviamo che l divide $\overline{n}$. Sia $x \in A^t$. Allora esiste $a \in A$ tale che $x = a^t$ e quindi

$$x^{\overline{n}} = (a^t)^{\overline{n}} = a^{\overline{t}d\overline{n}} = (a^n)^{\overline{t}} = 1,$$

da cui la tesi per il Corollario 1.1.11. Viceversa, poiché $a^t \in A^t$ per ogni $a \in A$, segue che $a^{tl} = 1$ per ogni $a \in A$. Dunque n divide tl, cioè

$$d\overline{n} \text{ divide } d\overline{t}l.$$

Dividendo per d, otteniamo

$$\overline{n} \text{ divide } \overline{t}l,$$

da cui, essendo $\overline{n}$ e $\overline{t}$ coprimi,

$$\overline{n} \text{ divide } l,$$

il che prova la seconda affermazione. Da questo segue in particolare che

$$exp(A^h) = k \text{ e } exp(A^k) = h \tag{3.1}$$

Proviamo la terza affermazione. Poiché h e k sono coprimi, esistono r e s in $\mathbf{Z}$ tali che

$$hr + ks = 1.$$

Da questo segue che, per ogni $a \in A$,

$$a = a^1 = a^{hr+ks} = (a^h)^r(a^k)^s \in A^hA^k,$$

da cui segue che

$$A = A^hA^k.$$

Infine, sia $x \in A^h \cap A^k$. Allora, per (3.1), $x^h = x^k = 1$, da cui

$$x = x^1 = x^{hr+ks} = (x^h)^r(x^k)^s = 1.$$

Infine, se $a \in A^k$, $a^h = 1$, quindi, per il Lemma 1.1.9, l'ordine di a divide h. Viceversa, sia x un elemento di ordine l con l che divide h. Allora l è coprimo con k (perché k è coprimo con h) e quindi, come sopra esistono degli interi r ed s tali che $1 = lr + ks$, da cui $x = x^1 = x^{lr+ks} = (x^l)^r(x^k)^s = (x^k)^s \in A^k$. ∎

Sia p un numero primo, indichiamo con A_p l'insieme degli elementi di A il cui ordine è una potenza di p. A_p si dice **componente p-primaria** di A.

Dalle regole delle potenze segue immediatamente che A_p è un p-sottogruppo di A, quindi, per il il Corollario 3.0.19, si ottiene

Lemma 3.1.2 *Se $|A_p|$ è finito, $|A_p|$ è una potenza di p.*

Lemma 3.1.3 *Sia p^t la massima potenza di p che divide n. Allora $A_p = A^{n/p^t}$.*

DIMOSTRAZIONE. Segue immediatamente dal punto (4) del Lemma 3.1.1 tenendo presente che p^t e n/p^t sono interi coprimi. ∎

Teorema 3.1.4 (DECOMPOSIZIONE PRIMARIA) *Sia A un gruppo abeliano di esponente finito n e sia $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ la fattorizzazione di n come prodotto di potenze dei numeri primi distinti $p_1, p_2, \dots, p_t$. Allora $A = A_{p_1} \times A_{p_2} \times \dots \times A_{p_t}$.*

DIMOSTRAZIONE. Per induzione su t. Se $t = 1$, allora $A = A_{p_1}$ e non c'è nulla da dimostrare. Sia $p = p_1$ e $K = A^{p^t}$. Per il Lemma 3.1.1, K è un gruppo di esponente $p_2^{k_2} p_3^{k_3} \dots p_t^{k_t}$ e

$$A = A_p \times K.$$

Per ipotesi induttiva

$$K = K_{p_2} \times K_{p_3} \times \dots \times K_{p_t},$$

dunque

$$A = A_{p_1} \times K_{p_2} \times \dots \times K_{p_t}.$$

Per il punto (4) del Lemma 3.1.1, $K_{p_i} = A_{p_i}$ per ogni $i \in \{2, \dots, t\}$, da cui segue la tesi. ∎

Concludiamo questa sezione osservando che il Teorema di Decomposizione Primaria può essere generalizzato a qualsiasi gruppo abeliano di torsione (per la definizione, vedi esercizio 3.5.1). Il lettore può provarci per esercizio.

3.2 Decomposizione di un p-gruppo abeliano finito

In questa sezione p è un numero primo e P è un p-gruppo abeliano finito.

Lemma 3.2.1 *Siano X e Y sottogruppi ciclici di P e supponiamo che $|X| \geq |Y|$. Allora esiste un sottogruppo ciclico K di XY tale che $XY = XK$ e $X \cap K = \{1\}$ (quindi $XY = X \times K$).*

DIMOSTRAZIONE. Siano x un generatore di X, y un generatore di Y e $T = X \cap Y$. Se $T = \{1\}$ l'asserto è dimostrato con $K = Y$. Supponiamo che $T \neq \{1\}$. Poiché X e Y hanno ordine una potenza di p, per il Teorema di Lagrange esistono degli interi a e b tali che

$$|X : T| = p^a \text{ e } |Y : T| = p^b.$$

Osserviamo che, poichè $|X| \geq |Y|$, $a \geq b$, in particolare

$$a - b \text{ è un intero maggiore o uguale a } 0.$$

Per quanto visto sui sottogruppi dei p-gruppi ciclici,

$$\langle x^{p^a} \rangle = T = \langle y^{p^b} \rangle$$

e quindi esiste un intero m coprimo con p tale che

$$y^{p^b} = x^{mp^a}.$$

Poichè m è coprimo con p, e x genera X, anche x^m genera X, quindi, a meno di sostituire x con x^m possiamo supporre che

$$y^{p^b} = x^{p^a}. \tag{3.2}$$

Sia $k = y^{-1}x^{p^{a-b}}$ e $K = \langle k \rangle$. Allora $K \leq XY$. D'altra parte $X \leq XK$ e, poiché $y = x^{p^{a-b}}k^{-1}$, anche $Y = \langle y \rangle \leq XK$, dunque $XY = XK$. Per il Secondo Teorema di Omomorfismo

$$|K/(X \cap K)| = |XK/X| = |XY/X| = |Y/(X \cap Y)| = |Y/T| = p^b,$$

quindi, per provare che $X \cap K = \{1\}$, basta provare che K ha ordine minore di p^b e infatti, per (3.2),

$$k^{p^b} = (y^{-1}x^{p^{a-b}})^{p^b} = (y^{p^b})^{-1}x^{p^a} = 1.$$

■

Lemma 3.2.2 *Sia X un sottogruppo ciclico di ordine massimo in P. Allora esiste un sottogruppo H tale che $P = XH$ e $X \cap H = \{1\}$*

Dimostrazione. Sia $\mathcal{K}$ il sottoinsieme dei sottogruppi di P che hanno intersezione identica con X. Chiaramente $\mathcal{K}$ è non vuoto ($\{1\} \in \mathcal{K}$). Sia H un elemento massimale, rispetto all'inclusione, di $\mathcal{K}$. In particolare

$$X \cap H = \{1\}.$$

Proviamo che $P = XH$. Supponiano per assurdo che $P > XH$ e sia $y \in P \backslash XH$. Poniamo $Y = \langle y \rangle$, $\overline{X} := XH/H$ e $\overline{Y} := YH/H$. Per il Secondo Teorema di Omomorfismo, la massimalità di $|X|$ ed il fatto che $X \cap H = \{1\}$ otteniamo

$$|\overline{Y}| = |(YH)/H| = |Y/(Y \cap H)| \leq |Y| \leq |X| = |X/(X \cap H)| = |(XH)/H| = |\overline{X}|.$$

Per il Lemma 3.2.1 esiste un sottogruppo $\overline{K}$ di $\overline{XY}$ tale che $\overline{XY} = \overline{XK}$ e $\overline{X} \cap \overline{K} = \{1\}$.

Per il Teorema di Corrispondenza esiste un sottogruppo K di XYH contenente H tale che $K/H = \overline{K}$. Poichè $\overline{XK} = \overline{XY}$ e $\overline{X} \cap \overline{K} = \{1\}$, per il Teorema di Corrispondenza segue che

$$XYH = XKH = XK \text{ e } X \cap K \leq H.$$

Quindi $K > H$, perché $Y \not\leq XH$ e

$$X \cap K = (X \cap X) \cap K = X \cap (X \cap K) \leq X \cap H = \{1\},$$

in contraddizione con la scelta massimale di H.

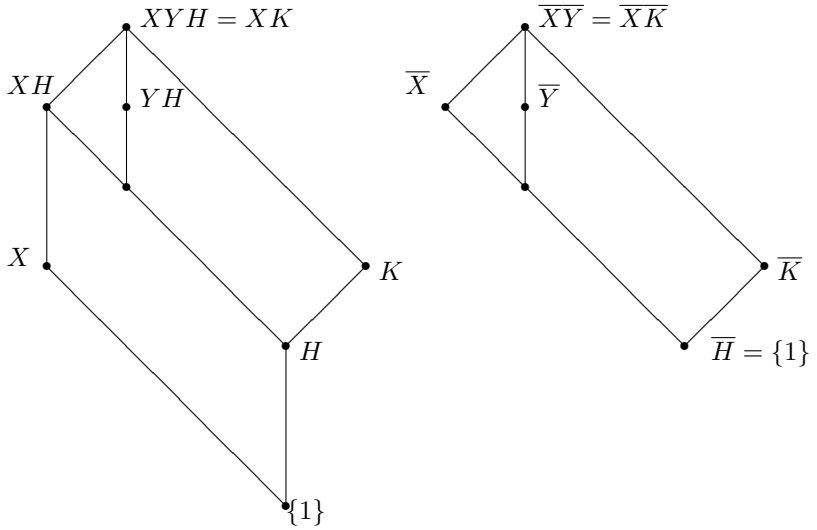


Fig. 1

■

Teorema 3.2.3 (Decomposizione dei p-gruppi abeliani finiti) *Sia p un numero primo e P un p-gruppo abeliano finito. Allora P è isomorfo ad un prodotto diretto di p-gruppi ciclici.*

Dimostrazione. Per induzione sull'ordine di P. Se $P = \{1\}$ non c'e' nulla da dimostrare. Supponiamo che $|P| > 1$ e sia X un sottogruppo di ordine massimo di P. Per il Lemma 3.2.2 esiste un sottogruppo H di P tale che $P = X \times H$. H è un p-gruppo di ordine $|P|/|X|$ e quindi, per ipotesi induttiva, H è isomorfo ad un prodotto diretto di p-gruppi ciclici. Ma allora, come nella dimostrazione del Teorema 3.1.4, anche P è isomorfo ad un prodotto di gruppi ciclici. ■

3.3 Il reticolo dei sottogruppi di $C_{p^h} \times C_p$

La situazione descritta nel Lemma 3.2.1 può essere chiarita dallo studio del reticolo dei sottogruppi di $C_{p^h} \times C_p$ dove p è un numero primo. Per semplificare le notazioni, poniamo $X := C_{p^h}$, $K := C_p$ e $P := C_{p^h} \times C_p$. Sia x un generatore di X e k un generatore di K.

Per prima cosa studiamo il caso in cui $h = 1$.

Lemma 3.3.1 *Se $P \cong C_p \times C_p$, allora P possiede esattamente $p+1$ sottogruppi diversi da P e da $\{1\}$. Se T_i e T_j sono due sottogruppi distinti di P e diversi da P e da $\{1\}$, allora $T_iT_j = P$ e $T_i \cap T_j = \{1\}$*

DIMOSTRAZIONE. P ha ordine p^2, dunque ogni sottogruppo proprio non identico di P ha ordine p e quindi è ciclico. Inoltre due qualsiasi sottogruppi propri distinti hanno intersezione identica ed il sottogruppo da essi generato è tutto P. Per contare quanti sono i sottoguppi ciclici, osserviamo che P contiene p^2-1 elementi diversi dall'identità. Poiché ogni elemento di $P\setminus\{1\}$ è contenuto in un sottogruppo ciclico e ciascun sottogruppo ciclico non identico contiene esattamente $p-1$ elementi, devono esserci esattamente $((p^2-1)/(p-1) =)p+1$ sottogruppi ciclici diversi dal sottogruppo identico. ∎

In particolare il diagramma di Hasse del reticolo dei sottogruppi di P è come nella figura 2:

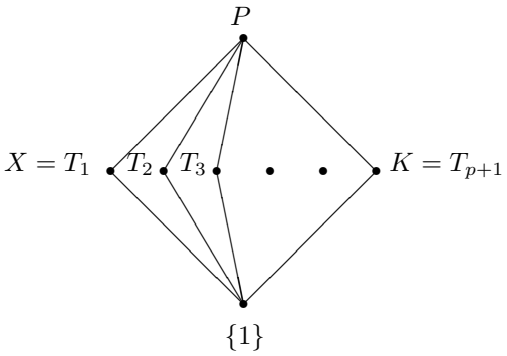


Fig. 2

Supponiamo ora che $h > 1$ e proviamo, per induzione su h che il diagramma di Hasse del reticolo dei sottogruppi di P è

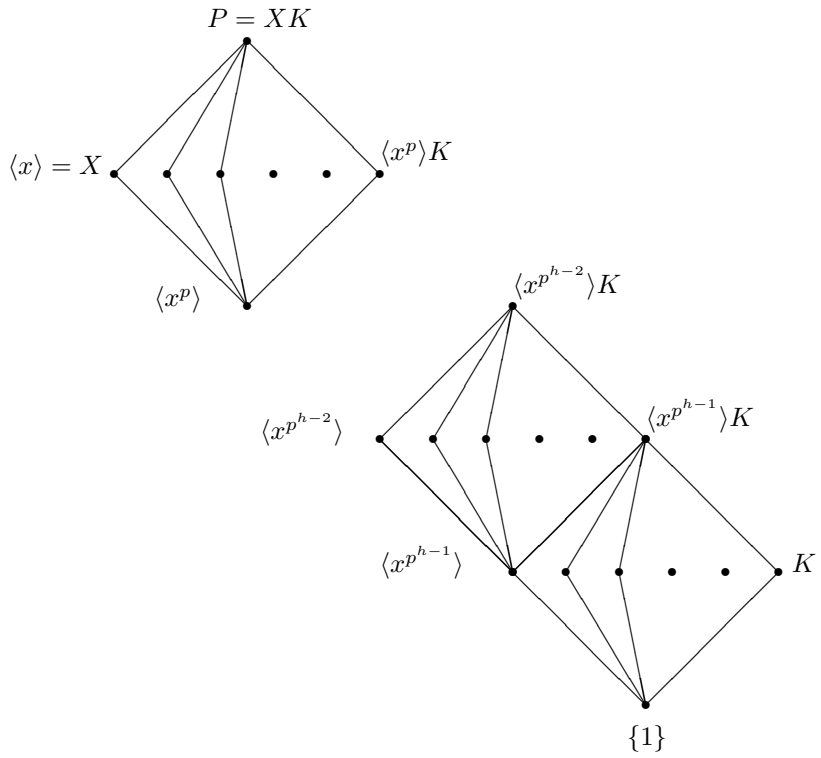


Fig. 3

Sia $X_0 = \langle x^{p^{h-1}} \rangle$ ed osserviamo che il gruppo quoziente P/X_0 è generato da X/X_0 e da KX_0/X_0 che sono ciclici e di ordine rispettivamente p^{h-1} e p. Per ipotesi induttiva e per il Teorema di Corrispondenza, il diagramma di Hasse del reticolo dei sottogruppi di P che contengono X_0 è come nella figura 3. Per il Lemma 3.3.1 basta allora dimostrare che ogni sottogruppo di P che non contiene X_0 è contenuto in X_0K. Sia T un sottogruppo di P che non contiene X_0 e sia $t \in T$. Proviamo che $t \in X_0K$, da cui seguirà la tesi. Poiché $T \leq P = \langle x, k \rangle$, esistono degli interi m e n tali che $t = x^m k^n$. Osserviamo che, poiché x e k commutano e $k^p = 1$,

$$t^p = x^{pm} k^{pn} = x^{pm}$$

D'altra parte $\langle x^{pm} \rangle$ è un sottogruppo di X che non contiene X_0 e quindi (poiché X_0 è contenuto in tutti i sottogruppi non identici di X) $\langle x^{pm} \rangle = \{1\}$, cioè $x^{pm} = 1$. Ne segue che p^{h-1} divide m, dunque $x^m \in X_0$ e quindi $t \in X_0K$.

3.4 La struttura dei gruppi abeliani finiti

Teorema 3.4.1 (Struttura dei gruppi abeliani finiti) *Ogni gruppo abeliano finito è isomorfo ad un prodotto diretto di gruppi ciclici.*

DIMOSTRAZIONE. Sia A un gruppo abeliano finito. Allora A è anche di esponente finito, quindi, per il Teorema di Decomposizione Primaria, A è isomorfo al prodotto diretto delle sue componenti primarie:

$$A = A_{p_1} \times A_{p_2} \times \ldots \times A_{p_t}.$$

D'altra parte, ciascuna componente primaria A_{p_i} è un p_i-gruppo abeliano finito e quindi, per il Teorema di Decomposizione dei p-gruppi finiti, è isomorfa ad un prodotto diretto di gruppi ciclici:

$$A_{p_i} = C_{i,1} \times C_{i,2} \times \ldots \times C_{i,s_i},$$

da cui la tesi. ∎

Sia ora, per ogni $i \in \{1, \ldots, t\}$ ed ogni $j \in \{1, \ldots, s_i\}$, $C_{i,j}$ definito come della dimostrazione del teorema precedente. Ordiniamo gli indici in modo che,

$$\text{se } j_1 < j_2, \text{ allora } |C_{i,j_1}| \geq |C_{i,j_2}| \text{ e quindi } |C_{i,j_2}| \text{ divide } |C_{i,j_1}|. \tag{3.3}$$

Inoltre, se s è il massimo degli s_i e $s_l < s$, poniamo, per comodità, $C_{l,m} = \{1\}$ per ogni $m \in \{s_l + 1, \ldots s\}$. Consideriamo la seguente tabella:

$$\begin{array}{ccccccccc}
A_{p_1} & = & C_{1,1} & \times & C_{1,2} & \times & \ldots & \times & C_{1,k} \\
A_{p_2} & = & C_{2,1} & \times & C_{2,2} & \times & \ldots & \times & C_{2,k} \\
. & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . \\
A_{p_t} & = & C_{t,1} & \times & C_{t,2} & \times & \ldots & \times & C_{t,k}
\end{array}$$

D'altra parte avremmo potuto fare prima il prodotto diretto lungo le colonne: siano $C_1, C_2, \ldots, C_k$ rispettivamente i prodotti delle colonne di indice $1, \ldots k$, cioè

$$\begin{array}{ccccccccc}
C_1 & = & C_{1,1} & \times & C_{2,1} & \times & \ldots & \times & C_{t,1} \\
C_2 & = & C_{1,2} & \times & C_{2,2} & \times & \ldots & \times & C_{t,2} \\
. & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . \\
C_k & = & C_{1,k} & \times & C_{2,k} & \times & \ldots & \times & C_{t,k}
\end{array}$$

Poiché il prodotto diretto è commutativo ed associativo, risulta anche

$$A = C_1 \times C_2 \times \ldots \times C_k.$$

Ora, se $i \neq j$, $C_{i,h}$ e $C_{j,k}$ sono gruppi ciclici di ordine coprimo perché sono contenuti rispettivamente nelle due distinte componenti primarie A_{p_i} e A_{p_j}, quindi, per il Lemma 3.0.20 ciascun C_h è ciclico. Inoltre, per la (3.3), per ogni $i \in \{2, \ldots, k\}$, $|C_i|$ divide $|C_{1-1}$. Abbiamo così dimostrato il seguente

Teorema 3.4.2 (Teorema dei Divisori Elementari) *Sia A un gruppo abeliano finito, allora esistono dei sottogruppi ciclici $C_1, C_2, \ldots, C_n$ di A tali che*

1. $A = C_1 \times C_2 \times \ldots \times C_k$ *e*
2. *se $j_1 < j_2$, allora $|C_{j_2}|$ divide $|C_{j_1}|$.*

Gli interi $|C_1|, |C_2| \ldots |C_k|$ si dicono **divisori elementari** di A, gli interi $|C_{i,j}|$ diversi da 1 si dicono **fattori invarianti** di A.

Chiaramente $|A| = |C_1| \cdot |C_2| \cdot \ldots \cdot |C_k|$ e $exp(A) = |C_1|$, in particolare A è ciclico se e solo se $|A| = \exp(A)$. Inoltre due gruppi abeliani finiti A e B sono tra loro isomorfi se e solo se hanno gli stessi divisori elementari (o, equivalentemente, gli stessi fattori invarianti con la stessa molteplicità).

3.5 Esercizi

Esercizio 3.5.1 *Un gruppo G si dice di torsione se ogni elemento di G ha ordine finito. Chiaramente un gruppo di esponente finito è di torsione, ma il viceversa non è vero. Sia infatti*

$$\mathbf{T} := \{\mathbf{z} \in \mathbf{C} | \mathbf{z^k} = \mathbf{1} \text{ per qualche } \mathbf{k} \in \mathbf{N} \setminus \{\mathbf{0}\}\}$$

*(**T** è l'insieme di tutte le radici complesse di 1)*

1. *Provare che **T** è un sottogruppo del gruppo moltiplicativo dei numeri complessi diversi da 0.*
2. *Provare che se $z \in \mathbf{T}$ esiste un intero positivo k tale che $z^k = 1$, dunque z ha periodo finito per ogni $z \in T$ e quindi **T** è di torsione).*
3. *Provare che, fissato comunque un intero positivo n, esistono elementi z di **T** tali che $z^n \neq 1$ (dunque **T** non è di esponente finito).*

Esercizio 3.5.2 *Con le notazioni del Lemma 3.1.1, provare che*

1. *Se t non è coprimo con n, $exp(A^t) = n/d$ dove d è il massimo comun divisore tra t e n.*
2. *Se t è coprimo con n, A^t=A.*

Esercizio 3.5.3 *Con le notazioni del Lemma 3.3.1, se $P \cong C_p \times C_p$ determinare $p+1$ elementi distinti $t_1, t_2, \ldots, t_{p+1}$ di P tali che $\langle t_1 \rangle, \langle t_2 \rangle, \ldots, \langle t_{p+1} \rangle$ siano $p+1$ sottogruppi distinti di ordine p*

Esercizio 3.5.4 *Si consideri la figura 3.*

1. *Provare che i sottogruppi*

$$P,\ \langle x \rangle K,\ \langle x^p \rangle K, \ldots, \langle x^{p^{h-2}} \rangle K,\ \langle x^{p^{h-1}} \rangle K$$

non sono ciclici, mentre tutti gli altri lo sono.

2. *determinare i generatori dei sottogruppi ciclici*

3. *determinarei sottogruppi ciclici di ordine massimo ed i sottogruppi ciclici massimali.*

4. *determinare i sottogruppi T che ammettono un complemento, cioè tali che esista un sottogruppo H di P con $TH = P$ e $T \cap H = \{1\}$*

Esercizio 3.5.5 *Sia G un p-gruppo ciclico.*

1. *Mostrare che l'insieme dei suoi sottogruppi è totalmente ordinato per inclusione.*

2. *Dedurre che gli unici sottogruppi di G che ammettono un complemento sono G e $\{1\}$.*

Esercizio 3.5.6 *Provare le osservazioni alla fine della sezione (4).*

Esercizio 3.5.7 *Si dimostri che il gruppo $\mathbf{Z}_2 \times \mathbf{Z}_2$ è abeliano ma non è ciclico.*

Esercizio 3.5.8 *Si dia un esempio di p-gruppo infinito.*

Esercizio 3.5.9 *Si provi che se G è un p-gruppo abeliano elementare, allora l'intersezione dei sottogruppi massimali di G è il sottogruppo identico.*

Esercizio 3.5.10 *Sia G un gruppo abeliano finito. Si provi che ogni sottogruppo di G ha un unico complemento se e solo se $|G|$ è prodotto di numeri primi distinti.*

Esercizio 3.5.11 *Sia A un gruppo abeliano finito. Si provi che, per ogni numero intero n coprimo con $|A|$, l'applicazione $\phi_n \colon A \to A$ definita, per ogni $a \in A$ da $a \mapsto a^n$ è un automorfismo di A tale che, per ogni sottogruppo B di A, $B^\phi = B$.*

Esercizio 3.5.12 *Si dia un esempio di gruppo finito non ciclico il cui ordine coincide con l'esponente.*

Esercizio 3.5.13 *Sia F un campo e sia T un sottogruppo finito del gruppo moltiplicativo di F. Si provi che T è ciclico. Suggerimento, sia n l'esponente di T, allora ogni elemento di T è soluzione del polinomio $x^n - 1$*

Esercizio 3.5.14 *Si dia un esempio di gruppo abeliano, ovviamente infinito, in cui nessuna componente primaria sia identica.*

Capitolo 4

Gruppi liberi e presentazioni

In questo capitolo introduciamo i gruppi liberamente generati da un insieme. Se G è liberamente generato da un suo sottoinsieme R, allora R si comporta in modo analogo a quello di una base di uno spazio vettoriale nel senso che ogni applicazione da R su un gruppo H può essere estesa in modo unico ad un omomorfismo di gruppi da G ad H. Proveremo che, per ogni insieme R, esiste un gruppo liberamente generato da un insieme di cardinalità pari a quella di R. Per questo definiremo il concetto analogo di monoide liberamente generato da un insieme ed otterremo il gruppo libero come quoziente di un monoide.

4.1 Gruppi liberi

4.1.1 Semigruppi e monoidi

Ricordiamo che un **semigruppo** è una coppia

$$(S, \cdot)$$

dove S è un insieme e $\cdot$ è un'operazione associativa su S. Un **monoide** è una tripla

$$(M, \cdot, 1)$$

dove $(M, \cdot)$ è un semigruppo e 1 è un elemento di M tale che, per ogni $m \in M$, $1 \cdot m = m \cdot 1 = m$. Dato un semigruppo $S, \cdot)$ che non sia un monoide, esiste un modo ovvio per ottenere da $S, \cdot)$ un monoide (cfr. [21] es. 5 Cap. 1.1): sia 1 un oggetto non contenuto in S (per esempio potremmo scegliere $1 = S$), sia

$$M := S \cup \{1\}$$

ed estendiamo l'operazione $\cdot$ di S ad un'operazione (che continuiamo a chiamare $\cdot$) su tutto M ponendo, per ogni $w \in S$,

$$1 \cdot w := w,\ w \cdot 1 := w \text{ e } 1 \cdot 1 := 1.$$

Si verifica immediatamente che, con tale operazione, $(M, \cdot)$ è un monoide. Come per i gruppi possiamo definire i morfismi di semigruppi (monoidi) come le applicazioni tra semigruppi che conservano le operazioni (e, nel caso dei monoidi, anche l'identità), i sottosemigruppi (sottomonoidi) come i sottoinsiemi non vuoti chiusi per l'operazione (e, nel caso dei monoidi, contenenti anche l'elemento 1), possiamo definire il sottosemigruppo (sottomonoide) generato da un sottoinsieme, le equivalenze compatibili con le operazioni e, come nel caso dei gruppi, si dimostra che se $(X, \cdot)$ è un semigruppo ($(X, \cdot, 1)$ è un monoide) e $\sim$ è una relazione d'equivalenza compatibile con l'operazione, allora l'insieme quoziente $X/\sim$ eredita in modo naturale un'operazione, ponendo, per ogni $[x]_\sim$, $[y]_\sim \in X/\sim$,

$$[x]_\sim \cdot [y]_\sim := [x \cdot y]_\sim$$

e, con tale operazione $(X/\sim, \cdot)$ è un semigruppo ($(X/\sim, \cdot, [1]_\sim)$ è un monoide).

4.1.2 Monoidi e gruppi finitamente generati

Sia G un gruppo (risp. monoide) e R un sottoinsieme di G. Diremo che G è un gruppo (monoide) **liberamente generato da** R se soddisfa la seguente

PROPRIETÀ UNIVERSALE DEI GRUPPI (MONOIDI) LIBERAMENTE GENERATI: *Per ogni gruppo (monoide) H ed ogni applicazione*

$$\phi\colon R \to H,$$

esiste un unico omomorfismo di gruppi (monoidi)

$$\overline{\phi}\colon G \to H$$

tale che

$$\overline{\phi}|_R = \phi.$$

Sia G un gruppo liberamente generato da R e H un gruppo generato da un sottoinsieme T. Se $|T| \leq |R|$ allora esiste una funzione $\phi\colon R \to H$ tale che $T = R^\phi$. Sia

$$\overline{\phi}\colon G \to H$$

l'omomorfismo di gruppi tale che $\overline{\phi}|_R = \phi$. Poiché

$$H = \langle T \rangle \leq \langle R^\phi \rangle \leq G^{\overline{\phi}},$$

segue che $\overline{\phi}$ è suriettivo, in particolare:

Teorema 4.1.1 *Se G è un gruppo liberamente generato da un insieme di cardinalità κ, allora ogni gruppo generato da κ elementi è immagine omomorfa di G.*

Un gruppo (monoide) G si dice **libero** se esiste un suo sottoinsieme R tale che G sia finitamente generato da R.

4.1.3 Esistenza di monoidi liberamente generati

Sia R un insieme. Una **parola** di **lunghezza** h nell'**alfabeto** R è una successione

$$(r_1, r_2, \ldots, r_h)$$

di elementi di R. Sia S l'insieme delle parole nell'alfabeto R. Se

$$(r_1, r_2, \ldots, r_h) \text{ e } (s_1, s_2, \ldots, s_k)$$

sono due parole in S, di lunghezze rispettivamente h e k, il loro **prodotto** è la successione

$$(r_1, r_2, \ldots, r_h, s_1, s_2, \ldots, s_k)$$

di lunghezza $h + k$. Si vede immediatamente che l'operazione $\cdot$ è associativa e quindi $(S, \cdot)$ è un semigruppo. Sia $(M, \cdot)$ è il monoide che si ottiene da S aggiungendo l'identità costruito come nel paragrafo precedente.

Teorema 4.1.2 *Siano R ed M come sopra, allora*

1. *$M = \langle R \rangle$;*
2. *M è un monoide liberamente generato da R.*

DIMOSTRAZIONE. La prima affermazione discende direttamente dalla costruzione di M. Sia $\phi\colon R \to H$ una funzione. Poniamo $1^{\overline{\phi}} := 1_H$ e, se $(r_1, r_2, \ldots, r_h)$ è una parola in M, poniamo

$$(r_1, r_2, \ldots, r_h)^{\overline{\phi}} := (r_1^{\phi}, r_2^{\phi}, \ldots, r_h^{\phi}).$$

Allora $\overline{\phi}$ è un omomorfismo di monoidi che estende ϕ ed è l'unico per la (versione per monoidi della) Proposizione 1.1.15. ∎

4.1.4 Esistenza e unicità di gruppi liberamente generati

Siano R ed M come nel paragrafo precedente e supponiamo che R sia l'unione disgiunta di due insiemi T e $\overline{T}$ equipotenti. Sia

$$inv\colon R \to R$$

una permutazione di ordine 2 tale che $T^{inv} = \overline{T}$. Definiamo ora una relazione d'equivalenza $\sim$ su M nel modo seguente. Se u e w sono due parole in M diremo che u e w sono adiacenti se esistono degli elementi a, b in M ed $x \in R$ tali che

$$u = ab \text{ e } w = axx^{inv}b$$

o viceversa. La relazione di adiacenza è una relazione simmetrica. Sia $\sim$ la sua chiusura transitiva: date due parole u e w, $u \sim w$ se e solo se esiste una successione

$$u_1, \ldots u_{n+1}$$

di parole in M tali che $u_1 = u$, $u_n = w$ e u_i è adiacente a u_{n+1} per ogni $i \in \{1, \dots n\}$. Il minimo intero n per cui esiste una successione con tali proprietà si dice **distanza** tra le parole u e w. Per induzione sulla distanza si vede facilmente che la relazione $\sim$ è una relazione d'equivalenza compatibile con l'operazione di M. Sia F il monoide quoziente di M modulo la relazione $\sim$. F è un gruppo perchè se

$$(r_1, r_2, \dots, r_h)$$

è una parola in M con $r_i \in R$, allora

$$[(r_h^{inv}, \dots, r_2^{inv}, r_1^{inv})]_\sim$$

è l'inverso in F di

$$[(r_1, r_2, \dots, r_h)]_\sim$$

Lemma 4.1.3 *Siano R T, M e F come sopra, allora*

1. *$F = \langle T \rangle$;*
2. *F è un gruppo liberamente generato dall'insieme T.*

Dimostrazione. La prima parte segue dal fatto che F è un quoziente di M e che $M = \langle T, T^{inv} \rangle$. Sia ora H un gruppo e

$$\phi \colon T \to H$$

un'applicazione. Estendiamo ϕ ad un'applicazione

$$\delta \colon R \to H,$$

ponendo, per ogni $t^{inv} \in T^{inv}$,

$$(t^{inv})^\delta := (t^\phi)^{-1}.$$

Per il Teorema 4.1.2 esiste un omomorfismo di monoidi

$$\overline{\delta} \colon M \to H$$

che estende δ. Proviamo ora che se u e v sono elementi di M, allora

$$u \sim v \text{ implica che } u^{\overline{\delta}} = v^{\overline{\delta}}. \tag{4.1}$$

Possiamo restringerci al caso in cui u e v sono adiacenti. Siano a, b in M ed $x \in R$ tali che

$$u = ab \text{ e } v = axx^{inv}b,$$

allora

$$u^{\overline{\delta}} = (ab)^{\overline{\delta}} = a^{\overline{\delta}} b^{\overline{\delta}} = a^{\overline{\delta}} x^{\overline{\delta}} (x^{inv})^{\overline{\delta}} b^{\overline{\delta}} = (axx^{inv}b)^{\overline{\delta}} = v^{\overline{\delta}}.$$

Da questo segue che $\overline{\delta}$ induce un omomorfismo $\overline{\phi}$ dal monoide quoziente F $(= M/\sim)$ a H definito da

$$[w]_\sim^{\overline{\phi}} := w^{\overline{\delta}}$$

che, per costruzione, coincide con ϕ su T. L'unicità di $\overline{\phi}$ segue dalla Proposizione 1.1.15. ∎

Teorema 4.1.4 ESISTENZA ED UNICITÀ DEI GRUPPI LIBERAMENTE GENERATI *Per ogni cardinale κ, esiste, a meno di isomorfismi, un unico gruppo liberamente generato da un insieme di cardinalità κ*

DIMOSTRAZIONE. Siano T e T^{inv} due insiemi di cardinalità κ tali che $T \cup T^{inv} = \emptyset$, $R := T \cap T^{inv}$ e inv una permutazione di ordine 2 di R che scambia T con T^{inv} (lasciamo al lettore provare l'esistenza di T^{inv} e della permutazione inv). L'esistenza di un gruppo F liberamente generato da T segue dal Lemma 4.1.3. Proviamo l'unicità di F. Sia S un altro insieme di cardinalità κ e sia H un gruppo liberamente generato da S. Dal fatto che $|T| = |S|$, segue che esiste una biiezione

$$\phi: T \to S.$$

Poiché F e H sono liberamente generati rispettivamente da T ed S, ϕ e ϕ^{-1} si estendono rispettivamente a due omomorfismi

$$\delta: F \to H$$

e

$$\gamma: H \to F.$$

Ora $\delta\gamma$ è un endomorfismo di F che induce l'applicazione identica su T. D'altra parte, poichè F è liberamente generato su T, l'applicazione identica su F è l'unica estensione dell'applicazione identica su T e quindi $\delta\gamma$ è l'applicazione identica su F. Ne segue che δ è un isomorfismo e quindi la tesi. ∎

Con le notazioni precedenti, se x è un elemento non identico di F, definiamo la **lunghezza** di x la minima lunghezza delle parole $(r_1, r_2, \ldots, r_h)$ in M tali che $[(r_1, r_2, \ldots, r_h)]_\sim = x$; diremo inoltre che 1_F ha lunghezza 0.

4.2 Presentazioni

Sia F un gruppo liberamente generato da un insieme T, sia W un sottoinsieme di F e sia $N := \langle W^F \rangle$ il sottogruppo di F generato dall'insieme

$$W^F := \{w^f | w \in W \text{ e } f \in F\}.$$

Chiaramente $N \trianglelefteq F$. Come in [1] indichiamo con $Grp(T: W)$ il gruppo quoziente F/N. Il gruppo $Grp(T: W)$ dice **gruppo generato da T con le relazioni** $\{w = 1 | w \in W\}$.

Se G è un gruppo, una **presentazione** di G è una coppia (T, W), tale che T è un insieme di generatori di G, W è un sottoinsieme di G e, se F è il gruppo libero generato da T e $N = \langle W^F \rangle$, allora N coincide con il nucleo dell'omomorfismo $\delta: F \to G$ che estende l'applicazione identica su T (e quindi δ induce un isomorfismo tra F/N e G). Anche per le presentazioni esiste una proprietà universale analoga a quella dei gruppi liberamente generati:

Teorema 4.2.1 (Proprietà universale delle presentazioni) *Sia*

$$G := Grp(T: W)$$

e sia ϕ una funzione da T in un gruppo H. Supponiamo che

1. $H = \langle W^\phi \rangle$ *e*
2. *per ogni*
$$r_1^{\epsilon_1} r_2^{\epsilon_2} \dots r_k^{\epsilon_k} \in W$$
con $r_i \in T$ e $\epsilon_i \in \{1, -1\}$ per ogni $i \in \{1, \dots, k\}$, risulta
$$(r_1^\phi)^{\epsilon_1} (r_2^\phi)^{\epsilon_2} \dots (r_k^\phi)^{\epsilon_k} = 1,$$

allora esiste un unico omomorfismo di gruppi

$$\overline{\phi}: G \to H$$

che estende ϕ, cioè tale che, per ogni $r \in T$, $r^\phi = r^{\overline{\phi}}$. In particolare H è isomorfo ad un quoziente di G.

Dimostrazione. Sia F il gruppo liberamente generato da T. Per la Proprietà universale dei gruppi liberamente generati esiste un'unico omomorfismo $\psi: F \to H$ che estende ϕ. Per la condizione *2.* $W \leq ker(\psi)$. Ne segue che, posto $N := \langle W^F \rangle$, anche $N \leq ker(\psi)$ e quindi ψ induce un omomorfismo

$$\overline{\phi}: F/N \to H,$$

(ben) definito da

$$(Nh)^{\overline{\phi}} := N(h^\psi)$$

(per ogni $Nh \in F/N$, con $h \in F$), da cui la tesi poichè $G = F/N$ e, per ogni $r \in T$, $r^\phi = r^\psi$. ∎

Ad esempio, se T è un insieme, ogni gruppo abeliano generato da $|T|$ elementi è immagine omomorfa del gruppo

$$Grp(T: \{x^{-1}y^{-1}xy | x, y \in T\}),$$

perché ogni gruppo abeliano generato da $|T|$ elementi ha un insieme di generatori $\overline{T}$ tali che $x^{-1}y^{-1}xy = 1$ per ogni $x, y \in \overline{T}$.

Dato un gruppo G con un'operazione $\cdot$, esiste un modo ovvio per costruire una presentazione di G: poiché G come gruppo è certamente generato dall'insieme G stesso, segue che l'applicazione identica su G induce un omomorfismo suriettivo δ tra il gruppo F liberamente generato dall'insieme G ed il gruppo G e quindi $Grp(G: ker(\delta))$ è una presentazione di G. Per fissare le notazioni, F è un quoziente del monoide liberamente generato dall'insieme $R := G \cup G^{inv}$ dove G^{inv} è un insieme disgiunto da G e inv è una permutazione di R di ordine 2

che manda G in G^{inv}. Indichiamo con $*$ l'operazione di F. Si presti attenzione al fatto che la restrizione di $*$ a G non coincide affatto con l'operazione $\cdot$ di G: infatti, mentre G è un gruppo rispetto all'operazione $\cdot$, non lo è rispetto all'operazione $*$: infatti $(G, \cdot, 1_G)$ può essere un gruppo finito, mentre $(F, *, 1_F)$ è generato da G ma non è mai finito; in particolare G non è chiuso rispetto all'operazione $*$. Si noti inoltre che

$$1_G \neq 1_F$$

e, se $g \in G$,

$$g * g^{inv} = 1_F$$

ma, se h è l'inverso di g rispetto all'operazione $\cdot$,

$$g^{inv} \neq h.$$

Nel seguito, se $g \in G$, riserveremo il simbolo g^{-1} solo per l'inverso di g nel gruppo $(G, \cdot, 1_G)$. Sia ora

$$W := \{a * b * (a \cdot b)^{inv} | \, a, b \in G\}.$$

e

$$N := \langle W^F \rangle.$$

Chiaramente $N \leq ker(\delta)$. Proviamo che $ker(\delta) = N$. Supponiamo infatti per assurdo che $N < ker(\delta)$ e sia x un elemento di lunghezza minima in $ker\delta \setminus N$. Sia r la lunghezza di x. Poichè $1_F \in N$, $r \geq 1$. Siano $x_1, x_2, \ldots, x_r \in G$ tali che

$$x = x_1 * x_2 * \ldots * x_r.$$

Poiché N è un sottogruppo normale di F, possiamo supporre che $x_1 \in G$. Se $r = 1$, allora, poichè la restrizione di δ a G è l'applicazione identica e $x \in ker(\delta)$,

$$1_G = x_1^{\delta} = x_1$$

e

$$1_G = 1_G * 1_G * 1_G^{inv} = 1_G * 1_G * (1_G \cdot 1_G)^{inv} \in W \subseteq N.$$

Supponiamo ora che $r \geq 2$. Allora esiste un elemento u di F di lunghezza $r - 2$ tale che

$$x = x_1 * x_2 * u.$$

Se $x_2 \in G^{inv}$, poniamo

$$z := (x_1 \cdot (x_2^{inv})^{-1})$$

e, se $x_2 \in G$, poniamo

$$z := (x_1 \cdot x_2).$$

Osserviamo che in entrambi i casi

$$z * x_2^{inv} * x_1^{inv} \in N,$$

infatti, nel primo caso

$$z * x_2^{inv} * x_1^{inv} = (x_1 \cdot (x_2^{inv})^{-1}) * x_2^{inv} * x_1^{inv}$$

che appartiene a W per definizione e, nel secondo caso, è l'inverso dell'elemento $x_1 * x_2 * (x_1 \cdot x_2)^{inv}$ che appartiene ancora a W. Dunque anche

$$z * x_2^{inv} * x_1^{inv} * x \in ker(\delta) \setminus N.$$

Ma

$$z * x_2^{inv} * x_1^{inv} * x = z * u$$

che ha lunghezza $r - 1$, una contraddizione. Riassumendo:

Proposizione 4.2.2 *Con le notazioni precedenti, se G è un gruppo, allora*

$$G \cong Grp(G : \{a * b * (a \cdot b)^{inv} | \, a, b \in G\}). \tag{4.2}$$

Osserviamo che le relazioni

$$a * b * (a \cdot b)^{inv} | \, a, b \in G$$

equivalgono alla tabella moltiplicativa del gruppo G, infatti l'elemento $a \cdot b$ corrisponde nella tabella moltiplicativa di G all'entrata di riga e colonna corrispondenti rispettivamente agli elementi a e b di G.

Un gruppo G si dice **finitamente presentato** se G ha una presentazione (T, W) tale che $|T| + |W|$ è finito.

Corollario 4.2.3 *Ogni gruppo finito è finitamente presentato*

4.3 Esercizi

Esercizio 4.3.1 *Provare che il gruppo additivo degli interi è libero sull'insieme* $\{1\}$.

Esercizio 4.3.2 *Si enunci e si dimostri il Teorema di Esistenza ed Unicità per monoidi finitamente generati*

Capitolo 5

Gruppi simmetrici

5.1 Richiami

In questo capitolo richiamiamo alcuni risultati elementari sulla generazione e sulla fusione degli elementi dei gruppi simmetrici e proveremo che i gruppi alterni A_n sono semplici e non abeliani se $n \geq 5$

Sia X un insieme, ricordiamo che una permutazione di X è una biiezione di X in se stesso e l'insieme S_X di tutte le permutazioni di X è un gruppo rispetto alla composizione di applicazioni. Se X è finito possiamo scegliere una permutazione di X in esattamente $|X|!$ modi distinti. Dunque

$$|S_X| = |X|!.$$

Se n è un numero naturale, indichiamo con I_n l'insieme $\{t \in \mathbf{N} | 1 \leq t \leq n\}$ e con S_n il gruppo S_{I_n} delle permutazioni di I_n.

Proposizione 5.1.1 *Se X è un insieme finito con n elementi, allora S_X è isomorfo a S_n.*

Se σ è una permutazione in S_X indichiamo con

$$mov(\sigma)$$

l'insieme

$$\{x \in X | x^\sigma \neq x\}$$

e, se Y è un sottoinsieme di X, indichiamo con

$$C_Y(\sigma)$$

l'insieme

$$\{y \in Y | y^\sigma = y\}.$$

Si osservi che, in particolare X è l'unione disgiunta di $mov(\sigma)$ e di $C_X(\sigma)$.

Due permutazioni σ e τ si dicono **disgiunte** se $mov(\sigma) \cap mov(\tau) = \emptyset$

Proposizione 5.1.2 *Siano σ e τ due permutazioni disgiunte in S_X. Allora $[\sigma, \tau] = 1_{S_X}$*

Sia k un intero maggiore o uguale a 2. Una permutazione γ in S_X si dice **ciclo di lunghezza** k se esistono degli elementi distinti $x_1, \ldots, x_k$ in X tali che

$mov(\gamma) = \{x_1, \ldots, x_k\}$,
$x_k^\gamma = x_1$ e, per ogni $i \in \{1, \ldots, k-1\}$, $x_i^\gamma = x_{i+1}$

In tal caso, per indicare γ useremo il simbolo

$$(x_1, x_2, \ldots, x_k).$$

I cicli di lunghezza 2 si dicono **trasposizioni** o **scambi**.

Proposizione 5.1.3 *Ogni permutazione diversa dall'identità si fattorizza come prodotto di cicli disgiunti. Inoltre questa fattorizzazione è unica a meno dell'ordine dei fattori. In particolare S_n è generato dai suoi cicli.*

Sia σ una permutazione in S_n, siano

$$\gamma_1, \ldots, \gamma_k$$

cicli disgiunti in S_n tali che

$$\sigma = \gamma_1 \ldots \gamma_k$$

e sia l_i la lunghezza del ciclo γ_i. Per la Proposizione 5.1.2 possiamo supporre che

$$l_1 \leq l_2 \leq \ldots \leq l_k.$$

In tal caso diremo che la k-upla $(l_1, \ldots, l_k)$ è il **tipo** della permutazione σ.

Proposizione 5.1.4 *Ogni permutazione si fattorizza come prodotto di trasposizioni. Tale fattorizzazione non è unica, ma se una permutazione si scrive come prodotto di k trasposizioni ed anche come prodotto di n trasposizioni, allora $k \equiv n \ (mod\ 2)$.*

Una permutazione σ di dice di **classe pari** (**dispari**) se σ è prodotto di un numero pari (dispari) di trasposizioni. Osserviamo che se $(x_1, x_2, \ldots, x_k)$ è un ciclo di S_X, allora

$$(x_1, x_2, \ldots, x_k) = (x_1, x_2)(x_1, x_3) \ldots (x_1, x_{k-1})(x_1, x_k).$$

In particolare

Proposizione 5.1.5 *Cicli di lunghezza pari hanno classe dispari e, viceversa, cicli di lunghezza dispari hanno classe pari*

Dalla Proposizione 5.1.4 segue immediatamente che l'insieme delle permutazioni di classe pari S_X è un sottogruppo normale di indice 2 in S_X. Tale sottogruppo si dice **gruppo alterno su** X e si indica con A_X o Alt_X. Come sopra, se $X = I_n$ scriveremo A_n o Alt_n al posto di A_X. Osserviamo che A_X è generato dalle permutazioni $(a,b)(c,d)$ al variare di a,b,c,d in X con $a \neq b$ e $c \neq d$. Chiaramente,

Lemma 5.1.6 *Siano a,b,c,d in X con $a \neq b$ e $c \neq d$. Allora*

1. *se $\{a,b\} = \{c,d\}$, allora $(a,b)(c,d) = 1$,*
2. *se $\{a,b\} \cap \{c,d\} = \emptyset$, allora $(a,b)(c,d)$ è di tipo $(2,2)$,*
3. *infine, se $\{a,b\} \cap \{c,d\}$ contiene un solo elemento (diciamo $b = d$), allora $(a,b)(c,d) = (a,c,b)$ è un ciclo di lunghezza 3.*

Proposizione 5.1.7 *Sia X un insieme.*

1. *A_X è generato dai cicli di lunghezza 3 di S_X.*
2. *Se $|X| \geq 5$, A_X è generato dalle permutazioni di tipo $(2,2)$ di S_X.*

DIMOSTRAZIONE. Se $|X| \in \{1,2\}$, allora $A_X = \{1\}$ e non c'è nulla da dimostrare. Siano a,b,c tre elementi distinti di X. Se $X = \{a,b,c\}$ allora $A_X = \langle (a,b,c) \rangle$ ed anche qua abbiamo finito. Sia $|X| \geq 4$ e $d \in X \setminus \{a,b,c\}$, allora

$$(a,b)(c,d) = (a,d,c)(a,d,b)$$

e quindi ogni permutazione di tipo (2,2) è prodotto di cicli di lunghezza 3. Supponiamo infine che $|X| \geq 5$ ed $e \in X \setminus \{a,b,c,d\}$. Allora

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

e quindi, se $|X| \geq 5$, ogni ciclo di lunghezza 3 è prodotto di permutazioni di tipo $(2,2)$. La tesi segue allora dal Lemma 5.1.6. ∎

Sia

$$(x_1, x_2, \ldots, x_k)$$

un ciclo di lunghezza k in S_X e sia $\sigma \in S_X$. Allora

$$\sigma^{-1}(x_1, x_2, \ldots, x_k)\sigma = (x_1^\sigma, x_2^\sigma, \ldots, x_k^\sigma). \tag{5.1}$$

Infatti, posto $\gamma := (x_1, x_2, \ldots, x_k)$, risulta, per ogni $i \in \{1, \ldots, k-1\}$,

$$(x_i^\sigma)^{\sigma^{-1}\gamma\sigma} = x_i^{\gamma\sigma} = x_{i+1}^\sigma,$$

e

$$(x_k^\sigma)^{\sigma^{-1}\gamma\sigma} = x_k^{\gamma\sigma} = x_1^\sigma,$$

Infine, se $x \notin \{x_1, \ldots, x_k\}$, allora

$$(x^\sigma)^{\sigma^{-1}\gamma\sigma} = x^{\gamma\sigma} = x^\sigma.$$

Da questo segue immediatamente

Corollario 5.1.8 *1. Due cicli di S_X sono coniugati in S_X se e solo se hanno la medesima lunghezza.*

2. Due permutazioni di S_X sono coniugate in S_X se e solo se hanno lo stesso tipo.

5.2 Struttura normale dei gruppi simmetrici

In questo capitolo determiniamo la struttura normale dei gruppi simmetrici. Questo capitolo segue essenzialmente la dimostrazione in [27].

Le strutture normali di S_2, S_3 e S_4 sono facili da verificare a mano: S_2 è ciclico di ordine 2, i suoi sottogruppi sono S_2 e $\{1\}$ e sono normali, i sottogruppi normali di S_3 sono S_3, A_3 e $\{1\}$ e i sottogruppi normali di S_4 sono S_4, A_4, il sottogruppo di A_4 generato dalle permutazioni di tipo $(2,2)$ (il sottogruppo di Klein) e $\{1\}$. Si osservi che in questi tre casi i sottogruppi normali coincidono con i termini della serie derivata. In particolare S_2, S_3 ed S_4 sono gruppi risolubili. Per $n \geq 5$ proveremo invece che S_n non è risolubile perchè contiene il sottogruppo A_n che è semplice e non abeliano. Questo è il punto critico nella dimostrazione di Galois che non esistono formule risolutive generali per le equazioni polinomiali di grado maggiore o uguale a 5, cioè che, per tali equazioni, non è possibile esprimere le radici a partire dai coefficienti con delle espressioni che coinvolgano le quattro operazioni e l'estrazione di radice n-esima.

Lemma 5.2.1 *Sia $n \geq 5$ ed N un sottogruppo non identico di A_n e normale in S_n. Allora $N = A_n$.*

DIMOSTRAZIONE. Sia σ un elemento non identico di N. Per l'Esercizio 5.3.4 esiste una trasposizione τ di S_n che non commuta con σ. Per il Corollario 5.1.8 $\sigma^{-1}\tau\sigma$ è una trasposizione e quindi $\sigma^{-1}\tau^{-1}\sigma\tau$ è un elemento non identico di N che è prodotto di due trasposizioni. In particolare per il Lemma 5.1.6 e la Proposizione 5.1.7, segue che

$$N \geq \langle [\sigma,\tau]^{\delta} | \delta \in S_n \rangle = A_n$$

da cui la tesi. ∎

Teorema 5.2.2 *Se $n \geq 5$, A_n è un gruppo semplice non abeliano.*

DIMOSTRAZIONE. Sia per assurdo S un sottogruppo normale proprio di A_n. Sia τ una trasposizione in S_n. Per l'Esercizio 5.3.3

$$S_n = \langle A_n, \tau \rangle. \tag{5.2}$$

Per il Lemma 5.2.1 e l'Esercizio 1.2.12, segue che τ non normalizza S e quindi S^{τ} è un sottogruppo normale di A_n diverso da S. Osserviamo che

$$SS^{\tau} \text{ e } S \cap S^{\tau} \text{ sono sottogruppi normali di } A_n \tag{5.3}$$

perché prodotto e risp. intersezione di sottogruppi normali di A_n. Inoltre

$$(SS^\tau)^\tau = S^\tau S^{\tau\tau} = S^\tau S = SS^\tau \tag{5.4}$$

e, similmente,

$$(S \cap S^\tau)^\tau = S^\tau \cap S^{\tau\tau} = S^\tau \cap S = S \cap S^\tau. \tag{5.5}$$

Da (5.2), (5.3), (5.4), (5.5) e l'Esercizio 1.2.12 segue che

$$SS^\tau \text{ e } S \cap S^\tau \text{ sono normali in } S_n. \tag{5.6}$$

Poichè $\{1\} < S < SS^\tau \leq A_n$ e $\{1\} \leq S \cap S^\tau < S < A_n$, da (5.6) e dal Lemma 5.2.1, segue che

$$\text{per ogni trasposizione } \tau,\ SS^\tau = A_n \text{ e } S \cap S^\tau = \{1\}. \tag{5.7}$$

Per il Secondo Teorema di Omomorfismo segue che

$$|A_n| = |S||S^\tau| = |S|^2,$$

in particolare S ha ordine pari, quindi, per l'Esercizio 1.2.14, S contiene un'involuzione ρ. Per l'Esercizio 5.3.2 esiste una trasposizione γ tale che

$$\rho^\gamma = \rho$$

e quindi

$$1 \neq \rho = \rho^\gamma \leq S \cap S^\gamma,$$

in contraddizione con (5.7). ∎

Corollario 5.2.3 *Se $n \geq 5$, gli unici sottogruppi normali di S_n sono $\{1\}$, A_n ed S_n.*

Dimostrazione. Sia N un sottogruppo normale di S_n. Se N contiene A_n, allora $N \in \{A_n, S_n\}$ perchè A_n è massimale in S_n. Se N non contiene A_n allora $N \cap A_n$ è un sottogruppo normale di S_n strettamente contenuto in A_n. Per Lemma 5.2.1

$$N \cap A_n = \{1\}.$$

Se, per assurdo, $N \neq \{1\}$, allora

$$S_n = NA_n$$

e quindi, per il Secondo Teorema di Omomorfismo

$$N \cong S_n/A_n \cong \mathbf{Z}/2\mathbf{Z}.$$

In particolare N è abeliano e quindi

$$N \leq C_{S_n}(N). \tag{5.8}$$

D'altra parte

$$[A_n, N] \leq A_n \cap N = \{1\}$$

e quindi anche

$$A_n \leq C_{S_n}(N) \tag{5.9}$$

Quindi, per l'Esercizio 1.2.12, $N \leq Z(S_n) = \{1\}$, in contraddizione con l'Esercizio 5.3.4 ■

5.3 Esercizi

Esercizio 5.3.1 *Si provi che se σ è una permutazione di tipo $(l_1, l_2, \ldots, l_k)$, allora l'ordine di σ è il minimo comune multiplo di $l_1, l_2, \ldots, l_k$.*

Esercizio 5.3.2 *Si provi che se ρ è un'involuzione di S_n, allora esiste una trasposizione γ di S_n tale che $\rho\gamma = \gamma\rho$.*

Esercizio 5.3.3 *Sia X un insieme e τ una trasposizione in S_X. Si provi che $S_X = \langle A_X, \tau \rangle$.*

Esercizio 5.3.4 *Sia X un insieme. Si provi che, se $|X| \geq 3$, $Z(S_X) = \{1\}$. In particolare si deduca che se σ è un elemento non identico di S_X, allora esiste una trasposizione τ tale che $\tau\sigma \neq \sigma\tau$.*

Esercizio 5.3.5 *Sia A_4 il gruppo alterno (cioè delle permutazioni di classe pari) sull'insieme $\{1,2,3,4\}$. Sia $N = \langle (1,2)(3,4), (1,3)(2,4) \rangle$ e sia $U = \langle (1,2)(3,4) \rangle$. Si dimostri che:*

1. *$N = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$;*
2. *N è un gruppo abeliano isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$;*
3. *$N \trianglelefteq A_4$;*
4. *$U = \{(1), (1,2)(3,4)\}$;*
5. *U é un gruppo abeliano isomorfo a $\mathbf{Z}_2$;*
6. *$U \trianglelefteq N$;*
7. *$U^{(1,2,3)} \neq U$ dunque $U \not\trianglelefteq A_4$;*
8. *si determinino tutti i sottogruppi, i sottogruppi subnormali ed i sottogruppi normali di A_4 e si rappresenti graficamente $\mathcal{L}(A_4)$;*
9. *si trovino degli elementi g_1, g_2, h_1, h_2 di A_4 tali che $g_i U = h_i U$ $(i = 1, 2)$, ma $g_1 g_2 U \neq h_1 h_2 U$.*

Esercizio 5.3.6 *Nel gruppo simmetrico S_4 consideriamo le permutazioni $\rho = (1,2,3,4)$ e $\sigma = (1,3)$.*

1. *Si provi che* $\sigma^2 = \rho^4 = 1$.
2. *Si provi che l'insieme* $D_8 = \{1, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ *è un sottogruppo di* S_4.
3. *Si determinino tutti i sottogruppi, i sottogruppi subnormali ed i sottogruppi normali di* D_8 *e si rappresenti graficamente* $\mathcal{L}(D_8)$. *In particolare si osservi che il sottogruppo formato dagli elementi* 1 *e* σ *è subnormale ma non normale.*

Il gruppo D_8 *si dice gruppo diedrale di ordine* 8. *Esso viene usualmente definito come gruppo delle simmetrie di un quadrato di vertici (in senso oantiorario)* $1, 2, 3, 4$*:* ρ *è la rotazione (in senso antiorario) di* $\pi/2$ *attorno al centro e* σ *è il ribaltamento attorno all'asse passante per i vertici* 2 *e* 4.

Capitolo 6

Commutatori e interderivato

In questa sezione introduciamo due strumenti per misurare la non commutatività tra elementi (il commutatore) e, elemento per elemento, tra due sottogruppi (l'interderivato). L'interderivato e le sue proprietà sono costantemente usate nella teoria dei gruppi; in particolare nel capitolo sui gruppi risolubili e nilpotenti useremo le proprietà dell'interderivato per costruire la serie delle chiusure normali, la serie derivata e la serie centrale discendente e dimostrarne le proprietà. Inoltre il Lemma 6.2.1 ed il Lemma dei Tre Sottogruppi (Esercizio 6.3.9) saranno costantemente utilizzati nello studio delle azioni dei gruppi sui gruppi.

6.1 Commutatori

Sia G un gruppo, a, b elementi di G. Ovviamente a e b commutano, cioè $ab \neq ba$, se e solo se

$$a^{-1}b^{-1}ab = 1.$$

L'elemento $a^{-1}b^{-1}ab$ si dice **commutatore** degli elementi a e b e si indica con

$$[a, b].$$

Si osservi che

$$ab = ba(ba)^{-1}ab = baa^{-1}b^{-1}ab = ba[a, b]$$

quindi il commutatore di a e b può essere visto certo senso come il residuo che si ottiene quando li si commuta.

Si osservi inoltre che l'applicazione

$$\begin{aligned}[\ , \ ]: \quad & G \times G \to G \\ & (a, b) \mapsto [a, b]\end{aligned}$$

definisce un'operazione su G. In generale però $[a,[b,c]] \neq [[a,b],c]$ (Esercizio 6.3.7), quindi tale operazione non è associativa.

Nel lemma seguente riassumiamo le principali regole di calcolo dei commutatori. Sono tutte immediate conseguenze della definizione di commutatore; la prima l'abbiamo appena dimostrata, la verifica delle altre è lasciata per esercizio.

Lemma 6.1.1 *Siano a, b e c elementi di un gruppo G. Allora valgono le seguenti identità:*

$C1$ $ab = ba[a,b]$;

$C2$ $[a,b] = [b,a]^{-1}$;

$C3$ $[ab,c] = [a,c]^b[b,c]$;

$C4$ $[a,bc] = [a,c][a,b]^c$;

$C5$ $[a,b^{-1}] = ([a,b]^{b^{-1}})^{-1}$;

$C6$ $[a^{-1},b] = ([a,b]^{a^{-1}})^{-1}$;

$C7$ (Identità di Hall-Witt) $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1$.

Osserviamo che l'Identità di Hall-Witt corrisponde, in teoria dei gruppi, a quella che, nella teoria delle algebre di Lie, si chiama Identità di Jacobi.

Un'importante proprietà dei commutatori è che essi sono conservati dagli omomorfismi di gruppo; si ha infatti il seguente risultato (anche qua la verifica è lasciata per esercizio).

Lemma 6.1.2 *Sia $\phi: G \to H$ un omomorfismo di gruppi e siano a, b elementi di G. Allora*

$$([a,b])^\phi = [a^\phi, b^\phi].$$

In particolare, se $g \in G$, allora

$$([a,b])^g = [a^g, b^g].$$

6.2 L'interderivato di due sottogruppi

Siano H e K due sottoinsiemi di un gruppo G. L'**interderivato** $[H,K]$ è il sottogruppo di G generato dai commutatori $[h,k]$ dove $h \in H$ e $k \in K$.

$$[H,K] = \langle [h,k] | h \in H, k \in K \rangle.$$

Le principali proprietà dell'interderivato sono le seguenti:

Lemma 6.2.1 *Siano H, K e L sottogruppi di un gruppo G, allora*

$I1$ $[H,K] = \{1\}$ *se e solo se ogni elemento di H commuta con ogni elemento di K.*

*I*2 *se* $H_1 \leq H$ *e* $K_1 \leq K$*, allora* $[H_1, K_1] \leq [H, K]$*;*

*I*3 $[H, K] = [K, H]$*;*

*I*4 $[H, K] \trianglelefteq \langle H, K \rangle$*;*

*I*5 $H \trianglelefteq \langle H, K \rangle$ *se e solo se* $[H, K] \leq H$

*I*6 $H[H, K]$ *è il più piccolo sottogruppo normale di* $\langle H, K \rangle$ *che contiene* H*;*

*I*7 (Lemma dei Tre Sottogruppi) *se*

$$[H, K, L] \text{ e } [K, L, H]$$

sono contenuti in un sottogruppo normale N *di* G*, allora anche*

$$[L, H, K]$$

è contenuto in N*.*

Dimostrazione. *I*1 e *I*2 discendono immediatamente dalla definizione di interderivato.

*I*3 segue dal punto *C*2 del Lemma 6.1.1 e dal fatto che H, K e $[H, K]$ sono sottogruppi.

*I*4: siano $a, b \in H$ e $c \in K$. Dal punto 3. del Lemma 6.1.1 si ottiene che,

$$[a, c]^b = [ab, c][b, c]^{-1} \in [H, K].$$

Poiché $[H, K]$ è generato dagli elementi $[a, c]$ dove $a \in H$ e $c \in K$, per l'Esercizio 1.2.8 segue che

$$H \leq N_G([H, K]).$$

D'altra parte $[H, K] = [K, H]$ quindi, scambiando i ruoli di H e K, si ottiene anche

$$K \leq N_G([H, K]),$$

da cui segue la tesi.

*I*5: sia $h \in H$ e $k \in K$. Dal punto 1. del Lemma 6.1.1 risulta

$$h^k = h[h, k],$$

quindi $h^k \in H$ se e solo se $[h, k] \in H$ da cui si ottiene 5.

*I*6: sia N il più piccolo sottogruppo normale di $\langle H, K \rangle$ che contiene H allora

$$[H, K] \leq [N, K] \leq N$$

per il punto precedente. Viceversa si osservi che, poichè $[H, K] \trianglelefteq \langle H, K \rangle$, $H[H, K]$ è un sottogruppo di $\langle H, K \rangle$. Quindi basta mostrare che per ogni $a \in K$ risulta $(H[H, K])^a = H[H, K]$. Ora se $r, h \in H$ e $k \in K$, allora, per il punto 1. del Lemma 6.1.1, risulta

$$(r[h, k])^a = r^a[h, k]^a = r[ra][h, k]^a$$

che appartiene a $H[H,K]$ per il punto 3., da cui segue il punto 6., essendo $H[H,K]$ generato dagli elementi $r[h,k]$ con $r,h \in H$ e $k \in K$.

Infine, $I7$ segue dall'Identità di Hall-Witt. ■

Dal fatto che i commutatori sono conservati dagli omomorfismi, segue che anche l'interderivato è conservato dagli omomorfismi:

Lemma 6.2.2 *Sia $\phi: G \to G^*$ un omomorfismo di gruppi e siano H, K sottogruppi di G, allora $[H,K]^\phi = [H^\phi, K^\phi]$.*

DIMOSTRAZIONE. Esercizio. ■

Se N è un sottogruppo normale di un gruppo G allora si può caratterizzare l'interderivato $[N,G]$ nel modo seguente:

Lemma 6.2.3 *Sia G un gruppo e $N \trianglelefteq G$. Allora*

$$N/[N,G] \leq Z(G/[N,G]).$$

Inoltre se K è un sottogruppo normale di G contenuto in N e tale che $N/K \leq Z(G/K)$ allora

$$[N,G] \leq K.$$

DIMOSTRAZIONE. Per ogni $h \in N$ e $g \in G$ risulta $hg = gh[h,g]$, da cui, passando al quoziente modulo $[N,G]$, si ottiene

$$h[N,G]g[N,G] = (hg)[N,G] = (gh)[h,g][N,G] = (gh)[N,G]$$

da cui $N/[N,G] \leq Z(G/[N,G])$. Infine sia K un sottogruppo normale di G contenuto in N e tale che $N/K \leq Z(G/K)$. Allora per ogni $h \in N$ e $g \in G$ risulta

$$(hg)K = hKgK = gKhK = (gh)K$$

, cioè $[h,g] = h^{-1}g^{-1}hg \in K$, da cui la tesi essendo $[N,G] = \langle [h,g] | h \in N, g \in G \rangle$. ■

In particolare, se G è un gruppo il sottogruppo $[G,G]$ si chiama **derivato** o **commutatore** di G e si indica con G' o anche con $G^{(1)}$. Dal Lemma 6.2.3 segue immediatamente che

Corollario 6.2.4 *Il derivato G' di un gruppo G è il più piccolo sottogruppo normale di G tale che il quoziente G/G' sia abeliano.*

Si osservi inoltre che, dal Lemma 6.2.2, segue che, se $\phi: G \to H$ un omomorfismo di gruppi, allora

$$(G')^\phi = (G^\phi)' \ (\leq H').$$

6.3 Esercizi

Esercizio 6.3.1 *Siano N e K due sottogruppi normali di G tali che $N \cap K = \{1\}$. Si provi che $[N, K] = \{1\}$.*

Esercizio 6.3.2 *Sia G un gruppo in cui ogni sottogruppo ha un unico complemento.*
a) Si provi che se H è un sottogruppo di G e K è un suo complemento, allora H normalizza K e K normalizza H. b) Si deduca che $[H, K]=\{1\}$. c) Si provi che ogni sottogruppo abeliano è centrale. d) Si provi che G è abeliano. suggerimento: per provare a) usare l'Esercizio 2.6.7

Esercizio 6.3.3 *Sia G un gruppo finito. Si provi che ogni sottogruppo di G ha un unico complemento se e solo se G è abeliano ed il suo ordine è prodotto di numeri primi distinti. suggerimento: usare gli Esercizi 3.5.10 e 6.3.2*

Esercizio 6.3.4 *Siano A, B e C sottogruppi di un gruppo G e supponiamo che $[A, C]$ sia normale in $\langle [A, C], B\rangle$. Si provi che $[AB, C] = [A, C][B, C]$.*

Esercizio 6.3.5 *Siano A, B e C sottogruppi di un gruppo G e supponiamo che A e C siano normali in $\langle A, B, C\rangle$. Si provi che $[AB, C] = [A, C][B, C]$.*

Osserviamo che, in generale, se A e C non sono normali in $\langle A, B, C\rangle$, allora il risultato non è più vero (vedi Esercizio 8.3.50.

Esercizio 6.3.6 *A, B e C sottogruppi di un gruppo G con $[A, B] = \{1\}$. Si provi che $[A, BC] = [A, C]$.*

Esercizio 6.3.7 *Siano a, b e c elementi di un gruppo G. Si provi con un esempio che non è vero che in generale $[[a, b], c] = [a, [b, c]]$, (*cioè l'operazione in G che ad una coppia di elementi associa il loro commutatore in generale non è associativa*).*

Analogamente si può dimostrare che, se H, K ed L sono sottogruppi di G, in generale $[[H, K], L]$ è diverso da $[H, [K, L]]$
Per indicare l'elemento $[[a, b], c]$ si usa di solito il simbolo $[a, b, c]$ e per indicare l'interderivato $[[H, K], L]$ si usa il simbolo $[H, K, L]$.

Esercizio 6.3.8 *Si provi l'identità di Hall-Witt:*

Esercizio 6.3.9 *Si provi il Lemma dei Tre Sottogruppi*

Capitolo 7

Gruppi risolubili e gruppi nilpotenti

In questo capitolo introduciamo la classe dei gruppi risolubili e la classe dei gruppi nilpotenti.

Un gruppo è risolubile se possiede una serie di lunghezza finita i cui fattori sono abeliani. Quindi la classe dei gruppi risolubili è la più piccola classe chiusa per estensioni che contiene i gruppi abeliani. Oltre a questo proveremo che la classe dei gruppi risolubili è anche chiusa per sottogruppi e quozienti. L'origine del nome discende dal Criterio di Risolubilità di Galois: un polinomio, a coefficienti in un campo di caratteristica 0, è risolubile per radicali se e solo se il suo gruppo di Galois è risolubile.

La classe dei gruppi nilpotenti, è una sottoclasse propria della classe dei gruppi risolubili. Vedremo che anche questa classe contiene la classe dei gruppi abeliani, è chiusa per sottogruppi e quozienti ma non è chiusa per estensioni. Vedremo inoltre che, in un gruppo nilpotente, ogni sottogruppo è subnormale o, equivalentemente, che ogni sottogruppo proprio è propriamente contenuto nel suo normalizzante. Questa propriet'a è fondamentale nell'analisi locale di un gruppo finito e, più avanti, dopo aver introdotto le azioni di gruppo e dimostrato i Teoremi di Sylow, vedremo che questa proprietà caratterizza i gruppi nilpotenti finiti. Vedremo inoltre che, per ogni numero primo p, ogni p-gruppo finito (cioè in cui ogni elemento ha ordine una potenza di p) è nilpotente e, viceversa, ogni gruppo nilpotente è prodotto di p-gruppi per primi p distinti. Quindi, sostanzialmente, lo studio dei gruppi nilpotenti finiti si riduce allo studio dei p-gruppi finiti.

Esiste infine un importante relazione tra la teoria dei gruppi finiti risolubili e quella dei gruppi finiti nilpotenti: nel Capitolo **??** vedremo infatti che, per il Teorema di Fitting (Teorema 10.1.9), ogni gruppo risolubile finito G è sostanzialmente controllato dal suo sottogruppo di Fitting che, è il massimo sottogruppo normale e nilpotente di G.

7.1 Serie abeliane e gruppi risolubili

Sia G un gruppo finito, H e K sottogruppi di G con $K \leq H$. Una serie subnormale da K a H

$$G_0 = H \geq G_1 \geq \ldots \geq G_k = K \tag{7.1}$$

si dice **abeliana** se G_{i-1}/G_i è un gruppo abeliano per ogni $i \in \{1, \ldots, k\}$.

Lemma 7.1.1 *Sia G un gruppo, H, K ed N un sottogruppi di G, con $H \leq K$, N normale in G, e*

$$G_0 = H \geq G_1 \geq \ldots \geq G_k = K \tag{7.2}$$

una serie abeliana da H a K di G. Allora la serie

$$G_0N/N \geq G_1N/N \geq \ldots \geq G_kN/N \tag{7.3}$$

è una serie abeliana da HN/N a KN/N.

DIMOSTRAZIONE. Segue immediatamente dal Teorema di Corrispondenza. ∎

Un gruppo G si dice **risolubile** se possiede una serie abeliana da G a $\{1\}$. Se G è un gruppo finito, per l'Esercizio 2.6.9 esiste una serie di composizione

$$H_0 = H \geq H_1 \geq \ldots \geq H_l = K \tag{7.4}$$

contenente la serie (7.1). Poichè i sottogruppi ed i quozienti di gruppi abeliani sono abeliani anche la serie (7.4) è abeliana e quindi i quozienti H_{i-1}/H_i sono ciclici di ordine primo. In particolare

Proposizione 7.1.2 *Un gruppo finito G è risolubile se e solo se possiede una serie*

$$H_0 = G \geq H_1 \geq \ldots \geq H_l = \{1\}$$

i cui fattori sono ciclici di ordine primo.

7.1.1 La serie derivata

Sia G un gruppo e G' il suo derivato. Definiamo per ogni $n \in \mathbf{N}$ il **derivato n-esimo** $G^{(n)}$ di G per induzione nel modo seguente:

1. $G^{(0)} = G$,
2. $G^{(1)} = G'$ e, per induzione,
3. $G^{(n+1)} = (G^{(n)})'$.

La serie

$$G^{(0)} = G \geq G^{(1)} \geq \ldots \geq G^{(n)} \geq G^{(n+1)} \geq \ldots$$

si dice **serie derivata**. Per il Corollario 6.2.4 $G^{(n+1)} \trianglelefteq G^{(n)}$ e $G^{(n+1)}/G^{(n)}$ è un gruppo abeliano per ogni $n \in \mathbf{N}$. La serie derivata è quindi una serie abeliana. Tra le serie abeliane, la serie derivata è quella che scende più rapidamente:

Proposizione 7.1.3 *Sia G un gruppo e*

$$G = G_0 \geq G_1 \geq \ldots \geq G_n$$

una serie abeliana di G. Allora per ogni $i \in \{0, \ldots, n\}$, risulta

$$G^{(i)} \leq G_i.$$

DIMOSTRAZIONE. Per induzione su i. Se $i = 0$, allora $G^{(0)} = G = G_0$. Supponiamo la tesi vera per $i - 1$, allora $G^{(i-1)} \leq G_{i-1}$, e quindi per il Lemma 6.2.1.2

$$G^{(i)} = (G^{(i-1)})' \leq (G_{i-1})'.$$

D'altra parte, poichè G_{i-1}/G_i è abeliano, per il Corollario 6.2.4, $(G_{i-1})' \leq G_i$, da cui la tesi ∎

Corollario 7.1.4 *Un gruppo G è risolubile se e solo se $G^{(k)} = \{1\}$ per qualche $k \in \mathbf{N}$.*

DIMOSTRAZIONE. Se esiste $k \in \mathbf{N}$ tale che $G^{(k)} = \{1\}$, allora la serie

$$G^{(0)} = G \geq G^{(1)} \geq \ldots \geq G^{(k)} = \{1\}$$

è una serie abeliana da G a $\{1\}$, da cui la tesi per l'Esercizio 6.2.1.4. Viceversa se G è risolubile, allora G possiede una serie abeliana

$$G_0 = G \geq G_1 \geq \ldots \geq G_k = \{1\}.$$

Per la Proposizione 7.1.3, $G^{(k)} \leq G_k = \{1\}$, da cui la tesi. ∎

Corollario 7.1.5 *Ogni sottogruppo ed ogni quoziente di un gruppo risolubile è risolubile.*

DIMOSTRAZIONE. Sia H un sottogruppo di un gruppo G. Per induzione su i si vede facilmente che, per ogni $i \in \mathbf{N}$, $H^{(i)} \leq G^{(i)}$. Quindi, se G è risolubile, per il Corollario 7.1.4, esiste $k \in \mathbf{N}$ tale che $H^{(k)} \leq G^{(k)} = \{1\}$, e dunque H è risolubile. Infine, se $\overline{G}$ è un quoziente di un gruppo risolubile G, allora $\overline{G}$ è risolubile per il Lemma 7.1.1. ∎

Se G è un gruppo risolubile, il più piccolo intero k tale che $G^{(k)} = \{1\}$ si dice **lunghezza derivata** di G. Per il Corollario 7.1.5, la lunghezza derivata è lil minimo delle lunghezze delle serie abeliane da G a $\{1\}$.

7.2 Serie centrali e gruppi nilpotenti

Sia G un gruppo e siano H e K sottogruppi normali di G con $H \geq K$. Una serie da H a K

$$H = G_0 \geq G_1 \geq \ldots \geq G_k = K$$

si dice **centrale** se per ogni $i \in \{1, \ldots, k\}$

1. $G_i \trianglelefteq G$ e
2. G_{i-1}/G_i è contenuto nel centro di G/G_i

Un gruppo che possiede una serie centrale da G a $\{1\}$ si dice **nilpotente**. Ovviamente ogni gruppo abeliano è nilpotente e, poiché una serie centrale è anche abeliana, segue che

Teorema 7.2.1 *Ogni gruppo nilpotente è risolubile.*

Non vale il viceversa, infatti S_3 è un gruppo risolubile ma non è nilpotente (il suo centro è identico). Dunque la nilpotenza è una condizione più forte della risolubilità. In particolare, questo mostra anche che la classe dei gruppi nilpotenti non è chiusa per estensioni.

Anche per le serie centrali vale un risultato analogo al Lemma 7.1.1:

Lemma 7.2.2 *Sia G un gruppo, H, K ed N un sottogruppi normali di G e*

$$G_0 = H \geq G_1 \geq \ldots \geq G_k = K \tag{7.5}$$

una serie centrale di G da H a K. Allora la serie

$$G_0N/N \geq G_1N/N \geq \ldots \geq G_kN/N \tag{7.6}$$

è una serie centrale di G/N da HN/N a KN/N.

Dimostrazione. Che la serie sia normale segue dal Teorema di Corrispondenza. Che, per ogni $i \in \{1, \ldots, k\}$, G_i/G_{i-1} sia contenuto nel centro di G segue dal fatto che, se un elemento di un gruppo $\overline{G}$ è centrale, lo sono anche la sue proiezioni nei quozienti di $\overline{G}$. ∎

7.2.1 La serie centrale ascendente

Il Teorema di Corrispondenza suggerisce un modo naturale per costruire induttivamente una serie centrale in un gruppo G partendo dal sottogruppo identico: poniamo infatti

1. $Z_0(G) = \{1\}$,
2. $Z_1(G) = Z(G)$ e, per induzione, sia

3. $Z_i(G)$ l'unico sottogruppo di G tale che $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.

Si osservi che, per il Teorema di Corrispondenza, $Z_i(G)$ esiste ed è unico , e la serie

$$Z_0(G) \leq Z_1(G) \leq \ldots \leq Z_{i-1(G)} \leq Z_i(G) \leq \ldots$$

è una serie centrale. Questa serie si dice **serie centrale ascendente** ed è caratterizzata dal fatto che, tra le serie centrali che partono da $\{1\}$, è quella che sale più rapidamente:

Lemma 7.2.3 *Sia*

$$G_0 = \{1\} \leq G_1 \leq \ldots \leq G_{i-1} \leq G_i \leq \ldots$$

una serie centrale. Allora per ogni $i \in \mathbf{N}$

$$G_i \leq Z_i(G).$$

DIMOSTRAZIONE. Per induzione su i. Se $i = 0$ allora $Z_0(G) = \{1\} = G_0$. Sia $i \geq 1$ e supponiamo per ipotesi induttiva che

$$G_{i-1} \leq Z_{i-1}(G) \leq Z_i(G).$$

Consideriamo la proiezione canonica

$$\pi\colon G/G_{i-1} \to G/Z_{i-1}(G).$$

Allora

$$\begin{aligned}(G_i/G_{i-1})^\pi &\leq (Z(G/G_{i-1}))^\pi \leq Z((G/G_{i-1})^\pi) = \\ &= Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G) = \\ &= (Z_i(G)/G_{i-1})^\pi.\end{aligned}$$

Quindi

$$G_i/G_{i-1} \leq Z_i(G)/G_{i-1}$$

e

$$G_i \leq Z_i(G).$$

■

Corollario 7.2.4 *Un gruppo G è nilpotente se e solo se la serie centrale ascendente termina con G.*

Corollario 7.2.5 *Se G è un gruppo nilpotente e*

$$Z_0(G) = \{1\} < Z_1(G) < \ldots < Z_k(G) = G$$

è la sua serie centrale ascendente, allora ogni serie centrale ha lunghezza maggiore o uguale a k.

Se G è un gruppo nilpotente, allora la lunghezza della serie centrale ascendente si dice **classe di nilpotenza** di G. Per il Lemma 7.2.3, la classe di nilpotenza è la minima lunghezza delle serie centrali di G da $\{1\}$ a G.

7.2.2 La serie centrale discendente

Sia G un gruppo. Definiamo ora, partendo da G e in modo analogo a quanto fatto per la serie derivata, una serie centrale discendente

$$\gamma_0(G) = G \geq \gamma_1(G) \geq \ldots \geq \gamma_{i-1}(G) \geq \gamma_i(G) \geq \ldots$$

ponendo

1. $\gamma_0(G) = G$ e, induttivamente,
2. $\gamma_i(G) = [\gamma_{i-1}(G), G]$

Per i punti 4. e 5. del Lemma 6.2.1 e l'induzione su i, si ottiene

$$\gamma_i(G) = [\gamma_{i-1}(G), G] \leq \gamma_{i-1}(G)$$

e, per il Lemma 6.2.3,

$$\gamma_{i-1}(G)/\gamma_i(G) \leq Z(G/\gamma_i(G)).$$

Dunque questa è una serie centrale e si chiama **serie centrale discendente**. Come abbiamo già anticipato, analogamente alla serie derivata, la serie centrale discendente è, tra le serie centrali che partono da G quella che scende nel modo più rapido.

Lemma 7.2.6 *Sia*

$$G_0 = G \geq G_1 \geq \ldots \geq G_{i-1} \geq G_i \geq \ldots$$

una serie centrale. Allora per ogni $i \in \mathbf{N}$

$$G_i \geq \gamma_i(G).$$

DIMOSTRAZIONE. Per induzione su i. Se $i = 0$ allora $\gamma_0(G) = G = G_0$. Sia $i \geq 1$ e supponiamo per ipotesi che $\gamma_{i-1}(G) \leq G_{i-1}$. Allora per il Lemma 6.2.3

$$G_i \geq [G_{i-1}, G]$$

e quindi, per il punto 2. del Lemma 6.2.1,

$$G_i \geq [G_{i-1}, G] \geq [\gamma_{i-1}(G), G] = \gamma_i(G)$$

da cui la tesi. ∎

Corollario 7.2.7 *Un gruppo G è nilpotente se e solo se la serie centrale discendente termina con il sottogruppo identico*

DIMOSTRAZIONE. Esercizio ∎

Corollario 7.2.8 *Se G è un gruppo nilpotente allora la sua classe di nilpotenza coincide con la lunghezza della serie centrale discendente.*

DIMOSTRAZIONE. Esercizio ■

Corollario 7.2.9 *Se G è un gruppo nilpotente, allora ogni suo sottogruppo ed ogni suo quoziente è nilpotente*

DIMOSTRAZIONE. La dimostrazione è del tutto analoga a quella del Corollario 7.1.5 ■

7.3 La serie delle chiusure normali

Sia N un sottogruppo di un gruppo G. Il sottogruppo $N[N, G]$ si dice **chiusura normale** di N in G. Per $I6$ del Lemma 6.2.1, $N[N, G]$ è il più piccolo (per inclusione) sottogruppo normale di G contenente N. Definiamo per induzione una serie

$$N^{(G,0)} \geq N^{(G,1)} = N[G, N] \geq N^{(G,2)} \geq \ldots \geq N^{(G,i)} \geq \ldots \tag{7.7}$$

ponendo,

1. $N^{(G,0)} = G$ e, per ogni $i \in \mathbf{N} \setminus \{0\}$,
2. $N^{(G,i)} = N[N^{(G,i-1)}, N]$.

La serie (7.7) si dice **serie delle chiusure normali** di N in G.

Si osservi che, per il Lemma 6.2.1 ciascun termine della serie delle chiusure normali è normale nel precedente, quindi la serie delle chiusure normali è una serie subnormale. Se N è un sottogruppo subnormale di G, la serie delle chiusure normali è, tra le serie subnormali da G a N quella che scende più rapidamente.

Teorema 7.3.1 *Sia N un sottogruppo subnormale di G. Sia*

$$N_0 = G \geq N_1 \geq \ldots \geq N_k = N$$

una serie subnormale da G a N. Allora

$$N_i \geq N^{(G,i)}$$

per ogni $i \in \{1, \ldots, k\}$.

DIMOSTRAZIONE. per induzione su i. Se $i = 1$, la tesi segue dal Lemma 6.2.1.6. Sia $i > 1$ e supponiamo che

$$N_{i-1} \geq N^{(G,i-1)}.$$

Per il Lemma 6.2.1.6 e .2 segue allora

$$N_i \geq N[N_{i-1}, N] \geq N[N^{(G,i-1)}, N] = N^{(G,i)}.$$

■

Dalla definizione di difetto di subnormalità segue immediatamente che

Corollario 7.3.2 *Sia N un sottogruppo subnormale di un gruppo G. Allora il difetto di subnormalità di N in G è uguale alla lunghezza della serie delle chiusure normali di N in G.*

Poniamo ora

1. $[G,_1 N] = [G, N]$ e, per induzione su i,
2. $[G,_{i+1} N] = [[G,_i N], N]$

(Attenzione a non confondere $[G_i, N]$ con $[G,_i N]$!).

Lemma 7.3.3 *Sia G un gruppo e N un sottogruppo di G, allora, per ogni intero positivo i,*

$SN1$ $[G,_i N] \trianglelefteq \langle N, [G,_i N]\rangle$*;*

$SN2$ $[G,_i N] \leq \gamma_i(G)$*;*

$SN3$ $N^{(G,i)} = N[G,_i N]$.

Dimostrazione. Le verifiche della $SN1$ e della $SN2$ sono lasciate per esercizio (seguono immediatamente per induzione su i). Proviamo la $SN3$ per induzione su i. Se $i = 1$ la tesi segue dalla definizione. Supponiamo $i > 1$ e la tesi vera per $i - 1$. Per l'Esercizio 6.3.4, tenendo presente che $[N, N] \leq N$, abbiamo

$$N^{(G,i)} = N[N^{(G,i-1)}, N] = N[N[G,_{i-1} N], N] = N[[G,_{i-1} N], N] = N[G,_i N].$$

■

Chiudiamo con quella che, forse, è la proprietà più importante dei gruppi nilpotenti finiti:

Lemma 7.3.4 *Sia G un gruppo nilpotente di classe k, allora ogni sottogruppo di G è subnormale di difetto minore od uguale a k.*

Dimostrazione. Sia N un sottogruppo di G. Allora $\gamma_k(G) = \{1\}$ e quindi, per il Lemma 7.3.3, $N^{(G,k)} = N[G,_k N] \leq N\gamma_k(G) = N$. ■

Il Teorema 7.3.4 può essere riformulato anche nel modo seguente:

Corollario 7.3.5 *Sia G un gruppo nilpotente finito e H un sottogruppo non identico di G. Allora $H \neq G$ se e solo se esiste un sottogruppo K di G tale che $H \trianglelefteq K$ e $H \neq K$.*

7.4 Esercizi

Esercizio 7.4.1 *Un gruppo G si dice* **perfetto** *se $G = G'$. Si provi che*

1. *Ogni gruppo semplice non abeliano è perfetto;*
2. *se G è un gruppo perfetto e N è un sottogruppo normale massimale di G, allora il quoziente G/N è un gruppo semplice non abeliano.*

Esercizio 7.4.2 *Siano a e b elementi di un gruppo G. Si provi che se $ab \in Z(G)$, allora*

$$ab = ba.$$

Esercizio 7.4.3 *Si provi che D_8 è un gruppo nilpotente.*

Esercizio 7.4.4 *Siano G un gruppo ed N un sottogruppo normale di G tale che N e G/N siano risolubili. Si provi che G è risolubile.*
Si deduca che il prodotto diretto $A \times B$ di due gruppi risolubili A e B è risolubile

Esercizio 7.4.5 *Si dia un esempio di un gruppo non nilpotente G che possiede un sottogruppo normale N tale che N e G/N sono nilpotenti.*

Esercizio 7.4.6 *Si dimostri che il prodotto diretto $A \times B$ di due gruppi nilpotenti A e B è nilpotente (*suggerimento: si provi che $Z(A \times B) = Z(A) \times Z(B)$ e si proceda per induzione sulla somma delle classi di nilpotenza di A e B*).*

Esercizio 7.4.7 *Sia G un gruppo finito e sia Z_∞ l'unione di tutti i termini della serie centrale ascendente di G. Si provi che:*

1. *Z_∞ è un sottogruppo normale di G;*
2. *Z_∞ è un sottogruppo nilpotente di G;*
3. *$Z(G/Z_\infty) = \{1\}$.*

Il sottogruppo Z_∞ si dice **ipercentro** di G.

Esercizio 7.4.8 *Sia G un gruppo finito. Indichiamo con $G^{(\infty)}$ l'intersezione di tutti i termini della serie derivata di G. Si provi che:*

1. *$G^{(\infty)}$ è un gruppo perfetto;*
2. *$G/G^{(\infty)}$ è risolubile;*
3. *se N è un sottogruppo normale di G tale che G/N è risolubile, allora $N \geq G^{(\infty)}$;*
4. *si deduca che se N_1 e N_2 sono sottogruppi normali di G tali che G/N_1 e G/N_2 sono risolubili, allora anche $G/(N_1 \cap N_2)$ è risolubile.*

Il sottogruppo $G^{(\infty)}$ si dice **residuo risolubile** di G

Esercizio 7.4.9 *Sia G un gruppo finito. Indichiamo con $\gamma_\infty(G)$ l'intersezione di tutti i termini della serie centrale discendente di G. Si provi che:*

1. $[\gamma_\infty(G), G] = \gamma_\infty(G)$;
2. $G/\gamma_\infty(G)$ *è nilpotente;*
3. *se N è un sottogruppo normale di G tale che G/N è nilpotente, allora $N \geq \gamma_\infty(G)$;*
4. *si deduca che se N_1 e N_2 sono sottogruppi normali di G tali che G/N_1 G/N_2 sono nilpotenti, allora anche $G/(N_1 \cap N_2)$ è nilpotente.*

Il sottogruppo $\gamma_\infty(G)$ si dice **residuo nilpotente** di G

Esercizio 7.4.10 *Sia G un gruppo nilpotente di classe k. Si dia una dimostrazione alternativa del Teorema 7.3.4 nel modo seguente: Sia $N = N_0$ un sottogruppo di G e si ponga $N_i = NZ_i(G)$. Si provi che la successione*

$$N_0 \leq N_1 \leq \ldots \leq N_k$$

è una serie subnormale da N a G.

Capitolo 8

Azioni di gruppi

Uno dei modi più efficaci per studiare i gruppi, in particolare i gruppi non abeliani, è quello di rappresentarli come gruppi di automorfismi di strutture matematiche. Più precisamente, se X è una struttura algebrico-relazionale e G è un gruppo, un'**azione** di G su X (o **rappresentazione**) di G come gruppo di automorfismi di X è un omomorfismo

$$\rho\colon G \to Aut(X).$$

Diremo, in tal caso, che G **agisce su** X via ρ. Quando non sarà necessario specificare l'azione ρ, scriveremo semplicemente x^g per indicare l'immagine x^{g^ρ} diell'elemento x di X tramite l'automorfismo g^ρ **indotto** da x via ρ. Per il Primo Teorema di Omomorfismo $G/\ker(\rho)$ è isomorfo ad un sottogruppo di $Aut(X)$. Quindi da informazioni sulla struttura X, che determina il suo gruppo degli automorfismi, si ottengono informazioni sul quoziente $G/\ker(\rho)$ di G. In particolare la rappresentazione ρ si dice **banale** se non da' informazioni su G, cioè se $G = \ker(\rho)$ e, al caso opposto, ρ si dice **fedele** se $\ker(\rho) = \{1\}$ (in questo caso G è isomorfo al gruppo di automorfismi che induce su X via ρ.

Esempio
Sia ρ una rappresentazione di G su un insieme X con n elementi. Allora $Aut(X) \cong S_n$ e quindi $|G/\ker(\rho)|$ deve essere un divisore di $n! = |S_n|$. In particolare, se $|G|$ non è un divisore di $n!$ e la rappresentazione non è triviale (cioè $\ker(\rho) \neq G$), G non è semplice perché $\ker(\rho)$ è un sottogruppo normale proprio non identico di G.

8.1 Azione di un gruppo su se stesso

Per mettere in pratica la strategia appena descritta è necessario trovare delle strutture opportune su cui rappresentare un gruppo G. Ovviamente G stesso (sia come insieme che come gruppo) è una struttura e quindi è uno dei principali candidati su cui cercare una rappresentazione. Nelle prossime sottosezioni

presenteremo due azioni fondamentali di un gruppo G su se stesso: una è per moltiplicazione a destra sul suo supporto, l'altra è per coniugio. Si tenga presente che la prima è un'azione su un insieme, la seconda è un'azione su un gruppo.

8.1.1 Azione di un gruppo sul suo supporto per moltiplicazione a destra

Sia G un gruppo. Per ogni $g \in G$ consideriamo l'applicazione

$$g^\delta : G \to G$$

definita, per ogni $x \in G$, da

$$x^{g^\delta} = xg.$$

Si vede facilmente che g^δ è una permutazione del supporto di G.

Teorema 8.1.1 *Sia G un gruppo, S_G il gruppo delle permutazioni del supporto di G e*

$$\delta : G \to S_G$$

la funzione che associa a ciascun elemento g di G la permutazione g^δ. Allora δ è un'azione di G sul suo supporto ed il nucleo di questa azione è $\{1\}$.

Dimostrazione. Per quanto appena visto δ è un'applicazione da G in S_G. Mostriamo che è un omomorfismo di gruppi. Siano g_1 e g_2 elementi di G, allora per ogni $x \in G$ risulta

$$x^{(g_1 g_2)^\delta} = x(g_1 g_2) = (xg_1)g_2 = (x^{g_1^\delta})g_2 = (x^{g_1^\delta})^{g_2^\delta} = x^{(g_1^\delta g_2^\delta)},$$

cioè

$$(g_1 g_2)^\delta = g_1^\delta g_2^\delta.$$

Infine $\ker(\delta) = \{g \in G | xg = x, \forall x \in G\} = \{1\}$. ∎

Corollario 8.1.2 (Teorema di Cayley) *Ogni gruppo è isomorfo ad un gruppo di permutazioni. Più precisamente ogni gruppo G è isomorfo ad un sottogruppo di S_X dove X è un insieme tale che $|X| = |G|$.*

Più in generale, sia H un sottogruppo di G e G/H l'insieme delle classi laterali destre di G su H. Per ogni $g \in G$ consideriamo l'applicazione

$$g^{\delta_{G/H}} : G/H \to G/H$$

definita, per ogni $Hx \in G/H$, da

$$(Hx)^{g^{\delta_{G/H}}} = H(xg).$$

Teorema 8.1.3 *Sia G un gruppo, $S_{G/H}$ il gruppo delle permutazioni di G/H e*

$$\delta_{G/H}: G \to Aut(G/H)$$

la funzione che ad ogni $g \in G$ associa la permutazione $g^{\delta_{G/H}}$. Allora $\delta_{G/H}$ è un'azione di G su G/H. Il nucleo di questa azione è l'insieme

$$core_G(H) := \bigcap_{x \in G} H^x$$

DIMOSTRAZIONE. La dimostrazione che $\delta_{G/H}$ è un omomorfismo di gruppi è analoga a quella del teorema precedente e viene lasciata per esercizio. Infine

$$\begin{aligned} \ker(\delta_{G/H}) &= \{g \in G | Hxg = Hx, \forall x \in G\} = \\ &\{g \in G | g \in x^{-1}Hx, \forall x \in G\} = \bigcap_{x \in G} H^x. \end{aligned}$$

■

Corollario 8.1.4 (TEOREMA DI CAYLEY GENERALIZZATO) *Sia G un gruppo ed H un sottogruppo di G. $G/core_G(H)$ è isomorfo ad un sottogruppo di $S_{G/H}$.*

Il sottogruppo $core_G(H)$ si chiama **cuore** di H in G ed è, come si vede facilmente, il più grande sottogruppo normale di G contenuto in H.

8.1.2 Azione di un gruppo su se stesso per coniugio

Sia G un gruppo. Per ogni $g \in G$, consideriamo l'applicazione

$$g^\gamma: G \to G$$

definita, per ogni $x \in G$, da

$$x^{g^\gamma} = g^{-1}xg.$$

Allora g^γ è un automorfismo di G. È chiaro infatti che g^γ è un'applicazione da G in se stesso. Inoltre se $x^{g^\gamma} = y^{g^\gamma}$, allora $g^{-1}xg = g^{-1}yg$ e quindi, moltiplicando a sinistra per g ed a destra per g^{-1} ambo i membri si ottiene $x = y$, dunque g^γ è iniettiva. Inoltre è suriettiva, perché per ogni $y \in G$ risulta

$$y = g^{-1}gyg^{-1}g = (gyg^{-1})^{g^\gamma}$$

Infine se $x, y \in G$ allora

$$(xy)^{g^\gamma} = g^{-1}xyg = g^{-1}xgg^{-1}yg = x^{g^\gamma}y^{g^\gamma}$$

cioè g^γ è un omomorfismo di gruppi.

Se $g \in G$, l'automorfismo g^γ definito nell'esempio precedente si dice **coniugio** per l'elemento g oppure **automorfismo interno** indotto da g.

Teorema 8.1.5 *Sia G un gruppo e $\gamma: G \to Aut(G)$ la funzione che a ciascun elemento g di G associa l'automorfismo (interno) g^γ di G. Allora γ è un omomorfismo di gruppi.*

DIMOSTRAZIONE. Dobbiamo mostrare che, per ogni $g, h \in G$,

$$g^\gamma h^\gamma = (gh)^\gamma,$$

ovvero che, per ogni $x \in G$,

$$x^{(g^\gamma h^\gamma)} = x^{(gh)^\gamma}.$$

Infatti

$$x^{(g^\gamma h^\gamma)} = (x^{g^\gamma})^{h^\gamma} = (g^{-1}xg)^{h^\gamma} = h^{-1}g^{-1}xgh = (gh)^{-1}xgh = x^{(gh)^\gamma}.$$

■

L'azione γ definita come nel Teorema 8.1.5 si dice **azione di G su se stesso per coniugio**. L'immagine G^γ di γ si dice **gruppo degli automorfismi interni** di G e si indica con $Inn(G)$. Il nucleo $\ker(\gamma)$ è il centro $Z(G)$ del gruppo G. Per il Primo Teorema di Omomorfismo risulta

$$Inn(G) \cong G/Z(G),$$

in particolare, se $Z(G) = \{1\}$, G è isomorfo ad un sottogruppo di $Aut(G)$.

Proposizione 8.1.6 $Inn(G) \trianglelefteq Aut(G)$

DIMOSTRAZIONE. Sia $g^\gamma \in Inn(G)$, con $g \in G$ e γ definita come nel Teorema 8.1.5, e sia $\alpha \in Aut(G)$. Mostriamo che $\alpha^{-1}g^\gamma\alpha = (g^\alpha)^\gamma$ e quindi è ancora un elemento di $Inn(G)$. Infatti, per ogni $x \in G$,

$$\begin{aligned} x^{(\alpha^{-1}g^\gamma\alpha)} &= (x^{\alpha^{-1}})^{g^\gamma\alpha} = (g^{-1}x^{\alpha^{-1}}g)^\alpha = (g^{-1})^\alpha (x^{\alpha^{-1}})^\alpha g^\alpha \\ &= (g^{-1})^\alpha x g^\alpha = x^{(g^\alpha)^\gamma}. \end{aligned}$$

■

Il gruppo quoziente $Aut(G)/Inn(G)$ si dice **gruppo degli automorfismi esterni** di G e si indica con $Out(G)$. Un gruppo si dice **completo** se $Z(G) = \{1\}$ e $Out(G) = \{1\}$. Se G è un gruppo semplice finito $Aut(G)$ è completo (Esercizio 8.3.16). Chiaramente, se G è un gruppo completo, G è isomorfo al suo gruppo di automorfismi. È interessante osservare l'analogia con un risultato simile sulle algebre di Lie ([18] Theorem 5.3 pag. 23) dove si prova che un'algebra di Lie semplice e di dimensione finita sui numeri complessi è isomorfa alla sua algebra delle derivazioni. A differenza delle algebre di Lie, però, un gruppo semplice finito G può avere automorfismi esterni, anche se $Out(G)$ è un gruppo risolubile e molto piccolo. Questo risultato è noto come la **Congettura di**

Schreier. L'unica dimostrazione che si conosca della Congettura di Schreier usa il Teorema di Classificazione dei Gruppi Semplici Finiti (CGSF). Sarebbe molto bello riuscire a dare una dimostrazione della Congettura di Schreier indipendente dalla CGSF. Tra i gruppi semplici finiti, i gruppi speciali lineari sono quelli che hanno gruppo degli automorfismi esterni più grande. Determineremo questo gruppo nella Sezione 11.6.5.

8.1.3 Azione per coniugio sulle sezioni normali

Sia G un gruppo e K ed N sottogruppi normali di G con $K \leq N$. Il gruppo quoziente N/K si dice **sezione normale** di G. Mostriamo ora come l'azione γ di G su se stesso per coniugio induce in modo naturale un'azione $\gamma_{N/K}$ su una sua sezione normale N/K di G.

Sia N/K una sezione normale di G e sia $g \in G$. Consideriamo l'applicazione

$$g^{\gamma_{N/K}}: N/K \to N/K$$

definita, per ogni $xK \in N/K$ (con $x \in N$), da

$$(xK)^{g^{\gamma_{N/K}}} = x^g K.$$

L'applicazione $g^{\gamma_{N/K}}$ è ben definita. Infatti, poichè $K \trianglelefteq G$, risulta

$$(xK)^{g^{\gamma_{N/K}}} = (xK)^g$$

e quindi non dipende dalla scelta del rappresentante x di xK. Inoltre, poiché $N \trianglelefteq G$ l'elemento x^g appartiene ancora a N e quindi $(xK)^{g^{\gamma_{N/K}}} = x^g K \in N/K$. Infine $g^{\gamma_{N/K}}$ è un automorfismo di N/K (la verifica è lasciata per esercizio). Come prima si vede facilmente che l'applicazione

$$\gamma_{N/K}: G \to Aut(N/K)$$

che ad ogni elemento g di G associa l'automorfismo $g^{\gamma_{N/K}}$ è un'azione di G sul gruppo N/K e si dice **azione di G su N/K per coniugio**. Il nucleo di questa azione si dice **centralizzante** di N/K in G e si indica con

$$C_G(N/K).$$

Riassumiamo

Proposizione 8.1.7 *Se N/K è una sezione normale di G allora $C_G(N/K)$ è un sottogruppo normale di G e $G/C_G(N/K)$ è isomorfo ad un sottogruppo di $Aut(N/K)$.*

8.1.4 Sottogruppi caratteristici

Dovrebbe essere a questo punto evidente quanto sia importante trovare sottogruppi normali N o, più in generale delle sezioni normali di G. Infatti questo

permette da un lato, come abbiamo visto nel primo capitolo, di ridurre la struttura di G in quella più semplice di G/N, N/K e K, dall'altro attiva il gruppo G che agisce per coniugio su N/K e quindi, modulo $C_G(N/K)$ si immerge in $Aut(N/K)$. Il problema diviene allora quello di trovare delle sezioni normali N/K che abbiano una struttura abbastanza semplice e di cui sia noto il gruppo degli automorfismi (come ad esempio i gruppi abeliani elementari, o i gruppi ciclici). La tentazione sarebbe quella di procedere per induzione, cioè, trovata una sezione normale N/K, se questa ha una struttura troppo complicata, passare alle sezioni normali di N/K e così via. Il difetto di questa strategia è che la normalità, come si è già osservato, non è una relazione transitiva e quindi non è detto che il sottogruppo che troviamo alla fine sia una sezione normale di tutto G. Questo ostacolo può essere aggirato considerando una relazione più forte della normalità che è quella di "*essere caratteristico in*" che ora definiamo.

Sia τ un automorfismo di un gruppo G e sia N un sottogruppo di G. N si dice τ-**invariante** se $N^\tau \leq N$. Un sottogruppo di G si dice **caratteristico** se è τ-invariante per ogni $\tau \in Aut(G)$. Per indicare che N è un sottogruppo caratteristico di G scriveremo $N <_{char} G$.

ESEMPI
Sia G un gruppo, allora

1. $Z(G) <_{char} G$;
2. $G' <_{char} G$;
3. l'intersezione $\Phi(G)$ di tutti i sottogruppi massimali di G è un sottogruppo caratteristico di G ($\Phi(G)$ si dice **sottogruppo di Frattini** di G);
4. i sottogruppi $\Omega_i(G) := \langle g \in G | g^{p^i} = 1 \rangle$ e $\mho_i(G) := \langle g^{p^i} | g \in G \rangle$ sono caratteristici in G.
5. Se G è abeliano e S è una componente primaria di G, allora S è caratteristico.

Osserviamo che un sottogruppo H di un gruppo G è normale se e solo se $H^g = H$ per ogni $g \in G$, cioè se e solo se $H^\sigma = H$ per ogni $\sigma \in Inn(G)$. Poiché $Inn(G) \leq Aut(G)$ ne segue che

Proposizione 8.1.8 *Un sottogruppo caratteristico è normale.*

Il viceversa in generale non è vero (vedi Esercizio 8.3.7).

Proposizione 8.1.9 *Siano K e H sottogruppi del gruppo G con $K \leq H$.*

1. *Se $K <_{char} H$ e $H <_{char} G$, allora $K <_{char} G$.*
2. *Se $K <_{char} H$ e $H \trianglelefteq G$, allora $K \trianglelefteq G$.*

DIMOSTRAZIONE. Dimostriamo il primo asserto, lasciando il secondo per esercizio. Supponiamo che $K <_{char} H$ e $H <_{char} G$. Sia $\sigma \in Aut(G)$. Allora $H^\sigma = H$ e quindi la restrizione $\sigma|_H$ di σ ad H è un automorfismo di H. Ne segue che $K^\sigma = K^{\sigma|_H} = K$ e quindi $K <_{char} G$. ■

Corollario 8.1.10 *Ogni termine della serie derivata di un gruppo è caratteristico*

Sia G un gruppo risolubile di lunghezza derivata k. Allora $A := G^{(k-1)}$ è un gruppo abeliano. Sia A_p una componente primaria non identica di A. Allora A_p è caratteristico in A e quindi anche in G. Sia ora $V := \Omega_1(A_p)$. Ovviamente $\{1\} \neq V$, inoltre risulta

$$V <_{char} A_p <_{char} A = G^{(k-1)} <_{char} G,$$

da cui segue che

$$V <_{char} G.$$

Abbiamo dimostrato il seguente

Corollario 8.1.11 *Se G è un gruppo risolubile, allora G possiede un sottogruppo caratteristico abeliano elementare non identico.*

La seguente proposizione è un supplemento al Teorema di Corrispondenza e descrive una situazione duale della Proposizione 8.1.9

Proposizione 8.1.12 *Sia K un sottogruppo caratteristico di un gruppo G e sia N un sottogruppo di G contenente K. Allora, se N/K è caratteristico in G/K, N è caratteristico in G.*

DIMOSTRAZIONE. Supponiamo che N/K sia caratteristico in G/K. Sia α un automorfismo di G. Allora si verifica facilmente che l'applicazione

$$\begin{array}{rcl} \overline{\alpha}: G/K & \to & G/K \\ gK & \mapsto & g^\alpha K \end{array}$$

è ben definita ed è un automorfismo di G/K. Poichè N/K è caratteristico in G/K risulta

$$N/K = (N/K)^{\overline{\alpha}} = N^\alpha/K$$

e quindi, per il Teorema di Corrispondenza $N = N^\alpha$ ■

Osserviamo che il viceversa non è vero infatti nel gruppo diedrale D_8 esiste un unico sottogruppo ciclico N di ordine 4 che è chiaramente caratteristico in D_8. Se $K = \Omega_1(N)$ allora K è caratteristico in D_8 ed il gruppo quoziente D_8/K è abeliano elementare e quindi i suoi unici sottogruppi caratteristici sono D_8/K e K/K (Esercizio 8.3.7), in particolare N/K non è caratteristico in D_8/K.

Corollario 8.1.13 *Se G è un gruppo finito risolubile, allora esiste una serie*

$$G_0 = G \geq G_1 \geq \ldots \geq G_k = \{1\}$$

di sottogruppi caratteristici di G tali che G_i/G_{i+1} è un gruppo abeliano elementare per ogni $i \in \{0, \ldots, k-1\}$

DIMOSTRAZIONE. Discende facilmente per induzione dal Corollario 8.1.11 e dalla Proposizione 8.1.12. ■

8.1.5 Prodotti semidiretti

Chiudiamo questo capitolo con un'utile applicazione delle azioni di gruppi sui gruppi: il prodotto semidiretto. Questa costruzione è una generalizzazione del prodotto diretto di due gruppi che ci permette

1. di classificare le estensioni spezzanti,
2. di costruire nuovi gruppi e, infine,
3. di trattare le azioni di un gruppo su un altro gruppo come se questa azione fosse il coniugio in un gruppo più grande che li contiene entrambi.

Sia G un gruppo ed N un suo sottogruppo normale. Ricordiamo che G è un'estensione spezzante di N se esiste un complemento K di N in G. In questa sezione mostreremo come sia possibile determinare la struttura di G dalla struttura di N, del suo complemento K e dall'azione indotta da K su N per coniugio.

Ad esempio nel caso particolare in cui gli elementi di K centralizzano N si vede facilmente che G è isomorfo al prodotto diretto di N per K via la mappa che manda la coppia (n, k) nell'elemento nk di G. Se K non centralizza N, è possibile generalizzare la costruzione del prodotto diretto di gruppi definendo un'operazione in $N \times K$ (che dipende dall'azione che K induce su N per coniugio) in modo che $N \times K$ con questa operazione risulti isomorfo a G.

Consideriamo dunque G un gruppo, non necessariamente finito, che sia un'estensione spezzante di un suo sottogruppo normale N e sia K un complemento di N. Allora $G = NK$ e quindi ogni elemento $g \in G$ si scrive come prodotto di un elemento di N per un elemento di K:

$$g = nk$$

(si osservi che poiché $N \cap K = \{1\}$ questa scrittura è unica, nel senso che se $nk = n'k'$, con n, n' in N e k, k' in K, allora $h = h'$ e $k = k'$). Sia ora g' un altro elemento di G allora esistono degli elementi $m \in N$ e $h \in K$ tali che

$$g' = mh.$$

Poiché $G(= NK)$ è chiuso rispetto al prodotto, anche gg' si scrive come prodotto di un elemento di N per un elemento di K. Infatti

$$gg' = nkmh = nkmk^{-1}kh = nm^{k^{-1}}kh \tag{8.1}$$

e, essendo $N \trianglelefteq G$, $nm^{k^{-1}}$ è un elemento di N. Si osservi che se N e K si centralizzano, allora $m^{k^{-1}} = m$ e $gg' = khnm$, cioè G è isomorfo al prodotto diretto di K e N.

L'uguaglianza (8.1) suggerisce come debba essere definita l'operazione che stiamo cercando. Siano infatti A e B due gruppi e sia $\rho\colon A \to Aut(B)$ un'azione di A su B. Definiamo nel prodotto diretto $B \times A$ un'operazione nel modo seguente:

$$(b, a) * (b', a') = (bb'^{(a^{-1})^{\rho}}, aa'). \tag{8.2}$$

Si verifica facilmente che $(B \times A)$ con l'operazione $*$ è un gruppo. Questo gruppo si chiama **prodotto semidiretto** di B con A via l'azione ρ e si indica con $B :^{\rho} A$ o semplicemente con $B : A$. Si osservi che, se ρ è la mappa che manda ogni elemento di A nell'automorfismo identico (cioè se l'azione di A su B è triviale), il prodotto semidiretto di B per A coincide con il prodotto diretto di gruppi. Si osservi che, a differenza del prodotto diretto, i ruoli dei due gruppi B ed A nel prodotto semidiretto sono distinti: A è *attivo* nel senso che *agisce* su B mentre B è *passivo*. Il seguente teorema caratterizza le estensioni spezzanti.

Teorema 8.1.14 *Sia G un'estensione spezzante di N, sia K un complemento di N in G e sia $\phi\colon K \to Aut(N)$ l'azione che K induce per coniugio su N. Allora G è isomorfo al prodotto semidiretto di N per K via ϕ.*

DIMOSTRAZIONE. Si consideri la mappa da $N :^{\phi} K$ in G che a (k, n) associa nk. Si vede facilmente che è un isomorfismo di gruppi. ∎

Un'altra importante applicazione dei prodotti semidiretti è che essi ci permettono di ridurre i problemi delle azioni di un gruppo su un gruppo all'azione indotta per coniugio. Sia infatti $\rho\colon A \to Aut(B)$ un'azione di un gruppo A su un gruppo B. Sia G il prodotto semidiretto di B per A via l'azione ρ, e siano

$$N := \{(b, 1) | b \in B\}$$

e

$$H := \{(1, a) | a \in A\}.$$

Ora N è isomorfo a B via l'applicazione ι_B che ad ogni $b \in B$ associa la coppia $(b, 1)$ e H è isomorfo ad A via l'applicazione ι_A che ad ogni $a \in A$ associa la coppia $(1, a)$. Inoltre $N \trianglelefteq G$, quindi $H \leq G = N_G(N)$ e l'azione ρ di A su B è equivalente all'azione indotta dal coniugio di H su N, cioè, per ogni $a \in A$ ed ogni $b \in B$, risulta:

$$(b^{(a^{\rho})})^{\iota_B} = (a, 1)^{-1}(1, b)(a, 1).$$

Useremo spesso questo fatto nel capitolo sulle azioni dei gruppi sui gruppi.

8.1.6 Gruppi diedrali

Come applicazione dei prodotti semidiretti classificheremo la seguente (importante) classe di gruppi.

Un gruppo **diedrale** è un gruppo generato da due involuzioni distinte. Sia G un gruppo generato da due involuzioni distinte r ed s e sia k l'ordine dell'elemento rs (dove $k \in \mathbf{N} \cup \{\infty\}$). Poiché r ed s sono involuzioni,

$$(rs)^r = (rs)^s = sr = (rs)^{-1}.$$

Da questo segue che $\langle rs \rangle$ è un sottogruppo normale di indice minore o uguale a 2 in G. Poiché G possiede due involuzioni distinte, G non è ciclico, quindi $|G : \langle rs \rangle| = 2$ e, se k è finito, $|G| = 2k$. Quindi G è l'estensione spezzante del gruppo $\langle rs \rangle$, che è ciclico di ordine k, con il gruppo $\langle r \rangle$ (o $\langle s \rangle$) che ha ordine 2 e r (o s) induce per coniugio su $\langle rs \rangle$ l'automorfismo che manda ogni elemento nel suo inverso. Il fatto che un gruppo diedrale sia estensione spezzante di un gruppo ciclico C con un gruppo di ordine 2 il cui generatore opera come l'inversione su C ci suggerisce un modo per costruire un gruppo diedrale di ordine infinito o di ordine $2k$ per ogni intero $k \geq 2$. Infatti se $\langle c \rangle$ è un gruppo ciclico di ordine k ($k \geq 2$) oppure di ordine infinito, ed α è l'automorfismo di $\langle c \rangle$ che manda ogni elemento nel suo inverso, allora, nel prodotto semidiretto $\overline{G}$ di $\langle c \rangle$ per $\langle \alpha \rangle$, gli elementi $(\alpha, 1)$ e (α, c) hanno ordine 2, generano $\overline{G}$ e $\overline{G}$ ha ordine infinito oppure $2k$ a seconda che l'ordine di c sia infinito o k.

Teorema 8.1.15 *1. Un gruppo è diedrale se e solo se è l'estensione spezzante di un sottogruppo ciclico C normale con un sottogruppo di ordine 2 e, per ogni $a \in G \setminus C$, a agisce su C per coniugio come l'automorfismo di C che inverte ogni elemento.*

2. A meno di isomorfismo, esiste un unico gruppo diedrale di ordine $2k$, per ogni intero k maggiore o uguale a 2, ed esiste un unico gruppo diedrale di ordine infinito;

Se k è un intero positivo, indicheremo con D_{2k} il gruppo diedrale di ordine $2k$ e con D_∞ il gruppo diedrale infinito.

Una conseguenza del Teorema 14.2.8 è che, in un gruppo semplice finito G, ogni sottogruppo generato da due involuzioni distinte è risolubile (in particolare è un sottogruppo proprio). Al contrario, come conseguenza del Teorema di Classificazione dei Gruppi Semplici Finiti, è stato dimostrato che, se p è un numero primo che divide l'ordine di G, la probabilità che due elementi distinti di ordine p generino tutto G tende a 1 al crescere dell'ordine di G. Questo, insieme al fatto che per il Teorema di Feit e Thompson ogni gruppo semplice finito non abeliano possiede involuzioni, è uno dei motivi per cui il primo 2 ha un ruolo privilegiato nella dimostrazione originale del Teorema di Classificazione e negli attuali progetti di revisione.

Più avanti daremo una costruzione geometrica dei gruppi diedrali come gruppi generati da due riflessioni di uno spazio euclideo.

8.2 Azione di un gruppo su un insieme

In questa sezione studieremo le rappresentazioni ρ di un gruppo G nel gruppo S_X delle permutazioni di un insieme X. Introdurremo a questo scopo la nozione di G-insieme. Il concetto di G-insieme può essere interpretato come una sorta di precursore di quello di spazio vettoriale su un campo K o, più in generale, di modulo destro su un anello R. Un modulo destro su un anello R è infatti una coppia (M, ρ), dove M è un gruppo abeliano e ρ è un omomorfismo di anelli da R nell'anello $End(M)$ degli endomorfismi di M (si osservi che, nel caso particolare in cui R sia un campo, (M, ρ) è esattamente uno spazio vettoriale su R). Analogamente un G-insieme è una coppia (X, ρ), dove X è un insieme e ρ, in questo caso, è una rappresentazione di G su X. Si osservi che, in particolare, uno spazio vettoriale su un campo K è anche un K^*-insieme dove K^* è il gruppo moltiplicativo di K. Per tradizione, nonostante siano una struttura più complessa, nei corsi di laurea gli spazi vettoriali vengono introdotti prima dei G-insiemi (mentre questi ultimi, a volte, non vengono neppure accennati). Tanto vale, quindi, approfittare della fatica fatta in algebra lineare e, come faremo, cercare di sviluppare la teoria dei G-insiemi in modo da evidenziare le analogie con gli spazi vettoriali o, più in generale, con la teoria dei moduli destri su un anello R. In particolare, come R stesso può essere visto come modulo destro su se stesso per moltiplicazione a destra (o un campo come spazio vettoriale di dimensione 1 su se stesso), così un gruppo G ha una struttura naturale di G-insieme via l'azione regolare a destra δ: il G-insieme (G, δ) si dice **G-insieme regolare destro**. Definiremo i G-sottoinsiemi, gli omomorfismi ed i quozienti di G insiemi e proveremo che i quozienti del G-insieme regolare a destra sono tutti e soli gli insiemi delle classi laterali destre di G modulo un suo sottogruppo. Vedremo che ogni G-insieme si decompone come unione disgiunta di G-orbite, cioè di G-sottoinsiemi minimali non vuoti e, analogamente a quanto accade per i sottomoduli ciclici, ogni G-orbita è isomorfa ad un quoziente del G-insieme regolare a destra. Questo è il risultato più importante di tutto il capitolo. Lo useremo in seguito per provare la nilpotenza dei p-gruppi, il Teorema di Sylow ed il Teorema di Schur-Zassenhaus. Negli spazi vettoriali, uno spazio vettoriale di dimensione 1 non ha quozienti propri, ma, in generale, un modulo destro ciclico su un anello R può avere quozienti propri. Così una G-orbita può avere quozienti propri. Un G-insieme privo di quozienti propri si dice **primitivo**, questi sono gli elementi semplici della teoria dei G-insiemi. Proveremo che se X è un G-insieme primitivo, allora X è isomorfo all'insieme delle classi laterali destre di G modulo un sottogruppo massimale.

8.2.1 G-insiemi

Per tutto il resto di questa sezione G è un gruppo, X un insieme e $\rho: G \to S_X$ un'azione di G su X. Chiameremo la coppia (X, ρ) un **G-insieme**. Come al solito, quando non sarà necessario specificare l'azione ρ, identificheremo il G-insieme (X, ρ) con il suo supporto X. In questo caso inoltre, se $x \in X$ e $g \in G$,

scriveremo semplicemente x^g al posto di $x^{\rho(g)}$. Se δ è l'azione regolare a destra di G sul suo supporto, il G-insieme (G, δ) si dice **G-insieme regolare destro**

8.2.2 G-sottoinsiemi e orbite

Un **G-sottoinsieme** di X (o un sottoinsieme **G-invariante**) è un sottoinsieme Y di X tale che per ogni $y \in Y$ ed ogni $g \in G$ risulti $y^g \in Y$. In questo caso diremo che G **agisce su** Y perché, come si vede facilmente, l'applicazione che ad ogni $g \in G$ associa la mappa $g^\rho|_Y$ è un'azione di G su Y. Per comodità, continueremo a chiamare ρ questa nuova azione.

Esempi

1. Se $X = G$ e ρ è l'azione di G per coniugio, allora i sottogruppi che sono sottoinsiemi G-invarianti sono esattamente i sottogruppi normali.

2. Se $X = G$ e ρ è l'azione di G su se stesso per moltiplicazione a destra, allora G è l'unico sottoinsieme G-invariante non vuoto di G.

3. Se V è uno spazio vettoriale su un campo K e K^* è il gruppo moltiplicativo degli elementi non nulli di K, allora V è un K^* insieme rispetto al prodotto usuale per scalari. I K^*-sottoinsiemi di V sono i sottoinsiemi chiusi per il prodotto per scalari non nulli. I sottospazi di V sono i K^*-sottoinsiemi di V che sono anche sottogruppi di $(V, +)$.

Si vede facilmente che l'unione e l'intersezione di G-sottoinsiemi sono ancora G-sottoinsiemi, cioè i G-sottoinsiemi di X formano un sottoreticolo del reticolo delle parti di X ordinato per inclusione. Gli elementi minimali di questo sottoreticolo si dicono **G-orbite**. Le proprietà fondamentali delle G-orbite sono riassunte nella seguente proposizione (la dimostrazione è lasciata per esercizio).

Proposizione 8.2.1 *Sia G un gruppo ed X un G-insieme.*

1. *Le G-orbite di X sono tutti e soli i sottoinsiemi del tipo*

$$x^G = \{x^g | g \in G\}$$

   al variare di x in X.

2. *Per ogni $x, y \in X$, $x^G = y^G$ se e solo se $y \in x^G$.*

3. *Le G-orbite di X formano una partizione di X ed ogni G-sottoinsieme è unione (disgiunta) di G-orbite.*

Se O è una G-orbita e $x \in O$, diremo che O è la **G-orbita di x**.

8.2.3 G-omomorfismi

Se (Y, σ) è un altro G-insieme, un **G-omomorfismo** (o **omomorfismo di G-insiemi**) tra X e Y è un'applicazione

$$\phi: X \to Y$$

tale che, per ogni $g \in G$ ed ogni $x \in X$, risulti

$$\phi(x^g) = (\phi(x))^g$$

(o, più precisamente $\phi(x^{g^\rho}) = (\phi(x))^{g^\sigma}$). Si osservi che questa condizione corrisponde, per gli spazi vettoriali, alla compatibilità delle applicazioni lineari con il prodotto per scalari. Come al solito i G-omomorfismi iniettivi, suriettivi e biiettivi si dicono rispettivamente **G-monomorfismi**, **G-epimorfismi** e **G-isomorfismi**. X e Y si dicono **G-isomorfi** se esiste un G-isomorfismo tra X e Y.

8.2.4 Quozienti di G-insiemi e Primo Teorema di Omomorfismo per G-insiemi

Nella Sottosezione1.1.5 abbiamo visto che, se N è un sottogruppo normale di G, la relazione $\sim_N$, definita, per ogni a e b in G, da $a \sim_n b$ se e solo se $ab^{-1} \in N$ è una congruenza su G. Se N non è normale, la relazione $\sim_N$ non è compatibile con l'operazione di G, ma è ancora un'equivalenza ed è compatibile con l'azione regolare a destra di G su se stesso. In questo caso, l'insieme quoziente $G/\sim_N$, non eredita da G la struttura di gruppo, ma solo quella di G-insieme dal G insieme regolare a destra.

In questa sottosezione introduciamo un'altra costruzione fondamentale per i G-insiemi, quella del quoziente di G-insiemi, e le nozioni di G-congruenza e G-partizione ad essa collegate.

Sia (X, ρ) un G-insieme, dove G è un gruppo e $\rho: G \to S_X$ è un'azione di G su X.

Una relazione d'equivalenza $\sim$ su X si dice **compatibile con l'azione di G** o **G-congruenza** se per ogni $x, y \in X$ ed ogni $g \in G$, risulta

$$x \sim y \iff x^{\rho(g)} \sim y^{\rho(g)}.$$

Si vede facilmente che le G-congruenze sono tutte e sole le equivalenze associate agli omomorfismi di G-insiemi, inoltre, se $\sim$ è una G-congruenza, per ogni $x \in X$, e per ogni $g \in G$,

$$[x]_\sim = [x^g]_\sim \text{ oppure } [x]_\sim \cap [x^g]_\sim = \emptyset.$$

Diremo che una partizione $\mathcal{P}$ di X è **compatibile con l'azione di G** o **G-partizione**, se $\mathcal{P}$ è associata ad una G-congruenza. Per quanto appena visto, $\mathcal{P}$ è una G-partizione se e solo se per ogni $\Delta \in \mathcal{P}$ e per ogni $g \in G$ risulta

$$\Delta^g \in \mathcal{P}. \tag{8.3}$$

La relazione precedente mostra che se $\mathcal{P}$ è una G-partizione, l'azione ρ di G su X induce in modo naturale un'azione, che per il momento chiamiamo $\rho_{\mathcal{P}}$, di G su $\mathcal{P}$ definita, appunto, come segue:

$$(\Delta)^{\rho_{\mathcal{P}}(g)} := \Delta^g.$$

In particolare, se $\mathcal{P}$ è l'insieme quoziente $X/\sim$ modulo la G-congruenza $\sim$, il G-insieme $(X/\sim, \rho_{X/\sim})$ si dice **G-insieme quoziente di X modulo $\sim$**.

Osserviamo che $\{X\}$ e $\{\{x\}|x \in X\}$ sono due G-partizioni di G e si dicono G-partizioni **banali**. Se X non ha altre G-partizioni diremo che l'azione di G su X è **primitiva** (G è **primitivo su** X, oppure X è un G-insieme **primitivo**).

Teorema 8.2.2 *(Primo Teorema di Omomorfismo per G-insiemi) Sia G un gruppo, X ed Y due G-insiemi e $f: X \to Y$ un omomorfismo di G-insiemi. Sia $\sim$ la relazione d'equivalenza associata a f e sia π la proiezione canonica di X sul G-insieme quoziente $X/\sim$. Allora esiste un'unica applicazione $\bar{f}: X/\sim \to Y$ tale che, per ogni $x \in X$, sia*

$$f(x) = \bar{f}(\pi(x)). \tag{8.4}$$

Inoltre $\bar{f}$ è un monomorfismo di G-insiemi ed è suriettivo se e solo se f lo è.

DIMOSTRAZIONE. Il Primo Teorema di Omomorfismo per insiemi prova che esiste un'unica applicazione $\bar{f}$ che soddisfa la (8.4) e tale applicazione è (ben) definita ponendo

$$\bar{f}([x]_\sim) = f(x)$$

per ogni $[x]_\sim \in X/\sim$. Inoltre $\bar{f}$ è iniettiva ed è anche suriettiva se e solo se f lo è. Resta quindi solo da dimostrare che $\bar{f}$ è un omomorfismo di G-insiemi. Sia dunque $g \in G$ e $[x]_\sim \in X/\sim$. Allora

$$\bar{f}([x]_\sim^g) = \bar{f}([x^g]_\sim) = f(x^g) = f(x)^g = (\bar{f}([x]_\sim)^g.$$

■

Nella prossima sezione proveremo che ogni G-orbita di un G-insieme X è isomorfa ad un quoziente del G-insieme regolare a destra. Chiudiamo questa sezione determinando tutti i quozienti del G-insieme regolare a destra.

Proposizione 8.2.3 *Sia $\mathcal{P}$ una G-partizione del G-insieme regolare a destra. Sia $Y \in \mathcal{P}$ con $1 \in Y$. Allora Y è un sottogruppo di G e $\mathcal{P} = G/Y$.*

DIMOSTRAZIONE. Per ogni $y \in Y$, poiché $y = 1y = 1^{\delta(y)}$ e $1 \in Y$, risulta $y \in Y \cap Y^{\delta(y)}$. Poiché $Y \in \mathcal{P}$ e $\mathcal{P}$ è una G-partizione, segue che $Y = Y^{\delta(y)}$ e quindi Y è un sottogruppo per l'Esercizio 8.3.20. Ne segue che $G/Y = \{Y^{\delta(g)}|g \in G\} \subseteq \mathcal{P}$. D'altra parte anche G/Y è una partizione di G, e quindi $G/Y = \mathcal{P}$.
■

8.2.5 Stabilizzatori puntuali e globali

Sia x un elemento di X, l'insieme degli elementi g di G tali che $x^g = x$, (cioè che lasciano *fisso* l'elemento x) si dice **stabilizzatore** o **centralizzante di un elemento** in G di x e si indica con $St_G(x)$, o con $C_G(x)$ o, più semplicemente con con G_x. Se Y è un sottoinsieme di X, indicheremo con G_Y lo **stabilizzatore globale** del sottoinsieme Y cioè:

$$G_Y := \{g \in G | y^g \in Y \text{ e } y^{g^{-1}} \in Y \text{ per ogni } y \in Y\}.$$

Si osservi che G_Y è esattamente lo stabilizzatore di Y come elemento di $\mathcal{P}(X)$nell'azione indotta di G su $\mathcal{P}(X)$. Infine indichiamo con $C_G(Y)$, oppure con $G_{[Y]}$, lo **stabilizzatore puntuale** o **centralizzante** di Y, cioè

$$G_{[Y]} := \{g \in G | y^g = y \text{ per ogni } y \in Y\}.$$

Proposizione 8.2.4 *Sia X un G-insieme, $x \in X$ e $Y \subseteq X$. Allora*

1. *G_x, G_Y e $G_{[Y]}$ sono sottogruppi di G;*
2. *$G_{[Y]} \leq G_Y$.*

DIMOSTRAZIONE. Esercizio 8.3.28. ∎

8.2.6 Punti fissi

Sia g un elemento di G, indichiamo con X_g l'insieme dei **punti fissi** di g, cioè:

$$X_g = \{x \in X | x^g = x\}.$$

Similmente, se H è un sottogruppo di G, indichiamo con $C_X(H)$ o con X_H l'insieme degli elementi di X che sono punti fissi per ogni elemento di H, cioè:

$$X_H = \{x \in X | x^h = x \text{ per ogni } h \in H\}.$$

X_H si dice anche **centralizzante** di H in X. Si noti la differenza con il centralizzante di un sottoinsieme di X definito nel paragrafo precedente: mentre G_Y è un sottogruppo di G, cioè l'oggetto che *agisce* su X, X_H è un sottoinsieme di X, cioè l'oggetto che *subisce* l'azione di G. Abbiamo scelto la medesima notazione (ed il medesimo nome) per i due centralizzanti per due motivi: uno è che nell'azione di un gruppo su se stesso per coniugio, queste due definizioni coincidono; l'altro motivo è per sottolineare la simmetria dei loro ruoli nella corrispondenza, tra i sottogruppi di G ed i sottoinsiemi di X, che a ciascun sottogruppo associa l'insieme dei suoi punti fissi e a ciascun sottoinsieme di X associa il suo centralizzante in G. Questa corrispondenza è alla base della Teoria di Galois (e non solo). Si osservi che, in generale, questa corrispondenza non è biunivoca. Nella proposizione che segue sono riassunti i risultati elementari di questa corrispondenza.

Proposizione 8.2.5 (Corrispondenza di Galois) *Sia G un gruppo che agisce su un insieme X. Sia $\mathcal{L}(G)$ il reticolo dei sottogruppi di G e $\mathcal{P}(X)$ l'insieme delle parti di X. Allora, per ogni H, K in $\mathcal{L}(G)$ e per ogni Y, Z in $\mathcal{P}(X)$,*

1. *se $H \geq K$ allora $X_H \subseteq X_K$;*
2. *se $Y \subseteq Z$ allora $G_{[Y]} \geq G_{[Z]}$;*
3. *$H \leq G_{X_H}$ e $X_{G_Y} \subseteq Y$;*
4. *$X_H = X_{G_{[X_H]}}$ e $G_{[Y]} = G_{[X_{G_{[Y]}}]}$;*
5. *Se Y è G-invariante, allora $G_Y \trianglelefteq G$;*
6. *Se H è un sottogruppo normale di G, allora X_H è G-invariante.*

Dimostrazione. Esercizio 8.3.29 ■

8.2.7 Orbite e stabilizzatori

Il seguente teorema è il risultato principale di questa sezione, ogni G-insieme X su cui G è transitivo è G-isomorfo al G-insieme $(G/G_x, \delta)$, dove x è un qualsiasi elemento di X δ è l'azione indotta da G per moltiplicazione a destra sull'insieme delle classi laterali destre di G_x in G. Negli Esercizi 8.3.33 e 8.3.34 mostreremo come questa strategia possa essere utilizzata.

Teorema 8.2.6 *Sia G un gruppo, X un G-insieme, O_x la G-orbita dell'elemento x di X,*

$$\phi\colon G \to O_x$$

l'applicazione definita da

$$\phi(g) = x^g$$

per ogni $g \in G$ e $\sim_\phi$ l'equivalenza associata a ϕ. Allora

1. *ϕ è un omomorfismo tra il G-insieme regolare a destra e O_x;*
2. *$[1]_{\sim_\phi} = G_x$;*
3. *ϕ induce un isomorfismo di G-insiemi $\bar{\phi}$ tra G/G_x e O_x.*

Dimostrazione. Per ogni $h \in G$, risulta

$$\phi(g^{\delta(h)}) = \phi(gh) = x^{gh} = (x^g)^h = (\phi(g))^h,$$

il che prova che ϕ è un omomorfismo di G-insiemi ed è chiaramente suriettivo. Il punto 2 segue dal fatto che $g \in [1]_{\sim_\phi}$ se e solo se

$$x^g = \phi(g) = \phi(1) = x^1 = x,$$

cioè se e solo se $g \in G_x$. Infine il punto 3 segue dal punto 2 e dalla Proposizione 8.2.3 ■

Il numero degli elementi di una G-orbita si dice **lunghezza** dell'orbita. Il numero delle classi laterali di un sottogruppo in un gruppo è l'indice di questo sottogruppo. Il Teorema 8.2.6 ha il seguente importante corollario.

Corollario 8.2.7 *Se G è finito e con le ipotesi del teorema precedente, la lunghezza dell'orbita dell'elemento x è uguale all'indice dello stabilizzatore di x in G.*

Questo risultato è dovuto a Lagrange ([26] pag. 84). Si osservi che quello che è comunemente noto come il Teorema di Lagrange (Teorema 1.1.4) altro non è che un caso particolare del Corollario 8.2.7 (Esercizio 8.3.32).

Val la pena impararsi a memoria l'enunciato di questo corollario, come se fosse una formula magica.

8.2.8 L'equazione delle orbite

Sia G un gruppo, X un G-insieme finito. Siano $O_{x_1}, \ldots, O_{x_n}$ le G-orbite distinte di X ($x_i \in X$ per ogni $i \in \{1, \ldots n\}$). Nel paragrafo precedente abbiamo mostrato che X è l'unione disgiunta di $O_{x_1}, \ldots, O_{x_n}$ e quindi

$$|X| = \sum_{i=1}^{n} |O_{x_i}|. \tag{8.5}$$

Un elemento x di X tale che per ogni $g \in G$ sia $x^g = x$ si dice **punto fisso** sotto l'azione di G. Chiaramente x è un punto fisso se e solo se $O_x = \{x\}$. Supponiamo che X abbia l punti fissi (ovviamente $l \in \{1, \ldots n\}$). Ora, a meno di riordinare gli indici, possiamo supporre che questi siano $x_1, \ldots, x_l$. Il secondo membro dell'equazione (8.5) può essere quindi scomposto nel modo seguente:

$$\sum_{i=1}^{n} |O_{x_i}| = \sum_{i=1}^{l} |O_{x_i}| + \sum_{i=l+1}^{n} |O_{x_i}|.$$

Per ogni $i \leq l$ $G_{x_i} = G$ e quindi la prima sommatoria del secondo termine è uguale a l.

L'equazione (8.5) diviene

$$|X| = l + \sum_{i=l+1}^{n} |O_{x_i}| \tag{8.6}$$

dove, ripetiamo, l è il numero dei punti fissi di X e $|O_{x_i}| > 1$ per ogni $i \in \{l, \ldots, n\}$. Per il Corollario 8.2.7 $|O_{x_i}| = |G : G_{x_i}|$ e quindi la (equazione.delle.classi.1) diviene

$$|X| = \sum_{i=1}^{n} |G : G_{x_i}| \tag{8.7}$$

e la 8.6 diviene

$$|X| = l + \sum_{i=l+1}^{n} |G : G_{x_i}|. \tag{8.8}$$

L'equazione (8.8) viene detta **Equazione delle Orbite**. Essa assume un significato particolare nel caso di gruppi di ordine potenza di un primo. Infatti per il Teorema di Lagrange $|G : G_{x_i}|$ divide $|G|$. Supponiamo ora che G abbia ordine p^k per un numero primo p ed un intero positivo k. Allora, per ogni $i \in \{l, \ldots, n\}$ p divide $|G : G_{x_i}|$. In particolare se p non divide $|X|$, allora $l > 0$ e X ha punti fissi. Abbiamo dimostrato il seguente risultato:

Proposizione 8.2.8 *Sia p un numero primo, k un intero positivo. Se G è un gruppo di ordine p^k che opera su un insieme X di ordine coprimo con p, allora X ha punti fissi.*

Corollario 8.2.9 *Sia p un numero primo e siano G e P gruppi di ordine p^k e p^t rispettivamente. Sia ρ un'azione di G su P e supponiamo che l'immagine di ρ sia contenuta in $Aut(P)$. Allora P contiene punti fissi diversi da* 1.

DIMOSTRAZIONE. Poiché, per ogni $g \in G$, $\rho(g)$ è un automorfismo di P, l'identità di P è un punto fisso per l'azione di G. Ma allora $P \setminus \{1\}$ è G-invariante ed il suo ordine è coprimo con p, da cui segue la tesi per la proposizione precedente. ∎

8.2.9 Azioni transitive e primitive

Sia X un G-insieme e supponiamo che per ogni $x, y \in X$ esista un elemento $g \in G$ tale che $x^g = y$. In questo caso $X = O_x$ per ogni $x \in X$. Una tale azione si dice **transitiva** e diremo che G opera **transitivamente** (o che G è **transitivo**) su X . Per il Teorema 8.2.6 X è G-isomorfo all'insieme delle classi laterali di G_x in G dove x è un qualsiasi elemento di X. D'altra parte, se $H \leq G$ l'azione di G su G/H per moltiplicazione a destra è ovviamente transitiva. Abbiamo mostrato il seguente risultato:

Proposizione 8.2.10 *I G-insiemi su cui il gruppo G opera transitivamente sono tutti e soli quelli G-isomorfi ad insiemi del tipo G/H con $H \leq G$ ove l'azione di G è quella indotta per moltiplicazione a destra.*

La transitività si eredita ai quozienti, infatti

Proposizione 8.2.11 *Sia G un gruppo ed X un G-insieme. Se G è transitivo su X, allora G è transitivo su ogni G-insieme quoziente di X.*

DIMOSTRAZIONE. Sia $\mathcal{P}$ una G-partizione di X e $\Delta_1, \Delta_2 \in \mathcal{P}$. Per $i \in \{1, 2\}$, sia

$$x_i \in \Delta_i \in \mathcal{P}.$$

Poichè G è transitivo su X, esiste un elemento g di G tale che $x_1^g = x_2$. Ne segue che

$$x_2 \in \Delta_1^g \cap \Delta_2$$

e quindi $\Delta_1^g = \Delta_2$

■

Sia G un gruppo ed X un G-insieme. Osserviamo che l'insieme delle G-orbite di X è una G-partizione di G, quindi

Lemma 8.2.12 *Sia ρ un'azione del gruppo G sull'insieme X. Se ρ è primitiva allora è transitiva.*

Sia $\mathcal{P}$ una G-partizione di X. Osserviamo che, dalla (8.3), segue che per ogni $\Delta \in \mathcal{P}$ e per ogni $g \in G$

$$\Delta^g = \Delta \text{ oppure } \Delta^g \cap \Delta = \emptyset. \tag{8.9}$$

In particolare da questo si ottiene che

Proposizione 8.2.13 *Se X è un G-insieme e $\mathcal{P}$ è una G-partizione allora, per ogni $\Delta \in \mathcal{P}$ ed ogni $x \in \Delta$, risulta*

$$G_x \leq G_\Delta.$$

In generale un sottoinsieme proprio Δ del G-insieme X che contenga almeno due elementi e che verifichi la condizione (8.9) di dice *dominio d'imprimitività* di X. La (8.9) mostra che se G non è primitivo allora esiste un dominio d'imprimitività in X. Viceversa, sia Δ un dominio d'imprimitività e $Y := \bigcap_{g\in G}(X \setminus \Delta^g)$. Allora $\{\Delta^g | g \in G\} \cup \{Y\}$ è una G-partizione non banale di G; dunque

Proposizione 8.2.14 *Sia G un gruppo ed X un G-insieme. G è primitivo su X se e solo se X non possiede domini d'imprimitività.*

Osserviamo inoltre che se G è transitivo ma non primitivo su X e Δ è un dominio d'imprimitività allora, dalla Proposizione 8.2.11, segue che $\{\Delta^g | g \in G\}$ è una G-partizione di X.

Dalla Proposizione 8.2.12 segue che le azioni primitive non banali sono transitive. Supponiamo che G sia un gruppo transitivo su X. Per il Teorema 8.2.6 l'azione di G su X è equivalente all'azione di Cayley di G sulle classi laterali dello stabilizzatore G_x di un (qualsiasi) elemento x di X. Osserviamo che, se $\mathcal{P}$ è una G-partizione di G, allora, per la Proposizione 8.2.11, G è transitivo su $\mathcal{P}$ e, per la Proposizione 8.2.13, se $x \in \Delta \in \mathcal{P}$ risulta $G_x \leq G_\Delta \leq G$. In particolare se G_x è un sottogruppo massimale di G allora G_Δ coincide con G_x oppure con G. Nel primo caso, dal Teorema 8.2.6 si ottiene che, come G-insiemi,

$$X \cong G/G_x \cong G/G_\Delta \cong \mathcal{P},$$

quindi

$$|X| = |G/G_x| = |G/G_\Delta| = |\mathcal{P}|,$$

da cui si ottiene che $\mathcal{P} = \{\{x\}|x \in X\}$. Nel secondo caso

$$G/G = G/G_\Delta \cong \mathcal{P}$$

e quindi $1 = |G/G| = |\mathcal{P}|$ da cui si ottiene $\mathcal{P} = X$. Dunque se G è transitivo su X e G_x è massimale ($x \in X$), allora G è primitivo. Viceversa supponiamo G sia transitivo su X e che G_x non sia massimale in G. Per il Teorema 8.2.6 l'azione di G su X è equivalente all'azione di Cayley a destra di G su G/G_x; basta quindi provare che quest'ultima azione non è primitiva. Sia $G_x < H < G$ e sia $\Delta = \{Gh|h \in H\}$. Si vede immediatamente che Δ è un dominio d'imprimitività di G/G_x da cui segue che l'azione di Cayley a destra di G su G/G_x non è primitiva. Questo prova

Teorema 8.2.15 *Sia G un gruppo transitivo su un insieme X e $x \in X$. G è primitivo su X se e solo se G_x è un sottogruppo massimale di G.*

8.2.10 Decomposizione di un'azione

Questo capitolo è dedicato alla decomposizione di un'azione. Sia G un gruppo, (X, ρ, G) un G-insieme ed Y un sottoinsieme G-invariante di X. Chiaramente l'azione ρ di G su X induce per restrizione un'azione ρ_Y su Y. Poichè Y è G-invariante, anche $X \setminus Y$ è G invariante, quindi ρ induce per restrizione anche un'azione $\rho_{X\setminus Y}$ di G su $X\setminus Y$. Nella prima sezione di questo capitolo mostreremo (Teorema 8.2.16) come si può controllare ρ attraverso le azioni ρ_Y e $\rho_{X\setminus Y}$. In questo modo possiamo ridurci a considerare le azioni transitive.

Sia quindi (X, ρ) un G-insieme e G transitivo e supponiamo che $\sim$ sia una G-congruenza non banale su X. Sia

1. $x \in X$,
2. $\Delta = [x]_\sim$,
3. W l'insieme quoziente $X/\sim$,
4. ρ_W l'azione di G su W indotta da ρ,
5. H lo stabilizzatore G_Δ in G di Δ sotto l'azione ρ_W,
6. ρ_Δ l'azione di H su Δ indotta dalla restrizione di ρ ad H.

Analogamente a quanto fatto per le azioni non transitive, vogliamo controllare ρ attraverso le azioni ρ_W di G su W e ρ_Δ di H su Δ.

Poiché G è transitivo, se $x \in X$ e $U = G_x$, possiamo supporre, per il teorema 8.2.6, che

1. $x = U$,
2. $X = G/U$ e

3. ρ sia l'azione di Cayley a destra di G su G/U.

Inoltre, se scegliamo $x \in \Delta$, allora

1. $U \leq H = G_\Delta$,
2. $\Delta = H/U = \{Uh | h \in H\}$ e
3. $W = \{(H/U)g | g \in G\} = \{\{(Uh)g | h \in H\} | g \in G\}$.

Ora la corrispondenza che ad ogni $(H/U)g \in W$ associa la classe laterale Hg di H in G è, come si verifica facilmente, un ben definito isomorfismo di G-insiemi tra (W, ρ_W) e $(G/H, \rho_{G/H})$, dove $\rho_{G/H}$ è l'azione di Cayley a destra di G su G/H.

Ci siamo ridotti quindi a controllare l'azione di Cayley a destra ρ di G su G/U attraverso le azioni $\bar{\rho}_{G/H}$ di G su G/H e $\rho_{H/U}$ di H su H/U.

A questo scopo introdurremo due strumenti, utili anche indipendentemente da questo contesto: il prodotto semidiretto, ed il prodotto intrecciato.

Fissata un'azione ϕ di un gruppo K su un gruppo N, il prodotto semidiretto di N con K via ϕ è un'estensione spezzante di N con K e, viceversa, ogni estensione spezzante di N con K è isomorfa ad un prodotto semidiretto di N per un gruppo K via l'azione che K induce su N per coniugio.

Se A è un gruppo, (Y, ρ_Y) un A-insieme e B è un altro gruppo, l'insieme B^Y delle applicazioni da Y in B con la somma puntuale (esercizio 1.2.1) è un gruppo. A partire dall'azione ρ di A su Y definiremo una rappresentazione ρ_Y^* di A sul gruppo B^Y. Il prodotto intrecciato $A \wr_{\rho_Y} B$ di B con A via ρ_Y è prodotto semidiretto di B^Y con A via ρ_Y^*. Se (Z, ρ_Z) un B-insieme si può definire un'azione $\rho_Y \wr \rho_Z$ del prodotto intrecciato $A \wr_{\rho_Y} B$ sul prodotto cartesiano $Y \times Z$.

Torniamo ora al gruppo G. Proveremo che esiste un omomorfismo di gruppi σ di G nel prodotto intrecciato $\bar{G} \wr_{\bar{\rho}_{G/H}} H$ ed una biiezione

$$\psi \colon G/U \to G/H \times H/U$$

che sia un isomorfismo tra i G-insiemi $(G/U, \rho)$ e $(G/H \times H/U, \sigma(\bar{\rho}_{G/H} \wr \rho_{H/U}))$. Per definire σ e ψ è conveniente studiare, al posto dell'azione $\rho_{G/H}$, l'azione equivalente indotta da $\rho_{G/H}$ su un sistema di rappresentanti T delle classi laterali destre di H in G.

Le tecniche di decomposizione introdotte in questo capitolo permettono, in linea di principio, di ridurre un problema sulle azioni di gruppo al caso delle azioni primitive. I gruppi di permutazione primitivi sono classificati dal Teorema di O'Nan-Scott che, a sua volta, dipende dal Teorema di Classificazione dei Gruppi Semplici Finiti.

8.2.11 Decomposizione di un'azione non transitiva

Teorema 8.2.16 *Sia G un gruppo, (X, ρ, G) un G insieme ed Y un sottoinsieme G-invariante di X. Allora $X \setminus Y$ è G-invariante e l'applicazione*

$$\begin{aligned}\tau\colon G/\ker(\rho) &\to G/\ker(\rho_Y) \times G/\ker(\rho_{X\setminus Y})\\ \ker(\rho)g &\mapsto (\ker(\rho_Y)g, \ker(\rho_X)g)\end{aligned}$$

è ben definita ed è un monomorfismo di gruppi.

DIMOSTRAZIONE. Siano $g, h \in G$ tali che $\ker(\rho)g = \ker(\rho)h$. Allora $gh^{-1} \in \ker(\rho)$. Poichè $\ker(\rho_Y) \cap \ker(\rho_{X\setminus Y}) = \ker(\rho)$, segue che $gh^{-1} \in \ker(\rho_Y) \cap \ker(\rho_{X\setminus Y})$ e quindi $\ker(\rho_Y)g = \ker(\rho_Y)h$ e $\ker(\rho_{X\setminus Y})g = \ker(\rho_{X\setminus Y})h$, cioè τ è ben definita. Si vede facilmente che τ è un omomorfismo di gruppi. Sia ora $\ker(\rho)g \in \ker(\tau)$ allora g induce l'identità su Y e su $X \setminus Y$ e quindi su tutto X. Ne segue che $g \in \ker(\rho)$ e quindi $\ker(\tau) = \{1\}$, cioè τ è iniettiva. ∎

Si osservi che in generale τ non è suriettiva. Infatti sia $X = \{1, 2, 3, 4\}$, G il sottogruppo di S_4 generato dall'elemento $(1, 2)(3, 4)$ e ρ l'immersione di G in S_4. Allora $Y := \{1, 2\}$ è un sottoinsieme G-invariante di X, e $(1, 2)(3, 4)$ induce lo scambio $(1, 2)$ su Y e lo scambio $(3, 4)$ su $X \setminus Y$, cioè

$$\rho_Y((1, 2)(3, 4)) = (1, 2) \text{ e } \rho_{X\setminus Y}((1, 2)(3, 4)) = (3, 4).$$

Ne segue che

$$\begin{aligned}\tau(G) &= \tau\langle(1, 2)(3, 4)\rangle = \langle((1, 2), (3, 4))\rangle < \langle((1, 2), 1), (1, (3, 4))\rangle\\ &= G/\ker(\rho_Y) \times G/\ker(\rho_{X\setminus Y}).\end{aligned}$$

8.2.12 Azione trasposta e prodotti intrecciati

Vediamo ora un tipo particolare di prodotto semidiretto. Sia T un insieme, H un gruppo ed H^T l'insieme delle applicazioni da T in H. Ricordiamo che (esercizio 1.2.1) se $f_1, f_2 \in H^T$, il prodotto puntuale di f_1 e f_2 è l'applicazione

$$f_1 \cdot f_2\colon T \to H$$

definita, per ogni $t \in T$, da

$$(f_1 \cdot f_2)(t) = (f_1(t))(f_2(t))$$

e H^T con il prodotto puntuale è un gruppo.

Sia ora ϕ una permutazione dell'insieme T e, per ogni $f \in H^T$, sia f^{ϕ^*} l'applicazione di H^T definita, per ogni $t \in T$ da

$$f^{\phi^*}(t) = f(t^{(\phi^{-1})}) \tag{8.10}$$

Si verifica facilmente che l'applicazione

$$\begin{aligned}\phi^*\colon\ H^T &\to H^T\\ f &\mapsto f^{\phi^*}\end{aligned}$$

è un automorfismo di H^T. Chiameremo ϕ^* **applicazione trasposta** dell'azione f.

In particolare se G un gruppo e (T, ρ) è un G-insieme, allora l'applicazione

$$\begin{aligned} \rho^*\colon \quad & G \to Aut(H^T) \\ & g \mapsto (g^\rho)^* \end{aligned}$$

è, come si verifica facilmente, una rappresentazione di G come gruppo di automorfismi del gruppo H^T che chiameremo **rappresentazione trasposta** di G su H indotta da ρ. Indichiamo con

$$G \wr_\rho H$$

il prodotto semidiretto di H^T con G via l'azione ρ^*. $G \wr_\rho H$ si dice **prodotto intrecciato** di H con G via l'azione ρ. Si osservi che

$$|G \wr_\rho H| = |G||H|^{|T|}. \tag{8.11}$$

Nel caso particolare in cui $T = G$ e ρ è l'azione regolare a destra di G sul suo supporto, il prodotto intrecciato $G \wr_\rho H$ si dice **prodotto intrecciato standard** di G con H e si indica semplicemente con $G \wr H$.

8.2.13 Prodotto intrecciato di azioni

Siano, come nella sezione precedente, G ed H gruppi, (T, ρ_T) un G-insieme e sia (Δ, ρ_Δ) un H-insieme. Per semplicità scriviamo, per ogni $(t, \delta) \in T \times \Delta$ ed ogni $(g, h) \in G \times H$,

$$t^g \text{ al posto di } t^{g^{\rho_T}} \text{ e } \delta^h \text{ al posto di } \delta^{h^{\rho_\Delta}}.$$

Definiamo un'azione $\rho_T \wr \rho_\Delta$ di $G \wr_{\bar\rho_T} H$ sul prodotto cartesiano $T \times \Delta$, ponendo, per ogni $(t, \delta) \in T \times \Delta$ ed ogni $(g, f) \in G \wr_{\bar\rho_T} H$

$$(t, \delta)^{(g,f)^{\rho_T \wr \rho_\Delta}} := (t^g, \delta^{f(t^g)}) \tag{8.12}$$

Lasciamo per esercizio la dimostrazione che $(g, f)^{\rho_T \wr \rho_\Delta}$ è una permutazione di $T \times \Delta$. Proviamo invece che

$$\rho_T \wr \rho_\Delta\colon G \wr_{\bar\rho_T} H \to Aut(T \times \Delta)$$

è un omomorfismo di gruppi. Siano $(t, \delta) \in T \times \Delta$ e $(g_1, f_1), (g_2, f_2) \in G \wr_{\bar\rho_T} H$, allora

$$\begin{aligned} ((t, \delta)^{(g_1,f_1)^{\rho_T \wr \rho_\Delta}})^{(g_2,f_2)^{\rho_T \wr \rho_\Delta}} &= (t^{g_1}, \delta^{f_1(t^{g_1})})^{(g_2,f_2)^{\rho_T \wr \rho_\Delta}} \\ &= (t^{g_1 g_2}, (\delta^{f_1(t^{g_1})})^{f_2(t^{g_1 g_2})}) \\ &= (t^{g_1 g_2}, \delta^{f_1^{g_2}(t^{g_1 g_2}) f_2(t^{g_1 g_2})}) \\ &= (t^{g_1 g_2}, \delta^{(f_1^{g_2} f_2)(t^{g_1 g_2})}) \\ &= (t, \delta)^{(g_1 g_2, f_1^{g_2} f_2)^{\rho_T \wr \rho_\Delta}} \\ &= (t, \delta)^{((g_1,f_1)(g_2,f_2))^{\rho_T \wr \rho_\Delta}}, \end{aligned}$$

da cui $(g_1, f_1)^{\rho_T \wr \rho_\Delta}(g_2, f_2)^{\rho_T \wr \rho_\Delta} = ((g_1, f_1)(g_2, f_2))^{\rho_T \wr \rho_\Delta}$.

Chiameremo l'azione $\rho_T \wr \rho_\Delta$ di $G \wr_{\rho_T} H$ su $T \times \Delta$ **prodotto intrecciato** delle azioni ρ_T e ρ_Δ.

Vogliamo ora determinare il nucleo di $\rho_T \wr \rho_\Delta$ in funzione dei nuclei di ρ_T e ρ_Δ. Per i nostri scopi sarà sufficiente trattare il caso in cui ρ_Δ è fedele, mentre il caso generale viene lasciato per esercizio.

Lemma 8.2.17 *Siano G ed H gruppi, (T, ρ_T) un G-insieme e (Δ, ρ_Δ) un H-insieme. Allora $\rho_T \wr \rho_\Delta$ è fedele se e solo se sia ρ_T che ρ_Δ sono fedeli.*

DIMOSTRAZIONE. Osserviamo che $(g, f) \in \ker(\rho_T \wr \rho_\Delta)$ se e solo se, per ogni $(t, \delta) \in T \times \Delta$, risulta

$$(t, \delta) = (t, \delta)^{(g,f)^{\rho_T \wr \rho_\Delta}} = (t^g, \delta^{f(t^g)})$$

e questo è vero se e solo se $g \in \ker(\rho_T)$ e, per ogni $t \in T$, $f(t) \in \ker(\rho_\Delta)$, da cui segue la tesi. ∎

Supponiamo ora che ρ_T non sia fedele. Indichiamo il gruppo $G/\ker(\rho_T)$ con $\bar{G}$. Se $g \in G$ indichiamo con $\bar{g}$ la classe laterale destra di $\ker(\rho_T)$ di rappresentante g e con $\bar{\rho}_T$ l'azione di $\bar{G}$ su T indotta da ρ_T.

Teorema 8.2.18 *Siano G ed H gruppi, (T, ρ_T) un G-insieme e (Δ, ρ_Δ) un H-insieme. Sia*

$$\iota \colon G \wr_{\rho_T} H \to \bar{G} \wr_{\bar{\rho}_T} H$$

l'applicazione definita, per ogni $(g, f) \in G \wr_{\rho_T} H$, da

$$(g, f)^\iota = (\bar{g}, f).$$

Allora

1. *ι è un omomorfismo suriettivo di gruppi,*
2. *$\rho_T \wr \rho_\Delta = \iota(\bar{\rho}_T \wr \rho_\Delta)$,*
3. *Se ρ_Δ è fedele allora $\bar{\rho}_T \wr \rho_\Delta$ è fedele e $\ker(\iota) = \ker(\rho_T \wr \rho_\Delta)$*

DIMOSTRAZIONE. Si osservi che se $f \in H^T$ e $g \in G$ allora, per ogni $t \in T$,

$$f^{\bar{g}}(t) = f(t^{\bar{g}^{-1}}) = f(t^{g^{-1}}) = f^g(t) \tag{8.13}$$

da cui $f^{\bar{g}} = f^g$. Siano ora (g_1, f_1) e $(g_2, f_{2)}$ in $G \wr_{\rho_T} H$. Allora

$$\begin{aligned}((g_1, f_1)(g_2, f_2))^\iota &= (g_1 g_2, f_1^{g_2} f_2)^\iota = (\bar{g}_1 \bar{g}_2, f_1^{g_2} f_2) = \\ &(\bar{g}_1 \bar{g}_2, f_1^{\bar{g}_2} f_2) = (\bar{g}_1, f_1)(\bar{g}_2, f_2) = (g_1, f_1)^\iota (g_2, f_2)^\iota,\end{aligned}$$

da cui segue che ι è un omomorfismo ed è ovviamente suriettivo.

Ora, per ogni $(t, \delta) \in T \times \Delta$ ed ogni$(g, f) \in G \wr_{\rho_T} H$, risulta

$$(t, \delta)^{(g,f)^{\rho_T \wr \rho_\Delta}} = (t^g, \delta^{f(t^g)}) = (t^{\bar{g}}, \delta^{f(t^{\bar{g}})}) = (t, \delta)^{(\bar{g},f)^{\bar{\rho}_T \wr \rho_\Delta}} = (t, \delta)^{(g,f)^{\iota(\bar{\rho}_T \wr \rho_\Delta)}},$$

da cui segue la 2..

Infine la 3. discende facilmente dal Lemma 8.2.17 e dalla 2.. ∎

8.2.14 Decomposizione di un'azione transitiva e non primitiva

In questa sezione G è un gruppo, U ed H sono sottogruppi di G con $U \leq H$. ρ è l'azione di Cayley a destra di G su G/U, $\rho_{G/H}$ è l'azione di Cayley a destra di G su G/H e $\rho_{H/U}$ è l'azione di Cayley a destra di H su H/U.

Trasversali

Un *trasversale destro* (o *sistema di rappresentanti* delle classi laterali destre di H in G) è un sottoinsieme T di G tale che per ogni $g \in G$

$$|Hg \cap T| = 1.$$

Si osservi che se $t = Hg \cap T$, allora $Hg = Ht$ e quindi T è un trasversale destro se e solo se

1. per ogni $t, s \in T$, $Ht = Hs$ se e solo se $t = s$ e
2. per ogni $g \in G$ esiste un unico $t \in T$ tale che $Hg = Ht$.

Per ogni $g \in G$ indichiamo con t_g l'unico elemento di $Hg \cap T$. Chiaramente l'applicazione

$$\begin{aligned} \tau\colon \quad & G/H \to T \\ & Hg \mapsto t_g \end{aligned}$$

è una biiezione tra G/H e T. Si osservi che $Hg = Ht_g$ e quindi

$$gt_g^{-1} \in H.$$

Definiamo un'azione ρ_T di G su T in modo che $(G/H, \rho_{G/H})$ e (T, ρ_T) siano G-insiemi isomorfi. Siano a in G e $t \in T$. $H(ta)$ è una classe laterale destra di H in G e quindi esiste un unico elemento $t^{a^{\rho_T}}$ di T tale che

$$H(ta) = Ht^{a^{\rho_T}}. \tag{8.14}$$

Si verifica facilmente che, per ogni $a \in G$, a^{ρ_T} è una permutazione di T e l'applicazione $\begin{aligned} \rho_T\colon \quad & G \to S_T \\ & a \mapsto a^{\rho_T} \end{aligned}$ è un'azione di G su T. Inoltre, per il modo in cui è stata costruita l'azione ρ_T, il G-insieme (T, ρ_T) è isomorfo a $(G/H, \rho_{G/H}$.

Le applicazioni ψ e σ

Chiaramente, per ogni $g \in G$, $Ug \subset Hg$ e Hg è l'unica classe laterale di H contenente Ug. Possiamo quindi definire un'applicazione

$$\begin{aligned} \psi\colon \quad & G/U \to (T \times H/U) && (8.15) \\ & Ug \mapsto (t_g, Ugt_g^{-1}). && (8.16) \end{aligned}$$

Si verifica facilmente che ψ è una biiezione tra G/U e $(T \times H/U)$.

Sia $\bar{G} = G/\ker(\rho_T)$, e $\bar{\rho}_T$ l'azione di $\bar{G}$ su T indotta da ρ_T. Vogliamo ora costruire un omomorfismo σ da G in $\bar{G} \wr_{\bar{\rho}_T} H$ in modo che ϕ sia un isomorfismo tra i G-insiemi $(G/U, \rho)$ e $(G/H \times H/U, \sigma\bar{\rho}_{G/H} \wr \rho_{H/U})$.

Per ogni $a \in G$ ed ogni $t \in T$, poniamo

$$f_a(t) := (t^{(a^{\rho_T})^{-1}} a)t^{-1}; \tag{8.17}$$

Dalla 8.17, scambiando t con $t^{a^{\rho_T}}$ segue immediatamente che

$$f_a(t^{a^{\rho_T}}) = ta(t^{a^{\rho_T}})^{-1} \text{ e quindi } ta = f_a(t^{a^{\rho_T}})t^{a^{\rho_T}}. \tag{8.18}$$

Dalla 8.14 segue che, per ogni $t \in T$, $f_a(t^{a^{\rho_T}})$ è un elemento di H quindi, tenendo presente che a^{ρ_T} è una permutazione di T, per ogni a in G, possiamo definire un'applicazione

$$\begin{array}{rccc} f_a\colon & T & \to & H \\ & t & \mapsto & (t^{(a^{\rho_T})^{-1}} a)t^{-1}. \end{array}$$

Siano ora $a, b \in G$. Vogliamo vedere in quale relazione sono f_a, f_b e f_{ab}. Sia $t \in T$, dalla 8.17 segue che

$$t(ab) = f_{(ab)}(t^{(ab)^{\rho_T}})t^{(ab)^{\rho_T}} = f_{(ab)}(t^{a^{\rho_T} b^{\rho_T}})t^{a^{\rho_T} b^{\rho_T}}. \tag{8.19}$$

D'altra parte

$$\begin{array}{rcl} t(ab) & = & (ta)b = (f_a(t^{a^{\rho_T}})t^{a^{\rho_T}})b = f_a(t^{a^{\rho_T}})(t^{a^{\rho_T}} b) \\ & = & f_a(t^{a^{\rho_T}})(f_b(t^{a^{\rho_T}})^{b^{\rho_T}} (t^{a^{\rho_T}})^{b^{\rho_T}}) \\ & = & (f_a(t^{a^{\rho_T}}) f_b(t^{a^{\rho_T} b^{\rho_T}})t^{a^{\rho_T} b^{\rho_T}} \\ & = & (f_a)^{b^{\rho_T^*}} (t^{a^{\rho_T} b^{\rho_T}}) f_b(t^{a^{\rho_T} b^{\rho_T}}))t^{a^{\rho_T} b^{\rho_T}} \\ & = & ((f_a)^{b^{\rho_T^*}} f_b(t^{a^{\rho_T}})(t^{a^{\rho_T} b^{\rho_T}}))t^{a^{\rho_T} b^{\rho_T}} \end{array} \tag{8.20}$$

Dalle 8.17 e 8.19 si ottiene

$$\begin{array}{rcl} f_{ab}(t^{(a,b)^{\rho_T}}) & = & f_a(t^{a^{\rho_T}}) f_b(t^{a^{\rho_T} b^{\rho_T}}) = (f_a^{b^{\rho_T^*}} (t^{a^{\rho_T} b^{\rho_T}}) f_b(t^{a^{\rho_T} b^{\rho_T}})) \\ & = & (f_a^{b^{\rho_T^*}} f_b)(t^{(ab)^{\rho_T}}), \end{array}$$

per ogni t in T, da cui segue

$$f_{ab} = (f_a^{b^{\rho_T^*}} f_b) \tag{8.21}$$

Sia ora

$$\sigma\colon G \to \bar{G} \wr_{\rho_T} H$$

L'applicazione definita, per ogni a in G, da

$$a^\sigma = (\bar{a}, f_a).$$

Proviamo che σ è un omomorfismo di gruppi. Per ogni $a, b \in G$ dalla 8.21 risulta infatti:

$$(ab)^\sigma = (\bar{a}\bar{b}, f_{ab}) = (\bar{a}\bar{b}, (f_a)^{b^{\rho_T^*}} f_b) = (\bar{a}\bar{b}, (f_a)^{\bar{b}^{\rho_T}{}^*} f_b) = (\bar{a}, f_a)(\bar{b}, f_b) = a^\sigma b^\sigma.$$

Sia ξ l'applicazione composta $\sigma(\bar{\rho}_T \wr \rho_{H/T})$. Per quanto appena visto ξ è un'azione di G su $T \times H/U$. Proviamo ora che ψ è un omomorfismo di G-insiemi tra $(G/U, \rho)$ e $(T \times H/U, \xi)$. Siano $a, g \in G$, $U_g \in G/U$, ed $h = gt_g^{-1}$ allora, dalla 8.18 si ottiene

$$\begin{aligned}
((Ug)^{a^\rho})^\psi &= ((Uht_g)^{a^\rho})^\psi = (U(ht_g)a))^\psi = (Uh(t_g a))^\psi \\
&= (Uh(f_a(t_g^{\bar{a}^{\bar{\rho}_T}})t_g^{\bar{a}^{\bar{\rho}_T}}))^\psi = (t_g^{\bar{a}^{\bar{\rho}_T}}, Uh(f_a(t_g^{\bar{a}^{\bar{\rho}_T}}))) \\
&= (t_g^{\bar{a}^{\bar{\rho}_T}}, (Uh)^{(f_a(t_g^{\bar{a}^{\bar{\rho}_T}}))^{\rho_{H/T}}}) = (t_g, Uh)^{(\bar{a}, f_a)^{\bar{\rho}_T \wr \rho_{H/U}}} \\
&= ((Uht_g)^\psi)^{a^\xi}.
\end{aligned}$$

Decomposizione di un'azione transitiva non primitiva

Teorema 8.2.19 *Siano*

U ed H sottogruppi di un gruppo G, con $U \leq H$,
T un trasversale destro di H in G,
ρ l'azione di Cayley a destra di G su G/U,
ρ_T l'azione di G su T indotta dall'azione di Cayley a destra di G su G/H,
$\bar{G}$ il gruppo quoziente $G/\ker(\rho_T)$,
per ogni $a \in G$, sia $\bar{a} = \ker(\rho_T)a$,
$\bar{\rho}_T$ l'azione di $\bar{G}$ su T indotta da ρ_T
$\rho_{H/U}$ l'azione di Cayley a destra di H su H/U,
σ l'applicazione da G in $\bar{G} \wr_{\rho_T} H$ che a ciascun elemento a di G associa la coppia $(\bar{a}, f_a)$, dove f_a è l'applicazione da T in H definita in 8.17
ξ l'applicazione composta $\sigma(\bar{\rho}_T \wr \rho_{H/U})$
ψ l'applicazione da G/U in $T \times H/U$ che manda ciascuna classe laterale Ug di U in G nella coppia (t_g, Ugt_g^{-1}).

Allora

1. *σ è un omomorfismo di gruppi*
2. *ξ è una azione di G su $T \times H/U$,*
3. *ψ è un isomorfismo di G insiemi tra $(G/U, \rho)$ e $T \times H/U, \xi$,*
4. *se $core_H(U) = \{1\}$, allora σ è iniettivo.*

DIMOSTRAZIONE. I punti 1., 2. e 3. sono stati dimostrati nella sottosezione precedente, il punto 4. discende immediatamente dal teorema 8.2.18 ■

Corollario 8.2.20 *ia H un sottogruppo normale di un gruppo G. Allora G è isomorfo ad un sottogruppo del prodotto intrecciato standard $G/H \wr H$*

DIMOSTRAZIONE. Usiamo le notazioni del teorema 8.2.19 con $U = \{1\}$. Allora ρ è l'azione regolare a destra, ed è quindi fedele. Per il teorema 8.2.19, σ è iniettiva inoltre

$$\ker(\rho) = \ker(\rho_T) = core_G(H) = H.$$

Segue allora che

$$G \cong G^\sigma \leq G/H \wr_{\rho_T} H \cong G/H \wr H.$$

■

8.3 Esercizi

Esercizio 8.3.1 *Dimostrare il corollario 8.1.4.*

Esercizio 8.3.2 *Sia G un gruppo finito e p il più piccolo divisore primo di $|G|$. Dimostrare che se H è un sottogruppo di indice p in G allora $H \trianglelefteq G$.*

Esercizio 8.3.3 *Sia G un gruppo e $\sigma \in Aut(G)$. Siano $H, K \leq G$ con $K \leq H$, si provi che:*

1. *$H^\sigma \cong H$;*
2. *$|H^\sigma : K^\sigma| = |H : K|$*
3. *se $K \trianglelefteq H$ allora $K^\sigma \trianglelefteq H^\sigma$ e $H^\sigma/K^\sigma \cong H/K$*
4. *se $S \subset G$ allora $\langle S^\sigma \rangle = (\langle S \rangle)^\sigma$*

Esercizio 8.3.4 *Determinare il centro dei gruppi S_3 e D_8.*

Esercizio 8.3.5 *Dimostrare che un gruppo semplice non abeliano ha centro identico.*

Esercizio 8.3.6 *Sia G un gruppo e sia $G/Z(G)$ abeliano, si provi che:*

1. *per ogni $a \in G$, l'applicazione*

$$[-, a]\colon G \to G$$

definita, per ogni $g \in G$, da

$$g^{[-,a]} = [g, a]$$

è un endomorfismo di G la cui immagine è contenuta in $Z(G)$;

2. *il nucleo di questo endomorfismo è* $C_G(a)$*;*

3. $G/C_G(a)$ *è isomorfo ad un sottogruppo di* $Z(G)$*.*

Esercizio 8.3.7 *Dimostrare che in un p-gruppo abeliano elementare* G *tutti i sottogruppi sono normali ma gli unici sottogruppi caratteristici sono* $\{1\}$ *e* G*.*

Esercizio 8.3.8 *Calcolare l'ordine di* $GL(n, \mathbf{Z}_p)$*.*

Esercizio 8.3.9 *Si provi che se* G *è un gruppo finito, allora per ogni primo* p *che divide* $|G/G'|$ *esiste un sottogruppo caratteristico* $G(p)$ *tale che* $G/G(p)$ *è un gruppo abeliano di ordine* p^k*, dove* p^k *è la massima potenza di* p *che divide* $|G/G'|$*.*

Esercizio 8.3.10 *Si provi che se* H *è un sottogruppo di un gruppo* G *allora esiste un* G*-insieme* (X, ρ) *ed un elemento* $x \in X$ *con* $H = G_x$*.*

Esercizio 8.3.11 *Si provi che se* N *è un sottogruppo normale di un gruppo* G*, allora esiste un* G*-insieme* (X, ρ) *con* $N = \ker(\rho)$*.*

Sia G un gruppo. Un elemento g di G si dice **non-generatore** se per ogni sottoinsieme X di G tale che $\langle X, g\rangle = G$, risulta $\langle X\rangle = G$.

Esercizio 8.3.12 *Sia* G *un gruppo finito, si provi che il sottogruppo di Frattini di* G *coincide con l'insieme dei non-generatori.*

Esercizio 8.3.13 *Sia* G *un gruppo e supponiamo che* G *possieda un p-sottogruppo abeliano elementare, normale e non identico* V *di ordine* p^n*. Supponiamo che* $|G/V|$ *sia coprimo con* $|GL(n, p)|$*. Allora* $V \leq Z(G)$*.*

Esercizio 8.3.14 *Sia* G *un gruppo e si consideri l'azione che* G *induce su se stesso per coniugio. Sia* H *il prodotto semidiretto di* G *per* G *via* ϕ*. Si provi che* H *è isomorfo al prodotto diretto* $G \times G$*.*

Esercizio 8.3.15 *Sia* G *un gruppo con* $Z(G) = \{1\}$*. Si provi che*

$$C_{Aut(G)}(Inn(G)) = \{1\}.$$

Si deduca che $Z(Aut(G)) = \{1\}$*.*

Esercizio 8.3.16 *Sia* G *un gruppo semplice finito. Si provi che* $Aut(G)$ *è completo (Suggerimento: sia* $\sigma \in Aut(Aut(G))$*, provare che*

$$G \cong Inn(G) \cong Inn(G)^\sigma \lhd Aut(G).$$

Dedurre che $\langle Inn(G), Inn(G)^\sigma\rangle = Inn(G) \times Inn(G)^\sigma$*. Per l'esercizio precedente,* $Inn(G) = Inn(G)^\sigma$ *e quindi* $\sigma \in Inn(Aut(G).)$

Esercizio 8.3.17 *Sia* ϕ *l'automorfismo di* $(\mathbf{Z}, +)$ *che manda ogni elemento di* $\mathbf{Z}$ *nel suo opposto e sia* D_∞ *il prodotto semidiretto di* $\mathbf{Z}$ *con* $\langle\phi\rangle$*. Si provi che*

1. *D_∞ è generato dagli elementi $(\phi, 0)$ e $(d|\mathbf{Z}, -1)(\phi, 0)(id_{\mathbf{Z}}, 1)$ che hanno ordine 2;*

2. *ogni gruppo diedrale è immagine omomorfa di D_∞.*

Il gruppo D_∞ si dice **gruppo diedrale di ordine infinito**.

Sia G un gruppo finito e sia (X, ρ) un G-insieme.

Esercizio 8.3.18 *Provare che, se G è transitivo su X, allora G è transitivo su ogni G-insieme quoziente di X.*

Esercizio 8.3.19 *Sia (Y, σ) un G-insieme ed $f: X \to Y$ un omomorfismo di G-insiemi. Provare le seguenti affermazioni:*

1. *se W è un G-sottoinsieme di X ed f è suriettiva, allora $\phi(W)$ è un G-sottoinsieme di Y;*

2. *l'affermazione precedente non è vera se si lascia cadere l'ipotesi che f non sia suriettiva;*

3. *se Z è un G-sottoinsieme di Y, allora $f^{-1}(Z)$ è un G-sottoinsieme di X;*

4. *se $\cong$ è una G-congruemza su Y, allora la relazione $\cong^{f^{-1}}$ su X, definita da*
$$x_1 \cong^{f^{-1}} x_2 \text{ se e solo se } f(x_1) \cong f(x_2),$$
è una G-congruenza su X;

5. *se f è suriettiva e $\cong$ è una G-congruemza su X, allora la relazione $\cong^f$ su Y, definita da*
$$y_1 \cong^f y_2 \text{ se esistono } x_i \in f^{-1}(y_i) \ (i \in \{1, 2\}) \text{ tali che } x_1 \cong x_2,$$
è ben definita ed è una G-congruenza su Y.

Esercizio 8.3.20 *Sia G un gruppo e δ l'azione regolare a destra di G su se stesso. Si provi che un sottoionsieme Y di G è un sottogruppo se e solo se per ogni $y \in Y$ risulta $Y^{\delta(y)} = Y$.*

Esercizio 8.3.21 *Sia G un gruppo finito e sia p il più piccolo divisore primo del suo ordine. Si dimostri che se H è un sottogruppo di G di indice p, allora H è normale in G.* (Suggerimento: si consideri l'azione di G per moltiplicazione a destra sull'insieme G/H).

Esercizio 8.3.22 *Siano G e p come nell'esercizio precedente. Sia N un sottogruppo normale di G di ordine p. Si dimostri che $N \leq Z(G)$.*

Esercizio 8.3.23 *Sia G un gruppo, X un G-insieme, $g \in G$ e $x \in X$. Si provi che*

$$G_x^g = G_{x^g}.$$

Si deduca che, se G è transitivo su X, il nucleo dell'azione è

$$\bigcap_{g \in G} (G_x)^g.$$

Esercizio 8.3.24 *(Argomento di Frattini) Sia G un gruppo e $\rho: G \to S_\Omega$ un'azione di G su un insieme Ω. Sia N un sottogruppo di G e supponiamo che la restrizione di ρ a N sia un'azione transitiva di N su Ω. Dimostrare che per ogni $\omega \in \Omega$ risulta*

$$G = G_\omega N.$$

*(*Suggerimento: se $g \in G$ allora, poiché N è transitivo su Ω, esiste n in N tale che $\omega^g = \omega^n$ da cui segue che $gn^{-1} \in G_\omega$ e $g = (gn^{-1})n \in G_\omega N$ *).*

Esercizio 8.3.25 *Sia G un gruppo, H e K sottogruppi di G. Si provi che H agisce transitivamente per moltiplicazione a destra sull'insieme delle classi laterali di K in $\langle H, K\rangle$ se e solo se K agisce transitivamente per moltiplicazione a destra sull'insieme delle classi laterali di H in $\langle H, K\rangle$.* (Suggerimento: usare la proposizione 1.1.7).

Esercizio 8.3.26 *Sia G un gruppo che agisce transitivamente su un insieme X. Si provi che, se $x \in X$, $N_G(G_x)$ agisce transitivamente su X_{G_x}.*

Esercizio 8.3.27 *Sia G un gruppo di permutazioni transitivo su un insieme X. Sia $x \in X$, U un sottogruppo di G contenuto in G_x. Si provi che $N_G(U)$ è transitivo su X_U se e solo se per ogni $g \in G$ tale che $U^g \leq G_x$ esiste $h \in G_x$ con $U^g = U^h$*

Esercizio 8.3.28 *Si provi la Proposizione 8.2.4.*

Esercizio 8.3.29 *Si provi la Proposizione 8.2.5.*

Esercizio 8.3.30 *Sia H un sottogruppo di un gruppo G si consideri l'azione di G per moltiplicazione a destra sull'insieme G/H. Si provi che, per ogni $g \in G$, risulta*

$$G_{Hg} = H^g.$$

Dall'esercizio precedente il nucleo di questa azione è

$$\bigcap_{g \in G} H^g.$$

Dimostrare che questo è il più grande sottogruppo normale di G contenuto in H. (Questo sottogruppo si dice **cuore** *di H in G e si indica con $core_G(H)$ oppure con H_G.*

Esercizio 8.3.31 *Sia G un gruppo, dimostrare che le seguenti affermazioni sono equivalenti:*

1. *G agisce transitivamente su un insieme di ordine n;*
2. *esiste un omomorfismo da G in S_n tale che l'immagine di G sia transitiva su $\{1, \ldots, n\}$;*
3. *G ha un sottogruppo di indice n.*

Esercizio 8.3.32 *Provare il Teorema di Lagrange (teorema 1.1.4) usando il teorema 8.2.7* (Suggerimento: Se $H \leq G$ H coincide con lo stabilizzatore in G della classe laterale destra H nell'azione per moltiplicazione a destra).

Esercizio 8.3.33 *Provare che se G è un gruppo finito e H è un sottogruppo proprio di G, allora*

$$|G| > |\bigcup_{g \in G} H^g|,$$

in particolare G non è unione di classi di coniugio di un suo sottogruppo. (suggerimento: poiché $H \geq N_G(H)$ e $|H \cap H^g| \geq 1$, l'unione delle classi di coniugio di H contiene al più $|G : H| \cdot (|H| - 1)$ elementi)

Esercizio 8.3.34 *Provare che se un gruppo G agisce transitivamente su un insieme X, allora esiste un elemento g di G che* **agisce senza punti fissi** *su X, cioè $x^g \neq x$ per ogni $x \in X$.* (Suggerimento: tradurre il problema all'azione di G sulle classi laterali di un suo sottogruppo H ed usare l'esercizio precedente).

Esercizio 8.3.35 *Sia G un gruppo che agisce transitivamente su un insieme X. Provare che*

$$\sum_{g \in G} |X_g| = |G|,$$

cioè ogni elemento di G lascia fisso in media un elemento di G. (Suggerimento: contare le coppie (x, g) in due modi diversi: il primo termine si ottiene contando per ogni $g \in G$ la cardinalità di $|X_g|$ e sommando queste cardinalità al variare di $g \in G$; il secondo termine si ottiene calcolando per ogni $x \in X$ la cardinalità di G_x e sommando queste cardinalità per tutti gli $x \in X$).

Esercizio 8.3.36 *Provare l'esercizio 8.3.34 usando l'esercizio8.3.35.* (Suggerimento: si osservi che l'identità di G lascia fissi tutti gli elementi di X).

Esercizio 8.3.37 *Sia G un gruppo $\{H_i\}_{i \in \mathcal{I}}$ una famiglia di sottogruppi di G. Sia V l'insieme delle classi laterali destre dei sottogruppi H_i, cioè*

$$V = \{H_i g | i \in \mathcal{I}, g \in G\}.$$

Definiamo una relazione di adiacenza $\leftrightarrow$ nell'insieme V nel modo seguente:

$$H_i g_1 \leftrightarrow H_j g_2 \text{ se e solo se } H_i g_1 \neq H_j g_2 \text{ e } H_i g_1 \cap H_j g_2 \neq \emptyset. \tag{8.22}$$

La coppia $\Gamma = (V, \leftrightarrow)$ è un grafo (semplice, non orientato e privo di cappi), gli elementi di V si dicono **vertici** *e gli elementi $\leftrightarrow$, cioè le coppie non ordinate (α, β) tali che $\alpha, \beta \in V$ e $\alpha \leftrightarrow \beta$ si dicono* **lati**. *Il grafo Γ si dice* **connesso** *se per ogni coppia di vertici α, β esiste un intero positivo n ed un insieme $\{\alpha_i | \alpha_i \in V\ , 0 \leq i \leq n\}$ tali che $\alpha = \alpha_0$, $\alpha_n = \beta$ e $\alpha_{i-1} \leftrightarrow \alpha_i$ per ogni $i = 1, \ldots, n$. Dimostrare che:*

1. *se $H_i g_1 \leftrightarrow H_j g_2$ allora $H_i \neq H_j$;*
2. *il gruppo G agisce per moltiplicazione a destra su Γ, cioè se $\alpha, \beta \in V$ con $\alpha \leftrightarrow \beta$ e $g \in G$, allora $\alpha g \leftrightarrow \beta g$;*
3. *il nucleo di questa azione è il più grande sottogruppo normale di G contenuto in ogni $\{H_i\}$, $i \in \mathcal{I}$;*
4. *se $\alpha = H_i g$, allora $G_\alpha = H_i^g$;*
5. *ogni vertice (lato) è coniugato in G con un elemento di $\{H_i\}_{i \in \mathcal{I}}$ ed ogni lato è coniugato con un lato del tipo (H_i, H_j), $i, j \in \mathcal{I}$;*
6. *in particolare, se $|\mathcal{I}| = 2$ allora G è transitivo sui lati e se α è un vertice, G_α agisce transitivamente per moltiplicazione a destra sull'insieme*

$$G_\alpha^{(1)} = \{\beta | \alpha \leftrightarrow \beta\};$$

7. *Γ è connesso se e solo se $G = \langle H_i | i \in \mathcal{I} \rangle$.*

Esercizio 8.3.38 *Sia N un sottogruppo normale di un gruppo G. Si provi che un sottogruppo K è un complemento di N in G se e solo se K è un trasversale destro di N in G.*

Esercizio 8.3.39 *Sia G un gruppo. Si provi che G è isomorfo ad un gruppo di permutazioni primitivo se e solo se G ha un sottogruppo massimale M tale che $core_G(M) = \{1\}$.*

Esercizio 8.3.40 *Sia Ω un grafo e $\rho: G \to Aut(\Omega)$ una rappresentazione di G su Ω. Si provi che, per ogni $\omega \in \Omega$, ed ogni intero non negativo d, l'insieme $\Delta^{(d)}$ dei vertici a distanza d da ω è G_ω-invariante.*

Esercizio 8.3.41 *Sia Ω un grafo connesso e $\rho: G \to Aut(\Omega)$ una rappresentazione di G su Ω. Supponiamo che G sia transitivo su Ω e, per ogni $\omega \in \Omega$, G_ω sia transitivo sull'insieme dei vertici adiacenti a ω. Allora G è primitivo su Ω.*

Sia G un gruppo e Ω un $G - insieme$. Diremo che G agisce in modo 2-**transitivo** (o, semplicemente, che G è 2-**transitivo** su Ω) se per ogni quadrupla (x_1, x_2, y_1, y_2) con $x_1 \neq x_2$ e $y_1 \neq y_2$, esiste un elemento g di G tale che $x_1^g = y_1$ e $x_2^g = y_2$.

Esercizio 8.3.42 *Si provi che se G è 2-transitivo su Ω, allora G è primitivo su Ω.*

Esercizio 8.3.43 *Si provi che G è 2-transitivo su Ω se e solo G è transitivo su Ω e, per ogni $x \in \Omega$, G_x è transitivo su $\Omega \setminus \{x\}$.*

Esercizio 8.3.44 *Sia G un gruppo che agisce in modo primitivo e fedele su un insieme Ω. Sia N un sottogruppo normale non identico di G. Si provi che $C_G(N)$ agisce in modo regolare su Ω. In particolare $|C_G(N)| = |\Omega|$.*

Esercizio 8.3.45 *Si provi che ogni gruppo semplice finito è isomorfo ad un gruppo di permutazioni primitivo.*

Esercizio 8.3.46 *Sia G un gruppo che agisce in modo primitivo su un insieme Ω. Sia N un sottogruppo normale di G. Si provi che se N non è contenuto nel nucleo dell'azione, allora N è transitivo su Ω.*

Nei prossimi esercizi vogliamo dimostrare una prima riduzione del Teorema di O'Nan-Scott per i gruppi finiti risolubili.

Esercizio 8.3.47 *Sia G un gruppo di permutazioni finito, primitivo e risolubile. Sia M un sottogruppo massimale di G con $core_G M = \{1\}$. Si provi che esiste un sottogruppo abeliano elementare V tale che $G = VT$ e $V \cap T = \{1\}$.*

Esercizio 8.3.48 *Siano G, M e V come nell'esercizio precedente. Si provi che $A = C_G(V)$.*

Esercizio 8.3.49 *Si provi che un gruppo risolubile finito è primitivo se e solo se é isomorfo ad un prodotto semidiretto di uno spazio vettoriale V finito con un sottogruppo risolubile M di $GL(V)$, tali che V sia privo di sottospazi M-invarianti propri.*

Dall'esercizio precedente segue che, per determinare i gruppi primitivi risolubili finiti, basta determinare, per ogni spazio vettoriale finito V, i sottogruppi risolubili di $GL(V)$ che sono irriducibili su V.

Esercizio 8.3.50 *Sia G il prodotto intrecciato standard di D_8 per C_2. Si provi che in G esistono tre sottogruppi A, B e C tali che $[AB, C] \neq [A, B][A, C]$.*

Capitolo 9

I Teoremi di Sylow e di Schur-Zassenhaus

In questo capitolo applicheremo il metodo delle azioni di gruppo per dimostrare alcuni risultati fondamentali della teoria dei gruppi: i teoremi di Sylow, Schur-Zassenhaus e la nilpotenza dei p-gruppi finiti. In ognuna di queste dimostrazioni dato un gruppo G si cercherà un opportuno insieme X ed una azione di G su X. Dalla struttura di X otterremo le informazioni su G che serviranno per concludere la dimostrazione.

Nel caso dei teoremi di Sylow e di Schur-Zassenhaus (per la parte che riguarda l'esistenza di certi sottogruppi), la scelta, fondamentale, del G-insieme X puó apparire non del tutto naturale ad una prima lettura. Per questo motivo vogliamo ora dare alcune indicazioni per tale scelta.

Osserviamo innanzitutto che, come si è visto nel capitolo sulle azioni di un gruppo su un insieme, sottogruppi e stabilizzatori sono la stessa cosa, nel senso che se H è un sottogruppo di un gruppo G, allora esiste un G-insieme X ed un elemento $x \in X$ tale che $H = G_x$ e, viceversa, dato un G-insieme X ed un elemento $x \in X$ lo stabilizzatore G_x di x in G è un sottogruppo di G. Dovremo quindi

1) *costruire un G-insieme X in modo che il sottogruppo di cui vogliamo provare l'esistenza sia lo stabilizzatore di un elemento di X.*

Abbiamo visto inoltre che, dato un elemento x di un G-insieme X, allora l'orbita x^G, come G-insieme, è isomorfa all'insieme G/G_x delle classi laterali destre di G_x in G con l'azione regolare a destra, dunque

2) *il candidato naturale per l'azione è l'azione regolare a destra ed il candidato per X sarà scelto tra i sottoinsiemi G-invarianti dell'insieme delle parti di G.*

Infine, poiché un sottogruppo è lo stabilizzatore di se stesso nell'azione regolare a destra di G sull'insieme delle parti di G,

3) *gli elementi di X dovranno essere sottoinsiemi di G che abbiano la proprietà del sottogruppo cercato.*

In pratica, nel Teorema di Sylow, dato un gruppo G di ordine $p^n m$ (con p^n potenza di un numero primo p ed m un intero primo con p) vogliamo provare l'esistenza di un sottogruppo S di G con la seguente proprieta':

$$|S| = p^n.$$

Il candidato naturale per X è quindi l'insieme dei sottoinsiemi di ordine p^n di G.

Analogamente, nel caso del Teorema di Schur-Zassenhaus, dato un sottogruppo di Hall (cioè un sottogruppo il cui ordine sia coprimo col suo indice) normale N di G vogliamo provare l'esistenza di un complemento K di N in G. Per l'Esercizio 8.3.38 un complemento di N in G è un sottogruppo K con la seguente proprietà:

$$H \textit{ è un trasversale destro di } N \textit{ in } G.$$

Quindi, in questo caso, il candidato per X sarà l'insieme dei trasversali destri di N in G (o, più precisamente, un suo G-insieme quoziente).

Come abbiamo già osservato in precedenza, la teoria delle rapprsentazioni permette di ottenere informazioni sul gruppo dalle informazioni sull'oggetto su cui il gruppo agisce. Ovviamente strutture diverse daranno informazioni di tipo diverso. Poiché l'unica informazione che la struttura di insieme fornisce è la sua cardinalit (nel senso che due insiemi sono isomorfi se e solo se hanno la stessa cardinalità), le rappresentazioni di un gruppo su un insieme forniscono informazioni aritmentiche sull'esistenza di sottogruppi o di punti fissi (come nei casi, rispettivamente, dell'esistenza dei sottogruppi di Sylow, oppure dell'esistenza di elementi centrali non identici nei p-gruppi finiti). D'altra parte, per dimostrare il coniugio dei p-sottogruppi di Sylow (così come dei complementi di Hall nel Teorema di Schur-Zassenhaus), useremo invece l'azione per coniugio sull'insieme parzialmente ordinato dei p-sottogruppi, in particolare sarà essenziale il fatto che se un p-sottogruppo H normalizza un p-Sylow S, allora $H \leq S$.

9.1 Il Teorema di Sylow

9.1.1 Esistenza dei Sylow

Teorema 9.1.1 (Teorema di Sylow - esistenza) *Sia G un gruppo finito. $|G| = p^n m$ con p un numero primo, m ed n numeri naturali e $(p, m) = 1$ (cioè p^n è la massima potenza di p che divide $|G|$). Allora esistono dei sottogruppi S di G con $|S| = p^n$.*

Dimostrazione. (Wielandt [32]) Consideriamo l'insieme X dei sottoinsiemi di ordine p^n di G. Allora

$$p \textit{ non divide } |X|. \tag{9.1}$$

(vedi Esercizi 9.5.1 e 9.5.2). Inoltre

$$G \text{ opera per moltiplicazione a destra su } X. \tag{9.2}$$

Infatti se $K \in X$ e $g \in G$, allora $Kg = \{kg | k \in K\}$ è ancora un sottoinsieme di ordine p^n.
Per il punto 3. della Proposizione 8.2.1, X è unione disgiunta delle sue G-orbite. Per (9.1) e per l'Equazione delle Orbite (8.6)

$$\text{esiste un'orbita } O \text{ tale che } p \text{ non divide } |O|. \tag{9.3}$$

Sia $K \in O$, per il corollario 8.2.7, $|O| = |G : G_K|$ e quindi

$$p \text{ non divide } |G : G_K|, \text{ in particolare } |G_K| \geq p^n. \tag{9.4}$$

Mostriamo ora che G_K è il sottogruppo cercato, cioè che

$$|G_K| = p^n.$$

Poniamo per comodità $G_K = S$. Per 9.4 basta mostrare che $|S| \leq p^n$. Osserviamo che

$$S \text{ agisce per moltiplicazione a destra su } K. \tag{9.5}$$

Infatti se $k \in K$ e $g \in S (= G_K)$ allora $kg \in K$, inoltre $kg = k$ se e solo se $g = 1$. Quindi

$$\text{per ogni } k \in K,\ S_k = \{1\}. \tag{9.6}$$

Per il Corollario 8.2.7 segue che, se O_k è una S-orbita di K, allora

$$|S| = |O_k| \leq |K| = p^n. \tag{9.7}$$

■

Se G ed S sono come nel teorema precedente allora S si dice p-**sottogruppo di Sylow** di G, o semplicemente p-**Sylow** di G. L'insieme dei p-Sylow di un gruppo G si indica con $Syl_p(G)$.

Molte dimostrazioni sui gruppi finiti fanno uso dell'induzione, o dell'argomento del controesempio minimo, dove, informazioni sui sottogruppi propri di un gruppo vengono usate per ottenere risultati su tutto il gruppo. Ovviamente, per poter mettere in pratica questa strategia, sono essenziali teoremi che garantiscano l'esistenza di sottogruppi. In questo senso, il Teorema 9.1.1 è un teorema d'esistenza di importanza fondamentale.

Come prima facile applicazione del Teorema 9.1.1 proviamo che

Proposizione 9.1.2 *Sia G un gruppo finito e p un numero primo. Allora G è un p-gruppo se e solo se $|G|$ è una potenza di p.*

DIMOSTRAZIONE. Se G è un gruppo di ordine una potenza del numero primo p, allora, per il Teorema di Lagrange, ogni suo sottogruppo ha per ordine una potenza di p, in particolare questo vale per i sottogruppi ciclici e quindi G

è un p-gruppo. Viceversa sia G un p-gruppo finito e q un divisore primo di $|G|$. Per il Teorema 9.1.1 esiste un q-Sylow di G. Per quanto appena visto Q è un q-gruppo e quindi ogni elemento di Q ha ordine una potenza di q. D'altra parte $Q \leq P$ che è un p-gruppo e quindi $q = p$. ∎

9.1.2 Coniugio dei Sylow

A differenza dei gruppi abeliani, non possiamo sperare che, in un qualsiasi gruppo finito G i p-Sylow siano unici: ad esempio in S_3 ci sono tre distinti 2-sottogruppi di Sylow. Vedremo, anzi, che, un gruppo finito G possiede un unico p-sottogruppo di Sylow, per ogni numero primo p, se e solo se G è nilpotente (Teorema 9.3.1. Questo fatto è una conseguenza di un'altra importantissima proprietà dei sottogruppi di Sylow: come si vede immediatamente, G agisce per coniugio su $Syl_p(G)$. La sorpresa è che, come dimostreremo ora, questa azione è transitiva.

Lemma 9.1.3 *Sia S un p-Sylow di un gruppo finito G. Sia T un sottogruppo di G di ordine p^t che normalizza S. Allora $T \leq S$. In particolare se anche $T \in Syl_p(G)$, allora $S = T$.*

Dimostrazione. Per la Proposizione 1.1.8 ST ha ordine una potenza di p. Poiché $|S|$ è la massima potenza di p che divide $|G|$ e, per il Teorema di Lagrange, $|ST|$ divide $|G|$, segue che $|ST| = |S|$ e quindi $T \leq S$ ∎

Corollario 9.1.4 *Sia $R \in Syl_p(G)$. Allora $\{R\}$ è l'unica R-orbita in $Syl_p(G)$ di lunghezza 1.*

Dimostrazione. Che $\{R\}$ sia una R-orbita è ovvio, poichè R normalizza se stesso. Mostriamo che è l'unica di lunghezza 1. Infatti se $\{S\}$ fosse un'altra R-orbita di lunghezza 1, allora R normalizzerebbe S e quindi, per il Lemma 9.1.3 $R = S$, ∎

Teorema 9.1.5 (Teorema di Sylow - coniugio e numero dei Sylow) *Sia G un gruppo finito. $|G| = p^n m$ con p un numero primo, m ed n numeri naturali tali che $(p, m) = 1$, allora*

SY1 il numero dei sottogruppi di G di ordine p^n è congruo a 1 modulo p;

SY2 se T è un sottogruppo di G di ordine p^k con $k \in \{1, \ldots, n\}$, allora esiste un p-Sylow S di G che contiene T;

SY3 G agisce transitivamente per coniugio su $Syl_p(G)$.

DIMOSTRAZIONE. Sia $R \in Syl_p(G)$. R agisce per coniugio su $Syl_p(G)$. Per il Corollario 9.1.4 $\{R\}$ è l'unica R orbita di $Syl_p(G)$ di lunghezza 1. D'altra parte, se O è un'altra R-orbita di $Syl_p(G)$, per il Corollario 8.2.7, $|O|$ divide p^n e quindi p divide $|O|$. Per l'Equazione delle Orbite segue immediatamente che

$$|Syl_p(G)| \equiv 1 (mod\, p). \tag{9.8}$$

Sia ora T un sottogruppo di G con $|T| = p^k$ ($k \in \{1, \ldots, n\}$). Anche T agisce per coniugio su $Syl_p(G)$. Per (9.8) e l'Equazione delle Orbite, esistono degli elementi $Syl_p(G)$ che sono lasciati fissi da T. Sia S uno di questi, allora, per il Lemma 9.1.3, $T \leq S$.

Infine, supponiamo per assurdo che G non sia transitivo su $Syl_p(G)$. Allora $Syl_p(G)$ è l'unione disgiunta di due sottoinsiemi G-invarianti non banali Y e W. Sia $S \in Y$ e $R \in W$. Ora S agisce per coniugio su W e $S \notin W$, quindi, per il Lemma 9.1.3, S non normalizza nessun elemento di W. Di nuovo per il Corollario 8.2.7 e per l'Equazione delle Orbite, segue che p divide $|W|$. Analogamente, invertendo i ruoli di S ed R, si prova che p divide $|Y|$, da cui segue che p divide $|Y| + |W| = |Syl_p(G)|$ il che contraddice (9.8). ∎

Corollario 9.1.6 *Se G è un gruppo finito, allora i p-sottogruppi massimali di G sono esattamente i p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Segue immediatamente da $SY2$ delTeorema 9.1.5. ∎

Da $SY3$ del Teorema 9.1.5 e dall'Argomento di Frattini, segue immediatamente un'importante proprietà di fattorizzazione dei gruppi finiti, che useremo costantemente in seguito[1]

Proposizione 9.1.7 FATTORIZZAZIONE DI FRATTINI *Sia N un sottogruppo finito e normale di un gruppo G. Sia $S \in Syl_p(N)$. Allora $G = NN_G(S)$.*

DIMOSTRAZIONE. Poichè $N \trianglelefteq G$, G agisce per coniugio su $Syl_p(N)$. Per $SY3$ del Teorema 9.1.5, N è transitivo su $Syl_p(N)$ e quindi, per l'Argomento di Frattini $G = NN_G(S)$. ∎

Dunque il gruppo G è controllato, "modulo" il sottogruppo normale N, dal normalizzante di un p-Sylow S di N.

Nel caso in cui S sia un p-Sylow di G, allora

1. S è normale in $N_G(S)$ e
2. $|S|$ è coprimo con $|N_G(S) : S|$.

[1]In quasi tutti i testi l'Argomento di Frattini si riferisce solo all'azione per coniugio di un gruppo finito sui suoi p-sottogruppi di Sylow e quindi coincide con quello che in questi appunti viene detta Fattorizzazione di Frattini. Ci è sembrato più trasparente, peró, dare una definizione più generale dell'Argomento di Frattini per qualsiasi azione

Corollario 9.1.8 *Sia S un p-sottogruppo di Sylow di un gruppo G. Se S è subnormale allora S è normale*

DIMOSTRAZIONE. Per induzione sul difetto di subnormalità d di S in G. Se $S \trianglelefteq G$ non c'è nulla da dimostrare. Altrimenti sia N la chiusura normale di S in G. Chiaramente S è un p-sottogruppo di Sylow di N ed il suo difetto di subnormalità in N è $d-1$. Per ipotesi induttiva $S \trianglelefteq N$, da cui la tesi per la Proposizione 9.1.7. ∎

9.2 Normalizzanti nei p-gruppi finiti

Teorema 9.2.1 *Sia p un primo, n un intero positivo e G un gruppo di ordine p^n. Sia N un sottogruppo normale di G. Allora $N \cap Z(G) \neq \{1\}$. In particolare il centro di G non è identico.*

DIMOSTRAZIONE. Per il Teorema di Lagrange (Teorema 1.1.4), $|N|$ divide p^n e quindi è una potenza di p. Si consideri l'azione di G su N per coniugio (vedi il paragrafo 8.1.3) e si osservi che $N \cap Z(G)$ è esattamente l'insieme dei punti fissi. Ovviamente 1 è un punto fisso, e G agisce quindi anche sull'insieme $N \setminus \{1\}$ che ha ordine coprimo con p. Per la Proposizione 8.2.8 esistono punti fissi in $N \setminus \{1\}$ e quindi $N \cap Z(G) \neq \{1\}$. ∎

Sia G un p-gruppo finito e consideriamo la serie centrale ascendente di G:

$$Z_0(G) = \{1\} \leq Z_1(G) = Z(G) \leq Z_2(G) \leq \ldots < Z_i(G) \leq Z_{i+1}(G) < \ldots.$$

Per il Teorema di Lagrange, per ogni intero $i \geq 0$, il quoziente $G/Z_i(G)$ ha ordine una potenza di p. Per il Teorema 9.2.1, se $G > Z_i(G)$, allora $Z(G/Z_i(G))$ non è identico e quindi

$$Z_{i+1}(G) > Z_i(G).$$

Poichè $|G|$ è finito esiste un intero k tale che $G = Z_k(G)$. Abbiamo così dimostrato che

Teorema 9.2.2 *Se G è un p-gruppo finito, allora G è nilpotente.*

Corollario 9.2.3 *Se G è un p-gruppo finito, allora ogni sottogruppo di G è subnormale.*

DIMOSTRAZIONE. Segue dal Teorema 9.2.2 e dal Teorema 7.3.4. ∎

Teorema 9.2.4 *Sia G un p-gruppo finito. Allora $\Phi(G)$ è il più piccolo sottogruppo normale di G tale che il quoziente sia abeliano elementare.*

DIMOSTRAZIONE. Sia M un sottogruppo massimale di G. Per l'esercizio 9.5.9 M ha indice p ed è normale. Quindi il gruppo quoziente G/M è un gruppo di ordine p, isomorfo quindi al gruppo $\mathbf{Z}_p$. In particolare G/M è abeliano e quindi $G' \leq M$. Poichè questo vale per ogni sottogruppo massimale di G, segue che il sottogruppo di Frattini $\Phi(G)$ contiene G' e quindi $G/\Phi(G)$ è abeliano. Inoltre se $g \in G$ allora $g^p \in M$ perchè, essendo G/M di ordine p, $g^p M = M$. Poiché anche questo vale per ogni sottogruppo massimale M, risulta $g^p \in \Phi(G)$ e quindi $G/\Phi(G)$ è abeliano elementare. Viceversa, se N è un sottogruppo di G tale che G/N è abeliano elementare, allora, per il Teorema di Corrispondenza e per l'Esercizio 3.5.9, N è l'intersezione di tutti i sottogruppi massimali di G che lo contengono e quindi $\Phi(G) \leq N$.

■

Si osservi che l'enunciato del Corollario 9.2.3 equivale a dire che se H è un sottogruppo proprio di G, allora H è propriamente contenuto nel suo normalizzante. Questa è una delle proprietà più importanti dei p-gruppi finiti. I due risultati che seguono mostrano come questa proprietà viene generalmente usata.

Lemma 9.2.5 *([1, Exercise 11.4]) Sia G un gruppo finito, p un numero primo, Ω un sottoinsieme G-invariante di p-sottogruppi di G, P un p-sottogruppo di G e Δ un sottoinsieme di $\Omega \cap \mathcal{L}(P)$ tale che Δ sia $\langle\Delta\rangle$-invariante. Allora o $\Delta = \Omega \cap \mathcal{L}(P)$, oppure esiste un sottogruppo $R \in \Omega \cap \mathcal{L}(P) \setminus \Delta$ tale che Δ sia R-invariante.*

DIMOSTRAZIONE. Sia $T := \langle\Delta\rangle$, $N = N_P(T)$ e $M = N_P(N)$. Chiaramente

$$N \leq M.$$

Supponiamo che, per ogni $R \in \Omega \cap \mathcal{L}(P) \setminus \Delta$, Δ non sia R-invariante. Allora

$$\Omega \cap \mathcal{L}(N) = \Delta$$

e quindi, poiché $\mathcal{L}N$ e Ω sono M-invarianti, segue che Δ è M-invariante. Ma allora M normalizza T e quindi

$$M = N.$$

Per il Corollario 9.2.3 (o meglio la sua forma equivalente), segue che $N = P$, e quindi ogni elemento di $\Omega \cap \mathcal{L}(P)$ normalizza T e quindi anche l'insieme $\Omega \cap \mathcal{L}(T)$, da cui la tesi. ■

Teorema 9.2.6 (TEOREMA DI BAER-SUZUKI [3]) *Sia G un gruppo finito, p un numero primo e R un p-sottogruppo di G tale che, per ogni $g \in G$, $\langle R, R^g\rangle$ sia un p-gruppo. Allora $R[R, G]$ è un p-gruppo.*

DIMOSTRAZIONE. Sia $\Omega := \{R^g | g \in G\}$ e $P \in Syl_p(G)$. Se $\Omega \subseteq \mathcal{L}(P)$.

$$R[R, G] = \langle\Omega\rangle \leq P,$$

da cui la tesi. Supponiamo quindi, per assurdo, che $\Omega \not\subseteq \mathcal{L}(P)$ e sia

$$\Gamma := \Omega \cap \mathcal{L}(P).$$

Per i Teoremi di Sylow, esistono elementi $g \in G$ tali che $\Gamma \neq \Gamma^g$. Tra questi sia g tale che $\Delta := \Gamma \cap \Gamma^g$ sia massimale e sia $T := \langle \Delta \rangle$. Per definizione Δ è $\langle \Delta \rangle$-invariante e, poiché $\Gamma \neq \Gamma^g$, Δ è propriamente contenuto sia in Γ che in Γ^g. Per il Lemma 9.2.5 esistono degli elementi R_1 e R_2 rispettivamente in $\Gamma \setminus \Delta$ e in $\Gamma^g \setminus \Delta$ che normalizzano Δ e quindi T. Per ipotesi $\langle R_1, R_2 \rangle$ è un p-gruppo e quindi anche $\langle R_1, R_2, T \rangle$ è un p-gruppo. Per i Teoremi di Sylow, esiste un coniugato P^h di P che contiene $\langle R_1, R_2, T \rangle$. In particolare $\Gamma \cap \Gamma^h$ contiene $\{R_1, R_2\} \cup \Delta$ che, a sua volta, contiene propriamente Δ. Quindi, per la scelta massimale di Δ, $\Gamma = \Gamma^h$. Ma allora $R_2 \in \Gamma$ e quindi $R_2 \in \Gamma \cap \Gamma^g \setminus \Delta = \Delta \setminus \Delta$, il che è assurdo. ∎

Osserviamo che questo risultato è stato generalizzato da Wielandt in [33]. Riportiamo qua sotto il teorema di Wielandt senza dimostrazione, e lasciamo come esercizio provare che da questo segue il Teorema di Baer-Suzuki

Teorema 9.2.7 *Sia R un sottogruppo di un gruppo finito G tale che, per ogni $g \in G$, R sia subnormale in $\langle R, R^g \rangle$. Allora R è subnormale in G.*

9.3 Caratterizzazione dei gruppi nilpotenti finiti

Il seguente teorema riduce lo studio dei gruppi nilpotenti finiti essenzialmente allo studio dei p-gruppi finiti.

Teorema 9.3.1 *Sia G un gruppo finito. Allora le seguenti affermazioni sono equivalenti:*

$NF1$ *G è nilpotente;*

$NF2$ *per ogni sottogruppo H di G, H è un sottogruppo proprio di G se e solo se H è un sottogruppo proprio di $N_G(H)$;*

$NF3$ *ogni sottogruppo di G è subnormale;*

$NF4$ *ogni sottogruppo di Sylow è normale*

$NF5$ *G è il prodotto diretto dei suoi sottogruppi di Sylow.*

DIMOSTRAZIONE. $NF2$ e $NF3$ sono equivalenti perché G è finito. $NF1$ implica $NF3$ per il Teorema 7.3.4. $NF3$ implica $NF4$ per il Corollario 9.1.8. Supponiamo sia vera $NF4$. Siano S_p un p-sottogruppo di Sylow ed S_q un q-sottogruppo di Sylow, con $S_p \neq S_q$. Per $SY3$ del Teorema 9.1.5 $p \neq q$, da cui $S_P \cap S_q = \{1\}$. Per il Lemma 6.2.1 risulta

$$\langle P, Q \rangle = P \times Q$$

da cui segue facilmente $NF5$. Infine $NF5$ implica $NF1$ per il Teorema 9.2.2 e per l'Esercizio 7.4.6. ∎

9.4 Il Teorema di Schur-Zassenhaus

Dato un gruppo finito G, un sottogruppo N di G tale che

$$(|N|, |G : N|) = 1$$

si dice **sottogruppo di Hall**.

Più precisamente, se $\pi = \pi(N)$ è l'insieme dei numeri primi che dividono $|N|$, diremo anche che N è un **π-sottogruppo di Hall**. Si osservi che i p-sottogruppi di Sylow sono esattamente i p-sottogruppi di Hall.

A differenza dei sottogruppi di Sylow, non sempre esistono π-sottogruppi di Hall per ogni sottoinsieme π di $\pi(G)$; ad esempio, il gruppo alterno A_5 non possiede $\{2, 5\}$-sottogruppi di Hall (vedi Esercizio 9.5.4). Vedremo, anzi, che l'esistenza di π-sottogruppi di Hall per ogni sottoinsieme π di $\pi(G)$ caratterizza i gruppi risolubili finiti (Teorema di Hall per i gruppi risolubili 9.4.8)

Se N è un sottogruppo di Hall di G, un **complemento di Hall** è un complemento K di N in G. Si osservi che, in questo caso, $|G : N| = |K|$, quindi se N è un sottogruppo di Hall di G, anche il suo complemento K è un sottogruppo di Hall.

Dato un sottogruppo di Hall N di G non sempre esistono complementi di Hall: l'esempio precedente mostra infatti che un 3-Sylow di A_5 non possiede complementi di Hall (che sarebbero $\{2, 5\}$-sottogruppi di Hall). Diverso è il caso in cui N è normale:

Teorema 9.4.1 (Teorema di Schur-Zassenhaus caso generale) *Sia G un gruppo finito e N un suo sottogruppo di Hall normale. Allora*

$SZ1$ esiste un complemento di N in G e

$SZ2$ se K_1 e K_2 sono due complementi di N in G, esiste un elemento n di N tale che $K_2 = K_1^n$.

Di questo teorema daremo solo la dimostrazione nel caso in cui N sia abeliano. Nell'Esercizio 9.5.14 viene data una traccia della dimostrazione dell'esistenza dei complementi nel caso generale e negli Esercizi 9.5.15 e 9.5.16 del coniugio dei complementi sotto l'ipotesi che N o, rispettivamente, G/N siano risolubili. L'ipotesi che N o G/N siano risolubili in realtà è sempre verificata: è una conseguenza del Teorema di Feit e Thompson [10] che afferma che ogni gruppo di ordine dispari è risolubile. Infatti, poiché N è di Hall, $|N|$ e $|G/N|$ sono coprimi e quindi uno dei due è di ordine dispari. Al momento non si conosce alcuna dimostrazione del Teorema di Schur-Zassenhaus, nella sua forma più generale, che non faccia uso del Teorema di Feit e Thompson.

Come abbiamo detto nell'introduzione, nella dimostrazione del Teorema di Schur-Zassenhaus cercheremo di costruire il sottogruppo cercato come stabilizzatore di un elemento sotto l'azione indotta dall'azione regolare a destra di G sull'insieme $\mathcal{T}$ dei trasversali destri di N in G. In effetti non sarà esattamente quest'azione che useremo, ma quella indotta su un G-insieme quoziente di $\mathcal{T}$.

Per comodità in quanto segue scegliamo gli indici $i \in \{1, \dots, n\}$ in modo che se

$$\{g_1, g_2, \dots, g_k\} \text{ e } \{h_1, h_2, \dots, h_k\}$$

sono trasversali di N in G, allora

$$Ng_i = Nh_i \text{ per ogni } i \in \{1, \dots, k\}.$$

Lemma 9.4.2 *Sia G un gruppo finito ed N un sottogruppo di G. Sia $\mathcal{T}$ l'insieme dei trasversali destri di N in G e $\{g_1, g_2, \dots, g_k\} \in \mathcal{T}$. Allora l'applicazione*

$$\phi \colon N^k \to \mathcal{T}$$

$$(n_1, \dots, n_k) \mapsto \{n_1 g_1, \dots, n_k g_k\}$$

è una biiezione. In particolare

$$|\mathcal{T}| = |N|^k. \tag{9.9}$$

DIMOSTRAZIONE. Se $(n_1, \dots, n_k)$ è un elemento di N^k, allora

$$Nn_i g_i = Ng_i$$

per ogni $i \in \{1, \dots, k\}$ e quindi anche

$$\{n_1 g_1, n_2 g_2, \dots, n_k g_k\}$$

è un trasversale destro di N in G. Dunque ϕ è ben definita e, come si vede facilmente, è iniettiva. Viceversa sia

$$\{h_1, h_2, \dots, h_k\}$$

un trasversale destro di N in G. Poichè

$$Ng_i = Nh_i \textit{ per ogni } i \in \{1, \dots, k\},$$

esistono degli elementi

$$n_1, n_2, \dots, n_k$$

di N tali che

$$h_i = n_i g_i \textit{ per ogni } i \in \{1, \dots, k\},$$

cioè

$$\{h_1, h_2, \dots, h_k\} = (n_1, \dots, n_k)^\phi$$

e ϕ è suriettiva. ∎

Con le notazioni del lemma precedente, sia $g \in G$ e

$$\{h_1, h_2, \ldots, h_k\} \in \mathcal{T}.$$

Allora anche

$$\{h_1 g, h_2 g, \ldots, h_k g\}$$

è un elemento di $\mathcal{T}$, infatti

$$\begin{aligned} Nh_1 g \cup Nh_2 g \cup \ldots \cup Nh_k g &= (Nh_1 \cup Nh_2 \cup \ldots \cup Nh_k)g \\ &= Gg = G. \end{aligned}$$

Dunque possiamo definire un'azione per moltiplicazione a destra di G su $\mathcal{T}$. Nella dimostrazione del Teorema di Schur-Zassenhaus definiremo un'equivalenza su $\mathcal{T}$ compatibile con l'azione di G ed useremo l'azione indotta sull'insieme quoziente. Il punto fondamentale di questa dimostrazione è che se N è un gruppo e k è un elemento di ordine coprimo con $|N|$, allora è sempre possible estrarre la radice k-esima degli elementi di N, cioè per ogni $m \in N$ esiste un elemento $n \in N$ tale che $n^k = m$ (vedi Esercizio 9.5.12).

Teorema 9.4.3 *Sia G un gruppo finito e N un suo sottogruppo di Hall abeliano e normale. Allora*

A1 esiste un complemento di N in G e

A2 se K_1 e K_2 sono due complementi di N in G, esiste un elemento n di N tale che $K_2 = K_1^n$.

Dimostrazione. Sia $\mathcal{T}$ l'insieme dei trasversali destri di N in G. Definiamo una relazione d'equivalenza $\sim$ su $\mathcal{T}$ nel modo seguente

$$\{h_1, h_2, \ldots, h_k\} \sim \{h'_1, h'_2, \ldots, h'_k\}$$

se esistono degli elementi

$$n_1, n_2, \ldots, n_k$$

di N tali che

1. $h'_i = h_i n_i$ per ogni $i \in \{1, \ldots, k\}$ e
2. $\prod_{i=1}^{k} n_i = 1$.

Si vede facilmente che $\sim$ è compatibile con l'azione di G per moltiplicazione a destra su $\mathcal{T}$. Sia infatti $g \in G$ e

$$\{h_1, h_2, \ldots, h_k\} \sim \{h'_1, h'_2, \ldots, h'_k\}$$

e siano

$$n_1, n_2, \ldots, n_k$$

elementi di N tali che

1. $h'_i = h_i n_i$ per ogni $i \in \{1, \dots, k\}$ e
2. $\prod_{i=1}^{k} n_i = 1$.

Allora

$$h'_i g = h_i n_i g = h_i g (g^{-1} n_i g)$$

quindi, essendo $N \trianglelefteq G$, risulta

$$(g^{-1} n_i g) \in N \text{ per ogni } i \in \{1, \dots, k\}$$

e

$$\prod_{i=1}^{k} g^{-1} n_i g = g^{-1} (\prod_{i=1}^{k} n_i) g = g^{-1} 1 g = 1,$$

cioè

$$\{h_1 g, h_2 g, \dots, h_k g\} \sim \{h'_1 g, h'_2 g, \dots, h'_k g\}.$$

Ne segue che possiamo definire un'azione di G sull'insieme quoziente $\mathcal{T}/\sim$ ponendo, per ogni $g \in G$ e $[\{h_1, h_2, \dots, h_k\}]_\sim \in \mathcal{T}/\sim$,

$$[\{h_1, h_2, \dots, h_k\}]_\sim^g := [\{h_1 g, h_2 g, \dots, h_k g\}]_\sim. \tag{9.10}$$

Si osservi inoltre che

$$|\mathcal{T}/\sim| = |N|. \tag{9.11}$$

Studiamo ora l'azione di N su $\mathcal{T}/\sim$, mostriamo che

$$N \text{ opera transitivamente su } \mathcal{T}/\sim, \tag{9.12}$$

cioè che se

$$[\{h_1, h_2, \dots, h_k\}]_\sim \text{ e } [\{g_1, g_2, \dots, g_k\}]_\sim$$

sono elementi di $\mathcal{T}/\sim$, allora esiste un elemento $n \in N$ tale che

$$[\{h_1 n, h_2 n, \dots, h_k n\}]_\sim = [\{g_1, g_2, \dots, g_k\}]_\sim. \tag{9.13}$$

Per il Lemma 9.4.2, esistono degli elementi

$$n_1, n_2, \dots, n_k$$

in N tali che

$$h_i = n_i g_i \text{ per ogni } i \in \{1, \dots, k\}. \tag{9.14}$$

Posto $m_i = n_i^{g_i}$ risulta $m_i \in N$ perchè $N \trianglelefteq G$ ed inoltre

$$h_i = n_i g_i = g_i g_i^{-1} n_i g_i = g_i m_i. \tag{9.15}$$

Sia

$$m = \prod_{i=1}^{k} m_i.$$

Poichè $(|N|, k) = (|N|, |G : N|) = 1$, per l'Esercizio 9.5.12, esiste $n \in N$ tale che

$$n^k = m^{-1}.$$

Poichè N è abeliano risulta

$$\prod_{i=1}^{k} m_i n = (\prod_{i=1}^{k} m_i)n^k = mm^{-1} = 1$$

e quindi

$$\begin{aligned} \{g_1, g_2, \ldots, g_k\} &\sim \{g_1 m_1 n, g_2 m_2 n, \ldots, g_k m_k n\} \\ &= \{h_1 n, h_2 n, \ldots, h_k n\}, \end{aligned}$$

da cui segue la (9.13). Da (9.12) e (9.11), si ottiene, Per il Corollario 8.2.7, che, se $\tau \in \mathcal{T}/\sim$,

$$|N : N_\tau| = |\{\tau^n | n \in N\}| = |\mathcal{T}/\sim| = |N|,$$

e quindi $N_\tau = \{1\}$. Per l'Esercizio (8.3.24) $G = G_\tau N$ e $G_\tau \cap N = N_\tau = \{1\}$, quindi G_τ è il complemento cercato.

Siano ora K_1 e K_2 due complementi di N in G. Si osservi che K_1 e K_2 sono anche due trasversali di N in G e $G_{[K_i]_\sim} = K_i$ per ogni $i = 1, 2$. Per (9.12) esiste $n \in N$ tale che $[K_1]_\sim^n = [K_2]_\sim$, quindi, per l'Esercizio 8.3.23,

$$K_2 = G_{[K_2]_\sim} = G_{[K_1]_\sim^n} = G^n_{[K_1]_\sim} = K_1^n.$$

■

Lemma 9.4.4 *Sia G un gruppo finito e risolubile. Allora, per ogni sottoinsieme π di $\pi(G)$, esistono π-sottogruppi di Hall e G agisce transitivamente per coniugio sull'insieme dei suoi π-sottogruppi di Hall*

Dimostrazione. Proviamo l'asserto per induzione sull'ordine di G. La tesi è banalmente soddisfatta se $|G| = 1$. Supponiamo quindi che $|G| > 1$ e la tesi vera per ogni gruppo risolubile di ordine minore di $|G|$. Poiché G è risolubile e non identico, esistono un primo p in $\pi(G)$ ed un p-sottogruppo non banale V normale in G. Poiché anche G/V è risolubile e $|G/V| < |G|$, G/V possiede π-sottogruppi di Hall e questi sono coniugati in G/V. Se $p \in \pi$, la tesi segue immediatamente perché la proiezione canonica $G \to G/V$ induce un isomorfismo di G-insiemi tra l'insieme dei π-sottogruppi di Hall di G e quello dei π-sottogruppi di Hall di G/V. Supponiamo quindi che $p \notin \pi$. Sia $\overline{H}$ un sottogruppo di G contenente V tale che $\overline{H}/V$ sia un π-sottogruppo di Hall di G/V. Poiché $p \notin \pi = \pi(\overline{H}/V)$, V è un p-Sylow normale di H e quindi, per il Teorema di Schur-Zassenhaus, esiste un complemento H di V in $\overline{H}$. Confrontando gli ordini, si vede immediatamente che H è un π-sottogruppo di Hall di G. Siano ora H_1 e H_2 due π-sottogruppi di Hall di G, allora H_1V/V e H_2V/V

sono π-sottogruppi di Hall di G/V e quindi, poiché V è normale in G, esiste $g \in G$ tale che

$$H_2^g V = (H_2 V)^g = H_1 V.$$

Ne segue che H_1 e H_2^g sono due complementi di V in $H_1 V$, quindi, per il Teorema di Schur-Zassenhaus, esiste $z \in V$ tale che

$$H_2^{gz} = (H_2^g)^z = H_1,$$

da cui la tesi. ∎

Per dimostrare il viceversa del Lemma 9.4.4, abbiamo bisogno di un importante risultato dovuto a Burnside.

Teorema 9.4.5 (Teorema $p^a q^b$ di Burnside) *Sia G un gruppo finito. Se $|\pi(G)| \leq 2$ G è risolubile.*

Questo teorema stato dimostrato nel 1904 da William Burnside in [8] usando la teoria dei caratteri. John Thompson osservò che con i metodi introdotti nel suo lavoro sugli N-gruppi citeN-group si poteva dare una dimostrazione del teorema di Burnside senza fare uso dei caratteri, cosa che fecero D. Goldschmidt [13], nel caso in cui entrambi i primi fossero dispari, e H. Bender [5], nel caso generale. Infine H. Matsuyama ne diede una versione semplificata in [23]. Per una dimostrazione con la teoria dei caratteri si veda [20, Theorem 3.10], per una senza si veda [27, Vol II Theorem 4.25].

Lemma 9.4.6 *Sia G un gruppo finito, N un sottogruppo normale di G, $\pi \subseteq \pi(G)$ e H un π-sottogruppo di Hall di G. Allora $N \cap H$ è un ρ-sottogruppo di Hall di N e NH/N è un σ-sottogruppo di Hall di G/N per opportuni sottoinsiemi ρ e σ di π.*

Dimostrazione. Segue immediatamente dalla Proposizione 1.1.7. ∎

Lemma 9.4.7 *Sia G un gruppo finito tale che per ogni $p \in \pi(G)$, esistono p'-sottogruppi di Hall, allora G è risolubile.*

Dimostrazione. Proviamo la tesi per induzione su G. La tesi è ovvia se $|G| = 1$. Supponiamo $|G| > 1$ e la tesi vera per ogni gruppo di ordine minore di $|G|$ che soddisfi le ipotesi. Per il Teorema di Burnside, possiamo inoltre supporre che $|\pi(G)| \geq 3$. Per ogni $p \in \pi(G)$, sia $p' := \pi(G) \setminus \{p\}$ e sia H_p un p'-sottogruppo di Hall di G. Chiaramente

$$\pi(H_p) = \pi(G) \setminus \{p\},$$

quindi

$$|H_p| < |G|.$$

Sia $q \in \pi(G) \setminus \{p\}$ e H_q un q'-sottogruppo di Hall di G. Allora $G = H_p H_q$ e quindi, per la proposizione 1.1.8, $H_p \cap H_q$ è un q'-sottogruppo di Hall di H_p. Ne segue che, per ogni $q \in \pi(H_p)$, H_p possiede q'-sottogruppi di Hall e quindi, per ipotesi induttiva, H_p è risolubile e non identico (perché $p \in \pi(G)$. Quindi esistono $r \in \pi(H_p)$ ed un r-sottogruppo normale e non identico V in H_p. Poiché $|\pi(G)| \geq 3$ esiste $q \in \pi(G) \setminus \{p, r\}$. Sia H_q un q'-sottogruppo di Hall di G. Poiché $r \neq q$, H_q contiene un r-sottogruppo di Sylow R di G. Per i Teoremi di Sylow, esiste un elemento $g \in G$ tale che

$$V \leq R^g \leq H_q^g.$$

Poiché H_q^g è ancora un q'-sottogruppo di Hall di G,

$$G = H_p H_q^g$$

e quindi

$$V^G = V^{H_p H_q^g} = V^{H_q^g} \leq H_q^g.$$

Ne segue che V^G è un sottogruppo proprio di G. Per il Lemma 9.4.6 V^G (rispettivamente G/V^G) possiede s'-sottogruppi di Hall per ogni primo $s \in \pi(V^G)$ (rispettivamente $s \in \pi(G/V^G)$. Per ipotesi induttiva V^G e G/V^G sono risolubili, quindi G è risolubile. ■

Teorema 9.4.8 *Sia G un gruppo finito, allora G è risolubile se e solo se per ogni sottoinsieme π di $\pi(G)$ esistono π-sottogruppi di Hall. In tal caso, per ogni $\pi \subseteq \pi(G)$, G agisce transitivamente per coniugio sull'insieme dei suoi π-sottogruppi di Hall*

DIMOSTRAZIONE. Segue immediatamente dal Lemma 9.4.4 e dal Lemm 9.4.7 ■

9.5 Esercizi

Esercizio 9.5.1 *Sia A un insieme di ordine t e X l'insieme dei sottoinsiemi di ordine k di A dove k è un intero positivo minore di t. Si provi che $|X| = t!/(t-k)!k!$.*

Esercizio 9.5.2 *Sia t un intero e $t = p^n m$ con p un numero primo, m ed n numeri naturali e $(p, m) = 1$. Si provi che p non divide $t!/(t-p^n)!p^n!$.* Suggerimento, si confrontino le volte che p appare come fattore del numeratore e del denominatore*).*

Esercizio 9.5.3 *Sia G un gruppo di ordine pq dove p e q sono numeri primi. Si dimostri che G ha un sottogruppo di Sylow normale.*

Esercizio 9.5.4 *Si dimostri che un gruppo semplice di ordine* 60 *non ha sottogruppi di ordine* 20.

Esercizio 9.5.5 *Sia G un gruppo e H un sottogruppo subnormale di G. Si provi che se $P \in Syl_p(G)$ allora $(P \cap H) \in Syl_p(H)$* (suggerimento: usare l'induzione sul difetto di subnormalità di H).

Esercizio 9.5.6 *Sia G un p-gruppo finito che agisce su un insieme finito Ω e tale che, per ogni $\omega \in \Omega$ esiste un sottogruppo $G(\omega)$ di G tale che ω sia l'unico punto fisso di G_ω in Ω. Si provi che*

1. *G è transitivo su Ω;*
2. *$|\Omega| \equiv 1$ mod p.*

Esercizio 9.5.7 *Sia G un gruppo, p un numero primo e $P \in Syl_p(G)$. Si provi che se P è normale in G allora P è caratteristico in G.*

Esercizio 9.5.8 *Sia G un p-gruppo finito. Si provi che esiste un sottogruppo caratteristico L di G tale G/L sia abeliano non identico.*

Esercizio 9.5.9 *Sia G un p gruppo finito e sia H un sottogruppo di G. Allora per ogni potenza p^k di p tale che $|H| \leq p^k \leq |G|$ esiste un sottogruppo K di G tale che $H \leq K \leq G$ e $|K| = p^k$. In particolare un sottogruppo massimale di G ha indice p (ed è normale).*

Esercizio 9.5.10 *Sia P un p-sottogruppo di un gruppo G. Si provi che $P \in Syl_p(G)$ se e solo se $P \in Syl_p(N_G(P))$.*

Un sottogruppo H di un gruppo G si dice *p-locale* se esiste un p-sottogruppo D tale che $H = N_G(D)$. H si dice *p-locale massimale* se H non è contenuto propriamente in nessun sottogruppo p-locale. Un problema importante per lo studio dei gruppi semplici è quello di provare che un sottogruppo p-locale massimale H di un gruppo G contiene un p-sottogruppo di Sylow di G o, in caso contrario, di determinare la struttura di H. Questo problema è noto come *pushing up problem*. Il seguente esercizio è il punto d'attacco di questo problema.

Esercizio 9.5.11 *Sia D un p-sottogruppo di un gruppo finito G ed $H = N_G(D)$. Sia $P \in Syl_p(H)$. Si provi che se esiste un sottogruppo un sottogruppo caratteristico di P che è normale in H e $P \notin Syl_p(G)$, allora H non è locale massimale.*

Esercizio 9.5.12 *Sia N un gruppo finito, k un intero coprimo con $|N|$. Si dimostri che per ogni $m \in N$ esiste un unico $n \in N$ tale che $n^k = m$.* Suggerimento: Poichè $(|N|, k) = 1$ esistono degli interi α, β tali che $\alpha|N| + \beta k = 1$. Si ponga $n = m^\beta$ e si concluda.

Si risolva direttamente, senza usare il teorema di Schur-Zassenhaus, il seguente esercizio.

Esercizio 9.5.13 *1. Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n per ogni $h, k \in \mathbf{N}$ tali che $n = hk$ e $(h, k) = 1$, allora posto $H = \langle g^k \rangle$ e $K = \langle g^h \rangle$ risulta $G = HK$ e $H \cap K = \{1\}$.*

2. Più in generale, sia A un gruppo abeliano, $A_{p_1}, \ldots, A_{p_k}$ le sue componenti primarie. Mostrare che dato un qualsiasi sottoinsieme X di $\{1., , , .k\}$ il sottogruppo

$$H = \prod_{i \in X} A_{p_i}$$

ha come complemento il sottogruppo

$$K = \prod_{j \in \{1,\ldots,k\} \setminus X} A_{p_j}.$$

Nei tre esercizi che seguono si dimostra il Teorema di Schur-Zassenhaus *modulo* il Teorema di Feit-Thompson. Vogliamo fare alcune osservazioni sulle dimostrazioni.

In ciascun esercizio si ragiona per assurdo: si suppone falsa la tesi e si considera un controesempio G di ordine minimo, quindi la tesi è verificata in tutti i sottogruppi e tutti i quozienti di G che soddisfano le ipotesi e si cerca di derivare una contraddizione. Questo è un tipo di ragionamento per induzione che viene usato costantemente in teoria dei gruppi. Ovviamente uno degli strumenti principali in questo caso è il secondo teorema di omomorfismo (è tutto quello che si usa per l'Esercizio 9.5.15).

Nell'Esercizio 9.5.14 il punto fondamentale è quando si utilizza l'argomento di Frattini per ridursi allo studio del normalizzante di un p-Sylow di N. Questo è un esempio di ragionamento locale: nella teoria locale dei gruppi, dato un gruppo G si cerca di dedurre informazioni di tipo *globale*, che riguardano cioè la struttura dell'intero gruppo, da informazioni di tipo *locale*, che riguardano la struttura dei sottogruppi p-locali (vedi premessa all'esercizio 9.5.11), dove p è un primo che divide $|G|$. L'argomento di Frattini è una chiave per poter applicare la teoria locale.

Infine una spiegazione sull'esercizio 9.5.16). Se il quoziente G/N fosse un q-gruppo, allora K_1 e K_2 sarebbero due q-Sylow di G e quindi sarebbero coniugati per il teorema di Sylow. L'idea della dimostrazione è quella di cercare di ridursi a questa situazione. Sfruttando la minimalità di G si riesce a dimostrare che K_1 e K_2 sono in un certo senso coniugati a meno dei loro q-Sylow e si mostra poi che i q-Sylow sono coniugati da un elemento di G che lascia fisso tutto il resto.

Esercizio 9.5.14 *Sia G un gruppo finito ed N un suo sottogruppo di Hall normale. Allora esistono complementi di N in G.*

Supponiamo falso l'asserto e sia G un controesempio di ordine minimo, cioè se H è un gruppo finito con $|H| < |G|$, ed M è un sottogruppo di Hall di H e normale, allora esistono dei complementi.

Passo 1 *Si provi che se L è un sottogruppo proprio di N (cioè $\{1\} < L < N$), allora L non è normale in G* (suggerimento: Se $L \trianglelefteq G$, si studi il quoziente G/L che ha ordine strettamente minore di G).

Passo 2 *Sia p un divisore primo di $|N|$ e $P \in Syl_p(N)$. Si dimostri che $G = NN_g(P)$.*

Passo 3 *Sia $\overline{G} = N_G(P)$ e $\overline{N} = N \cap N_G(P)$. Si provi che $\overline{N}$ è un sottogruppo di Hall di $\overline{G}$ e normale.*

Passo 4 *Si provi che esiste un complemento K di $\overline{N}$ in $\overline{G}$.* (Suggerimento: si distinguano i due casi $\overline{G} < G$ e $\overline{G} = G$. Nel primo caso la tesi segue dalla minimalità di G. Nel secondo caso si deduca dal passo 1 che N è un p-gruppo privo di sottogruppi caratteristici. In particolare $\Phi(N) = \{1\}$ e quindi N è abeliano elementare. Si applichi quindi il teorema 9.4.3).

Passo 5 *Si provi che K è un complemento di N in G.* (Suggerimento: si applichi il secondo teorema di omomorfismo e si calcolino gli ordini e gli indici dei gruppi trovati).

Esercizio 9.5.15 *Sia G un gruppo finito ed N un suo sottogruppo di Hall normale e risolubile. Allora, se K_1 e K_2 sono complementi di N in G, esiste un elemento n di N tale che $K_2 = K_1^n$.*

Passo 1 *Si supponga G un controesempio minimo e, come nell'esercizio precedente, si dimostri che nessun sottogruppo proprio di N è normale in G.*

Passo 2 *Per l'esercizio* **??** *N è abeliano e si concluda per il teorema 9.4.3.*

Esercizio 9.5.16 *Sia G un gruppo finito ed N un suo sottogruppo di Hall normale tale che G/N sia risolubile. Allora, se K_1 e K_2 sono complementi di N in G, esiste un elemento n di N tale che $K_2 = K_1^n$.*

Sia G un controesempio di ordine minimo.

Passo 1 *Sia q un divisore proprio di $|G/G'|$ e sia $\overline{G} = G'(q)$ (cfr. es 8.3.9). Allora $|\overline{G}| < |G|$ e N è un sottogruppo di Hall di $\overline{G}$ e normale in $\overline{G}$.*

Passo 2 *Sia $\overline{K}_i = K_i \cap \overline{G}$ ($i = 1, 2$). Si provi che per ogni $i \in \{1, 2\}$*

1. *$\overline{K}_i \trianglelefteq K_i$;*
2. *$\overline{K}_i$ è un complemento di N in $\overline{G}$;*
3. *per la minimalità di G, esiste un elemento s di N tale che ${\overline{K}_1}^s = \overline{K}_2$.*

Passo 3 *Sia $K_3 = K_1^s$. Si provi che*

1. *$K_3 \cap \overline{G} = \overline{K}_2$ e quindi $\overline{K}_2 \trianglelefteq K_3$;*
2. *esistono $Q_2, Q_3 \in Syl_q(G)$ tali che $K_i = \overline{K}_2 Q_i$.*

Passo 4 *Si deduca dal passo 2.1 e dal passo 3 che* $Q_2, Q_3 \in Syl_q(N_G(\bar{K}_2))$.

Passo 5 *Esiste* $t \in N_G(\bar{K}_2)$ *tale che* $Q_1^t = Q_2$.

Passo 6 *Posto* $g = st$, *si provi che* $K_1^g = K_2$.

Passo 7 *Si concluda mostrando che, poiché* $G = K_1N$, *esiste un elemento* $n \in N$ *tale che* $K_1^n = K_2$.

Capitolo 10

Azioni di gruppi su gruppi

Uno dei metodi più efficaci per indagare la struttura di un gruppo G è quello di studiare le azioni indotte per coniugio dai suoi sottogruppi sulle sezioni di G normalizzate da questi. Queste sono un caso di azioni di un gruppo su un gruppo, cioè di rappresentazioni $\rho\colon A \to Aut(B)$ di un gruppo A su un gruppo B. D'altra parte, nella sezione sui prodotti semidiretti, abbiamo visto che possiamo sempre ridurci al caso in cui A e B sono sottogruppi di un gruppo G, A normalizza B e ρ è l'azione indotta dal coniugio. Se $\rho\colon A \to Aut(B)$ è un'azione di un gruppo A su un gruppo B, conviene indicare con $Aut_A(B)$ l'immagine di A via ρ. Chiaramente

$$Aut_A(B) \cong A/\ker(\rho). \tag{10.1}$$

Nel caso in cui A e B sono sottogruppi di un gruppo A, con A che normalizza B e ρ è l'azione indotta dal coniugio, $\ker(\rho) = C_A(B)$ e quindi l'equazione (10.2) diviene

$$Aut_A(B) \cong A/C_A(B). \tag{10.2}$$

10.1 L'architettura di un gruppo finito

L'argomento di questa sezione è quello che spesso viene chiamato architettura di un gruppo finito: proveremo infatti che la struttura di ogni gruppo finito è controllata da certi sottogruppi caratteristici dalla struttura più semplice (come il sottogruppo di Fitting nei gruppi risolubili finiti e, pi in generale, il sottogruppo di Fitting Generalizzato nei gruppi finiti o i sottogruppi critici nei p-gruppi finiti) e dall'azione che questo gruppo induce per coniugio su questi sottogruppi caratteristici. Nelle restanti sezioni studieremo le azioni coprime e le azioni unipotenti che corrispondono alle azioni di un gruppo di automorfismi semisemplici (risp. unipotenti) di uno spazio vettoriale.

10.1.1 *cc*-sottogruppi

Sia G un gruppo finito ed F un sottogruppo di G. Diremo che F è un ***cc*-sottogruppo** [1] di G (dall'Inglese *centraliser closed*) se F contiene il proprio centralizzante, in simboli

$$C_G(F) \leq F. \tag{10.3}$$

La proprietà fondamentale dei *cc*-sottogruppi normali di G è che essi controllano la struttura di G: abbiamo visto infatti che, se N è un sottogruppo normale di G, allora G agisce per coniugio su N, il nucleo di questa azione è $C_G(N)$, dunque $G/C_G(N)$ è isomorfo ad un sottogruppo di $Aut(N)$ e quindi N controlla il quoziente $G/C_G(N)$ tramite $Aut(N)$. Ora, se F è normale ed è anche un *cc*-sottogruppo di G, $C_G(F) = Z(F)$ e quindi le informazioni su $C_G(F)$ (che non sono visibili in $Aut(F)$), vengono recuperate dalla struttura di F. A titolo di esempio citiamo il seguente lemma, la cui dimostrazione è elementare e lasciata per esercizio:

Lemma 10.1.1 *Se F è un cc-sottogruppo normale di un gruppo G, allora $|G|$ divide*

$$\frac{|F| \cdot |Aut(F)|}{[F : Z(F)]}.$$

Una strategia naturale, quindi, quella di cercare *cc*-sottogruppi normali di G che abbiano la struttura più elementare possibile. Che tali sottogruppi esistano, è un segno della straordinaria benevolenza del dio della matematica.

Il lemma seguente un'immediata conseguenza del fatto che la mappa che ad ogni sottogruppo associa il suo centralizzante inverte le inclusioni.

Lemma 10.1.2 *Se H è un cc-sottogruppo di G, ogni sottogruppo di G contenente H è un cc-sottogruppo.*

10.1.2 Il Teorema di Fitting

In questa sezione mostreremo che ogni gruppo finito risolubile possiede un *cc*-sottogruppo caratteristico e nilpotente.

Il p-radicale

Sia G un gruppo e P_1, P_2 due p-sottogruppi normali di G. Allora, per le proposizioni 1.1.7 e 1.1.8 $\langle P_1, P_2 \rangle = P_1P_2$ è ancora un p-sottogruppo normale di G. Segue da ciò che se $O_p(G)$ è il sottogruppo generato da tutti i p-sottogruppi normali di G, $O_p(G)$ è ancora un p-sottogruppo normale di G. $O_p(G)$ si dice p-**radicale** di G.

Esempi

[1] Attenzione, la definizione di *cc*-sottogruppo non è di uso comune, anzi, alcuni autori definiscono un CC-sottogruppo come un sottogruppo che contiene i centralizzanti di tutti i suoi elementi, una condizione evidentemente molto più forte della nostra.

- $O_3(S_3) = A_3$,
- $O_2(S_3) = \{1\}$,
- $O_2(D_8) = D_8$,
- $O_5(D_{30})$ è ciclico di ordine 5,
- $O_3(D_{30})$ è ciclico di ordine 3,
- $O_2(D_{30}) = \{1\}$.

Diamo alcune proprietà elementari del p-radicale:

Proposizione 10.1.3 *$O_p(G)$ è un sottogruppo caratteristico di G.*

DIMOSTRAZIONE. Segue immediatamente dal fatto che ogni automorfismo di G manda p-sottogruppi normali in p-sottogruppi normali. ∎

Corollario 10.1.4 *Se N è un sottogruppo normale di G, allora $O_p(N) \leq O_p(G)$.*

DIMOSTRAZIONE. $O_p(N) \leq_{char} N \trianglelefteq G$, da cui $O_p(N) \trianglelefteq G$ e quindi la tesi. ∎

Proposizione 10.1.5 *$O_p(G/O_p(G)) = \{1\}$*

DIMOSTRAZIONE. Segue immediatamente dal Teorema di Corrispondenza e dal Teorema di Lagrange ∎

Proposizione 10.1.6 *Se p e q sono primi distinti $[O_p(G), O_q(G)] = \{1\}$.*

DIMOSTRAZIONE. Segue immediatamente dal Lemma 6.2.1, tenendo presente che $O_p(G)$ ed $O_q(G)$ sono sottogruppi normali ed hanno intersezione identica. ∎

Il Sottogruppo di Fitting

Sia ora

$$F(G) = \langle O_p(G) | p \text{ divide } |G| \rangle.$$

Per la Proposizione 10.1.6 e il Teorema 9.3.1 $F(G)$ è un sottogruppo nilpotente. $F(G)$ si dice **sottogruppo di Fitting** o **radicale nilpotente** di G.

Proposizione 10.1.7 *$F(G)$ è caratteristico in G ed è il più grande sottogruppo normale nilpotente di G*

DIMOSTRAZIONE. Abbiamo già visto che $F(G)$ è un sottogruppo nilpotente ed è normale (anzi caratteristico) perchè è generato da sottogruppi caratteristici. Sia ora N un sottogruppo normale nilpotente di G. Dal teorema 9.3.1 segue che, per ogni divisore primo p di N, $O_p(N)$ è un p-sottogruppo di Sylow di N e quindi, per il corollario 10.1.4,

$$N = \langle O_p(N) | p \text{ divide } |N| \rangle \leq F(G).$$

■

Lemma 10.1.8 *Sia G un gruppo finito, allora $F(G)$ è generato da tutti i sottogruppi subnormali nilpotenti di G.*

DIMOSTRAZIONE. Sia N il sottogruppo di G generato dai sottogruppi subnormali nilpotenti di G. Allora N contiene tutti i sottogruppi normali nilpotenti di G e quindi anche $F(G)$. Viceversa proviamo che $F(G)$ contiene ogni sottogruppo subnormale nilpotente di G, da cui seguir che $N \leq F(G)$. Sia L un sottogruppo subnormale nilpotente di G proviamo, per induzione sul difetto di subnormalit di L in G che $L \leq F(G)$. Sia d tale difetto. Se $d = 1$, allora, L è un sottogruppo normale nilpotente di G e quindi contenuto in $F(G)$ per la Proposizione 10.1.7. Supponiamo che $d > 1$ e che la tesi sia vera per $d - 1$. Sia $M := L[L, G]$ la chiusura normale di L in G. Per il Teorema 7.3.1, L è subnormale di difetto $d - 1$ in M, quindi, per ipotesi induttiva, $L \leq F(M)$. D'altra parte $F(M)$ è un sottogruppo caratteristico di M ed M è normale in G, quindi, per la Proposizione 8.1.9 $F(M)$ è normale in G e dunque, essendo $F(M)$ nilpotente, $F(M) \leq F(G)$, da cui la tesi. ■

Il Teorema di Fitting

Teorema 10.1.9 *(Teorema di Fitting) Sia G un gruppo risolubile finito. Allora*

$$C_G(F(G)) \leq F(G) \tag{10.4}$$

DIMOSTRAZIONE. Poniamo $F = F(G)$, $C = C_G(F)$ e $Z = F \cap C$. Osserviamo che $Z = Z(F)$ e quindi Z è caratteristico in G. Supponiamo per assurdo che $C \not\leq F$. Allora l'insieme X dei sottogruppi subnormali di C che contengono propriamente Z è non vuoto. Sia A un elemento minimale di X. Per il Teorema di Corrispondenza, A/Z è un sottogruppo normale minimale non identico di C/Z. Poiché G è risolubile, anche G/Z e C/Z lo sono, quindi, per la minimalità di A/Z, A/Z è abeliano. Ne segue che

$$[[A, A], A] \leq [Z, A] \leq [F, C] = \{1\}$$

e quindi A è nilpotente. D'altra parte $A \lhd\lhd C \trianglelefteq G$, quindi A è subnormale in G. Per la proposizione 10.1.8, segue che $A \leq F = F(G)$, da cui, essendo $A \leq C$, risulta $A \leq Z$, cioè $A/Z = \{1\}$, contro la scelta di A. ■

10.1.3 Il Teorema di Bender-Fitting

La dimostrazione del Teorema di Fitting suggerisce come estenderlo in modo naturale lasciando cadere l'ipotesi di risolubilità. Infatti, il punto critico nella dimostrazione del Teorema di Fitting è che, se $C(F(G)$ non è contenuto in $F(G)$, allora $C(F(G)/Z(F(G)$ contiene un sottogruppo subnormale minimale non identico $A/Z(F(G))$ che, essendo G risolubile, deve essere abeliano. Senza l'ipotesi di risolubilità di G, il sottogruppo $A/Z(F(G))$ è un gruppo semplice, ma non necessariamente abeliano. Quindi, se si vuole generalizzare il Teorema di Fitting ad un qualsiasi gruppo finito, bisogna sostituire il sottogruppo di Fitting con un sottogruppo più grande che comprenda anche questi casi. Tale sottogruppo è il sottogruppo di Fitting Generalizzato, introdotto da Helmut Bender e generato dai sottogruppi subnormali nilpotenti e dalle componenti. Sorprendentemente, le proprietà delle componenti fanno sì che il sottogruppo di Fitting Generalizzato abbia ancora una struttura elementare il cui studio si riduce essenzialmente a quello del Fitting e di gruppi semplici non abeliani.

Componenti

Sia K un gruppo. K si dice **quasisemplice** se K è perfetto e $K/Z(K)$ è semplice.

Proposizione 10.1.10 *Sia K un gruppo quasisemplice ed N un sottogruppo normale proprio di K. Allora $N \leq Z(K)$.*

DIMOSTRAZIONE. Supponiamo che $N \not\leq Z(K)$. Poichè K/Z è semplice, segue, per il Teorema di Corrispondenza, che $K = NZ$. Dal Lemma 6.2.1 e dall'esercizio 6.3.6 segue allora

$$N \geq [K, N] \geq [K, NZ] = [K, K] = K,$$

da cui la tesi. ∎

Dalla Proposizione 10.1.10, segue che un gruppo quasisemplice un'estensione centrale non spezzante di un gruppo semplice. Dalla classificazione dei gruppi semplici finiti segue anche la classificazione dei gruppi quasisemplici finiti: in generale il centro di un gruppo quasisemplice finito risulta essere molto piccolo, quasi sempre ciclico e spesso banale.

Proposizione 10.1.11 *Sia K un gruppo tale che $K/Z(K)$ sia semplice non abeliano. Allora $K = K'Z(K)$ e K' è quasisemplice.*

DIMOSTRAZIONE. Poichè K non è risolubile,

$$K' \not\leq Z(K),$$

quindi $K'Z(K)/Z(K)$ è un sottogruppo normale non identico di $K/Z(K)$. Ma $K/Z(K)$ è semplice, quindi $K'Z(K)/Z(K) = K/Z(K)$, da cui

$$K'Z(K) = K.$$

Segue allora che

$$[K', K'] = [K'Z(K), K'Z(K)] = [K, K] = K'$$

e quindi K' è perfetto. Per il Secondo Teorema di Omomorfismo

$$K'/(K' \cap Z(K)) \cong K'Z(K)/Z(K) = K/Z(K).$$

Poichè $K/Z(K)$ è semplice, segue che $K' \cap Z(K) = Z(K')$ e quindi K' è quasisemplice. ∎

Lemma 10.1.12 *Se K un gruppo quasisemplice, l'azione indotta da $Aut(K)$ su $K/Z(K)$ è fedele.*

DIMOSTRAZIONE. Se T è il nucleo dell'azione indotta da $Aut(K)$ su $K/Z(K)$, allora

$$[K, T] \leq Z(K).$$

Quindi

$$[T, K, K] = [K, T, K] \leq [Z(K), K] = \{1\}.$$

Per il Lemma dei Tre Sottogruppi (Esercizio 6.3.9), segue che

$$[K, T] = [K, K, T] = \{1\}$$

∎

Sia G un gruppo. Una **componente** di G è un sottogruppo quasisemplice e subnormale. La proprietà più importante delle componenti è la seguente:

Teorema 10.1.13 *Sia K una componente di un gruppo G ed H un sottogruppo subnormale di G non contenente K. Allora $[H, K] = \{1\}$.*

DIMOSTRAZIONE. Possiamo supporre $G = \langle K, H \rangle$. Sia N la chiusura normale di H in G. Allora $G = \langle K, H \rangle = KN$ e, poichè H è subnormale in G, $N < G$; in particolare $K \not\leq N$. Proviamo, per induzione sul difetto di subnormalità n di K in G, che $[N, K] = \{1\}$. Se $n = 1$, allora $K \trianglelefteq G$ e, per il Lemma 6.2.1 e la Proposizione 10.1.10, risulta

$$[N, K] \leq N \cap K \leq Z(K),$$

da cui

$$[K, N, K] = [N, K, K] \leq [Z(K), K] = \{1\},$$

quindi, poiché K è perfetto, dal Lemma dei Tre Sottogruppi (esercizio 6.3.9), segue che

$$[K, N] = [K, K, N] = \{1\}.$$

Supponiamo ora che $n > 1$ e la tesi vera per $n-1$. Sia G_0 la chiusura normale di K in G e $N_0 = G_0 \cap N$. Allora

$$[K, N] \leq [G_0, N] \leq N_0.$$

Poichè K ha difetto di subnormalità $n-1$ in G_0 ed N_0 è un sottogruppo normale di G_0 non contenente K, per ipotesi induttiva risulta

$$[N_0, K] = \{1\},$$

da cui

$$[N, K, K] = [K, N, K] \leq [N_0, K] = \{1\}.$$

Ancora dal Lemma dei Tre Sottogruppi segue che

$$[K, N] = [K, K, N] = \{1\}.$$

Dunque $[K, N] = \{1\}$, da cui la tesi essendo $H \leq N$. ∎

Corollario 10.1.14 *Sia G un gruppo finito.*

1. *Se K_1 e K_2 sono due componenti distinte di G, allora $[K_1, K_2] = \{1\}$.*
2. *Se K è una componente di G, allora $[F(G), K] = \{1\}$.*

DIMOSTRAZIONE. Segue immediatamente dal Teorema 10.1.13. ∎

Il Sottogruppo di Fitting generalizzato ed il Teorema di Bender-Fitting

Sia G un gruppo finito. Poniamo

$$E(G) := \langle K | K \text{ è una componente di } G \rangle$$

e

$$F^*(G) = F(G)E(G).$$

Il sottogruppo $F^*(G)$ si dice **sottogruppo di Fitting generalizzato** di G. $E(G)$ si chiama **sottogruppo di Bender** di G. È immediato verificare che sia $E(G)$ che $F^*(G)$ sono sottogruppi caratteristici di G.

Teorema 10.1.15 *(Teorema di Bender-Fitting) Sia G un gruppo finito, allora*

$$C_G(F^*(G)) \leq F^*(G).$$

DIMOSTRAZIONE. Come nella dimostrazione del Teorema di Fitting, poniamo $F^* = F^*(G)$, $C = C_G(F^*)$, $Z = F^* \cap C$ e supponiamo per assurdo che $C \not\leq F^*$. Sia $A \leq G$ tale che A/Z sia un sottogruppo subnormale minimale non identico di C/Z. Proviamo che $A \leq F^*$, da cui seguirà una contraddizione come nella dimostrazione del Teorema di Fitting. Se A/Z è abeliano, allora

$$A \leq F(G) \leq F^*.$$

Se A/Z è semplice non abeliano, per la Proposizione 10.1.11, A' è una componente (e quindi è contenuta in F^*) e

$$A = A'Z \leq F^*.$$

■

Automorfismi del sottogruppo di Fitting generalizzato

Per il Teorema di Bender-Fitting e la discussione all'inizio di questa sezione, abbiamo visto che, se G è un gruppo finito G è controllato da $F^*(G)$ via $Aut(F^*(G))$. Vogliamo vedere in modo più dettagliato $Aut(F^*(G))$.

Se ϕ è un automorfismo di un gruppo G ed L è un sottogruppo caratteristico di G, indichiamo con $\phi|_L$ la restrizione di ϕ a L. Chiaramente $\phi|_L \in Aut(L)$ e l'applicazione che a ciascun $\phi \in Aut(G)$ associa la sua restrizione a L è un omomorfismo di gruppi da $Aut(G)$ a $Aut(L)$. Il seguente Lemma, la cui dimostrazione elementare, mostra come, nel caso in cui un gruppo G sia generato da sottogruppi caratteristici, possiamo ricostruire $Aut(G)$ dai gruppi di automorfismi di questi sottogruppi.

Lemma 10.1.16 *Sia G un gruppo finito e siano $L_1, \ldots, L_k$ sottogruppi caratteristici di G tali che*

$$G = \langle L_1, \ldots, L_k \rangle.$$

Allora l'applicazione

$$\begin{aligned} \tau\colon Aut(G) &\to \prod_{i=1}^{k} Aut(L_i) \\ \phi &\mapsto (\phi|_{L_1}, \ldots, \phi|_{L_k}) \end{aligned}$$

è un omomorfismo iniettivo di gruppi.

Segue immediatamente che

$$Aut(F^*(G)) \text{ è isomorfo ad un sottogruppo di } Aut(E(G)) \times Aut(F(G)).$$

Ora, se $K_1, \ldots K_t$ sono un sistema di rappresentanti delle classi di isomorfismo delle componenti di G, e H_i è il sottogruppo di G generato da tutte le

componenti di G isomorfe a K_i, allora, per ogni $i \in \{1, \ldots, k\}$, H_i è caratteristico in G,

$$E(G) = \prod_{i=1}^{k} H_i$$

e quindi

$$Aut(E(G)) \textit{è isomorfo ad un sottogruppo di } \prod_{i=1}^{k} Aut(H_i).$$

Fissiamo ora $i \in \{1, \ldots, k\}$. Un automorfismo di H_i manda componenti isomorfe a K_i in componenti isomorfe a K_i, quindi induce una permutazione dell'insieme T_i di queste componenti. Abbiamo quindi un'azione di $Aut(H_i)$ sull'insieme T_i, avente per nucleo l'intersezione degli stabilizzatori in H_i degli elementi di T_i. Si vede facilmente che tale nucleo è isomorfo al prodotto diretto

$$\prod_{K \in T_i} Aut(K)$$

e che qualsiasi permutazione dell'insieme T_i è indotta da un automorfismo di H_i. Infatti se K e $\overline{K}$ sono elementi di T_i, allora esiste un isomorfismo di gruppi ϕ tra K e $\overline{K}$. Sia τ l'automorfismo di H_i che agisce come ϕ sugli elementi di K, come ϕ^{-1} sugli elementi di $\overline{K}$ e come l'applicazione identica su ciascuna altra componente di H_i, allora τ scambia K con $\overline{K}$. Ne segue che $Aut(H_i)$ è isomorfo al prodotto semidiretto di $|T_i|$-copie di $Aut(K_i)$ con il gruppo delle permutazioni S_{T_i} dell'insieme T_i (o, in altri termini, al prodotto intrecciato di $Aut(K_i)$ con S_{T_i}).

Questo riduce lo studio di $Aut(E(G))$ allo studio degli automorfismi delle componenti. Per il Lemma 10.1.12, il gruppo degli automorfismi di una componente è isomorfo ad un sottogruppo del gruppo di automorfismi della sua sezione semplice non abeliana. Dalla classificazione dei gruppi semplici finiti segue anche la classificazione dei loro gruppi di automorfismi, quindi, in teoria, abbiamo un controllo completo su $Aut(E(G))$. Per inciso, gli automorfismi di un gruppo semplice non abeliano sono quasi sempre interni. Nelle Sezioni **??** e **??** calcoleremo i gruppi degli automorfismi dei gruppi speciali lineari proiettivi ne dei gruppi simplettici proiettivi. In ogni caso, se G è un gruppo semplice finito, il gruppo degli automorfismi esterni $Out(G)$ di un gruppo semplice G è sempre risolubile (questa, per inciso, è la Congettura di Schreier che, finora, è stata dimostrata solo come conseguenza della classificazione dei gruppi semplici finiti).

In modo analogo, anche $F(G)$ si decompone come il prodotto diretto delle sue componenti primarie, che sono caratteristiche in $F(G)$ e quindi

$$Aut(F(G)) \textit{è isomorfo ad un sottogruppo di } \prod_{p \in \pi(G)} Aut(O_p(G)).$$

Purtroppo, nonostante la loro struttura sia a prima vista facile da studiare (se non altro per l'abbondanza di sottogruppi normali), una classificazione dei p-gruppi finiti non sembra possibile (e quindi, tantomeno, quella dei loro gruppi di automorfismi). D'altra parte, come vedremo nella prossima sottosezione, ogni p gruppo finito possiede *cc*-sottogruppi caratteristici con una struttura che, a volte, può essere più semplice da studiare.

10.1.4 Sottogruppi critici

Sia p un numero primo e sia G un p-gruppo finito. Un **sottogruppo critico** di G è un *cc*-sottogruppo caratteristico F di G tale che

$$[G, F]\Phi(F) \leq Z(F).$$

Proposizione 10.1.17 *Siano p un numero primo e G un p-gruppo finito, allora G possiede sottogruppi critici.*

DIMOSTRAZIONE. Sia R l'insieme dei sottogruppi caratteristici T di G tali che $[G, T]\Phi(T) \leq Z(T)$. T è non vuoto perché contiene il sottogruppo identico di G. Sia F un sottogruppo massimale, per inclusione, contenuto in T. Proviamo che F è un *cc*-sottogruppo. Sia $C := C_G(F)$ e supponiamo per assurdo che C non sia contenuto in F. Sia $S := C \cap F = Z(F)$. Chiaramente F, S e C sono sottogruppi caratteristici di G e G/S è ancora un p-gruppo. Poiché C/S è normale in G/S, dal Teorema 9.2.1 segue che $C/S \cap Z(G/S)$ è un sottogruppo centrale non identico di G/S e quindi anche $\Omega_1(C/S \cap Z(G/S))$è un sottogruppo centrale non identico di G/S. Sia L un sottogruppo di G contenente S tale che $L/S = \Omega_1(C/S \cap Z(G/S))$. Poiché sia $[L, G]$ che $[F, G]$ sono contenuti in S, segue che

$$[LF, G] \leq S$$

quindi LF/S è centrale in G/S, (in particolare abeliano) e

$$[LF, S] \leq [L, S] \leq [C, F] = \{1\},$$

da cui segue che

$$[LF, G] \leq Z(LF). \tag{10.5}$$

D'altra parte sia F/S che L/S sono abeliani elementari (il primo dal Teorema 9.2.4 perché S contiene $\Phi(F)$, il secondo per la scelta di L) e quindi anche FL/S è abeliano elementare. Dal Teorema 9.2.4 segue che

$$\Phi(FL) \leq S \leq Z(FL). \tag{10.6}$$

Per (10.5) e (10.6), segue che FL è contenuto in T, contro la scelta massimale di F. ∎

10.1.5 Esercizi

Esercizio 10.1.18 *Sia G un gruppo. Si provi che se H è un p-sottogruppo subnormale di G, allora $H \leq O_p(G)$*

Esercizio 10.1.19 *Un sottogruppo N di un gruppo G si dice p-***locale** *se esiste un p-sottogruppo non identico T tale che $N = N_G(T)$. Si provi che:*

1. *se N è un sottogruppo p-locale, allora $N_G(N)$ è un sottogruppo p-locale;*

2. *se N è un sottogruppo p-locale massimale, allora $N = N_G(N)$.*

Esercizio 10.1.20 *Sia G un gruppo. Si provi che se H è un sottogruppo subnormale nilpotente di G, allora $H \leq F(G)$*

Esercizio 10.1.21 *Si determinino tutti i gruppi finiti risolubili G con $|F(G)| = 5$*

Esercizio 10.1.22 *Si determinino tutti i gruppi finiti risolubili con $F(G) \cong C_2 \times C_2$.*

Esercizio 10.1.23 *Si provi che se A è un sottogruppo caratteristico minimale di un gruppo finito G allora esistono dei sottogruppi semplici subnormali $S_1, S_2, \ldots, S_t$ tali che*

1. *$A = S_1 \times S_2 \times \ldots \times S_t$ e*

2. *G agisce transitivamente per coniugio su $\{S_1, S_2, \ldots, S_t\}$.*

Esercizio 10.1.24 *Sia N un sottogruppo subnormale di un gruppo G e K una componente di N. Si provi che K è una componente di G.*

Esercizio 10.1.25 *Si provi che un sottogruppo subnormale minimale di un gruppo finito G è contenuto in $F^*(G)$.*

Esercizio 10.1.26 *Sia G un gruppo finito, si provi che se H è un cc-sottogruppo normale di G contenente $F(G)$, allora H contiene $F^*(G)$*

Esercizio 10.1.27 *Sia G un gruppo finito, si provi che le seguenti condizioni sono equivalenti:*

1. *$F^*(G)$ è un p-gruppo;*

2. *$F^*(G) = O_p(G)$;*

3. *$C_G(O_p(G)) \leq O_p(G)$.*

10.2 Azioni coprime e azioni unipotenti

Nella sezione precedente abbiamo visto che un maggior ostacolo per lo studio dei gruppi finiti è costituito dallo studio dei gruppi degli automorfismi dei gruppi che hanno per ordine la potenza di un numero primo, non essendoci per questi alcuna classificazione.

D'altra parte, se p è un numero primo, un automorfismo di un p-gruppo finito ammette una decomposizione analoga alla ben nota decomposizione moltiplicativa di Jordan-Chevalley degli automorfismi di uno spazio vettoriale (vedi [**?**]). Questa analogia, che chiariremo in questa sezione, non dovrebbe sorprendere, perché il gruppo $GL(V)$, degli automorfismi di uno spazio vettoriale V, rispetta la struttura additiva di V e quindi agisce sul gruppo additivo $(V, +)$. Nel caso di un automorfismo α di un p-gruppo finito, vedremo che questa decomposizione coincide con la decomposizione di α nella sua p'-parte e nella sua p-parte. In particolare se α è un automorfismo di uno spazio vettoriale di dimensione finita su un campo finito di caratteristica p, questa è esattamente la decomposizione moltiplicativa di Jordan-Chevalley. Otterremo questo risultato dal contesto più generale delle azioni coprime e mostreremo inoltre che, a differenza della p-parte, la p'-parte può essere efficacemente controllata.

Sia, quindi, V uno spazio vettoriale di dimensione finita su un campo F. Un automorfismo σ di V si dice **semisemplice** se ogni sottospazio s-invariante di V ammette un complemento s-invariante. In particolare, se il polinomio minimo di σ si fattorizza in $F[x]$ come prodotto di fattori lineari, V è somma diretta di autospazi per σ.

All'estremo opposto, un automorfismo v si dice **unipotente** se il suo unico autovalore è 1. Si osservi che questo equivale a dire che esiste una bandiera

$$V_0 := \{0\} \leq V_1 \leq \ldots \leq V_n := V$$

di sottospazi v-invarianti, tali che, per ogni $i \in \{1, \ldots, n\}$, l'automorfismo v induce l'identità su ciascuno spazio quoziente V_i/V_{i-1}. In questo caso, può accadere che nessun sottospazio v-invariante abbia un complemento che sia ancora v-invariante: per esempio se V è uno spazio di dimensione 2, (v_1, v_2) è una base di V e v è l'automorfismo che fissa v_1 e manda v_2 in $v_1 + v_2$, allora $\langle v_1 \rangle$ è l'unico sottospazio v-invariante di V, ma non ha complementi v-invarianti.

Più precisamente, si può vedere che, se σ è un automorfismo semisemplice di V, allora $C_V(\sigma)$ è l'autospazio di autovalore 1, inoltre, se

$$[V, \sigma] := \{-v + v^\sigma | v \in V\},$$

allora anche $[V, \sigma]$ è un sottospazio σ-invariante di V e V si decompone nel modo seguente:

$$V = C_V(\sigma) \oplus [V, \sigma], \tag{10.7}$$

in particolare la serie "centrale" discendente si ferma al primo passo:

$$V \geq [V, \sigma] = [[V, \sigma], \sigma]$$

(si osservi che, se il polinomio minimo di σ si fattorizza completamente in $F[x]$, $[V, \sigma]$ è la somma degli autospazi relativi ad autovalori diversi da 1).

Al contrario, se ν è un automorfismo unipotente di V, esiste un intero positivo k tale che $[V,_k \nu] = \{0\}$, ovvero la serie centrale discendente

$$V \geq [V, \sigma] \geq [V, \sigma, \sigma] \geq \dots$$

termina con lo spazio nullo.

Se F è perfetto (in particolare se F è finito o algebricamente chiuso), ogni automorfismo di V ammette una decomposizione (moltiplicativa) di Jordan-Chevalley: cioè, per ogni $\alpha \in GL(V)$, esistono e sono unici un automorfismo semisemplice α_s ed un automorfisno unipotente α_u, tali che

1. $\alpha = \alpha_s \alpha_u$,
2. $\alpha_s \alpha_u = \alpha_u \alpha_s$ e
3. sia α_s che α_u si possono esprimere come polinomi in α.

Se F è finito, vedremo che un automorfismo di V è semisemplice se e solo se il suo ordine è coprimo con p (e quindi con $|V|$) ed è unipotente se e solo se il suo ordine è una potenza di p. In questo caso la decomposizione di Jordan-Chevalley assume un aspetto particolarmente semplice: se p è la caratteristica di F, e $|\alpha| = p^s m$ con $(m, p) = 1$, allora

$$\alpha_s = \alpha^{ap^s} \text{ e } \alpha_u = \alpha^{bm}, \tag{10.8}$$

dove a e b sono interi tali che $ap^s + bm = 1$.

Per vedere in concreto l'esempio più semplice, supponiamo che F sia finito e τ sia un'involuzione in $GL(V)$. Poiché $\tau^2 = 1$, il polinomio minimo di τ divide il polinomio $x^2 - 1$ i cui fattori lineari sono uguali o distinti a seconda che la caratteristica di F sia pari o dispari.

Se la caratteristica di F è dispari, per ogni $v \in V$,

$$(-v + v^\tau)^\tau = -v^\tau + v^{\tau^2} = -v^\tau + v = -(-v + v^\tau),$$

quindi gli elementi di $[V, \tau]$ sono autovettori per τ relativo all'autovalore -1. In particolare

$$[V, \tau] \cap C_V(\tau) = \{0\}.$$

Poiché, per ogni $v \in V$,

$$v = 1/2(v + v^\tau) - 1/2(-v + v^\tau)$$

e

$$(v + v^\tau)^\tau = v^\tau + v^{\tau^2} = v^\tau + v = v + v^\tau,$$

segue che $[V, \tau]$ è tutto l'autospazio relativo all'autovalore -1 e V si spezza come somma diretta degli autospazi $C_V(\tau)$ e $[V, \tau]$:

$$V = C_V(\tau) \oplus [V, \tau].$$

Se, invece, la caratteristica di F è pari, per ogni $v \in V$,

$$-v + v^\tau = v + v^\tau \in C_V(\tau),$$

dunque

$$[V, \tau] \leq C_V(\tau).$$

Come abbiamo osservato sopra, in questo caso, 1 è l'unico autovalore per τ, quindi, se τ non è l'automorfismo identico su V, V non si può decomporre come somma diretta di autospazi. Inoltre, si verifica direttamente (oppure, in modo più elegante, immergendo V e $\langle\tau\rangle$ nel loro prodotto semidiretto ed usando i risultati sull'interderivato) che τ fissa il sottospazio $[V, \tau]$ e induce l'applicazione identica sullo spazio quoziente $V/[V, \tau]$.

Sia ora A un gruppo che agisce su un gruppo B, non necessariamente un p-gruppo, ma tale che $|A|$ sia coprimo con $|B|$ e tale che A o B sia risolubile[2]. Immergendo A e B nel loro prodotto semidiretto, possiamo sempre ridurci al caso in cui A e B siano sottogruppi di un gruppo G che contiene B come sottogruppo normale e l'azione di A su B sia quella indotta dal coniugio. In questo caso B è un sottogruppo il cui ordine è coprimo con il suo indice e questa è la situazione del Teorema di Schur-Zassenhaus, che è il punto di partenza per lo studio delle azioni coprime. Un'immediata conseguenza del coniugio dei complementi nel Teorema di Schur-Zassenhaus è il Teorema di Decomposizione di Zassenhaus:

$$B = [B, A]C_B(A).$$

Per la Decomposizione di Zassenhaus, un'azione coprima non banale non può essere unipotente e, in particolare, se un automorfismo α di un p-gruppo finito B è unipotente, allora l'ordine di α è una potenza di p (si osservi che anche il viceversa è vero e segue, per induzione sull'ordine di B, dal Corollario 8.2.9).

Nella Sottosezione **??** mostreremo che le azioni coprime sono controllate da certe sezioni abeliane elementari. Più precisamente, se $\rho\colon A \to B$ è un'azione coprima, il Teorema 10.2.5 garantisce l'esistenza, per ogni $p \in \pi(B)$, di p-sottogruppi di Sylow di B che siano A-invarianti. Questo riduce essenzialmente lo studio dell'azione che A induce su questi p-sottogruppi di Sylow. Dalla Decomposizione di Zassenhaus otterremo diversi risultati che permettono di ridurre lo studio delle azioni coprime su p-gruppi S all'azione indotta su certe loro sezioni abeliane o abeliane elementari: in particolare su $S/\Phi(S)$ o, più in generale, su $T/\Phi(T)$ dove T è un *cc*-sottogruppo di S (Teorema $P \times Q$ di Thompson).

L'analogia tra le azioni semisemplici e le azioni coprime è ancora più evidente restringendosi alle azioni sui gruppi abeliani. In questo caso, se $\rho\colon AtoB$ è un'azione su un gruppo abeliano B, esattamente come succede per i gruppi di automorfismi semisemplici di uno spazio vettoriale,

[2]La risolubilità di A o B alla fine risulta essere superflua, perché segue dal Teorema di Feit e Thompson [10] che afferma che ogni gruppo di ordine dispari è risolubile. Tuttavia, nella dimostrazione del Teorema di Feit e Thompson, dove si suppone per assurdo l'esistenza di un controesempio minimo, cioè di un gruppo X di ordine dispari non risolubile di ordine minimo, l'azione coprima viene usata per studiare le azioni tra i sottogruppi propri di X, i quali, per la minimalità di $|X|$, sono necessariamente risolubili.

1. la Decomposizione di Zassenhaus si spezza: $B = [A, B] \times C_B(A)$ e

2. ogni sottogruppo A-invariante di B che ammette un complemento ammette anche un complemento A-invariante (Teorema di Maschke).

Osserviamo che la dimostrazione del Teorema di Maschke è indipendente dal Teorema di Schur-Zassenhaus, anche se l'argomento centrale di entrambe le dimostrazioni è il medesimo (e, per inciso, esistono dimostrazioni alternative del Teorema di Schur-Zassenhaus che usano il Teorema di Maschke). In particolare, se B sia uno spazio vettoriale su un campo F, il Teorema di Maschke equivale a dire che ogni automorfismo di ordine coprimo con la caratteristica di F è semisemplice.

Nel caso in cui invece A sia abeliano proveremo che, se A non è ciclico, B è generato dai centralizzanti dei sottogruppi massimali di A (Primo Teorema di Generazione) oppure dai centralizzanti degli elementi di A (Secondo Teorema di Generazione).

10.2.1 Azione coprima

Un'azione $\rho\colon A \to Aut(H)$ di un gruppo A su un gruppo H si dice **coprima** se

1. $|A/\ker(\rho)|$ e $|H|$ sono finiti e primi tra loro,

2. $A/\ker(\rho)$ o H è risolubile.

Lemma 10.2.1 *Siano A e B due sottogruppi di un gruppo G con $[A, B] \cap A = \{1\}$. Allora $N_B(A) = C_B(A)$.*

DIMOSTRAZIONE. Chiaramente $C_B(A) \leq N_B(A)$. Viceversa,

$$[A, N_B(A)] \leq [A, B]$$

e, per il Lemma 6.2.1.5,

$$[A, N_B(A)] \leq A.$$

Quindi

$$[A, N_B(A)] \leq [A, B] \cap A = \{1\},$$

da cui la tesi per il Lemma 6.2.1.1. ∎

Teorema 10.2.2 *(Sollevamento dei Centralizzanti) Siano A un gruppo che agisce su un gruppo B. Sia H un sottogruppo normale di B, A-invariante e di ordine coprimo con quello di A e supponiamo che A o H sia risolubile. Allora*

$$C_{B/H}(A) = C_B(A)H/H.$$

DIMOSTRAZIONE. Possiamo, come al solito, supporre che A e B siano sottogruppi del prodotto semidiretto G di B con A ed $A \cap B = \{1\}$. Sia $C \leq B$ tale che $H \leq C$ e $C/H = C_{B/H}(A)$. Chiaramente

$$C_B(A) \leq C$$

cioè, equivalentemente,

$$C_B(A) = C_C(A). \tag{10.9}$$

Viceversa proviamo che

$$C = HC_B(A).$$

Poiché A centralizza C/H, per il Lemma 6.2.3, $[A, C] \leq H$. Per il Lemma 6.2.1.5, segue che

$$AH \trianglelefteq AC.$$

Ora H è un sottogruppo di Hall normale in AH ed A è un suo complemento. Per il Teorema di Schur-Zassenhaus, essendo A o H risolubile, H è transitivo sui complementi di H in HA. Per l'Argomento di Frattini

$$C = HN_C(A)$$

da cui, per il Lemma 10.2.1 e la 10.9,

$$C = HN_C(A) = HC_C(A) = HC_B(A).$$

■

Corollario 10.2.3 *(Decomposizione di Zassenhaus) Sia A un gruppo che agisce su un gruppo B e supponiamo che l'azione sia coprima. Allora*

$$B = [A, B]C_B(A).$$

DIMOSTRAZIONE. Segue immediatamente dal Teorema di Sollevamento dei Centralizzanti con $H = [A, B]$. ■

Corollario 10.2.4 *Sia A un gruppo che agisce su un gruppo B e supponiamo che l'azione sia coprima. Allora*

$$[B, A] = [B, A, A].$$

DIMOSTRAZIONE. Dalla Decomposizione di Zassenhaus segue

$$[B, A] = [[A, B]C_B(A), A] = [[A, B], A] = [B, A, A].$$

■

10.2.2 Controllo dell'azione coprima

Teorema 10.2.5 *Sia $\rho: K \to Aut(N)$ un'azione di un gruppo K su un gruppo N. Supponiamo che $|K|$ coprimo con $|N|$ e K oppure N sia risolubile. Sia p un divisore primo di N, allora*

1. *esistono dei p-sottogruppi di Sylow K-invarianti di N;*
2. *$C_N(K)$ agisce transitivamente per coniugio sull'insieme dei p-sottogruppi di Sylow K-invarianti di N.*

DIMOSTRAZIONE. Come sopra possiamo considerare N come sottogruppo di Hall normale di un gruppo G e K il suo complemento. Sia S un p-sottogruppo di Sylow di N. Per l'argomento di Frattini, $G = NN_G(S)$. Poichè $N \cap N_G(S)$ è un sottogruppo di Hall normale di $N_G(S)$, esiste un complemento H di $N \cap N_G(S)$ in $N_G(S)$. Ora

$$NH = N(N \cap N_G(S))H = NN_G(S) = G$$

e

$$N \cap H = N \cap (H \cap N_G(S)) = (N \cap N_G(S)) \cap H = \{1\}$$

quindi H è un complemento di N in G. Per il Teorema di Schur-Zassenhaus H e K sono coniugati in N, esiste dunque un elemento n di N tale che

$$K = H^n \leq (N_G(S))^n = N_G(S^n)$$

cioè S^n è un p-sottogruppo di Sylow di N K-invariante, il che prova 1).

Siano ora S_1 ed S_2 due sottogruppi di Sylow K-invarianti. Per il Teorema di Sylow esiste un elemento $h \in N$ tale che

$$S_1^h = S_2.$$

Da ciò segue che

$$K^h \leq (N_G(S_1))^h = N_G(S_1^h) = N_G(S_2)).$$

e quindi

$$\langle K, K^h \rangle \leq N_G(S_2). \tag{10.10}$$

Sia

$$T = \langle K, K^h, S_2 \rangle.$$

Poichè $S_2 \in Syl_p(N) = Syl_p(G)$, per 10.10, S_2 è un p-sottogruppo di Sylow normale di T e K e K^h sono due suoi complementi. Per il Teorema di Schur-Zassenhaus esiste un elemento $g \in S_2$ tale che

$$K^h = K^g$$

e quindi, per il Lemma 10.2.1

$$hg^{-1} \in N_N(K) = C_N(K)$$

da cui la tesi essendo

$$S_1^{(hg^{-1})} = (S_1^h)^{g^{-1}} = S_2^{g^{-1}} = S_2.$$

■

Siano A e B gruppi e $\rho: A \to Aut(B)$ un'azione di A su B. Sia H/K una sezione di B con H e K A-invarianti (questo accade, ad esempio, se H e K sono sottogruppi caratteristici di B). Come abbiamo già visto altre volte, l'azione ρ di A su B induce in modo naturale un'azione $\rho|_{H/K}$ di A su H/K, ponendo, per ogni $\alpha \in A$ ed ogni $Kh \in H/K$,

$$Kh^{(\alpha^{\rho|_{H/K}})} = Kh^{\alpha}.$$

In generale avremo che

$$ker(\rho) \leq ker(\rho|_{H/K});$$

questo significa che $\rho|_{H/K}$ *perde* qualche informazione rispetto a ρ.

Nel caso in cui

$$ker(\rho) = ker(\rho|_{H/K}),$$

diremo che la sezione H/K **controlla** ρ. Si osservi che H/K controlla ρ se e solo se, per ogni $\alpha \in A$

$$[H, \alpha] \leq K \text{ se e solo se } \alpha \in ker(\rho).$$

Diremo che H/K **controlla l'azione coprima** se controlla ogni azione coprima.

Se H/K controlla ρ, tutte le informazioni che possiamo ottenere su A da ρ le possiamo ottenere anche da $\rho|_{H/K}$. Questo può essere vantaggioso se la struttura di H/K è più semplice da trattare di quella di B, come accade nei due seguenti risultati.

Teorema 10.2.6 *Sia B un gruppo finito. Allora $B/\Phi(B)$ controlla l'azione coprima.*

DIMOSTRAZIONE. Sia $A := \langle \alpha \rangle$ e supponiamo che A centralizzi $B/\Phi(B)$. Allora

$$[A, B] \leq \Phi(B)$$

e quindi, per la Decomposizione di Zassenhaus,

$$B = [A, B]C_B(A) \leq \Phi(B)C_B(A),$$

da cui $B = C_B(A)$ per l'esercizio 8.3.12. ■

Teorema 10.2.7 *Sia B un gruppo finito, i cc-sottogruppi subnormali controllano l'azione coprima.*

DIMOSTRAZIONE. Sia α un automorfismo di B il cui ordine sia coprimo con l'ordine di B e sia F un CC-sottogruppo subnormale di B. Proveremo solo il caso in cui F è normale in B, il caso generale segue poi per facile induzione sul difetto di subnormalità. Poniamo $A = \langle\alpha\rangle$. Poichè A centralizza F, risulta $[A, F] = \{1\}$ e quindi

$$[A, F, B] = \{1\}.$$

Poichè $F \trianglelefteq B$, si ha $[F, B] \leq F$ e quindi, come sopra,

$$[F, B, A] = \{1\}.$$

Per il Lemma dei Tre Sottogruppi si ottiene

$$[B, A, F] = \{1\},$$

cioè $[B, A]$ centralizza F e quindi, poichè F è un CC-sottogruppo, $[B, A] \leq F$. Da ciò e dall'Azione Coprima, segue che

$$[B, A] = [B, A, A] \leq [F, A] = \{1\}.$$

■

Il seguente corollario è una forma leggermente più debole del teorema precedente, ma spesso più facile da applicare.

Corollario 10.2.8 *(Teorema $P \times Q$ di Thompson) Siano P un p-sottogruppo e Q un p'-sottogruppo di un gruppo G, tali che $[P, Q] = \{1\}$. Se G agisce su un p-gruppo V e $C_V(P) \leq C_V(Q)$. Allora Q centralizza tutto V.*

DIMOSTRAZIONE. Passando al prodotto semidiretto di V con G, possiamo come al solito supporre che V sia un complemento normale di G in un gruppo X. In tal caso il sottogruppo PV è normalizzato da Q e $PCV(P)$ è un cc-sottogruppo di PV. Poichè, per ipotesi Q centralizza sia P che $C_V(P)$, dal Teorema 10.3.7, segue che Q centralizza tutto PV, in particolare centralizza V.
■

Osserviamo che, se V è abeliano o $p \neq 2$, la tesi resta vera sostituendo la condizione $[P, Q] = \{1\}$ con $[P, Q] \leq Q$. Dimostreremo questo nel caso in cui V è abeliano (Corollario 10.2.15). Per $p \neq 2$ il risultato è stato dimostrato da Thompson in [29] e Bender ne ha dato una dimostrazione alternativa in [**?**] (vedi anche [22, 8.5.3 Satz].

10.2.3 Azioni sulle serie

In questa sezione A e B sono gruppi e $\rho\colon A \to Aut(B)$ è un'azione di A su B. Studieremo l'azione di A sui fattori di una serie subnormale A-invariante (cioè una serie subnormale di B i cui membri sono anche A-invarianti) e proveremo che se A centralizza tutti i fattori di questa serie, allora $A/ker(\rho)$ è nilpotente,

Normalizzanti e centralizzanti di una serie

Siano B una serie subnormale

$$B_0 \lhd B_1 \lhd \ldots \lhd B_k$$

dal sottogruppo B_0 al sottogruppo B_k di B.

L'intersezione dei normalizzanti in A dei sottogruppi B_i si dice **normalizzante** della serie $\mathcal{B}$ e si indica con $N_A(\mathcal{B})$; dunque

$$N_A(\mathcal{B}) = \bigcap_{i=0}^{k} B_i.$$

Diremo che un sottogruppo P di A *normalizza* la serie $\mathcal{B}$ se $P \leq N_A(\mathcal{B})$.

La restrizione di ρ a $N_A(\mathcal{B})$, induce, per ogni $i \in \{0, \ldots, k-1\}$, un'azione ρ_i di $N_A(\mathcal{B})$ su B_i/B_{i+1}, ponendo, come al solito, per ogni $\alpha \in N_A(\mathcal{B})$ ed ogni $B_{1+1}g \in B_i/B_{i+1}$,

$$(B_{1+1}g)^{\alpha^{\rho_i}} = B_{1+1}(g^{\alpha^{\rho}}).$$

L'intersezione in $N_A(\mathcal{B})$ dei nuclei delle azioni ρ_i si dice **centralizzante** della serie $\mathcal{B}$ e si indica con $C_A(\mathcal{B})$; dunque

$$C_A(\mathcal{B}) = \bigcap_{i=0}^{k} ker(\rho_i).$$

Diremo che un sottogruppo F di A **centralizza** la serie $\mathcal{B}$ se $F \leq C_A(\mathcal{B})$. Osserviamo che F centralizza la serie $\mathcal{B}$ se e solo se la normalizza e, per ogni $i \in \{1, \ldots, k\}$,

$$[B_i, A] \leq B_{i-1}.$$

Inoltre, dalle definizioni, segue immediatamente che

$$C_A(\mathcal{B}) \trianglelefteq N_A(\mathcal{B}) \tag{10.11}$$

Azione Unipotente

Diremo che l'azione ρ di A su B è *unipotente* (o che A **è unipotente su** B) se A centralizza una serie subnormale

$$\{1\} = B_0 \lhd B_1 \lhd \ldots \lhd B_k = B$$

di B. Si osservi che, se B è uno spazio vettoriale e $\rho(A) \leq GL(B)$, questo equivale a dire che, per ogni $a \in A$, 1 è l'unico autovalore di $\rho(a)$.

Teorema 10.2.9 *Sia $\rho\colon A \to Aut(B)$ un'azione di un gruppo A su un gruppo B. Allora le seguenti affermazioni sono equivalenti:*

1. *ρ è unipotente;*

2. esiste un intero positivo n tale che $[B,_n A] = \{1\}$;

3. A centralizza una serie normale di B;

DIMOSTRAZIONE. Supponiamo che A centralizzi la serie subnormale

$$B_0 = B \geq B_1 \geq \ldots \geq B_k = \{1\}.$$

Proviamo, per induzione su $i \in \{1, \ldots, k\}$ che

$$[B,_i A] \leq B_i].$$

Ora, per ogni $i \in \{o, \ldots, k\}$,

$$[B_i, A] \leq B_{i+1}] \tag{10.12}$$

perchè $\rho|_{B_i/B_{i+1}}$ è triviale. Da ciò segue in particolare che $[B, A] \leq B_1$. Supponiamo ora che $[B,_i A] \leq B_i$, allora, per la 10.12

$$[B,_{i+1} A] = [[B,_i A], A]] \leq [B_i, A] \leq B_{i+1}.$$

Dunque 1. implica 2.. Da 2. segue 3. perchè la serie

$$B \geq [B, A] \geq [B,_2 A] \geq \ldots \geq [B,_n A] = \{1\}$$

è una serie normale di B (esercizio 10.3.3) ed è centralizzata da A. Infine 3. implica 1. perchè ogni serie normale è subnormale. ∎

Lemma 10.2.10 *Sia A un p-gruppo di automorfismi di un p-gruppo B. Allora* $C_B(A) \neq \{1\}$

DIMOSTRAZIONE. Segue dal teorema 9.2.1 applicato al prodotto semidiretto di B con A. ∎

Il seguente teorema è il risultato principale sull'azione unipotente su un p-gruppo.

Teorema 10.2.11 *Sia* $\rho: A \to B$ *un'azione di un gruppo A su un gruppo B e supponiamo che B sia un p-gruppo. Allora* ρ *è unipotente se e solo se* $A/ker(\rho)$ *è un p-gruppo.*

DIMOSTRAZIONE. Supponiamo che ρ sia unipotente, allora esiste un intero positivo n tale che $[B,_n A] = \{1\}$. Sia a un elemento di A di ordine coprimo con p. Per il Corollario 10.2.4,

$$[B, a] = [B, a, a] = [B,_n a] \leq [B,_n A] = \{1\},$$

cioè $a \in ker(\rho)$. Il viceversa, segue per induzione su B in modo analogo alla dimostrazione di 9.2.2 ∎

Se si lascia cadere l'ipotesi che B sia un p gruppo,

Teorema 10.2.12 *(Teorema di Hall sull'azione unipotente) Sia $\rho: A \to B$ un'azione unipotente di un gruppo A su un gruppo B. Allora $A/ker(\rho)$ è nilpotente.*

DIMOSTRAZIONE. Possiamo ridurci al caso in cui ρ è fedele e dimostrare che A è nilpotente. Poiché ρ è unipotente, per il Teorema 10.2.9 esiste un intero positivo n tale che

$$[B,_n A] = \{1\}.$$

Per ogni intero non negativo i, poniamo $B_i = [B,_i A]$, allora la serie

$$B_0 = B \geq B_1 \geq \ldots \geq B_n = \{1\}$$

è una serie normale di B centralizzata da A (si osservi che $B_i = \{1\}$ per ogni $i \geq n$). Proviamo, per induzione su $i + j$ che

$$[B_i, \gamma_j(A)] \leq B_{i+j+1}. \tag{10.13}$$

Se $j = 0$, allora la 10.13 diviene $[B_i, A] \leq B_{i+1}$ che è vera per la definizione di B_{i+1}. In particolare questo prova il caso $k = 0$. Supponiamo ora che $j \geq 1$ e la 10.13 sia vera per ogni coppia di interi non negativi i, j con $i + j < k$. Siano l, m interi non negativi con $l + m = k$. Allora, per il caso $m = 0$ e per ipotesi induttiva, si ottiene

$$[B_l, A, \gamma_{m-1}(A)] = [B_{l+1}, \gamma_{m-1}(A)] \leq B_{(l+1)+(m)} = B_{l+m+1}$$

e

$$[B_l, \gamma_{m-1}(A), A] \leq [B_{l+m}, A] = B_{l+m+1},$$

da cui, per il Lemma dei Tre Sottogruppi (Esercizio 6.3.9), segue

$$[B_l, \gamma_m(A)] \leq B_{l+m+1}.$$

In particolare

$$[B, \gamma_n(A)] \leq B_n = [B,_n A] = \{1\}.$$

Poichè ρ è fedele, segue da ciò che $\gamma_n(A) = 1$ e quindi A è nilpotente. ∎

Corollario 10.2.13 *Sia A un sottogruppo del gruppo di automorfismi di un gruppo B. Sia $\mathcal{B}$ una serie subnormale da B a $\{1\}$, Allora $C_A(\mathcal{B}) \leq F(N_A(\mathcal{B}))$.*

10.2.4 Azione coprima su un gruppo abeliano

In questa sezione A è un gruppo finito che agisce tramite una rappresentazione ρ su un gruppo abeliano B. Il fatto che B sia abeliano permette di costruire facilmente dei punti fissi per l'azione di A e, se l'azione è coprima, il gruppo B ammette utili fattorizzazioni come prodotto diretto di sottogruppi A-invarianti di cui faremo uso in seguito: la Decomposizione di Zassenhaus per gruppi abeliani ed il Teorema di Maschke, che è un risultato ancor più generale.

Punti fissi nei gruppi abeliani

Il modo ovvio per costruire in B punti fissi sotto l'azione di A è prendere le somme di tutti gli elementi di una A-orbita in B: infatti, per ogni $b \in B$ l'elemento

$$\prod_{a\in A} b^a \tag{10.14}$$

è un punto fisso per l'azione di A perché ogni elemento di A induce una permutazione sui fattori di 10.14 e B è abeliano. Si osservi che se b è un punto fisso di A, allora

$$\prod_{a\in A} b^a = b^{|A|}.$$

Ne segue che, se, l'esponente di B è coprimo con $|A|$ (in particolare, se l'azione è coprima), la funzione

$$\begin{array}{rccc} \mu\colon & B & \to & C_B(A) \\ & b & \mapsto & (\prod_{a\in A} b^a)^{|A|^{-1}} \end{array} \tag{10.15}$$

è idempotente e, come si vede facilmente, è un endomorfismo di B la cui immagine è $C_B(A)$. Inoltre, per ogni $b \in B$ ed ogni $x \in A$

$$\mu(b^x) = \mu(b) \tag{10.16}$$

(si osservi che l'elemento $\mu(b)$ può essere interpretato come la media delle immagini di b tramite gli elementi di A). Per quanto visto sugli endomorfismi idempotenti (cf. 2.2.2),

$$B = C_B(A) \times ker(\mu). \tag{10.17}$$

Ora, dalla 10.16, segue che, per ogni $b \in B$ ed ogni $x \in A$,

$$\mu([x, b] = \mu(b^x)\mu(b)^{-1} = 1,$$

cioè

$$[A, B] \leq ker(\mu). \tag{10.18}$$

D'altra parte, per la Decomposizione di Zassenhaus,

$$B = [A, B]C_B(A), \tag{10.19}$$

quindi, da 10.17 e 10.18, segue che, se B è abeliano, la Decomposizione di Zassenhaus diventa:

$$B = [A, B] \times C_B(A),$$

in particolare A agisce senza punti fissi come gruppo di automorfismi su $[A, B]$ (cioè l'unico punto fisso di $[A, B]$ sotto l'azione di A è l'identità). Riassumendo:

Teorema 10.2.14 *Sia A un gruppo finito e B un gruppo abeliano di ordine coprimo con A, e sia μ come sopra allora:*

1. *μ è un endomorfismo idempotente di B;*
2. *per ogni $b \in B$, $b \in C_B(A)$ se e solo se $b = \mu(b)$;*
3. *$B = [A, B] \times C_B(A)$,*
4. *A agisce senza punti fissi come gruppo di automorfismi su $[A, B]$.*

Come prima applicazione, abbiamo il seguente risultato che generalizza il Teorema $P \times Q$ di Thompson useremo in seguito:

Corollario 10.2.15 *Siano P un p-sottogruppo di G e Q un p'-sottogruppo di G tali che $[P, Q] \leq Q$. Se G e di ordine coprimo con p. Se G agisce su un p-gruppo abeliano V e $C_V(P) \leq C_V(Q)$, allora Q centralizza tutto V.*

DIMOSTRAZIONE. Poiché $|V|$ è coprimo con $|Q|$ e V è abeliano, per il Teorema 10.2.14.*3*

$$V = [V, Q] \times C_V(Q).$$

In particolare, poichè $C_V(P) \leq C_V(Q)$, segue che

$$C_{[V,Q]}(P) = \{1\}. \tag{10.20}$$

D'altra parte, poiché P normalizza Q ed agisce su V, $[V, Q]$ è un sottogruppo P-invariante di V e quindi, poiché sono entrambi p-gruppi, il Corollario 8.2.9 e l'equazione (10.20) implicano che, $[V, Q] = \{1\}$ ∎

Azione su $End(B)$

L'azione di A su B si estende in modo naturale ad un'azione si A su $End(B)$. Ricordiamo che B è un gruppo abeliano, $End(B)$ con la somma puntuale e la composizione di applicazioni è un anello. Il gruppo degli elementi invertibili di $End(B)$ è $Aut(B)$ e $Aut(B)$ agisce per coniugio su $End(B)$. Infatti, se $\alpha \in AutB$ e $\beta \in End(B)$, l'applicazione $\alpha^{-1}\beta\alpha$ è un endomorfismo di B (perché composizione di endomorfismi), l'applicazione

$$\begin{array}{rccc} \gamma_\alpha\colon & End(B) & \to & End(B) \\ & \phi & \mapsto & \alpha^{-1}\phi\alpha \end{array}$$

è un automorfismo dell'anello $End(B)$ e l'applicazione che ad ogni α in $Aut(B)$ associa γ_α è una rappresentazione di $Aut(B)$ su $End(B)$ (le verifiche sono lasciate al lettore).

Componendo l'azione ρ di A su B con l'azione per coniugio di $Aut(B)$ su $End(B)$ otteniamo un'azione di A su $End(B)$: se $a \in A$ e $\phi \in End(B)$, per ogni $b \in B$, risulta

$$b^{\phi^a} = b^{a^{-1}\phi a}. \tag{10.21}$$

Chiameremo quest'azione **azione indotta** da ρ su $End(B)$.

La dimostrazione dei seguenti risultati è elementare e lasciata per esercizio:

Lemma 10.2.16 *Sia A un gruppo che agisce via ρ su un gruppo abeliano B e sia ϕ un endomorfismo di B. Allora ϕ fissato dall'azione indotta da ρ su $End(B)$ se e solo se per ogni $a \in A$, $\rho(a)$ commuta con ϕ.*

Corollario 10.2.17 *Sia A un gruppo che agisce su un gruppo abeliano B e sia ϕ un endomorfismo di B fissato dall'azione indotta di A su $End(B)$. Allora $ker(\phi)$ e B^ϕ sono sottogruppi A-invarianti di B.*

Lemma 10.2.18 *Se B è un gruppo abeliano, i fattori primi di $|End(B)|$ sono gli stessi di $|B|$. In particolare, se un gruppo finito A agisce su B e l'azione è coprima, anche l'azione indotta su $End(B)$ è coprima.*

Teorema di Maschke

Lemma 10.2.19 *Sia A un gruppo finito che agisce su un gruppo abeliano B di esponente coprimo con $|A|$, sia π un endomorfismo idempotente di B tale che B^π sia A-invariante e sia $\mu: End(B) \to End(B)$ definita come sopra. Allora $B^\pi = B^{\mu(\pi)}$ e $\mu(\pi)$ è idempotente.*

DIMOSTRAZIONE. Poiché B^π è A-invariante e π induce l'identità su B^π, segue che, per ogni $b \in B^\pi$,

$$\begin{aligned} b^{\mu(\pi)} &= b^{|A|^{-1}\sum_{a\in A}\phi^a} = \\ &= (b^{\sum_{a\in A} a^{-1}\phi a})^{|A|^{-1}} = \\ &= (\prod_{a\in A} b^{a^{-1}\phi a})^{|A|^{-1}} = \\ &= (\prod_{a\in A} (b^{a^{-1}})^\phi)^a)^{|A|^{-1}} \\ &= (\prod_{a\in A} (b^{a^{-1}a})^{|A|^{-1}} = b, \end{aligned}$$

cioè $\mu(\pi)$ induce l'identità su B^π, da cui segue la tesi perchè B^π è A-invariante. ∎

Corollario 10.2.20 (TEOREMA DI MASCHKE) *Sia A un gruppo finito che agisce su un gruppo abeliano B. Sia H un sottogruppo A-invariante di B. Se esistono complementi di H in B, allora esistono anche complementi A-invarianti di H in B.*

DIMOSTRAZIONE. Sia K un complemento di H in B e sia π la proiezione di B su H rispetto alla decomposizione di B come prodotto di H e K. Per il corollario precedente $\mu(\pi)$ è idempotente ed ha H come immagine. Dunque G si decompone come prodotto diretto $H \times ker(\mu(\pi))$ e $ker(\mu(\pi))$ è un complemento A-invariante di H in G. ∎

10.3 Esercizi

Esercizio 10.3.1 *Sia G un gruppo finito, e p un numero primo. Si provi che $O_p(G/O_p(G) = \{1\}$*

Esercizio 10.3.2 *Sia G un gruppo finito, e p un numero primo. Si provi che se $O_p(G) \cap E(G) \in Syl_p(E(G))$, allora $O_p(G) \cap E(G) = \{1\}$ e $E(G) \leq O_{p'}(G)$.*

Esercizio 10.3.3 *Sia A un gruppo che agisce su un gruppo B. Si provi che la serie*

$$B \geq [B, A] \geq [B,_2 A] \geq \ldots \geq [B,_n A]$$

è una serie normale di B centralizzata da A.

Esercizio 10.3.4 *Si provi che la funzione μ definita in 10.15 è un endomorfismo di B.*

Esercizio 10.3.5 *Si dimostrino i Lemmi 10.2.16, 10.2.18 ed il Corollario 10.2.17*

Esercizio 10.3.6 *Sia p un primo, A un p'-gruppo e B un p-gruppo. Supponiamo che il prodotto diretto AxB agisca sul p-gruppo p. Si provi che se $[A, C_P(B)] = \{1\}$, allora $[A, P] = \{1\}$.*

Esercizio 10.3.7 *Usando l'esercizio precedente, si provi che in un p-gruppo i cc-sottogruppi controllano l'azione coprima.*

Capitolo 11

Gruppi lineari

In questo capitolo p è un numero primo, K è un campo di caratteristica p, V è uno spazio vettoriale di dimensione finita n su K. Indichiamo con $GL(V)$ l'insieme degli automorfismi di V, cioè delle applicazioni lineari biiettive di V in se stesso. $GL(V)$ si dice **gruppo generale lineare** su V.

Il gruppo generale lineare $GL(V)$ ed alcune sue sezioni che definiremo tra poco sono esempi importanti di gruppi per almeno due motivi: innanzitutto perché descrivono le simmetrie di uno spazio vettoriale. Inoltre, per il Teorema di Classificazione dei Gruppi Semplici Finiti, un gruppo semplice finito può essere ciclico di ordine primo, alternante, un gruppo finito di tipo Lie oppure uno dei 26 gruppi semplici sporadici. La famiglia dei gruppi semplici finiti di tipo Lie è in un certo senso la più importante e si divide a sua volta in diverse sottofamiglie, una delle quali è quella costituita dai PSL che si ottengono come quoziente del derivato di un GL modulo il centro. I gruppi appartenenti alle varie famiglie di gruppi semplici finiti di tipo Lie, presentano delle analogie nelle loro strutture che permettono una trattazione unificata e la sottofamiglia in cui queste strutture sono più evidenti e facili da studiare è quella dei PSL.

In questo capitolo cercheremo di limitare il più possibile l'uso delle matrici. Questo soprattutto perché nei gruppi di matrici la simmetria del gruppo non è evidente: ad esempio, se p è un numero primo, per i Teoremi di Sylow, tutti i p-Sylow sono coniugati, e quindi giocano il medesimo ruolo. D'altra parte se p è la caratteristica del campo, le matrici unitriangolari costituiscono un p-sottogruppo di Sylow privilegiato rispetto agli altri p-Sylow. Inoltre i conti con le matrici spesso nascondono la struttura de gruppo: ad esempio per dimostrare che gli insiemi delle matrici triangolari o unitriangolari a blocchi sono dei sottogruppi, si possono fare conti piuttosto noiosi con le matrici, oppure considerarli come normalizzanti e centralizzanti di bandiere (serie) di sottospazi ed ottenere il risultato immediatamente dalla teoria delel azioni sulle serie vedi sezione 10.2.3.

Ci sono due eccezioni in cui faremo uso delle matrici: una è per il calcolo dei determinanti, e questo perché la definizione di determinante attraverso la matrice associata ad un'applicazione lineare è spesso l'unica che viene presentata

ai corsi di algebra lineare. L'altra è come aiuto per visualizzare, quando è possibile, la struttura dei sottogruppi che vengono definiti (ad esempio nella decomposizione di Levi dei parabolici).

Nella prima sezione calcoleremo l'ordine di GL(V) e mostreremo che possiede un sottogruppo normale di indice $|K| - 1$: il gruppo speciale lineare $SL(V)$ su V. Introdurremo due strutture associate allo spazio V su cui $GL(V)$ e $SL(V)$ agiscono in modo naturale: lo spazio proiettivo $P(V)$ e lo spazio delle bandiere $\mathcal{F}(V)$. Mostreremo che i nuclei di queste azioni (sia sullo spazio proiettivo che sullo spazio delle bandiere) è dato dalle applicazioni scalari e definiremo i gruppi proiettivi $PGL(V)$ e $PSL(V)$. Proveremo infine che $PSL(V)$ è 2-transitivo su $P(V)$.

Nella seconda sezione introdurremo le trasvezioni: questi sono degli elementi di $SL(V)$ che hanno un ruolo analogo a quello dei 3-cicli nei gruppi alterni. Proveremo infatti che $SL(V)$ è generato dalle trasvezioni,

Nella terza sezione proveremo che $PSL(V)$ è semplice salvo i casi in cui $dimV = 2$ e $|K| \in \{2, 3\}$.

Nella quarta sezione studieremo la struttura p-locale di $PSL(V)$: proveremo che ogni p-locale di $PSL(V)$ è contenuto in un sottogruppo parabolico massimale e proveremo il teorema di Borel-Tits per $PSL(V)$: Se P è un parabolico massimale di $PSL(V)$, $F^*(P) = O_p(P)$ e determineremo le strutture di $F^*(P)$, di $P/F^*(P)$ e l'azione di P su $F^*(P)$.

Nella quinta sezione studieremo gli elementi di ordine coprimo con p.

Chiudiamo questa introduzione ricordando due risultati elementari di algebra lineare ed una loro immediata conseguenza che può essere interpretata come una versione per $GL(V)$ del Teorema di Witt sull'estensione delle isometrie.

Teorema 11.0.8 (Teorema del Completamento della Base)
Se $(v_1, \ldots, v_s)$ è un s-upla ordinata di elementi linearmente indipendenti di V, allora $s \leq n$ ed esistono dei vettori $v_{s+1}, \ldots, v_n$ di V tali che $(v_1, \ldots, v_n)$ sia una base di V.

Teorema 11.0.9 (Teorema di Estensione per Linearità)
Se $(v_1, \ldots, v_n)$ è una base di V e $w_1, \ldots, w_n$ sono elementi di V, allora esiste un unico endomorfismo f di V tale che $v_i^f = w_i$ per ogni $i \in \{1, \ldots, n\}$.

Teorema 11.0.10 *Siano V_1 e V_2 due spazi vettoriali di dimensione n sul campo K, siano U_1 ed U_2 sottospazi rispettivamente di V_1 e di V_2 e sia $f: U_1 \to U_2$ un isomorfismo. Allora esiste un isomorfismo $g: V_1 \to V_2$ tale che $g_{|_{U_1}} = f$.*

11.1 Azioni di GL(V) e SL(V)

Il gruppo generale lineare

Lemma 11.1.1 *$GL(V)$ agisce in modo regolare sull'insieme delle basi (ordinate) di V.*

DIMOSTRAZIONE. Per il Teorema di Estensione per Linearità, se $(v_1, \ldots, v_n)$ e $(w_1, \ldots, w_n)$ sono basi di V, allora esiste un endomorfismo g di V tale che $v_i^g = w_i$ per ogni $i \in \{1, \ldots, n\}$. Poiché g manda una base di V in un'altra base di V , segue che $g \in GL(V)$. Inoltre se $v_i^g = v_i$ per ogni $i \in \{1, \ldots, n\}$, allora $v^g = v$ per ogni $v \in V$ e quindi $g = 1$. ∎

Corollario 11.1.2 *Se $|K| = p^k$, allora*

$$|GL(V)| = p^{k(1+2+\ldots+(n-2)+(n-1))}(p^{kn} - 1)(p^{k(n-1)} - 1)\ldots(p^{k2} - 1)(p^k - 1). \tag{11.1}$$

DIMOSTRAZIONE. È un facile esercizio di algebra lineare provare che l'insieme delle basi ordinate di V ha esattamente

$$(p^{kn} - 1)(p^{kn} - p^k)(p^{kn} - p^{2k})\ldots(p^{kn} - p^{(k-2)}n)(p^k - p^{(k-1)n}).$$

elementi. Raccogliendo le potenze di p di ciascun fattore nell'equazione precedente, otteniamo la tesi. ∎

Corollario 11.1.3 *Se S è un p-sottogruppo di Sylow di $GL(V)$, allora S ha ordine $p^{k(1+2+\ldots+(n-2)+(n-1))}$.*

DIMOSTRAZIONE. Segue immediatamente dal corollario 11.1.2 e dal fatto che $p^i - 1$ è coprimo con p per ogni $i \in \mathbf{N}$. ∎

Il Gruppo Speciale Lineare

Indichiamo con $GL(n, K)$ l'insieme delle matrici di n righe ed n colonne a coefficienti in K ed a determinante diverso da zero. $GL(n, K)$ è un gruppo rispetto al prodotto righe per colonne. Fissata una base $(v_1, \ldots, v_n)$ di V, per ogni elemento g di $GL(V)$ esiste un unica matrice $(g_{i,j})$ in $GL(n, K)$ tale che

$$v_i^g = g_{i,1}v_1 + gi, 2v_2 + \ldots + g_{i,n}v_n.$$

La matrice $(g_{i,j})$ si dice **matrice associata a g rispetto alla base** $(v_1, \ldots, v_n)$. L'applicazione $\mu: GL(V) \to GL(n, K)$ che a ciascun $g \in GL(V)$ associa la matrice $(g_{i,j})$ è un isomorfismo di gruppi. Se $(w_1, \ldots, w_n)$ è un'altra base di V e $(\overline{g}_{i,j})$ è la matrice associata a g rispetto alla base $(w_1, \ldots, w_n)$, allora le matrici $(\overline{g}_{i,j})$ e $(g_{i,j})$ sono coniugate in $GL(n, K)$ e quindi hanno lo stesso determinante. Posto, per ogni $g \in GL(V)$, $det(g) := det(g_{i,j})$, segue che $det(g)$ è indipendente dalla base scelta. $det(g)$ si dice **determinante** di g. Dalle proprietà del determinante segue immediatamente che l'applicazione $det: GL(V) \to K^*$ che ad ogni elemento di $GL(V)$ associa il suo determinante è un'omomorfismo di gruppi e, come si vede facilmente, suriettivo. Il nucleo dell'applicazione det è

un sottogruppo normale di $GL(V)$, si chiama **gruppo speciale lineare** su V e si indica con $SL(V)$. Chiaramente gli elementi di $SL(V)$ sono tutti e soli gli elementi g di $GL(V)$ che hanno determinate 1. Per il Primo Teorema di Omomorfismo, $GL(V)/SL(V)$ è isomorfo al gruppo moltiplicativo K^* degli elementi di K diversi da zero.

Lemma 11.1.4 *Se $|K| = p^k$, allora*

$$|SL(V)| = p^{k(1+2+\ldots+(n-2)+(n-1))}(p^{kn}-1)(p^{k(n-1)}-1)\ldots(p^{k2}-1). \quad (11.2)$$

DIMOSTRAZIONE. Segue immediatamente dal corollario 11.1.2 e dal fatto che $K^* = p^k - 1$. ∎

Corollario 11.1.5 *Se $|K|$ è finito, $Syl_p(GL(V)) = Syl_p(SL(V))$*

DIMOSTRAZIONE. Segue immediatamente dai Teoremi di Sylow, dal corollario 11.1.2 e dal lemma 11.1.4 . ∎

Lemma 11.1.6 *$SL(V)$ agisce in modo regolare sull'insieme delle n-uple*

$$(\langle v_1\rangle, v_2, \ldots, v_n)$$

dove $(v_1, v_2, \ldots, v_n)$ è una base di V.

DIMOSTRAZIONE. Siano $(v_1, \ldots, v_n)$ e $(w_1, \ldots, w_n)$ due basi di V. Per il lemma11.1.1, esiste un elemento $\gamma \in GL(V)$ tale che $v_i^\gamma = w_i$. Scegliendo opportunamente il generatore w_1 di $\langle w_1\rangle$, possiamo supporre che γ abbia determinante 1, il che prova la transitività. L'azione è anch regolare perché se $\gamma \in SL(V)$ fissa i vettori $v_2, \ldots, v_n$ e fissa il sottospazio $\langle v_1\rangle$, allora γ fissa anche v_1 e quindi è l'identità. ∎

11.1.1 Alcune azioni di $GL(V)$ e $SL(V)$

L'azione di $GL(V)$ su $PG(V)$ e $\mathcal{F}(V)$

Chiaramente ogni applicazione lineare biiettiva γ di V in sè manda sottospazi in sottospazi conservandone la dimensione, e quindi induce in modo naturale una collineazione su $PG(V)$, ponendo, come al solito, per ogni $W \in PG(V)$,

$$W^\gamma := \{w^\gamma | w \in W\}.$$

Analogamente ogni collineazione β di $PG(V)$ conserva le bandiere di $\mathcal{F}(V)$ induce un automorfismo di $\mathcal{F}(V)$, ponendo per una bandiera $\mathcal{F} := (W_1, W_2, \ldots, W_t)$,

$$\mathcal{F}^\beta := (W_1^\beta, W_2^\beta, \ldots, W_t^\beta).$$

Ne segue che $GL(V)$ agisce in modo naturale su $PG(V)$ e su $\mathcal{F}(V)$ e, chiaramente, il nucleo di queste azioni è, in entrambi i casi, costituito dagli elementi γ di $GL(V)$ che fissano ogni sottospazio di V. Queste sono precisamente le applicazioni **scalari**, cioè gli elementi $\gamma \in GL(V)$per i quali esiste un elemento non nullo di a di K (dipendente da γ) tale che, per ogni $v \in V$, $v^\gamma = av$, infatti:

Proposizione 11.1.7 *Sia V uno spazio vettoriale su un campo K e sia $\gamma \in GL(V)$ tale che $W^\gamma = W$ per ogni sottospazio di dimensione 1 di V. Allora γ è un'applicazione scalare. In particolare, se Z è il nucleo dell'azione di G su $PG(V)$ (o su $\mathcal{F}(V)$). Allora Z è l'insieme delle applicazioni scalari.*

DIMOSTRAZIONE. Chiaramente un elemento γ di $GL(V)$ fissa ogni sottospazio di dimensione 1 se e solo se γ fissa ogni sottospazio di V, cioè se e solo se $\gamma \in Z$. Supponiamo che, per ogni sottospazio W di dimensione 1 in $P(V)$,

$$W^\gamma = W,$$

in particolare, se w è un generatore di W, esiste un elemento $a_w \in K^*$ tale che

$$w^\gamma = a_w w. \tag{11.3}$$

Se $V = W$ abbiamo finito. Supponiamo che $W < V$ e sia $u \in V \setminus W$. Come sopra esiste un elemento $a_u \in K^*$ tale che

$$u^\gamma = a_u u. \tag{11.4}$$

Poiché dev'essere anche $\langle u+w\rangle^\gamma = \langle u+w\rangle$, esiste un elemento $a_{u+w} \in K^*$ tale che

$$(u+w)^\gamma = a_{u+w}(u+w). \tag{11.5}$$

Da 11.3, 11.4 e 11.5, per la linearità di g segue

$$a_u u + a_w w = u^\gamma + w^\gamma = (u+w)^\gamma = a_{u+w}(u+w) = a_{u+w}u + a_{u+w}w,$$

da cui, essendo u e w linearmente indipendenti,

$$a_u = a_w = a_{u+w},$$

il che prova la tesi. ∎

Se Z è come sopra, il gruppo quoziente $GL(V)/Z$ si chiama **gruppo generale lineare proiettivo** e si indica con $PGL(V)$.

Lemma 11.1.8 *$Z \cong K^*$, in particolare, se $|K| = p^k$, Z è ciclico di ordine $p^k - 1$.*

DIMOSTRAZIONE. Se $\gamma \in Z$, allora esiste un elemento $\phi(\gamma) \in K^*$ tale che $v^\gamma = \phi(\gamma)v$ per ogni $v \in V$. La tesi segue immediatamente dal fatto che l'applicazione $\phi\colon Z \to K^*$ è, come si verifica facilmente, un isomorfismo di gruppi. ∎

Chiaramente, se $n = dim(V)$, $SL(V) \cap Z$ è l'insieme delle applicazioni scalari g tali che $v^g = av$ dove a è una radice n-esima di 1 in K. Poiché il gruppo moltiplicativo K^* è ciclico di ordine $p^k - 1$, l'insieme degli elementi $a \in K^*$ tali che $a^n = 1$ è ciclico di ordine d dove d è il massimo comun divisore di n e $p^k - 1$. Il gruppo quoziente $SL(V)/(SL(V) \cap Z)$ si chiama **gruppo speciale lineare proiettivo** e si indica con $PSL(V)$. Per il Secondo Teorema di Omomorfismo $PSL(V)$ è un sottogruppo normale di $PGL(V)$.

Proposizione 11.1.9 *Se $|K| = p^k$, allora*

1. $|PGL(V)| = p^{k(1+2+\ldots+(n-2)+(n-1))}(p^{kn} - 1)(p^{k(n-1)} - 1)\ldots(p^{k2} - 1)$;
2. $|PSL(V)| = p^{k(1+2+\ldots+(n-2)+(n-1))}(p^{kn} - 1)(p^{k(n-1)} - 1)\ldots(p^{k2} - 1)/d$ *dove d è il massimo comune divisore tra p^k e n.*

Osserviamo che

$$|GL(V)|_p = |SL(V)|_p = |PGL(V)|_p = |PSL(V)|_p.$$

Un sottogruppo H di $GL(V)$ o di $PGL(V)$ si dice **transitivo sulle bandiere** di $\mathcal{F}(V)$ se, per ogni coppia di bandiere dello stesso tipo

$$V_1 \leq V_2 \leq \ldots \leq V_l$$

e

$$W_1 \leq W_2 \leq \ldots \leq W_l$$

in $\mathcal{F}(V)$, esiste γ in H tale che

$$V_i^\gamma = W_i.$$

Proposizione 11.1.10 *$SL(V)$ (e quindi $PSL(V)$) è transitivo sulle bandiere di $\mathcal{F}(V)$ e, se $dim(V) \geq 2$, è anche 2-transitivo sui punti di $P(V)$.*

Dimostrazione. Siano

$$\mathcal{F}_1 = (V_1, V_2, \ldots, V_l) \text{ e } \mathcal{F}_2 = (W_1, W_2, \ldots, W_l)$$

due bandiere dello stesso tipo in $\mathcal{F}(V)$. Si osservi che, per ipotesi,

$$dim(V_i) = dim(W_i).$$

Sia $r_i = dim(V_i)$ e siano $(v_1, v_2, \ldots, v_n)$ e $(w_1, w_2, \ldots, w_n)$ due basi di V tali che

$$\langle v_1, \ldots, v_{r_i} \rangle = V_i \text{ e } \langle w_1, \ldots, w_{r_i} \rangle = W_i$$

per ogni $i \in \{1, \ldots, l\}$. Per il lemma 11.1.6 esiste $\gamma \in SL(V)$ tale che

$$\langle v_i^\gamma \rangle = \langle w_i \rangle \text{ per ogni } i \in \{2, \ldots, n\}$$

e quindi

$$V_i^\gamma = \langle v_1, \ldots, v_{r_i} \rangle^\gamma = \langle w_1, \ldots, w_{r_i} \rangle = W_{r_i}.$$

Infine, se (P_1, P_2) e (Q_1, Q_2) due coppie di punti di $P(V)$, tali che $P_1 \neq P_2$ e $Q_1 \neq Q_2$ allora gli insiemi $\{P_1, P_2\}$ e $\{Q_1, Q_2\}$ sono indipendenti. Siano v_1, v_2, w_1, w_2 generatori rispettivamente di P_1, P_2, Q_1, Q_2. Per il Teorema del Completamento della Base ed il Teorema di Estensione per Linearità esiste un elemento γ di $GL(V)$ tale che $v_i^\gamma = w_i$ $(i \in \{1, 2\})$. A meno di scambiare w_1 con un suo multiplo, possiamo supporre che $det(\gamma) = 1$ e quindi $\gamma \in SL(V)$. Ne segue che, per $i \in \{1, 2\}$,

$$P_i^\gamma = \langle v_i^\gamma \rangle = \langle w_i \rangle = Q_i.$$

■

Terminiamo questa sezione osservando che in generale $PGL(V)$ è un sottogruppo proprio del gruppo delle collineazioni di $PG(V)$. Infatti, ogni applicazione biiettiva ϕ di V in sè tale che

1. per ogni $v, w \in V$, risulta $(v + w)^\phi = v^\phi + w^\phi$ e
2. esiste un automorfismo di campi σ di K tale che, per ogni $a \in K$ e ogni $v \in V$, $(av)^\phi = a^\sigma v^\phi$

induce una collineazione su $P(V)$. Le applicazioni che soddisfano queste due condizioni si dicono **semilineari** e quelle biiettive formano un gruppo che si indica con $\Gamma L(V)$. Chiaramente, σ è l'applicazione identica su K se e solo se ϕ è lineare, quindi $GL(V)$ è un sottogruppo di $\Gamma L(V)$ e, si può vedere facilmente, è un sottogruppo normale ed il quoziente $\Gamma L(V)/GL(V)$ è isomorfo al gruppo degli automorfismi di K. Per il Teorema Fondamentale della Geometria Proiettiva ([28] Theorem 3.1, pag. 14), se $dim(V) \geq 3$, ogni collineazione di $P(V)$ è indotta da un elemento di $\Gamma L(V)$. In particolare, posto $P\Gamma L(V)$ il gruppo quoziente di $\Gamma L(V)$ modulo il sottogruppo delle applicazioni scalari, risulta che, se $dim(V) \geq 3$, allora $P\Gamma L(V) = Aut(P(V))$.

L'azione duale

Sia V^* lo spazio duale di V. Per ogni γ in G e per ogni $\phi \in V^*$, sia ϕ^{γ^*} l'applicazione

$$\begin{array}{rccc} \phi^{\gamma^*}\colon & V & \to & K \\ & v & \mapsto & \phi(v^{\gamma^{-1}}) \end{array}$$

è lineare e quindi un elemento di V^*, inoltre l'applicazione

$$\begin{array}{rccc} \gamma^*\colon & V^* & \to & V^* \\ & \phi & \mapsto & \phi^{\gamma^*} \end{array}$$

è un elemento di $GL(V^*)$ e l'applicazione

$$\begin{array}{rccc} *\colon & GL(V) & \to & GL(V^*) \\ & \gamma & \mapsto & \gamma^* \end{array} \tag{11.6}$$

è una rappresentazione di $GL(V)$ su V^* (le verifiche sono facili e lasciate al lettore).

Da questo segue, in generale, che data una rappresentazione lineare $\rho: G \to GL(V)$ di un gruppo G su V, l'applicazione

$$\begin{array}{rccc} \rho^*: & G & \to & GL(V^*) \\ & g & \mapsto & \rho(g))^* \end{array} \tag{11.7}$$

è una rappresentazione di G su V^* e si chiama **rappresentazione duale** della rappresentazione ρ. In particolare $*$ è la rappresentazione duale della rappresentazione naturale di $GL(V)$ su V.

In termini di matrici si vede facilmente che se M è la matrice associata ad un elemento γ di $GL(V)$ rispetto ad base $(e_1, \ldots, e_n)$ di V, allora la matrice associata a γ^* rispetto alla rispettiva base duale $(e_1^*, \ldots, e_n^*)$ è l'inversa della trasposta della matrice M (esercizio **??**).

Azione di $GL(W_1) \times GL(W_2)$ su $Hom(W_1, W_2)$

Proposizione 11.1.11 *Siano W_1 e W_2 spazi vettoriali sul campo K, siano G_1 e G_2 gruppi e, per $i \in \{1, 2\}$ sia $\rho_i: G_i \to GL(W_i)$ una rappresentazione di G_i su W_i. Allora*

1. *per ogni $\gamma \in G_1$ e $\delta \in G_2$ e per ogni $\phi \in Hom(W_1, W_2)$,*

$$(\gamma^{-1})^{\rho_1} \phi \delta^{\rho_2} \in Hom(W_1, W_2);$$

2. *per ogni $\gamma \in G_1$ e $\delta \in G_2$ l'applicazione*

$$\begin{array}{rccc} \rho_{(\gamma,\delta)}: & Hom(W_1, W_2) & \to & Hom(W_1, W_2) \\ & \phi & \mapsto & (\gamma^{-1})^{\rho_1} \phi \delta^{\rho_2} \end{array}$$

   è un automorfismo di $Hom(W_1, W_2)$ come gruppo abeliano (anzi, come K-spazio vettoriale);

3. *l'applicazione*

$$\begin{array}{rccc} \rho: & G_1 \times G_2 & \to & Aut(Hom(W_1, W_2)) \\ & (\gamma, \delta) & \mapsto & \rho_{(\gamma,\delta)} \end{array}$$

   è un'azione di $G_1 \times G_2$ su $Hom(W_1, W_2)$.

DIMOSTRAZIONE. Esercizio ■

11.2 Trasvezioni e Sottogruppi Radice

Un elemento non identico τ di $GL(V)$ si dice **trasvezione** se

1. $[V,\tau]$ è un sottospazio di dimensione 1 di V,
2. $C_V(\tau)$ è un iperpiano di V e
3. $[V,\tau] \leq C_V(\tau)$

Se τ è una trasvezione di $GL(V)$ i sottospazi $[V,\tau]$ e $C_V(\tau)$ si dicono rispettivamente **centro** e **asse** della trasvezione τ.

Proposizione 11.2.1 *Le trasvezioni di $GL(V)$ hanno determinante 1, quindi sono elementi di $SL(V)$.*

DIMOSTRAZIONE. Sia τ una trasvezione. Per il teorema del Completamento delle Basi esiste una base $(v_1,..,v_n)$ di V tale che

1. v_1 è un generatore del centro di τ
2. $(v_1, v_2, \ldots, v_{n-1})$ è una base dell'asse di τ.

Inoltre, a meno di scambiare v_n con un suo multiplo scalare, possiamo supporre che $v_n^\tau = v_1 + v_n$. Rispetto a tale base, la matrice associata alla trasvezione τ è

$$\begin{pmatrix} 1 & 0 & 0 & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 1 \end{pmatrix}, \tag{11.8}$$

che ha determinante 1. ∎

Più avanti avremo bisogno della seguente caratterizzazione delle trasvezioni. La dimostrazione è immediata e lasciata per esercizio.

Proposizione 11.2.2 *Sia τ una trasvezione di $GL(V)$ e w un generatore di $[V,\tau]$. Allora esiste una forma lineare $\alpha: V \to K$ tale che $C_V(\tau) \leq ker(\alpha)$ e, per ogni $v \in V$, $v^\tau = v + v^\alpha w$. Viceversa, se $\alpha: V \to K$ è una forma lineare e w è un vettore non nullo in $ker(\alpha)$, allora l'applicazione $\tau: V \to V$, definita, per ogni $v \in V$, da $v^\tau = v + v^\alpha w$, è una trasvezione di centro $\langle w \rangle$ ed asse $ker(\alpha)$.*

Se τ e γ sono elementi di $GL(V)$, allora

$$[V, \tau^\gamma] = [V^\gamma, \tau^\gamma] = [V,\tau]^\gamma \text{ e } (C_V(\tau))^\gamma = C_V(\tau^\gamma).$$

Da ciò segue che

$$C_{GL(V)}(\tau) \leq N_{GL(V)}[V,\gamma] \cap N_{GL(V)} C_V(\tau).$$

In particolare, se τ è una trasvezione di centro Z ed asse W, poiché γ conserva le dimensioni e le inclusioni tra i sottospazi di V, segue che τ^γ è una trasvezione

di centro Z^γ ed asse W^γ. Inoltre poiché $GL(V)$ è transitivo sulle basi di V, e per ogni trasvezione τ esiste una base la cui matrice associata è del tipo (11.8), segue che $GL(V)$ agisce transitivamente per coniugio sull'insieme delle sue trasvezioni e inoltre, posto,

$$P := N_{GL(V)}(Z) \cap N_{GL(V)}(W),$$

abbiamo che P contiene $C_{GL(V)}(\tau)$ e quindi

$$C_{GL(V)}(\tau) = C_P(\tau).$$

Sia ora $\gamma \in P$. Poichè γ normalizza Z e W e Z e V/W hanno dimensione 1, γ induce una moltiplicazione per uno scalare su Z e V/W. Siano a e b in K tali che

$$w^\gamma = aw \text{ per ogni } v \in Z \text{ e } (v+W)^\gamma = bv + W \text{ per ogni } v \in V.$$

In particolare, per ogni $v \in V$, esiste $w \in W$ tale che

$$v^\gamma = bv + w,$$

quindi

$$v^{\gamma\tau} = (bv+w)^\tau = bv^\tau + w = bv + b[v,\tau] + w,$$

e

$$v^{\tau\gamma} = (v+[v,\tau])^\gamma = v^\gamma + [v,\tau]^\gamma = bv + w + a[v,\tau],$$

da cui segue che $\gamma \in C_P(\tau)$ se e solo se $a = b$.

Riassumiamo quanto provato sopra nella seguente proposizione:

Proposizione 11.2.3 *Sia τ una trasvezione in $GL(V)$ di centro Z ed asse W e sia $\gamma \in GL(V)$. Allora*

1. *τ^γ è una trasvezione di centro Z^γ ed asse W^γ.*
2. *Un elemento γ di $GL(V)$ centralizza τ se e solo se normalizza Z e W ed induce la stessa applicazione scalare su Z e V/W nel senso che, se $a, b \in K$ sono tali che $w^\gamma = aw$ per ogni $v \in Z$ e $(v+W)^\gamma = bv + W$ per ogni $v \in V$, allora $a = b$.*
3. *$GL(V)$ è transitivo sull'insieme delle sue trasvezioni.*

Lemma 11.2.4 *Siano τ_1 e τ_2 due trasvezioni tali che $[V,\tau_1] \le C_V(\tau_2)$ e $[V,\tau_2] \le C_V(\tau_1)$. Allora $[\tau_1,\tau_2] = 1$ e $\tau_1\tau_2$ è o l'identità, o una trasvezione di centro contenuto in $\langle [V,\tau_1], [V,\tau_2] \rangle$.*

Dimostrazione. Per ogni $v \in V$, posto $\{i,j\} = \{1,2\}$, risulta

$$v^{\tau_i\tau_j} = (v+[v,\tau_i])^{\tau_j} = v^{\tau_j} + [v,\tau_i]^{\tau_j} = v + [v,\tau_i] + [v,\tau_j],$$

da cui la tesi. ∎

Sottogruppi Radice

Supponiamo ora che U sia un sottospazio massimale di V e sia Z un sottospazio di dimensione 1 contenuto in U. Sia T l'insieme di tutte trasvezioni di centro Z ed asse U e poniamo

$$R_{(Z,U)} := T \cup \{1\}.$$

Chiaramente $R_{(Z,U)} \subseteq Q_U$, quindi, per la dimostrazione della proposizione 11.4.10, $R_{(Z,U)}$ è un p-sottogruppo, inoltre, fissato $v \in V$, l'applicazione

$$\delta_v : V \to Z$$

che a $\tau \in R_{(Z,U)}$ associa $[v, \tau]$ è un omomorfismo di gruppi. Si vede facilmente che δ_v è biiettivo e quindi, poiché Z è uno spazio di dimensione 1, $R_{(Z,U)}$ è isomorfo al gruppo additivo $(K, +)$, che è un p-gruppo abeliano elementare di ordine p^k. $R_{(Z,U)}$ si dice **sottogruppo radice** associato alla bandiera $Z < U$.

Proposizione 11.2.5 *$SL(V)$ agisce transitivamente per coniugio sull'insieme dei suoi sottogruppi radice.*

DIMOSTRAZIONE. L'applicazione $(Z, U) \mapsto R_{(Z,U)}$ è un isomorfismo di $SL(V)$-insiemi (dove l'azione sui sottogruppi radice è quella indotta dal coniugio) e, per la proposizione 11.1.10, $SL(V)$ è transitivo sulle bandiere di tipo $(1, dim(V) - 1)$. ∎

Lemma 11.2.6 *Siano $v_1, v_2, \ldots, v_l, v, w$ vettori di V. Se v e w sono linearmente indipendenti e $v \notin \langle v_1, v_2, \ldots, v_l, w - v\rangle$, allora esiste una trasvezione τ di V tale che $\langle v_1, v_2, \ldots, v_l, w - v\rangle \leq C_V(\tau)$ e $v^\tau = w$.*

DIMOSTRAZIONE. Per ipotesi e per il Teorema del Completamento delle Basi, esiste un iperpiano U contenente $\langle v_1, v_2, \ldots, v_l, w - v\rangle$ e non contenente v. Ma allora esiste una trasvezione τ di asse U tale che $v^\tau = v + (w - v) = w$. ∎

Proposizione 11.2.7 *$SL(V)$ è generato dalle sue trasvezioni (e quindi dai suoi sottogruppi radice).*

DIMOSTRAZIONE. Possiamo supporre che $dim(V) \geq 2$, altrimenti $SL(V) = \{1\}$ e non c'è nulla da dimostrare. Sia T il sottogruppo generato dalle trasvezioni di $SL(V)$. Per la proposzione 11.2.1, $T \leq SL(V)$. Proviamo, per induzione su t, che, per ogni $t \in \{1, \ldots, n\}$,

T è transitivo sull'insieme Ω delle t-uple $(\langle v_1\rangle, v_2, \ldots, v_t)$, dove $v_1, v_2, \ldots, v_t$ sono t vettori linearmente indipendenti.

Siano $(\langle v_1\rangle, v_2, \ldots, v_t)$, e $(\langle w_1\rangle, w_2, \ldots, w_t)$, due t-uple come sopra. Sia $t = 1$. Se $\langle v_1\rangle = \langle w_1\rangle$ non c'è nulla da dimostrare, altrimenti, per il lemma 11.2.6,

esiste una trasvezione tale che $v_1^\tau = w_1$. Supponiamo ora che $t > 1$ e la tesi vera per $t-1$. Questo implica che esiste un elemento $\gamma \in T$ tale che

$$(\langle v_1^\gamma \rangle, v_2^\gamma, \ldots, v_{t-1}^\gamma v_t^\gamma) = (\langle w_1 \rangle, w_2, \ldots, w_{t-1}, v_t^\gamma).$$

In altre parole possiamo supporre che

$$v_i = w_i \text{ per ogni } i \in \{1, \ldots, t-1\}.$$

In questa situazione, poiché $v_1, v_2, \ldots, v_t$ sono linearmente indipendenti, per il lemma 11.2.6 esiste una trasvezione τ_1 di centro contenente $v_1 - v_t, v_2, \ldots, v_{t-1}$ tale che $v_t^{\tau_1} = v_1$. Analogamente esiste una trasvezione τ_2 di centro contenente $v_1 - v_t, v_2, \ldots, v_{t-1}$ tale che $w_t^{\tau_2} = v_1$, cioè

$$(\langle v_1 \rangle, v_2, \ldots, v_{t-1}, v_t)^{\tau_1} = (\langle u \rangle, v_2, \ldots, v_{t-1}, v_1)$$

e

$$(\langle v_1 \rangle, v_2, \ldots, v_{t-1}, w_t)^{\tau_2} = (\langle z \rangle, v_2, \ldots, v_{t-1}, v_1)$$

per degli opportuni vettori u e z non contenuti in $\langle v_1, v_2, \ldots, v_{t-1} \rangle$. Resta quindi da dimostrare che

esiste un elemento γ in $C_T(\langle v_1, v_2, \ldots, v_{t-1} \rangle)$ tale che $\langle u^\gamma \rangle = \langle z \rangle$.

Ovviamente, possiamo supporre che $\langle u \rangle \neq \langle z \rangle$. Poniamo

$$U := \langle u, v_1, v_2, \ldots, v_{t-1} \rangle, \quad Z := \langle z, v_1, v_2, \ldots, v_{t-1} \rangle, \text{ e } W := \langle v_1, v_2, \ldots, v_{t-1} \rangle.$$

Se $u \notin \langle z-u, v_1, v_2, \ldots, v_{t-1} \rangle$, la tesi segue dal lemma 11.2.6. Altrimenti $U = Z$ e W è un iperpiano di U. Ne segue che esiste uno scalare $a \in K$ tale che $u - az \in W$. Ma allora $u \notin \langle z - u, v_1, v_2, \ldots, v_{t-1} \rangle$ e, per il lemma 11.2.6, esiste una trasvezione γ che fissa U e manda u in az, e dunque $\langle u \rangle$ in $\langle z \rangle$. Questo prova che T è transitivo su Ω. D'altra parte $SL(V)$ è regolare su Ω e quindi $T = SL(V)$. ∎

Osserviamo che, alternativamente, questo risultato si sarebbe potuto ottenere dimostrando che ogni matrice $n \times n$ a determinante 1 può essere trasformata nella matrice identica tramite operazioni elementari sulle righe o sulle colonne (ad una riga (colonna) sostituire la medesima riga sommata ad un multiplo di un'altra riga(colonna)). Infatti queste operazioni corrispondono alla moltiplicazione a destra o a sinistra per matrici elementari associate a trasvezioni. Coerentemente con il proposito di evitare il più possibile i conti con le matrici, abbiamo preferito dimostrarlo usando le azioni.

Chiudiamo questo paragrafo con un risultato che ci servirà per dimostrare il Criterio di p-nilpotenza di Thompson (15.4.1). La dimostrazione è presa essenzialmente da [1, p.164].

Lemma 11.2.8 *Sia R un sottogruppo radice di $GL(V)$ e sia U un sottospazio R-invariante di V di dimensione* 1. *Allora $[U, R] = \{1\}$.*

DIMOSTRAZIONE. La tesi segue immediatamente perché $Aut(U) \cong K^*$ e K^* ha ordine coprimo con R. ∎

Lemma 11.2.9 *Sia W uno spazio vettoriale di dimensione 2 e siano R_1 e R_2 due distinti sottogruppi radice di $SL(W)$. Allora*

(a) R_1 agisce transitivamente per coniugio sull'insieme dei sottogruppi radice di $SL(W)$.

(b) $\langle R_1, R_2\rangle = SL(W)$

DIMOSTRAZIONE. Sia, per $i \in \{1,2\}$ z_i un generatore del sottospazio $[W, R_i]$. Poiché, $[W, R_1] \neq [W, R_2]$, i sottospazi di dimensione 1 di W diversi da $[W, R_i]$ sono tutti e soli del tipo $\langle az_i + z_{3-i}\rangle$ con a in K. Quindi R_i è transitivo sui sottospazi di dimensione 1 di W diversi da $[W, R_i]$. Poiché $\langle z_1 + z_2\rangle$ è un sottospazio di dimensione 1 diverso da $[W, R_1]$ e da $[W, R_2]$, ne segue che $\langle R_1, R_2\rangle$ è transitivo sui sottospazi di dimensione 1 di W. Poiché $dim(W) = 2$, per ogni sottogruppo radice R, $C_W(R) = [W, R]$ e quindi l'azione indotta per coniugio da $SL(W)$ sui sottogruppi radice è equivalente all'azione indotta da $SL(W)$ sui sottospazi di dimensione 1 di W. Dunque $\langle R_1, R_2\rangle$ è transitivo anche sui sottogruppi radice di $SL(W)$. Ma allora $\langle R_1, R_2\rangle$ contiene tutti i sottogruppi radice e dunque, per la Proposizione 11.2.7, coincide con $SL(W)$ ∎

Lemma 11.2.10 *Siano R_1 ed R_2 due sottogruppi radice di $GL(V)$ tali che $L := \langle R_1, R_2\rangle$ non sia un p-gruppo e sia $W := [V, L]$. Allora W è un sottospazio L-invariante di dimensione 2 di V e la restrizione a W induce una rappresentazione fedele di L su tutto $SL(W)$. In particolare $L \cong SL_2(K)$.*

DIMOSTRAZIONE. Poiché $L = \langle R_1, R_2\rangle$,

$$W = [V, L] = [V, R_1] + [V, R_2]$$

in particolare $dim(W) \leq 2$. Proviamo che

$$C_W(L) = \{0\}. \tag{11.9}$$

Supponiamo, per assurdo, che $C_W(L) \neq \{0\}$. Allora $dim(W/C_W(L)) \leq 1$ e, per il Lemma 11.2.9, $W/C_W(L)$ è centralizzato da R_1 e R_2 e quindi da L. Ma allora ogni elemento α di L, con $|\alpha|$ coprimo con p, centralizza la bandiera

$$\{0\} \leq C_W(L) \leq W \leq V$$

e quindi, per il Teorema 10.2.11, $\alpha = 0$, contro l'ipotesi che L non sia un p-gruppo, il che prova (11.9). Ne segue che

$$dim(W) = 2 \text{ e quindi } W = [V, R_1] \oplus [V, R_2]. \tag{11.10}$$

altrimenti $\{0\} \neq [V, R_1] = W = [V, R_2] \leq C_V(L) = \{0\}$. Poichè $C_V(L) = C_V(R_1) \cap C_V(R_2)$ e, per $i \in \{1, 2\}$, $C_V(R_i)$ è un iperpiano di V, segue che

$$dim(V/C_V(L) \leq 2. \tag{11.11}$$

Da (11.9), (11.10) e (11.11), segue che

$$V = W \oplus C_V(L),$$

e quindi $C_L(W) \leq CL(V) = \{1\}$, cioè L agisce fedelmente su W e la tesi segue per il Lemma 11.2.9(b), poiché R_1 e R_2 agiscono su W come sottogruppi radice distinti di $SL(W)$. ∎

Matrici associate

Può essere utile visualizzare le matrici associate ai sottogruppi introdotti: sia τ una trasvezione in $GL(V)$ di centro Z ed asse W e sia $(v_1, v_2, \ldots v_n)$ una base di V come nella dimostrazione del lemma 11.2.1. Allora le matrici associate agli elementi di $N_{GL(V)}(Z) \cap N_{GL(V)}(W)$ sono del tipo:

$$\begin{pmatrix} a & 0 & 0 \\ X_{2,1} & A & 0 \\ c & X_{3,2} & b \end{pmatrix}, \tag{11.12}$$

le matrici associate agli elementi di $C_{GL(V)}(\tau)$ sono del tipo:

$$\begin{pmatrix} a & 0 & 0 \\ X_{2,1} & A & 0 \\ c & X_{3,2} & a \end{pmatrix}, \tag{11.13}$$

le matrici associate agli elementi di $R_{(Z,W)}$ sono del tipo:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ c & 0 & 1 \end{pmatrix}, \tag{11.14}$$

dove $a, b, c \in K$ con $a, b \neq 0$, $A, I \in GL(n-2, K)$ con I matrice identica, $X_{2,1}$ una matrice con una colonna e $n-2$ righe e $X_{3,2}$ una matrice con una riga e $n-1$ colonne.

11.3 Il criterio di Iwasawa e semplicità di PSL(V)

11.3.1 Il criterio di Iwasawa

Teorema 11.3.1 *(Criterio di Iwasawa) Sia G un gruppo finito tale che*

1. *G è perfetto;*
2. *G agisce in modo primitivo su un insieme Ω;*

3. *Se $\omega \in \Omega$, esiste un sottogruppo risolubile R normale in G_ω tale che $R^G = G$;*

Allora ogni sottogruppo normale proprio di G è contenuto nel nucleo dell'azione.

DIMOSTRAZIONE. Sia N un sottogruppo normale di G non contenuto nel nucleo dell'azione. Per l'esercizio 8.3.46 N è transitivo su Ω e quindi, per l'Argomento di Frattini,

$$G = G_\omega N.$$

In particolare, poiché G_ω normalizza N,

$$G = R^G = R^{G_\omega N} = R^N \leq NR.$$

Poiché NR/N è isomorfo a $R/N \cap R$ che è un gruppo risolubile, ne segue che

$$G = G^\infty = (NR)^\infty \leq N,$$

da cui $N = G$. ∎

11.3.2 Semplicità di $PSL(V)$

Proposizione 11.3.2 *$SL(V)$ è perfetto tranne i due casi in cui $dim(V) = 2$ e $|K|$ ha ordine 2 o 3.*

DIMOSTRAZIONE. Poiché ogni trasvezione è contenuta in un gruppo radice e, per la Proposizione 11.2.5, SL(V) agisce transitivamente sui suoi gruppi radice, per la Proposizione 11.2.7 basta provare che esiste un gruppo radice generato da commutatori. Se $dim(V) \geq 3$, esistono due iperpiani distinti U e W con intersezione non nulla. Sia $0 \neq z \in U \cap W$, $w \in W \setminus U$ e $u \in U \setminus W$. Sia σ la trasvezione di asse W e centro $\langle z \rangle$ tale che $u^\sigma = u + z$ e, per ogni $a \in K$, sia τ_a la trasvezione di asse U e centro $\langle u \rangle$ tale che $w^{\tau a} = w + au$ (o l'applicazione identica se $a = 0$). Se $u \in U$,

$$u^{[\tau_a,\sigma]} = u^{\tau_a^{-1}\sigma^{-1}\tau_a\sigma} = u^{\sigma^{-1}\tau_a\sigma} = (u-z)^{\tau_a\sigma} = (u-z)^\sigma = u$$

Dunque $[\tau_a, \sigma]$ centralizza U. D'altra parte,

$$w^{[\tau_a,\sigma]} = w^{\tau_a^{-1}\sigma^{-1}\tau_a\sigma} = (w-au)^{\sigma^{-1}\tau_a\sigma} = (w-au-az)^{\tau_a\sigma} = (w-az)^\sigma = w-az.$$

Quindi $[\tau_a, \sigma]$ è una trasposizione in $R_{(U,Z)}$ dove $Z = \langle z \rangle$ e, al variare di $a \in K$ si possono ottenere in questo modo tutti gli elementi di $R_{(U,Z)}$.

Supponiamo ora che $dim(V) = 2$. Sia (u, w) una base di V, sia $U = \langle u \rangle$ e, per ogni $a, b \in K$ siano σ_a la trasvezione di centro ed asse U che manda w in $w + au$ e sia δ_b l'applicazione lineare che manda u in bu e w in $b^{-1}w$. Chiaramente σ_a e δ_b sono elementi di $SL(V)$ e

$$u^{[\delta_b,\sigma_a]} = u^{\delta_b^{-1}\sigma_a^{-1}\delta_b\sigma_a} = b^{-1}u^{\sigma_a^{-1}\delta_b\sigma_a} = b^{-1}u^{\delta_b\sigma_a} = u^{\sigma_a} = u.$$

e

$$\begin{aligned} w^{[\delta_b,\sigma_a]} &= w^{\delta_b^{-1}\sigma_a^{-1}\delta_b\sigma_a} = bw^{\sigma_a^{-1}\delta_b\sigma_a} = (bw-abu)^{\delta_b\sigma_a} = (w-ab^2u)^{\sigma_a} = \\ &= u+aw-ab^2w = w+a(1-b^2)u. \end{aligned}$$

Come sopra, segue che $[\delta_b, \sigma_a]$ è un elemento di $R(U,U)$ e, se b non è radice quadrata di 1 (ed un tale elemento esiste se K ha più di tre elementi), al variare di a in K si ottiene tutto il gruppo radice $R(U,U)$. ∎

Anche in questo caso può essere utile (e lo si lascia per esercizio) visualizzare le matrici associate alle applicazioni $\sigma, \tau_a, \sigma_a, \delta_b$ rispetto a delle basi opportune di V e calcolare le matrici associate ai commutatori $[\tau_a, \sigma]$ e $[\delta_b, \sigma_a]$.

Teorema 11.3.3 *Sia V uno spazio vettoriale di dimensione finita su un campo K. Se $dim(V) \geq 3$ oppure $|K| > 3$, ogni sottogruppo normale proprio di $SL(V)$ è contenuto nel centro di $SL(V)$. In particolare $PSL(V)$ è semplice.*

DIMOSTRAZIONE. Applichiamo il Criterio di Iwasawa all'azione di $SL(V)$ sull'insieme dei punti di $P(V)$. Per la proposizione 11.3.2, $SL(V)$ è perfetto. Per la proposizione 11.1.10 $SL(V)$ è 2-transitivo sui punti di $P(V)$ e qundi è primitivo per l'esercizio 8.3.42. Infine, sia Z un punto di $P(V)$. Per la proposizione 11.4.10, $C_{SL(V)}Z \cap C_{SL(V)}V/Z$ è un p-sottogruppo normale abeliano di$N_{SL(V)}(Z)$ e contiene ogni sottogruppo radice $R(Z,W)$ con $Z \leq W$. Per le proposizioni 11.2.5 e 11.2.7 $SL(V) = Q_W^{SL(V)}$ e quindi, per il Criterio di Iwasawa, ogni sottogruppo normale proprio di $SL(V)$ è contenuto nel centro di $SL(V)$. La seconda affermazione segue immediatamente dal Teorema di Corrispondenza. ∎

11.4 Sottogruppi parabolici in $GL(V)$ e in $SL(V)$

In questa sezione $G \in \{GL(V), SL(V)\}$ e $\mathcal{F}$ è la bandiera

$$V_1 < V_2 < \ldots < V_{s-1}$$

di V. Poniamo inoltre

$$V_0 := \{0\} \text{ e } V_s := V.$$

Il normalizzante della serie $V_1 < V_2 < \ldots < V_{s-1}$ si dice **normalizzante** della bandiera $\mathcal{F}$ e lo indicheremo con $N_G(\mathcal{F})$. Questo è, ricordiamo, l'intersezione degli stabilizzatori dei sottospazi $V_1, V_2, \ldots, V_{s-1}$. I normalizzanti delle camere si dicono **sottogruppi di Borel** di G, i normalizzanti delle bandiere non massimali si dicono **sottogruppi parabolici** di G.

Lemma 11.4.1 *Se $\mathcal{H}$ è una bandiera di V, con $\mathcal{H} \subseteq \mathcal{F}$ allora $N_G(\mathcal{F}) \leq N_G(\mathcal{H})$.*

DIMOSTRAZIONE. $N_G(\mathcal{F})$ normalizza ciascun sottospazio di $\mathcal{F}$ da cui la tesi, poichè $\mathcal{H} \leq \mathcal{F}$. ∎

Lemma 11.4.2 *Sia $\mathcal{F}$ come sopra. Se W è un sottospazio proprio di V non contenuto in $\mathcal{F}$, allora esiste $\gamma \in N_G(\mathcal{F})$ tale che $W^\gamma \neq W$.*

DIMOSTRAZIONE. Supponiamo innanzitutto che $\mathcal{F}$ sia una camera (quindi $s = n$) e sia $(v_1, \ldots, v_n)$ una base di V tale che, per ogni $k \in \{1, \ldots, n\}$,

$$V_k = \langle v_1, \ldots, v_k \rangle.$$

Sia i il minimo intero positivo tale che $W \leq V_i$. Poiché V_{i-1} è un iperpiano di V_i che non contiene W, esiste un elemento w di W tale che $(v_1, \ldots, v_{i-1}, w)$ sia una base di V_i. Ne segue che anche

$$(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n)$$

è una base di V. Poichè $W \notin \mathcal{F}$ e $W \leq V_i$, esiste $t \in \{1, \ldots, i-1\}$, tale che

$$v_t \notin W.$$

Sia γ l'automorfismo di V, definito da

$$v_j^\gamma = v_j \text{ per ogni } j \in \{1, \ldots, n\} \setminus \{i\}$$

e

$$w^\gamma = w + v_t.$$

Allora

$$V_j^\tau = V_j \text{ per ogni } j \in \{1, \ldots, n\}$$

e

$$W^\tau \neq W,$$

perchè $w + v_t \in W^\gamma \setminus W$.

Supponiamo ora che $\mathcal{F}$ non sia una camera. Per il Lemma A.4.1 esiste una camera $\overline{\mathcal{F}}$ contenente $\mathcal{F}$ e non contenente W. Per la prima parte di questa dimostrazione, esiste un elemento $\gamma \in N_G(\overline{\mathcal{F}})$ tale che $W^\gamma \neq W$. Per il Lemma 11.4.1, $N_G(\overline{\mathcal{F}}) \leq N_G(\mathcal{F})$, da cui la tesi. ∎

Teorema 11.4.3 *Siano V e G come sopra e sia $\mathcal{P}$ l'insieme dei sottogruppi parabolici di G. L'applicazione*

$$\begin{array}{rccc} \phi\colon & \mathcal{F}(V) & \to & \mathcal{P} \\ & \mathcal{H} & \mapsto & N_G(\mathcal{H}) \end{array}$$

è biiettiva e inverte le inclusioni. In particolare, i sottogruppi parabolici massimali sono tutti e soli i normalizzanti dei sottospazi propri di V.

DIMOSTRAZIONE. Se $\mathcal{F}$ è come sopra, per il Lemma 11.4.2, $V_1, \ldots, V_{s-1}$ sono tutti e soli i sottospazi propri di V normalizzati da $N_G(\mathcal{F})$, da cui segue che ϕ è biiettiva. Per il Lemma 11.4.1 ϕ inverte le inclusioni. ∎

Proposizione 11.4.4 *G agisce transitivamente per coniugio sull'insieme dei suoi sottogruppi di Borel.*

DIMOSTRAZIONE. Segue immediatamente dalla Proposizione 11.1.10e dall'Esercizio 8.3.23. ■

11.4.1 Il radicale unipotente

Il **centralizzante** di $\mathcal{F}$ è il centralizzante della serie

$$V_0 < V_1 < V_2 < \ldots < V_s$$

e lo indicheremo con $C_G(\mathcal{F})$. $C_G(\mathcal{F})$ si dice anche **radicale unipotente** del gruppo $N_G(\mathcal{F})$.

Proposizione 11.4.5 *$C_G(\mathcal{F})$ è un p-sottogruppo normale di $N_G(\mathcal{F})$.*

DIMOSTRAZIONE. Segue dal teorema 10.2.9 ■

Lemma 11.4.6 *Se T è un p-sottogruppo di G, allora T centralizza una bandiera di V.*

DIMOSTRAZIONE. Segue per induzione su n dal lemma 8.2.8 ■

Osserviamo che, a differenza del normalizzante, il funtore che ad ogni bandiera associa il suo centralizzante non inverte le inclusioni:

Lemma 11.4.7 *Se $\mathcal{F}$ e $\mathcal{H}$ sono bandiere di V, allora*

$$\mathcal{H} \leq \mathcal{F} \text{ se e solo se } C_G(\mathcal{H}) \leq C_G(\mathcal{F}).$$

DIMOSTRAZIONE. Segue immediatamente dalle definizioni. ■

Corollario 11.4.8 *I p-sottogruppi di Sylow di G sono tutti e soli i centralizzanti delle camere, più precisamente l'applicazione che a ciascuna camera di V associa il suo centralizzante in G è una biiezione tra l'insieme delle camere e l'insieme dei p-sottogruppi di Sylow di G*

Osserviamo che, se $\gamma \in G$, e $(\mathcal{F})$ è una camera in V, allora

$$C_G((\mathcal{F})^\gamma) = (C_G(\mathcal{F}))^\gamma,$$

ne segue che la proposizione 11.1.10 poteva essere dedotta come conseguenza dei Teoremi di Sylow. Viceversa il coniugio dei p-sottogruppi massimali di G segue dai lemmi 11.4.6 e 11.4.7 e dalla proposizione 11.1.10. Si può anche provare che il centralizzante di una camera ha per ordine la massima potenza di p che divide G e quindi dedurre da 11.4.6, 11.4.7 e 11.1.10, il teorema di Sylow per il gruppo G relativamente al primo p (dove $p = char(K)$!).

Il radicale unipotente in un parabolico massimale

Sia W un sottospazio proprio di V. Indichiamo con Q_W il sottogruppo

$$C_{GL(V)}(W) \cap C_{GL(V)}(V/W).$$

Proposizione 11.4.9 *Sia W un sottospazio proprio di V e sia Q_W come sopra. Allora*

1. *Q_W è un p-sottogruppo normale di $N_{GL(V)}(W)$;*
2. *$Q_W \leq SL(V)$;*
3. *per ogni $\alpha \in Q_W$, l'applicazione*

$$\begin{array}{rccc} \kappa_\alpha\colon & V/W & \to & W \\ & v+W & \mapsto & [v,\alpha] \end{array}$$

   è un omomorfismo ben definito di spazi vettoriali;

4. *l'applicazione*

$$\begin{array}{rccc} \kappa\colon & Q_W & \to & Hom(V/W,W) \\ & \alpha & \mapsto & \kappa_\alpha \end{array}$$

   è un isomorfismo di gruppi (l'operazione in $Hom(V/W,W)$ è la somma puntuale),

5. *Q_W è abeliano elementare di ordine*

$$|K|^{dim(W)\times dim(V/W)}.$$

DIMOSTRAZIONE. Poniamo $H := N_{GL(V)}(W)$. Per 10.11 Q_W è normale in H e, per 10.2.11 Q_W è un p-gruppo. Il punto *2* segue dal Corollario 11.1.5. Poiché $[V,\alpha] \leq W$ e W è abeliano, per il Lemma 6.1.1, l'applicazione

$$\begin{array}{ccc} V & \to & W \\ v & \mapsto & [v,\alpha] \end{array}$$

è un omomorfismo di gruppi il cui nucleo contiene W, da cui segue *3*. Proviamo il punto *4*. Per il Lemma 6.1.1 ed il fatto che

$$[V,Q_W] \leq W \leq C_V(Q_W),$$

l'applicazione κ è un omomorfismo di gruppi, inoltre è iniettivo perchè $\alpha \in ker(\kappa)$ se e solo se $[v,\alpha] = 0$ per ogni $v \in V$, che implica $\alpha = 1$, poiché α è un automorfismo di V. Inoltre κ è suriettiva perché, se

$$\phi\colon V/W \to W$$

è un omomorfismo di spazi vettoriali, allora l'applicazione $\alpha_\phi\colon V \to V$, definita, per ogni $v \in V$ da

$$v^{\alpha_\phi} := v + (v+W)^\phi$$

è, come si vede facilmente, un elemento di Q_W tale che $\kappa_{\alpha_\phi} = \phi$. Il punto *5* segue immediatamente. Infine, se $N = O_p(H)$, allora $Q \leq N$ e, posto $U := C_V(N)$, segue che $U \leq W$. D'altra parte, poiché H normalizza N e V, H normalizza anche $C_V(N)$ e quindi $H \leq N_{GL(V)}(U)$. ∎

Dalla proposizione 11.4.9 segue, in particolare, che gli elementi di Q_W sono tutte e sole le applicazioni del tipo

$$\begin{array}{rccc} \alpha\colon & V & \to & V \\ & v & \mapsto & v + (v+W)^\phi \end{array}$$

al variare di ϕ in $End(V/W, V)$. Inoltre, se β è un altro elemento di Q_W, allora

$$v^{\alpha\beta} = v + [v, \alpha] + [v, \beta], \tag{11.15}$$

in particolare questo vale per le trasvezioni di centro contenuto in W ed asse contenente W (che sono evidentemente elementi di Q_W).

Lemma 11.4.10 *Q_W è generato dalle trasvezioni di centro contenuto in W ed asse contenente W.*

DIMOSTRAZIONE. Siano α e ϕ come sopra e siano $(v_1, \dots v_t)$ una base di W e $(v_1^*, \dots v_t^*)$ la sua base duale. Per ogni $i \in \{1, \dots, t\}$ le applicazioni

$$\begin{array}{rccc} \tau_i & V & \to & V \\ & v & \mapsto & v + ((v+W)^\phi)^{v_i^*} v_i \end{array}$$

sono trasvezioni di centro $\langle v_i \rangle$ (quindi contenuto in W) ed asse contenente W e, per 11.15,

$$v^\alpha = v + (v+W)^\phi = v + \sum_{i=1}^{t} ((v+W)^\phi)^{v_i^*} v_i = v^{\prod_{i=1}^t \tau_i},$$

cioè

$$\alpha = \prod_{i=1}^{t} \tau_i,$$

da cui la tesi. ∎

11.4.2 La Decomposizione di Levi

In questa sezione $G = GL(V)$, $H_0 := N_G(\mathcal{F})$ è un sottogruppo parabolico di G, dove $\mathcal{F}$ è la bandiera

$$V_1 < V_2 < \ldots < V_{s-1},$$

e Q è il radicale unipotente di H. Poniamo inoltre $V_0 = \{0\}$ e $V_s = V$ e, per ogni $i \in \{1, \ldots, s\}$, sia W_i sia un complemento di V_{i-1} in V_i e sia

$$L_0 := \bigcap_{i=1}^{s} N_G(W_i).$$

Infine sia

$$Z_i := \bigoplus_{j \in \{1,\ldots,s\} \setminus \{i\}} W_j$$

e sia

$$G_i := N_G(W_i) \cap C_G(Z_i).$$

La Decomposizione di Levi nei parabolici di $GL(V)$

Teorema 11.4.11 *Con le notazioni precedenti, posto $H := H_0$ e $L := L_0$, per ogni $i \in \{1, \ldots, s\}$, valgono le seguenti affermazioni:*

1. $W_i \cong V_i/V_{i-1}$;
2. $V_i = W_1 \oplus W_2 \oplus \ldots \oplus W_i$;
3. *G_i induce, per restrizione su W_i, tutto il gruppo $GL(W_i)$;*
4. *G_i induce sul quoziente V_i/V_{i-1} tutto $GL(V_i/V_{i-1})$;*
5. $L = G_1 \times G_2 \times \ldots \times G_s$;

Dimostrazione. I punti *1* e *2* seguono immediatamente dalle definizioni e per induzione su i. I Punti *3*, *4* seguono, per induzione su i, dal Teorema di Estensione per Linearità. Infine, per come sono stati definiti i G_i, il prodotto dei G_i è diretto e contenuto in L. Dal punto *3* segue che, per ogni $\lambda \in L$, esiste un elemento

$$\gamma \in G_1 \times G_2 \times \ldots \times G_s$$

tale che, per ogni $i \in \{1, \ldots, s\}$,

$$[W_i, \lambda\gamma] = \{0\},$$

da cui $\lambda = \gamma^{-1} \in G_1 \times G_2 \times \ldots \times G_s$. ∎

Corollario 11.4.12 *L è un complemento di Q in H.*

Dimostrazione. Per il punto *2*,

$$L \leq H$$

e, per ogni $i \in \{1, \ldots, s\}$,

$$[W_i, Q \cap H] \leq W_i \cap V_{i-1} = \{0\},$$

e quindi

$$Q \cap H = \{1\}.$$

Per i punti *4* e *5* del Teorema 11.4.11, per ogni $\gamma \in H$ esiste un elemento $\lambda \in L$ tale che $\gamma\lambda$ induce l'identità su ciascun quoziente V_i/V_{i-1}, e quindi $\gamma\lambda \in Q$, da cui la tesi. ■

La Decomposizione di Levi nei parabolici di $SL(V)$

Siano H_0, Q, L_0 ed i W_i come sopra. Sia questa volta $L := (L \cap SL(V))$ e $H := (H_0 \cap SL(V))$. Inoltre, per ogni $i \in \{1, \ldots, s\}$, sia

$$\pi_i \colon L_0 \to G_i$$

la proiezione di L_0 su G_i associata alla decomposizione

$$L_0 = G_1 \times G_2 \times \ldots \times G_s.$$

Teorema 11.4.13 *Con le notazioni precedenti,*

1. $(L)^{\pi_i} = G_i$ *per ogni* $i \in \{1, \ldots, s\}$*;*
2. L_0/L *è isomorfo al gruppo moltplicativo* K^**;*
3. L *è un complemento di* Q *in* $H \cap SL(V)$*.*

Dimostrazione. Sia $\gamma \in G_i$, sia $j \in \{1, \ldots, s\} \setminus \{i\}$ e $(w_1, \ldots, w_t)$ una base di W_j. Sia δ l'automorfismo di V che manda w_1 in $det(\gamma)^{-1}w_1$, e induce l'identità su $\langle w_2, \ldots, w_t\rangle$ e su ciascun W_l con $l \in \{1, \ldots, s\} \setminus \{j\}$. Allora

$$\gamma\delta \in L \cap SL(V)$$

e

$$(\gamma\delta)^{\pi_i} = \gamma,$$

che prova *1.* Il punto 2 segue dal fatto che, per il punto 5 del Teorema 11.4.11 il determinante è un omomorfismo suriettivo di gruppi da L a K^* il cui nucleo è $(L \cap SL(V))$. Infine, il punto 3 segue dal Corollario 11.4.12 e dalla Legge Modulare di Dedekind (2.1.4. ■

Complementi di Levi

Continuiamo con le notazioni precedenti e poniamo ora $R \in \{GL(V), SL(V)\}$, $H := H_0 \cap R$ e $L := L_0 \cap R$. Il sottogruppo L si dice **complemento di Levi** di Q in H e la decomposizione

$$H = QL$$

si dice **decomposizione di Levi** di H. Ovviamente L dipende dalla scelta dei sottospazi $W_1, \ldots, W_s$ e quindi non è unico. Osserviamo che se, in particolare, $\mathcal{F}$ è una camera, allora

$$L \cong (K^*)^n \text{ se } R = GL(V) \text{ e } L \cong (K^*)^{n-1} \text{ se } R = SL(V)$$

e quindi i sottogruppi di Borel sono risolubili. È possibile determinare l'azione di L su $C_G(\mathcal{F})$, quindi la decomposizione di Levi determina completamente la struttura dei sottogruppi parabolici di $GL(V)$ e di $SL(V)$; lo faremo nella sezione 11.4.3 nel caso dei parabolici massimali.

Matrici associate

Fissiamo, per ogni W_i una base $(v_{i,1}, v_{i,2}, \ldots, v_{i,n_i})$. Rispetto alla base

$$(v_{1,1}, v_{1,2}, \ldots, v_{1,n_1}, v_{2,1}, v_{2,2}, \ldots, v_{2,n_2}, \ldots, v_{s,1}, v_{s,2}, \ldots, v_{s,n_s})$$

le matrici associate agli elementi di $N_R(\mathcal{F})$ sono del tipo:

$$\begin{pmatrix} A_1 & 0 & 0 & . & . & . & 0 & 0 \\ X_{2,1} & A_2 & 0 & . & . & . & 0 & 0 \\ X_{3,1} & X_{3,2} & A_3 & . & . & . & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ X_{s,1} & X_{s,2} & X_{s,3} & . & . & . & X_{s,s-1} & A_s \end{pmatrix},$$

le matrici associate agli elementi di $C_R(\mathcal{F})$ sono del tipo:

$$\begin{pmatrix} I_1 & 0 & 0 & . & . & . & 0 & 0 \\ X_{2,1} & I_2 & 0 & . & . & . & 0 & 0 \\ X_{3,1} & X_{3,2} & I_3 & . & . & . & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ X_{s,1} & X_{s,2} & X_{s,3} & . & . & . & X_{s,s-1} & I_s \end{pmatrix},$$

le matrici associate agli elementi di L sono del tipo:

$$\begin{pmatrix} A_1 & 0 & 0 & . & . & . & 0 & 0 \\ 0 & A_2 & 0 & . & . & . & 0 & 0 \\ 0 & 0 & A_3 & . & . & . & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 0 & A_s \end{pmatrix},$$

dove $X_{i,j}$ è una matrice $n_j \times n_i$, I_i è la matrice identica $n_i \times n_i$ e A_i è una matrice invertibile $n_i \times n_i$, con $det(A_1)det(A_2)\ldots det(A_s) = 1$ se $R = SL(V)$.

11.4.3 Azione sul radicale di un parabolico massimale

In questa sezione vogliamo completare lo studio della struttura di un parabolico massimale, cioè dello stabilizzatore H di un sottospazio proprio W di V. Di solito questa viene definita tramite l'azione di un complemento di Levi L sul prodotto tensore $(V/W)^* \otimes W$ (dove $(V/W)^*$ è il duale dello spazio V/W). Per evitare di introdurre i prodotti tensoriali, qui useremo invece la nozione equivalente di azione su $Hom(V/W, W)$. Definita un'azione ρ del complemento di Levi su $Hom(V/W, V)$, proveremo che l'isomorfismo naturale $\kappa: Q \mapsto Hom(V/W, W)$ definito nella Proposizione 11.4.10 è un isomorfismo di L-insiemi tra (Q, γ) e $(Hom(V/W, W), \rho)$ (dove γ è l'azione per coniugio di L su Q). Chi preferisce i prodotti tensori può tradurre tutto usando l'isomorfismo canonico tra $(V/W)^* \otimes W$ e $Hom(V/W, W)$.

Poniamo $G \in \{GL(V), SL(V)\}$ e $Z = Z(G)$. Sia inoltre W un sottospazio proprio di V, $H := N_G(W)$ e $Q := Q_W = C_G(W) \cap C_G(V/W)$.

Lemma 11.4.14 *$C_G(Q) = QZ$.*

DIMOSTRAZIONE. Per la Proposizione 11.4.9 Q è un $p-$gruppo abeliano elementare normale in H. Per il Lemma 11.4.10, Q è generato dalle trasvezioni di centro contenuto in W ed asse contenente W. Sia $\gamma \in C_H(Q)$. Per il punto 2 della Proposizione 11.2.3 γ fissa tutti i sottospazi di dimensione 1 di W e tutti gli iperpiani contenenti W, quindi induce un'applicazione scalare su W ed un'applicazione scalare su V/W. D'altra parte, se $w^\gamma = aw$ per ogni $w \in W$ e $(v + W)^\gamma = bv + W$ per ogni $v + W \in V/W$, sempre per il punto 2 della Proposizione 11.2.3, dev'essere $b = a$, da cui segue che γ è contenuta in Z. ∎

Fissiamo un complemento U di W in V, siano

$$G_W := N_{GL(V)}(W) \cap C_{GL(V)}(U),$$

$$G_U := N_{GL(V)}(U) \cap C_{GL(V)}(W)$$

e sia

$$L := (G_W \times G_U) \cap G.$$

Per i teoremi 11.4.11 e 11.4.13 L è un complemento di Levi di Q in H. Ovviamente $G_W \times G_U$ normalizza W e V/W e, per il Teorema 11.4.11, $G(W)$ induce tutto $GL(W)$ su W e centralizza V/W mentre G_U centralizza W ed induce tutto $GL(V/W)$ su V/W. Sia γ l'azione per coniugio di $G_1 \times G_2$ su Q e sia ρ l'azione definita nella Proposizione 11.1.11, con

$$W_1 := V/W, \;\; W_2 := W, \;\; G_1 = G_U \text{ e } G_2 = G_W$$

e dove ρ_i è l'azione indotta da G_i su W_i ($i \in \{1, 2\}$). Per il Lemma 11.4.10, Q è generato dalle trasvezioni di centro contenuto in W ed asse contenente W. Sia τ è una di queste trasvezioni, per la Proposizione 11.2.2, esistono $\alpha \in V^*$, con $W \leq ker(\alpha)$, e $w \in W$ tali che, per ogni $v \in V$,

$$v^\tau = v + v^\alpha w.$$

Lemma 11.4.15 *Con le notazioni precedenti, per ogni per ogni $v \in V$,*

1. *se $\gamma \in G_1$, allora $v^{\tau^\gamma} = v + (v^{\gamma^{-1}})^\alpha w = v + v^{\alpha^{\gamma^*}} w$;*
2. *se $\gamma \in G_2$, allora $v^{\tau^\gamma} = v + v^\alpha w^\gamma$*

DIMOSTRAZIONE. Se $\gamma \in G_1$, allora γ centralizza W, quindi, per ogni $v \in V$,

$$v^{\tau^\gamma} = v^{\gamma^{-1}\tau\gamma} = (v^{\gamma^{-1}} + ((v^{\gamma^{-1}})^\alpha w)^\gamma = v + (v^{\gamma^{-1}})^\alpha w,$$

Supponiamo ora che $\gamma \in G_2$. Poichè γ centralizza V/W e, $W \leq ker(\alpha)$, segue che, per ogni $v \in V$,

$$(v^{\gamma^{-1}})^\alpha = v^\alpha,$$

dunque

$$v^{\tau^\gamma} = v^{\gamma^{-1}\tau\gamma} = (v^{\gamma^{-1}} + (v^{\gamma^{-1}})^\alpha w)^\gamma = v + v^\alpha w^\gamma$$

■

Teorema 11.4.16 *Con le notazioni precedenti, l'isomorfismo naturale*

$$\kappa \colon Q \mapsto Hom(V/W, W)$$

definito nella Proposizione 11.4.10, è un isomorfismo di L-insiemi tra (Q, γ) e $(Hom(V/W, W), \rho)$

DIMOSTRAZIONE.

Poichè Q è generato dalle trasvezioni di centro contenuto in W ed asse contenente W, basta provare che, se τ è una di queste trasvezioni e $\gamma \in G_i$, allora

$$(\tau^\gamma)^\kappa = (\tau^\kappa)^\gamma \tag{11.16}$$

dove, ricordiamo,

$$\tau^\gamma = \gamma^{-1}\tau\gamma$$

e

$$(\tau^\kappa)^\gamma = \gamma^{-1}\tau^\kappa \text{ se } \gamma \in G_1,$$

oppure

$$(\tau^\kappa)^\gamma = \tau^\kappa\gamma \text{ se } \gamma \in G_2.$$

Come nel Lemma 11.4.15 siano $\alpha \in V^*$, con $W \leq ker(\alpha)$, e $w \in W$ tali che, per ogni $v \in V$,

$$v^\tau = v + v^\alpha w$$

e quindi

$$(v + W)^{\tau^\kappa} = [v, \tau] = v^\alpha w.$$

Se $\gamma \in G_1$, dal punto *1* del Lemma 11.4.15, segue che

$$(v + W)^{(\tau^\gamma)^\kappa} = (v^{\gamma^{-1}})^\alpha w = (v^{\gamma^{-1}} + W)^{\tau^\kappa} = (v + W)^{\gamma^{-1}\kappa} = (v + W)^{(\tau^\kappa)^\gamma},$$

che prova 11.16 nel caso $\gamma \in G_1$. Supponiamo ora che $\gamma \in G_2$. Dal punto *2* del Lemma 11.4.15, segue che

$$(v+W)^{(\tau^\gamma)^\kappa} = v^\alpha w^\gamma = (v^\alpha w)^\gamma = ((v+W)^{\tau^\kappa})^\gamma = (v+W)^{(\tau^\kappa)\gamma} = (v+W)^{(\tau^\kappa)^\gamma},$$

da cui la tesi. ∎

11.4.4 Il reticolo dei sottogruppi contenenti un Borel

In questa sezione $G \in \{GL(V), SL(V)\}$, $B := N_G(\mathcal{F})$ è un sottogruppo di Borel di G, dove $\mathcal{F}$ è la camera

$$V_1 < V_2 < \ldots < V_{n-1},$$

e S è il radicale unipotente di B (quindi $S \in Syl_p(G)$). Vogliamo studiare il reticolo dei sottogruppi H con $B \leq H \leq G$. Mostreremo che questi sono, oltre a B e G, tutti e soli i sottogruppi parabolici di G contenenti B ed il reticolo di questi sottogruppi è isomorfo al reticolo dei sottoinsiemi di $\{V_1, V_2, \ldots, V_{n-1}\}$ ordinato per inclusione (cioè $X \leq Y$ se e solo se $Y \subseteq X$).

Lemma 11.4.17 *Sia k un intero positivo con $k < n$. Sia Ω_k l'insieme dei sottospazi di V di dimensione k. Allora l'azione indotta da G su Ω_k è primitiva.*

DIMOSTRAZIONE. Sia Λ un sottoinsieme di Ω_k tale che, per ogni $g \in G$, $\Lambda \cap \Lambda^g \in \{\Omega_k, \emptyset\}$. Proviamo che se Λ contiene almeno due elementi distinti, allora $\Lambda = \Omega_k$, da cui seguirà la tesi. Siano U e W due elementi distinti di Λ e sia $d := dim(U \cap W)$. Sia $\Omega_{k,d}$ il grafo il cui insieme dei vertici è Ω_k e due vertici sono adiacenti se e solo se la loro intersezione ha dimensione d. Chiaramente l'azione indotta da G su Ω_k conserva le dimensioni delle intersezioni, quindi G induce un gruppo di automorfismi del grafo $\Omega_{k,d}$. Per il Teorema del Completamento delle basi ed il Teorema di Estensione per Linearità, G è transitivo su Ω_k e lo stabilizzatore di un vertice X è transitivo sull'insieme dei vertici adiacenti a X. Per l'Esercizio A.5.3 $\Omega_{k,d}$ è connesso quindi, per l'Esercizio 8.3.41, G è primitivo su G su Ω_k. ∎

Corollario 11.4.18 *Se $G \in \{GL(V), SL(V)\}$, ogni sottogruppo parabolico massimale di G è un sottogruppo massimale di G.*

Corollario 11.4.19 *Sia $G \in \{GL(V), SL(V)\}$ e siano $\mathcal{F}_1$ e $\mathcal{F}_2$ due bandiere in $GP(V)$ con $\mathcal{F}_1 \leq \mathcal{F}_2$ e $|\mathcal{F}_1| = |\mathcal{F}_2| - 1$. Allora $N_G(\mathcal{F}_2)$ è un sottogruppo massimale di $N_G(\mathcal{F}_2)$*

DIMOSTRAZIONE. Sia $\mathcal{F}_2$ la bandiera

$$W_1 < \ldots W_{i-1} < W_i < W_{i+1} \ldots < W_k,$$

sia $\mathcal{F}_1$ la bandiera

$$W_1 < \dots W_{i-1} < W_{i+1} \dots < W_k$$

e sia, per $j \in \{1, 2\}$,

$$H_j := N_G(\mathcal{F}_j).$$

Per il Teorema 11.4.11 H_1 induce tutto $GL(W_{i+1}/W_{i-1})$ sul quoziente W_{i+1}/W_{i-1}. In particolare, per il Lemma 11.4.17 e per il Teorema di Corrispondenza per spazi vettoriali, H_1 è primitivo sui sottospazi Z tali che $dim(Z) = dim(W_i)$ e $W_{i+1} < Z < W_{i-1}$. Ma allora $H_2 = N_{H_1}(\mathcal{F}_2)$ è un sottogruppo massimale di H_1 ∎

Sia ora

$$I := \{1, \dots, n-1\},$$

J un sottoinsieme di I e

$$\{t_1, \dots, t_k\} := I \setminus J \text{ con } t_i < t_{i+1} \forall i \in I \setminus J.$$

Sia $\mathcal{F}_J$ la bandiera

$$V_{t_1} < \dots < V_{t_k}$$

e

$$P_J := N_G(\mathcal{F}_J),$$

con la convenzione che $P_\emptyset = G$. Per definizione P_J è un sottogruppo parabolico di G se e solo se J è un sottoinsieme proprio di I. Inoltre $P_I = B$ e, per il lemma 11.4.1, se $J \subseteq K \subseteq I$, allora $P_K \leq P_J$.

Corollario 11.4.20 *Con le notazioni precedenti i sottogruppi P_J al variare di J tra i sottoinsiemi di I sono tutti e soli i sottogruppi di G contenenti B. Inoltre, se $[G : B]$ è il reticolo dei sottogruppi di G contenenti B ordinato per inclusione e $\mathcal{P}(I)$ è il reticolo dei sottoinsiemi di I ordinato per inclusione, allora l'applicazione*

$$\begin{array}{rccc} \lambda\colon & \mathcal{P}(I) & \to & [G:B] \\ & J & \mapsto & P_J \end{array}$$

è un isomorfismo di reticoli.

11.4.5 Sottogruppi parabolici in $PGL(V)$ e $PSL(V)$

Anche in questa sezione K è un campo finito di caratteristica p e V è uno spazio vettoriale di dimensione n su K. Sia inoltre $G \in \{GL(V), SL(V)\}$ e $Z = Z(G)$ (in particolare $G/Z \in \{PGL(V), PSL(V)\}$). Il fatto che Z fissi tutti i sottospazi di V, e quindi tutte le bandiere, ci permette di definire i sottogruppi parabolici di G/Z anch'essi come stabilizzatori di bandiere. Si vede immediatamente che H è un parabolico di G se e solo se H/Z è un sottogruppo parabolico di G/Z e l'applicazione che manda H in H/Z è una biiezione tra l'insieme dei parabolici di G e l'insieme dei parabolici di G/Z. Se H è un parabolico di G, la decomposizione di Levi di H si conserva in H/Z. Poichè Z è

coprimo con H i p-radicali di H e di H/Z sono isomorfi e, se L è un complemento di Levi in H, L/Z è un complemento di Levi in H/Z.

Purtroppo in G/Z si perde l'azione sui vettori di V e questo crea qualche difficoltà nello studiare G/Z: ad esempio i p-sottogruppi di G/Z non possono pù essere definiti direttamente come centralizzanti di bandiere. Invece, se T è un $p$sottogruppo di G/Z ogni volta dovremo considerare l'intersezione T_0 della sua antiimagine con un p-Sylow di G. Fortunatamente il fatto che $|Z|$ sia coprimo con p ci facilita molto. In particolare faremo uso dei seguenti risultati che sono elementari tranne il punto 2 del Lemma 11.4.22 che segue dal Teorema 10.2.2.

Lemma 11.4.21 *Sia H un sottogruppo di $GL(V)$, sia $N \leq H \cap Z(GL(V)$ e sia $W \leq V$. Allora*

1. $N_{H/N}(W) = N_H(W)/N$;
2. $C_{H/N}(W) = C_H(W)N/N$.

Lemma 11.4.22 *Sia H un gruppo, sia $N \trianglelefteq H$ e sia T un sottogruppo normale di H di ordine coprimo con $|N|$. Allora*

1. $N_{H/N}(TN/N) = N_H(T)/N$;
2. *se T o N è risolubile, allora $C_{H/N}(TN/N) = N_H(T)/N$.*

Corollario 11.4.23 *Sia K un campo finito di caratteristica p e sia V uno spazio vettoriale di dimensione n su K. T un parabolico massimale in $PGL(V)$ o $PSL(V)$. Allora*

$$F^*(T) = O_p(T).$$

Dimostrazione. Sia $G \in \{GL(V), SL(V)\}$ e $Z = Z(G)$, sia $W \leq V$ tale che $T = N_G(W)/Z$ e sia Q il p-radicale di $N_G(W)$. Allora $O_p(T) = QZ/Z$ e, per il Lemma 11.4.14 ed il Lemma 11.4.22

$$C_T(O_p(T)) \leq C_{G/Z}(QZ/Z) = C_G(Q)Z/Z \leq ZQ/Z = O_p(T),$$

da cui la tesi. ∎

11.4.6 Caratteristica Locale e Teorema di Borel-Tits per $PSL(V)$

Quando abbiamo introdotto le rappresentazioni di gruppi, abbiamo osservato che uno strumento fondamentale, per studiare un gruppo astratto G, è quello di rappresentarlo come gruppo di automorfismi di una data struttura. Il problema è trovare la struttura giusta e, in mancanza d'altro, trovarla all'interno del gruppo G stesso: ad esempio, per dimostrare l'esistenza di p-sottogruppi Sylow in un gruppo G abbiamo usato la rappresentazione di G su una famiglia di certi suoi sottoinsiemi indotta dall'azione regolare a destra.

Un tipico problema nella classificazione dei gruppi semplici finiti è provare che un certo gruppo G è isomorfo ad un certo sottogruppo R del gruppo di automorfismi di una certa struttura X. Una metodo è quello di cercare di costruire una struttura Y possibilmente isomorfa a X ed una rappresentazione fedele di G su Y che sia simile a quella di R su X. L'isomorfismo tra X e Y induce un monomorfismo ϕ da G in $Aut(X)$. A questo punto siamo ridotti a confrontare i due sottogruppi R e G^ϕ di $Aut(X)$. Può benissimo accadere che R e G non siano isomorfi, ma eventuali informazioni ulteriori sulla struttura di G possono permetterci di identificare i due sottogruppi.

Una strategia per costruire la struttura Y è

1. costruire una struttura $\overline{X}$ isomorfa alla struttura X all'interno del gruppo R;

2. caratterizzare astrattamente (cioè senza far uso dell'azione di R su X) la struttura $\overline{X}$;

3. usando la caratterizzazione astratta di $\overline{X}$, costruire una struttura analoga in G.

Per esempio, sia X lo spazio proiettivo associato ad uno spazio vettoriale V di dimensione finita su un campo finito K, e sia $R = PSL(V)$. R è un gruppo di permutazioni transitivo sull'insieme X, quindi X è isomorfo come R-insieme all'insieme $\overline{X}$ delle classi laterali dello stabilizzatore in R di un elemento di X. Gli stabilizzatori L dei punti di R soddisfano, ad esempio, la proprietà $|R : L|=|X|$. Quindi i candidati per la struttura Y sono gli insiemi del tipo $G/\sim_M$ delle classi laterali destre dei sottogruppi M di G tali che $|G : M| = |X|$. Purtroppo, come osservato sopra, questo non basta per concludere che G è isomorfo a R; infatti il gruppo S_X contiene diversi sottogruppi non isomorfi che sono transitivi su X: A_X, per esempio, che non è isomorfo a $PSL(V)$. Le cose vanno meglio se si considera l'azione di $PSL(V)$ sulla geometria proiettiva $PG(V)$ che è una struttura più complessa dello spazio proiettivo. Infatti $PSL(V)$ agisce su $PG(V)$ conservando le dimensioni dei sottospazi e le inclusioni. Per l'esercizio **??**, la geometria proiettiva $PG(V)$ è isomorfa[1]alla geometria Γ delle classi laterali dei parabolici massimali di $PSL(V)$ contenenti un fissato sottogruppo di Borel, l'incidenza tra sottospazi si traduce nel fatto che le due classi laterali corrispondenti hanno intersezione non vuota e due sottospazi hanno la medesima dimensione se e solo se corrispondono a due classi laterali del medesimo parabolico. Quindi, per caratterizzare astrattamente la geometria Γ basta caratterizzare astrattamente in $PSL(V)$ i sottogruppi parabolici massimali contenenti un dato sottogruppo di Borel. Il seguente lemma permette di individuare i parabolici massimali una volta che si conosca la caratteristica del campo.

Lemma 11.4.24 *Sia V uno spazio vettoriale di dimensione finita su un campo finito K di caratteristica p e sia $G \in \{GL(V), SL(V), PGL(V), PSL(V)\}$.*

[1]Per la definizione astratta di geometria (geometria di Tits) e di isomorfismo di geometrie si veda la sezione 13.3

I sottogruppi parabolici massimali di G sono tutti e soli i sottogruppi p-locali massimali di G

DIMOSTRAZIONE. Se H è un sottogruppo parabolico di G, allora

$$O_p(H) \neq \{1\} \text{ e } H \leq N_G(O_p(H)),$$

quindi ogni sottogruppo parabolico è contenuto in un sottogruppo p-locale. Basta allora dimostrare che ogni sottogruppo p-locale di G è contenuto in un sottogruppo parabolico di G. Sia $G \in \{GL(V), SL(V)\}$, sia $Z \leq Z(G)$ e sia T un p-sottogruppo non identico di G. Poiché T è un p-gruppo che agisce sul p-gruppo V, per il Corollario 8.2.9,

$$\{0\} < C_V(T) < V.$$

Poiché p è coprimo con $|Z|$, per il Lemma 11.4.21 ed il Lemma 11.4.22,

$$N_{G/Z}(TZ/Z) = N_G(T)/Z \leq N_G(C_V(T) = N_{G/Z}(C_V(T),$$

da cui la tesi. ∎

A questo punto resta il problema di dare una caratterizzazione (o, meglio, approssimazione) astratta della caratteristica di K cosa faremo adesso. Se H è un gruppo e r è un numero primo, diremo che H ha **caratteristica** r se

$$F^*(H) = O_r(H).$$

Per esempio, dal Lemma 11.4.23 segue che i sottogruppi parabolici massimali di $PSL(V)$ hanno caratteristica p Un gruppo G si dice di **caratteristica locale** r (in Inglese **characteristic-r-type**) se ogni sottogruppo r-locale di G ha caratteristica r. Per il Teorema di Borel-Tits [6], che tra poco dimostreremo nel caso di $PSL(V)$, ogni gruppo semplice finito di tipo Lie su un campo di caratteristica p ha caratteristica locale p. Sarebbe bello se fosse vero anche il viceversa, cioè che un gruppo semplice finito di caratteristica locale p è un gruppo semplice finito di tipo Lie su un campo di caratteristica p, ma non lo è. Infatti, ad esempio, ogni gruppo alterno A_p ha caratteristica locale p, molti dei gruppi sporadici hanno caratteristica locale 2. Inoltre esistono gruppi che hanno una doppia caratteristica locale (per esempio A_5, $PSL(2,4)$ e $PSL(2,5)$ sono isomorfi tra loro e quindi hanno caratteristica locale sia 2 che 3). Cionondimeno, in tutti i controesempi i p-Sylow hanno sottogruppi abeliani elementari di ordine minore a 3. Purtroppo non si conoscono dimostrazioni di questo fatto che non facciano uso del Teorema di Classificazione dei Gruppi Semplici Finiti anche se è al momento in corso un progetto per dimostrarlo [24].

Lemma 11.4.25 *Sia H un gruppo di caratteristica p, allora H è di caratteristica locale p. In particolare un gruppo G è di caratteristica locale p se e solo se i suoi sottogruppi p-locali massimali hanno caratteristica p.*

DIMOSTRAZIONE. Sia $F = O_p(H)$, T un p-sottogruppo non identico di H, $L = N_H(T)$ e $Q = O_pL$. Allora

1. $T \leq Q$,
2. $TC_F(T) \leq T(F \cap L) \leq Q$
3. $TC_F(T)$ contiene il proprio centralizzante in TF.

Ne segue che se A è un sottogruppo di $C_L(Q)$ di ordine coprimo con p, allora A centralizza $TC_F(T)$ e dunque, per il teorema $P \times Q$ di Thompson (10.3.7), A centralizza TF e quindi F. Ma $C_H(F) \leq F$ che è un p-gruppo, e quindi $A = \{1\}$. Dunque $C_L(Q)$ non ha elementi di ordine coprimo con p da cui segue la tesi. ∎

Possiamo adesso dimostrare il Teorema di Borel-Tits per $PSL(V)$.

Teorema 11.4.26 (TEOREMA DI BOREL-TITS PER $PSL(V)$) *Sia K un campo finito di caratteristica p e sia V uno spazio vettoriale di dimensione finita su K. Allora $PSL(V)$ ha caratteristica locale p.*

DIMOSTRAZIONE. Sia H un sottogruppo p-locale massimale di $PSL(V)$. Per il Lemma 11.4.24, H è un sottogruppo parabolico massimale di G. Per il Lemma 11.4.23, H ha caratteristica p, da cui segue la tesi per il Lemma 11.4.25 ∎

11.5 Decomposizione di Bruhat *da fare*

Definizione di armatura.

11.6 Elementi di ordine coprimo con la caratteristica

Come prima siano K un campo finito di caratteristica p e V uno spazio vettoriale di dimensione n su K. In questa sezione studiamo gli elementi di $GL(V)$ ordine coprimo con la caratteristica di K.

Ovviamente tutti gli elementi dello stabilizzatore di un'armatura di V hanno ordine che divide $|K| - 1$, e quindi coprimo con la caratteristica di K. D'altra parte, si vede facilmente che questi non esauriscono gli elementi di ordine coprimo (almeno nel caso in cui K sia finito. Sia infatti F un'estensione di un campo finito K di grado n. È ben noto che la moltiplicazione per elementi di K induce sul gruppo additivo $(F, +)$ una struttura di spazio vettoriale su K di dimensione n. Indicheremo questo spazio con V_K^F. Poiché $\dim(V) = n = \dim(V_K^F)$, esiste un isomorfismo di K-spazi vettoriali

$$\xi: V \to V_K^F. \tag{11.17}$$

Per ogni elemento a di F, sia

$$\mu_a \colon V_K^F \to V_K^F$$

l'applicazione definita, per ogni $v \in V_K^F$, da

$$v^{\mu_a} = av$$

(in parole povere, μ_a è l'applicazione indotta su V_K^F dalla moltiplicazione per a). Per la proprietà distributiva, μ_a è un endomorfismo di V_K^F come spazio vettoriale su K e, come si verifica facilmente, l'applicazione

$$\begin{array}{rccc} \mu\colon & F & \to & End(V_K^F) \\ & a & \mapsto & \mu_a \end{array} \tag{11.18}$$

è un omomorfismo iniettivo di anelli. Inoltre l'applicazione

$$\begin{array}{ccc} End(V) & \to & End(V_K^F) \\ \phi & \mapsto & \xi\phi\xi^{-1} \end{array} \tag{11.19}$$

è, come si vede facilmente, un isomorfismo di anelli. Questo fatto ci permetterà di ridurci, nel caso irriducibile, ad identificare V con V_K^F per una opportuna estensione finita F di K ed a studiare gli automorfismi indotti su V_K^F per moltiplicazione con elementi non nulli di F. Il caso generale sarà poi una immediata conseguenza del Teorema di Maschke.

11.6.1 Potenze irriducibili di cicli di Singer I

Da (11.18) e (11.19), segue che $End(V)$ contiene un sottoanello isomorfo a F e quindi $GL(V)$ contiene un sottogruppo ciclico S di ordine $|K|^n - 1$ isomorfo al gruppo moltiplicativo F^*. Un qualsiasi generatore di S si dice **ciclo di Singer** di $GL(V)$.

Se ϕ è un automorfismo di uno spazio vettoriale V diremo che V è **ϕ-irriducibile** se gli unici sottospazi μ_a-invarianti di V_K^F sono V_K^F e lo spazio nullo. Chiaramente V è irriducibile per l'azione di un ciclo di Singer.

Lemma 11.6.1 *Con le notazioni precedenti, se $F = K(a)$, allora V_K^F è μ_a-irriducibile.*

DIMOSTRAZIONE. Se $F = K(a)$, ogni elemento di V_K^F si ottiene come combinazione lineare a coefficienti in K di potenze di a. Sia W un sottospazio μ_a-invariante di V_K^F con $W \neq \{0\}$. Ovviamente $W \subseteq V_K^F$, proviamo che

$$V_K^F \subseteq W.$$

Sia w un elemento non nullo di W. Poiché w è invertibile come elemento del campo F e V_K^F è generato come spazio vettoriale su K da potenze di a, esistono un intero non negativo t e degli elementi $k_0, \ldots, k_t$ in K, tali che

$$w^{-1} = k_0 + k_1 a + k_2 a^2 + \cdots + k_t a^t.$$

Poichè $w \in W$ e W è μ_a-invariante, segue che

$$\begin{aligned} 1 = ww^-1 &= w(k_0 + k_1 a + k_2 a^2 + \cdots + k_t a^t) \\ &= k_0 w + k_1 wa + k_2 wa^2 + \cdots + k_t wa^t = \\ &= k_0 w + k_1 w^{\mu_a} + k_2 w^{\mu_a^2} + \cdots + k_t w^{\mu_a^t} \in W \end{aligned}$$

Se $v \in V_K^F$, esistono, come sopra, $r \in \mathbf{N}$ ed $h_0, \ldots, h_r$ in K tali che

$$v = h_0 + h_1 a + h_2 a^2 + \cdots + h_r a^r.$$

Quindi

$$\begin{aligned} v = 1 \cdot v = &= 1.(h_0 + h_1 a + h_2 a^2 + \cdots + h_r a^r) \\ &= h_0 \cdot 1 + h_1 \cdot 1a + h_2 \cdot 1a^2 + \cdots + h_r \cdot 1a^r) \\ &= h_0 \cdot 1 + h_1 \cdot 1^{\mu_a} + h_2 \cdot 1^{\mu_a^2} + \cdots + h_r \cdot 1^{\mu_a^r} \in W \end{aligned}$$

da cui segue che $V_K^F \subseteq W$. ∎

Sia σ un ciclo di Singer su V e a un generatore di F^* tale che

$$\mu_a = \xi^{-1} sigma \xi$$

. Diremo che una potenza σ^k è una **potenza irriducibile** di σ se $F = K(a^k)$.

Viceversa, usando le rappresentazioni di anelli, mostreremo che, se ϕ è un automorfismo di uno spazio V di dimensione finita su un campo K e tale che V sia ϕ-irriducibile, allora esistono un'opportuna estensione algebrica $K(a)$ di K ed un isomorfismo di K-spazi vettoriali

$$\xi \colon V \to V_K^K(a)$$

tali che

$$\phi = \xi \mu_a \xi^{-1}.$$

11.6.2 Cenni di rappresentazioni di anelli

Abbiamo definito una rappresentazione di un gruppo G su una struttura algebrico relazionale X come un omomorfismo di gruppi da G ad $Aut(X)$, che è un gruppo rispetto alla composizione. Ora, se X è un gruppo abeliano (o uno spazio vettoriale) V, l'insieme $End(V)$, degli endomorfismi di V, è un anello rispetto alla somma puntuale ed alla composizione di applicazioni. Questo ci permette di definire le rappresentazioni di anelli e svilupparne la teoria in modo analogo a quanto fatto con i gruppi. In questa sezione ci limiteremo ad introdurre i risultati elementari di questa teoria limitandoci (più o meno) ad i risultati di cui avremo bisogno per caratterizzare i cicli di Singer.

Sia V un gruppo abeliano ed R un anello con identità. Una **rappresentazione** ρ di R su V è un omomorfismo di anelli con identità da R nell'anello degli endomorfismi di V:

$$\rho \colon R \to End(V).$$

Come per gli automorfismi, anche per gli endomorfismi useremo la notazione esponenziale: l'immagine di un elemento v tramite un endomorfismo f sarà indicata con v^f. La coppia (V, ρ) si dice **R-modulo (destro)**; quando non sarà necessario specificare la rappresentazione ρ indicheremo, come al solito, il modulo (V, ρ) semplicemente con V e, per ogni $r \in R$ e $v \in V$ scriveremo v^r al posto di $v^{\rho(r)}$.

ESEMPI

1. Se V è un gruppo abeliano (o uno spazio vettoriale), R un sottoanello di $End(V)$ e ι è l'immersione di R in $End(V)$, allora (V, ι) è un R-modulo.

2. Se V è uno spazio vettoriale su un campo K, V è un K-modulo, dove la rappresentazione di K su V è quella che a ciascun elemento k di K associa la moltiplicazione per lo scalare k.

3. Sia V un gruppo abeliano e sia $z \in Z$. L'applicazione

$$\begin{array}{rccc} \mu_z\colon & V & \to & V \\ & v & \mapsto & v^z \end{array}$$

è un endomorfismo di V e l'applicazione

$$\begin{array}{rccc} \mu\colon & \mathbf{Z} & \to & End(V) \\ & r & \mapsto & \mu_z \end{array}$$

è una rappresentazione di $\mathbf{Z}$ su V. In questo modo, ogni gruppo abeliano ha una struttura naturale di $\mathbf{Z}$-modulo, ogni omomorfismo di gruppi abeliani è un omomorfismo di $\mathbf{Z}$-moduli e quindi la teoria dei gruppi abeliani coincide essenzialmente con la teoria degli $\mathbf{Z}$-moduli.

4. Sia V uno spazio vettoriale sul campo K e α un endomorfismo di V. Per ogni polinomio

$$p(x) := a_0 + a_1 x + \ldots + a_n x^n$$

in $K[x]$ sia $p(\alpha)$ la **valutazione** di $p(x)$ su α:

$$p(\alpha) := a_0 + a_1 \alpha + \ldots + a_n \alpha^n.$$

Allora l'applicazione

$$\begin{array}{rccc} \nu_\alpha\colon & K[x] & \to & End(V) \\ & p(x) & \mapsto & p(\alpha) \end{array} \tag{11.20}$$

è una rappresentazione di $K[x]$ su V. Vedremo in seguito come la struttura di V come $K[x]$-modulo via ν_α qui descritta sia molto utile per studiare le proprietà dell'endomorfismo α .

Analogamente a quanto fatto per le rappresentazioni di gruppi su insiemi, se V è un R-modulo, un **sotto-R-modulo** è un sottogruppo W di V tale che, per ogni $r \in R$, risulti

$$W^r \subseteq W.$$

Un R-modulo V si dice **semplice** o **irriducibile** se possiede esattamente due sotto-R-moduli: questo significa che $\{0\}$ e V sono gli unici sottomoduli e che $V \neq \{0\}$.

Lemma 11.6.2 *Sia $\alpha \in End(V)$ e ν_α) definita come in 11.20. Allora V è irriducibile se e solo se il $K[x]$-modulo (V, ν_α) è irriducibile.*

DIMOSTRAZIONE. Segue immediatamente dal fatto che $\alpha = \nu_\alpha(x)$ ■

Se $X \subseteq V$, anche l'intersezione $\langle X \rangle$ dei sotto-R-moduli di V che contengono X è ancora un sotto-R-modulo di V e si dice sotto-R-modulo di V **generato** da X. Un sotto-R-modulo W di V si dice **finitamente generato** se esiste un sottoinsime finito X di V tale che $W = \langle X \rangle$. In particolare, se $|X| = 1$, il sottomodulo $\langle X \rangle$ si dice **ciclico** e, se $X = \{v\}$, come al solito, lo indicheremo con $\langle v \rangle$ invece che con $\langle \{v\} \rangle$. Si vede facilmente che,

$$\langle v \rangle = \{v^r | r \in R\}. \tag{11.21}$$

Se U e W sono sottomoduli di V, il sottomodulo generato da U e V coincide con il sottogruppo $U + V$ generato da U e V. Se U e W sono R-moduli, la somma diretta di gruppi abeliani $U \oplus W$ eredita naturalmente da U e W una struttura di R-modulo ponendo, per ogni $(u, w) \in U \oplus W$ ed $r \in R$,

$$(u, w)^r := (u^r, w^r).$$

Con tale rappresentazione l'R-modulo $U \oplus W$ si dice **somma diretta (esterna)** degli R-moduli U e W. Come per i gruppi abeliani, se U e W sono sotto R-moduli di V tali che $V = U + W$ e $U \cap W = \{0\}$, allora U è isomorfo (come R-modulo alla somma diretta $U \oplus W$. In tal caso diremo che V è **somma diretta (interna)** di U e W.

Una congruenza $\equiv$ sul gruppo V tale che, per ogni $v, w \in V$ ed ogni $r \in R$, risulti

$$v \equiv w \text{ se e solo se } v^r \equiv w^r$$

si dice **compatibile con la rappresentazione** ρ di R o semplicemente **R-congruenza** di V. Le R-congruenze sono tutte e sole le congruenze di V associate ai sottogruppi di V che sono anche sotto-R-moduli. Se W è un sotto-R-modulo di V, il gruppo quoziente V/W eredita naturalmente da V una struttura di R-modulo ponendo, per ogni $v + W \in V/W$ ed $r \in R$,

$$(v + W)^r = v^r + W;$$

il fatto che W sia un sotto-R-modulo garantisce che questa definizione non dipende dalla scelta del rappresentante v di $v + W$. Con tale rappresentazione V/W si dice **modulo quoziente di V modulo il sottomodulo** W (a parziale giustificazione della cacofonia, si noti che la parola "modulo" è usata con due significati diversi nella definizione precedente).

Se U e V sono R-moduli, un omomorfismo di gruppi

$$\phi: U \to V$$

tale che, per ogni $u \in U$ e $r \in R$, risulti

$$\phi(u^r) = (\phi(u))^r$$

si dice **omomorfismo di R-moduli**. Due U e V si dicono **isomorfi** se esiste un **isomorfismo** (cioè un omomorfismo biiettivo di R-moduli) tra U e V. Se V e W sono R-moduli, indicheremo rispettivamente con $End_R(V)$ e $Aut_R(V)$, l'anello degli R-endomorfismi ed il gruppo degli R-automorfismi di V. Dalla definizione segue immediatamente che

Lemma 11.6.3 *$End_R(V) = C_{End(V)}(R)$, dove*

$$C_{End(V)}(R) := \{\alpha \in End(V) | v^{\alpha r} = v^{r\alpha} \text{ per ogni } v \in V \text{ e } r \in R\}.$$

In seguito avremo bisogno del seguente risultato:

Lemma 11.6.4 *Sia V uno spazio vettoriale sul campo K, siano α e β endomorfismi di V e siano ν_α e ν_β definite come in 11.20. Se (V, ν_α) e (V, ν_β) sono isomorfi come $K[x]$-moduli, allora esiste un elemento γ di $GL(V)$ tale che $\alpha = \gamma\beta\gamma^{-1}$.*

Dimostrazione. Supponiamo che γ sia un isomorfismo di $K[x]$-moduli tra (V, ν_α) e (V, ν_β), allora $\gamma \in GL(V)$ e, per ogni $v \in V$,

$$v^{\alpha\gamma} = (v^\alpha)^\gamma = (v^{\nu_\alpha(x)})^\gamma = (v^\gamma)^{\nu_\beta(x)} = (v^\gamma)^\beta = v^{\gamma\beta},$$

quindi, per ogni $v \in V$,

$$v^\alpha = v^{\gamma\beta\gamma^{-1}},$$

da cui la tesi. ∎

Vale il Primo Teorema di Omomorfismo per R-moduli (lasciamo al lettore il compito di enunciarlo e dimostrarlo). Osserviamo che per ogni $r \in R$, l'applicazione

$$\begin{array}{rccc} \delta_r: & R & \to & R \\ & s & \mapsto & sr \end{array}$$

è un endomorfismo del gruppo abeliano $(R, +)$ e l'applicazione

$$\begin{array}{rccc} \delta: & R & \to & End(R,+) \\ & r & \mapsto & \delta_r \end{array}$$

è una rappresentazione di R su R e si chiama **rappresentazione regolare (destra)** di R su se stesso e l'R-modulo (R, δ) si dice **R-modulo regolare (destro)**. Si verifica immediatamente che i sotto-R-moduli del modulo regolare sono esattamente gli ideali destri di R.

Se $v \in V$, posto

$$Ann_R(v) := \{r \in R | v^r = 0\}$$

risulta che $Ann_R(v)$ è un ideale destro di R (quindi un sottomodulo del modulo regolare) e, se V è ciclico generato da v, vale il seguente risultato (che come il teorema sull'indice dello stabilizzatore (8.2.7) è una conseguenza immediata del Primo Teorema di Omomorfismo):

Teorema 11.6.5 *Sia R un anello e (V, ρ) un R-modulo destro ciclico generato da v ($v \in V$). Allora l'applicazione*

$$\begin{array}{rccc} \gamma\colon & R & \to & V \\ & r & \mapsto & v^r \end{array}$$

è un omomorfismo tra gli R-moduli (R, δ) e (V, ρ). In particolare (V, ρ) è isomorfo al modulo quoziente $R/Ann_R(v)$. e γ induce una biiezione tra gli ideali destri di R contenenti $Ann_R(v)$ ed i sottomoduli di (V, ρ).

Anche per gli omomorfismi di R-moduli vale il Teorema di Corrispondenza:

Teorema 11.6.6 *(*Teorema di Corrispondenza per Moduli*) Sia R un anello e M ed N due R-moduli. $\phi\colon M \to N$ un omomorfismo di gruppi e $K = \ker \phi$. Sia $\mathcal{L}$ il reticolo dei sottomoduli di M contenenti K e $\mathcal{L}'$ il reticolo dei sottomoduli di N che sono contenuti in $\phi(M)$. Allora l'applicazione che ad ogni $H \in \mathcal{L}$ associa $\phi(H)$ è un isomorfismo di reticoli tra $\mathcal{L}$ e $\mathcal{L}'$.*

Analogamente a quanto accade nelle rappresentazioni di gruppi, se (V, ρ) è un R-modulo, il nucleo di ρ coincide con

$$Ann_R(V) := \bigcap_{v \in V} Ann_R(v)$$

e questo è anche il massimo ideale bilatero contenuto in ciascun $Ann_R(v)$ al variare di v in V. In particolare, se R è un anello commutativo e V è ciclico generato da v, allora

$$Ann_R(v) = Ann_R(V).$$

Si noti però anche che, a differenza di quanto accade nelle azioni transitive di gruppi, un R-modulo ciclico può avere sottomoduli ed essere anche decomponibile come somma diretta di sottomoduli (ad esempio il gruppo ciclico di ordine 6 ha sottogruppi propri e si decompone come somma diretta di un gruppo ciclico di ordine 2 ed uno di ordine 3), infine un R-modulo può essere indecomponibile in somma diretta di sottomoduli propri e, ciononostante, possedere sottomoduli propri (ad esempio un sottogruppo ciclico di ordine 4).

Il seguente risultato è una conseguenza immediata del Teorema 11.6.5 e del Teorema di Corrispondenza.

Corollario 11.6.7 *Sia R un anello e sia V un R-modulo. Allora V è irriducibile se solo se $Ann_R(V)$ è un ideale massimale di V.*

11.6.3 Potenze irriducibili di cicli di Singer II

Sia α un endomorfismo di V tale che V sia α-irriducibile.

Per il Teorema 11.6.5 ed il Corollario 11.6.7 (e ricordando che $K[x]$ è commutativo), esiste un ideale massimale M di $K[x]$ tale che

$$V \text{ è isomorfo, come } K[x]\text{-modulo, a } K[x]/M.$$

Poiché M è massimale, l'anello quoziente $K[x]/M$ è un campo, anzi, più precisamente è un'estensione di K di grado n (vedi, ad esempio [17], Teorema 5.3.1). Indichiamo con F il campo $K[x]/M$ e sia $a := x + M$. Allora $F = K(a)$ e quindi, se μ è definita come in 11.18,

$$\mu_a \text{ è una potenza irriducibile di un ciclo di Singer di } V_K^F.$$

Ne segue che V_K^F è uno spazio vettoriale μ_a-irriducibile di dimensione n su K e, di nuovo, esiste un ideale massimale $\overline{M}$ di $K[x]$, tale che

$$V_K^F \text{ è isomorfo, come } K[x]\text{-modulo, a } K[x]/\overline{M}.$$

Poiché la funzione μ manda ogni elemento di M nell'endomorfismo nullo di V_K^F, segue che $M \leq \overline{M}$, cioè V_K^F è isomorfo ad un quoziente di V. Poiché V e V_K^F hanno la medesima dimensione come spazi vettoriali su K segue che

$$(V, \nu_\alpha) \text{ e } (V_K^F, \nu_{\mu_a}) \text{ sono isomorfi come } K[x]\text{-moduli.}$$

In particolare, per il Lemma 11.6.4, α è una potenza irriducibile di un ciclo di Singer di $GL(V)$. Abbiamo così dimostrato il seguente teorema:

Teorema 11.6.8 *Sia n un intero positivo, K un campo finito e sia V uno spazio vettoriale di dimensione n su K. Sia α un elemento di $GL(V)$ tale che V sia α-irriducibile. Allora α è una potenza irriducibile di un ciclo di Singer di $GL(V)$.*

11.6.4 Automorfismi coprimi di uno spazio vettoriale

In quanto segue V è uno spazio vettoriale di dimensione finita su un campo finito K di caratteristica p, A è un sottogruppo di $GL(V)$ di ordine coprimo con p e R_A è il sottoanello di $End(V)$ generato da A. Poichè ogni elemento di R_A è combinazione lineare a coefficienti in K di elementi di A, segue immediatamente che R_A è un anello commutativo e che gli R_A-sottomoduli di V sono esattamente i sottospazi A-invarianti di V. In particolare

Lemma 11.6.9 *V si decompone come somma diretta di R_A-moduli irriducibili.*

DIMOSTRAZIONE. Sia $n := dim(V)$. Proviamo il Teorema per induzione su n. Se $n = 0$ o V è irriducibile la tesi è ovvia. Supponiamo $n > 0$, V non irriducibile e la tesi vera per ogni intero non negativo minore di n. Sia U un R_A-sottomodulo non nullo di dimensione minima. Allora U è irriducibile

e, per il Teorema di Maschke (Teorema 10.2.20), U ha un complemento A-invariante W, Per l'osservazione precedente W è un R_A-sottomodulo di V e $dim(W) = n - dim(U) < n$. Per ipotesi induttiva W è somma diretta di R_A-sottomoduli irriducibili, da cui la tesi. ∎

Ci siamo quindi ridotti a studiare gli R_A-moduli irriducibili. Quello che segue è, probabilmente, il risultato più importante sugli R-moduli irriducibili.

Lemma 11.6.10 LEMMA DI SCHUR *Sia R un anello e V un R-modulo irriducibile. Allora $End_R(V)$ è un anello con divisione.*

DIMOSTRAZIONE. Proviamo che ogni elemento non nullo di $End_R(V)$ è invertibile. Sia $\phi \in End_R(V) \setminus \{0\}$. Allora $\ker(\phi) < V$ e $\{0\} < Im(\phi)$. Poiché $\ker(\phi)$ e $Im(\phi)$ sono sottomoduli di V e V è irriducibile segue che $\ker(\phi) = \{0\}$ e $Im(\phi) = V$, cioè ϕ è un automorfismo e quindi è invertibile. ∎

Corollario 11.6.11 *Se V è irriducibile come R_A-modulo, allora A è ciclico, di ordine coprimo con la caratteristica di K ed ogni suo generatore induce una potenza irriducibile di un ciclo di Singer su V.*

DIMOSTRAZIONE. Poichè R_A è un anello commutativo, per il Lemma 11.6.3,

$$A \subseteq R_A \leq C_{End(V)}(R_A) = End_{R_A}(V).$$

Poichè V è un R_A-modulo irriducibile $End_{R_A}(V)$ è un anello con divisione, in particolare R_A è un campo, perché sottoanello commutativo finito di un anello con divisione, e A è un sottogruppo moltiplicativo di un campo e quindi è ciclico per l'Esercizio 3.5.13. Inoltre, se p è la caratteristica di K e $L \in Syl_p(A)$, per il Corollario 8.2.8 $C_V(L)$ è un sotto A-modulo non nullo di V e quindi coincide con V, perché V è irriducibile. Ma allora $L \leq C_{GL(V)}(V) = \{1\}$, e quindi A è coprimo con la caratteristica di K. Infine l'ultima affermazione segue dal Teorema 11.6.8. da cui la tesi. ∎

Osserviamo che $End_{R_A}(V)$ è sempre commutativo perché, per il Teorema di Wedderburn, ogni anello con divisione finito è un campo, ma, ovviamente, contiene R_A (A) solo se R_A (A) è commutativo.

Teorema 11.6.12 *Sia $\rho: A \to GL(V)$ una rappresentazione di un gruppo abeliano finito A su uno spazio vettoriale V di dimensione finita su un campo finito K e supponiamo che $|A|$ sia coprimo con la caratteristica di K. Allora V è somma diretta di sottospazi A-invarianti minimali*

$$V_1 \oplus V_2 \oplus \ldots \oplus V_k. \tag{11.22}$$

Per ogni $i \in \{1, \ldots k\}$, sia $A_i := Aut_A(V_i)$, allora A_i è ciclico e ogni generatore di A_i induce su V_i una potenza irriducibile di un ciclo di Singer.

DIMOSTRAZIONE. La decomposizione in 11.22 esiste per Lemma 11.6.9. Per il Corollario 11.6.11, A_i è ciclico e ogni generatore di A_i è una potenza irriducibile di un ciclo di Singer di $GL(V_i)$ ■

Per un gruppo abeliano A indichiamo con $\mathcal{C}(A)$ l'insieme dei sottogruppi L di A tali che A/L sia ciclico

Corollario 11.6.13 *Con le notazioni del Teorema 11.6.12,*

$$V = \langle C_V(L) | L \in \mathcal{C}(A) \rangle \tag{11.23}$$

DIMOSTRAZIONE. Siano, per ogni $i \in \{1, \ldots, k\}$ V_i ed A_i come nella dimostrazione del Teorema 11.6.12. Poichè $A_i \cong A/C_A(V_i)$ e A_i è ciclico, segue che $C_A(V_i) \in \mathcal{C}(A)$ per ogni $i \in \{1, \ldots, k\}$. Da cui segue la tesi, poiché $V_i \leq C_V(C_A(V_i))$ e quindi

$$V = \bigoplus_{i=1}^{k} V_i \leq \sum_{i=1}^{k} C_V(C_A(V_i)) \leq \sum_{L \in \mathcal{C}(A)} C_V(L) \leq V.$$

■

La dimostrazione del seguente lemma mostra come risultati sull'azione coprima sugli spazi vettoriali possono essere generalizzati a risultati sull'azione coprima sui gruppi.

Corollario 11.6.14 *Sia A un gruppo abeliano finito che agisce su un gruppo B di ordine coprimo con $|A|$. Allora*

$$B = \langle C_B(L) | L \in \mathcal{C}(A) \rangle$$

DIMOSTRAZIONE. Sia B un controesempio di ordine minimo.

Prima riduzione: *B è un r-gruppo per un opportuno numero primo r.*

Infatti, per il Teorema 10.2.5, B è il prodotto dei suoi sottogruppi di Sylow A-invarianti. Se l'ordine di B non è la potenza di un numero primo, ogni sottogruppo di Sylow T di B ha ordine minore di B e quindi, se T è A-invariante,

$$T = \langle C_T(L) | L\mathcal{C}(A) \rangle$$

D'altra parte, $C_T(L) \leq C_B(L)$ per ogni $T \leq B$ e quindi

$$\begin{aligned} B &= \langle T | T \in Syl(B) \text{ e } T^A = T \rangle = \langle C_T(L) | T \in Syl(B),\ T^A = T \text{ e } L \in \mathcal{C}(A) \rangle \\ &= \langle C_B(L) | L \in \mathcal{C}(A) \rangle, \end{aligned}$$

contro l'ipotesi.

Seconda riduzione: *B è abeliano elementare.*

Per il Teorema 10.2.6 $A/C_A(V)$ si rappresenta fedelmente su $B/\Phi(B)$, in particolare, per ogni $L \leq A$,

$$L \leq C_A(B) \text{ se e solo se } L \leq C_A(B/\Phi(B))$$

e quindi, per la scelta minimale di B, se $(\Phi(B) \neq \{1\}$,

$$B/\Phi(B) = \langle C_{B/\Phi(B)}L | L \in \mathcal{C}(A)\rangle = \langle C_B L | L \in \mathcal{C}(A)\rangle,$$

contro l'ipotesi.

Quindi B è un r-gruppo abeliano elementare, in particolare uno spazio vettoriale sul campo con r elementi, da cui segue la contraddizione finale per il Corollario 11.23 ■

Moduli su domini a ideali principali

Finiamo questa sezione con un breve cenno alla struttura dei moduli finitamente generati su domini ad ideali principali. Non useremo nel seguito del libro i risultati citati in questo paragrafo, e per le dimostrazioni rimandiamo a [17] o [21]. Tuttavia questi risultati sono fondamentali per lo studio dei gruppi lineari (e non solo) e, per questo motivo li segnaliamo al lettore.

Se R è un dominio ad ideali principali (in particolare se $R = \mathbf{Z}$ oppure R è l'anello $K[x]$ dei polinomi a coefficienti in un campo K), ogni R-modulo V finitamente generato è isomorfo ad una somma diretta di R-moduli ciclici (e quindi di quozienti dell'R-modulo regolare R); questo è il Teorema di Struttura dei Moduli Finitamente Generati su Domini ad Ideali Principali ([21] sezione 3.8).

La decomposizione di V come somma diretta di sotto-R-moduli ciclici

$$V \cong V_1 \oplus V_2 \oplus \ldots \oplus V_t \tag{11.24}$$

in generale non è unica, nemmeno a meno di una permutazione degli indici, ma ci sono due tipi di decomposizione particolarmente utili:

Una si ottiene scegliendo i sotto-R-moduli ciclici $V_1, V_2, \ldots, V_t$ in modo tale che,

$$Ann_R(V_1) \geq Ann_R(V_2) \geq \ldots \geq Ann_R(V_t).$$

In questo caso i generatori degli ideali $Ann_R(V_1), Ann_R(V_2), \ldots, Ann_R(V_t)$ si dicono **divisori elementari** dell'R-modulo V. Si osservi che,

$$Ann_R(V_t) = Ann_R(V). \tag{11.25}$$

Inoltre, posto $V_i = \langle v_i \rangle$, poiché R è commutativo, risulta

$$Ann_R(V_i) = Ann_R(v_i)$$

L'altra decomposizione si ottiene scegliendo i sottomoduli ciclici $V_1, V_2, \ldots, V_t$ in modo tale che gli ideali $Ann_R(V_i$ siano primari e, in questo caso i generatori degli ideali $Ann_R(V_1), Ann_R(V_2), \ldots, Ann_R(V_t)$ si dicono **fattori invarianti** dell'R-modulo V.

Si osservi che i sottomoduli che compaiono nelle due decomposizioni non sono ovviamente gli stessi, né il numero di fattori nelle due decomposizioni è lo stesso.

Abbiamo già parlato di divisori elementari e di fattori invarianti nella sezione 3.4 sulla struttura deii gruppi abeliani e una facile riflessione dovrebbe convincere il lettore che i fattori invarianti ed i divisori elementari di un gruppo abeliano A sono rispettivamente i fattori invarianti ed i divisori elementari dello $\mathbf{Z}$-modulo (A, μ). E, infatti, il Teorema di Struttura dei Gruppi Abeliani Finiti è un caso particolare del Teorema di Struttura dei Moduli Finitamente Generati su Domini ad Ideali Principali (ogni gruppo abeliano finito è finitamente generato come $\mathbf{Z}$-modulo!).

Chiaramente sia la successione dei fattori invarianti sia quella dei divisori elementari di un R-modulo V individuano V a meno di isomorfismi e viceversa queste successioni sono determinate da V a meno di una permutazione e della moltiplicazione per elementi invertibili di R, in particolare due R-moduli U e V sono isomorfi se e solo se hanno le stesse successioni di divisori elementari (di fattori invarianti), a meno di una permutazione e del prodotto per elementi invertibili di R.

Il seguente risultato discende immediatamente dal Teorema di Struttura dei Moduli Finitamente Generati su Domini ad Ideali Principali:

Teorema 11.6.15 *Siano α e β due endomorfismi di uno spazio vettoriale V sul campo K. Allora α e β sono coniugate tramite un elemento di $GL(V)$ se e solo se i $K[x]$-moduli (V, ν_α) e (V, ν_β) hanno gli stessi divisori elementari (fattori invarianti).*

Sia α un endomorfismo di uno spazio vettoriale V sul campo K, sia

$$V \cong V_1 \oplus V_2 \oplus \ldots \oplus V_t$$

una decomposizione del $K[x]$-modulo (V, ν_α) come somma diretta di sottomoduli ciclici tali che

$$Ann_{K[x]}(V_1) \geq Ann_{K[x]}(V_2) \geq \ldots \geq Ann_{K[x]}(V_t)$$

e, per ogni $i \in \{1, \ldots, t\}$, sia $m_i(x)$ un generatore monico di $Ann_{K[x]}(V_i)$. Poniamo

$$m_\alpha(x) := m_t(x)$$

e

$$\chi_\alpha(x) := \prod_{i \in 1}^{t} m_i(x).$$

Il polinomio $m_\alpha(x)$ si dice **polinomio minimo** di α. Si vede facilmente che $m_\alpha(x)$ è il polinomio monico di grado minimo che annulla l'endomorfismo α, cioè tale che

$$v^{m_\alpha(\alpha)} = 0$$

per ogni $v \in V$. Inoltre ogni polinomio che annulla α è un multiplo di $m_\alpha(x)$.

Il polinomio $\chi_\alpha(x)$ si chiama **polinomio caratteristico** di α (ed è proprio il solito polinomio caratteristico).

Teorema 11.6.16 *Sia α un endomorfismo di uno spazio vettoriale V sul campo K. Il $K[x]$-modulo (V, ν_α) è ciclico se e solo se il polinomio minimo di α coincide con il polinomio caratteristico di α.*

11.6.5 Automorfismi di GL(V) DA FARE

11.7 Esercizi

Esercizio 11.7.1 *Sia $\alpha \in GL(V)$. Provare che l'applicazione $\gamma_\alpha: V \to V$ definita, per ogni $v \in V$ da*

$$\gamma_\alpha(v) = [v, \alpha]$$

è un omomorfismo di spazi vettoriali di nucleo $C_V(\alpha)$ e immagine $[V, \alpha]$. In particolare $dim([V, \alpha]) + dim(C_V(\alpha)) = dim(V)$.

Esercizio 11.7.2 *Sia V uno spazio vettoriale sul campo con p elementi e sia $\alpha \in GL(n, p)$ e $A := \langle \alpha \rangle$. Provare che α è una trasvezione se e solo se*

1. *$|V|/|C_V(A)| \leq |A|$ e*
2. *A* **agisce in modo quadratico su** *V, cioè $[V, A, A] = \{0\}$.*

. (Si osservi che le due condizioni implicano che $C_V(\alpha)$ è un iperpiano di V e quindi, per l'Esercizio 11.7.1 $|[V, \alpha]| = p$).

Esercizio 11.7.3 *Con le notazioni della Proposizione 11.4.10, per ogni $\lambda \in K$ ed ogni $\alpha \in Q_W$, definiamo l'applicazione $\lambda\alpha$nel modo seguente:*

$$\begin{array}{rccc} \lambda\alpha: & V & \to & V \\ & v & \mapsto & v + \lambda[v, \alpha] \end{array} .$$

1. *Si provi che $\lambda\alpha \in Q_W$;*
2. *si provi che l'applicazione $K \times Q_W : Q_W$ che alla coppia (λ, α) associa la funzione $\lambda\alpha$ definisce una struttura di spazio vettoriale sul campo K su Q_W;*
3. *si provi che, con tale struttura di spazio vettoriale su Q_W, l'applicazione κ è un isomorfismo di spazi vettoriali;*
4. *si provi che se τ è una trasvezione di centro Z ed asse U con $Z \leq W \leq U$, allora $\tau \in Q_W$ ed il sottogruppo radice $R_{Z,U}$ è il sottospazio di W generato da τ.*

Esercizio 11.7.4 *Sia Σ un armatura in $P(V)$ dimostrare che ogni bandiera in $\Delta(\Sigma)$ è contenuta in una camera di $\Delta(\Sigma)$*

Esercizio 11.7.5 *Provare che il sottografo $\Delta(\Sigma)$ del grafo $\mathcal{F}(V)$ è connesso*

Esercizio 11.7.6 *Provare che, date due bandiere $\mathcal{F}_1$ e $\mathcal{F}_2$, esiste un'armatura Σ che le supporta entrambe.*

Esercizio 11.7.7 *Provare che il grafo $\mathcal{F}(V)$ è connesso*

Esercizio 11.7.8 *Siano $\mathcal{F}_1$ e $\mathcal{F}_2$ due bandiere di V e siano Σ e Σ^* due telai che supportano entrambe sia $\mathcal{F}_1$ che $\mathcal{F}_2$. Provare che esiste un elemento $\gamma \in N_{PGL(V)}(\mathcal{F}_1) \cap N_{PGL(V)}(\mathcal{F}_2)$, tale che $\Sigma^\gamma = \Sigma^*$*

Esercizio 11.7.9 *Provare che $PGL(V)$ è transitivo sulle coppie $(\Sigma, \mathcal{F})$, dove Σ è un'armatura in V e $\mathcal{F}$ è una bandiera supportata da Σ*

Esercizio 11.7.10 *Sia $G \in \{GL(V), SL(V)\}$ e $\mathcal{F}$ una bandiera in V. Provare che $N_G(\mathcal{F}) = N_G(C_G(\mathcal{F}))$ (suggerimento: usare l'induzione sul rango di $\mathcal{F}$).*

Esercizio 11.7.11 *Sia $\tau \in SL(V)$. Si provi τ è una trasvezione se e solo se $C_V(\tau)$ è un iperpiano;*

Capitolo 12

Forme bilineari e isometrie

12.1 Forme bilineari

In quanto segue, K è un campo, V, è uno spazio vettoriali su K e f è una **forma bilineare** su V, cioè una funzione

$$f: V \times V \to K$$

tale che, per ogni $a \in K$ ed ogni $v_1, v_2, w_1, w_2 \in V$, le seguenti condizioni sono soddisfatte:

1. $f(v_1 + v_2, w_1) = f(v_1, w_1) + f(v_2, w_1)$;
2. $f(v_1, w_1 + w_2) = f(v_1, w_1) + f(v_1, w_2)$;
3. $f(av_1, w_1) = af(v_1, w_1) = f(v_1 + aw_1)$.

Il termine "bilineare" è giustificato dal fatto che, come si vede immediatamente, una funzione $f: V \times V \to K$ è bilineare se e solo se, per ogni $\overline{v}, \overline{w} \in V$, le applicazioni

$$\begin{array}{rccc} f_{\overline{v}}: & V & \to & K \\ & w & \mapsto & f(\overline{v}, w) \end{array} \tag{12.1}$$

e

$$\begin{array}{rccc} f_{\overline{w}}: & V & \to & K \\ & v & \mapsto & f(v, \overline{w}) \end{array} \tag{12.2}$$

sono lineari.

Osserviamo che $f_{\overline{v}}$ e $f_{\overline{w}}$ sono elementi del duale V^* di V e le applicazioni

$$\begin{array}{rccc} \sigma_f: & V & \to & V^* \\ & v & \mapsto & f_{\overline{v}} \end{array} \tag{12.3}$$

e

$$\begin{array}{rccc} \delta f: & V & \to & V^* \\ & w & \mapsto & f_{\overline{w}} \end{array} \tag{12.4}$$

sono lineari.

f si dice **degenere** se esiste un vettore z in V tale che $f(zv) = 0$ per ogni $v \in V$.

Lemma 12.1.1 *Le seguenti affermazioni sono equivalenti:*

1. *f è non degenere;*
2. *$ker(\sigma_f) = \{0\}$;*
3. *$ker(\delta_f) = \{0\}$;*

Sia ora

$$(v_1, v_2, \ldots, v_n)$$

una base di V e sia

$$(v_1^*, v_2^*, \ldots, v_n^*)$$

la sua base duale. Se la forma bilineare f non è degenere, l'applicazione σ_f è un isomorfismo tra V ed il suo duale V^* e quindi, posto, per ogni $i \in \{1, \ldots, n\}$,

$$v_i^\wedge := (v_i^*)^{\sigma_f^{-1})},$$

la n-upla

$$(v_1^\wedge, v_2^\wedge, \ldots, v_n^\wedge) \tag{12.5}$$

è una base di V tale che

$$f(v_i, v_j^\wedge) = \delta_{i,j} \text{ per ogni } i, j \in \{1, \ldots n\} \tag{12.6}$$

dove $\delta_{i,j}$ è il Delta di Kronecker. Chiameremo la base 12.5 **base duale rispetto alla forma** f della base $(v_1, v_2, \ldots, v_n)$. Osserviamo che le condizioni 12.6 caratterizzano completamente la base 12.5. Infatti si poteva dimostrare direttamente che esiste un unica n-upla di vettori $(v_1^\wedge, v_2^\wedge, \ldots, v_n^\wedge)$ che verifica le condizioni 12.6 e tale n-upla è una base di V. Osserviamo infine che, in generale, $(v_i^\wedge)^\wedge$ non coincide con v_i (ad esempio, se f è alternante, $(v_i^\wedge)^\wedge = -v_i$). Ciononostante, nei casi delle forme blineari che ci interessano soprattutto, le forme bilineari simmetriche o alternanti (o forme sesquilineari), sarà sempre

$$\langle (v_i^\wedge)^\wedge \rangle = \langle v_i \rangle. \tag{12.7}$$

Lemma 12.1.2 *Sia $(v_1, ..., v_n)$ una base di V. f è completamente determinata dai valori che assume sulle coppie (v_i, v_j), ossia dalla matrice $(f(v_i, w_j))_{i,j}$ di n righe e n colonne a coefficienti in K.*

Dimostrazione. Se

$$v = \sum_{i=1}^{n} a_i v_i \text{ e } w = \sum_{j=1}^{n} b_j v_j,$$

la tesi si ottiene sviluppando per bilinearità $f(v,w)$. ∎

Con le notazioni precedenti, la matrice

$$G_f := (f(v_i, v_j))_{i,j}$$

si dice **matrice di Gram** associata a f rispetto alla base $(v_1, ..., v_n)$ di V. Posto

$$\mathbf{a} := (a_1, ..., a_n)$$

e

$$\mathbf{b} := (b_1, ..., b_n)$$

$f(v,w)$ è uguale al prodotto righe per colonne

$$\mathbf{a} G_f \mathbf{b}^t,$$

(dove $\mathbf{b}^t$ è la trasposta della n-upla riga $(b_1, .., b_m)$). Osserviamo che la matrice di Gram G_f coincide con la matrice associata a σ_f rispetto alla base $(v_1, ..., v_n)$ ed alla sua base duale $(v_1^*, ..., v_n^*)$ dello spazio duale V^*. In particolare

Lemma 12.1.3 *Con le notazioni precedenti f è non degenere se e solo se G_f è non degenere*

12.1.1 Forme bilineari riflessive

In questa sezione f è una forma bilineare **riflessiva** su V, cioè una forma bilineare su V che verifica la seguente proprietà:

$$f(v,w) = 0 \text{ implica che } f(w,v) = 0.$$

Il **nucleo** (o **radicale**) di f è l'insieme

$$rad(f) := \{z \in V | f(v,z) = 0 \text{ per ogni } v \in V\}.$$

Si vede facilmente che $rad(f)$ è un sottospazio di V e f è degenere se e solo se $rad(f) \neq \{0\}$. Se W è un sottospazio di V l'insieme

$$W^\perp := \{v \in V | f(v,w) = 0 \text{ per ogni } w \in W\}$$

si dice **ortogonale** di W. Chiaramente $V^\perp = rad(V)$. Se U e W sono sottospazi di V tali che $U \leq W^\perp$ e $U \cap W = \{0\}$ diremo che il sottospazio $U+W$ è **somma diretta ortogonale** di U e W.

I seguenti due risultati dovrebbero essere ben noti. La facile dimostrazione segue dalle definizioni ed è lasciata al lettore.

Lemma 12.1.4 *Se U e W sono sottospazi di V risulta*

1. *$U \leq W$ se e solo se $W^\perp \leq U^\perp$,*

2. $W \leq (W^\perp)^\perp$.

Se f è non degenere, abbiamo una relazione precisa tra un sottospazio W ed il suo ortogonale:

Lemma 12.1.5 *Sia f è non degenere e siano U e W sottospazi di V, allora*

1. $dim(W) = dim(V) - dim(W^\perp)$,
2. $W = (W^\perp)^\perp$,
3. *se $W \cap W^\perp = \{0\}$, V è somma diretta ortogonale di W e $W^\perp$*
4. $\langle U^\perp, W^\perp\rangle = (U \cap W)^\perp$ *e* $U^\perp \cap W^\perp = \langle U \cap W\rangle^\perp$

Lemma 12.1.6 *Sia f non degenere e U un sottospazio isotropo di V e sia X un complemento di U in $U^\perp$. Allora $X \cap X^\perp = \{0\}$.*

Dimostrazione. Poiché $X \leq U^\perp$, risulta

$$U \leq X^\perp,$$

quindi, per il punto 4 del Lemma 12.1.5,

$$\langle X^\perp, X\rangle = \langle X^\perp, U, X\rangle = \langle X^\perp, U^\perp\rangle = (W \cap U)^\perp = \{0\}^\perp = V$$

■

Lemma 12.1.7 *Sia f non degenere, $(v_1, \ldots, v_n)$ una base di V e $(v_1^\wedge, \ldots, v_n^\wedge)$ la sua base duale rispetto a f. Se $W = \langle v_1, \ldots, v_k\rangle$, allora $W^\perp = \langle v_{k+1}^\wedge, \ldots, v_n^\wedge\rangle$*

Dimostrazione. Chiaramente

$$\langle v_{k+1}^\wedge, \ldots, v_n^\wedge\rangle \leq W^\perp = \langle v_1, \ldots, v_k\rangle^\perp$$

e quindi la tesi segue dal punto 1. del Lemma 12.1.5. ■

Un sottospazio W di V si dice **isotropo** (o **totalmente isotropo**) se $W \leq W^\perp$ (o, equivalentemente, se f induce la forma nulla su W, cioè $f(w_1, w_2) = 0$ per ogni $w_1, w_2 \in W$). Un vettore w di V si dice **isotropo** se $\langle w\rangle$ è isotropo.

Osserviamo che se Z è un sottospazio di $V^\perp$, allora f induce una forma bilineare (che, come al solito, indichiamo ancora con f) su V/Z, ponendo, per ogni $v, w \in V$,

$$f(v + Z, w + Z) := f(v, w).$$

Infatti questa applicazione è ben definita perchè $Z \leq V^\perp$ ed è chiaramente bilineare (lasciamo le facili verifiche per esercizio).

Lemma 12.1.8 *Sia f una forma bilineare riflessiva su uno spazio V, sia $Z \leq V^\perp$ e W un sottospazio di V contenente Z. Allora*

1. *W è isotropo se e solo se W/Z è isotropo;*
2. *in particolare f induce una forma bilineare non degenere su $V/V^\perp$;*
3. *Se U è un sottospazio di V con $Z \leq U \leq Z^\perp$, allora $Z \leq U^\perp$ e $(U/Z)^\perp = U^\perp/Z$.*

DIMOSTRAZIONE. Tutte le affermazioni seguono immediatamente dall'osservazione precedente. ∎

Un sottospazio U di V si dice **piano iperbolico** se ha dimensione 2 ed esiste una base (u, v) di U tale che u e v sono isotropi e $f(u, v) = 1$. In tal caso diremo che la coppia di vettori (u, v) è una **coppia iperbolica** . Un sottospazio H di V si dice **iperbolico** spazio iperbolico se H è somma diretta ortogonale di piani iperbolici.

12.1.2 Forme bilineari alternanti

In questa sezione f è una forma bilineare f **alternante** su V, cioè una forma bilineare su V tale che

$$f(v, v) = 0 \text{ per ogni } v \in V. \tag{12.8}$$

Se v e w sono vettori di V, sviluppando per bilinearità $f(v + w, v + w)$, otteniamo

$$0 = f(v+w, v+w) = f(v, v) + f(w, w) + f(v, w) + f(w, v) = f(v, w) + f(w, v),$$

cioè

$$f(v, w) = -f(w, v) \text{ per ogni } v, w \in V. \tag{12.9}$$

In particolare:

Lemma 12.1.9 *Ogni forma bilineare alternante su V è riflessiva.*

Se la caratteristica di K è diversa da 2, si può dimostrare facilmente che la 12.9 implica la 12.8, se la caratteristica è 2 la condizione 12.8 è più forte della condizione 12.9.

Lemma 12.1.10 *Sia v un vettore di V non contenuto in $rad(f)$. Allora esiste un vettore u tale che (u, v) sia una coppia iperbolica.*

DIMOSTRAZIONE. Se $w \in V \setminus \langle v \rangle^\perp$, allora, posto

$$u := f(v, w)^{-1} w,$$

la coppia (u, v) è iperbolica. ∎

Proposizione 12.1.11 *Sia H un sottospazio iperbolico massimale di V. Allora $V = (H^\perp)^\perp$ ed è somma diretta ortogonale di H e $H^\perp$. In particolare, se f è non degenere, $V = H$ ed ha dimensione pari.*

DIMOSTRAZIONE. Segue per induzione su $dim(V)$, il Lemma 12.1.5 ed il Lemma 12.1.10 ∎

Uno **spazio simplettico** è una coppia (V, f) dove V è uno spazio vettoriale e f è una forma bilineare alternante non degenere su V. Come al solito, quando non sarà necessario specificare la forma f, useremo il simbolo V per indicare lo spazio simplettico (V, f).

Se f è non degenere, abbiamo visto che V ha dimensione pari. Sia $dim(V) = 2n$ con $n \in \mathbf{N} \setminus \{0\}$. Una base $(u_1, w_1, \ldots, u_n, w_n)$ di V si dice **iperbolica** le coppie (u_i, w_i) sono iperboliche e V è somma diretta ortogonale dei piani iperbolici

$$\langle u_i, w_i \rangle.$$

Lemma 12.1.12 *Se $(u_1, w_1, \ldots, u_n, w_n)$ è una base iperbolica di V, allora*

$$(u_1^\wedge, w_1^\wedge, \ldots, u_n^\wedge, w_n^\wedge) = (w_1, -u_1, \ldots, w_n, -u_n)$$

DIMOSTRAZIONE. Segue immediatamente dalla definizione di base iperbolica e dall'unicità della base duale. ∎

Matrici di Gram associate ad una forma simplettica

Chiaramente la matrice di Gram associata ad f rispetto ad una base iperbolica $(u_1, w_1, \ldots, u_n, w_n)$ di V è una matrice diagonale a blocchi del tipo

$$\begin{pmatrix} T & 0 & . & . & . & 0 \\ 0 & T & . & . & . & 0 \\ 0 & 0 & . & . & . & 0 \\ 0 & 0 & . & . & . & 0 \\ 0 & 0 & . & . & . & 0 \\ 0 & 0 & . & . & . & T \end{pmatrix} \tag{12.10}$$

dove T è la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{12.11}$$

In seguito, per visualizzare alcuni sottogruppi del gruppo delle isometrie di V, come sottogruppi di matrici sono utili anche altre due basi che si ottengono permutando gli elementi della base $(u_1, v_1, \ldots, u_n, v_n)$: una è la base

$$(u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n); \tag{12.12}$$

rispetto a questa base la matrice di Gram associata a f diventa:

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \tag{12.13}$$

dove I è la matrice identica $n \times n$. L'altra è la base

$$(u_1, u_2, \ldots, u_n, v_n, v_{n-1}, \ldots, v_1); \tag{12.14}$$

rispetto a questa base la matrice di Gram associata a f diventa:

$$\begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix} \tag{12.15}$$

dove J è la matrice

$$\begin{pmatrix} 0 & 0 & . & . & . & 0 & 1 \\ 0 & 0 & . & . & . & 1 & 0 \\ 0 & 0 & . & . & . & 0 & 0 \\ 0 & 0 & . & . & . & 0 & 0 \\ 0 & 1 & . & . & . & 0 & 0 \\ 1 & 0 & . & . & . & 0 & 0 \end{pmatrix}. \tag{12.16}$$

12.2 Isometrie

In quanto segue, K è un campo, V, è uno spazio vettoriale su K e f è una **forma bilineare** su V.

Sia W uno spazio vettoriale su K e $g\colon W \times W \to K$ una forma bilineare su W. Un'isomorfismo di spazi vettoriali $\gamma\colon V \to W$ si dice (f, g)-**isometria** (o, semplicemente **isometria**) se, per ogni $(v, w) \in V \times V$,

$$g(v^\gamma, w^\gamma) = f(v, w).$$

In tal caso diremo che gli spazi V e W sono (f, g)-**isometrici** isometrici, spazi (o **isometrici**). Un'**isometria di** V (o **isometria su** V) è una (f, f)-isometria di V in se stesso. L'insieme delle isometrie di V è un sottogruppo del gruppo degli automorfismi di V e si chiama **gruppo delle isometrie** gruppo delle isometrie di (V, f) e si indica con $O(V, f)$. In generale ($O(V, f)$ è un sottogruppo proprio di $Aut(V)$, però, se f è la forma costantemente nulla i due gruppi coincidono:

Lemma 12.2.1 *Se $f(v, w) = 0$ per ogni v, w in V, allora $O(V, f) = Aut(V, f)$.*

Lemma 12.2.2 *Sia $(v_1, ..., v_n)$ una base di V, sia W un'altro spazio vettoriale sul campo K e sia g una forma bilineare su W. Un isomorfismo di spazi vettoriali $\alpha\colon V \to W$ è un'isometria di se e solo se, per ogni $i, j \in \{1, \ldots, n\}$, $f(v_i, v_j) = g(v_i^\alpha, v_j^\alpha)$.*

Dimostrazione. Se

$$v = \sum_{i=1}^{n} a_i v_i \text{ e } w = \sum_{j=1}^{n} b_j v_j,$$

la tesi si ottiene sviluppando per bilinearità $f(v,w)$ e $g(v^\alpha, w^\alpha)$. ∎

Corollario 12.2.3 *Sia $(v_1, u_1, \ldots, v_n, u_n)$ una base iperbolica di V e $\gamma \in Aut(V)$. Allora $\gamma \in O(V,f)$ se e solo se*

$$(v_1^\gamma, u_1^\gamma, \ldots, v_n^\gamma, u_n^\gamma)$$

è un'altra base iperbolica di V

Teorema 12.2.4 *Due spazi simplettici sono isometrici se e solo se hanno la medesima dimensione.*

DIMOSTRAZIONE. Segue immediatamente dal Corollario 12.2.3 e dalla Proposizione 12.1.11 ∎

Se μ in $GL(V)$, G è la matrice di Gram associata a f ed M è la matrice associata a μ entrambe rispetto alla base $(v_1, ..., v_n)$, allora

$$f(v^\mu, w^\mu) = \mathbf{a}MG\mathbf{b}M^t = \mathbf{a}MGM^t\mathbf{b}^t. \tag{12.17}$$

In particolare, μ è un'isometria di (V,f) se e solo se la 12.17 vale per ogni $\mathbf{a}, \mathbf{b} \in K^n$, cioè se e solo se

$$MGM^t = G. \tag{12.18}$$

Dalla 12.18, poichè $det(M) = det(M^t)$, segue

Lemma 12.2.5 *Siano μ ed M come sopra. Se f è non degenere, allora $det(M) \in \{1, -1\}$.*

Una proprietà importante delle isometrie è che, se G è un gruppo d'isometrie che fissa un sottospazio W, chiaramente G lascia invariato anche il sottospazio $W^\perp$ e le due azioni indotte da G rispettivamente su W e su $V/W^\perp$, sono legate l'una con l'altra come si può evincere dal seguente risultato. Più avanti, nel caso delle forme simplettiche, daremo la relazione precisa tra queste due azioni.

Teorema 12.2.6 PROPRIETÀ FONDAMENTALE DELLE ISOMETRIE *Sia f una forma bilineare riflessiva su uno spazio vettoriale V, sia G un sottogruppo di $O(V,f)$ e siano U e W sottospazi di V.*

1. *Se $[U,G] \leq W$, allora $[W^\perp, G] \leq U^\perp$.*

2. *In particolare, se f è non degenere,*

$$[U,G] \leq W \text{ se e solo se } [W^\perp, G] \leq U^\perp.$$

DIMOSTRAZIONE. Poiché γ è un'isometria, se $[U, G] \leq W$, per ogni $z \in W^{\perp}$, $\gamma \in G$ e $u \in U$, risulta

$$\begin{aligned} f(u, [z, \gamma]) &= f(u, -z + z^{\gamma}) = f(u, -z) + f(u, z^{\gamma}) = \\ &= f(-u, z) + f(u^{\gamma^{-1}}, z) = f(-u + u^{\gamma^{-1}}, z) = \\ &= f([u, \gamma^{-1}], z) = 0 \end{aligned}$$

da cui segue la prima affermazione. La seconda segue immediatamente dalla prima scambiando rispettivamente U e W con $W^{\perp}$ e $U^{\perp}$ e tenendo presente che, poiché f è non degenere, per ogni sottospazio X di V risulta $X = X^{\perp\perp}$. ∎

Lemma 12.2.7 *Se V e G sono come nel Teorema 12.2.6, allora*

$$[V, G] \leq (C_V(G))^{\perp}.$$

Se f è non degenere, allora vale l'uguaglianza:

$$[V, G] = (C_V(G))^{\perp}.$$

DIMOSTRAZIONE. Poiché

$$[C_V(G), G] = \{0\}$$

e

$$V = \{0\}^{\perp},$$

la tesi segue immediatamente dal Teorema 12.2.6. ∎

Sia W un sottospazio di V e sia H il normalizzante di W in $O(V, f)$. Se f è una forma bilineare riflessiva non degenere, la relazione tra le azioni indotte da H su W e, rispettivamente, sullo spazio quoziente $V/W^{\perp}$ può essere descritta precisamente utilizzando l'azione duale: Siano infatti ρ l'azione indotta da H su W, sia ρ^* la sua azione duale (vedi 11.7) su V^* e sia $\overline{r}ho$ l'azione indotta da H sullo spazio quoziente $V/W^{\perp}$. Sia, infine, σ_f definita come in 12.3.

Lemma 12.2.8 *Con le notazioni precedenti l'applicazione σf è un omomorfismo suriettivo da V in W^* il cui nucleo è $W^{\perp}$ ed inoltre induce un isomorfismo di H-insiemi tra $(V/W^{\perp}, \overline{\rho})$ e (W^*, ρ^*).*

DIMOSTRAZIONE. Abbiamo già visto che σ_f è lineare ed è suriettivo con nucleo $W^{\perp}$ perché f è non degenere. Se $\gamma \in H$, indichiamo con γ^* l'immagine di γ tramite la rappresentazione duale ρ^*. Allora, per ogni $v, w \in W$,

$$w^{(v^{\gamma})^{\sigma_f}} = f(v^{\gamma}, w) = f(v, w^{\gamma^{-1}}) = w^{(v^{\sigma_f})^{\gamma^*}},$$

cioè

$$(v^{\gamma})^{\sigma_f} = (v^{\sigma_f})^{\gamma^*},$$

da cui la tesi. ∎

Abbiamo già sottolineato che, quando si studia una rappresentazione di un gruppo su una certa struttura, è importante studiare le relazioni tra questa rappresentazione e quelle indotte sulle sottostrutture e sulle strutture quozienti. Il risultato principale in questo senso sarà il Lemma di Witt che dimostreremo nella prossima sezione nel caso delle forme simplettiche. Chiudiamo ora, dimostrando alcuni risultati elementari ma che ci saranno molto utili in seguito. In particolare ci permettono di ridurre lo studio dei gruppi di isometrie a quelli che conservano una forma bilineare non degenere.

Lemma 12.2.9 *Sia f una forma bilineare riflessiva su uno spazio V, sia $G := O(V, f)$, sia V la somma diretta ortogonale di due sottospazi Z e U e siano rispettivamente $\alpha \in O(Z, f_Z)$ e $\beta \in O(U, f_U)$. Allora esiste un'unico elemento $\delta \in G$ che induce per restrizione α su Z e β su U. In particolare*

$$N_G(Z) \cap N_G(U) \cong O(Z, f_Z) \times O(U, f_U).$$

DIMOSTRAZIONE. Poiché V è la somma diretta di Z e U, esiste un'unica applicazione lineare δ che induce per restrizione α su Z e β su U. Chiaramente δ è un'isomorfismo e, se $z_1, z_2 \in Z$ e $u_1, u_2 \in U$, allora

$$\begin{aligned} f((z_1+u_1)^\delta, (z_2+u_2)^\delta) &= f(z_1^\alpha + u_1^\beta, z_2^\alpha + u_2^\beta) = f(z_1^\alpha, z_2^\alpha) + f(u_1^\beta, u_2^\beta) = \\ &= f(z_1, z_2) + f(u_1, u_2) = f(z_1 + u_1, z_2 + u_2), \end{aligned}$$

cioè $\delta \in G$. ∎

Corollario 12.2.10 *Sia f una forma bilineare riflessiva su uno spazio V, sia $G := O(V, f)$ e sia U un complemento di $V^\perp$ in V. Allora*

1. *$V^\perp$ è invariante per l'azione di G;*
2. *siano rispettivamente $\alpha \in GL(V^\perp)$ e $\beta \in O(U, f)$, allora esiste un'unico elemento $\delta \in G$ che induce per restrizione α su $V^\perp$ e β su U.*
3. *$N_G(U) \cong GL(V^\perp) \times O(U, f)$,*
4. *se $\gamma \in G$ e $\overline{\gamma}$ è l'applicazione lineare indotta da γ sullo spazio quoziente $V/V^\perp$, cioè*
$$(v + V^\perp)^{\overline{\gamma}} := v^\gamma + V^\perp,$$
allora $\overline{\gamma} \in O(V/V^\perp, f)$;
5. *l'applicazione da G in $O(V/V^\perp, f)$, che a ciascun $\gamma \in G$ associa $\overline{\gamma}$, è un omomorfismo suriettivo di gruppi;*

DIMOSTRAZIONE. Poiché V è G-invariante e gli elementi di G sono isometrie, anche $V^\perp$ è G-invariante. Da questo e dal Lemma 12.2.9 seguono facilmente tutte le restanti affermazioni, tenendo presente, per il punto 5, che l'applicazione, che a ciascun u in U associa $u+V^\perp$, è un'isometria tra $O(U,f)$ e $O(V/V^\perp,f)$. ∎

12.2.1 Il Lemma di Witt per gli spazi simplettici

In quanto segue (V,f) e (W,g) sono spazi simplettici di dimensione $2n$ sul medesimo un campo K (in particolare V e W sono isometrici). Se U è un sottospazio di V (di W), indichiamo con f_U la restrizione di f (di g) a $U \times U$. Chiaramente f_U (g_U) è una forma bilineare alternante su U ed è non degenere se e solo se $U \cap U^\perp = \{0\}$. Se U e Z sono sottospazi rispettivamente di V e W, per un'isometria tra U e Z intendiamo una (f_U, g_Z)-isometria.

Lemma 12.2.11 *Siano U e Z sottospazi rispettivamente di V e W e $\alpha: U \to Z$ un'isometria. Se $U \cap U^\perp = \{0\}$, allora esiste un'isometria $\overline{\alpha}: V \to W$ che estende α.*

DIMOSTRAZIONE. Poiché $U \cap U^\perp = \{0\}$ e α è un'isometria tra U e Z, anche $Z \cap Z^\perp = \{0\}$. In particolare

$$V = U \oplus U^\perp = Z \oplus Z^\perp. \tag{12.19}$$

Poiché $dim(U) = dim(Z)$, segue che anche $U^\perp$ e $Z^\perp$ sono spazi simplettici ed hanno la medesima dimensione. Per il Teorema 12.2.4, esiste un'isometria $\beta: U^\perp \to Z^\perp$. Per 12.19, ogni vettore v di V si decompone in modo unico come somma di un vettore x_v in U e di un vettore y_v in $U^\perp$. Sia $\overline{\alpha}: V \to V$ definita, per ogni $v \in V$, da

$$v^{\overline{\alpha}} := x_v^\alpha + y_v^\beta.$$

Allora $\overline{\alpha}$ è un'isometria di V che estende α. ∎

Lemma 12.2.12 *Sia U un sottospazio isotropo di V e sia $(u_1, \ldots, u_t)$ una base di U. Sia X un complemento di U in $U^\perp$. Allora esistono $w_1, \ldots, w_t$ in V tali che $(u_1, w_1, \ldots, u_t, w_t)$ sia una base iperbolica di $X^\perp$.*

DIMOSTRAZIONE. Per induzione su $dim(V)/2$. Se $dim(V) = 2$ la dimostrazione segue immediatamente dal fatto che ogni vettore isotropo appartiene ad una base iperbolica di V. Supponiamo $dim(V) > 2$. Per il Lemma 12.1.6 $X \cap X^\perp = \{0\}$ e, poiché $X \leq U^\perp$, U è un sottospazio (isotropo) di $X^\perp$. Possiamo quindi supporre che

$$V = X^\perp,$$

quindi

$$X = \{0\} \text{ e } U = U^\perp.$$

Sia

$$W := \langle u_2, \ldots, u_t \rangle.$$

Allora W è un iperpiano di U e U è un iperpiano di $W^\perp$. Sia Y un complemento di W in $W^\perp$ contenente il vettore u_1. Per il Lemma 12.1.6

$$Y \cap Y^\perp = \{0\}$$

e quindi Y è un piano iperbolico. Sia $w_1 \in Y$ tale che (u_1, w_1) sia una coppia iperbolica di Y. Poiché V è somma diretta ortogonale di Y e $Y^\perp$ e poiché W è un sottospazio isotropo di $Y^\perp$, esistono dei vettori $w_2, \ldots, w_t$ tali che $(u_2, w_2, \ldots, u_t, w_t)$ sia una base iperbolica di $Y^\perp$. Ma allora

$$(u_1, w_1, u_2, w_2, \ldots, u_t, w_t)$$

è una base iperbolica di $X^\perp$. ∎

Lemma 12.2.13 *Siano U e Z sottospazi rispettivamente di V e W e sia $\alpha: U \to Z$ un'isometria. Se U è isotropo, allora esiste un'isometria $\overline{\alpha}: V \to W$ che estende α.*

DIMOSTRAZIONE. Poiché U è isotropo, anche Z è un sottospazio isotropo di W. Siano X e Y complementi rispettivamente di U in $U^\perp$ e di Z in $Z^\perp$. Allora

$$dim(X) = dim(U^\perp) - dim(U) = dim(Z^\perp) - dim(Z) = dim(Y).$$

Siano

$$(u_1, \ldots, u_t) \text{ e } (z_1, \ldots, z_t)$$

basi rispettivamente di U e di Z. Per il Lemma 12.2.12 esistono dei vettori

$$(v_1, \ldots, v_t) \text{ e } (w_1, \ldots, w_t)$$

rispettivamente in $X^\perp$ e in $Y^\perp$, tali che

$$(u_1, v_1, \ldots, u_t, v_t) \text{ e } (z_1, w_1, \ldots, z_t, w_t)$$

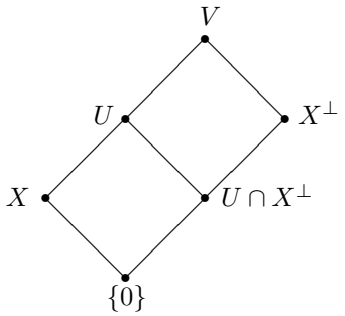
siano basi iperboliche rispettivamente di $X^\perp$ e $Y^\perp$. Sia $\beta: X^\perp \to Y^\perp$, l'applicazione lineare definita, per ogni $i \in \{1, \ldots, t\}$ da

$$\beta(u_i) = z_i \text{ e } \beta(v_i) = w_i.$$

Per punto 2. del Lemma 12.2.2 β è un'isometria e, poiché $X^\perp \cap X = \{0\}$, per il Lemma 12.2.11, β si estende ad un'isometria $\overline{\alpha}$ tra V e W. ∎

Teorema 12.2.14 (LEMMA DI WITT PER GLI SPAZI SIMPLETTICI) *Siano (V, f) e (W, g) spazi simplettici della medesima dimensione, sia U un sottospazio di V e sia $\alpha: U \to W$ un'applicazione lineare che induca una $(f|_U, g|_{U^\alpha})$-isometria tra U e U^α. Allora esiste una (f, g)-isometria $\overline{\alpha}: V \to W$ tale che $\overline{\alpha}|_U = \alpha$.*

DIMOSTRAZIONE. Per induzione su $dim(U)$. Se U è isotropo, (in particolare se $dim(U) \leq 1$) la tesi scende dal Corollario 12.2.13. Supponiamo quindi che $dim(U) > 1$ e U non sia isotropo. Allora esiste un sottospazio non nullo X di U tale che $X \cap X^\perp = \{0\}$ e quindi V è somma diretta ortogonale di X e $X^\perp$. Per la Legge Modulare di Dedekind, risulta $U = (U \cap X^\perp) \oplus X$, dunque i sottospazi sono disposti come nel seguente diagramma:



In particolare, poichè $X \neq \{0\}$, $U \cap X^\perp < U$. Per ipotesi induttiva $\alpha|_{U \cap X^\perp}$ si estende ad un'isometria

$$\beta: X^\perp \to (X^\alpha)^\perp.$$

Per ogni vettore v di V sia

$$v = x_v + \overline{x}_v$$

la decomposizione unica di v come somma di un vettore x_v di X e di un vettore $\overline{x}_v$ di $X^\perp$ e sia

$$\overline{\alpha}: V \to W$$

l'applicazione lineare definita, per ogni $v \in V$ da

$$v^{\overline{\alpha}} := x_v^\alpha + \overline{x}_v^\beta.$$

Allora $\overline{\alpha}$ è un'isometria e, come si vede facilmente, $\overline{\alpha}|_U = \alpha$. ∎

Chiudiamo questa sezione con una conseguenza del Lemma 12.2.12 che ci servirà per dimostrare alcune proprietà dei telai simplettici.

Lemma 12.2.15 *Sia X un sottospazio iperbolico di V e sia U un sottospazio isotropo massimale di $X^\perp$. Allora X è un complemento di U in $U^\perp$*

DIMOSTRAZIONE. Poichè X è iperbolico, V è somma diretta ortogonale di X e $X^\perp$. In particolare

$$U \cap X \leq X^\perp \cap X = \{0\} \text{ e } \langle U, X \rangle \leq U^\perp.$$

Quindi resta da dimostrare che $U^\perp \leq \langle U, X \rangle$ o, equivalentemente per la Legge Modulare di Dedekind, che

$$U = U^\perp \cap X^\perp.$$

Ora, se $x \in U^\perp \cap X^\perp$, lo spazio $\langle U, x\rangle$ è isotropo e quindi, per la massimalità di U coincide con U, da cui la tesi. ∎

Lemma 12.2.16 (Completamento delle basi iperboliche) *Sia X un sottospazio iperbolico di V e sia W un sottospazio isotropo di $X^\perp$. Sia*

$$(x_1, w_1, \ldots, x_k, w_k)$$

una base iperbolica di X e sia

$$(w_{k+1}, \ldots, w_{k+t})$$

una base di W. Allora esistono dei vettori $x_{k+1}, \ldots, x_n$ e $w_{k+t+1} \ldots, w_n$ tali che

$$(x_1, w_1, \ldots, x_n, w_n)$$

sia una base iperbolica di V

Dimostrazione. Poiché X è iperbolico, V è somma diretta ortogonale di X e di $X^\perp$. Basta quindi provare che la base

$$(w_{k+1}, \ldots, w_{k+t})$$

di W può essere completata ad una base iperbolica di $X^\perp$. Sia U un sottospazio isotropo massimale di $X^\perp$ contenente W. Per il Teorema di Completamento delle Basi esistono $w_{k+t+1}, \ldots, w_{k+t+l} \in U$ tali che

$$(w_{k+t+1}, \ldots, w_{k+t+l})$$

sia una base di U. Per il Lemma 12.2.15 X è un complemento di U in $U^\perp$ e quindi la tesi segue dal Lemma 12.2.12. ∎

Capitolo 13

Gruppi Simplettici

In questo capitolo V è uno spazio vettoriale di dimensione $2n$ sul campo K e f è una forma bilineare alternante non degenere su V.

13.1 Il Gruppo Simplettico

Il **gruppo simplettico** $Sp(V)$ è il gruppo delle isometrie di V. Studieremo la struttura dei gruppi simplettici sulla linea di come abbiamo fatto per i gruppi lineari. Incominciamo con determinare l'ordine di $Sp(V)$: come abbiamo fatto nel caso di $GL(V)$ proveremo che $Sp(V)$ agisce in modo regolare sull'insieme delle basi simplettiche e calcoleremo il numero di queste basi.

Teorema 13.1.1 *Sia V uno spazio simplettico di dimensione $2n$ su un campo K di ordine q con $q = p^k$, dove p è un numero primo. Allora*

$$|Sp(V)| = \prod_{i=1}^{n}(q^{2i} - 1)q^{2i-1} = q^{n^2}\prod_{i=1}^{n}(q^{2i} - 1)$$

Lemma 13.1.2 *$Sp(V)$ agisce regolarmente sull'insieme delle basi iperboliche.*

DIMOSTRAZIONE. Segue immediatamente dal Lemma 12.2.2 e dal Teorema di Estensione per Linearità. ∎

Dimostriamo ora il Teorema 13.1.1.

Per il Corollario 8.2.7 segue che l'ordine di $Sp(V)$ coincide con la cardinalità dell'insieme delle basi iperboliche di V. Osserviamo che V possiede

$$(q^{2n} - 1)$$

vettori isotropi diversi dal vettore nullo. Se u_1 è un vettore isotropo non nullo, $V \setminus \langle u_1 \rangle^{\perp}$ ha

$$(q^{2n} - q^{2n-1})$$

elementi e l'insieme

$$\{\langle w\rangle \setminus \{0\} | w \in V \setminus \langle u_1\rangle^\perp\}$$

è una partizione di $V \setminus \langle u_1\rangle^\perp$ in cui ciascun elemento contiene esattamente $q-1$ vettori e di questi uno solo forma una coppia iperbolica con u_1. Ne segue che una coppia iperbolica (u_1, w_1) di V può esser scelta in esattamente

$$(q^{2n}-1)(q^{2n}-q^{2n-1})(q-1)^{-1} = (q^{2n}-1)q^{2n-1}$$

modi distinti. Posto

$$U = \langle u_1, w_1\rangle,$$

abbiamo che

$$V = U \oplus U^\perp,$$

e $U^\perp$ è anch'esso simplettico. Quindi, per ipotesi induttiva, $U^\perp$ possiede

$$\prod_{i=1}^{n-1}(q^{2i}-1)q^{2i-1}$$

basi simplettiche. La tesi segue allora perché

$$(u_1, v_1, u_2, v_2, \ldots, u_n, v_n)$$

è una base simplettica di V se e solo se

$$(u_2, v_2, \ldots, u_n, v_n)$$

è una base simplettica per $U^\perp$.

13.2 Conseguenze del Lemma di Witt

Lemma 13.2.1 *1. $Sp(V)$ agisce transitivamente sui sottospazi isotropi della medesima dimensione di V,*

2. più in generale, $Sp(V)$ agisce transitivamente sulle bandiere del medesimo tipo di sottospazi isotropi di V.

3. Il nucleo dell'azione di $Sp(V)$ sull'insieme degli spazi isotropi di V ha ordine è generato dall'applicazione che manda ogni vettore di V nel suo opposto.

DIMOSTRAZIONE. Chiaramente l'insieme dei sottospazi isotropi di V è invariante per l'azione di $Sp(V)$ e lo stesso vale per l'insieme delle bandiere di sottospazi isotropi di V e $Sp(V)$ conserva le dimensioni le inclusioni e (quindi) i tipi. La transitività segue immediatamente dal Lemma di Witt, poichè qualsiasi applicazione lineare biiettiva tra spazi isotropi è un'isometria. Infine, se $\lambda \in Sp(V)$ fissa tutti i sottospazi isotropi di V, allora fissa tutti i sottospazi di dimensione 1 e quindi, per la Proposizione 11.1.7, λ è un'applicazione scalare.

Poichè λ è un'isometria, se (u, v) è una coppia iperbolica, dev'essere $(u^\lambda, v^\lambda) \in \{(u, v), (-u, -v)\}$, da cui la tesi. ∎

Segue, da questo lemma, che un oggetto naturale su cui rappresentare $Sp(V)$ è l'insieme dei di sottospazi isotropi di V e lo spazio delle bandiere ad essa associato. Il nucleo Z di questa azione ha ordine 1 o 2 a seconda che la caratteristica di K sia 2 u un primo dispari ed il gruppo $Sp(V)/Z$ si indica con $PSp(V)$ e si chiama **gruppo proiettivo simplettico** su V. Faremo uso in seguito di questa rappresentazione, che formalizzeremo nella sezione 13.3. Concludiamo questa sezione con due conseguenze del Lemma di Witt sull'azione di $Sp(V)$ sui punti di $P(V)$ che useremo nella sezione 13.6.

Lemma 13.2.2 *Sia U un sottospazio di dimensione 1 di V e sia H lo stabilizzatore in $Sp(V)$ di U. Allora le H-orbite di U sono*

$$\{U\},\ \{W | dim(W) = 1,\ W \leq U^\perp,\ W \neq U\} \text{ e } \{W | dim(W) = 1,\ W \not\leq U^\perp\}$$

Dimostrazione. Siano

$$A := \{W | dim(W) = 1,\ W \leq U^\perp,\ W \neq U\} \text{ e } B := \{W | dim(W) = 1,\ W \not\leq U^\perp\}.$$

Chiaramente $\{U\}$, A e B sono invarianti per H. Proviamo che H è transitivo su A e B. Sia $C \in \{A, B\}$ e W e Z in C. Siano u, w, z elementi non nulli rispettivamente di U, W e Z e, se $C = B$, sia z scelto in modo che $f(u, z) = f(u, w)$. Allora l'applicazione lineare

$$\alpha : \langle U, W \rangle \to \langle U, Z \rangle$$

definita da $u^\alpha = u$ e $w^\alpha = z$ è un'isometria tra $\langle U, W \rangle$ e $\langle U, Z \rangle$. Per il Lemma di Witt α si estende ad un elemento di H. ∎

Lemma 13.2.3 *$Sp(V)$ agisce in modo primitivo sui punti di $P(V)$.*

Dimostrazione. $Sp(V)$ è transitivo sui punti di $P(V)$ per il Corollario 13.2.2. Sia B un blocco di imprimitività e siano U, W due elementi distinti di B. In particolare

$$U^\perp \neq W^\perp \text{ e quindi} (V \setminus U^\perp) \neq (V \setminus W^\perp) \tag{13.1}$$

Se U e W sono ortogonali tra loro, per il 13.2.2, B contiene tutti i sottospazi di dimensione 1 ortogonali a W. Tra questi, per 13.1, ce ne sono di non ortogonali a U. Sia X uno di questi. Allora B contiene $\{U, X\}$ e $\{U, W\}$ e quindi, per il Lemma 13.2.2, tutto V. Se U e W non sono ortogonali tra loro, B contiene tutti i sottospazi di dimensione 1 non ortogonali a W. Come sopra, per 13.1, esiste almeno un sottospazio Y che è ortogonale a U e di nuovo si conclude per il Lemma 13.2.2. ∎

Lemma 13.2.4 *Ogni sottospazio isotropo massimale di V ha dimensione n.*

DIMOSTRAZIONE. Se

$$(u_1, w_1, u_2, w_2, \ldots, u_n, w_n)$$

è una base iperbolica di V, il sottospazio

$$\langle u_1, u_2, \ldots, u_n \rangle$$

è chiaramente isotropo massimale ed ha dimensione n. Basta quindi dimostrare che i sottospazi isotropi massimali di V hanno tutti la medesima dimensione. Siano infatti U e Z due sottospazi isotropi massimali di V. Possiamo supporre che $dim(U) \leq dim(Z)$. Allora ogni applicazione lineare iniettiva α da U in Z induce un'isometria tra U e U^α e tale isometria, per il Lemma di Witt 12.2.14 si estende ad un'isometria di V. Poichè U è isotropo massimale, anche U^α è isotropo massimale e quindi $U^\alpha = Z$, da cui la tesi. ∎

13.3 La geometria simplettica

In questa sezione V è uno spazio vettoriale di dimensione $2n$ sul campo K e f è una forma bilineare alternante non degenere su f. Chiaramente $Sp(V) \leq GL(V)$ e quindi $Sp(V)$ agisce sulla geometria proiettiva $GP(V)$. Questo, però, non è l'oggetto ideale su cui rappresentare $Sp(V)$: osserviamo infatti che ogni isometria di (V, f) manda sottospazi isotropi in sottospazi isotropi. Poichè, se $n > 2$ esistono sottospazi isotropi e non isotropi della medesima dimensione, $Sp(V)$ non è transitivo sull'insieme dei sottospazi di una dimensione fissata (e quindi tanto meno sulle bandiere di $GP(V)$). D'altra parte, come abbiamo accennato nella sezione precedente, il fatto che $Sp(V)$ agisce anche sull'insieme $GSp(V)$ dei sottospazi isotropi di V suggerisce di rappresentare $Sp(V)$ su una particolare sottogeometria di Tits di $GP(V)$: la **geometria simplettica** associata a (V, f). Questa è la tripla $(GSp(V), dim, *)$ dove $dim\colon GSp(V) \to \{1, \ldots, n\}$ è la funzione che ad ogni sottospazio associa la sua dimensione e $*$ è la relazione d'incidenza definita, per ogni $U, W \in GSp(V)$ da $U * W$ se e solo se $U \leq W$ oppure $W \leq V$. Questa è evidentemente una sottogeometria di $GP(V)$ e, come al solito, indicheremo la tripla $(GSp(V), dim, *)$ semplicemente con $GSp(V)$. Come esempio, per mostrare i vantaggi della geometria simplettica sulla geometria proiettiva per rappresentare $Sp(V)$, osserviamo che, se U e W sono sottospazi isotropi di V, ogni isomorfismo tra gli spazi vettoriali U e W è un'isometria e quindi, per il Lemma di Witt (Lemma 12.2.11), si estende ad un'isometria di (V, f). In particolare,

Lemma 13.3.1 *$GL(n, K) \leq Sp(2n, K)$ e $Sp(V)$ è transitivo sull'insieme dele bandiere del medesimo tipo di $GSp(V)$.*

13.3.1 Bandiere e telai simplettici

Bandiere simplettiche

Una **bandiera simplettica** è una bandiera nella geometria di Tits $GSp(V)$, quindi un insieme $\{W_i|1 \leq i \leq k\}$ dove, per ogni $i \in \{1, \ldots, k\}$, W_i è un sottospazio isotropo non nullo e

$$W_1 < W_2 < \ldots W_k. \tag{13.2}$$

Come per le bandiere in $PG(V)$, useremo la serie 13.2 per indicare la bandiera $\{W_1, \ldots W_k\}$. Analogamente le **camere simplettiche** ed i **muri simplettici** sono rispettivamente le camere in $GSp(V)$ ed i muri in $GSp(V)$. Si osservi che, per il Lemma 13.2.4, le bandiere e le camere simplettiche di V sono rispettivamente le bandiere e le camere proiettive dei sottospazi isotropi massimali di V. In particolare, le camere simplettiche hanno rango n. Indicheremo con $\mathcal{S}(V)$ l'insieme delle bandiere simplettiche di V.

Dal Lemma 12.1.5 segue immediatamente che, se

$$\mathcal{F} := \{W_i|1 \leq i \leq k\}$$

è una bandiera (camera) simplettica, con

$$W_1 < W_2 < \ldots < W_{k-1} < W_k,$$

allora

$$\{W_i|1 \leq i \leq k\} \cup \{W_i^\perp|1 \leq i \leq k\}$$

è una è una bandiera (camera) proiettiva, che indicheremo con $\mathcal{F}^\circ$, tale che

$$W_1 < \ldots < W_k \leq W_k^\perp < W_{k-1}^\perp < \ldots < W_2^\perp < W_1^\perp.$$

Indicheremo con $\mathcal{S}^\circ(V)$ l'insieme $\{\mathcal{F}^\circ|\mathcal{F} \in \mathcal{S}(V)\}$.

Osserviamo che, se $\phi \in Sp(V)$ normalizza un sottospazio W di V, allora deve normalizzare anche il suo ortogonale $W^\perp$. Da questo segue che $GSp(V)^\circ$ è invariante per l'azione di $Sp(V)$ e l'applicazione $\mathcal{F} \mapsto \mathcal{F}^\circ$ è un isomorfismo di $Sp(V)$-insiemi tra $\mathcal{S}(V)$ e $\mathcal{S}^\circ(V)$ che, inoltre, conserva le inclusioni tra bandiere. L'insieme $\mathcal{F}^\circ$ ci servirà per definire i telai e gli appartamenti simplettici.

Lemma 13.3.2 *Ogni muro di $GSp(V)$ è contenuto in almeno tre camere di $GSp(V)$.*

Dimostrazione. Sia $\mathcal{B}$ un muro simplettico e

$$\mathcal{F} := W_1 < W_2 < \ldots < W_{n-1} < W_n$$

una camera simplettica contenente $\mathcal{B}$. Osserviamo che, se $W_n \in \mathcal{B}$, allora $\mathcal{B} \setminus W_n$ è un muro proiettivo di $GP(W_n)$ e ogni camera proiettiva di $GP(W_n)$ è una camera simplettica di $GSp(V)$. Se, invece, $W_n \notin \mathcal{B}$, allora $\mathcal{B}$ è un muro proiettivo di $GP(W_{n-1}^\perp)$ e ogni camera proiettiva di $GP(W_{n-1}^\perp)$ contenente $\mathcal{B}$ è anche una camera simplettica di $GSp(V)$. La tesi segue allora dal Lemma A.4.1. ∎

Telai ed appartamenti simplettici

Un **telaio simplettico** è un insieme del tipo

$$\{\langle u_i\rangle | 1 \leq i \leq n\} \cup \{\langle v_i\rangle | 1 \leq i \leq n\},$$

dove $(u_1, v_1, \ldots, u_n, v_n)$ una base iperbolica di V. Se Σ è un telaio simplettico, l'**appartamento simplettico** $\Delta_{Sp}(\Sigma)$ associato a Σ è l'insieme delle bandiere simplettiche supportate da Σ:

$$\Delta_{Sp}(\Sigma) = \Delta(\Sigma) \cap \mathcal{S}(V).$$

Lemma 13.3.3 *Se Δ è un appartamento simplettico in $GSp(V)$, allora Δ contiene esattamente $2^m(n!)$ camere simplettiche.*

DIMOSTRAZIONE. Con le notazioni precedenti, possiamo supporre che $\Delta := \Delta_{Sp}(\Sigma)$. Sia

$$W_1 < \ldots < W_n$$

una camera simplettica contenuta in Δ. Poichè W_n è un sottospazio isotropo di dimensione n, dev'essere

$$|W_n \cap \{u_j, v_j\}| = 1$$

per ogni $j \in \{1, \ldots, n\}$. Inoltre se $k \in \{1, \ldots, n\}$ è tale che $W_n \leq \langle W_{n-1}, P_k\rangle$, allora

$$W_{n-1} \leq \langle R_1, \ldots, R_{k-1}, R_{k+1}, \ldots, R_n\rangle.$$

Procedendo in questo modo, per induzione si ottiene che esiste una permutazione $\sigma \in S_n$ tale che

$$W_i \cap \{u_{j^\sigma}, v_{j^\sigma}\} = 1$$

per ogni $j \in \{1, \ldots, i\}$, e quindi

$$W_i = \langle W_i \cap \{u_{j^\sigma}, v_{j^\sigma}\} | 1 \leq j \leq i\}\rangle.$$

Viceversa, comunque si prenda una permutazione $\sigma \in S_n$ e comunque si scelga $e_j \in \{u_{j^\sigma}, v_{j^\sigma}\}$, l'insieme

$$\{\langle e_1, \ldots, e_i\rangle | i \in \{1, \ldots, n\}\}$$

è una camera simplettica. Poichè ci sono $n!$ scelte per la permutazione σ e 2^m scelte di $e_j \in \{u_{j^\sigma}, v_{j^\sigma}\}$ al variare di $j \in \{1, \ldots, n\}\}$ e poiché scelte distinte danno luogo a camere distinte, esistono esattamente $2^m(n!)$ camere simplettiche in Δ. ∎

Lemma 13.3.4 *Se Δ è un appartamento simplettico, ogni muro di Δ è contenuto in due camere di $GSp(V)$.*

DIMOSTRAZIONE. Sia $\mathcal{M}$ un muro simplettico, sia Sia

$$\mathcal{F} := W_1 < \ldots < W_n$$

una camera simplettica contenente $\mathcal{M}$, sia $j \in \{1, \ldots, n\}$ tale che

$$\mathcal{M} = W_1 < \ldots < W_{j-1} < W_{j+1} < \ldots < W_n$$

e sia $(u_1, v_1, \ldots, u_n, v_n)$ una base iperbolica tale che $W_i = \langle u_i \rangle$ per ogni $i \in \{1, \ldots, n\}$. Allora l'unica altra camera contenente $\mathcal{M}$ supportata dal telaio simplettico

$$\{\langle u_1 \rangle, \langle v_1 \rangle, \ldots, \langle u_n \rangle, \langle v_n \rangle\}$$

è

$$W_1 < \ldots < W_{j-1} < \langle W_{j-1}, v_j \rangle < W_{j+1} < \ldots < W_n.$$

■

Sia

$$\Sigma := \{P_1, \ldots, P_{2n}\}$$

un telaio proiettivo di V,

$$(e_1, \ldots, e_{2n})$$

una base di V tale che

$$P_i = \langle e_i \rangle.$$

Per ogni $i \in \{1, \ldots, n\}$, sia $e_i^\wedge$ è definito come in 12.5, e indichiamo con $P_i^\wedge$ il sottospazio $\langle e_i^\wedge \rangle$, e con $\Sigma^\wedge$ l'insieme $\{P_1^\wedge, \ldots, P_{2n}^\wedge\}$. Chiaramente $\Sigma^\wedge$ è un telaio proiettivo e, se Σ è un telaio simplettico di V, allora $\Sigma = \Sigma^\wedge$. Per il Corollario 12.1.7, se $\mathcal{F}$ è una bandiera simplettica supportata dal telaio Σ, allora $\mathcal{F}$ è supportata anche dal telaio $\Sigma^\wedge$.

Lemma 13.3.5 *Se $\mathcal{F}$ e $\mathcal{F}'$ sono due bandiere simplettiche in $GS_p(V)$, allora esiste un appartamento simplettico che le contiene entrambe.*

DIMOSTRAZIONE. Possiamo supporre che $\mathcal{F}$ e $\mathcal{F}'$ siano camere simplettiche. Sia

$$\mathcal{F} := W_1 < \ldots < W_n$$

e sia

$$\mathcal{F}' := U_1 < \ldots < U_n.$$

Per il Lemma A.4.3 esiste un telaio Σ che supporta sia $\mathcal{F}$ che $\mathcal{F}'$ e, per l'osservazione precedente, anche $\Sigma^\wedge$ supporta sia $\mathcal{F}$ che $\mathcal{F}'$. L'idea della dimostrazione è costruire due sottoinsiemi Σ_{W_n} e $\Sigma_n^\wedge$ rispettivamente di Σ e di $\Sigma^\wedge$ in modo che $\Sigma_{W_n} \cup \Sigma_n^\wedge$ possa essere completato fino ad ottenere un telaio simplettico con la proprietà che ogni sottospazio di $\mathcal{F}$ e $\mathcal{F}'$ sia generato da un sottoinsieme di $\Sigma_{W_n} \cup \Sigma_n^\wedge$.

Se X è un sottospazio di V sia

$$\Sigma_X := \{P \in \Sigma | P \leq X\}$$

e, se $j \in \{1, \ldots, n\}$, sia

$$\Sigma_j^\wedge := \{P^\wedge | P^\wedge \leq U_j \text{ e } P^\wedge \not\leq W_n\}.$$

Chiaramente

$$W_i = \langle \Sigma_{W_i} \rangle$$

e, per il Lemma A.4.4,

$$W_i \cap U_j = \langle \Sigma_{W_i \cap U_j} \rangle.$$

Dunque

$$U_j = \langle \Sigma_{W_i \cap U_j} \cup \Sigma_j^\wedge \rangle.$$

Sia $P^\wedge \in \Sigma_j^\wedge$. Poichè W_n è un sottospazio isotropo massimale di V e poiché $(P^\wedge)^\perp \cap W_n$ ha codimensione 1 in W_n, esiste un unico $P \in \Sigma_{W_n}$ tale che $P \not\leq (P^\wedge)^\perp$. Sia

$$\Sigma_n^\wedge := \{P_1^\wedge, \ldots, P_k^\wedge\}$$

e sia

$$\Sigma_{W_n} := \{P_1, \ldots, P_n\}$$

con gli indici scelti in modo che, per ogni $j \in \{1, \ldots, k\}$, $\langle P_j^\wedge, P_j \rangle$ sia un sottospazio iperbolico di V. Chiaramente possiamo scegliere dei generatori w_i di P_i, con $i \in \{1, \ldots, n\}$, e dei generatori x_j di $P_j^\wedge$, con $j \in \{1, \ldots, k\}$ che soddisfano le ipotesi del Corollario 13.2.2. Esistono quindi dei vettori $x_{k+1}, \ldots, x_n$ tali che

$$(x_1, w_1, \ldots, x_n, w_n)$$

sia una base iperbolica di V. Posto

$$P_t^\wedge := \langle x_t \rangle$$

per ogni $t \in \{k + 1' \ldots, n\}$, l'insieme

$$\{P_1, P_1^\wedge \ldots P_n, P_n^\wedge\}$$

è un telaio simplettico che supporta sia $\mathcal{F}$ che $\mathcal{F}'$. ∎

13.4 Sottogruppi parabolici di $Sp(V)$

In questa sezione, analogamente a quanto fatto per i gruppi lineari, definiremo i sottogruppi di Borel, i sottogruppi parabolici ed i loro radicali unipotenti in $Sp(V)$. Il Lemma di Witt ed il fatto che ogni automorfismo di un sottospazio isotropo è un'isometria ci permetteranno di sfruttare gli analoghi risultati

dimostrati per i gruppi lineari. I **sottogruppi di Borel** di $Sp(V)$ sono i normalizzanti in $Sp(V)$ delle camere simplettiche, e i **sottogruppi parabolici** di $Sp(V)$ sono normalizzanti in $Sp(V)$ delle bandiere simplettiche non massimali. In tutta questa sezione poniamo

$$G := Sp(V)$$

ed inoltre $\mathcal{F}$ è la bandiera simplettica

$$W_1 < \ldots < W_k,$$

dove, per ogni $i \in \{1, \ldots, n\}$, W_i è un sottospazio isotropo di V. Poniamo inotre

$$W_0 := \{0\} \text{ e } W_{k+1} := W_k^{\perp}.$$

Come abbiamo osservato sopra,

$$N_G(\mathcal{F}) = N_G(\mathcal{F}^{\circ}),$$

dove $\mathcal{F}^{\circ}$ è la bandiera

$$W_1 < \ldots < W_k \leq W_k^{\perp} < \ldots < W_1^{\perp}.$$

Lemma 13.4.1 *Se $\mathcal{H}$ e è una bandiera simplettica di V, con $\mathcal{H} \subseteq \mathcal{F}$, allora $N_G(\mathcal{F}) \leq N_G(\mathcal{H})$.*

Dimostrazione. Segue immediatamente dal Lemma 11.4.1 ed il fatto che $N_{Sp(V)}(\mathcal{H}) = N_{GL(V)}(\mathcal{H}) \cap Sp(V)$. ∎

Lemma 13.4.2 *Se W è un sottospazio isotropo non nullo e non contenuto in $\mathcal{F}$, allora esiste $\gamma \in N_G(\mathcal{F})$ tale che $W^{\gamma} \neq W$.*

Dimostrazione. Si adatti, per esercizio, la dimostrazione del Lemma 11.4.2, usando il fatto che ogni isomorfismo lineare tra sottospazi isotropi di V si può estendere, per il Lemma di Witt, ad un'isometria di V. ∎

Teorema 13.4.3 *Siano V e G come sopra, sia $\mathcal{F}_{Sp}(V)$ l'insieme delle bandiere simplettiche di V e sia $\mathcal{P}$ l'insieme dei sottogruppi parabolici di G. Allora l'applicazione*

$$\begin{array}{rccc} \phi\colon & \mathcal{F}_{Sp}(V) & \to & \mathcal{P} \\ & \mathcal{H} & \mapsto & N_G(\mathcal{H}) \end{array}$$

è biiettiva e inverte le inclusioni. In particolare, i sottogruppi parabolici massimali di G sono tutti e soli i normalizzanti dei sottospazi isotropi non nulli di V.

DIMOSTRAZIONE. Se $\mathcal{F}$ è come sopra, per il Lemma 13.4.2, $W_1, \ldots, W_k$ sono tutti e soli i sottospazi isotropi non nulli di V normalizzati da $N_G(\mathcal{F})$, da cui segue che ϕ è biiettiva. Per il Lemma 13.4.1 ϕ inverte le inclusioni. ∎

Proposizione 13.4.4 *G agisce transitivamente per coniugio sull'insieme dei suoi sottogruppi di Borel.*

DIMOSTRAZIONE. Segue immediatamente dalla Proposizione 13.3.1 e dall'Esercizio 8.3.23. ∎

Il radicale unipotente

Il **centralizzante** di $\mathcal{F}$ in G è il centralizzante della serie

$$W_0 < W_1 < W_2 < \ldots < W_{k+1}$$

e lo indicheremo con $C_G(\mathcal{F})$. Come per i gruppi lineari, $C_G(\mathcal{F})$ si dice anche **radicale unipotente** del gruppo $N_G(\mathcal{F})$.

Proposizione 13.4.5 *$C_G(\mathcal{F})$ è un p-sottogruppo normale di $N_G(\mathcal{F})$.*

DIMOSTRAZIONE. Per il Lemma 12.2.6

$$C_G(\mathcal{F}) \leq C_G(\mathcal{F}^\circ) \leq C_{GL(V)}(\mathcal{F}^\circ)$$

e, quindi, la tesi segue dal Teorema 10.2.9 ∎

Lemma 13.4.6 *Se T è un p-sottogruppo di G, allora T centralizza una bandiera simplettica di V.*

DIMOSTRAZIONE. Per induzione sulla dimensione di V. Sia

$$W := C_V(T).$$

Per il Lemma 8.2.8 $W \neq \{0\}$. Poichè gli elementi di T sono isometrie (o per il Lemma 12.2.6), T normalizza $W^\perp$ e quindi, ancora per il Lemma 8.2.8

$$C_{W^\perp}(T) \neq \{0\}.$$

Poniamo

$$W_1 := C_{W^\perp}(T).$$

Poichè

$$W_1 \leq W^\perp \cap C_V(T) = W^\perp \cap W,$$

W_1 è isotropo. Per il Lemma 12.1.8 f induce su $W_1^\perp/W_1$ una forma bilineare non degenere e, chiaramente, alternante. Sia $\overline{V}$ lo spazio quoziente $W_1^\perp/W_1$.

Poichè T normalizza W_1 e $W_1^\perp$, T agisce su $\overline{V}$ e, per come è definita la forma bilineare indotta da f su $\overline{V}$, gli elementi di T inducono delle isometrie su $\overline{V}$. Per ipotesi induttiva T centralizza una serie

$$\{0\} = \overline{W}_1 < \overline{W}_2 < \overline{W}_3 < \ldots < \overline{W}_{k-1} < \overline{W}_k \leq \overline{W}_{k+1} = \overline{W}_k^\perp$$

in $\overline{V}$. Per ogni $i \in \{2, \ldots, k+1\}$, sia W_i l'antiimagine di $\overline{W}_i$ in V. Per il Lemma 12.1.8 W_i è isotropo per ogni $i \in \{1, \ldots, k\}$ e $W_{k+1} = W_k^\perp$. Quindi T centralizza la bandiera simplettica $W_1 < \ldots < W_k$. ∎

Lemma 13.4.7 *Se $\mathcal{F}$ e $\mathcal{H}$ sono bandiere di V, allora*

$$\mathcal{H} \leq \mathcal{F} \text{ se e solo se } C_G(\mathcal{H}) \leq C_G(\mathcal{F}).$$

DIMOSTRAZIONE. Segue immediatamente dalle definizioni. ∎

Corollario 13.4.8 *I p-sottogruppi di Sylow di G sono tutti e soli i centralizzanti delle camere, più precisamente l'applicazione che a ciascuna camera di V associa il suo centralizzante in G è una biiezione tra l'insieme delle camere e l'insieme dei p-sottogruppi di Sylow di G*

Azione di $N_{Sp(V)}(W)$ sulla bandiera $\{0\} < W \leq W^\perp < V$

Sia W un sottospazio isotropo di V e sia $H := N_G(W)$. Poichè W è isotropo, per il Corollario 12.2.10, ogni elemento di $GL(W)$ si estende ad un'isometria di $W^\perp$ ed ogni isometria dello spazio quoziente $W^\perp/W$ è indotta da un'isometria dello spazio $W^\perp$. Poiché $W^\perp/W$ è uno spazio simplettico, H induce su $W^\perp/W$ tutto il gruppo $Sp(W^\perp/W)$. Infine, per il Lemma 12.2.8, H induce su $V/W^\perp$ tutto $GL(V/W^\perp)$ e le azioni di H su W e su $V/W^\perp$ sono come descritte nel Lemma 12.2.8.

Matrici associate

Sia W un sottospazio isotropo di dimensione k di V e sia

$$(w_1, u_1, \ldots, w_n, u_n)$$

una base iperbolica di V tale che

$$(w_1, \ldots w_k)$$

sia una base di W (una tale base esiste per il Lemma di Witt, oppure per il Lemma 13.2.2). Rispetto alla base

$$(w_1, w_2, \ldots, w_{n-1}, w_n, u_n, u_{n-1}, \ldots, u_2, u_1) \tag{13.3}$$

le matrici associate agli elementi di $N_G(W)$ sono del tipo

$$\begin{pmatrix} A & 0 & 0 \\ C & B & 0 \\ D & C' & A' \end{pmatrix}. \tag{13.4}$$

Dove A e A' sono due matrici $k \times k$, la matrice A può essere scelta arbitrariamente in $GL(k, K)$ e la matrice A' è completamente determinata dalla matrice A (e viceversa). Similmente le matrici C e C' sono legate tra loro: la scelta di una, che può essere arbitraria, determina quella dell'altra. Infine la matrice B può essere scelta come una qualsiasi matrice in $Sp(n-k, K)$ e la matrice D è una qualsiasi matrice $k \times k$ a coefficienti in K. Se Q è radicale unipotente di $N_G(W)$ in G, cioè il centralizzante

$$C_G(W) \cap C_G(W^\perp/W) \cap C_G(V/W^\perp)$$

della serie

$$\{0\} < W \leq W^\perp < V,$$

le matrici associate agli elementi di Q rispetto alla base 13.3, sono matrici del tipo 13.4, con le ulteriori condizioni che A, A' e B sono matrici identiche. Lasciamo al lettore le verifiche ed il compito di trovare la precisa relazione tra le matrici A ed A' e, rispettivamente C e C', usando la relazione 12.18, dove M è una matrice del tipo 13.4 e G_f è la matrice 12.15.

13.5 Sottogruppi radice simplettici

In questa sezione V è uno spazio vettoriale di dimensione $2n$ sul campo K, f è una forma bilineare alternante non degenere su V e $G = Sp(V)$.

Nel capitolo sui gruppi lineari, se $L := N_{GL(V)}(W)$ è un parabolico massimale di $GL(V)$, abbiamo usato i sottogruppi radice $R_{Z,U}$, con $Z \leq W \leq U$, per studiare la struttura di L, in particolare per provare il Teorema di Borel-Tits. Nel caso dei gruppi simplettici, se $H := N_G(W)$ è un sottogruppo parabolico massimale di G, con W sottospazio proprio ed isotropo di V, e Q è il suo radicale unipotente, ci sono due tipi di sottogruppi radice contenuti in Q: i sottogruppi associati a radici lunghe e quelli associati a radici corte (il motivo di questa terminologia sarà spiegato nella sezione 14.2.1). I sottogruppi associati a radici lunghe sono quelli generati da trasvezioni simplettiche (cioè trasvezioni che sono anche isometrie di V) aventi il medesimo centro (e quindi, essendo isometrie, il medesimo asse). Gli elementi non identici dei sottogruppi associati alle radici corte si ottengomo, invece, estendendo a V le trasvezioni dei sottospazi isotropi massimali di V (come abbiamo già osservato più volte, se Y è un sottospazio isotropo massimale di V, per il Lemma 13.3.1, ogni $\gamma \in GL(Y)$ si estende ad un'isometria di V, in particolare questo vale anche per le trasvezioni di Y). Può essere utile visualizzare fin d'ora le matrici associate agli elementi di tali gruppi: usando le notazioni alla fine della sezione precedente, vedremo che le trasvezioni simplettiche generano il sottogruppo di Q i cui elementi sono associati a matrici

del tipo

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ D & 0 & 1 \end{pmatrix}. \tag{13.5}$$

Agli elementi che generano i gruppi associati a radici corte sono associate matrici del tipo

$$\begin{pmatrix} 1 & 0 & 0 \\ C & 1 & 0 \\ 0 & C' & 1 \end{pmatrix}. \tag{13.6}$$

per opportune matrici C e C' che dipendono l'una dall'altra (vedi sezione precedente). Si osservi che l'insieme delle matrici del tipo 13.6 non è un sottogruppo, ma genera un sottogruppo il cui derivato si può dimostrare essere l'insieme delle matrici del tipo 13.5.

13.5.1 Gruppi di radici lunghe e trasvezioni simplettiche

Una trasvezione in G si dice **trasvezione simplettica**. Se τ è una trasvezione simplettica, per la Proprietà Fondamentale delle Isometrie,

$$C_V(\tau) = [V, \tau]^\perp.$$

Come si può vedere facilmente, questo implica che, se $[V, \tau] = \langle u \rangle$, esiste un elemento $a_\tau \in K \setminus \{0\}$ tale che, per ogni $v \in V$,

$$v^\tau = v + a_\tau f(v, u)u. \tag{13.7}$$

Viceversa, una qualsiasi trasvezione τ che verifica la 13.7 per un opportuno scalare a_τ, è simplettica. Fissato un sottospazio U di dimensione 1 il sottogruppo $X_{U,U^\perp}$ generato dalle trasvezioni di G di centro U, si dice **gruppo di radice lunga**. Si verifica immediatamente che $X_{U,U^\perp}$ è abeliano isomorfo al gruppo additivo $(K, +)$.

Sia T il sottogruppo di G generato dalle trasvezioni simplettiche di V. Vogliamo mostrare che $T = G$.

Lemma 13.5.1 *T è transitivo su $V \setminus \{0\}$.*

DIMOSTRAZIONE. Siano u e w in $V \setminus \{0\}$. Se $f(u, w) \neq 0$, sia $\tau\colon V \to V$ la trasvezione simplettica definita, per ogni $v \in V$, da

$$v^\tau = v + f(u, w)^{-1} f(v, u - w)(u - w).$$

Allora

$$u^\tau = w.$$

Se $f(u, w) = 0$, sia

$$z \in V \setminus (\langle u \rangle^\perp \cup \langle w \rangle^\perp).$$

Per la prima parte, esistono due trasvezioni simplettiche ρ e σ tali che $u^\rho = z$ e $z^\sigma = w$, da cui la tesi. ∎

Lemma 13.5.2 *G è transitivo sull'insieme dei gruppi di radici lunghe di V.*

Lemma 13.5.3 *T è transitivo sulle coppie iperboliche di V.*

DIMOSTRAZIONE. Siano (u, x) e (w, y) due coppie iperboliche, vogliamo provare che esiste un elementoo α in T tale che $(u^\alpha, x^\alpha) = (w, y)$. Per il Lemma 13.5.1, posso supporre che $u = w$ e trovare α in $C_T(u)$. Se $f(x, y) \neq 0$ sia $\alpha: V \to V$ definita, per ogni $v \in V$, da

$$v^\alpha = v + f(x, y)^{-1} f(v, x - y)(x - y).$$

Poichè $(x - y) \in \langle u \rangle^\perp$, α è una trasvezione simplettica che centralizza u e, inoltre, $x^\alpha = y$. Se $f(x, y) = 0$, come nel Lemma 13.5.1, sia

$$z \in V \setminus (\langle x \rangle^\perp \cup \langle y \rangle^\perp).$$

Per la prima parte, esistono due trasvezioni simplettiche ρ e σ in $C_T(u)$ tali che $x^\rho = z$ e $z^\sigma = y$, da cui la tesi. ∎

Lemma 13.5.4 *Siano U e W sottospazi di V tali che V somma diretta ortogonale di U e W.*

1. *$C_G(U) \cong Sp(W)$.*
2. *Sia τ una trasvezione simplettica di W, allora τ si estende ad una trasvezione simplettica di V.*

DIMOSTRAZIONE. Esercizio 13.12.7 ∎

Teorema 13.5.5 *$Sp(V)$ è generato da trasvezioni simplettiche*

DIMOSTRAZIONE. Per induzione su $dim(V)$. Sia (u, v) una coppia iperbolica di V, sia $U = \langle u, v \rangle$ e sia $H = C_G(U)$. Per l'argomento di Frattini ed il Lemma 13.5.3, $G = TH$. Se $dim(V) = 2$, $U = V$ e quindi $H = \{1\}$ da cui la tesi. Supponiamo che $dim(V) > 2$. per il Lemma 13.5.4.1 $H \cong Sp(U^\perp)$. Per ipotesi induttiva $Sp(U^\perp)$ è generato da trasvezioni simplettiche di $U^\perp$ e, per il Lemma 13.5.4.2, queste si estendono a trasvezioni simplettiche di V. Quindi H è generato da trasvezioni simplettiche di V, da cui la tesi. ∎

Matrici associate

Siano u e τ come sopra. Siano $u := u_1$ e sia $v_1 \in V$ tale che (u_1, v_1) sia una coppia iperbolica. Per il Corollario 13.2.2 esistono dei vettori $u_2, \ldots, u_n, v_2, \ldots, v_n$ tali che

$$(u_1, v_1, u_2, v_2, \ldots, u_n, v_n)$$

sia una base iperbolica di V. Riordinando la base come in 12.14, otteniamo che la matrice associata a τ rispetto alla base

$$(u_1, u_2, \ldots, u_{n-1}, u_n, v_n, v_{n-1} \ldots, v_2, v_1)$$

è

$$\begin{pmatrix} 1 & 0 & 0 & . & . & . & 0 & 0 & 0 \\ 0 & 1 & 0 & . & . & . & 0 & 0 & 0 \\ 0 & 0 & 1 & . & . & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 1 & 0 & 0 \\ 0 & 0 & 0 & . & . & . & 0 & 1 & 0 \\ 1 & 0 & 0 & . & . & . & 0 & 0 & 1 \end{pmatrix} \tag{13.8}$$

13.5.2 Gruppi di radici corte

Sia $a \in K \setminus \{0\}$, siano u e z in V tali che

$$f(u, z) = 0$$

e sia $\tau_{(a,u,z)}$ l'applicazione da V in V definita, per ogni $v \in V$ da

$$v^{\tau_{(a,u,z)}} := v + a(f(v, u)z + f(v, z)u). \tag{13.9}$$

Lasciamo al lettore la facile verifica che $\tau_{(a,u,z)} \in G$. Definiamo

$$X_{u,z} := \{\tau_{(a,u,z)} | a \in K \setminus \{0\}, v \in V \text{ e } u \in \langle v \rangle^\perp\} \cup \{1\}\}.$$

Si vede facilmente che $X_{u,z}$ è un sottogruppo di G isomorfo al gruppo $(K, +)$ e si dice **sottogruppo associato ad una radice corta** di G. Osserviamo che, se $b, c \in K \setminus \{0\}$,

$$\begin{aligned} v^{\tau_{(a,bu,cz)}} &= v + a(f(v, bu)cz + f(v, cz)bu) = \\ &= v + abc(f(v, u)z + f(v, z)u) = v^{\tau_{(abc,u,z)}}, \end{aligned}$$

in particolare, per ogni $b, c \in K \setminus \{0\}$,

$$X_{u,z} = X_{bu,cz}.$$

Lemma 13.5.6 *Siano $U := \langle u \rangle$, $Z := \langle z \rangle$, $\tau := \{\tau_{(a,u,z)}$ e $H := N_G(U)$*

1. *τ normalizza U e Z e quindi normalizza anche $U\perp$ e $Z^\perp$;*
2. *τ induce su $U^\perp$ una trasvezione di centro $Z^\perp \cap U^\perp$.*
3. *τ induce sullo spazio quoziente V/U una trasvezione di centro $\langle Z, U \rangle / U$ ed asse $U^\perp/U$*
4. *$C_H(\tau)$ normalizza U, $U^\perp$ e induce la medesima applicazione scalare su U e su $U^\perp/(Z^\perp \cap U^\perp)$.*

5. *$C_H(\tau)$ normalizza $\langle U, Z\rangle$ e induce su $\langle Z, U\rangle/U$ e su $V/U^\perp$ la medesima applicazione scalare.*

DIMOSTRAZIONE. I punti 1, 2 e 3 seguono immediatamente dalle definizioni. I punti 3 e 4 seguono rispettivamente dai punti 2 e 3 e dal punto 2 della Proposizione 11.2.3. ■

Matrici associate

Poniamo $u := u_1$ e $z := v_{n-1}$. Per il Lemma 13.2.2 esistono dei vettori $u_2, \ldots, u_n, v_1, v_2, \ldots, v_{n-2}, v_n$ tali che

$$(u_1, v_1, u_2, v_2, \ldots, u_n, v_n)$$

sia una base iperbolica di V. Come sopra, riordinando la base come in 12.14, otteniamo che la matrice associata a $\tau_{(a,u_1,v_2)}$ è

$$\begin{pmatrix} 1 & 0 & 0 & . & . & . & 0 & 0 & 0 \\ -a & 1 & 0 & . & . & . & 0 & 0 & 0 \\ 0 & 0 & 1 & . & . & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 1 & 0 & 0 \\ 0 & 0 & 0 & . & . & . & 0 & 1 & 0 \\ 0 & 0 & 0 & . & . & . & 0 & a & 1 \end{pmatrix} \tag{13.10}$$

13.6 Semplicità di $PSp(V)$

In questa sezione useremo il Criterio di Iwasawa per dimostrare il seguente teorema:

Teorema 13.6.1 *$Sp(2n, q)$ è semplice tranne i casi $Sp(2, 2)$, $Sp(2, 3)$ e $Sp(4, 2)$.*

Prima di iniziare la dimostrazione vogliamo discutere le tre eccezioni. Le prime due sono conseguenza della seguente uguaglianza:

Lemma 13.6.2 *$SL(2, p) = Sp(2, p)$*

DIMOSTRAZIONE. Questo segue dal fatto che, in dimensione 2, se G_f è la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

la condizione 12.18 si verifica se e solo se $det(M) = 1$. ■ La terza eccezione segue dalla seguente immersione:

Lemma 13.6.3 *Se $n \geq 2$, allora S_{2n+2} è isomorfo ad un sottogruppo di $Sp(2n, 2)$. In particolare $SL(4, 2) = S_6$*

DIMOSTRAZIONE. Sia Ω un insieme di ordine $2n+2$ e sia V l'insieme delle partizioni $\{A, B\}$ di Ω tali che A abbia ordine pari. Osserviamo che, se $\triangle$ è la differenza simmetrica, e $\{A_i, B_i\} \in V$, per $i \in \{1, 2\}$, allora anche $\{A_1 \triangle A_2, B_1 \triangle B_2\} \in V$ e l'applicazione

$$\begin{array}{rccc} +: & V \times V & \to & V \\ & (\{A_1, B_1\}, \{A_2, B_2\}) & \mapsto & \{A_1 \triangle A_2, B_1 \triangle B_2\} \end{array}$$

è un'operazione associativa che definisce su V una struttura di 2-gruppo abeliano elementare (e quindi di spazio vettoriale sul campo $GF(2)$ di ordine 2). Inoltre l'applicazione

$$\begin{array}{rccc} f: & V \times V & \to & GF(2) \\ & (\{A_1, B_1\}, \{A_2, B_2\}) & \mapsto & |\{A_1 \cap A_2| + 2\mathbf{Z}, \end{array}$$

è una forma bilineare alternante non degenere su V. Poiché, come si verifica immediatamente, S_{2n+2} agisce fedelmente come gruppo di isometrie di (V, f), segue la prima affermazione. La seconda affermazione si ottiene dalla prima confrontando gli ordini dei rispettivi gruppi. ∎

Proviamo che $Sp(V)$ soddisfa le ipotesi del Criterio di Iwasawa. Per il Lemma 13.2.3 $Sp(V)$ agisce in modo primitivo sull'insieme dei punti della geometria proiettiva $GP(V)$. Per il Lemma **??** G è generato da trasvezioni simplettiche e quindi dai sottogruppi $X_{U,U^\perp}$ associati alle radici lunghe (dove U è un sottospazio di dimensione 1 di V) che sono isomorfi al gruppo additivo di K e quindi abeliani. Per il Lemma **??** i sottogruppi associati alle radici lunghe formano un'unica classe di coniugio. Infine il sottogruppo $X_{U,U^\perp}$ è contenuto nel normalizzante in $Sp(V)$ di U. Per il Criterio di Iwasawa resta quindi da dimostrare che $Sp(V)$ è perfetto, ovvero che ogni trasvezione simplettica è un commutatore di elementi di $Sp(V)$. Ora, se $|K| > 3$, questo è già vero in dimensione 2 per il Lemma 13.6.2, e quindi è vero per ogni dimensione di V. Per $|K| = 2$

13.7 La Decomposizione di Levi nei parabolici di $Sp(V)$

13.8 Azione sul radicale di un parabolico massimale di $Sp(V)$

13.9 Il reticolo dei sottogruppi contenenti un Borel in $Sp(V)$

13.10 Sottogruppi parabolici di $PSp(V)$

13.11 Teorema di Borel-Tits per $PSp(V)$

In questa sezione $G := Sp(V)$.

Lemma 13.11.1 *Sia P un p-sottogruppo non identico di G e $T := N_G(P)$ un sottogruppo p-locale di G. Allora esiste un sottogruppo parabolico massimale H di G che contiene T.*

DIMOSTRAZIONE. Per l'esercizio 8.2.8 $U := C_V(P)$ è diverso da $\{0\}$. Poichè $P \in G$ e P normalizza U, P e T normalizzano anche $U^\perp$ e quindi, di nuovo per l'esercizio 8.2.8,$C_{U^\perp}(P)$ è non identico. Poichè $C_{U^\perp}(P) \leq U \cap U^\perp$, il sottospazio $C_{U^\perp}(P)$ è isotropo e chiaramente

$$T = N_G(P) \leq N_G(C_{U^\perp}(P)),$$

che è parabolico massimale in G. ∎

Sia ora W un sottospazio proprio non isotropo di V, $H := N_G(W)$ e Q il radicale unipotente di H.

Lemma 13.11.2 *Q contiene tutte le trasvezioni simplettiche di centro contenuto in W e tutti i sottogruppi $X_{u,z}$ associati a radici corte tali che $u \in W$ e $z \in W^\perp$*

DIMOSTRAZIONE. Una trasvezione simplettica τ di centro Z centralizza $Z^\perp$ e V/Z. Se $Z \leq W$, allora

$$W \leq W^\perp \leq Z^\perp.$$

Quindi τ centralizza $W^\perp$ e V/W, in particolare, centralizza anche W, $W^\perp/W$ e $V/W^\perp$. Sia ora $X_{u,z}$ un sottogruppo associato ad una radice corta con $u \in W$ e $z \in W^\perp$. Poiché

$$\langle u, z\rangle =\leq W^\perp,$$

segue che

$$X_{u,z} \leq C_G(\langle u\rangle^\perp \cap \langle z\rangle^\perp) \leq C_G(W).$$

Per il Lemma 12.2.6, segue che

$$X_{u,z} \leq C_G(V/W^\perp).$$

Infine, poichè $u \in W$ e $z \in W^\perp$, segue, dalla 13.9, che

$$X_{u,z} \leq C_G(W^\perp/W).$$

■

Lemma 13.11.3 *Sia λ è un elemento di ordine coprimo con p di $C_G(Q)$, allora λ è un'applicazione scalare.*

DIMOSTRAZIONE. Per il Lemma 13.11.2, ogni sottospazio di dimensione 1 di W è centro di una trasvezione simplettica in W ed ogni iperpiano di V contenente W è asse di una tale trasvezione. Quindi λ fissa tutti i sottospazi di W e di $V/W^\perp$. Ne segue, come nel Lemma 11.4.14 che λ induce su W e su $V/W^\perp$ la medesima applicazione scalare. Sia questa la moltiplicazione per lo scalare a. Per il Lemma 13.5.6 λ induce la moltiplicazione per a su ciascun $\langle Z, U\rangle/U$ con $U \in W$ e $Z \in W^\perp$, quindi λ induce la moltiplicazione per a anche su $W^\perp/W$. Quindi λ è il prodotto della moltiplicazione per lo scalare a con un elemento unipotente γ che centralizza la serie

$$\{0\} < W < W^\perp < V.$$

Ma λ ha ordine coprimo con p, quindi $\gamma = 1$ e λ è la moltiplicazione per a. ■

Corollario 13.11.4 TEOREMA DI BOREL-TITS PER $PSp(V)$ *Se V è uno spazio vettoriale di dimensione $2n$ su un campo di caratteristica p, allora $PSp(V)$ è un gruppo di caratteristica locale p.*

13.12 Esercizi

Esercizio 13.12.1 *Sia f una forma bilineare riflessiva su uno spazio V di dimensione finita. Si provi che f induce una forma bilineare non degenere (che continuiamo a chiamare f) sullo spazio quoziente $V/radf$ ponendo, per ogni $v, w \in V$,*

$$f(v + rad(f), u + rad(f)) = f(v, u).$$

Si provi inoltre che la forma indotta su $V/rad(f)$ è non degenere. Osservazione: questo fatto permette di restringere lo studio delle forme bilineari riflessive allo studio delle forme riflessive non degeneri

Esercizio 13.12.2 *Si dimostri il Lemma 12.1.6.*

Esercizio 13.12.3 *Si provi che, se $\mathcal{F}$ è una camera simpettica, allora $\mathcal{F}^\circ$ è una camera proiettiva.*

Esercizio 13.12.4 *Si provi che per ogni $S \in Syl_p(Sp(V)$ esiste $S^\circ \in Syl_p(GL(V))$ tale che $S = S^\circ \cap Sp(V)$.*

Esercizio 13.12.5 *Si provi che, se τ è una trasvezione simplettica in $Sp(V)$, allora esiste $S \in Syl_p(Sp(V)$ tale che $\tau \leq Z(S)$.*

Esercizio 13.12.6 *Si provi che un sottogruppo associato ad una radice lunga di $Sp(V)$ non è contenuto nel centro di un p-Sylowq di $Sp(V)$.*

Esercizio 13.12.7 *Si dimostri il Lemma 13.5.4*

13.12.7

Capitolo 14

Sistemi di Tits

La teoria dei sistemi di Tits permette di trattare in modo uniforme diversi aspetti dei gruppi finiti di tipo Lie: nei capitoli precedenti, abbiamo determinato la struttura normale e la struttura parabolica dei gruppi lineari e simplettici, quegli stessi risultati, come mostreremo ora, si potevano ottenere in generale con la teoria dei sistemi di Tits. Non svolgeremo tutte le dimostrazioni, ma per alcune di queste daremo solo indicazioni bibliografiche.

14.1 Sistemi di Tits

Un **sistema di Tits** o **coppia** BN è una quadrupla (G, B, N, S) dove G è un gruppo, B ed N sono sottogruppi di G ed S è un insieme finito di classi laterali di $B \cap N$ in N tali che le seguenti condizioni siano soddisfatte:

1. $B \cap N$ è un sottogruppo normale di N,
2. $N/(B \cap N)$ è generato da S
3. $G = \langle B, N \rangle$,
4. per ogni $s \in S$ e $w \in N/(B \cap N)$, allora
$$sBw \subseteq BwB \cup BswB,$$
5. per ogni $s \in S$
$$B^s \neq B.$$

Nei punti 4. e 5. si osservi che $B \cap N$ è contenuto nel nucleo delle azioni per moltiplicazione a destra (rispettivamente a sinistra, e per coniugio) di N sull'insieme delle classi laterali destre di B (rispettivamente sull'insieme delle classi laterali sinistre e sull'insieme dei coniugati di B). Se $w \in N/B \cap N$, le notazioni wB, Bw e B^w sono da intendere rispettivamente $\overline{w}B$, $B\overline{w}$ e $B^{\overline{w}}$

dove $\overline{w}$ è un elemento di N tale che $w = (B \cap N)\overline{w}$. Questa è una convenzione comunemente adottata nella teoria dei sistemi di Tits.

La sezione $N/B \cap N$ si dice **gruppo di Weyl** e la indicheremo con W. I gruppi di Weyl, come vedremo, hanno un ruolo centrale nella teoria dei sistemi di Tits (G, B, N, S).

14.1.1 Sistemi di Tits per i gruppi lineari

In questo paragrafo V è uno spazio vettoriale di dimensione n su un campo K e $G \in \{GL(V), SL(V)\}$. Inoltre

$$(v_1, v_2, \ldots, v_n)$$

è una base di V, Σ è il telaio

$$\{\langle v_1\rangle, \langle v_2\rangle, \ldots, \langle v_n\rangle\},$$

e $\mathcal{F}$ la camera

$$V_1 < V_2 < \ldots < V_n,$$

dove

$$V_i := \langle v_1, \ldots, v_i\rangle.$$

Per comodità, se X è un sottospazio di V, indichiamo con $\Sigma \cap X$ l'insieme $\{P \in \Sigma | P \leq X\}$. Indichiamo inoltre con B il sottogruppo di Borel che normalizza la bandiera $\mathcal{F}$ e con N il normalizzante di Σ. N si dice sottogruppo **monomiale** di G e le matrici associate agli elementi di V rispetto alla base $(v_1, v_2, \ldots, v_n)$ si dicono **monomiali** e sono caratterizzate dal fatto di avere esattamente un'unica entrata diversa da zero in ciascuna riga ed in ciascuna colonna (e determinante uguale a 1). Si osservi che N agisce su Σ permutandone i punti ed il nucleo dell'azione è $B \cap N$: infatti, se γ è un elemento di N che fissa tutti i punti di Σ, allora fissa anche ogni bandiera supportata da Σ e quindi è contenuto in B. Viceversa, se δ è un elemento di $B \cap N$, allora δ normalizza $\Sigma \cap V_i$ per ciascun $i \in \{1, \ldots, n\}$. Poiché

$$\Sigma \cap V_i = \{\langle v_1\rangle, \ldots \langle v_i\rangle\}$$

segue facilmente per induzione su i che δ fissa $\langle v_i\rangle$ per ogni $i \in \{1, \ldots, n\}$ e quindi è contenuto nel nucleo dell'azione di N su Σ. Poniamo

$$H := B \cap N \text{ e } W := N/H$$

Dalla discussione precedente, segue che W è isomorfo ad un sottogruppo del gruppo delle permutazioni di Σ. D'altra parte, per il Teorema di Estensione per Linearità, ogni permutazione di Σ è indotta da un'applicazione lineare ϕ che può essere scelta in $SL(V)$ (perche?). In particolare, poichè $|\Sigma| = n$,

$$W \text{ è isomorfo a } S_n.$$

Per ogni $i \in \{1, \ldots, n-1\}$, sia s_i la trasposizione di W che scambia $\langle v_i\rangle$ con $\langle v_{i+1}\rangle$ e viceversa e sia

$$S := \{s_1, s_2, \ldots, s_{n-1}\}.$$

Per **??** W è generato da S. Il risultato principale di questa sezione è il seguente.

Teorema 14.1.1 *Sia V uno spazio vettoriale di dimensione n su un campo K e $G \in \{GL(V), SL(V)\}$. Siano B, N ed S definiti come sopra, allora (G, B, N, S) è un sistema di Tits.*

Le prime due condizioni dei sistemi di Tits sono state dimostrate nella discussione precedente. Per le restanti sono necessari alcuni risultati sull'azione di G su $PG(V)$.

Lemma 14.1.2 *Sia Σ' un telaio in $PG(V)$ che supporta $\mathcal{F}$. Allora esiste un elemento β in B, tale che $\Sigma^\beta = \Sigma'$ (e quindi anche $(\Delta(\Sigma))^\beta = \Delta(\Sigma')$).*

DIMOSTRAZIONE. Per induzione su n. Se $n = 1$ non c'e' nulla da dimostrare perchè $\Sigma = \Sigma' = \{\mathcal{F}\}$. Supponiamo che $n \geq 2$ e sia

$$\Sigma' := \{\langle w_1\rangle, \langle w_2\rangle \ldots, \langle w_n\rangle\}.$$

Poichè $\mathcal{F}$ è supportata da Σ e da Σ', risulta

$$\langle v_1, \ldots, v_i\rangle = \langle w_1, \ldots, w_i\rangle = V_i$$

per ogni $i \in \{1, \ldots, n\}$ Ne segue che, $\Sigma \setminus \{v_n\}$ e $\Sigma' \setminus \{w_n\}$ sono due telai in $PG(V_{n-1})$ contenenti la camera

$$\overline{\mathcal{F}} := V_1 < \ldots < V_{n-2}.$$

Per il Teorema di Estensione per Linearità, esiste un elemento $\beta \in B$ che manda $\Sigma \setminus \{v_n\}$ in $\Sigma' \setminus \{w_n\}$, Poichè $(v_1, \ldots, v_n)$ e $(w_1, \ldots, w_n)$ sono basi di V, tale elemento puo' essere scelto in modo che $v_n^\beta = w_n$. ∎

Lemma 14.1.3 *W è regolare su $\Delta(\Sigma)$.*

DIMOSTRAZIONE. Segue dal fatto che W è regolare sull'insieme delle permutazioni di Σ e le permutazioni di Σ sono in biiezione con le bandiere supportate da Σ. ∎

Lemma 14.1.4 *$G = BNB$, in particolare $G = \langle B\rangle$.*

DIMOSTRAZIONE. Sia $\gamma \in G$. Per il Lemma A.4.3 esiste un appartamento Δ che contiene $\mathcal{F}^\gamma$ e $\mathcal{F}$. Per il Lemma 14.1.2 esiste un elemento $\beta \in B$ tale che $\Delta^\beta = \Delta(\Sigma)$ e quindi

$$\mathcal{F}^{\gamma\beta} \in \Delta(\Sigma).$$

Per 14.1.3 esiste un elemento $\nu \in N$ tale che

$$\mathcal{F}^{\gamma\beta\nu} = \mathcal{F},$$

cioè $\gamma\beta\nu \in B$. Ma allora

$$\gamma \in B\nu\beta \leq BNB,$$

da cui la tesi. ∎

Lemma 14.1.5 *Siano $\mathcal{U}$ e $\mathcal{W}$ due bandiere supportate da entrambi i telai Σ_1 e Σ_2. Allora esiste $\phi \in SL(V)$ che fissa ciascun sottospazio di $\mathcal{U}$ e di $\mathcal{W}$ e tale che $(\Sigma_1)^\phi = \Sigma_2$.*

DIMOSTRAZIONE. Osserviamo che ogni biiezione tra Σ_1 e Σ_2 è indotta da un elemento di $SL(V)$. Cerchiamo quindi una tale biiezione che fissi anche ogni sottospazio di $\mathcal{U}$ e di $\mathcal{W}$. Sia $i \in \{1, 2\}$. Siano $\mathcal{U}$ e $\mathcal{W}$ rispettivamente le bandiere (scritte con gli indici decrescenti)

$$U_1 > U_2 > \ldots > U_h$$

e

$$W_1 > W_2 > \ldots > W_k.$$

Proviamo la tesi per induzione su $n = dim(V)$. Se $n = 1$ la tesi è ovvia. Supponiamo che $n > 1$. Per il Lemma A.4.4, possiamo supporre che

$$V = \langle U_1, W_1 \rangle.$$

Sia $\mathcal{Z}$ la bandiera

$$Z_2 > \ldots > Z_m,$$

dove,

$$\{Z_2 \ldots, Z_m\} = \{W_j \cap U_1 | j \in \{i, \ldots, k\}\}.$$

Per ipotesi induttiva esiste un elemento $\gamma \in SL(U_1)$ che fissa ciascun sottospazio delle bandiere $\mathcal{U} \setminus \{U_1\}$ e $\mathcal{Z}$ e tale che

$$(\Sigma_1 \cap U_1)^\gamma = \Sigma_2 \cap U_1. \tag{14.1}$$

Per ogni $j \in \{1, \ldots, k\}$ sia

$$\Delta_{i,j} = \Sigma_i \cap (W_j \cap U_1)$$

e

$$\Gamma_{i,j} := (\Sigma_i \cap W_j) \setminus \Delta_{i,j}.$$

Allora

$$\Gamma_{i,1} \supseteq \Gamma_{i,2} \supseteq \ldots \supseteq \Gamma_{i,k}, \tag{14.2}$$

$$\Sigma_i \cap W_j \text{ è unione disgiunta di } \Delta_{i,j} \text{ e } \Gamma_{i,j}$$

e

$$\Sigma_i \text{ è unione disgiunta di } \Sigma_i \cap U_1 \text{ e } \Gamma_{i,j}. \tag{14.3}$$

e quindi W_j è la somma diretta di $\langle \Delta_{i,j} \rangle$ e $\langle \Gamma_{i,j} \rangle$. Per 14.2 esiste una biiezione τ tra $\Gamma 1, 1$ e $\Gamma_{1,2}$ tale che

$$\Gamma_{1,j}^\tau = \Gamma_{2,j},$$

per ogni $j \in \{1, \ldots, k\}$ e quindi, per 14.3, esiste una biiezione σ tra Σ_1 e Σ_2 tale che :

$$P^\sigma = P^\gamma \text{ se } P \in \Sigma_1 \cap U_1$$

e

$$P^\sigma = P^\tau \text{ se } P \in \Sigma_1 \setminus U_1$$

Se $\phi \in SL(V)$ induce σ, allora ϕ soddisfa la tesi. ∎

Corollario 14.1.6 *Se $w \in W$, $s \in S$, allora $sBw \leq BwB \cup BswB$.*

DIMOSTRAZIONE. Siano σ e ν elementi di N tali $H\sigma = s$ e $H\nu = w$ e sia $\sigma\beta\nu \in sBw$ con $\beta \in B$. Vogliamo mostrare che

$$\sigma\beta\nu \in BwB \cup BswB.$$

Poichè $s \in S$, σ scambia due punti di Σ e quindi, posto

$$\mathcal{B} := \mathcal{F} \cap \mathcal{F}^\sigma,$$

$\mathcal{B}$ è un muro in $GP(V)$. Inoltre

$$\mathcal{B}^\sigma = \mathcal{B}$$

perché σ scambia anche $\mathcal{F}$ e $\mathcal{F}^\sigma$ tra loro e

$$\mathcal{B}^\beta = \mathcal{B}$$

perchè $\beta \in B = N_G(\mathcal{F}) \leq N_G(\mathcal{B})$. In particolare

$$\mathcal{B}^\nu = \mathcal{B}^{\sigma\beta\nu} \subseteq \mathcal{F}^{\sigma\beta\nu}.$$

Per il Lemma A.4.3 esiste un telaio Σ' che supporta sia $\mathcal{F}$ che $\mathcal{F}^{\sigma\beta\nu}$, e quindi anche $\mathcal{B}^\nu$. D'altra parte, poiché Σ supporta sia $\mathcal{F}$ che $\mathcal{B}$ e ν normalizza Σ, anche

$$\Sigma \text{ supporta sia } \mathcal{F} \text{ che } \mathcal{B}^\nu.$$

Per il Lemma 14.1.5 esiste $\phi \in B$ che normalizza $\mathcal{B}^\nu$ tale che

$$(\Sigma')^\phi = \Sigma.$$

Ne segue che $\mathcal{F}^{\sigma\beta\nu\phi}$ è una camera di Σ che contiene il muro $\mathcal{B}^\nu$. D'altra parte, per come è stato definito $\mathcal{B}$, $\mathcal{F}^\nu$ e $\mathcal{F}^{\sigma\nu}$ sono due camere che contengono $\mathcal{B}^\nu$ e, per il Lemma A.4.2 sono le uniche camere di Σ che lo contengono. Quindi

$$\mathcal{F}^{\sigma\beta\nu\phi} \in \{\mathcal{F}^\nu,\ \mathcal{F}^{\sigma\nu}\}.$$

Se $\mathcal{F}^{\sigma\beta\nu\phi} = \mathcal{F}^\nu$, allora $\sigma\beta\nu\phi\nu^{-1} \in B$, cioè

$$\sigma\beta\nu \in B\nu\phi^{-1} \leq B\nu B,$$

se $\mathcal{F}^{\sigma\beta\nu\phi} = \mathcal{F}^{\sigma\nu}$, allora $\sigma\beta\nu\phi\nu^{-1}\sigma^{-1} \in B$, cioè

$$\sigma\beta\nu \in B\sigma\nu\phi^{-1} \leq B\sigma\nu B,$$

da cui la tesi. ∎

Possiamo ora completare la dimostrazione del Teorema14.1.1. Infatti il punto 3) della definizione di sistema di Tits segue dal Lemma 14.1.4, il punto 4) segue dal Lemma 14.1.6 ed il punto 5) segue dal Lemma 14.1.3.

Chiudiamo questo paragrafo con un'altra conseguenza del Lemma 14.1.5.

Corollario 14.1.7 *Siano w_1 e w_2 in W. Allora $Bw_1B = Bw_2B$ se e solo se $w_1 = w_2$.*

DIMOSTRAZIONE. Per ogni $i \in \{1, 2\}$, sia $\nu_i \in N$ tale che $H\nu_i = w_i$. Per ipotesi, esistono β_1, β_2 in B tali che

$$\nu_2 = \beta_1\nu_1\beta_2. \tag{14.4}$$

Proviamo che

$$\{\mathcal{F},\ \mathcal{F}^{\nu_2}\} \subseteq \Sigma \cap \Sigma^{\beta_2}. \tag{14.5}$$

Poiché $\beta_i \in B = N_G(\mathcal{F})$, otteniamo che

$$\mathcal{F} \in \Sigma \cap \Sigma^{\beta_2}$$

e, poichè $\nu_i \in N_G(\Sigma)$ dalla 14.4, segue che $\mathcal{F}^{\nu_2} \in \Sigma$ e

$$\mathcal{F}^{\nu_2} = \mathcal{F}^{\beta_1\nu_1\beta_2} = \mathcal{F}^{\nu_1\beta_2} \in \Sigma^{\beta_2},$$

il che prova la 14.5 Per il Lemma 14.1.5 esiste $\phi \in B \cap N_G(\mathcal{F}^{\nu_2})$ tale che

$$\Sigma^{\beta_2\phi} = \Sigma,$$

dunque $\beta_2\phi \in H \trianglelefteq H$. Ma allora

$$\mathcal{F}^{\nu_2} = \mathcal{F}^{\nu_1\beta_2} = \mathcal{F}^{\nu_1\beta_2\phi} = \mathcal{F}^{(\nu_1\beta_2\phi\nu_1^{-1})\nu_1} = \mathcal{F}^{\nu_1},$$

e quindi $\nu_1\nu_2^{-1} \in H$, da cui la tesi. ∎

14.1.2 Sistemi di Tits per i gruppi simplettici

14.2 Gruppi di Weyl

14.2.1 Gruppi di riflessioni

Sia V uno spazio vettoriale su un campo K di caratteristica diversa da 2 e sia

$$f\colon V \times V \to V$$

una forma bilineare simmetrica non degenere su uno spazio vettoriale V. Sia W un iperpiano di V tale che $W \cap W^{\perp} = \{0\}$. Una **riflessione** ρ di **asse** W è un'isometria non identica di V che fissa tutti gli elementi di W.

Lemma 14.2.1 *Siano V, f e W come sopra. Allora esiste un'unica riflessione ρ di asse W. Tale riflessione fissa tutti gli elementi di W e manda ogni elemento di $W^\perp$ nel suo opposto.*

DIMOSTRAZIONE. Sia

$$v \in W^\perp \setminus \{0\},$$

allora

$$W^\perp = \langle v \rangle \text{ e } V = W \oplus \langle v \rangle.$$

Quindi esiste un'applicazione lineare ρ che fissa W e manda ogni vettore di $W^\perp$ nel suo opposto. Tale applicazione è un'isometria di (V, f), infatti se $z \in V$, allora esistono $w \in W$ e $k \in K$ tali che

$$z = w + kv. \tag{14.6}$$

Ma allora, essendo v e w ortogonali,

$$\begin{aligned} f(z^\rho, z^\rho) &= f(w^\rho + kv^\rho, w^\rho + kv^\rho) = f(w^\rho, w^\rho) + f(kv^\rho, kv^\rho) = \\ &= f(w, w) + f(-kv, -kv) = f(w, w) + f(kv, kv) = \\ &= f(w + kv, w + kv) = f(z, z). \end{aligned}$$

Proviamo ora l'unicità: Sia σ una riflessione di asse W. Poiché σ centralizza W, normalizza anche $W^\perp$, quindi, se

$$v \in W^\perp \setminus \{0\},$$

allora

$$v^\sigma \in W^\perp = \langle v \rangle,$$

dunque esiste uno scalare k in K tale che

$$v^\sigma = kv.$$

Poiché

$$f(v, v) = f(v^\sigma, v^\sigma) = k^2 f(v, v),$$

dev'essere $k \in \{1, -1\}$ cioè

$$v^\sigma \in \{v, -v\}.$$

Poiché σ centralizza W ma non V e $V = W \oplus \langle v \rangle$, dev'essere

$$v^\sigma = -v.$$

■

Se W è un iperpiano di V tale che $W \cap W^\perp = \{0\}$ indicheremo con ρ_W l'unica riflessione di centro W. La retta $W^\perp$ si dice **centro** di ρ_W.

Corollario 14.2.2 *Una riflessione ha ordine* 2.

DIMOSTRAZIONE. Sia ρ una riflessione e W il suo asse. Allora ρ^2 lascia fisso ogni vettore di W e di $W^\perp$, quindi induce l'identità su tutto V. ∎

Lemma 14.2.3 *Sia ρ una riflessione di asse W e sia $v \in W^\perp \setminus \{0\}$. Allora, per ogni $z \in V$, risulta*

$$z^\rho = z - 2\frac{f(z,v)}{f(v,v)}v.$$

DIMOSTRAZIONE. Sia $z \in V$, si vede facilmente che il vettore

$$z - \frac{f(z,v)}{f(v,v)}v$$

è ortogonale a v e quindi è contenuto in W. Dunque la decomposizione 14.6 coincide con

$$z = (z - \frac{f(z,v)}{f(v,v)}v) + \frac{f(z,v)}{f(v,v)}v.$$

Da ciò segue che

$$z^\rho = \frac{f(z,v)}{f(v,v)}v^\rho + (z - \frac{f(z,v)}{f(v,v)}v)^\rho = -\frac{f(z,v)}{f(v,v)}v + (z - \frac{f(z,v)}{f(v,v)}v) = z - 2\frac{f(z,v)}{f(v,v)}v,$$

Da cui la tesi. ∎

Se K è il campo dei numeri reali, una forma bilineare simmetrica f si dice **definita positiva** se $f(v,v) > 0$ per ogni $v \in V \setminus \{0\}$. Ricordiamo che, a meno di isometrie esiste un'unica forma bilineare simmetrica definita positiva su V ed esiste una base rispetto alla quale la matrice di Gram associata a questa forma è la matrice identica (esercizio 14.3.2). Uno **spazio euclideo** è una coppia (V, f), dove V è uno spazio vettoriale di dimensione finita sui numeri reali e f è una forma bilineare definita positiva su V. Se (V, f) è uno spazio euclideo, e $v, z \in V$, lo scalare $f(v,z)/f(v,v)$ è il coseno dell'angolo θ tra v e z. Nel caso degli spazi euclidei reali, la formula del Lemma 14.2.3 si traduce nella seguente, più nota ai geometri:

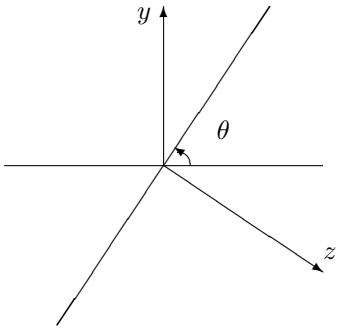
$$z^\rho = z - 2\cos(\theta)v.$$

Un **gruppo di riflessoni** è un gruppo generato da riflessioni di uno spazio euclideo. Il prodotto di due riflessioni in uno spazio euclideo si dice **rotazione**.

Per il Lemma 14.2.2 il gruppo D generato da due riflessioni distinte σ e τ in uno spazio euclideo (V, f) è un gruppo diedrale e, per il Teorema 14.2.8, il sottogruppo generato dalla rotazione $\sigma\tau$ è un sottogruppo normale di indice 2 in D. Per l'esercizio 14.3.5 l'ordine di D dipende solo dall'angolo tra i due assi delle riflessioni

Lemma 14.2.4 *Siano infatti y e z due vettori linearmente indipendenti e non isotropi di V, siano σ e ρ le riflessioni di asse rispettivamente $y^\perp$ e $z^\perp$ e sia θ l'angolo formato dai rispettivi assi. Allora $\sigma\rho$ è una rotazione di 2θ.*

Siano infatti y e z due vettori linearmente indipendenti e non isotropi di V, siano σ e ρ le riflessioni di asse rispettivamente $y^\perp$ e $z^\perp$ e sia θ l'angolo formato dai rispettivi assi come nel seguente disegno:



Per il

Ora sia V di dimensione 2 e K il campo dei numeri reali. Sia (v_ρ, v_σ) una base di V e sia

$$(,): V \times V \to \mathbf{R}$$

la forma bilineare simmetrica la cui matrice di Gram associata rispetto alla base (v_ρ, v_σ) è

$$\begin{pmatrix} 1 & cos(2\pi/k) \\ cos(2\pi/k) & 1 \end{pmatrix}$$

e siano ρ e σ le due riflessioni di asse rispettivamente v_ρ e v_σ

Sia E il piano euclideo reale, cioè lo spazio vettoriale di dimensione 2 su $\mathbf{R}$ con il prodotto scalare usuale $<,>$, cioè la forma bilineare la cui matrice di Gram associata rispetto alla base canonica di $\mathbf{R}^2$ è

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ricordiamo che, se $v \in E$, una **riflessione** ρ di centro v in E è un'isometria che manda v in $-v$ e fissa puntualmente $v^\perp$. Si vede facilmente che Sia infatti v_ρ e v_σ, due vettori sul piano euclideo reale tali che l'angolo compreso tra essi sia $2\pi/k$ e siano

Sistemi di radici

14.2.2 Gruppi di Coxeter

In questa sezione introduciamo brevemente i gruppi di Coxeter. Un gruppo di Coxeter, di cui daremo tra poco la definizione precisa, è un gruppo G generato da un insieme $R := \{r_1, \dots r_n\}$ di involuzioni che soddisfano unicamente a relazioni del tipo $(r_i r_j)^{m_{i,j}} = 1$. I gruppi diedrali ed i gruppi simmetrici sono gruppi di Coxeter. L'importanza di questa classe di gruppi nei gruppi finiti (così come per

lo studio delle algebre di Lie, dei gruppi di Lie e dei gruppi algebrici) discende soprattutto dal fatto che essi compaiono, nel ruolo di gruppi di Weyl, come sottogruppi dei gruppi semplici di tipo Lie e ne condizionano profondamente la struttura: per esempio, i gruppi classici sono quasi sempre determinati dai loro gruppi di Weyl e dal campo di definizione (le sole eccezioni sono i gruppi di tipo B_n e C_n che, per $n > 2$, non sono isomorfi pur avendo gruppi di Weyl isomorfi).

Non daremo un'esposizione comprensiva della teoria dei gruppi di Coxeter, che non rientra nello spirito di un testo introduttivo alla teoria dei gruppi finiti come questo. Non daremo, quindi, tutte le dimostrazioni, rimandando per queste il lettore alla vasta letteratura sulla teoria dei gruppi di Coxeter: citiamo, ad esempio la sezione 29 di [1], la monografia [19], il capitolo 1 di [7] o il paragrafo 4 del capitolo 3 della parte I di [27].

Per mantenere questo testo autosufficiente, non useremo esplicitamente la teoria dei gruppi di Coxeter, ma vogliamo sottolineare come, usando questa teoria, diversi risultati nei capitoli sui gruppi lineari e simplettici, possono essere dimostrati in un modo alternativo (e più generale) (vedi ad esempio [1] sezione 43) di cui daremo un cenno.

Sia n un intero positivo. Una **matrice di Coxeter** di **rango** n è una matrice simmetrica $n \times n$ a coefficienti interi, in cui le entrate nella diagonale hanno tutte valore 1 e le altre hanno valore maggiore o uguale a 2. Un **Sistema di Coxeter** associato ad una matrice di Coxeter $M = (m_{i,j})$ è una coppia (G, S) dove

1. G è un gruppo e

2. $S := \{s_1, \ldots, s_n\}$ è un sottoinsieme di G tali che

$$G = Grp(\{s_1, \ldots, s_n\} : \{(s_i s_j)^{m_{i,j}} | 1 \leq i, j \leq n\})$$

Un gruppo G si dice **gruppo di Coxeter** se esiste un suo sottoinsieme S tale che (G, S) sia un sistema di Coxeter. La cardinalità di S si dice **rango di Coxeter** di G.

Lemma 14.2.5 *Se (G, S) è un sistema di Coxeter, gli elementi di S sono involuzioni.*

DIMOSTRAZIONE. Sia $(m_{i,j}, i, j \in \{1, \ldots, n\}$, la matrice di Coxeter associata a G. Poiché $m_{i,i} = 1$, gli elementi di S o sono l'identità o sono involuzioni. Proviamo che non sono l'identità. Sia $\langle a \rangle$ un gruppo ciclico di ordine 2. Poiché $(aa)^{m_{i,j}} = 1$ per ogni $i, j \in \{1, \ldots, n\}$, per la proprietà universale delle presentazioni esiste un unico omomorfismo di gruppi $\phi: G \to H$ tale che $s^\phi = a$ per ogni $s \in S$. Quindi, per ogni $s \in S$, $s \notin ker(\phi)$, da cui la tesi. ∎

Se $G, S)$ è un sistema di Coxeter e r, s sono due elementi distinti di S, allora rs è il prodotto di due involuzioni, quindi

$$sr = rrsr = rs^r$$

in particolare

$$|rs| = |sr|$$

il che spiega la condizione di simmetria imposta alle matrici di Coxeter.

Tutte le informazioni su una matrice di Coxeter possono essere visualizzate nel suo *diagramma di Coxeter*: se $M := (m_{i,j})$ è una matrice di Coxeter, il **diagramma di Coxeter** associato a M è un multigrafo (cioè un grafo in cui due vertici possono essere connessi da più lati) composto da n vertici $x_1, \ldots, x_n$ tali che x_i e x_j sono connessi da $m_{i,j} - 2$ lati. Ad esempio, il diagramma di Coxeter associato alla matrice

$$\begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \\ 2 & 2 & 4 & 1 \end{pmatrix}$$

è

(14.7)

Se due nodi in un diagramma di Coxeter sono connessi da k lati, con $k \in \mathbf{N}$, useremo anche la notazione

Osserviamo che, dato un diagramma di Coxeter Δ con n nodi (con n intero positivo), per ottenere una presentazione del gruppo Coxeter associato a Δ, basta considerare il gruppo generato da n involuzioni $s_1, s_2, \ldots, s_n$ soggetto alle relazioni $(s_i s_j)^{m_{i,j}}$ dove $m_{i,j}$ è il numero dei lati che connettono i nodi corrispondenti alle involuzioni s_i ed s_j: ad esempio il gruppo di Coxeter G associato al diagramma 14.7 ha la seguente presentazione:

$$G = Grp(\{s_1, s_2, s_3, s_4\} : \{(s_1 s_2)^3, (s_2 s_3)^3, (s_3 s_4)^4 \text{ e } (s_i s_j)^2 \text{ se } |i-j| > 1\ \})$$

Lemma 14.2.6 *Sia (G, S) un sistema di Coxeter e Δ il diagramma di Coxeter associato a G. Siano $\Delta_1, \ldots, \Delta_r$ le componenti connesse di Δ e, per ogni $k \in \{1, \ldots, n\}$, sia G_k il sottogruppo di G generato dagli elementi di S corrispondenti ai nodi in Δ_k . Allora $G = G_1 \times G_2 \times \ldots \times G_r$.*

Dimostrazione. Sia D il prodotto diretto esterno di $G_1, G_2, \ldots, G_r$. Se $s \in S \cap G_i$, indichiamo con $\overline{s}$ la r-upla $(1, \ldots, s, \ldots, 1)$ che vale s al posto i e 1 altrove e sia

$$\overline{S} := \{\overline{s} | s \in S\}.$$

Se r e s appartengono a due distinte componenti connesse di Δ allora $(rs)^2 = 1$, il che equivale a dire che r e s commutano. Quindi G è il prodotto centrale di $G_1, G_2, \ldots, G_r$ e dunque esiste un omomorfismo suriettivo di gruppi ϕ da D su G tale che

$$\overline{s}^{\phi} = s$$

per ogni $s \in S$. D'altra parte $|\overline{rs}| = |rs|$ per ogni $r, s \in S$, quindi, per la proprietà universale delle presentazioni, esiste un omomorfismo suriettivo δ da G su D tale che

$$s^{\delta} = \overline{s}.$$

Ma allora $\delta\phi$ è un omomorfismo che induce l'applicazione identica su S e quindi è l'applicazione identica su G, da cui segue che ϕ è un isomorfismo e δ è il suo inverso. ■

Un gruppo di Coxeter si dice **irriducibile** se il suo diagramma di Coxeter è connesso.

Sia G un gruppo generato da un insieme S. Se $g \in G$, la **lunghezza** di g **relativa** all'insieme S è la minima lunghezza di una parola w nell'alfabeto $S \cup S^{-1}$ tale che $w = g$.

Lemma 14.2.7 *Sia G un gruppo generato da un insieme S di involuzioni. Allora (G, S) è un sistema di Coxeter se e solo se la seguente condizione è soddisfatta:*
EXCHANGE CONDITION: *Sia $s_i \in S$ per ogni $i \in \{0, \ldots, n\}$ e $g = s_1 s_2 \ldots s_n$. Se $s_0 h$ ha lunghezza minore o uguale a quella di g, allora esiste un indice $k \in \{1, \ldots, n\}$ tale che*

$$s_0 s_1 \ldots s_{k-1} = s_1 \ldots s_{k-1} s_k.$$

DIMOSTRAZIONE. Vedi [1] 29.4 ■

Questa è una importante caratterizzazione dei gruppi di Coxeter tra i gruppi generati da involuzioni: usando il Lemma 14.2.7, si può provare, ad esempio, che i gruppi di riflessioni finiti (che introdurremo tra poco e tra i quali ci sono i gruppi simmetrici finiti) sono gruppi di Coxeter.

14.2.3 Gruppi di Coxeter di rango 2 e gruppi diedrali

Innanzitutto osserviamo che, a meno di isomorfismo, esiste un unico gruppo di Coxeter di rango 1 ed è il gruppo ciclco di ordine 2 che corrisponde alla ed alla matrice di Coxeter

(1)

ed il cui diagramma di Coxeter è

I gruppi di Coxeter di rango 2 hanno come matrice associata la matrice

$$\begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix}$$

dove k è un intero maggiore o uguale a 2, il cui diagramma di Coxeter è

(14.8)

Questi sono tutti e soli i gruppi *diedrali* finiti: un gruppo **diedrale** è un gruppo generato da due involuzioni distinte.

Sia G un gruppo generato da due involuzioni r ed s e sia k l'ordine dell'elemento rs. Poiché r ed s sono involuzioni,

$$(rs)^r = (rs)^s = sr = (rs)^{-1}.$$

Da questo segue che $\langle rs\rangle$ è un sottogruppo normale di indice minore o uguale a 2 in G. Poiché G possiede due involuzioni distinte, G non è ciclico, quindi $|G : \langle rs\rangle| = 2$ e $|G| = 2k$ oppure infinito se k è infinito. Quindi G è l'estensione spezzante del gruppo $\langle rs\rangle$, che è ciclico di ordine k, con il gruppo $\langle r\rangle$ (o $\langle s\rangle$) che ha ordine 2 e r (o s) induce per coniugio su $\langle rs\rangle$ l'automorfismo che manda ogni elemento nel suo inverso. Segue infine che G ha la presentazione

$$G \cong Grp(r, s : r^2, s^2, (rs)^k)$$

e quindi G è un gruppo di Coxeter di rango 2 il cui diagramma di Coxeter associato è come in 14.8.

Il fatto che un gruppo diedrale sia estensione spezzante di un gruppo ciclico C con un gruppo di ordine 2 il cui generatore opera come l'inversione su C ci suggerisce un modo per costruire un gruppo diedrale di ordine infinito o di ordine $2k$ per ogni intero $k \geq 2$. Infatti se $\langle c\rangle$ è un gruppo ciclico di ordine k ($k \geq 2$) oppure di ordine infinito, ed α è l'automorfismo di $\langle c\rangle$ che manda ogni elemento nel suo inverso, allora, nel prodotto semidiretto $\overline{G}$ di $\langle c\rangle$ per $\langle\alpha\rangle$, gli elementi $(\alpha, 1)$ e (α, c) hanno ordine 2, generano $\overline{G}$ e $\overline{G}$ ha ordine infinito oppure $2k$ a seconda che l'ordine di c sia infinito o k.

Teorema 14.2.8 *Per ogni intero k maggiore o uguale a 2 esiste, a meno di isomorfismo, un unico gruppo diedrale di ordine $2k$ le seguenti condizioni sono equivalenti*

1. *G è un gruppo finito generato da due involuzioni distinte;*
2. *G possiede un sottogruppo ciclico C normale di indice 2 e se $a \in G \setminus C$ allora a agisce su C per coniugio come l'automorfismo di C che inverte ogni elemento.*
3. *G è un gruppo di Coxeter di rango 2*

Teorema 14.2.9 *A meno di isomorfismo esiste un unico gruppo diedrale G di ordine infinito e G possiede un sottogruppo ciclico C normale di indice 2 e se $a \in G \setminus C$ allora a agisce su C per coniugio come l'automorfismo di C che inverte ogni elemento.*

Osserviamo che il gruppo di Klein $C_2 \times C_2$ è diedrale ed il suo diagramma di Coxeter è

(14.9)

Esiste anche una costruzione geometrica dei gruppi diedrali finiti: se ρ e σ sono due riflessioni (vedi la definizione nel paragrafo successivo) nel piano euclideo reale ed i loro assi formano un angolo di π/k, allora il prodotto $\rho\sigma$ è una rotazione di $2\pi/k$. Questo si vede facilmente, e lo lasciamo per esercizio, scrivendo le matrici di ρ e σ rispetto ad una base ortonormale del piano euclideo.

La costruzione geometrica dei gruppi diedrali accennata alla fine del paragrafo precedente può essere generalizzata a tutti i gruppi di Coxeter finiti. Se G è un gruppo di Coxeter finito di rango n con matrice di Coxeter associata $(m_{i,j})$, si prendono n vettori $v_1, v_2, \ldots, v_n$ in uno spazio euclideo reale di dimensione n in modo che l'angolo tra v_i e v_j sia $2\pi/m_{i,j}$, per ogni $i, j \in \{1, \ldots, n\}$. Il gruppo generato dalle riflessioni di centro v_i, per ogni $i \in \{1, \ldots, n\}$ si dimostra essere isomorfo a G. Ci sono due ostacoli da superare: uno è provare che esistano dei vettori $v_1, v_2, \ldots, v_n$ che abbiano tali angoli tra loro, l'altro è che le riflessioni aventi per centro questi vettori generino un gruppo di Coxeter. Nella discussione che segue daremo una traccia di questa costruzione.

I gruppi simmetrici come gruppi di Coxeter

Osserviamo innanzitutto che, per ogni intero positivo k, con $k \geq 2$, esiste un gruppo diedrale di ordine $2k$, infatti se se $\langle c \rangle$ è un gruppo ciclico di ordine k ($k \geq 2$) oppure di ordine infinito, ed α è l'automorfismo di $\langle c \rangle$ che manda ogni elemento nel suo inverso, allora, nel prodotto semidiretto $\overline{G}$ di $\langle c \rangle$ per $\langle \alpha \rangle$, gli elementi $(\alpha, 1)$ e (α, c) hanno ordine 2 e generano $\overline{G}$, quindi $\overline{G}$ è un gruppo diedrale di ordine infinito (se c ha ordine infinito) oppure $2k$ (se c ha ordine k).

sia, infatti, G un gruppo generato da due involuzioni r e s tali che $(rs)^n = 1$ per un certo intero non negativo n.

Si osservi che, poiché r_i e r_j hanno ordine 2, $m_{i,i} = 1$ e, inoltre, $r_j r_i$ è l'inverso di $r_i r_j$ e quindi ha lo stesso ordine di $r_i r_j$, cioè $m_{i,j} = m_{j,i}$.Quindi un gruppo di Coxeter è completamente descritto dalla matrice simmetrica $(m_{i,j})$, che si dice, appunto, matrice di Coxeter. Un altro modo, equivalente, per descrivere un gruppo di Coxeter è attraverso il grafo di Coxeter: questo è un multigrafo il cui insieme dei vertici coincide con l'insieme R e due vertici r_i ed r_j sono conessi da $m_{i,i} - 2$ lati. Si può dimostrare che, se il grafo di Coxeter è sconnesso, il gruppo di Coxeter corrispondente è prodotto diretto dei gruppi di Coxeter corrispondenti alle componenti connesse. Questo riduce lo studio dei gruppi di Coxeter a quelli irriducibili, cioè quelli il cui grafo di Coxeter è connesso. È relativamente facile classificare a meno d'isomorfismo i gruppi di Coxeter irriducibili finiti (cfr. [19] o [27]): essi rientrano in quattro famiglie infinite (A_n, B_n, C_n e $I_2(m)$) o in sei casi sporadici (E_6, E_7, E_8, F_4, H_3 e H_4).

I gruppi di Coxeter possono essere caratterizzati dal fatto di essere generati da involuzioni e soddisfare una particolare condizione sulle parole: la *condizione di scambio* (*exchange condition*. Questo fatto permette di dimostrare che i gruppi di riflessioni finiti ed i gruppi di Weyl sono gruppi di Coxeter, anzi, nel caso di gruppi finiti, i gruppi di riflessioni coincidono con i gruppi di Coxeter.

14.3 Esercizi

Esercizio 14.3.1 *Si provi che, se V è uno spazio vettoriale su un campo di caratteristica diversa da 2 e $(.): V \times V \to V$ è una forma bilineare simmetrica non degenere su V, allora ogni isometria ρ, tale che $dim([V, \rho]) = 1$ è una riflessione.*

Esercizio 14.3.2 *Sia V uno spazio vettoriale di dimensione n sul campo dei numeri reali. Si provi che se f è una forma bilineare definita positiva, allora esiste una base di V rispetto alla quale la matrice di Gram associata a f è la matrice identica. Suggerimento: se v_1 è un vettore non nullo di V, lo spazio V si decompone come la somma diretta di $\langle v \rangle$ e di $\langle v \rangle^\perp$. Si provi che f induce una forma bilineare definita positiva su $\langle v \rangle^\perp$ e si provi, per induzione su n che V possiede una base $(v_1, v_2, \ldots v_n)$ i cui vettori siano a due a due ortogonali. Si normalizzi infine tale base dividendo ciascun vettore v_i per la radice quadrata di $f(v_i, v_i)$.*

Esercizio 14.3.3 *Si classifichino tutte le forme bilineari simmetriche su uno spazio V di dimensione finita sul campo dei numeri reali. Per l'esercizio 13.12.1, qui e nell'esercizio seguente ci si può restringere alle forme non degeneri*

Esercizio 14.3.4 *Si classifichino tutte le forme bilineari simmetriche su uno spazio V di dimensione finita su un campo finito.*

Esercizio 14.3.5 *Sia (V, f) uno spazio euclideo e siano $r, s, t \in \mathbf{R} \setminus \{0\}$ Si provi che il gruppo delle isometrie di (V, f) è transitivo sull'insieme delle coppie di vettori non nulli (v, w) tali che $f(v, v) = r$, $f(w, w) = s$, $f(v, w) = t$ (suggerimento si osservi che V è somma diretta di $\langle v, w \rangle$ e di $\langle v, w \rangle^\perp$ che sono spazi euclidei).*

Capitolo 15

Analisi locale

15.1 Introduzione

Per analisi locale si intende lo studio delle proprietà dei sottogruppi p-locali di un gruppo (p un numero primo) e di come queste proprietà si riflettono su tutto il gruppo. Uno degli esempi più importanti è la fusione: se Gè un gruppo ed H è un sottogruppo di G, due elementi a e b (risp. due sottoinsiemi A e B) di H si dicono **fusi** in G se sono coniugati in G[1]. Se ogni elemento di H è fuso solo con se stesso, diremo che la fusione di H in G è **banale**. La conoscenza della fusione nei sottogruppi di Sylow in un gruppo finito è di fondamentale importanza nello studio dei gruppi finiti[2]. In questo capitolo, usando la mappa transfer, mostreremo che la fusione in un p-sottogruppo di Sylow controlla l'esistenza di p-quozienti propri (Teorema del Sottogruppo Focale di Higman), in particolare, l'assenza di fusione in un p-sottogruppo di Sylow P (ovviamente abeliano) di G implica l'esistenza di un complemento normale di P (Teorema del p-Complemento Normale di Burnside. Un'aspetto fondamentale della fusione è che questa è una proprietà locale (Teorema di Fusione di Alperin). Come

[1]Qualche autore, per esempio [14], impone anche la condizione che a e b non siano gi coniugati in H. In questi appunti, coerentemente con [27] e [1], non verr fatta distinzione tra coniugio e fusione. Seguendo la tradizione useremo, in quanto segue, il termine fusione al posto di coniugio

[2]In anni recenti è stato introdotto il concetto di *fusion system* su un p-gruppo P che può essere descritto come una categoria i cui oggetti sono i sottogruppi di P e l'insieme dei morfismi è definito in modo da approssimare i monomorfismi tra gli elementi di P indotti per coniugio da elementi di un ipotetico gruppo G avente P come sottogruppo di Sylow. Esistono p-gruppi P e fusion systems su P che sono *esotici*, cioè che non sono realizzabili all'interno di un gruppo G avente P come p-Sylow. Molti concetti e proprietà dei gruppi finiti possono essere naturalmente generalizzati ai fusion systems, per esempio si può definire la normalità e quindi la semplicità. Esiste un progetto in corso per classificare i fusion systems semplici sulla traccia della classificazione dei gruppi semplici finiti, dove diversi argomenti risultano essere più semplici per i fusion systems il completamento di tale progetto e la classificazione dei fusion systems semplici esotici potrebbe portare ad una significativa semplificazione della classificazione dei gruppi semplici finiti. Un'introduzione ai fusion systems travalica gli scopi di questo testo, rimandiamo il lettore interessato a questo argomento ai testi [9] e [2]

conseguenza immediata del Teorema di Fusione di Alperin, vedremo che anche l'esistenza di p-complementi normali è controllata localmente (Teorema del p-complemento di Frobenius).

15.2 Transfer e fusione

In questa sezione G è un gruppo finito, H un sottogruppo di G e

$$\alpha: H \to A$$

un omomorfismo da H in un gruppo abeliano $A(= (A, +))$. Vogliamo costruire in modo canonico a partire da α un omomorfismo

$$\mathcal{V}_\alpha: G \to A.$$

Chiaramente, l'esistenza di elementi $g \in G \setminus ker(V)$ implica che $G' < G$. Costruiremo $\mathcal{V}_\alpha$ a partire da un trasversale destro di H in G e mostreremo che tale costruzione è indipendente dal trasversale scelto. Per questo abbiamo bisogno di alcune proprietà dei trasversali.

15.2.1 Trasversali

Sia T un trasversale destro di H in G. Poichè G è l'unione disgiunta delle classi laterali destre Ht, al variare di t in T, segue che per ogni $g \in G$ ed ogni $t \in T$ esiste un'unico elemento

$$f_g(t) \text{ in } T$$

tale che

$$tg \in Hf_g(t)$$

con $f_g(t) \in T$ e quindi esiste un'unica coppia

$$(h_g^T(t), f_g^T(t)) \text{ in } H \times T$$

tale che

$$tg = h_g^T(t) f_g^T(t).$$

Chiaramente, per ogni $g \in G$ la funzione

$$f_g^T: t \mapsto f_g^T(t)$$

è una permutazione di T e l'azione

$$f^T: g \mapsto f_g^T$$

è un'azione di G su T, inoltre l'applicazione

$$t \mapsto Ht$$

è un isomorfismo tra i G-insiemi (T, f^T) e $(G/\ H, \delta)$ (dove, al solito δ è l'azione indotta da G su $G/\ H$ per moltiplicazione a destra).

Proposizione 15.2.1 *Con le notazioni precedenti, per ogni $x, y \in G$,*

1. $f^T_{xy}(t) = f^T_y(f_x(t))$
2. $h^T_{xy}(t) = h^T_x(t)(h^T_y(f^T_x(t)))$

DIMOSTRAZIONE. Poniamo $f := f^T$ ed $h := h^T$ Sia $t \in T$. Per quanto detto sopra, $t(xy)$ si scrive in modo unico come prodotto dell'elemento $h_{xy}(t)$ di H con l'elemento $f_{xy}(t)$ di T. D'altra parte

$$\begin{aligned} t(xy) &= (tx)y = (h_x(t)f_x(t))y = h_x(t)(f_x(t)y) = h_x(t)(h_y(f_x(t))f_y(f_x(t))) \\ &= (h_x(t)(h_y(f_x(t))))(f_y(f_x(t))), \end{aligned}$$

da cui la tesi, essendo $h_x(t)(h_y(f_x(t))) \in H$ e $f_y(f_x(t)) \in T$. ∎

Sia ora S un altro trasversale destro di H in G, vogliamo vedere che relazione esiste tra h^T e h^S. Osserviamo che, per ogni elemento $t \in T$, esiste un unico elemento $\phi(t) \in Ht \cap S$, quindi l'applicazione

$$\phi\colon t \mapsto \phi(t) \tag{15.1}$$

è una biiezione tra T ed S e, per ogni $t \in T$,

$$Ht = H\phi(t).$$

In particolare, posto, per ogni $t \in T$,

$$h(t) := \phi(t)t^{-1},$$

abbiamo che

$$h(t) \in H.$$

Proposizione 15.2.2 *Con le notazioni precedenti, per ogni $x \in G$ ed ogni $t \in T$,*

$$h^S_x(\phi(t)) = h(t)(h^T_x(t)h(f^T_x(t)))^{-1} \tag{15.2}$$

DIMOSTRAZIONE. Sia $t \in T$ e $x \in G$, calcoliamo $\phi(t)x$ come prodotto dell'elemento $h^S_x(\phi(t))$ di H e dell'elemento $f^S_x(\phi(t))$. Per la definizione di $h(t)$,

$$\begin{aligned} \phi(t)x &= (h(t)t)x = h(t)(tx) = h(t)(h^T_x(t)f^T_x(t)) \\ &= h(t)(h^T_x(t)(h(f^T_x(t)))^{-1}\phi(f^T_x(t))) \\ &= (h(t)(h^T_x(t)h(f^T_x(t)))^{-1})\phi(f^T_x(t))) \end{aligned}$$

da cui la tesi, essendo $h(t)(h^T_x(t)h(f^T_x(t)))^{-1} \in H$ e $\phi(f^T_x(t)) \in S$. ∎

15.2.2 Transfer

Sia T un trasversale destro di H in G. Il **transfer** da G su A rispetto all'omomorfismo α è l'applicazione $\mathcal{V}_\alpha^T: G \to A$ definita, per ogni $g \in G$, da

$$\mathcal{V}_\alpha^T: x \mapsto \sum_{t\in T}(h_x^T(t))^\alpha. \tag{15.3}$$

La lettera $\mathcal{V}_\alpha$ deriva da *Verlagerung* che è il termine tedesco per indicare il transfer.

Lemma 15.2.3 *Siano T ed S due trasversali destri di H in G. Allora $\mathcal{V}_\alpha^S = \mathcal{V}_\alpha^T$*

DIMOSTRAZIONE. Sia ϕ definita come in (15.1). Per la definizione 15.3, la Proposizione 15.2.2 e poiché f^T è una permutazione di T, abbiamo

$$\begin{aligned} x^{\mathcal{V}_\alpha^S} &= \sum_{s\in S}(h_x^S(s))^\alpha = \sum_{t\in T}(h_x^S(\phi(t)))^\alpha \\ &= \sum_{t\in T}(h(t)(h_x^T(t)h(f_x^T(t)))^{-1})^\alpha \\ &= \sum_{t\in T}(h(t)^\alpha + (h_x^T(t))^\alpha - (h(f_x^T(t)))^\alpha \\ &= \sum_{t\in T}(h(t)^\alpha + \sum_{t\in T}(h_x^T(t))^\alpha - \sum_{t\in T}(h(f_x^T(t)))^\alpha \\ &= \sum_{t\in T}(h_x^T(t))^\alpha = x^{\mathcal{V}_\alpha^T}. \end{aligned}$$

■

Nel seguito scriveremo quindi semplicemente $\mathcal{V}_\alpha$ al posto di $\mathcal{V}_\alpha^T$

Lemma 15.2.4 *Il transfer $\mathcal{V}_\alpha: G \to A$ è un omomorfismo di gruppi*

DIMOSTRAZIONE. Siano x e y elementi di G e T un trasversale destro di G, allora, per il secondo punto della Proposizione 15.2.1 e poiché f_x^T è una permutazione di T,

$$\begin{aligned} (xy)^{\mathcal{V}_\alpha} &= \sum_{t\in T}(h_{xy}^T(t))^\alpha \\ &= \sum_{t\in T}(h_x^T(t)(h_y^T(f_x^T(t))))^\alpha \\ &= \sum_{t\in T}(h_x^T(t))^\alpha + \sum_{t\in T}(h_y^T(f_x^T(t)))^\alpha \\ &= \sum_{t\in T}(h_x^T(t))^\alpha + \sum_{t\in T}(h_y^T(t))^\alpha = x^{\mathcal{V}_\alpha} + y^{\mathcal{V}_\alpha}. \end{aligned}$$

■

Teorema 15.2.5 *Sia H un sottogruppo di un gruppo G e sia $\alpha: H \to A$ un omomorfismo di H in un gruppo abeliano A. Sia $\mathcal{V}_\alpha$ il transfer di G su A, allora, per ogni $u \in H$,*

$$u^{\mathcal{V}_\alpha} = |G : H| u^\alpha \tag{15.4}$$

DIMOSTRAZIONE. Sia $u \in H$ e siano

$$O_1, \ldots, O_s$$

le orbite di $G/\sim_H$ per l'azione di $\langle u \rangle$ indotta dalla moltiplicazione a destra. Sia, per ogni $i \in \{1, \ldots, s\}$,

$$n_i := |O_i| - 1$$

e t_i un elemento di G tale che

$$Ht_i \in O_i.$$

Allora

$$O_i = \{Ht_i, Ht_iu, \ldots, Ht_iu^{n_i}\}$$

e, posto, per ogni $i \in \{1, \ldots, s\}$,

$$T_i := \{t_i, t_iu, \ldots, t_iu^{n_i}\},$$

abbiamo che $T_i \cap T_j = \emptyset$ se $i \neq j$ ($j \in \{1, \ldots, s\}$) e

$$T := \bigcup_{i=1}^{s} T_i$$

è un trasversale destro di H in G. Ora, per ogni $j \in \{0, \ldots, n_i - 1\}$, $(t_iu^j)u \in T$, quindi

$$h_u^T(t_iu^j) = 1 \text{ per ogni } j \in \{0, \ldots, n_i - 1\}. \tag{15.5}$$

Inoltre, poichè

$$(Ht_iu^{n_i})u = Ht_i$$

segue che

$$(t_iu^{n_i})u = h_u^T(t_iu^{n_i})t_i$$

è la decomposizione di $(t_iu^{n_i})u$ come prodotto dell'elemento $h_u^T(t_iu^{n_i})$ di H con l'elemento t_i di T e quindi

$$h_u^T(t_iu^{n_i}) = t_iu^{n_i+1}t_i^{-1}. \tag{15.6}$$

Calcoliamo ora $u^{\mathcal{V}_\alpha}$ rispetto al trasversale T. Per le uguaglianze (15.5) e(15.6), abbiamo

$$\begin{aligned} u^{\mathcal{V}_\alpha} &= \sum_{t \in T} (h_u^T(t))^\alpha = \sum_{i=1}^{s} \sum_{j=0}^{n_i} (h_u^T(t_iu^j))^\alpha \\ &= \sum_{i=1}^{s} (h_u^T(t_iu^{n_i}))^\alpha = \sum_{i=1}^{s} (t_iu^{n_i+1}t_i^{-1})^\alpha \end{aligned}$$

$$\begin{aligned} &= \sum_{i=1}^{s}(t_i^\alpha + (n_1+1)u^\alpha - t_i^\alpha) \\ &= (\sum_{i=1}^{s}(n_i+1))u^\alpha = |G:H|u^\alpha. \end{aligned}$$

■

15.2.3 Il Sottogruppo focale

Sia H un sottogruppo di G. Il **sottogruppo focale** di H in G è il sottogruppo

$$Foc_G(H) := \langle [h,g] | h \in H, g \in G \text{ e } h^g \in H \rangle$$

In altre parole $Foc_G(H)$ è il sottogruppo di H generato dai quozienti delle coppie di elementi di H che sono fusi in G.

Proposizione 15.2.6 *1. $[H,H] \leq Foc_G(H)$, in particolare $Foc_G(H)$ è un sottogruppo normale di H e $H/Foc_G(H)$ è abeliano*

2. La fusione in H è banale se e solo se $Foc_G(H) = \{1\}$

DIMOSTRAZIONE. Segue immediatamente dalle definizioni. ■

Se π è un insieme di numeri primi è un facile esercizio dimostrare che esiste un sottogruppo normale minimo di G tale che il quoziente sia un π-gruppo (cfr. Esercizio 15.6.1). Tale sottogruppo è caratteristico in G, si chiama **π-residuo** e si indica con $O^\pi(G)$. Si osservi inoltre che $O^\pi(G)[G,G]$ è il minimo sottogruppo normale di G tale che il gruppo quoziente $G/O^\pi(G)[G,G]$ sia un π-sottogruppo abeliano. Infine se H è un π-sottogruppo di Hall di G, allora

$$G = HO^\pi(G). \tag{15.7}$$

Il seguente Teorema, che è il punto centrale di questa sezione, mostra la relazione l'esistenza di π-quozienti abeliani e la fusione in un π-sottogruppo di Hall.

Teorema 15.2.7 (TEOREMA DEL SOTTOGRUPPO FOCALE DI HIGMAN) *Sia H un π-sottogruppo di Hall di un gruppo G. Allora*

1. *$Foc_G(H) = H \cap ker(\mathcal{V}_\alpha) = Foc_G(H) = H \cap [G,G]$;*
2. *$H/Foc_G(H) \cong G/O^\pi(G)[G,G]$.*

DIMOSTRAZIONE. Per definizione

$$Foc_H(G) \leq H \cap [G,G]. \tag{15.8}$$

Sia α la proiezione canonica di H sul quoziente abeliano $H/Foc_G(H)$ e sia $\mathcal{V}_\alpha$ il transfer di G su $H/Foc_G(H)$. Poiché $H/Foc_G(H)$ è un π-gruppo abeliano, segue che

$$[G,G]O^\pi(G) \leq ker\mathcal{V}_\alpha \tag{15.9}$$

Poichè $|G:H|$ è coprimo con $|H|$ (e quindi con $|H/Foc_G(H)|$), segue, per il Teorema 15.2.5 e per l'Esercizio 3.5.11 che

$$Foc_G(H) \leq H \cap ker(\mathcal{V}_\alpha)$$

e

$$H^{\mathcal{V}_\alpha} = \{Foc_G(H)h^{|G:H|} | h \in H\} = \{Foc_G(H)h | h \in H\} = H/Foc_G(H),$$

cioè la restrizione del transfer $\mathcal{V}_\alpha$ ad H è suriettiva. Quindi, per il Primo Teorema di Omomorfismo,

$$Foc_G(H) = H \cap ker(\mathcal{V}_\alpha) \tag{15.10}$$

Da (15.8), (15.9) e (15.10) segue allora che

$$Foc_G(H) \leq H \cap [G,G] \leq H \cap [G,G]O^\pi(G) \leq H \cap ker\mathcal{V}_\alpha = Foc_G(H),$$

da cui segue la prima affermazione. La seconda segue dalla prima perché

$$\begin{aligned} H/Foc_G(H) &= H/(H \cap [G,G]O^\pi(G)) \cong H[G,G]O^\pi(G)/([G,G]O^\pi(G)) \\ &= G/([G,G]O^\pi(G)). \end{aligned}$$

■

Si confronti il seguente corollario con il Teorema di Schur-Zassenhaus.

Corollario 15.2.8 *Sia H un π-sottogruppo di Hall di G. Se la fusione in H è banale, esiste un complemento normale K di H in G.*

DIMOSTRAZIONE. Sia $\mathcal{V}_\alpha$ come nella dimostrazione precedente. Poichè la fusione in H è banale $Foc_G(H) = \{1\}$ e quindi, per il Teorema 15.2.7 $ker(\mathcal{V}_\alpha)$ è un sottogruppo normale di G che complementa H. ■

Si osservi che il sottogruppo K del Corollario 15.2.8 coincide con $O^(\pi)(G)$.

15.2.4 Proprietà locali della fusione

Abbiamo già accennato all'importanza dei sottogruppi p-locali (p un numero primo) nello studio di un gruppo finito G (vedi, ad esempio, l'Esercizio 9.5.11, o il Teorema di Borel-Tits): supponiamo cher p divida G e $O_p(G) = \{1\}$ (in particolare se G è semplice), allora esistono sottogruppi p-locali (per i Teoremi di Sylow) e questi sono tutti sottogruppi propri. In questo caso, quindi, la

classe dei sottogruppi p-locali è un importante serbatoio di sottogruppi propri di G e, per questo motivo, l'*analisi locale*, cioè lo studio dei sottogruppi p-locali di G, è fondamentale per usare l'induzione nel dimostrare le proprietà di G. Schematicamente, la filosofia è quella di partire da ipotesi su G, vedere come queste ipotesi influenzano le proprietà p-locali di G, cioè riguardanti la struttura dei sottogruppi p-locali e, infine, come le informazioni sulla struttura sottogruppi p-locali (su cui valgono le ipotesi induttive) si ritraducano in informazioni *globali* su G. Un tipico esempio (e l'argomento di questa sezione) di come una proprietà locale si traduca in proprietà globale è la fusione in G (Teoremi di Fusione di Burnside e Alperin). Nella sessione successiva, come conseguenza, vedremo come altro esempio, e ancor più evidente, l'esistenza di p-complementi normali (Criteri di p-Nilpotenza di Burnside, Frobenius e Thompson): se ogni (nel caso di Frobenius) o, sotto certe ipotesi, qualche (nel caso di Burnside e Thompson) sottogruppo p-locale ha un p-complemento normale (la proprietà locale) allora G ha un p-complemento normale (proprietà globale).

Argomenti chiave nelle dimostrazioni di questa sezione sono la transitività dell'azione per coniugio di G sull'insieme dei suoi p-sottogruppi di Sylow e che, in un p-gruppo P, un sottogruppo non identico T di P è propriamente contenuto in P se e solo se è propriamente contenuto in $N_P(T)$ (vedi Teorema 9.3.1).

Sia N un sottogruppo di $N_G(H)$ contenente H. Diremo che N **controlla la fusione** di H in G se, per ogni coppia di sottoinsiemi A e B di H, A e B sono fusi in G se e solo se sono fusi in N.

Sia $S \in Syl_p(G)$ e sia A un sottoinsieme non vuoto di S. Diremo che A è **completamente normalizzato** (**fully normalised**) da S se $N_S(A) \in Syl_p(N_G(A))$

La seguente proposizione, che è il punto di partenza per la dimostrazioni dei Teoremi di Fusione di Burnside e Alperin, mostra come la fusione tra sottoinsiemi completamente normalizzati di un p-Sylow sia controllata localmente.

Proposizione 15.2.9 *Sia $S \in Syl_p(G)$ e siano A e B un sottoinsiemi non vuoti di S e completamente normalizzati da S. Allora A e B sono fusi in G se e solo se sono fusi in $N_G(N_S(B))$.*

DIMOSTRAZIONE. Sia g un elemento di G tale che $A^g = B$ e sia $\overline{S} := N_S(A^g)$. Poiché A^g è completamente normalizzato da S e S^g, $\overline{S}$ e $\overline{S}^g$ sono p-sottogruppi di Sylow di $N_G(A)$. Per i Teoremi di Sylow, esiste $h \in N_G(A^g)$ tale che

$$(\overline{S}^g)^h = \overline{S},$$

cioè

$$gh \in N_G(\overline{S}) \text{ e } A^{gh} = A^g.$$

■

Corollario 15.2.10 *Sia $S \in Syl_p(G)$. Se ogni sottoinsieme non vuoto di S è completamente normalizzato da S, allora due sottoinsiemi non vuoti di S sono*

fusi in G se e solo se sono fusi nel normalizzante di un sottogruppo non identico di S.

Corollario 15.2.11 (Teorema di Fusione di Burnside) *Sia $S \in Syl_p(G)$. Se S è abeliano $N_G(S)$ controlla la fusione di S in G.*

Dimostrazione. Segue immediatamente dalla Proposizione 15.2.9 e dal fatto che un gruppo abeliano normalizza ogni suo sottoinsieme. ∎

Se si lascia cadere la condizione che ogni sottoinsieme non vuoto di S è completamente normalizzato da S, il Corollario 15.2.10 non è più vero: ad esempio sia

1. V uno spazio di dimensione 3 su un campo finito di caratteristica p,
2. $\mathcal{F} : V_1 < V_2$ una bandiera massimale di V,
3. $G = GL(V)$ e $S = C_G(\mathcal{F})$,
4. T_1 l'insieme delle trasvezioni di centro V_1
5. T_2 l'insieme delle trasvezioni di asse V_2
6. $H_i := N_G(V_i)$, per $i \in \{1, 2\}$.

Allora $S \in Syl_p(G)$ e, per la Proposizione 11.2.5 e un facile esercizio, tutte le trasvezioni in S sono contenute in $T_1 \cup T_2$ e sono coniugate in G, ma, chiaramente, una trasvezione nel centro di S non può essere fusa in $N_G(S)$ con una trasvezione non centrale.

D'altra parte, per $i \in \{1, 2\}$, $T_i \subseteq H_i$ e H_i agisce transitivamente per coniugio su T_i. Poichè

$$T_1 \cap T_2 = Z(P) \setminus \{1\} \neq \emptyset$$

segue che ogni trasvezione di T_1 è fusa in H_1 con una trasvezione centrale ed una trasvezione centrale è fusa in H_2 con ogni trasvezione di T_2.

Può essere utile visualizzare questo con le matrici associate ad una base opportuna di V: Nella prima riga sono rappresentate le generiche matrici di H_1 e H_2, nella seconda compaiono gli elementi di h_1 e h_2 che coniugano rispettivamente la prima matrice t_1 della terza riga nella seconda t e la seconda matrice della terza riga nella terza t_2. Si noti che $\{h_i, t_i, t\} \subseteq H_i$ e $\{t_i, t\} \subseteq O_p(H_i)$.

$$\begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix} \qquad \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Quello che possiamo vedere da questo esempio è che t_1 e t_2 sono fusi in G, non sono fusi in $N_G(S)$, ma posso passare da t_1 a t_2 coniugando prima t_1 e t con un elemento h_1 del normalizzante di un sottogruppo Q_1 $(= O_p(H_1))$ che contiene sia t_1 che t e poi coniugare t e t_2 con un elemento h_2 del normalizzante di un sottogruppo Q_2 $(=O_p(H_2))$ che contiene sia t che t_2. Si noti che, poiché t è centrale in S, $S \leq N_G(\{t\})$ e quindi

$$N_S(\{t\}) = S \in Syl_p(N_G(\{t\})),$$

cioè, per ogni trasvezione in S, è fusa in G con una trasvezione t tale che $\{t\}$ è completamente normalizzato da S. Questo fatto è vero in generale:

Lemma 15.2.12 *Sia $S \in Syl_p(G)$. Allora, per ogni sottoinsieme A di P esiste un elemento $g \in G$ tale che A^g è completamente normalizzato da S..*

DIMOSTRAZIONE. Sia $Q \in Syl_p(N_G(A))$ tale che $N_S(A) \leq Q$ e sia $\overline{S}$ un p-sottogruppo di Sylow di G contenente Q. Per i Teoremi di Sylow, esiste un elemento $g \in G$ tale che $S = \overline{S}^g$. Poiché

$$N_{\overline{S}}(A) = Q \in Syl_p(N_G(A)),$$

traslando con g si ottiene

$$N_S(A^g) = N_{\overline{S}^g}(A^g) = Q^g \in Syl_p(N_G(A^g)).$$

■

Per un importante risultato di Alperin, la procedura, descritta nell'esempio precedente, di spezzare la fusione in G in una serie di fusioni in sottogruppi p-locali, funziona in generale. Sia infatti p un numero primo, P un p-sottogruppo di Sylow di un gruppo G e $\mathcal{F}$ un insieme di sottogruppi di P. Sia A un sottoinsieme non vuoto di P e sia $\Gamma_{\mathcal{F},A}$ il grafo i cui vertici sono i sottoinsiemi di P che sono fusi con A e tali che due vertici A_i e A_j sono adiacenti se e solo se esiste un elemento Q_i in $\mathcal{F}$ ed un elemento $h_i \in N_G(Q_i)$, tali che

1. $\{A_i, A_j\} \subseteq Q_j$,
2. $A_i^{h_i} = A_j$,
3. Q_i è completamente normalizzato da P.

Sia $g \in G$ tale che anche $A^g \subseteq S$. Diremo che A e A^g sono **$\mathcal{F}$-coniugati via** g se esiste un intero n tale che, per ogni $i \in \{1, \ldots, n-1\}$, esistono degli elementi Q_i in $\mathcal{F}$ e degli elementi h_i in Q_i tali che $A_i^{h_i} = A_{i+1}$ e $g = h_1 h_2 \cdot \ldots \cdot h_{n-1}$. Se A e A^g sono $\mathcal{F}$-coniugati via g, scriveremo $A \sim_{\mathcal{F}} A^g$.

Si osservi che la definizione precedente non richiede soltanto che esista un cammino $(A_1, A_2, \ldots, A_n)$ in $\Gamma_{\mathcal{F},A}$ con $A_1 = A$ e $A_n = A^g$, ma anche che g sia il prodotto degli elementi h_i che coniugano in Q_i A_i con $A_i + 1$.

Per la dimostrazione del Teorema di Alperin useremo i due seguenti risultati (le cui dimostrazioni sono elementari e lasciate per esercizio).

Lemma 15.2.13 *Sia Q un p-sottogruppo di G. Siano A e B due insiemi di generatori di Q fusi in G. Allora, per ogni $g \in G$ tale che $A^g = B$, $g \in N_G(Q)$.*

Lemma 15.2.14 *Sia $S \in Syl_p(G)$, A, B e C sottoinsiemi non vuoti di S tali che A sia $\mathcal{F}$-coniugato con B via g_A e B sia $\mathcal{F}$-coniugato con C via g_B. Allora A $\mathcal{F}$-coniugato con C via $g_a g_b$*

Teorema 15.2.15 (Teorema di Fusione di Alperin) *Sia G un gruppo finito, p un numero primo, $S \in Syl_p(G)$ e $\mathcal{F}$ una famiglia di sottogruppi di S tale che, per ogni sottogruppo T di G, esista un sottogruppo Q di S fuso con T e completamente normalizzato da S. Allora, per ogni sottoinsieme non vuoto A di S ed ogni $g \in G$ tale che $A^g \leq S$, A e A^g sono $\mathcal{F}$-coniugati via g. In particolare, A e A^g sono $\mathcal{L}(S)$-coniugati (dove $\mathcal{L}(S)$ è l'insieme dei sottogruppi di S).*

Dimostrazione. Sia $B := A^g$, $X \in \{A, B\}$ e $T_X := \langle X \rangle$. Per ipotesi esiste un elemento $h_A \in G$ tale che, posto

$$Q := T_A^{h_A},$$

Q sia un sottogruppo di S completamente normalizzato da S. Si osservi che, simmetricamente,

$$Q = T_B^{h_B} \text{ dove } h_B := g^{-1} h_A.$$

Proviamo il teorema per induzione su $l := |S : Q| \, (= |S : T_X|)$. Se $l = 1$, A e B generano S ed il risultato segue dal Lemma 15.2.13. Supponiamo $n > 1$, vogliamo trovare degli $\mathcal{F}$-coniugati A^{g_A} e B^{g_B}, rispettivamente di A e B, che generano Q. Il teorema seguirà allora dal Lemma 15.2.13 e dal Lemma 15.2.14. Sia $\overline{T}_X := N_P(T_X)$. Poiché $\overline{T}_X^{h_X}$ è un p-sottogruppo di $N_G(Q)$ e Q è completamente normalizzato da S, esiste $k_X \in N_G(Q)$ tale che

$$\overline{T}_X^{h_X k_X} \leq N_S(Q).$$

Sia, per $X \in \{A, B\}$,

$$g_X := h_X k_X.$$

Poiché $n > 1$, $T_X < S$ e quindi

$$T_X < \overline{T}_X.$$

Poiché $\overline{T}_X$ e $\overline{T}_X^{g_X}$ sono due p-sottogruppi di S e $|S : \overline{T}_X| < n$, per ipotesi induttiva $\overline{T}_X$ e $\overline{T}_X^{g_X}$ sono $\mathcal{F}$-coniugati via g_X e quindi anche X e X^{g_X} sono $\mathcal{F}$-coniugati via g_X. Ora però

$$\langle X^{g_X} \rangle = \langle X \rangle^{g_X} = T_X^{h_X k_X} = Q^{k_X} = Q,$$

quindi A^{g_A} e B^{g_B} sono insiemi di generatori di U. D'altra parte, poichè $B = A^g$,

$$B^{g_B} = A^{g g_B} = (A^{g_A})^{g_A^{-1} g g_B}$$

e quindi, per il Lemma 15.2.13, posto $h := g_A^- 1 g g_B$, abbiamo

$$h \in N_G(Q) \text{ e } g = g_A h g_B^- 1.$$

Ne segue che

- A è $\mathcal{F}$-coniugato via g_A con A^{g_A},
- A^{g_A} è $\mathcal{F}$-coniugato via h con B^{g_B} e
- B^{g_B} è $\mathcal{F}$-coniugato via g_B^{-1} con B

e quindi, per il Lemma 15.2.14, A è $\mathcal{F}$-coniugato via g $(= g_A h g_B^- 1)$ con B. L'ultima affermazione segue immediatamente dal Lemma 15.2.12. ■

Le applicazioni e le inclusioni usate nella dimostrazione sono rappresentate nel seguente schema:

		$\overline{T}_A \sim_{\mathcal{F}} \overline{T}_A^{g_A}$		(ipotesi induttiva)		$\overline{T}_B \sim_{\mathcal{F}} \overline{T}_B^{g_B}$			
				$N_G(Q)$ / $N_S(Q)$					
$\overline{T}_A$	$\overset{h_A}{\longmapsto}$	$\overline{T}_A^{h_A}$	$\overset{k_A}{\longmapsto}$	$\overline{T}_A^{g_A}$		$\overline{T}_B^{g_B}$	$\overset{k_B^{-1}}{\longmapsto}$	$\overline{T}_B^{h_B}$	$\overset{h_B^{-1}}{\longmapsto}$ $\overline{T}_B$
T_A	$\longmapsto$	$T_A^{h_A}$	$=$	$T_A^{g_A} = Q$		$Q = T_B^{g_B}$	$=$	$T_B^{h_B}$	$\longmapsto$ T_B
A	$\longmapsto$	A^{h_A}	$\longmapsto$	A^{g_A}	$\overset{h}{\longmapsto}$	B^{g_B}	$\longmapsto$	B^{h_B}	$\longmapsto$ B

Come abbiamo osservato, la condizione che due sottoinsiemi A e B di un p-sottogruppo di Sylow S di G siano $\mathcal{F}$-coniugati 'e più forte della semplice esistenza di un cammino in $\Gamma_{\mathcal{F},A}$ da A a B. Ci si potrebbe domandare se dimostrare solo l'esistenza di un cammino avrebbe potuto essere più semplice, ma non è così. Il Teorema di Alperin è un esempio di come un risultato più forte possa essere più semplice da dimostrare che uno più debole. Questa è una caratteristica tipica delle dimostrazioni per induzione (come quella del Teorema di Alperin e come quelle di molti altri risultati sui gruppi finiti), dove una tesi più forte rafforza automaticamente anche le ipotesi induttive.

15.2.5 Controllo locale della p-nilpotenza

Sia p un numero primo. Un gruppo finito G si dice *p-nilpotente* se G possiede un p'-sottogruppo di Hall normale. Nei seguenti due lemmi evidenziamo alcune proprietà elementari della p-nilpotenza (le facili dimostrazioni sono omesse, ma seguono immediatamente dal Secondo Teorema di Omomorfismo 2.1.1).

Lemma 15.2.16 *Sia G un gruppo e p un primo. Se G è p-nilpotente, allora*

(a) ogni sottogruppo di G è p-nilpotente.

(b) ogni quoziente di G è p-nilpotente.

Lemma 15.2.17 *Sia G un gruppo, p un primo e N un sottogruppo normale di G di ordine coprimo con p.*

(a) Se $O^p(G)$ è p-nilpotente, anche G è p-nilpotente.

(b) Se G/N è p-nilpotente, anche G è p-nilpotente.

Vedremo in questa sezione che, sotto certe condizioni, in particolare se $O_p(G) = \{1\}$, l'implicazione in (a) si può invertire: cioè, se ogni sottogruppo proprio di G è p-nilpotente, allora G è p-nilpotente. Per il Teorema del Sottogruppo Focale, infatti, l'esistenza di p-quozienti è controllata dalla fusione in un p-sottogruppo di Sylow e, per il Teorema di Fusione di Alperin, questa è a sua volta controllata dalla fusione nei sottogruppi p-locali. Non dovrebbe quindi sorprendere che anche l'esistenza di p-quozienti, in particolare, la p-nilpotenza sia in qualche modo controllata dai sottogruppi locali. Questo verrà chiarito dai criteri di p-nilpotenza di Burnside e Frobenius che dimostreremo in questa sezione. Si osservi che, se $O_pG = 1$, ogni sottogruppo p-locale di G è un sottogruppo proprio. Questo mostra ancora una volta l'importanza dei sottogruppi p-locali nello studio di un gruppo G con $O_p(G) = 1$ (in particolare se G è semplice). Spesso, in una dimostrazione per induzione, non è necessario che tutti i sottogruppi propri soddisfino l'ipotesi induttiva, ma solo tutti sottogruppi locali, anzi, a volte neppure tutti: nella sezione **??**,infatti, proveremo il criterio di p-nilpotenza di Thompson, che mostra che la p-nilpotenza è controllata dai normalizzanti di due particolari sottogruppi caratteristici di un p-sottogruppo di Sylow.

Incominciamo con un caso speciale.

Teorema 15.2.18 (Criterio di p-nilpotenza di Burnside *Sia G un gruppo, p un numero primo e $S \in Syl_p(G)$ con S abeliano. Allora G è p-nilpotente se e solo se $N_G(S)$ è p-nilpotente.*

Dimostrazione. Per il Lemma 15.2.16, se G è p-nilpotente ogni suo sottogruppo è p-nilpotente, quindi $N_G(S)$ è p-nilpotente. Supponiamo che $N_G(S)$ sia p-nilpotente e sia K un p' sottogruppo di Hall normale di $N_G(S)$. Allora $N_G(S) = SK$ e quindi, poichè S è abeliano e ovviamente normale in $N_G(S)$

$$[S, N_G(S)] = [S, SK] = [S, K] \leq S \cap K = \{1\},$$

Quindi la fusione di S in $N_G(S)$ è banale. Per il Teorema di Fusione di Burnside, la fusione di S in G è banale e quindi, per Corollario 15.2.8, G ha un p-complemento normale, cioè G è p-nilpotente. ∎

Teorema 15.2.19 Teorema del p-complemento di Frobenius *Sia G un gruppo, p un numero primo e $S \in Syl_p(G)$. Le seguenti affermazioni sono equivalenti:*

(a) G è p-nilpotente;

(b) Ogni sottogruppo p-locale è p-nilpotente;

(c) Per ogni sottogruppo T di S, $Aut_G(T)$ è un p-gruppo.

DIMOSTRAZIONE. L'implicazione $(a) \Rightarrow (b)$ segue dal Lemma 15.2.16[(a)]. Supponiamo (b) e sia T un sottogruppo di S. Allora $N_G(T)$ è p-nilpotente per (b). Sia K un p-complemento normale in $N_G(P)$. Allora $[T, K] \leq T \cap K = \{1\}$ perché T e K hanno ordini coprimi. Ne segue che $K \leq C_G(T)$ e quindi $|Aut_G(T)|$ (che è uguale a $[N_G(T) : C_G(T)]$) divide $[N_G(T) : K]$ che è una potenza di p. Proviamo infine che (c) implica (a). Supponiamo per assurdo che ciò non sia vero e sia G sia un controesempio di ordine minimo che soddisfa (c), ma non (a). In particolare

$$O_p(G) = 1. \tag{15.11}$$

Per i Lemmi Lemma 15.2.16[(a)] e 15.2.17

$$G = O^p(G) \tag{15.12}$$

Proviamo che

$$S \textit{controlla la fusione in } S. \tag{15.13}$$

Siano A e B due sottoinsiemi non vuoti di S fusi in G. Sia $d := d(A, B)$ la distanza di B da A nel grafo $\Gamma_{\mathcal{F},A}$. Proviamo, per induzione su n che A e B sono fusi in S. Se $n = 1$ esiste un sottogruppo Q di S completamente normalizzato da S contenente A e B e tale che esista un elemento $h \in N_G(Q)$ con $A^h = B$. Poiché, per (**??**) $G > N_G(Q)$, per la minimalità di $|G|$, $N_G(Q)$ è p-nilpotente. Ne segue che esistono due elementi k ed l tali che $h = kl$, con k in un p-complemento normale in $N_G(Q)$ ed l un p-elemento che può essere scelto in S, poiché Q è completamente normalizzato da S. Poiché $[A, k] \leq [Q, K] \leq Q \cap K = \{1\}$, segue che

$$B = A^h = A^k l = A^l.$$

Supponiamo ora $n > 1$ e la tesi vera per $n - 1$. Siano $A_1 = A$, $A_n = B$ e

$$(A_1, A_2, ..., A_{n-1}, A_n)$$

un cammino da A a B in $\Gamma_{\mathcal{F},A}$. Per ipotesi induttiva esiste $l \in S$ tale che $A^l = A_1^l = A_{n-1}$ e, per il caso $n = 1$ esiste $m \in S$ tale che $A^{lm} = A_{n-1}^m = A_n = B$. Ma allora $A^l m = B$ e $lm \in S$, il che prova (15.13).

Per il Teorema del sottogruppo focale e 15.12

$$S/Foc_G(S) \cong G/O^p(G)[G, G] \cong \{1\} \tag{15.14}$$

e, poiché S controlla la fusione di S in G,

$$Foc_G(S) = [S, S]. \tag{15.15}$$

Da (15.14) e (15.15) segue che $S/[S, S] = \{1\}$, da cui $S = \{1\}$, perché S è un p-gruppo finito e quindi risolubile. Ma allora G è un p'-gruppo e quindi G è esso stesso un p-complemento normale in sè, la contraddizione finale. ∎

15.3 La Fattorizzazione di Thompson

In questa sezione, che è ispirata essenzialmente da [1, sezione 32] e da [15, sezione 26], introduciamo una strategia, dovuta a John Thompson, per studiare i gruppi di caratteristica p, dove p è un numero primo, in particolare i sottogruppi p-locali dei gruppi semplici finiti di caratteristica locale p. Nelle sezioni seguenti, useremo questa strategia per dimostrare il Teorema di Fattorizzazione di Thompson, il Criterio di p-nilpotenza di Thompson ed il Teorema di Thompson (si, sempre lui!) sulla nilpotenza del nucleo di Frobenius.

Sia, H un gruppo di caratteristica p ed $S \in Syl_p(H)$. Ricordiamo che, per il Teorema di Bender-Fitting (Teorema 10.1.15), questo equivale a dire che $H/Z(O_p(H))$ è isomorfo ad un sottogruppo di $Aut(O_p(H))$. È quindi naturale studiare l'azione di H su $O_p(H)$. Questo, però, può rivelarsi molto difficile, perché per ogni p-gruppo finito Q esiste un gruppo finito G con $Q = F^*(G)$ (Esercizio 15.6.7), ma la strategia di Thompson, almeno nel caso in cui H sia un sottogruppo p-locale in un gruppo semplice finito di caratteristica locale p, fornisce una chiave per superare questo ostacolo. Per introdurre questa strategia è utile andare a vedere cosa succede negli esempi classici di gruppi di caratteristica p, che, per il Teorema di Borel-Tits (che abbiamo dimostrato per i gruppi lineari e simplettici), sono i sottogruppi parabolici dei gruppi semplici finiti di tipo Lie su un campo di caratteristica p. Consideriamo, in particolare il caso in cui H sia lo stabilizzatore di un iperpiano in $PSL(n, p^k)$, con $n \geq 3$, che, ricordiamo, è un parabolico massimale di $PSL(n, p^k)$. Ora posto $V := O_p(H)$ e $L := Aut_H(V)$, abbiamo che

V1 *V è abeliano elementare,*

V2 $O_p(L) = \{1\}$

V3 *L è isomorfo ad un quoziente di $GL(n-1, p^k)$ e quindi il p'-residuo di L è isomorfo ad un quoziente di $SL(n-1, p^k)$, in particolare è generato da (immagini di) sottogruppi radice.*

(Disegnare le matrici associate può aiutare a visualizzare la situazione). Vedremo che le condizioni V2 e V3 sono essenziali per provare l'esistenza di sottogruppi di H isomorfi a $SL(2, p)$

Ovviamente non possiamo aspettarci che questo accada in generale. Conviene quindi raffinare la scelta di $O_p(H)$ sostituendolo con un suo sottogruppo H-invariante ed abeliano elementare. La prima scelta cadrebbe ovviamente su $\Omega_1(Z(O_p(H)))$, che, però, ha il difetto di non soddisfare sempre la condizione V2. Per questo dobbiamo ulteriormente raffinare $\Omega_1(Z(O_p(H)))$ sostituendolo con un suo sottogruppo H-invariante che definiamo nella prossima sottosezione.

15.3.1 Moduli p-riducibili e quadratici

Sia p un numero primo, H un gruppo di caratteristica p ed $S \in Syl_p(H)$. Un sottogruppo abeliano elementare e H-invariante V di H si dice **p-riducibile**, se

$$O_p(Aut_H(V)) = \{1\}.$$

Si vede facilmente che H possiede tali sezioni, anzi, si può dimostrare che, ad esempio, H possiede un unico sottogruppo p-riducibile massimale (Esercizio 15.6.8). Per i nostri scopi, sar sufficiente provare che il sottogruppo

$$V_H := \Omega_1(Z(S))[\Omega_1(Z(S)), H], \tag{15.16}$$

è p-riducibile.

Lemma 15.3.1 *V_H è un sottogruppo p-riducibile e caratteristico in H.*

DIMOSTRAZIONE. Per i Teoremi di Sylow, V_H è caratteristico in H. Sia $S \in Syl_p(H)$. Poiché $O_p(H) \leq S$, e H ha caratteristica p,

$$\Omega_1(Z(S)) \leq C_H(S) \leq C_H(O_p(H)) = Z(O_p(H))$$

e, poiché $Z(O_p(H)) \trianglelefteq H$, segue che

$$V_H = \Omega_1(Z(S))[\Omega_1(Z(S)), H] \leq \Omega_1(Z(O_p(H)))$$

e, quindi, V_p è abeliano elementare. Infine, siano $C = C_H(V_p)$ e D la preimmagine in H di $O_p(H/C)$. Per il Teorema di Corrispondenza, $D \trianglelefteq H$, quindi $S \cap D \in Syl_p(D)$, in particolare $S \cap D$ supplementa $C \cap D$ in D. Inoltre, poiché V_H è generato da coniugati di $\Omega_1(Z(S))$, basta provare che

$$[D, \Omega_1(Z(S))] = \{1\}. \tag{15.17}$$

Poiché $CS \leq C_H(Z(S))$, segue che

$$D = (D \cap C)(S \cap D) \leq C_H(Z(S)). \tag{15.18}$$

da cui la tesi. ∎

Ora, il passo successivo è quello di trovare elementi di H che agiscono come trasvezioni su V_H.

Per l'Esercizio 11.7.2, un elemento a in $H \setminus C_H(V_H)$ induce una trasvezione su V_H se, posto $A := \langle a \rangle$ e $\overline{A} := AC_H(V_H)/C_H(V_H)$, le seguenti condizioni sono soddisfatte:

A1 $|A||C_{V_H}(A)| \geq |V_H|$ e

A2 $[V_H, A, A] = \{0\}$

Si noti che, se $|\overline{A}| = p$, A2 segue immediatamente da A1, perché, in tal caso, $V_H/C_{V_H}(A)$ ha ordine minore o uguale a p e quindi, poiché l'ordine del suo gruppo di automorfismi è coprimo con p, $V_H/C_{V_H}(A)$ è centralizzato da A.

Concentriamoci per il momento sulla condizione TF4. Vedremo che, se esistono sottogruppi di H che soddisfano TF4, ne esistono anche nell'insieme $\mathcal{A}(H)$ dei p-sottogruppi di H che sono abeliani elementari di ordine massimo.

Conviene però partire da una situazione un po' più generale: sia G un gruppo che agisce fedelmente su un p-gruppo abeliano elementare V (useremo la

notazione moltiplicativa anche per V). Diremo che V è **F-modulo** o **failure-of-factorization modulo** per G con **offensore** A, se esiste un p-sottogruppo abeliano elementare A di G tale che

$$|A||C_V(A)| \geq |V|.$$

Se V è un F-modulo per G con offensore A e $[V, A, A] = \{1\}$, diremo che V è un **modulo quadratico** per A ed A si dice **offensore quadratico**.

In generale, ma lo proveremo solo nel caso in cui G sia risolubile (Corollario 15.3.3), se V è un F-modulo per G, allora G contiene anche un offensore quadratico A di V (vedi [15, Proposition 26.8, p. 149]).

Un buon terreno dove trovare offensori è l'insieme $\mathcal{P}(G, V)$ dei sottogruppi abeliani elementari non identici A di G tali che, per ogni sottogruppo B di A,

$$|A||C_V(A)| \geq |B||C_V(B)|, \tag{15.19}$$

infatti,

Lemma 15.3.2 *Sia V uno spazio vettoriale di dimensione finita su un campo finito di caratteristica p e G un sottogruppo di $GL(V)$. Se $A \in \mathcal{P}(G, V)$, allora*

(a) $[V : C_V(A)] = p$;

(b) $|A||C_V(A)| \geq |V|$.

In particolare, ogni elemento di $\mathcal{P}(G, V)$ è un offensore.

Viceversa, se A è un offensore minimale (per inclusione), allora A è un elemento minimale di $\mathcal{P}(G, V)$.

DIMOSTRAZIONE. Prendendo $B = \{1\}$ nell'equazione 15.19 si ottiene (a) immediatamente e (b) segue dal Corollario 8.2.9. Viceversa, sia A un'offensore minimale e $B \leq A$. Se $B = \{1\}$ la disuguaglianza 15.19 è soddisfatta perché A è un'offensore e se $B \neq \{1\}$, è soddisfatta per la minimalità di A. ∎

Ad esempio, se A è un sottogruppo radice di V, allora A è un elemento di $\mathcal{P}(GL(V), V)$, perchè, per ogni sottogruppo proprio B di A, $C_V(B) = C_V(A)$ e quindi $|B||C_V(B)| < |A||C_V(A)| = |V|$. In particolare, nessun sottogruppo proprio di un sottogruppo radice è un elemento di $\mathcal{P}(GL(V), V)$ (e, se il campo di definizione di V non ha ordine primo, l'insieme di tali sottogruppi è non vuoto).

La condizione $[V, A, A] = \{1\}$ equivale a dire che A è contenuto nel radicale unipotente del sottogruppo parabolico massimale di $GL(V)$ che fissa lo spazio $[V, A]$. In particolare, se A è un'offensore quadratico minimale di V, ci si può aspettare che A sia un sottogruppo radice:

Lemma 15.3.3 *Con le ipotesi e le notazioni del Lemma 15.3.2, se G è risolubile, $O_p(G) = \{1\}$ e A è un'offensore minimale, allora $|A| = p$. In particolare A è generato da una trasvezione ed esiste $g \in G$ tale che $\langle A, A^g \rangle \cong SL(2, p)$ con $p \in \{2, 3\}$.*

DIMOSTRAZIONE. Poichè $O_p(G) = \{1\}$ e G è risolubile, $F^*(G) = F(G)$ ed ha ordine coprimo con p, quindi, per il Teorema di Fitting (Teorema 10.1.9),

$$[A, F(G)] \neq \{1\}. \tag{15.20}$$

Poiché A è abeliano, per il Lemma 11.6.14,

$$F(G) = \langle C_{F(G)}(B) | B <_{max} A \rangle \tag{15.21}$$

Poichè $C_{F(G)}(B)$ normalizza B e V, segue che, per ogni $B <_{max} A$,

$$[C_{F(G)}(B), C_V(B)] \leq C_V(B). \tag{15.22}$$

Ora, se, per assurdo, $|A| > p$, per ogni sottogruppo massimale B di A, la scelta di A implica che la disuguaglianza 15.19 deve essere stretta, il che è possibile solo se

$$C_V(B) = C_V(A) \text{ per ogni } B <_{max} A \tag{15.23}$$

e quindi, da (15.21) e (15.22), segue che $[F(G), C_V(A)] \leq C_V(A)$, cioè

$$[F(G), C_V(A), A] = \{1\}.$$

Poiché, ovviamente, anche $[C_V(A), A, F(G)] = \{1\}$, dal Lemma dei Tre Sottogruppi (Esercizio 6.3.9), segue che

$$[A, F(G), C_V(A)] = \{1\}.$$

Per il Corollario 10.2.15, con $P = A$ e $Q = [A, F(G)]$, segue che $[A, F(G)]$ centralizza V e quindi, poiché l'azione di G su V è fedele,

$$[A, F(G)] = \{1\},$$

in contraddizione con (15.20). Dunque

$$|A| = p$$

e, per quanto osservato all'inizio di questa sezione, questo implica che A è un sottogruppo radice. Poiché $O_p(G) = \{1\}$, per il Teorema di Baer-Suzuki (Lemma 9.2.6), esiste un coniugato A^g di A in G tale che $L := \langle A, A^g \rangle$ non sia un p-gruppo. Per il Lemma 11.2.10, $L \cong SL(2, p)$. Poiché $L \leq G$ e G è risolubile, per la Proposizione 11.3.2, $p \in \{2, 3\}$. ∎

Un sottoinsieme $\mathcal{P}$ di $\mathcal{P}(G, V)$ si dice **stabile**[3] se

ST1 per ogni $A \in \mathcal{P}$ ed ogni $g \in G$, $A^g \in \mathcal{P}$;

ST2 se $A \in \mathcal{P}$ e B è un sottogruppo non identico di A contenuto in $\mathcal{P}(G, V)$, allora anche $B \in \mathcal{P}$.

[3] Avvertenza, questa definizione è presa da [1]. Però il termine *stabile* in questo contesto è usato anche con un altro significato (vedi [15, Definition 25.3, p. 141])

Torniamo ora al caso in cui $G = Aut_H(V_H)$ e poniamo $V := V_H$. Come sopra, per ogni $L \leq H$, indichiamo con $\overline{L}$ l'immagine di L via la proiezione di H su $Aut_H(V)$, in particolare $\overline{H} = Aut_H(V)$. Sia $\mathcal{A}(H)$ l'insieme dei sottogruppi abeliani elementari di ordine massimo di H e sia

$$\mathcal{P}(H) := \{\overline{A} | A \in \mathcal{A} \text{ e } \overline{A} \neq \{1\}\}.$$

Lemma 15.3.4 *$\mathcal{P}(H)$ è un sottoinsieme stabile di $\mathcal{P}(\overline{H}, V)$.*

Dimostrazione. Per definizione $\mathcal{P}(H)$ soddisfa ST1. Proviamo che soddisfa ST2. Sia B^* un sottogruppo proprio di $\overline{A}$, C l'antiimagine di B^* in H e $B := C \cap A$. Poiché $C \leq AC_H(V)$, per la Legge Modulare di Dedekind otteniamo $C = BC_H(V)$. In particolare B è un sottogruppo proprio di A e

$$B^* = \overline{B} \text{ e } C_A(V) = C_B(V) \tag{15.24}$$

Poichè A e V sono p-sottogruppi abeliani elementari di H, anche

$$AC_V(A) \text{ e } BC_V(B) \text{ sono abeliani elementari,} \tag{15.25}$$

da cui, per la massimalità di $|A|$, segue che

$$A = AC_V(A) \text{ e } |A| \geq |BC_V(B)|. \tag{15.26}$$

In particolare

$$C_V(A) = A \cap V = B \cap V = C_V(B) \leq C_A(V) = C_B(V) \tag{15.27}$$

e

$$B \cap C_V(B) = B \cap V \tag{15.28}$$

Ora

$$\begin{aligned} |\overline{A}||C_V(\overline{A})| &= |\overline{A}||C_V(A)| = \frac{|A|}{|C_A(V)|}|C_V(A)| \overset{(15.27)}{=} \frac{|A|}{|C_B(V)|}|B \cap V| \\ &\overset{(15.26)}{>} \frac{|BC_V(B)|}{|C_B(V)|}|B \cap V| \overset{(15.28)}{=} \frac{|B||C_V(B)|}{|C_B(V)||B \cap V|}|B \cap V| \\ &= \frac{|B||C_V(B)|}{|C_B(V)|} = |\overline{B}||C_V(B)| = |\overline{B}||C_V(\overline{B})|. \end{aligned}$$

■

Corollario 15.3.5 *Se H è risolubile e $\mathcal{P}(H)$ è non vuoto, gli elementi minimali di $\mathcal{P}(H)$ inducono trasvezioni su V_H. In particolare $p \in \{2, 3\}$ e H contiene sezioni isomorfe a $SL(2, p)$.*

DIMOSTRAZIONE. Poiché $\mathcal{P}(H)$ è stabile, gli elementi minimali di $\mathcal{P}(H)$ sono offensori minimali e quindi la tesi segue dal Corollario 15.3.3. ∎

Come abbiamo anticipato, l'esistenza di offensori implica l'esistenza di offensori quadratici in generale, non solo, cioè, sotto l'ipotesi che il gruppo che agisce sia risolubile. Questa è una conseguenza del seguente teorema, noto come Teorema di Sostituzione di Thompson (in Inglese Thompson Replacement Theorem.

Teorema 15.3.6 [TEOREMA DI SOSTITUZIONE DI THOMPSON] *Sia P un p-gruppo e V un sottogruppo abeliano elementare normale di P. Sia A in $\mathcal{A}(P)$ tale che $[A, P] \not\leq A$. Allora esiste un elemento $A_1 \in \mathcal{A}(P)$, tale che $[V, A_1] \neq \{1\}$ e $[V, A_1, A_1] = \{1\}$.*

Per la dimostrazione si veda [14, 8.2.3, 8.2.5, p. 272, 273], oppure [22, 9.2.1, p. 206].

15.3.2 Il Sottogruppo di Thompson

Sia p un numero primo. Indichiamo con J_p il funtore che ad ogni gruppo finito p associa il sottogruppo $J_p(G)$ di G generato dai p-sottogruppi abeliani elementari di ordine massimo. $J_p(G)$ si dice **sottogruppo di Thompson** di G (relativo al primo p). Se G è un gruppo di caratteristica locale p (in particolare se G è un p-gruppo, scriveremo semplicemente $J(G)$ al posto di $J_p(G)$.

Le proprietà fondamentali di J_p (e di verifica immediata) sono:

Lemma 15.3.7 *Sia G un gruppo finito, allora*

J1 *$J_p(G)$ sia caratteristico in G;*

J2 *se L è un sottogruppo di G contenente un elemento di $\mathcal{A}(G)$, allora $J_p(L) = J_p(G)$;*

J3 *se $P \in Syl_p(G)$, $J_p(G) = J_p(P)[J_p(P), G]$.*

Possiamo ora enunciare e dimostrare il risultato centrale di questa sezione:

Teorema 15.3.8 FATTORIZZAZIONE DI THOMPSON *Sia p un numero primo, H un gruppo risolubile di caratteristica p e $S \in Syl_p(H)$.*

(a) Se $J(S)$ centralizza $\Omega_1(Z(S))$, allora $H = N_H(J(S))C_H(\Omega_1(Z(S)))$ (in questo caso H ammette la Fattorizzazione di Thompson), oppure

(b) Se $J(S)$ non centralizza $\Omega_1(Z(S))$, allora $p \in 2, 3$ e $Aut_{J(H)}(\Omega_1(Z(S))$ contiene un sottogruppo isomorfo a $SL_2(p)$ (la Fattorizzazione di Thompson fallisce).

DIMOSTRAZIONE. Sia $\overline{J} := Aut_{J(G)}(V_H)$. Osserviamo che $J(S)$ centralizza V_H se e solo se V_H non è un F-modulo per $Aut_{J(G)}(V_H)$. Per il Lemma 15.3.4 V_H non è un F-modulo per $J(S)$ se e solo se $\mathcal{P}(H) = \emptyset$. Per i Teoremi di Sylow, $S^* := S \cap C_H(V_H)$ è un p-sottogruppo di Sylow di $C_H(V_H)$ e, per l'Argomento di Frattini,

$$H = N_H(S^*)C_H(V_H). \tag{15.29}$$

Poichè $\Omega_1(Z(S)) \leq V_H$, segue che

$$C_H(V_H) \leq C_H(\Omega_1(Z(S))). \tag{15.30}$$

Ora, se V_H non è un F-modulo per $\overline{J}$, $\mathcal{P}(H) = \emptyset$, quindi $J(H)$ centralizza $V_(H)$ e dunque, poiché $J(S) \leq J(H)$,

$$J(S) \leq C_H(V_H) \trianglelefteq H.$$

Per J2 segue che

$$J(S) = J(S^*),$$

in particolare $J(S)$ è un sottogruppo caratteristico di $J(S^*)$ e quindi

$$N_H(S^*) \leq N_H(J(S)). \tag{15.31}$$

Da (15.29), (15.30) e (15.31) segue allora che

$$H = N_H(J(S))C_H(\Omega_1(Z(S))).$$

Se invece V_H è un F-modulo per $J(S)$, per il Lemma 15.3.4, $\mathcal{P}(H) \neq \emptyset$ e la tesi segue per il Corollario15.3.3. ∎

Chiudiamo questa sezione osservando che George Glauberman ha dato una precisa descrizione di $J(H)$ e della sua azione su V_H nel caso in cui H sia risolubile e ci sia fallimento della fattorizzazione (per la dimostrazione si veda [1, 32.3, p. 163] oppure [22, 9.3.7, p.219]):

Teorema 15.3.9 (TEOREMA DI GLAUBERMAN SUL FALLIMENTO DELLA FATTORIZZAZIONE NEI GRUPPI RISOLUBILI) *Con le notazioni del Teorema 15.3.8, se la fattorizzazione di Thompson fallisce, allora $p \in \{2, 3\}$ ed esistono un intero positivo n e dei sottogruppi $J_1, \ldots, J_n$, tali che*

1. $J(H) = J_1 \times \ldots \times J_n$;
2. $V_H = C_{V_H)}(J(H) \times [V_H, J(H)]$;
3. $[V_H, J(H)] = [V_H, J_1] \times [V_H, J_2] \times \ldots \times [V_H, J_n]$;
4. *per ogni $i \in \{1, \ldots, n\}$, $[V_H, J_i]$ ha ordine p^2 e J_i è isomorfo a $SL(2, p)$, centralizza $[V_H, J_j]$, se $i \neq j$, ed agisce per coniugio come $SL([V_H, J_i])$ su $[V_H, J_i]$.*
5. *H permuta per coniugio i sottogruppi $J_i[V_H, J_i]$.*

15.4 Il Criterio di p-nilpotenza di Thompson

Teorema 15.4.1 CRITERIO DI p-NILPOTENZA DI THOMPSON *Sia G un gruppo finito, p un numero primo dispari e $S \in Syl_p(G)$. Allora G è p-nilpotente se e solo se $N_G(J(S))$ e $C_G(\Omega_1(Z(S)))$ sono p nilpotenti.*

DIMOSTRAZIONE. Supponiamo per assurdo che la tesi sia falsa e sia G un controesempio di ordine minimo ed S un p-sottogruppo di Sylow di G. Poiché le ipotesi sono soddisfatte da ogni sottogruppo di G contenente S, per la scelta minimale di G

$$\textit{ogni sottogruppo proprio di } G \textit{ contenente } S \textit{ è } p\textit{-nilpotente.} \tag{15.32}$$

Inoltre, se N è un sottogruppo normale di G di ordine coprimo con p, il gruppo quoziente G/N soddisfa ancora le ipotesi, quindi è p-nilpotente. Ma allora, per il Lemma 15.2.17(b), G è nilpotente, contro la scelta di G. Quindi

$$O_{p'}(G) = \{1\}. \tag{15.33}$$

Studiamo $F^*(G)$, vogliamo provare che

$$G \textit{ ha caratteristica } p. \tag{15.34}$$

Per il Criterio di p-nilpotenza di Frobenius (Teorema 15.2.19), esistono sottogruppi p-locali che non sono p-nilpotenti. Tra questi sia H tale che, posto $Q := S \cap H$, Q abbia ordine massimo. Per i Teoremi di Sylow,

$$Q \in Syl_p(H) \tag{15.35}$$

Proviamo che

$$Q = S. \tag{15.36}$$

Se $Q < S$, allora $Q < N_S(Q)$ e quindi, se C è per un sottogruppo caratteristico di Q,

$$Q < N_S(Q) \leq N_S(C) = S \cap N_G(C). \tag{15.37}$$

Per la scelta massimale di Q, $N_G(C)$ è p-nilpotente. Poiché $N_H(C) \leq N_G(C)$, anche $N_H(C)$ è p-nilpotente. In particolare $N_H(J(Q))$ e $N_H(\Omega_1(Z(Q))$ (e quindi anche $C_H(\Omega_1(Z(Q)))$ sono p-nilpotenti. Se $H < G$, per la minimalità di G, H è p-nilpotente, contro la scelta di H. Quindi $H = G$, e dunque $Q = S$ per (15.35) e G è p-locale, in particolare

$$O_p(G) \neq \{1\}. \tag{15.38}$$

Per ogni sottogruppo H di G sia $\overline{H} := HO_p(G)/O_p(G)$. Per l'Esercizio 10.3.1,

$$O_p(\overline{G}) = \{1\}. \tag{15.39}$$

In particolare $N_{\overline{G}}(J(\overline{S}))$ e $C_{\overline{G}}(\Omega_1(Z(\overline{S}))$ sono sottogruppi propri di $\overline{G}$ contenenti $\overline{S}$. Quindi anche le loro antiimagini in G sono sottogruppi propri di G

contenenti S e quindi, per 15.32, sono p-nilpotenti. Per il Lemma 15.2.16(a), segue che $N_{\overline{G}}(J(\overline{S}))$ e $C_{\overline{G}}(\Omega_1(Z(\overline{S}))$ sono p-nilpotenti, quindi, per 15.38 e la scelta minimale di G

$$\overline{G} \text{ è } p\text{-nilpotente .} \tag{15.40}$$

Per il Lemma 15.2.16(a), i sottogruppo di $\overline{G}$ sono p-nilpotenti. Quindi, poiché $E(\overline{G})$ è perfetto,

$$\overline{E(G)} \leq E(\overline{G}) \leq O_{p'}(\overline{G}),$$

in particolare $O_p(G) \cap E(G)$ è un p-sottogruppo di Sylow di $E(G)$. Per l'Esercizio 10.3.2 e (15.33),

$$E(G) \leq O_{p'}(G) = \{1\}, \tag{15.41}$$

il che, con (15.33), prova (15.34). Sia $H \in \{N_G(J(S)), C_G(\Omega_1(Z(S)))\}$. Proviamo che

$$H = S.$$

Infatti, se K è un p-complemento di S in H, poiché K e $O_p(G)$ sono sottogruppi normali di H,

$$[K, O_p(G)] \leq K \cap O_p(G) = \{1\}.$$

e quindi, per (15.34) ed il Teorema di Bender-Fitting (Teorema 10.1.15,

$$K \leq C_G(O_p(G) \leq O_p(G),$$

quindi, poiché ha ordine coprimo con p, $K = \{1\}$. Ne segue che

$$N_G(J(S))C_G(\Omega_1(Z(S))) = S. \tag{15.42}$$

Sia ora $r \in \pi(G) \setminus p.$ e sia $R \in Syl_r(G)$, allora $R \leq O_{p,p'}(G)$. Per l'argomento di Frattini,

$$G = N_G(Z(R))O_{p,p'}(G)$$

quindi $N_G(Z(R))O_p(G)$ contiene un p-sottogruppo di Sylow di G che, a meno di scambiare R con un suo coniugato, possiamo supporre essere S. Quindi S normalizza $Z(R)O_p(G)$. Sia

$$G^* := Z(R)P.$$

Se, per assurdo $G_0 \neq G$, allora, per (15.32), G_0 sarebbe p-nilpotente e quindi

$$Z(R) = O_{p'}(G_0) \trianglelefteq G_0$$

e quindi, per (15.34) ed il Teorema di Bender-Fitting (Teorema 10.1.15,

$$Z(R) \leq C_G(O_p(G) \leq O_p(G),$$

Poiché $Z(R)$ ha ordine coprimo con p, segue che $Z(R) = \{1\}$ contro l'ipotesi che $r \in \pi(G)$ e $R \in Syl_r(G)$. Dunque

$$R = Z(R) \text{ e } G = PR \text{ in particolare } G \text{ è risolubile .}$$

Per il Teorema 15.3.8, e (15.42),

$$G = N_G(J(S))C_G(\Omega_1(Z(S))) = S,$$

la contraddizione finale. ∎

15.5 Azione senza punti fissi

Nella sua tesi di dottorato, John Thompson dimostrò il seguente risultato, risolvendo un problema aperto da molti anni:

Teorema 15.5.1 (Teorema di Thompson sulla nilpotenza del nucleo di Frobenius) *Sia G un gruppo finito che ammette un automorfismo di ordine primo senza punti fissi. Allora G è nilpotente*

Vogliamo chiudere questo capitolo (e probabilmente questi appunti) con la dimostrazione di questo Teorema, perché, oltre alla sua importanza, è un bell'esempio di come usare le tecniche finora sviluppate.

15.5.1 Gruppi di Frobenius

Sia H un gruppo finito, diremo che H è un **gruppo di Frobenius**[4] se possiede due sottogruppi propri A e B tali che

1. B è normale in H,
2. $H = AB$ e $A \cap B = \{1\}$
3. per ogni $a \in A \setminus \{1\}$, $C_B(a) = \{1\}$

Se A e B sono come sopra A si dice **complemento di Frobenius** e B si dice **nucleo di Frobenius**. Osserviamo che ogni elemento di ordine primo del complemento di Frobenius agisce senza punti fissi sul nucleo.

Lemma 15.5.2 *Se H è un gruppo di Frobenius con complemento A e nucleo B, allora $(|A|, |B|) = 1$.*

Dimostrazione. Se r è un numero primo che divide $|A|$ e a è un r-elemento non identico di A, allora, per l'Argomento di Frattini, esiste un r-sottogruppo di Sylow R di B tale che R sia a-invariante. Se per assurdo $R \neq \{1\}$, per il Corollario 8.2.9 $\{1\} \neq C_R(a) \leq C_B(a) = \{1\}$, una contraddizione. ∎

Lemma 15.5.3 *Se H è un gruppo di Frobenius con complemento A e nucleo B, allora, per ogni $b \in B \setminus \{1\}$, $A \cap A^b = \{1\}$. In particolare $N_H(A) = A$.*

Dimostrazione. Sia $b \in B$ e $a \in A \cap A^b \setminus \{1\}$. Allora $[a, b] \in [[A, B] \leq B$, perché B è normale in H. D'altra parte, peró, $[a, b] = a^{-1}a^b \in A^b$ e quindi $[a, b] \in A^b \cap B = \{1\}$, da cui $b \in C_B(A) = \{1\}$. ∎

[4] La definizione di gruppo di Frobenius che viene data normalmente (vedi, ad esempio [22, p. 72,73] è diversa da quella data in questi appunti, si può però dimostrare che le definizioni sono equivalenti usando la teoria dei caratteri (vedi [27, Theorem 2.6, p. 280] oppure [20, Theorem 7.2, p. 100]). Una dimostrazione di questa equivalenza senza uso dei caratteri è un problema aperto da molti decenni.

Sia H un gruppo. Una **partizione** di H è un insieme finito e non vuoto $\mathcal{P}$ di sottogruppi di H tale che

$$H \setminus \{1\} = \dot{\bigcup}_{x \in \mathcal{P}} (P \setminus \{1\}). \tag{15.43}$$

Lemma 15.5.4 *Se H è un gruppo di Frobenius con complemento A e nucleo B, allora l'insieme*

$$\mathcal{P}(H) := \{A^b | b \in B\} \cup \{B\}$$

è una partizione di H.

Dimostrazione. Sia

$$H^* := \bigcup_{X \in \mathcal{P}} X \setminus \{1\}.$$

Per i Lemmi 15.5.2 e 15.5.3 H^* è unione disgiunta dei sottoinsiemi $X \setminus \{1\}$ al variare di $X \in \mathcal{P}(H)$. Chiaramente $H^* \subseteq H \setminus \{1\}$. Proviamo che $H^* = H \setminus \{1\}$ contando gli elementi di H^*: ciascun coniugato di A contribuisce con $|A| = 1$ elementi. Per il Lemma 15.5.3 ed il Corollario 8.2.7, ci sono esattamente $|H : A| = |B|$ coniugati di A in $\mathcal{P}$. Quindi i coniugati di $A \setminus \{1\}$ contribuiscono con $|B|(|A| - 1) = |B||A| - |B| = |H| - |B|$ elementi e quindi, aggiungendo i $|B| - 1$ elementi di $B \setminus \{1\}$, si ottiene $|H^*| = |H| - 1 = |H \setminus \{1\}$, da cui la tesi. ∎

Lemma 15.5.5 *(vedi [22, 8.3.1, p. 170] Sia $\mathcal{B}$ una partizione di un gruppo finito H e supponiamo che H agisca su un gruppo abeliano finito non identico V tale che $(|V|, |\mathcal{B}|-1) = 1$. Allora esiste un elemento B di $\mathcal{B}$ tale che $C_V(B) \neq \{1\}$*

Dimostrazione. Poiché V è abeliano, dato un elemento v di V ed un sottogruppo B di H, è facile costruire un elemento in $C_V(B)$: basta prendere il prodotto v_B degli elementi della B-orbita di v:

$$v_B := \prod_{b \in B} v^b = v(\prod_{b \in B \setminus \{1\}} v^b).$$

Supponiamo ora, per assurdo, che $C_V(B) = 1$ per ogni $B \in \mathcal{B}$, in particolare $v_B = 1$ per ogni $B \in \mathcal{B}$ e $v_H = \{1\}$, perchè ciò che centralizza tutto H deve centralizzare anche tutti i suoi sottogruppi. Posto, $k := |\mathcal{B}| - 1$, poiché $\mathcal{B}$ è una partizione di H segue che, per ogni $v \in V$,

$$v^{-k} = v^{-k}(\prod_{B \in \mathcal{B}} v_B) = v_H = 1. \tag{15.44}$$

Ma, per ipotesi, $(|V|, k) = 1$ e quindi (15.44) implica che $v = 1$ per ogni $v \in V$, contro la scelta di V. ∎

Corollario 15.5.6 *Sia H un gruppo di Frobenius con complemento di Frobenius A e nucleo di Frobenius B che agisce su un gruppo abeliano V di ordine coprimo con H. Se $C_V(B) = \{1\}$, allora $C_V(A) \neq \{1\}$.*

DIMOSTRAZIONE. Sia $\mathcal{P}(H)$ come nel Lemma 15.5.4. Allora $|\mathcal{P}(H)| - 1 = |B|$ e B è coprimo con $|V|$. Poichè $C_V(B) = \{1\}$, per Il Lemma 15.5.5, esiste $b \in B$ tale $C_V(A^b) \neq \{1\}$ e, poichè V è H-invariante, segue che anche $C_V(A) \neq \{1\}$. ∎

15.5.2 Dimostrazione del Teorema di Thompson

In questa sottosezione r è un numero primo, G è un gruppo finito, α è un automorfismo di G di ordine r e tale che $C_G(\alpha) = \{1\}$. Sia $A := \langle\alpha\rangle$, ovviamente $C_G(\alpha) = C_G(A) = C_G(\beta)$ per ogni $\beta \in A \setminus \{1\}$. Incominciamo con una serie di riduzioni elementari.

Lemma 15.5.7 *α agisce senza punti fissi su ogni sottogruppo A-invariante di G.*

DIMOSTRAZIONE. Questo è ovvio. ∎

Lemma 15.5.8 *$|G|$ è coprimo con r*

DIMOSTRAZIONE. Per l'Argomento di Frattini, G possiede r-sottogruppi di Sylow α-invarianti. Sia S uno di questi. Se, per assurdo, $S \neq \{1\}$, per il Corollariopfondamentale1 esisterebbero punti fissi per α in S, ma questo contraddice il Lemma 15.5.7. Quindi $S = \{1\}$ e, poiché $S \in Syl_r(G)$, questo implica che r non divide $|G|$. ∎

Lemma 15.5.9 *Se V è un sottogruppo normale ed A-invariante di G α agisce senza punti fissi su G/V.*

DIMOSTRAZIONE. Questo segue dal Teorema del Sollevamento dei Centralizzanti (Teorema 10.2.2). ∎

Lemma 15.5.10 *Per ogni $\beta \in A \setminus \{1\}$, l'applicazione $g \mapsto [g, \beta]$ è una permutazione di G.*

DIMOSTRAZIONE. Basta provare che l'applicazione è iniettiva. Se $g, h \in G$ e $[g, \beta] = [h, \beta]$ allora $g^{-1}\beta^{-1}g = h^{-1}\beta^{-1}h$, da cui si ottiene $\beta hg^{-1}\beta^{-1} = hg{-}1$. Ma allora $hg{-}1 \in C_G(\beta) = \{1\}$, da cui $h = g$ ∎

Lemma 15.5.11 *Se $r = 2$, G è abeliano.*

DIMOSTRAZIONE. Per il Lemma 15.5.10, $G = [G, \alpha]$ e α inverte $[g, \alpha]$ per ogni $g \in G$. Ma allora l'inversione è un automorfismo di G e questo può succedere solo se G è abeliano. ∎

Siamo ora pronti per dimostrare il Teorema 15.5.1.

DIMOSTRAZIONE. Sia ora G un controesempio di ordine minimo al Teorema 15.5.1. Come al solito incominciamo a studiare $F^*(G)$. Proviamo che

$$F(G) = \{1\}. \tag{15.45}$$

Supponiamo, per assurdo, che $F(G) \neq \{1\}$, sia q un divisore primo di $F(H)$ e $V := \Omega_1(Z(O_q(G)))$. Allora V è un q-sottogruppo abeliano elementare ed A-invariante di G. Per la scelta minimale di G ed il Lemma 15.5.9, G/V è nilpotente e quindi,

$$\textit{per ogni primo } p \textit{ e per ogni } P \in Syl_r(G),\ PV \textit{ è normale in } G. \tag{15.46}$$

In particolare, prendendo $p = q$, otteniamo che

$$\textit{per ogni primo } q \textit{ che divide } F(G),\ \textit{e per ogni } T \in Syl_q(G),\ T \textit{ è normale in } G. \tag{15.47}$$

Poiché G non è nilpotente, esiste un primo p ed un un p-sottogruppo di Sylow P di G che è A-invariante e non normale in G. Proviamo che

$$P \textit{ agisce fedelmente per coniugio su } V. \tag{15.48}$$

Infatti $C_P(V)$ è un p-sottogruppo di PV centralizzato da V e normalizzato da P, quindi è normale in PV e dunque contenuto in $O_p(RV)$. D'altra parte, per (15.46) $PV \trianglelefteq G$, quindi $O_p(PV) \leq O_p(G)$, che, per (15.47) coincide con $\{1\}$, da cui la tesi. In particolare anche $Z(P)$ agisce fedelmente su Q. Per il Lemma 15.5.6, con $Z(P) = B$, segue che $C_{(Z(P)}(A) \neq \{1\}$, una contraddizione che prova (15.45). Da (15.45), la scelta minimale di G ed il Lemma 15.5.7, segue che

$$G \textit{ non possiede sottogruppi normali propri ed } A\textit{-invarianti.} \tag{15.49}$$

Poiché G non è nilpotente, esiste un primo dispari p che divide $|G|$. Per L'argomento di Frattini, esiste un p-sottogruppo di Sylow S di G. In particolare $J(S)$ e $\Omega_1(Z(S))$ sono p-sottogruppi non identici ed A-invarianti di G, quindi, per (15.45), $N_G(J(S))$ e $C_G(\Omega_1(Z(S)))$ sono sottogruppi propri e dunque, per il Lemma 15.5.7, $N_G(J(S))$ e $C_G(\Omega_1(Z(S)))$ sono nilpotenti (in particolare p-nilpotenti). Per il Criterio di p-nilpotenza di Thompson, (Teorema 15.4.1), G è p-nilpotente. Ora, però, se K è un complemento normale di S in G, K è un sottogruppo proprio e caratteristico in G (in particolare A-invariante), il che contraddice (15.49). ∎

Corollario 15.5.12 *Il nucleo di un gruppo di Frobenius è nilpotente*

DIMOSTRAZIONE. Segue immediatamente dal Teorema 15.5.1, perché ogni elemento di ordine primo del complemento di Frobenius agisce senza punti fissi. ■

15.6 Esercizi

Esercizio 15.6.1 *Sia G un gruppo finito e π un insieme di numeri primi.*

1. *Si provi che se H e K sono sottogruppi normali di G tali che G/H e G/K sono π-gruppi, allora $H \cap K$ è ancora un sottogruppo normale di G tale che il quoziente sia un π-gruppo;*
2. *si deduca che esiste un sottogruppo normale minimo $O^\pi(G)$ tale che il quoziente $G/O^\pi(G)$ sia un π-gruppo;*
3. *si provi che $O^\pi(G)$ è caratteristico in G;*
4. *si provi che $O^\pi(G)$ è il sottogruppo di G generato dai p-sottogruppi di Sylow di G per i primi p che non sono contenuti in π;*
5. *si provi che $O^\pi(G)[G,G]$ è il minimo sottogruppo normale di G tale che il gruppo quoziente $G/O^\pi(G)[G,G]$ sia un π-sottogruppo abeliano;*
6. *si provi che se H è un π-sottogruppo di hall di G, allora $G = HO^\pi(G)$.*

Il seguente esercizio permette una definizione alternativa di sottogruppo completamente normalizzato che quella che si usa nei fusion systems, dove non esiste un gruppo ambiente G.

Esercizio 15.6.2 *Sia S un p-sottogruppo di Sylow di un gruppo finito G e sia A un sottoinsieme non vuoto di S. Si provi che A è completamente normalizzato in S se e solo se $|N_S(A)| \geq |N_S(B)|$ per ogni sottoinsieme B di S fuso in G con A.*

Sia H un sottogruppo di un gruppo G e U un sottoinsieme non vuoto di H. U si dice **debolmente chiuso** in H rispetto a G se U è l'unico G-coniugato di U contenuto in H.

Esercizio 15.6.3 *Sia p un primo, G un gruppo e $P \in Syl_p(G)$. sia W un sottogruppo di P debolmente chiuso rispetto a G. Si provi che $N_G(W)$ controlla la fusione di P in G in $C_G(W)$.*

Esercizio 15.6.4 *Sia G un gruppo finito e sia p il più piccolo numero primo che divide l'ordine di G. Si provi che se un p-sottogruppo di Sylow di G è ciclico, allora G è p-nilpotente*

Esercizio 15.6.5 *Sia G un gruppo finito. Si provi che se tutti i sottogruppi di Sylow di G sono ciclici, allora G è risolubile.*

Esercizio 15.6.6 *Si provi che, per ogni numero primo r, il complemento di Frobenius di un gruppo di Frobenius non contiene r-sottogruppi abeliani elementari di ordine r^2.*

Si può dimostrare che, se r è un numero primo dispari, un r-gruppo finito privo di sottogruppi abeliani elementari di ordine r^2 è ciclico. Dagli esercizi 15.6.5 e 15.6.6, segue quindi che, se il complemento di Frobenius di un gruppo di Frobenius H è di ordine dispari, allora il complemento (e quindi, per il Corollario 15.5.12, tutto H) è risolubile.

Se $r = 2$ i quaternioni sono un controesempio alla tesi dell'esercizio 15.6.6, ma si può dimostrare facilmente che gli unici 2-gruppi finiti non ciclici privi di sottogruppi abeliani elementari di ordine p^2 sono i quaternioni ed i quaternioni generalizzati (vedi [1, Exercise 8.4, p. 115]).

Esercizio 15.6.7 *Si provi che, per qualsiasi p-gruppo Q, esiste un gruppo G con $F^*(G) \cong Q$ e $G > F^*$, e per ogni gruppo finito A con $O_p(A) = \{1\}$ esiste un gruppo finito G di caratteristica p con $A \cong G/O_p(G)$*

Esercizio 15.6.8 *Sia G un gruppo di caratteristica p e sia $\mathcal{R}_p$ l'insieme dei p sottogruppi abeliani elementari normali R di G tali che $O_p(G/C_G(R)) = \{1\}$ e sia*

$$R_p(G) := \langle R | R \in \mathcal{R}_p \rangle.$$

Si provi che

a $R_p(G)$ è un sottogruppo caratteristico di G,

b $R_p(G)$ è abeliano elementare,

c $R_p(G)$ è p-riducibile,

$R_p(G)$ si dice **cuore p-riducibile** *di G. È il massimo sottogruppo p-riducibile di G.*

Esercizio 15.6.9 *Sia G un sottogruppo parabolico di $PSL(n, p^k)$. Si determini $V_p(G)$ suggerimento: si incominci con i parabolici massimali.*

Esercizio 15.6.10 *Sia p un numero primo, V uno spazio vettoriale su un campo finito K di caratteristica p e sia H un sottogruppo parabolico massimale di $GL(V)$. Si determinino gli elementi di $\mathcal{P}(H, V)$ che sono quadratici su V*

Appendice A

Strutture e loro automorfismi

Il concetto di struttura o, quello equivalente, di categoria (che viene usato in [1], permette di trattare in modo unificato molti aspetti delle rappresentazioni dei gruppi su insiemi, gruppi, spazi vettoriali, grafi, geometrie e reticoli.

Diamo qui una versione semplificata del concetto di struttura algebrico-relazionale: a differenza della definizione di struttura comunemente usata in teoria dei modelli, quella che diamo ha lo svantaggio di non permettere di definire gli omomorfismi tra strutture diverse, ma solo gli endomorfismi di una struttura data. Quella che diamo, comunque, è sufficiente per trattare le azioni di gruppi ed ha il vantaggio di essere più trasparente.

A.1 Strutture algebrico-relazionali

Sia X un insieme ed n un'intero positivo, ricordiamo che un'**operazione** (risp. **relazione**) **n-aria**, su X è un'applicazione $f\colon X^n \to X$ (risp. un sottoinsieme r di X^n). L'intero n si dice **tipo** dell'operazione (risp. relazione).

Esempi:

1. L'addizione negli interi è un'operazione di tipo 2.
2. In uno spazio vettoriale su un campo K, ogni elemento k di K è un'operazione di tipo 1.
3. In un grafo la relazione di adiacenza è una relazione binaria sull'insieme dei vertici.

Una **struttura algebrico-relazionale** $\mathcal{X}$ è una quadrupla (X, F, R, C) dove

1. X è un insieme, detto il **supporto** di $\mathcal{X}$;
2. F è un insieme di operazioni su X;

3. R è un insieme di relazioni su X;

4. C è un sottoinsieme di X (le **costanti**).

Esempi

1. Un insieme X è una struttura del tipo $(X, \emptyset, \emptyset, \emptyset)$.

2. Un gruppo è una struttura $(G, \{\cdot\}, \emptyset, \emptyset)$, dove G è un insieme non vuoto $\cdot$ è un'operazione binaria.

3. Un anello con unità è una struttura $(R, \{+, \cdot\}, \emptyset, \{1\})$, dove R è un insieme non vuoto $+$ e $\cdot$ sono operazioni binarie e 1 è un elemento di R (l'identità moltiplicativa).

4. Uno spazio vettoriale $\mathcal{V}$ su un campo K è una struttura

$$(V, \{+\} \cup \{f_k | k \in K\}, \emptyset, \emptyset)$$

dove V è un insieme non vuoto $+$ è un'operazione binaria e, per ogni $k \in K$, f_k è un'operazione 1-aria.

Quando non è necessario specificare gli insiemi F, R, C si indica una struttura $\mathcal{X} = (X, F, R, C)$ semplicemente con X.

A.2 Endomorfismi ed automorfismi di strutture

Diamo ora una definizione generale di endomorfismo ed automorfismo per strutture algebrico-relazionali, nei casi particolari che a noi interessano (insiemi, gruppi, grafi, spazi vettoriali) mostreremo che gli endomorfismi e gli automorfismi di strutture sono esattamente quelli soliti.

Un **endomorfismo** ψ di una struttura $\mathcal{X}$ è una applicazione di X in sè che conserva le operazioni e le relazioni, cioè tale che per ogni intero positivo n, per ogni $f \in F$, per ogni $r \in R$ di tipo n ed ogni $x_1, \ldots, x_n \in X$ sia

1. $((x_1, \ldots, x_n)^f)^\psi = (x_1^\psi, \ldots, x_n^\psi)^f$,

2. se $(x_1, \ldots, x_n) \in r$ allora $(x_1^\psi, \ldots, x_n^\psi) \in r$.

3. $c^\psi = c$ per ogni $c \in C$.

Un endomorfismo ψ di $\mathcal{X}$ si dice **automorfismo** se ψ è una permutazione di X tale che

$$(x_1, \ldots, x_n) \in r \text{ se e solo se } (x_1^\psi, \ldots, x_n^\psi) \in r.$$

Si osservi che se l'insieme R delle relazioni è non vuoto esistono degli endomorfismi biiettivi che non sono automorfismi.

Esempi

1. Se X è un insieme non vuoto, ogni applicazione di X in sè è un endomorfismo ed ogni permutazione di X è un automorfismo.

2. Se $\mathcal{X} = (X, \leq)$ è un insieme parzialmente ordinato, un automorfismo di $\mathcal{X}$ è una permutazione ϕ di X tale che per ogni $a, b \in X$ sia $a \leq b$ se e solo se $a^\phi \leq b^\phi$.

3. Se $\mathcal{X}$ è uno spazio vettoriale sul campo K, un endomorfismo di $\mathcal{X}$ è una applicazione ϕ di X in sè tale che, per ogni $a, b \in X$ e per ogni $k \in K$, risulti $(a+b)^\phi = a^\phi + b^\phi$ e $(ka)^\phi = k(a^\phi)$.

A.3 Il gruppo degli automorfismi di una struttura

Si vede facilmente che l'insieme degli automorfismi di una struttura $\mathcal{X}$ è un gruppo rispetto alla composizione di applicazioni. Infatti la composizione di applicazioni è associativa, la mappa identica è l'elemeno neutro e l'applicazione inversa di un automorfismo è ancora un automorfismo. Tale gruppo si chiama **gruppo degli automorfismi** della struttura $\mathcal{X}$ e si indica con $Aut(\mathcal{X})$. Osserviamo che diverse strutture algebriche possono avere lo stesso supporto: ad esempio lo spazio vettoriale $(V, +, K)$ sul campo K, il gruppo abeliano $(V, +)$ e l'insieme V sono tre strutture algebriche distinte aventi tutte l'insieme V come supporto. Si vede immediatamente che i gruppi di automorfismi di queste strutture sono sottogruppi del gruppo degli automorfismi del supporto. Nel nostro caso $Aut(V, +, K)$ e $Aut(V, +)$ sono sottogruppi di $Aut(V)$. Inoltre, poichè ogni automorfismo dello spazio vettoriale $(V, +, K)$ è anche un automorfismo del gruppo abeliano $(V, +)$, risulta

$$Aut(V, +, K) \leq Aut(V, +)$$

cioè più *ricca* è una struttura, più *piccolo* è il suo gruppo di automorfismi.

Nelle prossime due sottosezioni calcoleremo i gruppi degli automorfismi rispettivamente di un gruppo ciclico e di un gruppo abeliano elementare. Sono due esempi importanti perché, come si vedrà in seguito nel capitolo delle azioni di un gruppo su un gruppo, essi compaiono costantemente nello studio dell'architettura di un gruppo finito.

A.3.1 Il gruppo degli automorfismi di un gruppo ciclico

Se G è un gruppo abeliano l'insieme degli endomorfismi di G è dotato in modo naturale di una struttura di anello: se σ e τ sono endomorfismi di G, la loro somma $\sigma + \tau$ è definita per ogni $g \in G$ da

$$g^{\sigma+\tau} = g^\sigma g^\tau,$$

mentre il loro prodotto è la composizione di applicazioni. Questo anello si chiama **anello degli endomorfismi** di G e si indica con $End(G)$. Il gruppo degli

automorfismi di G coincide con il gruppo degli elementi invertibili di $End(G)$. In generale non è facile calcolare gli automorfismi di un gruppo. Nel caso di un gruppo abeliano G è più facile determinare $End(G)$ e quindi i suoi elementi invertibili che determinare direttamente gli automorfismi. Come esempio calcoliamo il gruppo degli automorfismi di un gruppo ciclico e di un p-gruppo abeliano elementare.

Sia $G = \langle g \rangle$ un gruppo ciclico generato dall'elemento g. Allora ogni elemento di G è del tipo g^k con $k \in \mathbf{Z}$. Per ogni intero n sia σ_n l'applicazione da G in sè definita da

$$\sigma_n \colon g^k \mapsto g^{kn}$$

per ogni $g^k \in G$. Si vede facilmente che σ_n è un omomorfismo da G in se stesso. Possiamo quindi definire una applicazione

$$\begin{array}{rccc} \sigma\colon & \mathbf{Z} & \to & End(G) \\ & n & \mapsto & \sigma_n. \end{array}$$

È facile verificare che σ è un omomorfismo di anelli ed è suriettiva infatti se $\tau \in End(G)$, allora $g^\tau = g^{n^*}$ per un opportuno intero n^*. Inoltre, per ogni $g^k \in G$ risulta $(g^k)^\tau = (g^\tau)^k = g^{n^* k} = (g^k)^{n^*}$, cioè $\tau = (n^*)^\sigma$. Sia ora $m \in \ker(\sigma)$ Allora $g^m = 1$ e quindi, se $|G|$ è finito, m è un multiplo di $|G|$, altrimenti $m = 0$. Per il primo teorema di omomorfismo per anelli risulta:

Proposizione A.3.1 *Sia G un gruppo ciclico. Se G è infinito*

$$End(G) \cong \mathbf{Z},$$

se G è finito

$$End(G) \cong \mathbf{Z}_{|G|}.$$

Si noti che $End(G)$ è commutativo essendo isomorfo ad un quoziente dell'anello $\mathbf{Z}$, quindi anche $Aut(G)$ è abeliano. Gli elementi invertibili di $\mathbf{Z}$ sono 1 e -1, quindi se G è infinito, i suoi automorfismi sono l'identità e la mappa che manda ogni elemento nel suo inverso. Questi formano un gruppo abeliano di ordine 2. Se G è finito, gli elementi invertibili di $\mathbf{Z}_{|G|}$ sono le classi $n + |G|\mathbf{Z}$ dove n è primo con $|G|$, in particolare $|Aut(G)| = \Phi(|G|)$ ove Φ è la funzione di Eulero. Abbiamo così dimostrato il seguente risultato:

Proposizione A.3.2 *Sia G un gruppo ciclico. Allora*

- *Se G è infinito, $Aut(G)$ è isomorfo a $\mathbf{Z}_2$.*
- *Se G è finito, $Aut(G)$ è isomorfo al gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbf{Z}_{|G|}$.*

A.3.2 Il gruppo degli automorfismi di un p-gruppo abeliano elementare

Sia p un numero primo un p-gruppo finito G si dice **abeliano elementare** se G è isomorfo al prodotto diretto

$$\underbrace{\mathbf{Z}_p \times \mathbf{Z}_p \times \ldots \times \mathbf{Z}_p}_{n-volte}$$

per un opportuno numero naturale n diverso da 0. Chiaramente $|G| = p^n$ e l'intero n si dice **rango** di G.

Sia $(G, +)$ un p-gruppo abeliano elementare (per comodità, in quanto segue useremo la notazione additiva). Sia $z + p\mathbf{Z} \in \mathbf{Z}_p$. Definiamo un'applicazione

$$\begin{array}{rccc} \phi\colon & \mathbf{Z}_p \times G & \to & G \\ & (z + p\mathbf{Z}, g) & \mapsto & zg \end{array}$$

Poichè G è un p-gruppo abeliano elementare, ϕ è ben posta e, come si verifica immediatamente, definisce su G una struttura di spazio vettoriale sul campo $\mathbf{Z}_p$. Si verifica facilmente che gli endomorfismi di G come gruppo sono anche endomorfismi di G come spazio vettoriale su $\mathbf{Z}_p$. Poiché G è finito, G ha dimensione finita su $\mathbf{Z}_p$. Sia questa n. Allora $|G| = p^n$. Fissata una base $v_1, \ldots, v_n$ di G, si può definire un isomorfismo di anelli tra $End(G)$ e l'anello delle matrici $n \times n$ a coefficienti in $\mathbf{Z}_p$ (ricordiamo che questo isomorfismo associa alla matrice $(a_{i,j})$ l'endomorfismo α di G definito da $(\sum_{i=1}^n b_i v_i)^\alpha = \sum_{j=1}^n \sum_{i=1}^n b_i a_{i,j} v_j$. Il gruppo degli automorfismi di G è quindi isomorfo al gruppo moltiplicativo delle matrici invertibili $n \times n$ a coefficienti in $\mathbf{Z}_p$. Il gruppo degli automorfismi di G come spazio vettoriale su $\mathbf{Z}_p$ si indica con $GL(G, \mathbf{Z}_p)$, il gruppo delle matrici $n \times n$ invertibili a coefficienti in $\mathbf{Z}_p$ si indica con $GL(n, \mathbf{Z}_p)$. Abbiamo dimostrato il seguente risultato:

Proposizione A.3.3 *Se G è un p-gruppo finito abeliano elementare, allora $|G| = p^n$ per un opportuno intero n e risulta:*

$$Aut(G) \cong GL(G, \mathbf{Z}_p) \cong GL(n, \mathbf{Z}_p).$$

A.4 Grafi e geometrie

Le definizioni di questa sezione seguono quelle dalla Sezione 3 di [1].

A.4.1 Grafi

Un **grafo** è una coppia $(V, \mathcal{R})$ dove V è un insieme i cui elementi si dicono **vertici** ed una relazione simmetrica $\mathcal{R}$ i cui elementi si dicono **lati**. Se x e y sono vertici con $(x, y) \in \mathcal{R}$ diremo che x e y sono **adiacenti**. Spesso useremo anche simboli come $*$ oppure $\leftrightarrow$ per indicare la relazione simmetrica in un grafo e, come è usuale, scriveremo $x\mathcal{R}y$ per $(x, y) \in \mathcal{R}$. Dati due vertici x e y nel

grafo $(V, \mathcal{R})$, un **cammino di lunghezza** n nel grafo $(V, \mathcal{R})$, è una successione di vertici

$$(u_1, \dots u_n)$$

tali che $u_1 = x$, $u_n = y$ e, per ogni $i \in \{1, \dots, n-1\}$

$$u_i \text{ è adiacente a } u_{i+1}.$$

Se x è un vertice di $(V, \mathcal{R})$, l'insieme dei vertici $y \in V$ tali che esista un cammino tra x e y si dice **componente connessa di** $(V, \mathcal{R})$ **contenente** x. L'insieme delle componenti connesse di $(V, \mathcal{R})$ è una partizione di V. Se x e y sono due vertici contenuti nella medesima componente connessa del grafo $(V, \mathcal{R})$ la **distanza** tra x e y è il minimo delle lunghezze dei cammini tra x e y. Se x e y appartengono a distinte componenti connesse diremo che la distanza tra x e y è infinita. In entrambi i casi indicheremo con $d(x, y)$ la distanza tra x e y.

Se $(V, \mathcal{R})$ e $(W, \mathcal{S})$ sono grafi, un'applicazione

$$\phi \colon V \to W$$

che conserva l'adiacenza, cioè tale che, per ogni $(x, y) \in \mathcal{R}$, $(x^\phi, y^\phi) \in \mathcal{S}$, si dice **omomorfismo di grafi** tra $(V, \mathcal{R})$ e $(W, \mathcal{S})$. Un **isomorfismo** tra $(V, \mathcal{R})$ e $(W, \mathcal{S})$ è un omomorfismo biiettivo, tale che anche il suo inverso sia un omomorfismo. Un **automorfismo** di $(V, \mathcal{R})$ è un isomorfismo tra $(V, \mathcal{R})$ e se stesso.

A.4.2 Le geometrie di Tits

Sia I un insieme finito. Una **geometria di Tits su** I è una tripla $(\Gamma, \lambda, *)$ dove $(\Gamma, *)$ è un grafo e λ una funzione da Γ a I tale che, per ogni $u, v \in \Gamma$ con $\lambda(u) = \lambda(v)$, risulta $u * v$ se e solo se $u = v$. Se $u \in \Gamma$ diremo che $\lambda(u)$ è il **tipo** di u. La relazione $*$ si dice **relazione d'incidenza** della geometria $(\Gamma, \lambda, *)$ e due vertici adiacenti si dicono anche **incidenti**. Se $(\Gamma_1, \lambda_1, *_1)$ e $(\Gamma_2, \lambda_2, *_2)$ sono geometrie sullo stesso insieme I, un'applicazione

$$\phi \colon \Gamma_1 \to \Gamma_2$$

tale che

1. ϕ **conserva i tipi**, cioè $\lambda_1(u) = \lambda_2(u^\phi)$ per ogni $u \in \Gamma_1$ e
2. ϕ **conserva l'incidenza**, cioè $u^\phi *_2 v^\phi$ per ogni $u, v \in \Gamma_1$ con $u * v$,

si dice **omomorfismo** di geometrie (si osservi che un omomorfismo di geometrie è, in particolare, un omomorfismo di grafi). Un **isomorfismo** di geometrie è un omomorfismo biiettivo di geometrie e tale che anche il suo inverso sia un omomorfismo di geometrie. Se $(\Gamma, \lambda, *)$ è una geometria, un **automorfismo** di$(\Gamma, \lambda, *)$ è un'applicazione $g \colon \Gamma \to \Gamma$ che è un isomorfismo di geometrie. Come al solito l'insieme degli automorfismi di una geometria $(\Gamma, \lambda, *)$ è un gruppo e lo indicheremo con $Aut(\Gamma)$. Come al solito, scriveremo Γ per la geometria $(\Gamma, \lambda, *)$.

Data una geometria Γ una **bandiera** in Γ è un sottoinsieme $\mathcal{F}$ di Γ in cui ogni coppia di vertici è incidente. In particolare, ogni bandiera contiene al più un vertice per ciascun tipo e quindi l'applicazione λ induce un'applicazione iniettiva tra $\mathcal{F}$ e I. Il sottoinsieme $\lambda(\mathcal{F})$ di I si dice **tipo** della bandiera $\mathcal{F}$. Il **residuo** della bandiera $\Gamma_{\mathcal{F}}$ di $\mathcal{F}$ è l'insieme dei vertici di $\Gamma \setminus \mathcal{F}$ che sono incidenti con ogni elemento di $\mathcal{F}$. $\Gamma_{\mathcal{F}}$ eredita in modo naturale la struttura di geometria su $I \setminus \lambda(\mathcal{F})$

A.4.3 La geometria proiettiva e lo spazio delle bandiere

Sia V uno spazio vettoriale di dimensione n su un campo K. L'insieme dei sottospazi di dimensione 1 di V si dice **spazio proiettivo** associato a V e lo indicheremo con $P(V)$. La **geometria proiettiva** associata a V è l'insieme di tutti i sottospazi propri di V e la indicheremo con $PG(V)$. I sottospazi di dimensione 1 di V si dicono **punti** di $PG(V)$. Due elementi U e W di $PG(V)$ si dicono **incidenti** se $U \leq W$ oppure $W \leq U$ e scriveremo $U * W$. Chiaramente la coppia $(GP(V), *)$ è un grafo. Allora Sia ora $I_n = \{1, \ldots, n-1\}$ e

$$\dim\colon PG(V) \to I_n$$

la funzione che a ciascun sottospazio W di V associa $dim(W)$. Allora la tripla $(P(V), \dim, *)$ è una geometria di Tits su I, e si chiama la **geometria proiettiva** su V. Gli automorfismi di $(P(V), \dim, *)$ come geometria di Tits si dicono anche **collineazioni**.

Un insieme non vuoto $\{P_1, P_2, \ldots, P_l\}$ di punti di $PG(V)$ si dice **indipendente** se $dim(P_1 + P_2 + \ldots + P_l) = l$. Chiaramente un insieme indipendente di punti proiettivi contiene al più n punti ($n = dim(V)$) ed ogni suo sottoinsieme non vuoto è indipendente. Un insieme indipendente di n punti si dice **armatura** (**frame** in inglese). Una serie

$$V_1 < V_2 < \ldots < V_s$$

di sottospazi propri di V si dice **bandiera** di V. Se $\mathcal{F}$ è la bandiera

$$V_1 < V_2 < \ldots < V_s$$

di V, l'intero positivo s si dice **rango** di $\mathcal{F}$ e l'insieme

$$\{dim(V_1), dim(V_2), \ldots, dim(V_s)\}$$

si dice **tipo** di $\mathcal{F}$ (si noti che il rango di una bandiera coincide con la cardinalità del suo tipo). Una bandiera di V si dice **bandiera massimale** o **camera** se il suo rango coincide con $dim(V) - 1$. Chiaramente il tipo di una bandiera massimale è l'insieme $\{1, 2, \ldots, n-1\}$. Una bandiera di V di rango $n-2$ dice **muro**. L'insieme delle bandiere di V si indica con $\mathcal{F}(V)$ e si chiama **spazio delle bandiere** di V. Se $\mathcal{H}$ è una bandiera

$$W_1 < W_2 < \ldots < W_l$$

di V tale che

$$\{V_1, V_2, \ldots, V_s\} \subseteq \{W_1, W_2, \ldots, W_l\},$$

diremo che $\mathcal{F}$ **è contenuta** nella bandiera $\mathcal{H}$ e scriveremo

$$\mathcal{F} \subseteq \mathcal{H}.$$

Per il Teorema del Completamento delle Basi, ogni bandiera è contenuta in una camera.

Lemma A.4.1 *Ogni muro di $\mathcal{F}(V)$ è contenuto in almeno tre camere.*

DIMOSTRAZIONE. Sia $\mathcal{F}$ la camera

$$V_1 < \ldots < V_{n-1}$$

e poniamo $V_0 := \{0\}$ e $V_n := \{V\}$. Poiché ogni spazio vettoriale di dimensione 2 contiene almeno tre sottospazi di dimensione 1, per ogni $i \in \{0, \ldots, n-1\}$ esistono almeno tre sottospazi distinti W tali che $V_{i-1} < W < V_{i+1}$ e, per ciscuno di questi sottospazi,

$$V_1 < \ldots < V_{i-1} < W < V_{1+1} < \ldots < V_{n-1}$$

è una camera che contiene il muro

$$V_1 < \ldots < V_{i-1} < V_{1+1} < \ldots < V_{n-1}$$

■

Se $\overline{\mathcal{F}}_1$ e $\overline{\mathcal{F}}_2$ sono due camere, diremo che $\overline{\mathcal{F}}_1$ e $\overline{\mathcal{F}}_2$ sono **adiacenti** se esiste un muro contenuto sia in $\overline{\mathcal{F}}_1$ che in $\overline{\mathcal{F}}_2$. Se $\mathcal{F}_1$ e $\mathcal{F}_2$ sono due bandiere, diremo che $\mathcal{F}_1$ e $\mathcal{F}_2$ sono **adiacenti** se esistono due camere $\overline{\mathcal{F}}_1$ e $\overline{\mathcal{F}}_2$ adiacenti tali che $\mathcal{F}_i$ è contenuta in $\overline{\mathcal{F}}_i$ ($i \in \{1, 2\}$). Chiaramente la relazione di adiacenza tra le bandiere è una relazione simmetrica e definisce una struttura di grafo su $\mathcal{F}(V)$.

Se Σ è l'armatura

$$\{P_1, P_2, \ldots, P_n\}$$

e $\mathcal{F}$ è la bandiera

$$(V_1 < V_2 < \ldots < V_s),$$

diremo che Σ **supporta** $\mathcal{F}$ se per ogni $i \in \{1, \ldots, s\}$ esiste un sottoinsieme Σ_i di Σ, tale che V_i è generato dai punti in Σ_i. L'insieme delle bandiere supportate dall'armatura Σ si dice **appartamento** associato a Σ e si indica con $\Delta(\Sigma)$.

Lemma A.4.2 *Se Σ è un'armatura ogni muro in $\Delta(\Sigma)$ è contenuto in due sole camere di $\Delta(\Sigma)$*

DIMOSTRAZIONE. Sia Σ l'armatura

$$\{P_1, P_2, \ldots, P_n\}$$

e sia, per ogni $i \in \{1, \ldots, n-1\}$

$$V_i := \langle P_1, \ldots, P_i \rangle.$$

Sia $j \in \{1, \ldots, n-1\}$ e

$$W_j = \langle P_1, \ldots, P_{j-1}, P_{j+1} \rangle.$$

Allora le uniche camere di $\Delta(\Sigma)$ che contengono il muro

$$V_1 < \ldots < V_{j-1} < V_{j+1} < \ldots < V_{n-1}$$

sono

$$V_1 < \ldots < V_{j-1} < V_j < V_{j+1} < \ldots < V_{n-1}$$

e

$$V_1 < \ldots < V_{j-1} < W_j < V_{j+1} < \ldots < V_{n-1}.$$

■

Lemma A.4.3 *Siano $\mathcal{F}$ e $\mathcal{F}'$ due bandiere, allora esiste un appartamento che le contiene entrambe.*

DIMOSTRAZIONE. Per induzione su $n = dim(V)$. Poniamo

$$W_n := V.$$

Poiché ogni bandiera è contenuta in una camera, possiamo supporre che $\mathcal{F}$ e $\mathcal{F}'$ siano rispettivamente le camere

$$V_1 < \ldots < V_{n-1} \text{ e } W_1 < \ldots < W_{n-1}.$$

Sia i il massimo intero in $\{1, \ldots, n-1\}$, tale che

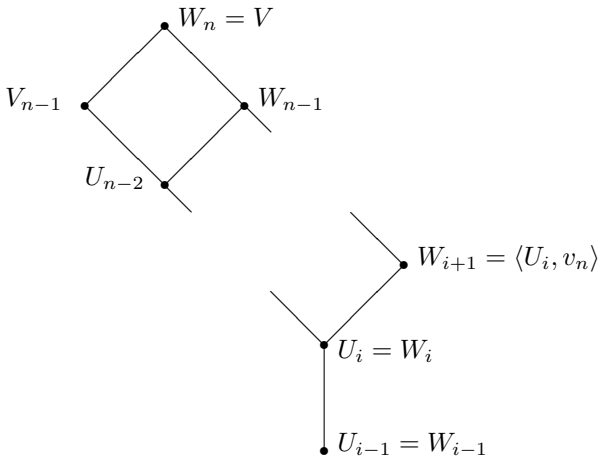
$$W_i \leq V_{n-1}$$

e sia $v_n \in W_{i+1} \setminus V_{n-1}$. Poniamo

$$U_j := W_{j+1} \cap V_1, \text{ se } j > i$$

e

$$U_j := W_j \cap V_1, \text{ se } j \leq i.$$



Allora

$$W_{j+1} = \langle U_j, v_n \rangle$$

per ogni $j > i$ e

$$V_1 < \ldots < V_{n-2} \text{ e } U_1 < \ldots < U_{n-2}$$

sono due camere di V_{i-1}. Per ipotesi induttiva esiste un appartamento $\overline{\Delta}$ In $\mathcal{F}(V_{n-1})$ che le contiene entrambe. Sia

$$\{\langle v_1 \rangle, \ldots \langle v_{n-1} \rangle\}$$

un'armatura che supporta $\overline{\Delta}$, allora

$$\{\langle v_1 \rangle, \ldots \langle v_{n-1} \rangle, \langle v_n \rangle\}$$

è un'armatura in $\mathcal{F}(V)$ che supporta $\mathcal{F}$ e $\mathcal{F}'$, da cui la tesi. ∎

Lemma A.4.4 *Siano U e W sottospazi di V e sia Σ un'armatura che supporta sia U che W. Allora Σ supporta anche $U \cap W$ e $\langle U, W \rangle$.*

Dimostrazione. Sia $\Sigma := \{\langle v_i \rangle | 1 \leq i \leq n\}$, dove $(v_1, \ldots, v_n)$ è una base di V. Ordiniamo gli indici in modo che

$$\{v_1, \ldots, v_r\} \subseteq U \cap W,$$

$$\langle v_1, \ldots, v_s \rangle = U$$

e

$$\langle v_1, \ldots, v_r, v_{s+1}, \ldots, v_t \rangle = W.$$

Chiaramente

$$\langle U, W \rangle = \langle v_1, \ldots, v_t \rangle,$$

e quindi Σ supporta $\langle U, W \rangle$. Inoltre

$$r \leq dim(U \cap W) = dim(U) + dim(W) - dim(\langle U, W \rangle) = s + (r + (t - s)) - t = r,$$

quindi $r = dim(U \cap W)$ e

$$\langle v_1, \ldots, v_r \rangle = U \cap W,$$

da cui la tesi. ■

Il grafo delle classi laterali

Sia G un gruppo, H e K due sottogruppi di G e sia $\Gamma_{H,K}$ il grafo il cui insieme dei vertici è l'insieme di tutte le classi laterali destre di H e K in G e due classi laterali destre sono adiacenti se e solo se sono distinte ed hanno intersezione non vuota. Si osservi che una classe laterale destra di H può essere adiacente solo ad una classe laterale destra di K. Più in generale, se $\mathcal{S}$ è una famiglia di sottogruppi di G, il grafo $\Gamma_{\mathcal{S}}$ è il grafo il cui insieme dei vertici è l'insieme di tutte le classi laterali destre degli elementi di $\mathcal{S}$ e, come sopra, due classi laterali destre sono adiacenti se e solo se sono distinte ed hanno intersezione non vuota. Il grafo $\Gamma_{\mathcal{S}}$ si dice **grafo delle classi laterali** dei sottogruppi di $\mathcal{S}$.

Sia $G = GL(V)$

$$\mathcal{F} := (V_1, V_2, ..., V_n)$$

una bandiera di sottospazi di V tali che $i = dim(V_i)$, quindi

$$V_n = V \text{ e } V_1 \leq V_2 \leq \ldots \leq V_n$$

e sia , per ogni $i \in \{1, \ldots, n-1\}$,

$$N_G(V_i) := \{g \in G | v^g \in V_i \text{ e } v^{g^{-1}} \in V_i \text{ per ogni } v \in V_i\}.$$

Allora, per ogni $i \in \{1, \ldots, n-1\}$, $N_G(V_i)$ è un sottogruppo di G e vedremo in seguito che, posto

$$\mathcal{S}_{\mathcal{F}} = \{N_G(V_i) | i \in \{1, \ldots, n-1\}\},$$

la geometria delle classi laterali $\Gamma(G, \mathcal{S}_{\mathcal{F}})$ è isomorfa alla geometria proiettiva associata a $P(V)$ e G si può rappresentare in modo equivalente sulle due geometrie (esercizio **??**).

Questo è un fatto importante perchè, se K è un campo finito di caratteristica p, la famiglia di sottogruppi propri $\mathcal{S}_{\mathcal{F}}$, può essere caratterizzata intrinsecamente in $GL(V)$ (cioè senza far uso della rappresentazione naturale di $GL(V)$ su

V) come la famiglia dei sottogruppi p-locali massimali di G contenenti un dato p-sottogruppo di Sylow. Le definizioni di p-sottogruppo di Sylow e di sottogruppo p-locale saranno date più avanti, per ora vogliamo solo osservare come la struttura di questi sottogruppi influisca sulla struttura di tutto gruppo. Lo studio delle relazioni tra la struttura p-locale (cioè riguardante i sottogruppi p-locali) e la struttura globale di un gruppo si chiama **Analisi Locale** ed è uno strumento molto importante per lo studio dei gruppi finiti: nel caso di $GL(V)$ ad esempio, possiamo ricostruire la geometria proiettiva dalla struttura p-locale di G.

A.5 Esercizi

Esercizio A.5.1 *Sia G un gruppo finito e $\mathcal{S}$ una famiglia di sottogruppi di G. Dimostrare che il grafo $\Gamma_{\mathcal{S}}$ è connesso se e solo se $G = \langle H | H \in \mathcal{S} \rangle$.*

Esercizio A.5.2 *Siano d k ed n interi positivi, con $d < k < n$ e $k > n/2$, e sia Γ_k il grafo i cui vertici sono i sottoinsiemi di ordine k dell'insieme $\{1, \ldots, n\}$ e due vertici sono adiacenti se e solo se la loro intersezione ha ordine d. Si provi che Γ_k è connesso.*

Esercizio A.5.3 *Siano d, k ed n interi, con $o \leq d < k < n$, e sia V uno spazio vettoriale di dimensione n su un campo K e sia $\Omega_{k,d}$ il grafo i cui vertici soni i sottospazi di dimensione k di V e e due vertici sono adiacenti se e solo se la loro intersezione ha dimensione d. Si provi che Ω_k è connesso.*

Esercizio A.5.4 *Sia V uno spazio vettoriale di dimensione n su un campo K e siano U e W sottospazi di V con $U < W$. Si provi che il residuo della bandiera (U, W) in $GP(V)$ è isomorfo a $GP(W/U)$.*

Bibliografia

[1] M. Aschbacher, *Finite Group Theory,* Cambridge University Press, Cambridge, 1986.

[2] M. Aschbacher, R. Kessar, B. Oliver, *Fusion Systems in Algebra and Topology,* Cambridge University Press, Cambridge, 2011.

[3] R. Baer, *Engelsche Elemente Noetherscher Gruppen*, Math. Ann. **133**, (1957), 256-276.

[4] H. Bender, *Über den Groβten p' Normalteiler in p-auflösbaren Gruppen*, Archiv **18**, (1967), 15-16.

[5] H. Bender, *A group theoretic proof of Burnside's p^aq^b-theorem*, Math. Z. **126**, (1972), 327-338.

[6] A. Borel, J. Tits, *Eléments unipotents et sousgroupes paraboliques des groupes réductifs*, Inv. Math. **12** (1971), 97-104.

[7] N. Bourbaki, *Lie Groups and Lie Algebras, 4, 5 ,6* Springer Berlin-Heidelberg 2008.

[8] W. Burnside, *On groups of order p^aq^b*, Proc. London Math. Soc. (2) **1**, (1904) 388-392.

[9] D. Craven, *The Theory of Fusion Systems,* Cambridge University Press, Cambridge, 2011.

[10] W. Feit, J.G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13**, (1963), 775-1029.

[11] R. W. Carter, *Simple Groups of Lie Type* John Wiley & Sons - New York 1972.

[12] G. Glauberman,*Failure of factorization in p-solvable groups*, Quart. J. Math. Oxford **24** (1973) 71-107.

[13] D. M. Goldschmidt, *A group theoretic proof of Burnside's p^aq^b-theorem for odd primes*, Math. Z. **113**, (1970) 373-375.

[14] D. Gorenstein, *Finite Groups,* Second Edition, Chelsea, New York, 1980.

[15] D. Gorenstein, R. Lyons, R. Solomon, *The Classification of Finite Simple Groups , Number 2*, Amer. Math. Soc. Surveys and Monographs, **40**, **nr. 2** 1996.

[16] P. Hall, *A characteristic property of a soluble group*, J. London Math. Soc. **12**, (1937), 188-200.

[17] I. N. Herstein, *Algebra*, Editori Riuniti, Roma 1984.

[18] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer, New York-Berlin-Heidelberg, 1972.

[19] J. E. Humphreys, *Reflection Groups and Coxeter Groups* Cambridge University Press, Cambridge 1990.

[20] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, New York 1976.

[21] N. Jacobson, *Basic Algebra I*, W. H. Freeman & Co., 1974.

[22] H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups, An Introduction*, Springer, New York-Berlin-Heidelberg 2004.

[23] H. Matsuyama, *Solvability of groups of order* $2^a q^b$ Osaka J. Math. **10**, (1973), 375-378.

[24] U. Meierfrankenfeld, *Finite groups of Local Characteristic p. An Overview*, Proceedings of the L.M.S. Durham symposium, Durham, UK, July 16-26, 2001. River Edge, NJ: World Scientific, (2003), 155-192.

[25] R. Schmidt, *Subgroups Lattices of Groups*, Walter de Gruyter, Berlin - New York, 1994.

[26] R. Solomon, *Abstract Algebra*, A.M.S., Providence, 2003.

[27] M. Suzuki, *Group Theory I,II*, Springer, New York-Heidelberg-Berlin, 1982;1986.

[28] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann, Berlin, 1992.

[29] J. G. Thompson, *Fixed points of p-groups acting on p-groups*, Math. Z. **80**, (1964), 12-13,

[30] J. G. Thompson, *Nonsolvable groups all of whose local subgroups are solvable I-VI*, Bull AMS **74** 383-437, (1968); Pacific J. Math. **33**, 451-536, (1970), **39**, 483-534, (1971), **48**, 511-192, (1973), **50**, 215-297, (1974), **51**, 573-630, (1974)

[31] H. Weyl, *Symmetry* Princeton University Press, 2015.

[32] H. Wielandt, *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. **10**, (1959), 401-402.

[33] H. Wielandt, *Kriteririum für Subnormalität in endlichen Gruppen*, Math. Z. **138**, (1974), 199-203.

Indice analitico

$<$ max, 10
$Aut_A(B)$, 145
$Aut_R(V)$, 204
$End_R(V)$, 204
F-modulo, 281
$Sp(V)$, 229
$\mathcal{A}(H)$, 283
$\mathcal{L}(G)$, 13
$\sim_{\mathcal{F}}$, 274
cc-sottogruppo, 146
p-gruppo, 34
p-radicale, 146
p-residuo, 270
p-riducibile, 279
$\mathcal{R}_p$, 293
$\mathcal{S}p(V)$, 233
$\mathcal{S}^\circ(V)$, 233
$mathcalF$-coniugati, 274

, 219, 221
$\Delta_{Sp}(\Sigma)$, 234
R-congruenza, 204
R-modulo, 203
R-modulo regolare, 205
$\mathcal{F}^\circ$, 233
$\mathcal{P}(G, V)$, 281
congruenza compatibile con una rappresentazione, 204
modulo quoziente, 204
omomorfismo di moduli, 204
rappresentazione di anelli, 202
rappresentazione regolare di anelli, 205

adiacenti, 82
agire, 89
alfabeto, 47
analisi locale, 88
anello degli endomorfismi di un gruppo abeliano, 80
applicazione scalare, 175
applicazione semilineare, 177
asse di una riflessione, 254
automorfismo di grafi, 82
automorfismo di gruppi, 15
automorfismo di una struttura, 79
automorfismo esterno, 92
automorfismo interno, 91, 92
azione 2-transitiva, 123
azione banale, 89
azione coprima, 159
azione di un gruppo, 89
azione fedele, 89
azione indotta sugli endomorfismi, 168
azione per coniugio, 92
azione per coniugio su una sezione, 93
azione quadratica, 212
azione senza punti fissi, 121
azione unipotente, 164

bandiera, 84
bandiera simplettica, 233
base duale rispetto ad una forma bilineare non degenere, 216

camera, 84
camera simplettica, 233
centralizzante, 18, 105
centralizzante di un sottoinsieme, 106
centralizzante di una bandiera, 188
centralizzante di una bandiera simplettica, 238
centralizzante di una serie, 164
centralizzante di una sezione, 93
centralizzare, 18

centro, 14, 92
centro di una riflessione, 255
CGSF, 92
chiusura normale, 73
ciclo, 54
ciclo di Singer, 202
classe di nilpotenza, 71
classe di una permutazione, 54
classe laterale destra, 11
classe laterale sinistra, 11
collineazione, 83
commutatore di due elementi, 61
complemento, 22
complemento di Frobenius, 288
complemento di Hall, 133
completamente normalizzato, 272
componente connessa, 82
componente di un gruppo, 150
componente primaria, 35
Congettura di Schreier, 153
coniugio, 91
controllo dell'azione coprima, 162
controllo della fusione, 272
controllo di un'azione, 162
coppia iperbolica, 219
coppiaBN, 249
costanti di una struttura, 78
cuore di un sottogruppo, 91

derivato n-esimo, 68
determinante di un'applicazione lineare, 173
diagramma di Coxeter, 259
difetto di subnormalità, 24
distanza in un grafo, 82
distanza tra due parole, 48
divisori elementari di un gruppo abeliano finito, 42
divisori elementari di un modulo, 210

elementi coniugati, 14
elementi fusi, 265
elemento centrale, 92
elemento coniugato, 14
endomorfismi di una struttura, 79
endomorfismo di gruppi, 15
endomorfismo idempotente, 23
esponente di un gruppo, 12
estensione di gruppi, 22
estensione spezzante, 22, 30

failure-of-factorization modulo, 281
fattori di composizione, 25
fattori di una serie, 25
fattori invarianti di un gruppo abeliano finito, 42
fattori invarianti di un modulo, 210
fattorizzazione come prodotto semidiretto, 22
Fattorizzazione di Frattini, 129
forma bilineare, 215, 221
forma bilineare alternante, 219
forma bilineare degenere, 216
forma bilineare riflessiva, 217
forma definita positiva, 256
frame, 84
fusion system, 265
fusione banale, 265

generatori, 11
geometria di Tits, 83
geometria proiettiva, 83
geometria simplettica, 232
grafo, 82
grafo delle classi laterali, 87
gruppi isomorfi, 15
gruppo, 9
gruppo p-primario, 34
gruppo abeliano, 10
gruppo abeliano elementare, 81
gruppo alterno, 55
gruppo ciclico, 11
gruppo commutativo, 10
gruppo completo, 92
gruppo degli automorfismi di una struttura, 79
gruppo di Coxeter, 258
gruppo di Coxeter irriducibile, 260
gruppo di esponente finito, 12
gruppo di Frobenius, 288
gruppo di riflessioni, 256
gruppo di torsione, 11

gruppo di Weyl, 250
gruppo diedrale, 97, 261
gruppo diedrale di ordine infinito, 100
gruppo finitamente presentato, 52
gruppo finito, 10
gruppo generale lineare, 171
gruppo generale lineare proiettivo, 175
gruppo generato da un insieme, 11
gruppo liberamente generato, 45
gruppo nilpotente, 70
gruppo perfetto, 75
gruppo primario, 33
gruppo proiettivo simplettico, 231
gruppo quasisemplice, 149
gruppo quoziente, 14
gruppo risolubile, 68
gruppo semplice, 24
gruppo simplettico, 229
gruppo speciale lineare, 174
gruppo speciale lineare proiettivo, 176
gruppo transitivo sulle bandiere, 176
GSp(V), 232

identità, 9
incidenza di sottospazi, 83
inclusione tra bandiere, 84
inclusione tra serie, 25
indice, 11
insieme indipendente, 84
interderivato, 62
inverso, 9
involuzione, 11
ipercentro, 75
irriducibile, 206
isometria, 221
isomorfismo di gruppi, 15
isomorfismo di moduli, 204
isotropo, 218

lato di un grafo, 82
Lemma dei Tre Sottogruppi, 65
Lemma di Schur, 208
lunghezza di un cammino, 82
lunghezza derivata, 69
lunghezza di un ciclo, 54
lunghezza di una serie, 24
lunghezza in un gruppo liberamente generato, 49
lunghezza in un monoide liberamente generato, 47
lunghezza relativa ad un insieme di generatori, 260

matrice associata ad un'applicazione lineare, 173
matrice di Coxeter, 258
matrice di Gram, 217
modulo ciclico, 204
modulo finitamente generato, 204
modulo quadratico, 281
modulo semplice, 206
monoide libero, 45
monomiali, 250
monomorfismo di gruppi, 15
muro, 84
muro simplettico, 233

non-generatore, 99
normalizzante, 18
normalizzante di una bandiera, 186
normalizzante di una serie, 164
normalizzare, 14
notazione additiva, 10
nucleo di Frobenius, 288
nucleo di un omomorfismo, 13
nucleo di una forma bilineare, 217

offensore, 281
offensore quadratico, 281
omomorfismo di gruppi, 13
operazione, 9
operazione associativa, 9
operazione n-aria, 78
ordine, 11
ordine di un gruppo, 10
ortogonale, 217

parola, 47
partizione di un gruppo, 289
periodo, 11
permutazione, 9
permutazioni disgiunte, 53

piano iperbolico, 219
polinomio caratteristico, 212
polinomio minimo di un endomorfismo, 211
prodotto di due elementi in un gruppo, 9
prodotto di parole, 47
prodotto puntuale di funzioni, 16
prodotto semidiretto, 97
proiezione associata ad una decomposizione, 23
proiezione canonica, 15
proprietà universale dei gruppi liberamente generati, 45
Proprietà universale delle presentazioni, 50
punti proiettivi, 83
punto fisso, 106, 108

radicale di una forma bilineare, 217
radicale nilpotente, 147
radicale unipotente, 188
radicale unipotente in Sp(V), 238
raffinamento di una serie, 25
rango di Coxeter, 258
rango di un p-gruppo abeliano elementare, 81
rango di una bandiera, 84
rango di una matrice di Coxeter, 258
rappresentazione di un gruppo, 89
rappresentazione duale, 178
relazione di incidenza, 83
relazione n-aria, 78
residuo nilpotente, 76
residuo risolubile, 75
reticolo dei sottogruppi, 13
riflessione, 254, 257
rotazione, 256

scambio, 54
semigruppo, 46
semisemplice, 156
serie abeliana, 68
serie centrale, 69
serie centrale ascendente, 70
serie centrale discendente, 72
serie delle chiusure normali, 73
serie derivata, 68
serie di composizione, 24
serie di composizione tra due sottogruppi, 24
serie equivalenti, 27
serie subnormale di un gruppo, 24
serie subnormale tra due sottogruppi, 24
sezione normale, 92
sistema di Coxeter, 258
sistema di generatori, 11
sistema di Tits, 249
somma diretta esterna di moduli, 204
somma diretta interna di sottomoduli, 204
somma diretta ortogonale, 217
sottogruppi di Borel di $Sp(V)$, 237
sottogruppi parabolici di $Sp(V)$, 237
sottogruppo, 10
sottogruppo p-locale, 155
sottogruppo associato ad una radice corta, 243
sottogruppo caratteristico, 94
sottogruppo commutatore, 64
sottogruppo critico, 154
sottogruppo derivato, 64
sottogruppo di Bender, 151
sottogruppo di Borel, 186
sottogruppo di Fitting, 147
sottogruppo di Fitting generalizzato, 151
sottogruppo di Frattini, 94
sottogruppo di Sylow, 127
sottogruppo focale, 270
sottogruppo generato, 11
sottogruppo invariante, 94
sottogruppo massimale, 10
sottogruppo monomiale, 250
sottogruppo normale, 14
sottogruppo normale massimale, 24
sottogruppo parabolico, 186
sottogruppo proprio, 10
sottogruppo quasinormale, 17
sottogruppo radice, 181
sottogruppo subnormale, 24
sottoinsieme debolmente chiuso, 292

sottomodulo generato da un insieme, 204
spazio delle bandiere, 84
spazio euclideo, 256
spazio irriducibile, 202
spazio proiettivo, 83
stabile, 282
stabilizzatore di un elemento, 105
stabilizzatore globale, 105
stabilizzatore puntuale, 106
struttura algebrico-relazionale, 78
supporto di un gruppo, 9
supporto di una struttura, 78

telaio, 84
telaio simplettico, 234
Teorema del Sottogruppo Focale, 270
Teorema di Sostituzione di Thompson, 284
Teorema Fondamentale della geometria Proiettiva, 177
tipo di una bandiera, 84
tipo di una operazione, 78
tipo di una relazione, 78
totalmente isotropo, 218
transfer, 267
trasposizione, 54

unipotente, 156

V_H, 279
valutazione, 203
vertice di un grafo, 82