Corso di Laurea in Matematica - Università di Firenze

Appunti per il corso di ALGEBRA II

Anno Accademico 2006-2007.

Testi suggeriti per la consultazione

- T. Hungerford, *Abstract Algebra: an Introduction*, Harcourt & Brace.
- M. Artin, *Algebra*, Bollati - Boringhieri.
- N. Jacobson, *Basic Algebra 1*, Freeman & Co.

V - I GRUPPI

0.1 Operazioni

Sia A un insieme non vuoto. Una **operazione** (binaria) su A è un'applicazione

$$* : A \times A \longrightarrow A \ .$$

Se $*$ è una operazione su A, allora per ogni $(a, b) \in A \times A$, sciveremo $a * b$. Anzi, il più delle volte (quando non si corra il rischio di confondere) tralasceremo anche di assegnare un simbolo all'operazione e scriveremo semplicement ab.

Esempi. 1) Sono operazioni le usuali "somma" $+$ e "prodotto" $\cdot$ definite sugli insiemi $\mathbb{N}$, $\mathbb{Z}, \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. La sottrazione, nel significato corrente, è una operazione su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, ma non è una operazione su $\mathbb{N}$, dato che la differenza di due numeri interi non è, in genere, un numero intero.

2) Se X è un insieme, allora $\cap$, $\cup$, $\triangle$, $\setminus$ sono operazioni su $A = \mathcal{P}(X)$.

3) Se X è un insieme non vuoto, allora la *composizione* $\circ$ è una operazione sull'insieme X^X di tutte le applicazioni di X in se stesso.
(**Osservazione Importante**) La composizione è anche una operazione sull'insieme $Sym(X)$ di tutte le applicazioni biettive di X in se stesso; infatti, come sappiamo, la composizione di due applicazioni biettive è biettiva.

Dalla definizione data, risulta che su un insieme non vuoto A è possibile in genere definire moltissime operazioni. La maggior parte di esse è tuttavia scarsamente importante (secondo il punto di vista delle strutture algebriche - come si capirà meglio andando avanti). La proprietà fondamentale che, il più delle volte (ma non sempre!), esclude operazioni poco interessanti o di difficile studio è la cosiddetta *associatività*.

Definizione. Un'operazione $*$ sull'insieme A si dice **associativa** se, per ogni $a, b, c \in A$,

$$(a * b) * c = a * (b * c).$$

Definizione. Un **semigruppo** è una coppia $(A, \cdot)$ dove A è un insieme e $\cdot$ una operazione **associativa** su A.

Osservazione importante. Se $(A, \cdot)$ è un semigruppo, allora, per ogni $a, b, c \in A$ possiamo scrivere senza ambiguità

$$a \cdot b \cdot c$$

intendendo con ciò l'elemento $(a \cdot b) \cdot c \ = a \cdot (b \cdot c)$.

Questa osservazione si estende ad una stringa finita qualunque di elementi di A. Ad esempio se $a_1, a_2, a_3, a_4 \in A$, allora:

$a_1 \cdot ((a_2 \cdot (a_3 \cdot a_4)) = a_1 \cdot ((a_2 \cdot a_3) \cdot a_4)) = a_1 \cdot (a_2 \cdot a_3 \cdot a_4) = (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = (a_1 \cdot a_2 \cdot a_3) \cdot a_4 =$ etc.

elemento che scriviamo semplicemente: $a_1 \cdot a_2 \cdot a_3 \cdot a_4$.

Più in generale, per ogni $n \geq 1$ e $a_1, a_2, \ldots, a_n \in A$, possiamo individuare senza ambiguità l'elemento

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n \ .$$

(anche questa affermazione, che appare ovvia, andrebbe provata con rigore, operazione non difficile ma noiosa - la cosa più delicata è enunciare correttamente in modo formale la proprietà, poi si può procedere per induzione sul numero n di elementi. Chi è interessato trova una dimostrazione sui testi di Jacobson e Artin.)

Esercizio. Su $\mathbb{Z} \times \mathbb{Z}$ si definisca l' operazione $*$ ponendo, per ogni $(x, y), (x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) * (x_1, y_1) = (x, y_1)$. Si dica se $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigruppo.

Soluzione. Siano $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$. Allora
$(x, y) * ((x_1, y_1) * (x_2, y_2)) = (x, y) * (x_1, y_2) = (x, y_2) = (x, y_1) * (x_2, y_2) = ((x, y) * (x_1, y_1)) * (x_2, y_2)$, dunque l'operazione $*$ è associativa , e $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigruppo.

Definizione. Sia $\cdot$ una operazione sull'insieme A. Un sottoinsieme B di A si dice **chiuso** (rispetto a $\cdot$) se, per ogni $b, b' \in B$ risulta $b \cdot b' \in B$.

Se B è un sottoinsieme chiuso, allora si può definire su B l'operazione $\cdot$ *indotta* da A (cioè quella definita dalla restrizione della operazione $A \times A \longrightarrow A$ ad una operazione $B \times B \longrightarrow B$, dove la regola che determina il prodotto rimane la stessa). Ovviamente se l'operazione su A è associativa, anche l'operazione indotta su un sottoinsieme chiuso è tale. Una proprietà elementare ma importante dei sottoinsiemi chiusi è che l'intersezione di due o più di essi è ancora un sottoinsieme chiuso.

Proposizione 0.1.1 *Sia $(A, \cdot)$ un insieme con operazione, e siano X, Y sottoinsiemi chiusi. Allora $X \cap Y$ è chiuso. Più in generale, se $\mathcal{F}$ è una famiglia qualsiasi di sottoinsiemi chiusi di A , allora $\bigcap_{X \in \mathcal{F}} X$ è un sottoinsieme chiuso.*

Dimostrazione. Proviamo direttamente il caso generale. Sia $\mathcal{F}$ una famiglia di sottoinsiemi chiusi di A , e sia $W = \bigcap_{X \in \mathcal{F}} X$. Siano $x, y \in W$, allora $x, y \in X$ per ogni $X \in \mathcal{F}$ e poichè tali X sono chiusi, si ha $x \cdot y \in X$ per ogni $X \in \mathcal{F}$, cioè $x \cdot y \in W$. Dunque W è chiuso.

Definizione. Sia $(A, \cdot)$ un semigruppo. Un sottoinsieme chiuso di A si dice **sottosemigruppo** di A.

Esempi 1) L'insieme $2\mathbb{Z}$ dei numeri interi pari è un sottosemigruppo di $(\mathbb{Z}, +)$ e di $(\mathbb{Z}, \cdot)$, mentre l'insieme dei numeri dispari è un sottosemigruppo di $(\mathbb{Z}, \cdot)$ ma non di $(\mathbb{Z}, +)$.
2) Sia X un insieme infinito e poniamo $F(X) = \{\ Y \subseteq X \mid |Y|$ è finito $\}$. Allora $F(X)$ è un sottosemigruppo dei semigruppi $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$, $(\mathcal{P}(X), \triangle)$. Si studi per esercizio il caso $I(X) = \{\ Y \subseteq X \mid |Y| = \infty\ \}$.

Un semigruppo $(A, \cdot)$ ammette se stesso come sottosemigruppo. Un sottosemigruppo di un semigruppo è, con l'operazione indotta, un semigruppo.
Dalla Proposizione 1.1 segue che l'intersezione di sottosemigruppi di un semigruppo è un sottosemigruppo. Sia $(A, \cdot)$ un semigruppo e sia X un sottoinsieme di A; allora

l'intersezione di tutti i sottosemigruppi che contengono X (almeno uno c'è: A stesso) è un sottosemigruppo, ed è il minimo (rispetto alla relazione di inclusione) sottosemigruppo di $(A,\cdot)$ che contiene il sottoinsieme X; esso si chiama il **sottosemigruppo generato** da X.

Chiaramente, un sottosemigruppo che contiene un sottoinsieme X deve contenere tutti i prodotti del tipo $x_1x_2\cdots x_n$ con $x_1, \ldots, x_n$ elementi (non necessariamente distinti) di X. Il sottosemigruppo generato da X è proprio l'insieme di tali prodotti. Ad esempio l'insieme $D = \{\ 2^n \mid n \geq 1\ \}$ è il sottosemigruppo generato da $\{2\}$ nel semigruppo $(\mathbb{Z},\cdot)$. Infatti D è un sottosemigruppo e contiene $\{2\}$. Sia S un sottosemigruppo di $(\mathbb{Z},\cdot)$ con $2 \in S$; allora si prova per induzione su n, che $2^n \in S$. Infatti $2^1 = 2 \in S$ e se $2^n \in S$ allora $2^{n+1} = 2^n 2 \in S$ dato che S è chiuso. Quindi $D \subseteq S$ per ogni sottosemigruppo S che contiene $\{2\}$, e dunque D è il sottosemigruppo generato da $\{2\}$.
Con un altro esempio, sia X un insieme e $Y, Z, U \subseteq X$; allora il sottosemigruppo generato da $\{Y, Z, U\}$ in $(\mathcal{P}(X), \cap)$ è $\{\ Y,\ Z,\ U,\ Y \cap Z,\ Y \cap U,\ Z \cap U,\ Y \cap Z \cap U\ \}$.

Definizione. Una operazione $*$ sull'insieme A si dice **commutativa** se, per ogni $a, b \in A$ risulta:

$$a * b = b * a\ .$$

Esempi. 1) Sono commutative le operazioni di somma e moltiplicazione in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; mentre non è commutativa la sottrazione.

2) Sono commutative le operazioni $\cap$, $\cup$, $\triangle$ sull'insieme $\mathcal{P}(X)$.

3) Se $|X| \geq 2$ la composizione in X^X non è commutativa. Infatti siano a, b elementi distinti di X e si considerino le applicazioni $f, g : X \to X$ definite da

$$f(x) = a \text{ per ogni } x \in X \quad \text{e} \quad g(x) = b \text{ per ogni } x \in X\ ;$$

allora $(f \circ g)(a) = f(g(a)) = f(b) = a$, mentre $(g \circ f)(a) = g(f(a)) = g(a) = b$. Quindi $f \circ g \neq g \circ f$.
Se $|X| \geq 3$ la composizione in $Sym(X)$ non è commutativa. Infatti siano a, b, c elementi distinti di X ; si considerino le permutazioni $\sigma, \tau : X \to X$ definite da

$$\sigma(a) = b\ ,\ \sigma(b) = a\ ,\ \sigma(x) = x \text{ per ogni altro } x \in X$$

$$\tau(a) = c\ ,\ \tau(c) = a\ ,\ \tau(x) = x \text{ per ogni altro } x \in X$$

e si provi che $\sigma \circ \tau \neq \tau \circ \sigma$.

Non si dà un nome particolare ad un insieme dotato di operazione commutativa. Se $(A,\cdot)$ è un semigruppo e l'operazione è commutativa, si dice che $(A,\cdot)$ è un semigruppo commutativo.

Elementi identici e monoidi

Definizione. Sia $(A,\cdot)$ un semigruppo. Un elemento $e \in A$ si dice **elemento identico** (o identità, o elemento neutro) se, per ogni $a \in A$:

$$a \cdot e = a = e \cdot a\ .$$

Proposizione 0.1.2 *Sia $(A,\cdot)$ un semigruppo, e siano e, e' elementi identici su A. Allora $e = e'$.*

Dimostrazione. Se $e,\ e'$ sono elementi identici, si ha:

$$e = e \cdot e' = e'$$

dove la prima uguaglianza sussiste perchè e' è un elemento identico, e la seconda perchè e è un elemento identico.

Dunque se un semigruppo $(A, \cdot)$ ha un elemento identico, esso è unico. Lo si denota, in generale, con 1_A.

Definizione. *Un semigruppo dotato di elemento identico si dice* **monoide**.

Esempi. 1) Sono monoidi i semigruppi $(\mathbb{N}, +)\ , (\mathbb{Z}, +)\ , (\mathbb{Q}, +)\ , (\mathbb{R}, +)\ , (\mathbb{C}, +)$ (l'elemento identico è 0); sono monoidi i semigruppi $(\mathbb{N}, \cdot)\ , (\mathbb{Z}, \cdot)\ , (\mathbb{Q}, \cdot)\ , (\mathbb{R}, \cdot)\ , (\mathbb{C}, \cdot)$ (l'elemento identico è 1)

2) Se X è un insieme e $A = \mathcal{P}(X)$, allora
$(A, \cap)$ è un monoide, con identità X ;
$(A, \cup)$ è un monoide, con identità $\emptyset$;
$(A, \triangle)$ è un monoide, con identità $\emptyset$.

3) Se X è un insieme non vuoto, allora $(X^X, \circ)$ e $(Sym(X), \circ)$ sono monoidi con elemento identico ι_X.

Un monoide $(M, \cdot)$ si dice *commutativo* se l'operazione $\cdot$ è commutativa.

Definizione. Un sottoinsieme B di un monoide $(M, \cdot)$ si dice **sottomonoide** se

$$(1)\quad B \text{ è chiuso} \qquad (2)\quad 1_M \in B\ .$$

Esempi. 1) Pwr $n \in \mathbb{N}$, l'insieme $\{\ m \in \mathbb{N} \mid m \geq n\ \} \cup \{0\}$ è un sottomonoide di $(\mathbb{N}, +)$.
2) Se $r \in \mathbb{R}$, allora gli insiemi $\{\ r^n \mid n \in \mathbb{N}\}$ e $\{\ r^n \mid n \in \mathbb{Z}\}$ sono sottomonoidi di $(\mathbb{R}, \cdot)$.
3) Sia X un insieme non vuoto e fissiamo $x \in X$. L'insieme $S_x = \{\ f \in X^X \mid f(x) = x\ \}$ è un sottomonoide del monoide $(X^X, \circ)$. Infatti, $\iota_X \in S_x$ (perchè $\iota_X(x) = x$), e per ogni $f, g \in S_X$, $(f \circ g)(x) = f(g(x)) = f(x) = x$ dunque $f \circ g \in S_X$.

Un monoide M ha almeno due sottomonoidi: M stesso e $\{1_M\}$. Per i sottomonoidi valgono inoltre le osservazioni fatte per i sottosemigruppi. In particolare l'intersezione di una famiglia di sottomonoidi di un monoide M è un sottomonoide, e, se X è un sottoinsieme di M, il sottomonoide generato da X è l'intersezione di tutti i sottomonoidi che contengono X.
Ad esempio il sottomonoide di $(\mathbb{Z}, \cdot)$ generato dall'insieme $\{2\}$ è $\{\ 2^n \mid n \geq 0\ \}$ (infatti per definizione deve contenere $1 = 2^0$).

Esercizio. Si determini il sottomonoide S generato da $2, 3$ in $(\mathbb{N}, +)$.

Soluzione. Osserviamo che se un sottomonoide di $(\mathbb{N}, +)$ contiene l'elemento n, allora, per la chiusura rispetto alla somma, deve contenere tutti i multipli positivi di n, incluso 0. Quindi S che è un sottomonoide che contiene 2, contiene tutti i numeri pari positivi. Sia ora $d \geq 3$ un numero dispari, allora $d - 3$ è un numero pari positivo, quindi $d - 3 \in S$ e poichè S è chiuso, $d = 3 + (d - 3) \in S$. Dunque $S \supseteq \mathbb{N} \setminus \{1\}$. Ora, si verifica facilmente che $\mathbb{N} \setminus \{1\}$ è un sottomonoide di $(\mathbb{N}, +)$, quindi $S = \mathbb{N} \setminus \{1\}$.

Inversi e gruppi.

Proposizione 0.1.3 *Sia $(M, \cdot)$ un monoide con elemento identico 1_M, e sia $a \in M$. Se b, c sono elementi di M tali che $ba = 1_M = ac$, allora $b = c$.*

Dimostrazione. Siano $a, b, c \in M$ come nelle ipotesi. Allora :

$$b = b \cdot 1_M = b(ac) = (ba)c = 1_M \cdot c = c \ .$$

Un elemento b tale che $ba = 1_M$ si dice inverso sinistro di a ; un elemento c tale che $ac = 1_M$ si dice inverso destro di a. Mentre è possibile che un elemento di un monoide abbia diversi inversi sinistri o diversi inversi destri (si pensi alle applicazioni), la proposizione precedente implica che se un elemento a di un monoide ha un inverso sinistro e un inverso destro allora questi coincidono (in tal caso a ha, quindi, un unico inverso sinistro che è anche l'unico inverso destro).

Definizione. Sia $(M, \cdot)$ un monoide con elemento identico 1_M. Un elemento $a \in M$ si dice **invertibile** se esiste $b \in M$ tale che

$$a \cdot b = 1_M = b \cdot a \ .$$

in tal caso b è unico, si denota con a^{-1} e si chiama l'**elemento inverso** di a in M.

Dunque, per la Proposizione 1.3, un elemento è invertibile se e solo se ha un inverso sinistro ed un inverso destro. E' inoltre chiaro che se il monoide M è commutativo, allora la condizione $ba = 1_M$ implica $ab = 1_M$ e quindi una delle due è sufficiente a stabilire che b è inverso di a.
L' elemento identico 1_M di un monoide M è invertibile, e coincide con il proprio inverso.

Proposizione 0.1.4 *Sia $(M, \cdot)$ un monoide con elemento identico 1_M, e siano a, b elementi invertibili di M. Allora*

(i) a^{-1} è invertibile e $(a^{-1})^{-1} = a$;

(ii) ab è invertibile e $(ab)^{-1} = b^{-1}a^{-1}$.

Dimostrazione. La dimostrazione è essenzialmente la stessa che abbiamo già visto per le applicazioni.
(i) Poichè

$$(a^{-1})a = 1_M = a(a^{-1})$$

si ha che a^{-1} è invertibile e, per l'unicità dell'inverso, $(a^{-1})^{-1} = a$.
(ii) Se a e b sono invertibili:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1_M b = b^{-1}b = 1_M \ ;$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1_M a^{-1} = aa^{-1} = 1_M$$

dunque ab è invertibile e, per l'unicità dell'inverso, $(ab)^{-1} = b^{-1}a^{-1}$.

Dalla Proposizione 4 e dall'osservazione che la precede, segue che, se M è un monoide, il sottoinsieme $U(M)$ di tutti gli elementi invertibili di M è un sottomonoide.

Esempi. 1) Gli elementi invertibili del monoide $(\mathbb{Z}, \cdot)$ sono 1 e -1, quindi $U(\mathbb{Z}, \cdot) = \{1, -1\}$. Gli elementi invertibili del monoide $(\mathbb{Q}, \cdot)$ sono tutti i numeri razionali diversi da 0, quindi $U(\mathbb{Q}, \cdot) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0, \}$ (e similmente per $\mathbb{R}$ e $\mathbb{C}$).

2) Sia X un insieme e sia Y un elemento invertibile del monoide $(\mathcal{P}(X), \cap)$, allora esiste $Z \in \mathcal{P}(X)$ tale che $Y \cap Z = X$ (X è l'elemento neutro), e quindi deve essere $Y = X$; dunque $U(\mathcal{P}(X), \cap) = \{X\}$. Similmente si osserva che $U(\mathcal{P}(X), \cup) = \{\emptyset\}$.

3) Se X è un insieme, $U(X^X, \circ) = Sym(X)$.

Definizione. Un **gruppo** è un *monoide in cui ogni elemento è invertibile* .

Quindi un insieme con operazione $(G, \cdot)$ è un gruppo se e solo se sono soddisfatte le seguenti condizioni:

1. *Per ogni* $a, b, c \in G$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. *Esiste* $1_G \in G$ *tale che, per ogni* $a \in G$: $a1_G = a = 1_G a$.
3. *Per ogni* $a \in G$ *esiste* $b \in G$ *tale che* $a \cdot b = 1_G = b \cdot a$ (tale b è quindi unico e si denota con a^{-1}).

Esempi. 1) Sono gruppi i monoidi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ e $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, dove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

2) Se X è un insieme non vuoto, allora $(Sym(X), \circ)$ è un gruppo, detto il *Gruppo Simmetrico* su X.

3) Se X è un insieme, allora $(\mathcal{P}(X), \triangle)$ è un gruppo. Infatti, l'elemento neutro è $\emptyset$ e, per ogni $Y \in \mathcal{P}(X)$, $Y \triangle Y = \emptyset$, quindi Y coincide con il proprio inverso. Non sono invece gruppi (tranne nel caso banale $X = \emptyset$) i monoidi $(\mathcal{P}(X), \cap)$ e $(\mathcal{P}(X), \cup)$.

4) Se $(M, \cdot)$ è un monoide, allora l'insieme $U(M)$ degli elementi invertibili di M è un gruppo rispetto alla operazione indotta da M.

Un gruppo si dice **commutativo** (o **abeliano**) se l'operazione è commutativa. Per i gruppi (o monoidi) commutativi, a volte è conveniente utilizzare la cosiddetta *notazione additiva* in cui l'operazione si denota con il simbolo $+$ (mentre la notazione che usiamo in generale, in cui il simbolo dell'operazione è un puntino oppure viene omesso, si dice moltiplicativa). In notazione additiva il simbolo per l'elemento neutro è 0_M (o, semplicemente, 0); se $(A, +)$ è un monoide commutativo, un elemento $a \in A$ è invertibile se esiste $b \in A$ tale che $a + b = 0$, in tal caso si scrive $b = -a$ (invece di $b = a^{-1}$) e $-a$ si chiama *l'opposto* di a. L'enunciato della Proposizione 4 diventa : se a, b sono invertibli, $-(-a) = a$ e $-(a + b) = -b + (-a) = -a + (-b)$ (perchè M è commutativo). Infine, se $(A, +)$ è un gruppo, e $x, y \in A$, si adotta la convenzione di scrivere $x + (-y) = x - y$.

Esercizio. Sia G un gruppo, e sia $g^{-1} = g$ per ogni $g \in G$. Si dimostri che G è commutativo.
Soluzione. Siano $g, h \in G$. Allora $hg = h^{-1}g^{-1} = (gh)^{-1} = gh$.

Potenze. Sia G un gruppo e sia $g \in G$ e $z \in \mathbb{Z}$. La potenza z-esima g^z di g si definisce induttivamente nella maniera seguente:

$$g^0 = 1_G \ ;$$

$$\text{se } z \geq 0 \ , \quad g^{z+1} = g^z g \ ;$$

$$\text{se } z \leq -1 \ , \quad g^z = (g^{-1})^{-z}.$$

In pratica, se $z \geq 0$,

$$g^z = \underbrace{g \cdot g \cdot \ldots \cdot g}_{\text{z volte}}$$

Dalla definizione, tenendo conto che $(g^{-1})^{-1} = g$ segue in particolare che, per ogni $z \in \mathbb{Z}$,

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

Osserviamo anche che, se $n < 0$:

$$g^n g = (g^{-1})^{-n} g = (g^{-1})^{-n-1+1} g = (g^{-1})^{-n-1} g^{-1} g = (g^{-1})^{-n-1} = g^{n+1}.$$

Abbiamo dato la definizione di potenze di un elemento in un gruppo, ma le stesse definizioni valgono, limitando opportunamente gli esponenti, ad elementi in un semigruppo o in un monoide. Così, in un semigruppo le potenze di un elemento sono definite come sopra per esponenti $z \geq 1$, e nel caso di un monoide per esponenti $z \geq 0$. Similmente, la seguente proposizione, che enunciamo e dimostriamo per i gruppi, sussiste, restringendo il dominio degli esponenti, anche per semigruppi e monoidi.

Proposizione 0.1.5 *Sia G un gruppo, $g \in G$ e siano $n, m \in \mathbb{Z}$. Allora*

(i) $g^{n+m} = g^n g^m$;

(ii) $g^{nm} = (g^n)^m$.

Dimostrazione. (i) Se $m = 0$, $g^{n+0} = g^n = g^n \cdot 1_G = g^n g^0$.
Sia ora $m \geq 0$ e procediamo per induzione su m; se, per ipotesi induttiva, $g^{n+m} = g^n g^m$ allora:

$$\begin{aligned} g^{n+(m+1)} = g^{(n+m)+1} = g^{n+m} g^1 \qquad & \text{(per definizione)} \\ = (g^n g^m) g^1 \qquad & \text{(per ipotesi induttiva)} \\ = g^n (g^m g^1) = g^n g^{m+1} \ . \qquad & \text{(per definizione)} \end{aligned}$$

Sia ora $m \leq -1$. Allora, per le osservazioni fatte sopra, e per il caso precedente :

$$g^{n+m} = (g^{-1})^{-n+(-m)} = (g^{-1})^{-n} (g^{-1})^{-m} = g^n g^m \ .$$

(ii) Se $m = 0$ allora $g^{n0} = g^0 = 1_G = (g^n)^0$. Se $m = 1$, $g^{n1} = g^n = (g^n)^1$.
Sia ora $m \geq 1$ e procediamo per induzione su m; se, per ipotesi induttiva, $g^{nm} = (g^n)^m$ allora, usando il punto (i) :

$$g^{n(m+1)} = g^{nm+n} = g^{nm} g^n = (g^n)^m g^n = (g^n)^m (g^n)^1 = (g^n)^{m+1} \ .$$

Quindi la proprietà è provata per $m \geq 1$. Ora osserviamo che per il caso (i) , $g^{-n} g^n = g^{-n+n} = g^0 = 1_G$ e quindi, per ogni $n \in \mathbb{Z}$,

$$g^{-n} = (g^n)^{-1}.$$

Se $m \leq -1$, usando il caso positivo, si ha quindi

$$g^{nm} = g^{(-n)(-m)} = (g^{-n})^{-m} = ((g^n)^{-1})^{-m} = (g^n)^m \ .$$

Notazione additiva. In notazione additiva è preferibile adottare una diversa notazione per le potenze di un elemento, sotto forma di multipli. Se $(A,+)$ è un gruppo additivo, $a \in A$ e $n \in \mathbb{N}$, si scrive

$$\begin{aligned} &0a = 0_A \ ; \\ &na = a + a + \ \ldots \ + a \qquad \text{(n volte)}; \\ &(-n)a = n(-a) = -(na) \ . \end{aligned}$$

e la Proposizione 5 diventa: per ogni $a \in A$ e $m, n \in \mathbb{Z}$,

$$(n+m)a = na + ma \qquad\qquad (nm)a = n(ma) \ .$$

In generale, se G è un gruppo, $x, y \in G$ e $z \in \mathbb{Z}$ allora $(xy)^z \neq x^z y^z$. Infatti, ad esempio:

$$(xy)^2 = x^2y^2 \ \Leftrightarrow \ xyxy = xxyy \ \Leftrightarrow \ x^{-1}xyxyy^{-1} = x^{-1}xxyyy^{-1} \ \Leftrightarrow \ yx = xy.$$

Quello che si può dire è il seguente fatto, la cui facile dimostrazione lasciamo per esercizio.

Proposizione. *Sia G un gruppo, $g, h \in G$ con $gh = hg$. Allora, per ogni $z \in \mathbb{Z}$, $(gh)^z = g^z h^z$.*

Si dice che un semigruppo S soddisfa la legge di cancellazione se, per ogni $a, b, c \in S$, da $ab = ac$ segue $b = c$, e da $ba = ca$ segue $b = c$. Ad esempio, il monoide $(\mathbb{Z}^*, \cdot)$ soddisfa la legge di cancellazione, mentre, in generale, il monoide $(X^X, \circ)$ non la soddisfa (lo si verifichi con un esempio). Una proprietà elementare ma fondamentale di un gruppo è che esso soddisfa la legge di cancellazione.

Proposizione 0.1.6 (Legge di cancellazione). *Sia G un gruppo, e siano $a, b, c \in G$. Se $ab = ac$ allora $b = c$. Se $ba = ca$ allora $b = c$.*

Dimostrazione. Sia G un gruppo, e siano $a, b, c \in G$ tali che $ab = ac$. Allora, moltiplicando a sinistra per a^{-1} si ha

$$b = 1_G b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = 1_G c = c \ .$$

La dimostrazione che $ba = ca \ \Rightarrow \ b = c$ si fa allo stesso modo moltiplicando a destra per a^{-1}.

Esercizio. Sia G un gruppo, e siano $g, h \in G$ tali che $g^2h^2 = h^2g^2$ e $(gh)^3 = g^3h^3$. Si provi che $gh = hg$.
Soluzione. Per le ipotesi su g, h si ha $(gh)^3 = g^3h^3 = (gg^2)(h^2h) = g(g^2h^2)h = gh^2g^2h$; cioè $(gh)(gh)(gh) = (gh)(hg)(gh)$ e quindi, per la legge di cancellazione, $gh = hg$.

Matrici.

Un esempio molto importante di operazione, e strettamente legato alla composizione di applicazioni, è il prodotto (righe per colonne) di matrici. Lo studio delle matrici è parte del corso di Geometria. Richiamiamo qui, senza dimostrazione, solo alcuni fatti.

Sia $1 \leq n \in \mathbb{N}$. Una **Matrice quadrata di ordine n** a coefficienti reali è una tabella

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

dove i coefficienti a_{ij} sono numeri reali. Denoteremo con $M_n(\mathbb{R})$ l'insieme di tutte le matrici quadrate di ordine n a coefficienti reali.
Se $A = (a_{ij}) \in M_n(\mathbb{R})$, allora, per ogni $i = 1, 2, \ldots, n$ la n-upla di numeri reali

$$(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

è detta **i-esima riga** della matrice A. Mentre la **i-esima colonna** di A è

$$(a_{1i}\ a_{2i}\ \cdots\ a_{ni}).$$

Il **prodotto** di due matrici quadrate di ordine n, $A = (a_{ij})$, $B = (b_{ij})$ è definito nella maniera seguente: $(a_{ij})(b_{ij}) = (c_{ij})$ dove, per ogni $i, j = 1, 2, \ldots, n$

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}\ .$$

Cioè il coefficiente di posto ij nella matrice prodotto è

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \ldots + a_{in}b_{nj}$$

ovvero il prodotto (scalare) della i-esima riga di A per la j-esima colonna di B.

Esempi:

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + (-\frac{1}{2} \cdot \frac{1}{2}) & 1 \cdot (-1) + (-\frac{1}{2}) \cdot (-2) \\ -2 \cdot 0 + 3 \cdot \frac{1}{2} & -2 \cdot (-1) + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{3}{2} & -4 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 1 \\ 3 & 0 & 1 \\ -2 & \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 5 & \frac{1}{4} & 2 \\ 3 & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Si verifica che, per ogni $n \geq 1$ il prodotto di matrici quadrate di ordine n è una operazione associativa. Inoltre la **matrice identica**

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ . & . & \cdots & . \\ . & . & \cdots & . \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

è l'elemento identico. Quindi $(M_n(\mathbb{R}), \cdot)$ è un monoide. Se $n \geq 2$ il prodotto di matrici non è commutativo, ad esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Ad ogni matrice quadrata reale A è associato un numero reale $|A| = Det(A)$ detto **determinante** di A. La definizione generale di determinante di una matrice e le sue proprietà sono parte del corso di Geometria. Qui ricordo solo il caso di matrici di ordine $n = 2, 3$. (Una matrice di ordine 1 è un numero reale e coincide con il suo determinante)

$$Det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$$Det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}Det\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + (-1)a_{12}Det\begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13}Det\begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Ad esempio

$$Det\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} = 1 \cdot Det\begin{pmatrix} 2 & \frac{1}{2} \\ 1 & 0 \end{pmatrix} + (-1)0 \cdot Det\begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} + (-1) \cdot Det\begin{pmatrix} 0 & 2 \\ -\frac{1}{2} & 1 \end{pmatrix} =$$

$$= 1(2 \cdot 0 - 1\frac{1}{2}) - 0 - 1(0 \cdot 1 - 2(-\frac{1}{2})) = -\frac{1}{2} - 0 - 1 = -\frac{3}{2}.$$

Una proprietà molto importante del determinante è che per ogni $A, B \in M_n(\mathbb{R})$:

$$Det(A \cdot B) = Det(A)Det(B).$$

Inoltre, per ogni $n \geq 1, Det(I_n) = 1$.

Un altro fatto fondamentale (che si vedrà al corso di Geometria) è che una matrice $A \in M_n(\mathbb{R})$ è **invertibile** se e solo se $Det(A) \neq 0$.
Dunque $\{ A \in M_n(\mathbb{R}) \mid Det(A) \neq 0 \}$ è l'insieme degli elementi invertibili di $M_n(\mathbb{R})$ e quindi, con l'operazione di prodotto righe per colonne, è un **gruppo** che si denota con $GL(n, \mathbb{R})$ e si chiama il gruppo Lineare Generale di ordine n su $\mathbb{R}$.

Rimandiamo al corso di Geometria per le regole generali per determinare la inversa di una matrice invertibile. Qui riporto, al fine di comprendere esempi ed esercizi, il caso $n = 2$.

Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R})$ (quindi $\Delta = Det(A) \neq 0$). Allora

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}.$$

Ha senso considerare matrici quadrate, prodotto di matrici, e determinanti, anche a coefficienti in $\mathbb{Q}$, $\mathbb{C}$ o in $\mathbb{Z}$, o più in generale su ogni insieme R dotato di operazioni di somma e moltiplicazione con determinate proprietà (gli anelli commutativi, che studieremo più avanti). L'insieme di esse costituisce un monoide e si denota con $M_n(\mathbb{Q})$, $M_n(\mathbb{Z})$ etc.
Nel caso di coefficienti in $\mathbb{Z}$ risulta che le matrici invertibili in $M_n(\mathbb{Z})$ sono quelle il cui determinante è 1 o -1, e costituiscono un gruppo denotato con $GL(n, \mathbb{Z})$.

Omomorfismi e isomorfismi

Definizione. 1) Siano $(S, \cdot)$ e $(S', *)$ due semigruppi. Un **omomorfismo** (di semigruppi) di S in S' è una applicazione $\phi : S \longrightarrow S'$ tale che, per ogni $x, y \in S$,

$$\phi(x \cdot y) = \phi(x) * \phi(y) \ .$$

2) Siano $(M, \cdot)$ e $(M', *)$ due monoidi. Un **omomorfismo** (di monoidi) di M in M' è una applicazione $\phi : M \longrightarrow M'$ tale che, per ogni $x, y \in M$,

$$\phi(x \cdot y) = \phi(x) * \phi(y) \qquad \text{e} \qquad \phi(1_M) = 1_{M'} \ .$$

Un **isomorfismo** di semigruppi (monoidi) è un **omomorfismo biettivo**. Un **automorfismo** di un semigruppo (monoide) S è un isomorfismo di S in se stesso.

Proposizione 0.1.7 *Siano $(S, \cdot)$, $(S', *)$ semigruppi (monoidi), e sia $\phi : S \longrightarrow S'$ un isomorfismo. Allora $\phi^{-1} : S' \longrightarrow S$ è un isomorfismo.*

Dimostrazione. Siano $a, b \in S'$. Allora, poichè ϕ è un omomorfismo

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

e, poichè ϕ è iniettiva, si ha

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

(se S è monoide, $\phi(1_S) = 1_{S'}$ e dunque $\phi^{-1}(1_{S'}) = 1_S$) quindi ϕ^{-1} è un omomorfismo; poichè è anche biettiva, ϕ^{-1} è un isomorfismo.

Osserviamo che se $(S, \cdot)$ è un semigruppo (monoide), l'applicazione identica ι_S è un isomorfismo di S in se stesso (quindi un automorfismo). Un'altra proprietà importante degli omomorfismi e isomorfismi è che la composizione di due di essi è ancora un omomorfismo.

Proposizione 0.1.8 *Siano $(A, \cdot)$, $(B, \cdot)$, $(C \cdot)$ semigruppi (monoidi), e $\phi : A \longrightarrow B$, $\psi : B \longrightarrow C$ omomorfismi. Allora $\psi \circ \phi : A \longrightarrow C$ è un omomorfismo . Se ϕ e ψ sono isomorfismi, $\psi \circ \phi$ è un isomorfismo.*

Dimostrazione. Siano $a, b \in A$. Allora, poichè ϕ e ψ sono omomorfismi

$$\psi \circ \phi(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi(a))(\psi \circ \phi(b))$$

dunque $\psi \circ \phi$ è un omomorfismo. Se ϕ e ψ sono isomorfismi, allora sono biettive e quindi $\psi \circ \phi$ è biettiva e pertanto è un isomorfismo.

Definizione. 1) Siano $(G, \cdot)$, $(G', *)$ gruppi. Un **omomorfismo** (di gruppi) di G in G' è una applicazione $\phi : G \longrightarrow G'$ tale che, per ogni $x, y \in G$,

$$\phi(x \cdot y) = \phi(x) * \phi(y) \ .$$

2) Un **isomorfismo** tra i gruppi $(G, \cdot)$ e $(G', *)$ è un **omomorfismo biettivo** di G in G'.

Osserviamo che nella definizione di omomorfismo di gruppi non viene richiesto esplicitamente, come per i monoidi, che $\phi(1_G) = 1_{G'}$. La ragione è che nel caso dei gruppi ciò viene necessariamente.

Proposizione 0.1.9 *Siano* $(G,\cdot)$, $(G',*)$ *gruppi, e sia* $\phi: G \longrightarrow G'$ *un omomorfismo. Allora* $\phi(1_G) = 1_{G'}$ *e per ogni* $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.

Dimostrazione. Sia $b = \phi(1_G)$. Allora

$$b * b = \phi(1_G) * \phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) = b$$

moltiplicando a destra per b^{-1} si ottiene $b = b * b * b^{-1} = b * b^{-1} = 1_{G'}$.
Sia ora $g \in G$, allora

$$\phi(g^{-1}) * \phi(g) = \phi(g^{-1} \cdot g) = \phi(1_G) = 1_{G'}$$

e quindi $\phi(g^{-1}) = (\phi(g))^{-1}$.

Due gruppi G , G' si dicono **isomorfi** se esiste un isomorfismo da G in G'. Si scrive in tal caso $G \simeq G'$. Dalle proposizioni e osservazioni precedenti segue che $G \simeq G$ (mediante l'applicazione identica), se $G \simeq G'$ allora $G' \simeq G$, e che se $G \simeq G'$ e $G' \simeq G''$ allora $G \simeq G''$. (si osservi che una applicazione tra due gruppi G, G' è un omomorfismo (isomorfismo) di gruppi se e solo se è un omomorfismo (isomorfismo) di G in G' considerati come semigruppi). Similmente si definiscono semigruppi e monoidi isomorfi e si fanno le stesse osservazioni, ma in questo corso ci occuperemo principalmente di gruppi, quindi esponiamo i concetti con particolare riferimento a questo tipo di struttura.
Come già suggerisce la Proposizione 9, se due gruppi sono isomorfi allora soddisfano le stesse proprietà strutturali come gruppi. Tutto ciò che, relativamente all'operazione, si può affermare per uno dei due gruppi vale, passando attraverso la corrispondenza biunivoca stabilita dall'isomorfismo, anche per l'altro gruppo. Parlando informalmente, si giunge a dire che due gruppi isomorfi sono "lo stesso" gruppo.

Esempi. 1) Sia P l'insieme dei numeri reali strettamente maggiori di zero. Allora P è un gruppo con l'operazione di moltiplicazione. L'applicazione logaritmo naturale $P \longrightarrow \mathbb{R}$ definita da, per ogni $x \in P$, $x \mapsto log_e(x)$ è un isomorfismo del gruppo moltiplicativo $(P,\cdot)$ nel gruppo additivo $(\mathbb{R},+)$. Infatti, è biettiva e per ogni $x, y \in P$, $log_e(xy) = log_e(x) + log_e(y)$. L'applicazione inversa è la funzione esponenziale, ed è un isomorfismo da $(\mathbb{R},+)$ in $(P,\cdot)$. (naturalmente si ottiene un isomorfismo anche considerando il logaritmo in una qualsiasi base positiva $\neq 1$ fissata)

2) Sia X un insieme. Allora l'applicazione $\mathcal{C} : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ definita da, per ogni $Y \in \mathcal{P}(X)$, $\mathcal{C}(Y) = X \setminus Y$ è un isomorfismo del monoide $(\mathcal{P}(X),\cap)$ nel monoide $(\mathcal{P}(X),\cup)$. Infatti, $\mathcal{C}$ è biettiva (coincide con la propria inversa), e per ogni $X, Z \in \mathcal{P}(X)$ si ha, per la legge di De Morgan (Parte I, Prop. 4), $\mathcal{C}(Y \cup Z) = X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z) = \mathcal{C}(Y) \cap \mathcal{C}(Z)$.

3) L'applicazione $Det : M_2(\mathbb{R}) \longrightarrow \mathbb{R}$ definita nelle pagine precedenti, è un omomorfismo del monoide $M_2(\mathbb{R})$ nel monoide $(\mathbb{R},\cdot)$, e l'applicazione $Det : GL(2,\mathbb{R}) \longrightarrow \mathbb{R}^*$ è un omomorfismo del gruppo $GL(2,\mathbb{R})$ nel gruppo $(\mathbb{R}^*,\cdot)$. Le stesse affermazioni valgono per matrici di qualsiasi ordine $n \geq 1$.

4) Sia G un gruppo, e sia $g \in G$. La proposizione 5 implica che la applicazione $\gamma : \mathbb{Z} \to G$ definita da, per ogni $z \in \mathbb{Z}$, $\gamma(z) = g^z$ è un omomorfismo del gruppo $(\mathbb{Z},+)$ nel gruppo G.

Definizione. Un omomorfismo di un gruppo G in se stesso si dice **endomorfismo** di G; un isomorfismo di G in se stesso si dice **automorfismo** di G.

Dalla Proposizione 8 e l'osservazione che la precede segue che l'insieme $End(G)$ di tutti gli endomorfismi di un gruppo G è un monoide rispetto all'operazione di composizione

(è un sottomonoide di $(G^G, \circ)$). Dalle Proposizioni 7, 8 segue inoltre il fatto importante che l'insieme $Aut(G)$ di tutti gli automorfismi di un gruppo G è un gruppo rispetto all'operazione di composizione; $(Aut(G), \circ)$ si chiama **Gruppo degli Automorfismi** di G.

Esercizio. Sia G un gruppo. Si dimostri che l'applicazione $f : G \longrightarrow G$ definita da, per ogni $g \in G$, $f(g) = g^{-1}$ è un automorfismo se e solo se G è commutativo.

Soluzione. Sia G un gruppo. Supponiamo che l'applicazione f sia un omomorfismo, allora per ogni $g, h \in G$,

$$g^{-1}h^{-1} = f(g)f(h) = f(gh) = (gh)^{-1} ,$$

dunque $gh = ((gh)^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = (h^{-1})^{-1}(g^{-1})^{-1} = hg$, e quindi G è commutativo. Viceversa, sia G commutativo. Allora, per ogni $g, h \in G$,

$$f(gh) = (gh)^{-1} = (hg)^{-1} = g^{-1}h^{-1} = f(g)f(h)$$

dunque f è un omomorfismo. Poichè f è una applicazione biettiva (coincide con la propria inversa), essa è un automorfismo.

Avremo più avanti ancora molte cose da dire sugli omomorfismi e isomorfismi tra gruppi, e sul gruppo degli automorfismi.

ESERCIZI

1. Sia S un insieme non vuoto. Si provi che l'operazione definita su S da $(a, b) \mapsto a$ è associativa.

2. Sia X un insieme e sia $Y \subseteq X$. Si provi che $(\mathcal{P}(Y), \cup)$ è un sottomonoide del monoide $(\mathcal{P}(X), \cup)$.

3. Sia M un monoide e X un insieme non vuoto. Sull'insieme M^X di tutte la applicazioni di X in M si definisca una operazione $(f, g) \mapsto f \cdot g$ ponendo, per ogni $f, g \in M^X$ e ogni $x \in X$: $(f \cdot g)(x) = f(x)g(x)$. Si provi che $(M^X, \cdot)$ è un monoide.

4. Sia M un monoide e sia $a \in M$. Si provi che se, per qualche $n \geq 1$, a^n è invertibile allora a è invertibile.

5. Siano $(A, \cdot)$, $(B, *)$ semigruppi. Sul prodotto diretto $A \times B$ si definisca una operazione ponendo, per ogni $(a, b), (a_1, b_1) \in A \times B$:

$$(a, b)(a_1, b_1) = (a \cdot a_1, b * b_1) .$$

Si dimostri che, con tale operazione, $A \times B$ è un semigruppo. Si provi che se A e B sono monoidi (gruppi), allora $A \times B$ è un monoide (gruppo).

6. Nel monoide $(\mathbb{N}^{\mathbb{N}}, \circ)$ si consideri l'elemento f definito da, per ogni $n \in \mathbb{N}$

$$f(n) = \begin{cases} n & \text{se } n \text{ è pari} \\ 2n & \text{se } n \text{ è dispari} \end{cases}$$

Si determini il sottomonoide generato da f.

7. Sia M un monoide che soddisfa la legge di cancellazione. Si provi che se M è finito allora è un gruppo. [sugg.: per ogni $a \in M$ si consideri la applicazione da M in se stesso definita da $x \mapsto ax$; usando la proprietà di cancellazione si provi che è iniettiva e quindi ...] Si dica se la stessa affermazione vale se M è infinito.

8. Si provi che nel monoide $M_2(\mathbb{R})$ non vale la legge di cancellazione.

9. Sia $\phi : G \to G'$ un omomorfismo di gruppi. Procedendo per induzione su n, si provi che, per ogni $x_1, x_2, \ldots, x_n \in G : \phi(x_1 x_2 \cdots x_n) = \phi(x_1)\phi(x_2) \cdots \phi(x_n)$.

10. Sia $(G, \cdot)$ un gruppo e sia $a \in G$ tale che $ag = ga$ per ogni $g \in G$. Su G si definisca una nuova operazione $*$, ponendo, per ogni $x, y \in G : x * y = x \cdot a \cdot y$. Si provi che $(G, *)$ è un gruppo, e cha la applicazione

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & a^{-1}x \end{array}$$

è un isomorfismo del gruppo $(G, \cdot)$ nel gruppo $(G, *)$.

0.2 Gruppi e sottogruppi

Sottogruppi

Definizione. Sia G un gruppo. Un sottoinsieme H di G si dice **sottogruppo** (e si scrive $H \leq G$) se soddisfa alle seguenti proprietà

(1) H è chiuso; cioè, per ogni $x, y \in H$, $xy \in H$;

(2) $1_G \in H$;

(3) per ogni $x \in H$, $x^{-1} \in H$.

Un sottogruppo H di un gruppo G è un gruppo rispetto all'operazione indotta da G. Viceversa si può provare che se un sottoinsieme S di un gruppo G è un gruppo rispetto all'operazione indotta, allora è un sottogruppo di G nel senso della definizione data (lo si verifichi per esercizio, il punto essenziale è dimostrare che l'elemento identico di S rispetto all'operazione indotta è proprio 1_G).
Dalla definizione segue immediatamente che se $S \leq H$ e $H \leq G$, allora $S \leq G$. Osserviamo anche che ogni gruppo G ha almeno due sottogruppi: G stesso e $\{1_G\}$. $\{1_G\}$ è detto il *sottogruppo banale* di G, mentre un sottogruppo H si dice *proprio* se $H \neq G$.

In notazione additiva le condizioni affinchè un sottoinsieme H di un gruppo additivo A sia un sottogruppo si scrivono:

$$(1)\ \forall x, y \in H,\ x + y \in H \qquad (2)\ 0_A \in H \qquad (3)\ \forall x \in H,\ -x \in H\ .$$

Esempi 1) (**importante**) Sia $n \in \mathbb{N}$ e indichiamo con $n\mathbb{Z}$ l'insieme di tutti i multipli interi di n; cioè

$$n\mathbb{Z} = \{\ nz \mid z \in \mathbb{Z}\ \}.$$

Allora $n\mathbb{Z}$ è un sottogruppo del gruppo $(\mathbb{Z}, +)$. Infatti,
(1) $0 = n0 \in n\mathbb{Z}$;
(2) se $x, y \in n\mathbb{Z}$ esistono $z, z_1 \in \mathbb{Z}$ tali che $x = nz$, $y = nz_1$; quindi $x + y = nz + nz_1 = n(z + z_1) \in n\mathbb{Z}$;
(3) se $x = nz \in n\mathbb{Z}$ allora $-x = -(nz) = n(-z) \in n\mathbb{Z}$.
Vedremo più avanti (Teorema 1) che tutti i sottogruppi del gruppo $(\mathbb{Z}, +)$ sono di questo tipo.

2) Sia X un insieme e sia $Y \subseteq X$. Allora

$$S_Y = \{\ f \in Sym(X) \mid f(Y) = Y\ \}$$

è un sottogruppo del gruppo $Sym(X)$. Infatti
(1) $\iota_X \in S_Y$;
(2) se $f, g \in S_Y$, allora $(f \circ g)(Y) = f(g(Y)) = f(Y) = Y$, dunque $(f \circ g) \in S_Y$;
(3) se $f \in S_Y$, allora $f^{-1}(Y) = f^{-1}(f(Y)) = (f^{-1} \circ f)(Y) = \iota_X(Y) = Y$, e dunque $f^{-1} \in S_Y$.

In questi esempi, la prova che determinati sottoinsiemi sono sottogruppi è consistita nel verificare che essi soddisfano alle tre condizioni della definizione di sottogruppo. In genere però risulterà più conveniente utilizzare il criterio stabilito dal seguente Lemma.

Lemma (Criterio per sottogruppi). *Siano G un gruppo e $H \subseteq G$. Allora sono equivalenti:*

(i) $H \leq G$;

(ii) $H \neq \emptyset$ *e, per ogni* $x, y \in H,\ xy^{-1} \in H$.

Dimostrazione. (i) $\Rightarrow$ (ii). Sia $H \leq G$. Allora $1_G \in H$, in particolare è $H \neq \emptyset$. Se $x, y \in H$, allora $y^{-1} \in H$ per il punto (3) della definizione di sottogruppo e quindi $xy^{-1} \in H$ per il punto (1) della definizione. Quindi H soddisfa la condizione (ii).

(ii) $\Rightarrow$ (i). Sia H sottoinsieme di G che verifica la condizione (ii); proviamo che $H \leq G$. Poichè H non è vuoto, esiste $x \in H$ e quindi, per la condizione (ii) applicata alla coppia $x, x \in H,\ 1_G = xx^{-1} \in H$.
Sia $h \in H$, allora per quanto visto sopra $1_G, h \in H$ e, per la condizione (ii), $h^{-1} = 1_G h^{-1} \in H$.
Rimane da verificare che H è chiuso. Siano $h, g \in H$; allora, per quanto già dimostrato, $g^{-1} \in H$ e quindi, per la condizione (ii) applicata alla coppia h, g^{-1}, si ha $hg = h(g^{-1})^{-1} \in H$.

Il criterio per sottogruppi a cui facevamo cenno è l'implicazione (ii) $\Rightarrow$ (i) di questo Lemma.

Esempio. Sia $1 \leq n \in \mathbb{N}$. Nell'insieme $\mathbb{C}$ dei numeri complessi, consideriamo il sottoinsieme delle radici n-esime dell'unità:

$$U_n = \{\ z \in \mathbb{C}^* \mid z^n = 1\ \}\ .$$

Allora U_n è un sottogruppo del gruppo moltiplicativo $(\mathbb{C}^*, \cdot)$. Infatti $U_n \neq \emptyset$ perchè $1 \in U_n$, e per ogni $z_1, z_2 \in U_n$ si ha $(z_1 z_2^{-1})^n = z_1^n (z_2^{-1})^n = z_1^n (z_2^n)^{-1} = 1 \cdot 1 = 1$; dunque $z_1 z_2^{-1} \in U_n$. Per il criterio dei sottogruppi, $U_n \leq \mathbb{C}^*$.

Sia ora g un fissato (ma generico) elemento di un gruppo G. Le proprietà delle potenze implicano che l'insieme di tutte le potenze intere di g,

$$< g >= \{\ g^z \mid z \in \mathbb{Z}\ \}$$

è un sottogruppo di G. Si chiama il **sottogruppo ciclico generato** da g. Se H è un qualche sottogruppo di G che contiene g, allora, per la chiusura rispetto a prodotti ed inversi, H deve contenere tutte le potenze intere di g; cioè $H \supseteq < g >$. Quindi $< g >$ è il minimo sottogruppo di G che contiene l'elemento g.
Osserviamo che un sottogruppo ciclico è commutativo. Infatti per ogni $g \in G$ e ogni $n, m \in \mathbb{Z}$, $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$.

In *notazione additiva*, il sottogruppo ciclico generato da un elemento a è l'insieme dei multipli interi di a; ovvero $< a >= \{\ za \mid z \in \mathbb{Z}\ \}$. Dimostriamo ora l'importante fatto che tutti i sottogruppi del gruppo additivo $(\mathbb{Z}, +)$ sono ciclici. Per quanto appena osservato, se $a \in \mathbb{Z}$ allora il sottogruppo ciclico generato da a è $a\mathbb{Z} = \{\ az \mid z \in \mathbb{Z}\ \}$.

Teorema 0.2.1 *Sia H un sottogruppo del gruppo additivo $\mathbb{Z}$. Allora esiste $n \in \mathbb{N}$ tale che $H = n\mathbb{Z}$.*

Dimostrazione. Sia $H \leq \mathbb{Z}$. Se $H = \{0\}$ allora $H = 0\mathbb{Z}$.
Supponiamo quindi che $H \neq \{0\}$. Allora esiste $0 \neq a \in H$; poichè H è un sottogruppo, si ha anche $-a \in H$. Ora, uno di questi due elementi di H è un numero positivo non nullo, quindi l'insieme

$$\mathcal{S} = \{\ m \in H \mid m > 0\ \}$$

è un sottoinsieme non vuoto dei numeri naturali. Sia $n = min(\mathcal{S})$. Abbiamo osservato sopra che $n\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$. Proviamo che $H = n\mathbb{Z}$.
Poichè $n \in H$ ed H è un sottogruppo, H contiene tutti i multipli di n, cioè $n\mathbb{Z} \subseteq H$. Viceversa, sia $b \in H$; poichè $n \neq 0$ possiamo dividere b per n; esistono cioè $q, r \in \mathbb{Z}$ tali che

$$b = nq + r \qquad \text{e} \qquad 0 \leq r < n\ .$$

Ora, $nq \in H$ per quanto visto sopra, e quindi

$$r = b - nq \in H\ ;$$

se fosse $r > 0$ allora $r \in \mathcal{S}$ e quindi, per la scelta di $n = min(\mathcal{S})$, sarebbe $n \leq r$ che contraddice la proprietà del resto. Dunque $r = 0$, cioè $b = nq \in n\mathbb{Z}$. Quindi $H \subseteq n\mathbb{Z}$ e pertanto $H = n\mathbb{Z}$.

Quindi i sottogruppi di $\mathbb{Z}$ sono tutti e soli i sottoinsiemi del tipo $n\mathbb{Z}$. Osserviamo anche che la dimostrazione del Teorema fornisce un indicazione, dato $\{0\} \neq H \leq \mathbb{Z}$, per trovare un generatore di H: è il minimo intero positivo non nullo che appartiene ad H.

Applichiamo questo fatto per fare una osservazione interessante. Dati $n, m \in \mathbb{N}$ poniamo

$$n\mathbb{Z} + m\mathbb{Z} = \{\ x + y \mid x \in n\mathbb{Z},\ y \in m\mathbb{Z}\ \} = \{\ nz_1 + mz_2 \mid z_1, z_2 \in \mathbb{Z}\ \}\ .$$

Si dimostri per esercizio che $n\mathbb{Z}+m\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$. Proviamo che se $d = MCD(n, m)$ allora $d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$. Infatti, siano $r, s \in \mathbb{Z}$ tali che $n = ds$, $m = dr$; allora per ogni $z_1, z_2 \in \mathbb{Z}$, $nz_1 + mz_2 = dsz_1 + drz_2 = d(sz_1 + rz_2) \in d\mathbb{Z}$ e quindi $n\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$. Per il viceversa, siano $a, b \in \mathbb{Z}$ tali che $d = na + mb$; allora, per ogni $z \in \mathbb{Z}$, $dz = (na + mb)z = n(az) + m(bz) \in n\mathbb{Z} + m\mathbb{Z}$ e dunque $d\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$. Quindi $d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$.

Si dimostri per esercizio che $n\mathbb{Z} \leq m\mathbb{Z}$ se e solo se $m|n$ e che se $c = m.c.m.(n, m)$ allora $c\mathbb{Z} = n\mathbb{Z} \cap m\mathbb{Z}$.

Per i sottogruppi vale un analogo della Proposizione 1. La facile dimostrazione è lasciata per esercizio.

Proposizione 0.2.2 *Sia G un gruppo, e siano H, K sottogruppi di G. Allora $H \cap K \leq G$. Più in generale, se $\mathcal{F}$ è una famiglia qualsiasi non vuota di sottogruppi di G, allora $\bigcap_{X \in \mathcal{F}} X$ è un sottogruppo di G.*

Osservazione. Dato un gruppo G, l'insieme $\mathcal{S}(G)$ di tutti i sottogruppi di G ordinato per inclusione (di insiemi) è un insieme parzialmente ordinato. La proposizione 2.2 dice, in particolare, che dati $H, K \leq G$ (cioè $H, K \in \mathcal{S}(G)$), $H \cap K$ è il massimo sottogruppo di G contenuto in H ed in K; cioè $H \cap K$ è l'estremo inferiore di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$.
In generale (vedi esercizio sotto), l'unione insiemistica di due sottogruppi non è un sottogruppo. Tuttavia, dati due sottogruppi H, K del gruppo G, possiamo considerare la famiglia di tutti i

sottogruppi di G che contengono H e K - cioè la famiglia dei maggioranti di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$. Essa è non vuota perchè contiene almeno il sottogruppo G, quindi, per la Proposizione 2.2, ha un minimo che è l'intersezione di tutti i suoi membri. Tale sottogruppo si denota con $\langle H, K\rangle$ ed è pertanto il minimo sottogruppo di G che contiene sia H che K. In altri termini $\langle H, K\rangle$ è l'estremo superiore di $\{H, K\}$ in $(\mathcal{S}(G), \subseteq)$.
Da quanto osservato, risulta quindi che $(\mathcal{S}(G), \subseteq)$ è un reticolo. Esso si chiama **reticolo dei sottogruppi** di G.

Esercizio. *Siano A, B sottogruppi del gruppo G. Si provi che se $G = A \cup B$, allora $G = A$ oppure $G = B$.*

Soluzione. Siano A, B sottogruppi propri del gruppo G e supponiamo per assurdo $G = A \cup B$. Ora, $B \not\subseteq A$ perchè se così fosse sarebbe $G = A \cup B = A$ (contro l'ipotesi che A sia un sottogruppo proprio); e similmente $A \not\subseteq B$. Dunque esistono $a \in A \setminus B$ e $b \in B \setminus A$. Considero ab. Se $ab \in A$ allora $b = a^{-1}(ab) \in A$ contro la scelta di b; quindi $ab \notin A$. Similmente $ab \notin B$. Quindi $ab \notin A \cup B$, assurdo.

Il Gruppo S_3.

Questo paragrafo è di fatto un esercizio. Illustriamo i concetti introdotti sinora per descrivere il gruppo simmetrico su un insieme di ordine 3. Più avanti studieremo i gruppi simmetrici in generale e più in dettaglio.

Sia S_3 il gruppo simmetrico sull'insieme $\{1, 2, 3\}$, cioè il gruppo di tutte le permutazioni di $\{1, 2, 3\}$. Come sappiamo, S_3 contiene 6 elementi. Ogni elemento $\sigma \in S_3$ può essere descritto mediante la tabella

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$$

(osserviamo che, essendo σ una applicazione biettiva, la seconda riga della tabella contiene tutti gli elementi $\{1, 2, 3\}$). Allora

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Poniamo quindi

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

allora

$$\gamma^2 = \gamma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

componendo ancora con γ si trova $\gamma^3 = \gamma^2 \circ \gamma = \iota$. Quindi $\gamma^2 = \gamma^{-1}$. Se consideriamo un qualunque numero intero z possiamo scrivere $z = 3q + r$ con $r \in \{0, 1, 2\}$, dunque

$$\gamma^z = \gamma^{3q+r} = \gamma^{3q} \circ \gamma^r = (\gamma^3)^q \circ \gamma^r = \iota^q \circ \gamma^r = \iota \circ \gamma^r = \gamma^r \ ;$$

il sottogruppo ciclico generato da γ (che denotiamo con A) è quindi composto dai tre elementi

$$\iota = \gamma^0 \ , \quad \gamma \ , \quad \gamma^2 \ .$$

γ si dice un **ciclo** di ordine 3, o un 3-ciclo (perchè permuta ciclicamente i tre elementi 1,2,3). Chiaramente, il gruppo ciclico generato da $\gamma^2 = \gamma^{-1}$ coincide con $A =< \gamma >$.
Poniamo ora

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

queste applicazioni "scambiano" due elementi e fissano i rimanenti; si chiamano **trasposizioni**. Allora, per ogni $i = 1, 2, 3$, $\tau_i^2 = \iota$ e quindi, ragionando come abbiamo fatto con γ , il sottogruppo T_i generato da τ_i è

$$T_i =< \tau_i >= \{ \iota , \tau_i \} .$$

Abbiamo quindi elencato tutti gli elementi di S_3. Sono

$$\iota , \gamma , \gamma^2 , \tau_1 , \tau_2 , \tau_3 ;$$

ed abbiamo determinato tutti i sottogruppi ciclici di S_3 che sono

$$\{\iota\} , A , T_1 , T_2 , T_3 .$$

In particolare, S_3 non coincide con alcuno dei suoi sottogruppi ciclici; cosa che poteva essere anche stabilita osservando che S_3 non è abeliano, ad esempio

$$\tau_1 \circ \tau_2 = \gamma \neq \gamma^2 = \tau_2 \circ \tau_1$$

(vedremo in seguito che ogni gruppo non commutativo di ordine 6 è isomorfo a S_3 e che i gruppi di ordine minore o uguale a 5 sono commutativi. Quindi S_3 è il più piccolo gruppo non commutativo).

Vediamo ora che i sottogruppi elencati costituiscono l'insieme di tutti i sottogruppi propri di S_3. Sia $H \leq S_3$ e supponiamo che H contenga due distinte trasposizioni, diciamo τ_1 e τ_2 ; allora H contiene $\tau_2 \circ \tau_1 = \gamma^2$ e $\tau_1 \circ \tau_2 = \gamma$ e quindi contiene anche $\gamma \circ \tau_1 = \tau_3$; dunque $H = S_3$. Similmente si ragiona a partire dalla altre coppie di trasposizioni.

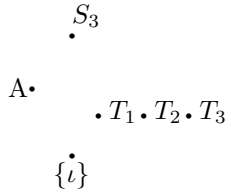
Supponiamo allora che H contenga un'unica trasposizione τ_i; se $H \neq < \tau_i >= T_i$, H contiene o γ o γ^2. Se $\gamma \in H$ allora H contiene $\tau_i \circ \gamma = \tau_{\gamma(i)}$ contro l'assunzione che H contenga un'unica trasposizione. Allo stesso modo, se $\gamma^2 \in H$ allora $\tau_{\gamma(i)} = \gamma^2 \circ \tau_i \in H$ contro l'assunzione su H. Quindi $H =< \tau_i >= T_i$.

Infine, se H non contiene trasposizioni, allora $H = \{1\}$ o $H =< \gamma >= A$.

In conclusione, i sottogruppi di S_3 sono

$$\{\iota\} , A , T_1 , T_2 , T_3 , S_3 .$$

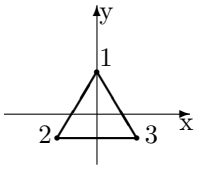
Dal controllo dei loro elementi si vede che se H, K sono sottogruppi propri e distinti di S_3 allora $H \cap K = \{1\} = \{\iota\}$. Quindi il reticolo dei sottogruppi di S_3 è il seguente:



Osserviamo che dallo studio dei sottogruppi fatto sopra segue, tra l'altro, che date due distinte trasposizioni, ad esempio τ_1, τ_2, il più piccolo sottogruppo che le contiene è S_3; si dice allora che S_3 è **generato** dalle trasposizioni τ_1, τ_2 (o che $\{\tau_1, \tau_2\}$ è un insieme di generatori di S_3), e si scrive $S_3 = \langle \tau_1, \tau_2 \rangle$. Ogni elemento di S_3 si scrive come un prodotto i cui fattori sono τ_1, τ_2, o loro inversi (che in questo caso coincidono con gli stessi generatori); infatti: $\iota = \tau_1 \circ \tau_2$, $\gamma = \tau_1 \circ \tau_2$, $\gamma^2 = \tau_2 \circ \tau_1$ e $\tau_3 = \tau_1 \circ \tau_2 \circ \tau_1$.

Osserviamo infine che gli ordini dei sottogruppi di S_3 sono: 1, 2, 3, 6. Ognuno divide l'ordine del gruppo S_3. Questo fatto è una proprietà fondamentale dei gruppi finiti, che dimostreremo nel prossimo paragrafo. Per il momento abbiamo dovuto impiegare un certo lavoro per studiare il gruppo S_3 (che è un gruppo piccolo); nei paragrafi seguenti introdurremo strumenti più raffinati per lo studio dei gruppi, che alla fine faranno apparire come quasi banale questa discussione di S_3.

Il gruppo S_3 può anche essere visto (il termine tecnico è *rappresentato*) come il **gruppo delle simmetrie** di un triangolo equilatero. Consideriamo un triangolo equilatero Δ sul piano, con i vertici numerati con 1, 2, 3; per comodità fissiamo un riferimento cartesiano con origine il centro del triangolo e asse y passante per il vertice 1:

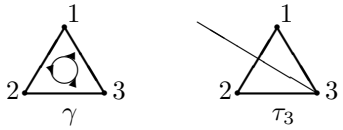


Consideriamo ora l'insieme di tutti i movimenti rigidi del piano che mutano il triangolo Δ in se stesso. Essi sono:

- *l'identità*;
- *le rotazioni (antiorarie) intorno all'origine di* $\frac{2\pi}{3}$ *e* $\frac{4\pi}{3}$ *radianti* (120 e 240 gradi);
- *le tre riflessioni lungo gli assi del triangolo.*

L'insieme γ di queste sei applicazioni (biettive) del piano in se costituisce un gruppo mediante la composizione, che si chiama gruppo delle simmetrie di Δ; ad esempio la composizione della rotazione di $\frac{2\pi}{3}$ radianti con la riflessione lungo l'asse y è la riflessione lungo l'asse passante per il vertice 3, l'inversa della rotazione di $\frac{2\pi}{3}$ radianti è la rotazione di $\frac{4\pi}{3}$ radianti, etc.

Ora, si può definire un isomorfismo da Γ in S_3 associando ad ogni elemento di Γ la permutazione da esso indotta sull'insieme $\{1, 2, 3\}$ dei vertici di Δ. Ad esempio, alla rotazione di $\frac{2\pi}{3}$ radianti corrisponde il 3-ciclo γ, alla riflessione lungo l'asse passante per il vertice 3 corrisponde la trasposizione τ_3, etc. Il sottoinsieme di Γ costituito dalle rotazioni (inclusa l'identità, che è la rotazione di un angolo nullo) è un sottogruppo ciclico, e corrisponde in S_3 al sottogruppo $< \gamma >$.



Considerazioni simili si possono fare per un qualunque poligono (regolare) o più in generale una qualunque figura piana. Ad esempio il gruppo delle simmetrie di una circonferenza con centro l'origine è un gruppo infinito che contiene tutte le rotazioni e tutte le riflessioni lungo rette passanti per l'origine. Per **esercizio** si studi il caso di un quadrato; si provi che il suo gruppo delle simmetrie contiene 8 elementi e non è commutativo (tale gruppo si chiama *gruppo diedrale* di ordine 8)

Gruppi Ciclici

Definizione. Un gruppo G si dice **ciclico** se esiste un elemento $g \in G$ tale che G è il sottogruppo generato da g; cioè

$$G =< g >= \{ g^z \mid z \in \mathbb{Z} \} .$$

In tal caso, g si dice un **generatore** di G.

(In notazione additiva, un gruppo A è ciclico se esiste $a \in A$ tale che $A = \{ za \mid z \in \mathbb{Z} \}$).

Esempi. 1) $(\mathbb{Z}, +)$ è un gruppo ciclico con generatore 1 (un altro possibile generatore è -1 ; si verifichi che questi sono i soli possibili generatori di $\mathbb{Z}$).

2) S_3 non è un gruppo ciclico (si veda il paragrafo precedente).

Abbiamo già osservato che un gruppo ciclico è abeliano. Il gruppo $\mathbb{Z}$ è il modello fondamentale per i gruppi ciclici. Vediamo ad esempio che, così come avviene per $\mathbb{Z}$, ogni sottogruppo di un gruppo ciclico è ciclico. La dimostrazione di questo fatto ricalca quella data per $\mathbb{Z}$ (Teorema 2.1); ne diamo quindi una esposizione rapida. Cercate di completarla e di capire che quella per $\mathbb{Z}$ è la "stessa" dimostrazione.

Proposizione 0.2.3 *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Dimostrazione. Sia $G =< g >$ un gruppo ciclico con generatore g, e sia $H \leq G$. Se $H = \{1_G\}$ allora $H =< 1_G >$. Sia quindi $H \neq \{1_G\}$; allora esiste $0 \neq z \in \mathbb{Z}$ tale che $g^z \in H$. Poichè H è un sottogruppo si ha anche $g^{-z} \in H$. Quindi non è vuoto l'insieme $\{ 0 \neq m \in \mathbb{N} \mid g^m \in H \}$. Sia n il minimo di tale insieme. Allora $g^n \in H$ e quindi $< g^n > \leq H$. Viceversa, se $h = g^z \in H$, si divide z per n : $z = nq + r$ con $0 \leq r \leq n - 1$. Quindi $g^r = g^{z-nq} = g^z(g^n)^{-q} \in H$ da cui segue, per la scelta di n, $r = 0$. Quindi $h = g^z = g^{nq} = (g^n)^q \in < g^n >$ e dunque $H \leq < g^n >$. Quindi $H =< g^n >$ è ciclico.

I due esempi seguenti illustrano come la classe dei gruppi ciclici si suddivida naturalmente in due tipologie; quelli infiniti e quelli finiti. Agli esempi seguirà una proposizione che descrive in generale la differenza tra il caso finito e quello infinito.

Esempi. 1) Consideriamo la matrice

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R}) .$$

e consideriamo il gruppo ciclico $G =< g >$. L'elemento identico di tale gruppo è la matrice identica di ordine 2. Proviamo per induzione che per ogni $n \in \mathbb{N}$ si ha $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Infatti ciò è vero per $n = 0, 1$; supposto vero per n si ha

$$g^{n+1} = g^n g = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 1+n \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

dunque l'affermazione è provata. Osserviamo quindi che per $0 > z \in \mathbb{Z}$ si ha

$$g^z = (g^{|z|})^{-1} = \begin{pmatrix} 1 & |z| \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} .$$

In questo caso quindi, per ogni $0 \neq z \in \mathbb{Z}$ si ha $g^z \neq 1_G$, e $g^x = g^y$ se e solo se $x = y$. In particolare quindi $|G| = \infty$.
Provate inoltre per esercizio che i soli possibili generatori del gruppo G sono la matrice g e la sua inversa (dimostrate cioè che se $z \neq \pm 1$ allora il sottogruppo generato da g^z non contiene g), e che l'omomorfismo $\gamma : \mathbb{Z} \to G$, definito da $\gamma(z) = g^z$, è un isomorfismo.

2) Consideriamo la matrice

$$h = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in GL(2, \mathbb{R}) \ .$$

e consideriamo il gruppo ciclico $H =< h >$. Facendo i calcoli, si trova

$$h^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \qquad h^3 = h^2 h = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

e così via :

$$h^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad h^5 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \qquad h^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = 1_H \ .$$

Abbiamo in particolare trovato un intero strettamente positivo $n = 6$ tale che $h^6 = 1_H$ e 6 è il **più piccolo** naturale non nullo per cui avviene ciò. (Si osservi anche che $h^5 = h^{-1}$)
Ora, dato $z \in \mathbb{Z}$, lo dividiamo per 6: $z = 6q + r$ con $r \in \{0, 1, 2, 3, 4, 5\}$. Si ha allora:

$$h^z = h^{6q+r} = (h^6)^q h^r = 1^q h^r = h^r \ .$$

Dunque possiamo concludere che

$$H =< h >= \{ \ h^r \mid 0 \leq r \leq 5 \ \} = \{ \ h^0 = 1, \ h, \ h^2, \ h^3, \ h^4, \ h^5 \ \}$$

e $| < h > | = 6$.

Ordine di un elemento. Sia g un elemento del gruppo G. L'**ordine** di g, che si denota con $|g|$, è per definizione

il minimo numero intero $n \geq 1$ tale che $g^n = 1_G$, se esiste; ed è ∞ se un tale intero non esiste (ovvero se $g^n \neq 1_G$ per ogni $n \geq 1$).

Proposizione 0.2.4 *Sia $G =< g >$ un gruppo ciclico. Si verifica uno dei casi seguenti.*

(1) Se $|g| = n \geq 1$, allora $|G| = n$ e $G = \{ \ g^0 = 1_G, \ g, \ g^2, \ \ldots, \ g^{n-1} \}$.

(2) Se $|g| = \infty$, allora $|G| = \infty$ e tutte le potenze di g sono distinte (cioè, per ogni $z, w \in \mathbb{Z}$, $g^z = g^w \Leftrightarrow z = w$).

Dimostrazione. (1) Sia $n \geq 1$ e $|g| = n$. Per definizione, n è il minimo numero naturale non nullo tale che $g^n = 1_G$. Se $z \in \mathbb{Z}$, possiamo dividere z per n : $z = nq + r$ con $0 \leq r \leq n - 1$. Allora

$$g^z = g^{nq+r} = (g^n)^q g^r = (1_G)^q g^r = g^r \ ;$$

dunque $G = \{ \ g^r \mid 0 \leq r \leq n-1 \ \} = \{ \ 1_G, \ g, \ \ldots, \ g^{n-1} \ \}$. Per concludere, verifichiamo che gli elementi $1_G = g^0, \ g, \ g^2, \ \ldots, \ g^{n-1}$ sono tutti distinti. Infatti se $0 \leq i \leq j \leq n-1$ e $g^i = g^j$, allora $j - i \geq 0$ e $g^{j-i} = g^j (g^i)^{-1} = 1_G$ e quindi, per la minimalità di n , $j - i = 0$ cioè $i = j$, come si voleva. In particolare, $|G| = n$.

(2) Sia ora $|g| = \infty$. Allora, per ogni $n \geq 1$, $g^n \neq 1_G$. Siano $z, w \in \mathbb{Z}$, $z \geq w$, con $g^z = g^w$, allora

$$g^{z-w} = g^z (g^w)^{-1} = 1_G$$

e quindi $z - w = 0$ cioè $z = w$. Dunque potenze di g con esponenti distinti sono distinte e, in particolare, $|G| = \infty$.

Esercizio. Si provi che due gruppi ciclici dello stesso ordine sono isomorfi.

Esercizio. Si provi che il gruppo additivo dei numeri razionali non è ciclico.

Consideriamo ora un gruppo ciclico $G =< g >$ di ordine finito n. Dalla dimostrazione della proposizione 2.4 segue che, dato $z \in \mathbb{Z}$, $g^z = g^r$ dove r è il resto della divisione di z per n. In particolare

$$g^z = 1_G \quad \Leftrightarrow \quad |g| = n \text{ divide } z \ .$$

Ora, gli elementi di G sono $1_G,\ g,\ g^2,\ \ldots,\ g^{n-1}$. Sia $0 \leq a \leq n-1$ e sia $d = \frac{n}{(a,n)}$; allora n divide ad e quindi $(g^a)^d = g^{ad} = 1_G$, d'altra parte, se $1_G = (g^a)^m = g^{am}$ allora $n|am$ e quindi $\frac{n}{(a,n)}$ divide m (dato che non ha fattori comuni con $\frac{a}{(a,n)}$). Dunque d è l'ordine dell'elemento g^a di G; cioè

$$| < g^a > | = \frac{n}{(a,n)} \ .$$

Da questa osservazione segue che per ogni divisore d di n, l'elemento $g^{\frac{n}{d}}$ genera un sottogruppo di $< g >$ di ordine d; quindi

se G è un gruppo ciclico di ordine n, allora G ha un sottogruppo di ordine d per ogni divisore d di n.

Ad esempio se $G =< g >$ ha ordine 40, allora il sottogruppo generato da g^5 ha ordine 8. Tale sottogruppo è

$$\{\ 1_G,\ g^5,\ (g^5)^2,\ (g^5)^3,\ \ldots,\ (g^5)^7\ \} = \{1_G,\ g^5,\ g^{10},\ g^{15},\ g^{20},\ g^{25},\ g^{30},\ g^{35}\}\ .$$

Si provi per **esercizio** che questo è l'unico sottogruppo di $< g >$ di ordine 8. Si generalizzi quindi la cosa provando che

per ogni divisore d di n un gruppo ciclico di ordine n ha uno e un solo sottogruppo di ordine d.

Esercizio. Sia g un elemento di un gruppo e $n, m \in \mathbb{Z}$, si dimostri che $< g^n > \leq < g^m >$ se e solo se $m|n$.

Un'altra conseguenza della osservazione di sopra è se $< g >$ ha ordine finito n e $0 \leq a \leq n-1$, allora $|g^a| = n$ (e quindi $< g^a > = < g >$) se e solo se $(a, n) = 1$. Cioè

il numero di generatori distinti di un gruppo ciclico di ordine n coincide con il numero di interi positivi strettamente minori di n e coprimi con n.

Tale numero si denota con $\phi(n)$ dove ϕ si chiama la **funzione di Eulero**. In particolare, in un gruppo ciclico di ordine primo ogni elemento non nullo è un generatore.
Non è difficile valutare $\phi(n)$:

Esercizio. 1) Si dimostri che se p è un numero primo, allora per ogni $a \geq 1$:

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).$$

2) Si dimostri che se $(n, m) = 1$ allora $\phi(nm) = \phi(n)\phi(m)$.
3) Si provi che se $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ con $p_1,\ p_2,\ \ldots,\ p_s$ primi distinti, allora

$$\phi(n) = \prod_{i=1}^{s} p_i^{a_i - 1}(p_i - 1).$$

Ad esempio, $\phi(40) = \phi(5)\phi(2^3) = (5-1)(2-1)2^2 = 4 \cdot 4 = 16$. Se $< g >$ ha ordine 40, allora i suoi generatori distinti sono gli elementi g^a con $1 \leq a \leq 39$ e $(a, 40) = 1$, cioè $a = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$.

Classi laterali e Teorema di Lagrange.

Sia H un sottogruppo del gruppo G e sia $x \in G$. La **classe laterale sinistra** di x modulo H è il *sottoinsieme* di G:

$$xH = \{\ xh \mid h \in H\ \}\ .$$

Esempio. Sia $G = S_3$ e H il sottogruppo generato dalla trasposizione τ_1 (cioè $H = \{\iota,\ \tau_1\}$). Allora:
$H = \iota H = \tau_1 H$,
$\tau_2 H = \{\tau_2 \circ \iota,\ \tau_2 \circ \tau_1\} = \{\tau_2,\ \gamma^2\} = \gamma^2 H$,
$\tau_3 H = \{\tau_3 \circ \iota,\ \tau_3 \circ \tau_1\} = \{\tau_3,\ \gamma\} = \gamma H$.

Osserviamo alcuni aspetti di questo esempio. Intanto elementi diversi possono dare la stessa classe laterale; le classi trovate sono disgiunte e costituiscono una partizione di G come insieme. Infine abbiamo trovato 3 classi laterali che contengono tutte lo stesso numero di elementi del sottogruppo considerato H. Questi fatti non sono peculiari di questo esempio ma, come proveremo in questo paragrafo, valgono in generale.
Innanzi tutto vediamo che l'insieme delle classi laterali sinistre modulo un sottogruppo è sempre una partizione del gruppo. Infatti, le classi laterali sono classi di equivalenza di una opportuna relazione di equivalenza che è determinata dal sottogruppo.

Sia H un sottogruppo del gruppo G. Sull'insieme G consideriamo la relazione $\sim_H$ definita ponendo per ogni $x, y \in G:\ x \sim_H y$ se $x^{-1}y \in H$.

Verifichiamo che tale relazione è una equivalenza su G.

- E' riflessiva: infatti per ogni $x \in G,\ x^{-1}x = 1_G \in H$.

- E' simmetrica: infatti per ogni $x, y \in G$, se $x \sim_H y$ allora $x^{-1}y \in H$ e quindi $y^{-1}x = (x^{-1}y)^{-1} \in H$, cioè $y \sim_H x$.

- E' transitiva : infatti se $x, y, z \in G$ sono tali che $x \sim_H y$ e $y \sim_H z$, allora $x^{-1}y \in H$ e $y^{-1}z \in H$, quindi $x^{-1}z = x^{-1}yy^{-1}z \in H$, cioè $x \sim_H z$.

Ora, per ogni $x \in G$ la classe di equivalenza

$$[x] = \{\ y \in G \mid x \sim_H y\ \}$$

coincide con la classe laterale xH, infatti

$$y \in xH \quad \Leftrightarrow \quad \text{esiste } h \in H \text{ tale che } y = xh \quad \Leftrightarrow \quad x^{-1}y = h \text{ con } h \in H \quad \Leftrightarrow \quad x \sim_H y$$

Da ciò segue la proprietà fondamentale che l'insieme delle classi laterali sinistre (distinte) modulo H

$$\{\ xH \mid x \in G\ \}$$

è l'insieme quoziente modulo la equivalenza $\sim_H$ e quindi è una **partizione** di G. Inoltre, poichè due classi di equivalenza coincidono se e solo se i loro rappresentati sono in relazione, si ha il seguente fatto, che è bene avere sempre presente.

$$\textit{Per ogni } \ x, y \in G,\ xH = yH \textit{ se e solo se } \ x^{-1}y \in H \textit{ se e solo se } y \in xH\ .$$

Esercizio. Utilizzando la definizione di classe laterale sinistra, si dimostri direttamente che classi laterali distinte, modulo lo stesso sottogruppo, sono disgiunte

In *notazione additiva* le classi laterali modulo un sottogruppo H in un gruppo additivo A sono i sottoinsiemi

$$a + H = \{\ a + b \mid b \in H\ \}$$

con $a \in A$; e $a + H = b + H$ se e solo se $a - b \in H$ (si ricordi che la notazione additiva si applica a gruppi commutativi).

Definizione. Sia G un gruppo e $H \leq G$. L'**indice** di H in G è il numero di classi laterali (sinistre) di G modulo H. Tale numero di denota con

$$[G : H]\ .$$

Se il gruppo G è finito allora l'indice di ogni sottogruppo è un numero naturale; ad esempio l'indice del sottogruppo H generato dalla trasposizione τ_1 in S_3 è 3. Se il gruppo G è infinito, allora l'indice di un sottogruppo può essere sia un numero naturale che infinito, come vedremo con esempi più avanti. Osserviamo anche che le classi laterali modulo il sottogruppo banale $\{1_G\}$ contengono tutte un solo elemento e che quindi $[G : \{1_G\}] = |G|$.

Un **caso molto importante** è quello dei sottogruppi di $\mathbb{Z}$. Sia $n \geq 1$ e consideriamo il sottogruppo $n\mathbb{Z}$ di $\mathbb{Z}$. Siano $x, y \in \mathbb{Z}$, allora

$$x \sim_{n\mathbb{Z}} y \quad \Leftrightarrow \quad x - y \in n\mathbb{Z} \quad \Leftrightarrow \quad n|x - y \quad \Leftrightarrow \quad x \equiv y \pmod{n}\ ,$$

quindi l'equivalenza associata al sottogruppo $n\mathbb{Z}$ coincide con la congruenza modulo n. Di conseguenza le classi laterali modulo $n\mathbb{Z}$ sono le classi di congruenza (o classi resto) modulo n. Questo si può rivedere direttamente; per ogni $a \in \mathbb{Z}$,

$$a+n\mathbb{Z} = \{\ b = a+nz \mid z \in \mathbb{Z}\ \} = \{\ b \mid b-a = nz,\ z \in \mathbb{Z}\ \} = \{\ b \mid n|b-a\ \} = \{\ b \mid b \equiv a \pmod{n}\ \}\ .$$

detto ancora in un altro modo: $a + n\mathbb{Z} = b + n\mathbb{Z} \quad \Leftrightarrow \quad a \equiv b \pmod{n}$.

Dalla teoria delle congruenze in $\mathbb{Z}$ sappiamo che ci sono n distinte classi di congruenza modulo n : $[0],\ [1],\ [2],\ \ldots,\ [n-1]$. Quindi ci sono n classi laterali di $\mathbb{Z}$ modulo $n\mathbb{Z}$, che sono

$$n\mathbb{Z},\ \ 1 + n\mathbb{Z},\ \ 2 + n\mathbb{Z},\ \ldots,\ (n-1) + n\mathbb{Z}\ ;$$

dunque

$$[\mathbb{Z} : n\mathbb{Z}] = n$$

e per ogni $z \in \mathbb{Z},\ z + n\mathbb{Z} = r + n\mathbb{Z}$ dove r è il resto della divisione di z per n.

Il seguente Teorema stabilisce in particolare una proprietà fondamentale dei gruppi finiti: che *l'ordine di ogni sottogruppo di un gruppo finito* **divide** *l'ordine del gruppo.* Questo fatto è veramente alla base dello studio dei gruppi finiti.

Teorema di Lagrange. *Sia G un gruppo finito, e sia $H \leq G$. Allora*

$$|G| = [G : H]|H| \ .$$

Dimostrazione. Innanzi tutto proviamo che le classi laterali di G modulo H contengono tutte lo stesso numero $|H|$ di elementi. Infatti per ogni classe xH esiste la biezione

$$\sigma_x :\ H \ \longrightarrow \ xH$$

definita ponendo per ogni $h \in H,\ \sigma_x(h) = xh$. Tale applicazione è iniettiva perchè se $\sigma_x(h) = \sigma_x(h')$ allora $xh = xh'$ e quindi, per la legge di cancellazione, $h = h'$; ed è suriettiva per la definizione di classe laterale xH.
Ora, le classi laterali costituiscono una partizione di G. Quindi se $[G : H] = n$ e denotiamo con $K_1,\ K_2,\ \ldots,\ K_n$ le classi laterali distinte di G modulo H, G è l'unione disgiunta $G = K_1 \cup K_2 \cup \ldots \cup K_n$, dunque

$$|G| = \sum_{i=1}^{n} |K_i| = \sum_{i=1}^{n} |H| = n|H| = [G : H]|H| \ ,$$

e la dimostrazione è completa.

Ad esempio, se $|G| = 6$ i possibili ordini dei sottogruppi di G sono 1,2,3 e 6. Studiando S_3 abbiamovisto che per ogni divisore di 6 esiste in S_3 almeno un sottogruppo di tale ordine. Tuttavia, in generale non è vero che se G è un gruppo finito allora per ogni divisore d di $|G|$ deve necessariamente esistere un sottogruppo di ordine d; vedremo in seguito un esempio in cui ciò non avviene. Dimostreremo più avanti anche il notevole Teorema di Sylow, che afferma in particolare che se p è un primo e p^m divide $|G|$ allora G ha un sottogruppo di ordine p^m.

Una prima importante conseguenza del Teorema di Lagrange è il seguente

Corollario 0.2.5 *Sia G un gruppo finito. Allora l'ordine di ogni elemento di G divide l'ordine di G.*

Dimostrazione. Sia G un gruppo finito e $g \in G$. Allora, per definizione, l'ordine di g è l'ordine del sottogruppo $< g >$ e questo, per il Teorema di Lagrange, divide $|G|$.

Osserviamo che da questo corollario segue anche che, se G è un gruppo finito, allora $g^{|G|} = 1_G$ per ogni $g \in G$.

Ecco un'altra immediata e interessante applicazione del Teorema di Lagrange.

Proposizione 0.2.6 *Sia p un primo. Allora ogni gruppo di ordine p è ciclico.*

Dimostrazione. Sia G un gruppo di ordine primo p e sia $1_G \neq g \in G$. Allora il sottogruppo $< g >$ di G non è banale e il suo ordine divide $|G| = p$. Dunque deve essere $< g >= G$.

Vediamo ora un esempio di studio delle classi laterali modulo un sottogruppo; la cosa fondamentale è individuare un opportuno *insieme di rappresentanti*, cioè un insieme di elementi del gruppo, le classi laterali dei quali siano distinte e siano tutte quelle del gruppo. Ad esempio, $\{0,\ 1,\ 2, \ldots,\ n-1\}$ è un insieme di rappresentanti del gruppo $\mathbb{Z}$ modulo il sottogruppo $n\mathbb{Z}$.

Esempio. Fissato un numero primo p , nel gruppo additivo $\mathbb{Q}$ dei numeri razionali consideriamo il sottoinsieme

$$S = \{\ \frac{m}{n} \in \mathbb{Q} \mid p \not| n\ \}\ .$$

$S \leq \mathbb{Q}$; infatti $S \neq \emptyset$ e se $\frac{m}{n}, \frac{r}{s} \in S$ allora $\frac{m}{n} - \frac{r}{s} = \frac{ms-nr}{ns} \in S$ perchè p non divide ns dato che è primo e non divide n ne s. Quindi $S \leq \mathbb{Q}$ per il criterio dei sottogruppi.

Studiamo ora le classi laterali di $\mathbb{Q}$ modulo S ; proviamo che l'insieme

$$\mathcal{R} = \{\ 0,\ \frac{r}{p^i}\ \mid i \in \mathbb{N},\ 1 \leq r \leq p^i - 1 \ \text{ e } \ (r,p) = 1\ \}$$

è un insieme di rappresentanti di $\mathbb{Q}$ modulo S.
Sia $x = \frac{m}{n} \in \mathbb{Q}$, con $(m,n) = 1$. Se $p \not| n$ allora $x \in S = 0 + S$. Altrimenti $p \not| m$ e $n = ap^i$ con $i \geq 1$ e $(a, p^i) = 1$. Poichè a, p^i sono coprimi, esistono $b, r \in \mathbb{Z}$ tali che

$$ar + bp^i = m \qquad\qquad (*)$$

osservo che si può prendere $1 \leq r \leq p^i - 1$, infatti posso sostituire r in $(*)$ con il suo resto della divisione per p^i che non è zero perchè p non divide m. Allora $\frac{r}{p^i} \in \mathcal{R}$ e

$$x - \frac{r}{p^i} = \frac{m}{ap^i} - \frac{r}{p^i} = \frac{m - ra}{ap^i} = \frac{bp^i}{ap^i} = \frac{b}{a} \in S$$

quindi

$$x + S = \frac{r}{p^i} + S\ .$$

Dunque la classi $y + S$ con $y \in \mathcal{R}$ sono tutte le classi di $\mathbb{Q}$ modulo S. Verifichiamo che sono tutte distinte. Se $\frac{r}{p^i}, \frac{s}{p^j} \in \mathcal{R}$ con $j \geq i$, allora

$$\frac{r}{p^i} + S = \frac{s}{p^j} + S \quad \Leftrightarrow \quad \frac{r}{p^i} - \frac{s}{p^j} \in S \quad \Leftrightarrow \quad \frac{rp^{j-i} - s}{p^j} \in S$$

ora, se $j \neq i$, p non divide il numeratore (perchè non divide s) e quindi $\frac{rp^{j-i}-s}{p^j} \notin S$; dunque $i = j$ e allora $\frac{r}{p^i} - \frac{s}{p^j} = \frac{r-s}{p^i} \in S$ se e solo se p^i divide $r - s$ il che implica, dato che $r, s < p^i$, $r = s$. Dunque

$$\frac{r}{p^i} + S = \frac{s}{p^j} + S \quad \Leftrightarrow \quad i = j \ \text{ e } \ r = s\ .$$

osserviamo in particolare che $[\mathbb{Q} : S] = \infty$.

Concludiamo questo paragrafo con due osservazioni sugli indici che sono marginali per quanto riguarda gli argomenti di questo corso, ma possono essere utili nella risoluzione di qualche problema; considerate la dimostrazione come esercizio.

Proposizione 0.2.7 *Siano* H, K *sottogruppi di indice finito del gruppo* G*, allora*

1) (formula del prodotto) Se $K \leq H$ *allora* $[G : K] = [G : H][H : K]$*;*

2) (Lemma di Poincarè) $[G : H \cap K] \leq [G : H][G : K]$*.*

Dimostrazione 1) Sia $[G : H] = n$, $[H : K] = m$ e siano $g_1H, \ldots, g_nH$ le classi laterali distinte di G modulo H e $h_1K, \ldots, h_mK$ quelle di H modulo K. Consideriamo le classi

$$(g_ih_j)K \text{ di } G \text{ modulo } K \text{ con } i = 1, \ldots, n \;\; j = 1, \ldots, m \qquad (*)$$

di G modulo K. Se $(g_ih_j)K = (g_rh_s)K$ allora $h_s^{-1}g_r^{-1}g_ih_j = (g_rh_s)^{-1}(g_ih_j) \in K$, in particolare poichè $K \leq H$, $h_s^{-1}g_r^{-1}g_ih_j = y \in H$ e quindi $g_r^{-1}g_i = h_syh_j^{-1} \in H$, da cui $g_rH = g_iH$ e $r = i$; dunque $h_s^{-1}h_j = h_s^{-1}g_r^{-1}g_ih_j \in K$ e quindi $h_sK = h_jK$ da cui $s = j$. Dunque tutte la classi in (*) sono distinte, quindi $[G : K] \geq nm = [G : H][G : K]$.
Sia ora $g \in G$, allora, per qualche $i = 1, \ldots n \;:\; g \in g_iH$ dunque esiste $y \in H$ tale che $g = g_iy$; similmente esistono un indice $j = 1, \ldots, m$ ed un elemento $x \in K$ tali che $y = h_jx$. Quindi $g = g_iy = h_jg_ix \in h_jg_iK$ da cui $gK = h_jg_iK$. Dunque la classi in $(*)$ sono tutte le classi di G modulo K e pertanto $[G : K] = nm = [G : H][G : K]$.

2) Si applichi la legge di cancellazione per dimostrare che per ogni $g \in G : gH \cap gK = g(H \cap K)$. Da ciò segue facilmente che il numero di classi di G modulo $H \cap K$ è al più $nm = [G : H][G : K]$.

A partire da un sottogruppo H di un gruppo G si definiscono anche le **classi laterali destre** modulo H; per ogni $g \in G$ si pone

$$Hg = \{\ hg \mid h \in H\ \}\ .$$

Le classi laterali destre sono le classi di equivalenza della relazione di equivalenza definita ponendo per ogni $x, y \in G \;:\; x \sim y$ se $xy^{-1} \in H$.
Quindi l'insieme $\{\ Hx \mid x \in G\ \}$ è una partizione di G, e per ogni $x, y \in G$ si ha $Hx = Hy$ se e solo se $xy^{-1} \in H$. Inoltre valgono le stesse osservazioni fatte per le classi sinistre riguardo al loro numero e cardinalità. In particolare vale il Teorema di Lagrange e il fatto che *il numero di classi laterali destre modulo* H *coincide con* $[G : H]$, *il numero di classi laterali sinistre.*

Osserviamo che, in generale, per un $H \leq G$ e un $g \in G$ non è detto che la classe Hx coincida con la classe xH. Ad esempio, se $G = S_3$ e $H = \{\iota,\ \tau_1\}$ è il sottogruppo generato dalla trasposizione τ_1, allora:
$H\tau_2 = \{\iota \circ \tau_2,\ \tau_1 \circ \tau_2\} = \{\tau_2,\ \gamma\} \neq \{\tau_2,\ \gamma^2\} = \tau_2H$.

Ovviamente, se il gruppo G è commutativo, allora $Hx = xH$ per ogni $H \leq G$ ed ogni $x \in G$.

Esercizio. Siano H e K sottogruppi del gruppo G e $x, y \in G$. Si provi che se $Hx = Ky$ allora $H = K$.

Soluzione. Sia $Hx = Ky$ e osserviamo che allora $x = 1x \in Ky$ e dunque $Kx = Ky$. Quindi, se $h \in H$, allora $hx \in Hx = Ky = Kx$ e quindi esiste $k \in K$ tale che $hx = kx$ cioè $h = k \in K$. Dunque $H \subseteq K$. Analogamente si prova che $K \subseteq H$ e quindi $H = K$.

ESERCIZI

1. Si provi che l'insieme

$$\{\ \frac{m}{2^i}\ |\ m \in \mathbb{Z},\ i \in \mathbb{N}\ \}$$

è un sottogruppo del gruppo $(\mathbb{Q}, +)$.

2. Si provi che l'insieme $\{\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\ |\ a, b, d \in \mathbb{R},\ a \neq 0 \neq d\ \}$ è un sottogruppo del gruppo $GL(2, \mathbb{R})$.

3. Sia X un insieme finito e sia $\mathcal{B} = \{\ Y\ |\ Y \subseteq X,\ |Y| \text{ è pari }\}$. Si provi che $\mathcal{B}$ è un sottogruppo del gruppo $(\mathcal{P}(X), \triangle)$.

4. Siano a, b elementi del gruppo G tali che $ab = ba$. Si provi che l'insieme $\{\ a^u b^v\ |\ u, v \in \mathbb{Z}\ \}$ è un sottogruppo di G.

5. Si scriva la tavola di moltiplicazione di S_3.

6. Sia **R** un rettangolo i cui lati adiacenti hanno lunghezza diversa. Si provi che il gruppo delle simmetrie di **R** è commutativo, ha ordine 4, e tutti i suoi elementi hanno ordine 2.

7. Nel gruppo moltiplicativo $\mathbb{Q}^*$ si considerino i sottogruppi

$$A =< -\frac{1}{2} >, \qquad B =< \frac{1}{3} >, \qquad C =< -2 >, \qquad D =< 2 > \ .$$

Si determinino $A \cap B$, $A \cap C$, $C \cap D$, e $[C : C \cap D]$.

8. Sia $G =< g >$ un gruppo ciclico di ordine 14. Si descrivano esplicitamente il sottogruppo di ordine 7, ed i generatori di G.

9. Sia $P = \{\ x \in \mathbb{R}\ |\ x > 0\ \}$. Si provi che $P \leq \mathbb{R}^*$ e si determini l'indice $[\mathbb{R}^* : P]$.

10. Sia $\phi : G \to G'$ un omomorfismo di gruppi e sia g un elemento di ordine finito di G. Si provi che $|\phi(g)|$ divide $|g|$.

11. Siano a, b elementi di un gruppo G tali che $ab = ba$ e $< a > \cap < b >= \{1_G\}$. Si provi che $|ab| = m.c.m.(|a|, |b|)$.

12. Per ogni intero $k \geq 1$ sia $U_k = \{\ z \in \mathbb{C}\ |\ z^k = 1\ \}$ il gruppo moltiplicativo delle radici k-esime dell'unità. Sia $n|m$, si provi che $U_n \leq U_m$ e si determini l'indice $[U_m : U_n]$.

13. Siano H, K sottogruppi di ordine finito del gruppo G. Si provi che se $(|H|, |K|) = 1$ allora $H \cap K = \{1_G\}$.

14. Sia $T = \{\ \frac{m}{3^i}\ |\ m \in \mathbb{Z},\ i = 0, 1\ \}$. Si provi che $\mathbb{Z} \leq T \leq \mathbb{Q}$ (additivamente). Si calcoli quindi l'indice $[T : \mathbb{Z}]$ trovando un opportuno insieme di rappresentanti di T modulo $\mathbb{Z}$.

15. Sia p un primo. Si provi che se G è un gruppo di ordine p^n per qualche intero $n \geq 1$, allora G contiene un elemento di ordine p.

0.3 Sottogruppi normali e Quozienti

Sottogruppi normali

Definizione. Sia G un gruppo. Un sottogruppo H di G si dice sottogruppo **normale** (e si scrive $H \trianglelefteq G$) se per ogni $g \in G$:

$$Hg = gH \ .$$

I sottogruppi normali sono molto importanti perchè, come vedremo tra breve, sull'insieme delle classi laterali modulo un sottogruppo normale (sinistre o destre non ha rilevanza perchè coincidono) è possibile definire una operazione che lo rende un gruppo.
Dalla definizione segue immediatamente che in un qualunque gruppo G, il sottogruppo banale $\{1_G\}$ e G sono sottogruppi normali. Un gruppo G si dice *semplice* se $\{1_G\}$ e G sono i soli sottogruppi normali di G. Ad esempio ogni gruppo di ordine primo è semplice (perchè per il Teorema di Lagrange in un gruppo G di ordine primo, $\{1_G\}$ e G sono i soli sottogruppi). I gruppi semplici sono estremamente importanti nella teoria dei gruppi e in altri ambiti (la dimostrazione di Galois che non esiste una formula risolutiva per le equazioni di quinto grado, o superiore, si basa sul fatto che un certo gruppo - il cosiddetto gruppo alterno A_5 che definiremo più avanti - è semplice), tuttavia il loro studio esula dal programma di questo corso.

Osserviamo inoltre che in un gruppo commutativo ogni sottogruppo è normale. Questo, tranne che per alcune eccezioni (il gruppo dei quaternioni che anche definiremo più avanti), non è il caso dei gruppi non commutativi.

Esempio. Come osservato in precedenza il sottogruppo generato da una trasposizione di S_3 non è normale in S_3. Consideriamo invece il sottogruppo $A = \{\iota,\ \gamma,\ \gamma^2\}$ generato dal ciclo γ di ordine 3. Allora $[S_3 : A] = |S_3|/|A| = 2$ e le classi laterali sinistre di S_3 modulo A sono

$$A = \gamma A = \gamma^2 A \qquad \text{e} \qquad \tau_1 A = \tau_2 A = \tau_3 A \ = S_3 \setminus A,$$

ognuna delle quali coincide con la classe laterale destra con lo stesso rappresentante; quindi $A \trianglelefteq S_3$.

Esercizio. Si dimostri che ogni sottogruppo di indice 2 di un gruppo è normale.

Anche per la proprietà di normalità è conveniente disporre di un criterio che sia più maneggevole della verifica diretta della definizione.

Lemma (Criterio di normalità). *Sia H un sottogruppo del gruppo G. Allora sono equivalenti:*

i) $H \trianglelefteq G$.

ii) *Per ogni* $h \in H$ *e ogni* $g \in G$: $g^{-1}hg \in H$.

Dimostrazione i) $\Rightarrow$ ii). Sia H normale in G, e siano $h \in H$, $g \in G$. Allora $hg \in Hg = gH$ quindi esiste $h_1 \in H$ tale che $hg = gh_1$ da cui, moltiplicando a sinistra per g^{-1}, si ottiene $g^{-1}hg = h_1 \in H$. Quindi H soddisfa la proprietà ii).

ii) $\Rightarrow$ i). Supponiamo che il sottogruppo H soddisfi la proprietà ii), e sia $g \in G$. Sia $x \in Hg$, allora esiste $h \in H$ tale che $x = hg$; quindi per la proprietà soddisfatta da H, $g^{-1}x = g^{-1}hg \in H$ da cui segue $x = g(g^{-1}hg) \in gH$; dunque $Hg \subseteq gH$. Viceversa sia $y = gh$ un generico elemento di gH; allora $y = (ghg^{-1})g \in Hg$ perchè $ghg^{-1} = (g^{-1})^{-1}h(g^{-1}) \in H$. Quindi $gH \subseteq Hg$ e dunque $Hg = gH$ e $H \trianglelefteq G$.

Se G è un gruppo e $g, x \in G$, l'elemento $g^{-1}xg$ si chiama **coniugato** di x tramite g; è importante osservare che in genere si tratta di un elemento diverso da x (infatti, $g^{-1}xg = x \quad \Leftrightarrow \quad xg = gx$).

Esempio. Sia G l'insieme di tutte le matrici reali

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{con} \quad ac \neq 0 \ .$$

Si provi che G è un gruppo. Si consideri quindi il sottoinsieme

$$N = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid 0 \neq b \in \mathbb{R} \} \ .$$

Proviamo che $N \trianglelefteq G$. Innanzi tutto occorre verificare che N è un sottogruppo di G. Infatti N non è vuoto e per ogni $x = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \in N$:

$$xy^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b - b_1 \\ 0 & 1 \end{pmatrix} \in N \ ;$$

dunque $N \leq G$.
Verifichiamo ora la normalità usando il criterio del Lemma. Siano

$$x = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in N \qquad \text{e} \qquad g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \ ,$$

allora

$$g^{-1}xg = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & \frac{cs}{a} \\ 0 & 1 \end{pmatrix} \in N \ ;$$

quindi $N \trianglelefteq G$.

Esercizio. Si provi che se H, K sono sottogruppi normali del gruppo G allora $H \cap K \trianglelefteq G$. Più in generale, se $\mathcal{F}$ è una famiglia di sottogruppi normali di G allora $\bigcap_{H \in \mathcal{F}} \trianglelefteq G$.

Gruppi quoziente

Sia G un gruppo e $N \trianglelefteq G$. Denotiamo con G/N l'insieme delle classi laterali di G modulo N, cioè

$$\frac{G}{N} = \{ \ gN \mid g \in G \ \} \ .$$

Su tale insieme definiamo una operazione (che si denota con lo stesso simbolo dell'operazione di G (quindi in generale semplicemente accostando gli elementi), ponendo, per ogni $xN,\ yN \in G/N$:

$$(xN)(yN) = xyN \ .$$

Verifichiamo che si tratta di una **buona definizione**. Infatti se $x_1,\ y_1 \in G$ sono tali che

$$x_1N = xN \quad \text{e} \quad y_1N = yN \ ,$$

allora

$$x^{-1}x_1 \in N \quad \text{e} \quad y^{-1}y_1 \in N$$

poichè $N \trianglelefteq G$, per il Lemma precedente si ha:

$$y^{-1}(x^{-1}x_1)y \in N$$

e quindi

$$(xy)^{-1}(x_1y_1) = (y^{-1}x^{-1})x_1(yy^{-1})y_1 = (y^{-1}x^{-1}x_1y)(y^{-1}y_1) \in N \ ,$$

dunque

$$xyN = x_1y_1N$$

il risultato non dipende dalla scelta dei rappresentanti delle classi.

(Si provi per esercizio che se N non è normale allora non si può definire una operazione allo stesso modo.)

Teorema 0.3.1 *Sia N un sottogruppo normale del gruppo G, allora l'insieme G/N con l'operazione definita sopra è un gruppo, detto* **Gruppo Quoziente** *(di G modulo N), e si ha*

1) $1_{G/N} = 1_GN = N$;

2) per ogni $xN \in G/N$: $(xN)^{-1} = x^{-1}N$.

Dimostrazione. Siano $aN,\ bN,\ cN \in G/N$, allora:

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN)$$

dunque l'operazione su G/N è associativa.
Per ogni $xN \in G/N$ si ha $N \cdot xN = 1_GN \cdot xN = (1_Gx)N = xN = xN \cdot N$ e

$$(xN)(x^{-1}N) = (xx^{-1})N = 1_GN = N \ ,$$

quindi G/N è un gruppo con elemento identico la classe $1_GN = N$ e tale che $(xN)^{-1} = x^{-1}N$ per ogni elemento $xN \in G/N$.

Osserviamo che se $N \trianglelefteq G$ allora $|G/N| = [G : N]$. In particolare, per il Teorema di Lagrange, se G è un gruppo finito allora *l'ordine di G/N divide l'ordine di G.*

Esempio. Consideriamo il gruppo S_3 ed il suo sottogruppo $A =< \gamma >$ che abbiamo visto essere normale. Allora $S_3/A = \{\ A,\ \tau_1A\ \}$ è un gruppo, il cui elemento identico è A e l'operazione è data da:

$A \circ A = A, \quad A \circ \tau_1 A = \tau_1 A, \quad \tau_1 A \circ A = \tau_1 A, \quad \tau_1 A \circ \tau_1 A = A.$

In *notazione additiva* il simbolo che si usa per l'operazione del gruppo quoziente è ancora $+$; quindi se N è un sottogruppo (normale) di un gruppo additivo A allora

$$\frac{A}{N} = \{\ a + N \mid a \in A\ \}\ ,$$

e per ogni $a, b \in A$

$$(a + N) + (b + N) = (a + b) + N\ ;$$

inoltre $0_{A/N} = 0 + N = N$ e $-(a + N) = -a + N$.

(Si osservi che se N è un sottogruppo di un gruppo commutativo A, allora A/N è un gruppo commutativo.)

Consideriamo il **caso importante** del gruppo $\mathbb{Z}$. Poichè $\mathbb{Z}$ è un gruppo commutativo, ogni suo sottogruppo è normale. Sia $n \geq 1$, allora come abbiamo visto nella sezione precedente:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\ a + n\mathbb{Z} \mid a = 0,\ 1,\ 2,\ \ldots,\ n-1\ \}\ .$$

In quanto quoziente di $\mathbb{Z}$ esso è un gruppo additivo di ordine n che si chiama il **gruppo delle classi resto modulo n**, il cui elemento neutro è $0 + n\mathbb{Z}$. Denoteremo tale gruppo anche con $\mathbb{Z}_n$.

Per comodità, quando non ci siano ambiguità riguardo al modulo n, indicheremo gli elementi di $\mathbb{Z}_n$ (cioè le classi di congruenza modulo n) semplicemente ponendo una linea sopra al rappresentante: $\overline{a}$ invece di $a + n\mathbb{Z}$.

La somma di classi si esegue sommando i rappresentanti (e riducendo poi modulo n). Così, se $n = 7$:

$$\mathbb{Z}_7 = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\ \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6}\ \}\ ;$$

e si ha ad esempio

$$\overline{4} + \overline{5} = \overline{9} = \overline{2} \qquad -\overline{4} = \overline{-4} = \overline{3}$$

$$\overline{4} - [\overline{5} - (\overline{6} + \overline{2})] = \overline{4 - [(5 - (6 + 2)]} = \overline{4 - (-3)} = \overline{7} = \overline{0}\ .$$

Osserviamo che i quozienti di $\mathbb{Z}$ consentono di rispondere affermativamente alla domanda se per ogni naturale $n \geq 1$ esista un gruppo di ordine n (basta prendere $\mathbb{Z}_n$).

Esercizio. Si scriva la tabella di addizione del gruppo $\mathbb{Z}_7$.

Esercizio. Si osservi che, per ogni $n \in \mathbb{N}$, $\mathbb{Z}_n$ è ciclico generato dall'elemento $\overline{1}$. Più in generale, si provi che ogni quoziente di un gruppo ciclico è ciclico.

Omomorfismi

Sia $\phi : G \to G'$ un omomorfismo di gruppi. Denotiamo con $Im(\phi)$ l'immagine della applicazione ϕ, cioè

$$Im(\phi) = \phi(G) = \{\ \phi(x) \mid x \in G\ \}\ .$$

La proposizione seguente completa in un certo senso la Proposizione 9 della Sezione 1.

Proposizione 0.3.2 *Sia* $\phi : G \to G'$ *un omomorfismo di gruppi; allora* $Im(\phi) \leq G'$.

Dimostrazione. Chiaramente $Im(\phi) \neq \emptyset$. Se $a, b \in Im(\phi)$ allora esistono $x, y \in G$ tali che $\phi(x) = a,\ \phi(y) = b$, e quindi

$$ab^{-1} = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in Im(\phi) \ ;$$

per il criterio dei sottogruppi, $Im(\phi) \leq G'$.

Esercizio. Sia $\phi : G \to G'$ un omomorfismo di gruppi; si provi che per ogni $g \in G$ e ogni $z \in \mathbb{Z}$: $\phi(g^z) = (\phi(g))^z$.

Definizione. Sia $\phi : G \to G'$ un omomorfismo di gruppi. Il **nucleo** $Ker(\phi)$ di ϕ è l'insieme degli elementi di G la cui immagine tramite ϕ è l'elemento identico; cioè

$$Ker(\phi) = \{\ x \in G \mid \phi(x) = 1_{G'}\ \} = \phi^{-1}(1_{G'}) \ .$$

Vediamo subito due importanti proprietà del nucleo di un omomorfismo.

Teorema 0.3.3 *Sia* $\phi : G \to G'$ *un omomorfismo di gruppi; allora* $Ker(\phi) \trianglelefteq G$.

Dimostrazione. Innanzi tutto $Ker(\phi) \neq \emptyset$, infatti (Proposizione 9 della sez. 1) $\phi(1_G) = 1_{G'}$ e quindi $1_G \in Ker(\phi)$. Siano $x, y \in Ker(\phi)$, allora

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} = 1_{G'}1_{G'} = 1_{G'}$$

e quindi $xy^{-1} \in Ker(\phi)$; per il criterio dei sottogruppi, $Ker(\phi) \leq G$.
Siano ora $x \in Ker(\phi)$ e $g \in G$, allora

$$\phi(g^{-1}xg) = \phi(g^{-1})\phi(x)\phi(g) = (\phi(g))^{-1}1_{G'}\phi(g) = (\phi(g))^{-1}\phi(g) = 1_{G'}$$

quindi $g^{-1}xg \in Ker(\phi)$ e dunque, per il criterio di normalità, $Ker(\phi) \trianglelefteq G$.

Teorema 0.3.4 *Sia* $\phi : G \to G'$ *un omomorfismo di gruppi; allora* ϕ *è iniettivo se e solo se* $Ker(\phi) = \{1_G\}$.

Dimostrazione. ($\Rightarrow$) Sia ϕ un omomorfismo. Allora $\phi(1_G) = 1_{G'}$, e se ϕ è iniettivo nessun altro elemento di G ha immagine $1_{G'}$; quindi $Ker(\phi) = \{1_G\}$.

($\Leftarrow$) Sia ϕ un omomorfismo tale che $Ker(\phi) = \{1_G\}$, e siano $x, y \in G$ tali che $\phi(x) = \phi(y)$. Allora

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = \phi(x)\phi(x)^{-1} = 1_{G'} \ ,$$

cioè $xy^{-1} \in Ker(\phi)$ e quindi $xy^{-1} = 1_G$ da cui $x = y$; dunque ϕ è iniettivo.

Sia N un sottogruppo normale del gruppo G. Si verifica facilmente che la applicazione

$$\pi : G \to G/N$$

$$g \mapsto gN$$

è un omomorfismo suriettivo di gruppi; si chiama la *proiezione canonica* di G su G/N. Notiamo che

$$g \in \ker(\pi) \quad \Leftrightarrow \quad \pi(g) = 1_{G/N} \quad \Leftrightarrow \quad gN = N \quad \Leftrightarrow \quad g \in N \ ,$$

dunque $Ker(\pi) = N$.

Quest'ultima osservazione, insieme con il Teorema 3, ci consente di affermare che *un sottoinsieme di un gruppo è un sottogruppo normale se e solo se è il nucleo di qualche omomorfismo del gruppo.*

Proveremo ora che se $\phi : G \to G'$ è un omomorfismo di gruppi; allora $G/Ker(\phi)$ è isomorfo a $Im(\phi)$. Si tratta di un fatto molto importante che dedurremo da una versione per omomorfismi del Teorema 2 della prima dispensa.

Sia $\phi : G \to G'$ un omomorfismo di gruppi, sia $K = Ker(\phi)$, e sia $\pi : G \to G/K$ la proiezione canonica. Cominciamo con l'osservare che la relazione $\sim_\phi$ associata alla applicazione ϕ coincide con la relazione $\sim_K$ associata al sottogruppo K ; infatti, per ogni $x, y \in G$:

$$x \sim_K y \quad \Leftrightarrow \quad x^{-1}y \in K \quad \Leftrightarrow \quad \phi(x^{-1}y) = 1_{G'} \quad \Leftrightarrow \quad \phi(x)^{-1}\phi(y) = 1_{G'} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad \phi(x) = \phi(y) \quad \Leftrightarrow \quad x \sim_\phi y \ .$$

Quindi la classe di equivalenza modulo $\sim_\phi$ di un qualunque elemento g di G coincide con la classe laterale gK , e il quoziente G/K coincide con l'insieme quoziente $G/\sim_\phi$. Applicando il Teorema citato alla applicazione ϕ , si ha che esiste un'unica applicazione $\overline{\phi} : G/K \to G'$ tale che $\overline{\phi}$ è iniettiva e $\overline{\phi} \circ \pi = \phi$. Tale $\overline{\phi}$ è definita da, per ogni $gK \in G/K$:

$$\overline{\phi}(gK) = \phi(g) \ ;$$

inoltre $\overline{\phi}(G/K) = Im(\phi)$.
Siano ora $xK, yK \in G/K$, allora

$$\overline{\phi}(xK \cdot yK) = \overline{\phi}(xyK) = \phi(xy) = \phi(x)\phi(y) = \overline{\phi}(xK)\overline{\phi}(yK) \ ,$$

quindi tale $\overline{\phi}$ è un **omomorfismo** iniettivo di gruppi. Abbiamo quindi dimostrato il

Primo Teorema di Omomorfismo per Gruppi. *Sia $\phi : G \to G'$ un omomorfismo di gruppi, $K = Ker(\phi)$, e π la proiezione canonica. di G su G/K. Allora esiste un unico omomorfismo $\overline{\phi} : G/K \to G'$ tale che $\overline{\phi} \circ \pi = \phi$; inoltre $\overline{\phi}$ è iniettivo e $Im(\overline{\phi}) = Im(\phi)$.*

Corollario 0.3.5 *Sia $\phi : G \to G'$ un omomorfismo di gruppi. Allora $\frac{G}{Ker(\phi)} \simeq Im(\phi)$. (in particolare, se ϕ è suriettivo allora $G/Ker(\phi) \simeq G'$.)*

Il seguente esercizio è una prima applicazione di questo risultato, e ne suggerisce la forza.

Esercizio. Sia $\phi : G \to H$ un omomorfismo di gruppi finiti tali che $(|G|, |H|) = 1$. Si provi che ϕ è l'omomorfismo banale, cioè che $\phi(g) = 1_H$ per ogni $g \in G$.

Soluzione. Sia $K = Ker(\phi)$, allora per il Teorema di omomorfismo G/K è isomorfo a $Im(\phi)$; in particolare, $|G/K| = |Im(\phi)|$. Ma, per il Teorema di Lagrange, $|G/K| = [G : K]$ divide $|G|$, e $|Im(\phi)|$ divide $|H|$. Poichè $|G|$ e $|H|$ sono coprimi, deve essere $|G/K| = |Im(\phi)| = 1$, cioè $G = K$ e quindi $\phi(g) = 1_H$ per ogni $g \in G$.

Vediamo un'altra applicazione

Proposizione 0.3.6 *Ogni gruppo ciclico è isomorfo a un quoziente di* $\mathbb{Z}$.

Dimostrazione. Sia $G =< g >$ un gruppo ciclico. Allora la applicazione $\phi : \mathbb{Z} \to G$ definita da, per ogni $z \in \mathbb{Z} \ : \ \phi(z) = g^z$ è un omomorfismo suriettivo di gruppi. Per il Teorema di omomorfismo, G è isomorfo a $\mathbb{Z}/Ker(\phi)$. (si completi il quadro, provando che $Ker(\phi) = n\mathbb{Z}$ se $|G| = n$, e $Ker(\phi) = \{0\}$ se $|G| = \infty$ - in particolare ogni gruppo ciclico infinito è isomorfo a $\mathbb{Z}$.)

Il primo Teorema di omomorfismo è un risultato molto importante. Da un punto di vista concettuale, esso dice che le immagini omomorfe di un gruppo si possono descrivere "all'interno" del gruppo stesso, mediante la descrizione dei suoi quozienti. In questo senso lo abbiamo utilizzato nell'esercizio di sopra. Su un piano pratico può essere utile per provare, mediante la considerazione di opportuni omomorfismi, l'esistenza di determinati quozienti in un gruppo dato. Vediamo un esempio.

Esercizio. Sia $\mathbb{R}^+$ il gruppo moltiplicativo dei numeri reali strettamente maggiori di zero. Si provi che il gruppo moltiplicativo $\mathbb{C}^*$ ha un quoziente isomorfo a $\mathbb{R}^+$.

Soluzione. Dato un numero complesso $z = a + ib$ $(a, b \in \mathbb{R})$, definiamo il modulo di z:

$$|z| = \sqrt{a^2 + b^2} \ .$$

Si verifica facilmente che, per ogni $z,\ z_1 \in \mathbb{C} : \ |zz_1| = |z||z_1|$, che per ogni $a \in \mathbb{R}^+,\ |a| = a$, e che $|z| = 0 \ \Leftrightarrow \ z = 0$. Quindi la applicazione $\mathbb{C}^* \ \to \ \mathbb{R}^+$ che associa ad ogni $z \in \mathbb{C}^*$ il suo modulo è un omomorfismo suriettivo di gruppi. Posto U il nucleo di tale omomorfismo, si ha, per il primo Teorema di omomorfismo, che $\mathbb{C}^*/U$ è isomorfo a $\mathbb{R}^+$.
Per completare, osserviamo che $U = \{ \ z \in \mathbb{C}^* \mid |z| = 1 \ \}$ è l'insieme dei numeri complessi che nel piano complesso stanno sulla circonferenza unitaria con centro l'origine. Gli elementi del quoziente sono le circonferenze con centro l'origine e raggio non nullo.

Esercizio. Si provi che il gruppo additivo $(\mathbb{C}, +)$ ha un quoziente isomorfo al gruppo additivo $(\mathbb{R}, +)$.

Esercizio. Si provi che il gruppo moltiplicativo $\mathbb{C}^*$ ha un quoziente isomorfo al gruppo additivo $(\mathbb{R}, +)$.

Se H, K sono sottoinsiemi di un gruppo G, si pone

$$HK = \{ \ xy \mid x \in H,\ y \in K \ \}.$$

Anche nel caso, che è quello che ci interessa, in cui H e K sono sottogruppi, in generale HK non è un sottogruppo (vedi paragrafo seguente).
Ovviamente, in notazione additiva, invece di HK si scrive $H + K = \{ \ x + y \mid x \in H,\ y \in K \ \}$.

Lemma 0.3.7 *Sia G un gruppo e siano $H \leq G$ e $N \trianglelefteq G$. Allora HN è un sottogruppo di G.*

Dimostrazione. $1_G = 1_G 1_G \in HN$, quindi $HN \neq \emptyset$. Siano ora, $h, h_1 \in H$, $x, x_1 \in N$; poichè N è normale, $h_1(xx_1^{-1})h_1^{-1} \in N$ e quindi

$$(hx)(h_1x_1)^{-1} = hxx_1^{-1}h_1^{-1} = h(h_1^{-1}h_1)xx_1^{-1}h_1^{-1} = (hh_1^{-1})(h_1xx_1^{-1}h_1^{-1}) \in HN$$

quindi $HN \leq G$.

Lemma 0.3.8 *Sia $\phi : G \to G'$ un omomorfismo suriettivo di gruppi. Allora*

1) $H \leq G \quad \Rightarrow \quad \phi(H) \leq G'$;

2) $H \trianglelefteq G \quad \Rightarrow \quad \phi(H) \trianglelefteq G'$;

3) $T \leq G' \quad \Rightarrow \quad \phi^{-1}(T) \leq G$;

4) $T \trianglelefteq G' \quad \Rightarrow \quad \phi^{-1}(T) \trianglelefteq G$.

Dimostrazione. 1) E' simile alla dimostrazione della Proposizione 1, e la lasciamo per esercizio.

2) Sia $H \trianglelefteq G$, allora $\phi(H) \leq G'$ per il punto 1). Siano $a \in \phi(H)$, $b \in G'$. Poichè ϕ è suriettiva, esistono $h \in H$, $g \in G$, tali che $\phi(h) = a$ e $\phi(g) = b$. Essendo $H \trianglelefteq G$ si ha $g^{-1}hg \in H$ e quindi

$$b^{-1}ab = \phi(g^{-1})\phi(h)\phi(g) = \phi(g^{-1}hg) \in \phi(H)$$

dunque $\phi(H) \trianglelefteq G'$.

3) Sia $T \leq G'$ e $\phi^{-1}(T)$ la controimmagine di T. Poichè $1_{G'} \in T$, si ha $1_G \in \phi^{-1}(T)$. Se $x, y \in \phi^{-1}(T)$ allora $\phi(x)$, $\phi(y) \in T$ e quindi $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in T$; dunque $\phi^{-1}(T) \leq G$.

4) Sia $T \trianglelefteq G'$; allora $\phi^{-1}(T) \leq G$ per il punto 3). Siano $x \in \phi^{-1}(T)$, $g \in G$; allora $\phi(x) \in T$ e poichè T è normale in G' ,

$$\phi(g^{-1}xg) = \phi(g^{-1})\phi(x)\phi(g) = \phi(g)^{-1}\phi(x)\phi(g) \in T \ ,$$

dunque $\phi^{-1}(T) \trianglelefteq G$.

Osservazione. Si mostri con un esempio che il punto 2) di questo Lemma non vale in generale se ϕ non è suriettiva; mentre i punti 1), 3), 4) del Lemma valgono anche senza l'ipotesi di suriettività. Tale ipotesi non è tuttavia molto restrittiva: dato un omomorfismo $\phi : G \to G'$, si può sempre definire, poichè $\phi(G)$ è un gruppo, un omomorfismo suriettivo restringendo a $\phi(G)$ il codominio originario di ϕ. Questa osservazione si applica anche al prossimo Teorema che mostra che la struttura dei sottogruppi di una immagine omomorfa (o, che è la stessa cosa, di un quoziente) di un gruppo G si legge a partire dalla struttura dei sottogruppi di G stesso.

Teorema di Corrispondenza. *Sia $\phi : G \to G'$ un omomorfismo suriettivo di gruppi e $N = Ker(\phi)$. Allora ϕ definisce una biezione tra l'insieme dei sottogruppi di G che contengono N e l'insieme di tutti i sottogruppi di G'. Tale corrispondenza conserva inclusioni e normalità.*

Dimostrazione. Poniamo

$$\mathcal{L} = \{ \ H \mid H \leq G \ \text{ e } \ N \leq H \ \}$$

$$\mathcal{S} = \{\ T \mid T \leq G'\ \}\ .$$

Per il punto 1) del Lemma 2 si può definire una applicazione da $\mathcal{L}$ in $\mathcal{S}$ che associa ad ogni elemento di $\mathcal{L}$ la sua immagine tramite ϕ. Definiamo cioè la applicazione

$$\Phi :\ \mathcal{L}\ \rightarrow\ \mathcal{S}$$

$$H \mapsto\ \phi(H)\ .$$

Chiaramente, se $H, H_1 \in \mathcal{L}$ e $H \leq H_1$, allora $\phi(H) \leq \phi(H_1)$, e per il Lemma 2, se $H \in \mathcal{L}$ è normale in G allora $\phi(H) \trianglelefteq G'$.
Rimane dunque da provare che Φ è biettiva. Sia $T \in \mathcal{S}$ e sia $H = \phi^{-1}(T)$. Allora $H \leq G$ per il Lemma 2; inoltre, poichè $1_{G'} \in T$,

$$N = Ker(\phi) = \phi^{-1}(1_{G'}) \subseteq \phi^{-1}(T) = H\ ,$$

quindi $H \in \mathcal{L}$ e, per definizione di controimmagine, $\phi(H) \subseteq T$. Ma poichè ϕ è suriettiva, $\phi(H) = \phi(\phi^{-1}(T)) = T$, infatti se $y \in T$, esiste $g \in G$ tale che $\phi(g) = y$; tale g appartiene a $\phi^{-1}(T) = H$. Quindi Φ è suriettiva.
Siano ora $H, K \in \mathcal{L}$ tali che $\Phi(H) = \Phi(K)$ (cioè $\phi(H) = \phi(K)$). Allora, per ogni $h \in H$ esiste $g \in K$ tale che $\phi(g) = \phi(h)$; quindi $\phi(hg^{-1}) = 1_{G'}$, cioè $hg^{-1} \in Ker(\phi) = N$. Ma $N \subseteq K$ dunque $hg^{-1} \in K$ da cui segue $h \in K$. Quindi $H \subseteq K$. Similmente si prova che $K \subseteq H$. Dunque $H = K$ e la applicazione Φ è iniettiva, concludendo la dimostrazione.

Esercizio. Sia $\phi :\ G\ \rightarrow\ G'$ un omomorfismo suriettivo di gruppi e $N = Ker(\phi)$. Si provi che per ogni $N \leq G$, $\phi^{-1}(\phi(H)) = HN$. Si provi che per ogni $N \leq H \leq G$, $[G : H] = [G' : \phi(H)]$.

Il Teorema di Corrispondenza dice in sostanza che, dato un omomorfismo suriettivo di gruppi, il reticolo dei sottogruppi dell'immagine coincide con il reticolo dei sottogruppi del dominio che contengono il nucleo. Una immediata e importante applicazione riguarda i sottogruppi di un gruppo quoziente.

Teorema 0.3.9 *Sia G un gruppo e $N \trianglelefteq G$. Allora i sottogruppi del gruppo quoziente G/N sono tutti e soli quelli del tipo H/N al variare di H nell'insieme dei sottogruppi di G che contengono N.*

Dimostrazione. Si applica il Teorema di Corrispondenza alla proiezione canonica $\pi : G\ \rightarrow\ G/N$, che è un omomorfismo suriettivo il cui nucleo è N. Quindi i sottogruppi di G/N sono le immagini tramite la proiezione dei sottogruppi H di G tali che $N \leq H$. Ora, se $N \leq H$ possiamo vedere N come sottogruppo di H ; chiaramente $N \trianglelefteq H$, e si ha

$$\pi(H) = \{\ \pi(x) \mid x \in H\ \} = \{\ xN \mid x \in H\ \} = \frac{H}{N}\ .$$

Esempio. Consideriamo il caso di un quoziente $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. I suoi sottogruppi sono in corrispondenza con i sottogruppi $m\mathbb{Z}$ di $\mathbb{Z}$ tali che $m\mathbb{Z} \geq n\mathbb{Z}$. Si dimostri che $m\mathbb{Z} \geq n\mathbb{Z}$ se e solo se $m|n$. Quindi, i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono tutti e soli quelli del tipo

$$\frac{m\mathbb{Z}}{n\mathbb{Z}} = \{\ x + n\mathbb{Z} \mid x \in m\mathbb{Z}\ \} = \{\ mz + n\mathbb{Z} \mid z \in \mathbb{Z}\ \} = \{\ mz + n\mathbb{Z} \mid 0 \leq mz \leq n - 1\ \}$$

con $m|n$.
Ad esempio, sottogruppi di $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$ sono, utilizzando la convenzione di indicare con una barra le classi resto ($a + 12\mathbb{Z} = \overline{a}$):

$$\begin{aligned}
\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{1},\ \overline{2},\ \ldots, \overline{11}\ \}\ ,\\
2\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{2},\ \overline{4},\ \overline{6},\ \overline{8},\ \overline{10}\ \}\ ,\\
3\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{3},\ \overline{6},\ \overline{9}\ \}\ ,\\
4\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{4},\ \overline{8}\ \}\ ,\\
6\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{6}\ \}\ ,\\
12\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0}\ \}\ .
\end{aligned}$$

Secondo Teorema di Omomorfismo. Sia G un gruppo e siano $H \leq G$ e $N \trianglelefteq G$. Allora:

1) $H \cap N \trianglelefteq H$;
2) $\frac{HN}{N} \simeq \frac{H}{H \cap N}$.

Dimostrazione. Consideriamo la restrizione $\eta : H \to G/N$ ad H della proiezione canonica $\pi : G \to G/N$ (quindi $\eta(h) = hN$ per ogni $h \in H$). Allora η è un omomorfismo di gruppi, e

$$Ker(\eta) = \{\ h \in H \mid \eta(h) = 1_{G/N}\ \} = \{\ h \in H \mid hN = N\ \} = \{\ h \in H \mid h \in N\ \} = H \cap N\ ,$$

in particolare, per il Teorema 3, $H \cap N \trianglelefteq H$.
Osserviamo ora che, per il Lemma 1, $HN \leq G$ e che per ogni $h \in H,\ n \in N\ :\ hnN = hN$, infatti $h^{-1}(hn) = n \in N$. Dunque

$$Im(\eta) = \{\ \eta(h) \mid h \in H\ \} = \{\ hN \mid h \in H\ \} = \{\ hnN \mid hn \in HN\ \} = \frac{HN}{N}\ .$$

Quindi, per per il Primo Teorema di Omomorfismo

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}\ .$$

Esempi. 1) Nel gruppo S_3 consideriamo il sottogruppo normale $A = <\gamma>$ ed il sottogruppo $T = \{\iota,\ \tau_1\}$ generato dalla trasposizione τ_1. Allora $S_3 = AT$ e $A \cap T = \{\iota\}$; quindi, per il secondo Teorema di omomorfismo

$$\frac{S_3}{A} = \frac{AT}{A} \simeq \frac{T}{A \cap T} = T\ .$$

(l'isomorfismo da T a S_3/A è dato da $\iota \mapsto A,\ \tau_1 \mapsto \tau_1 A$.)

2) Abbiamo osservato in precedenza che per ogni $n, m \in \mathbb{N}$,

$$n\mathbb{Z} + m\mathbb{Z} = (n,m)\mathbb{Z} \quad \text{e} \quad n\mathbb{Z} \cap m\mathbb{Z} = [n,m]\mathbb{Z}\ .$$

Quindi per il secondo Teorema di omomorfismo

$$\frac{(n,m)\mathbb{Z}}{n\mathbb{Z}} = \frac{n\mathbb{Z} + m\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{m\mathbb{Z}}{n\mathbb{Z} \cap m\mathbb{Z}} = \frac{m\mathbb{Z}}{[n,m]\mathbb{Z}}\ ;$$

(si determini esplicitamente un isomorfismo tra questi due gruppi).
In particolare, se $(n,m) = 1$, $\mathbb{Z}/n\mathbb{Z} \simeq m\mathbb{Z}/nm\mathbb{Z}$; ad esempio $3\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z}$.

Esiste anche un cosiddetto **terzo** teorema di omomorfismo che enunciamo solamente, lasciando la dimostrazione per esercizio.

Teorema 0.3.10 *Siano H, K sottogruppi normali del gruppo G e sia $K \leq H$, allora*

$$\frac{H}{K} \trianglelefteq \frac{G}{K} \qquad e \qquad \frac{G}{H} \simeq \frac{G/K}{H/K} .$$

Ad esempio, se $m|n$ allora

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} .$$

Prodotto di gruppi

Dati due sottoinsiemi A e B di un gruppo G, abbiamo definito *prodotto* di A e di B il sottoinsieme di G

$$AB = \{ab|\ a \in A, b \in B\}$$

Se A e B sono *sottogruppi* di G, il prodotto AB non è necessariamente un sottogruppo, come mostra il seguente esempio.

Esempio Consideriamo in S_3 i sottogruppi $T_1 =< \tau_1 >$ e $T_2 =< \tau_2 >$, dove $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ e $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{pmatrix}$. Allora $AB = \{\iota, \tau_1, \tau_2, \tau_1\tau_2\}$ non è un sottogruppo di G, dato che $\tau_1\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ e quindi $(\tau_1\tau_2)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \notin AB$.

Proposizione 0.3.11 *Siano A, B sottogruppi di un gruppo G. Allora*

AB è un sottogruppo di G se e solo se $AB = BA$.

Dimostrazione. $\Rightarrow$) Supponiamo che AB sia un sottogruppo di G. Sia $x = ba \in BA$, con $b \in B$ e $a \in A$. Allora $b = 1_G b \in AB$ e $a = a1_G \in AB$ e quindi, siccome AB è un sottogruppo, $x \in AB$. Segue $BA \subseteq AB$. Sia, viceversa, $x \in AB$. Allora, sfruttando ancora l'ipotesi $AB \leq G$, $x^{-1} \in AB$ e quindi $x^{-1} = ab$ con $a \in A$ e $b \in B$. Dunque $x = b^{-1}a^{-1} \in BA$ e $AB \subseteq BA$.

$\Leftarrow$) Supponiamo $AB = BA$. Siano $x_1, x_2 \in AB$ con $x_1 = a_1b_1$ e $x_2 = a_2b_2$, $a_1, a_2 \in A$, $b_1, b_2 \in B$. Abbiamo $x_1x_2^{-1} = a_1b_1b_2^{-1}a_2^{-1}$. Osserviamo che $b_1b_2^{-1}a_2^{-1} \in BA = AB$ e quindi $b_1b_2^{-1}a_2^{-1} = a_3b_3$ per opportuni $a_3 \in A$ e $b_3 \in B$. Dunque $x_1x_2^{-1} = a_1a_3b_3 \in AB$ e, dato che AB è non vuoto ($1_G = 1_G1_G \in AB$), AB è un sottogruppo di G.

La condizione di cui sopra e' sicuramente verificata se almeno uno dei due sottogruppi è normale:

Corollario 0.3.12 *Sia $N \trianglelefteq G$. Allora per ogni $B \leq G$, $NB = BN$ e $NB \leq G$.*

Esercizio. Più in generale, se $A, B \leq G$ e $b^{-1}Ab = A$ per ogni $b \in B$, allora $AB \leq G$.

Lemma 0.3.13 *Siano A e B sottogruppi del gruppo G. Allora*

a) *ogni elemento $g \in AB$ si può scrivere in $|A \cap B|$ modi distinti come prodotto di un elemento di A e di un elemento di B;*

b) $|AB||A \cap B| = |A||B|$. *Se G è finito,*

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Dimostrazione. a) Consideriamo l'applicazione $\phi : A \times B \to G$ definita ponendo, per ogni $(a, b) \in A \times B$, $\phi((a, b)) = ab$. Osserviamo che, in generale, ϕ *non* è un omomorfismo. E' immediato osservare che $Im(\phi) = AB$. Sia $g \in AB$, $g = ab$ con $a \in A$ e $b \in B$, e proviamo che $\phi^{-1}(g) = \{(at, t^{-1}b) |\ t \in A \cap B\}$. Infatti $\phi((at, t^{-1}b)) = g$ e se, per $c \in A$ e $d \in B$, $\phi((c, d)) = cd = g = ab$ allora $t = a^{-1}c = bd^{-1} \in A \cap B$ e $c = at$, $b = t^{-1}b$. Quindi $|\phi^{-1}(g)| = |A \cap B|$ ovvero per $|A \cap B|$ coppie distinte $(c, d) \in A \times B$ vale $g = cd$.

b) L'insieme delle controimmagini $\{\phi^{-1}(g)\}$ è una partizione di $A \times B$ e quindi

$$|A \times B| = |A||B| = \Sigma_{g \in AB} |\phi^{-1}(g)| = |AB||A \cap B|.$$

Osservazione. Dal Lemma precedente segue, in particolare, che se $A, B \leq G$ e $A \cap B = \{1_G\}$ allora ogni $g \in AB$ si rappresenta in modo *unico* come prodotto di un elemento di A e di un elemento di B.

Esempio Siano $A =< \gamma >$ e $T =< \tau >$ sottogruppi del gruppo simmetrico S_3, dove $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e τ e' una trasposizione. Per il Corollario, AT è un sottogruppo di S_3, dato che $A \trianglelefteq S_3$. Inoltre, poichè $A \cap T = \{\iota\}$,

$$|AT| = \frac{|A||T|}{|A \cap T|} = 3 \cdot 2 = |S_3|$$

e quindi $AT = S_3$.

Consideriamo ora un tipo di prodotto molto importante, il *prodotto diretto*:

Definizione. Sia G un gruppo e H, K sottogruppi di G. G si dice **prodotto diretto (interno)** di H e K se:

1) $G = HK$;

2) $H, K \trianglelefteq G$;

3) $H \cap K = \{1_G\}$.

In tal caso scriviamo: $G = H \times K$.

Esercizi 1) Sia $G = \{z \in \mathbb{C} |\ z^6 = 1\}$ il gruppo moltiplicativo delle radici seste dell'unità e siano $H = \{z \in \mathbb{C} |\ z^3 = 1\}$ e $K = \{z \in \mathbb{C} |\ z^2 = 1\}$ sottogruppi di G. Provare che $G = H \times K$.
2) Sia $\phi : G \to G_0$ un isomorfismo di gruppi e $H, K \leq G$. Provare che se $G = H \times K$ allora $G_0 = H_0 \times K_0$, con $H_0 = \phi(H)$ e $K_0 = \phi(K)$.

Diamo ora una descrizione alternativa del prodotto diretto di due sottogruppi:

Teorema 0.3.14 *Sia G un gruppo e $H, K \leq G$. Allora $G = H \times K$ se e solo se:*

a) *ogni elemento di G si scrive in uno ed un solo modo come prodotto di un elemento di H e di un elemento di K;*

b) *per ogni $h \in H$, $k \in K$, $hk = kh$.*

Dimostrazione. Sia $G = H \times K$. Poichè $G = HK$, per ogni $g \in G$ esistono $h \in H$, $k \in K$ tali che $g = hk$. Ma $H \cap K = \{1_G\}$ e dunque per il Lemma 4.3 tale scrittura è unica e a) è dimostrata. Siano infine $h \in H$, $k \in K$ e $x = h^{-1}k^{-1}hk$. Siccome $K \trianglelefteq G$, $h^{-1}k^{-1}h \in K$ e quindi $x = (h^{-1}k^{-1}h)k \in K$. Analogamente, dato che $H \trianglelefteq G$, $k^{-1}hk \in H$ e $x = h^{-1}(k^{-1}hk) \in H$. Dunque $x \in H \cap K = \{1_G\}$. Segue $kh = kh1_G = khh^{-1}k^{-1}hk = hk$ e pertanto vale b).
Supponiamo viceversa che valgano a) e b). Se $g \in G$, per a) esistono $h \in H$, $k \in K$ tali che $g = hk$. Quindi $G \subseteq HK$ ovvero $HK = G$. L'unicità di scrittura, per il Lemma 4.3, equivale a $H \cap K = \{1_G\}$. Resta da provare $H, K \trianglelefteq G$. Sia $g \in G$, $g = hk$ con $h \in H$, $k \in K$, e sia $x \in K$. Allora, dato che per b) $xh = hx$, abbiamo $g^{-1}xg = k^{-1}h^{-1}xhk = k^{-1}h^{-1}hxk = k^{-1}xk \in K$. Quindi K è un sottogruppo normale di G. Analogamente si prova che anche H è un sottogruppo normale di G.

Fino a qui abbiamo considerato il prodotto di due sottogruppi di un gruppo. Possiamo ora introdurre un concetto più generale, il prodotto diretto (esterno) di gruppi arbitrari, ovvero non necessariamente contenuti in un comune gruppo "ambiente".
Definizione. Dati i gruppi G_1, G_2 si definisce **prodotto diretto (esterno)** di G_1 e G_2 l'insieme $G_1 \times G_2 = \{(g_1, g_2) |\ g_1 \in G_1,\ g_2 \in G_2\}$ con l'operazione definita ponendo, per $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$,

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$$

Esercizio: Verificare che l'operazione data definisce una struttura di gruppo su $G_1 \times G_2$.

Proposizione 0.3.15 *Sia $G = G_1 \times G_2$ il prodotto diretto esterno dei gruppi G_1 e G_2 e siano*
$H_1 = \{(g_1, 1_{G_2}) |\ g_1 \in G_1\}$ *e* $H_2 = \{(1_{G_1}, g_2) |\ g_2 \in G_2\}$. *Allora :*

1) *H_1 e H_1 sono sottogruppi normali di G ;*

2) *$H_1 \simeq G_1$ e $H_2 \simeq G_2$;*

3) *G è prodotto diretto interno dei sottogruppi H_1 e H_2 .*

Dimostrazione. Siano $\pi_1 : G \to G_1$ e $\pi_2 : G \to G_2$ applicazioni definite ponendo, per $g = (g_1, g_2) \in G$, $\pi_1(g) = g_1$ e $\pi_2(g) = g_2$. Poiche' π_1, π_2 sono omomorfismi (verificare per esercizio), i rispettivi nuclei $Ker(\pi_1) = H_2$ e $Ker(\pi_2) = H_1$ sono sottogruppi normali di G. Inoltre, le restrizioni $\pi_{1|H_1} : H_1 \to G_1$ e $\pi_{2|H_2} : H_2 \to G_2$ sono isomorfismi. La suriettività segue infatti subito dalla definizione dei π_i. Inoltre, $Ker(\pi_{1|H_1}) = H_1 \cap H_2 = \{1_G\}$ e, analogamente, $Ker(\pi_{2|H_2}) = \{1_G\}$ e quindi i π_1 e π_2 sono iniettivi. Dunque 1) e 2) sono provate. Per provare 3) osserviamo che, se $g = (g_1, g_2) \in G$,

$g = (g_1, 1_{G_2})(1_{G_1}, g_2) \in H_1H_2$ e quindi $G = H_1H_2$. Inoltre, per ogni $(g_1, 1_{G_2}) \in H_1$ e $(1_{G_1}, g_2) \in H_2$, vale $(g_1, 1_{G_2})(1_{G_1}, g_2) = (g_1, g_2) = (1_{G_1}, g_2)(g_1, 1_{G_2})$.

Osservazione: Per la Proposizione 4.4, ogni gruppo isomorfo al prodotto diretto esterno di due gruppi è prodotto diretto interno di sottogruppi isomorfi ai gruppi dati. Nel seguito, quindi, parleremo semplicemente di prodotto diretto, tralasciando la distinzione tra i casi interno ed esterno.

Esercizio Siano C_n e C_m gruppi ciclici di ordine rispettivamente n e m. Provare che il prodotto diretto $C_n \times C_m$ è ciclico se e solo se $(n, m) = 1$.

Fino a qui abbiamo considerato prodotti di due gruppi. Più in generale, se $H_1, H_2, \ldots, H_n$ sono sottogruppi di G, possiamo definire il prodotto

$$H_1H_2 \ldots H_n = \{g \in G |\ g = h_1h_2 \ldots h_n \text{ con } h_i \in H_i, i = 1, 2, \ldots, n\}$$

Esercizio Provare che se $H_1, H_2, \ldots, H_n$ sono sottogruppi normali di G allora $H_1H_2 \ldots H_n$ è un sottogruppo di G.

Definiamo ora il prodotto diretto (esterno) di n gruppi, dove n è un qualunque intero positivo.

Definizione Siano $G_1, G_2, \ldots, G_n$ gruppi ($n \in \mathbb{N}_0$). Nell' insieme

$$G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) |\ g_i \in G_i \text{ per } i = 1, 2, \ldots, n\}$$

definiamo una operazione ponendo:

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$$

Rispetto a tale operazione $G_1 \times G_2 \times \ldots \times G_n$ è un gruppo, detto **prodotto diretto (esterno)** dei gruppi $G_1, G_2, \ldots, G_n$.

Osserviamo che, se $G = G_1 \times G_2 \times \ldots \times G_n$, $1_G = (1_{G_1}, 1_{G_2}, \ldots, 1_{G_n})$ e, per ogni $(g_1, g_2, \ldots, g_n) \in G$, $(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$.

Analogamente a quanto visto nella Proposizione 4.4, ogni prodotto diretto esterno è prodotto di opportuni sottogruppi, isomorfi ai fattori "esterni". La dimostrazione del seguente risultato, che omettiamo, è simile a quella della Proposizione 4.4.

Proposizione 0.3.16 *Sia $G = G_1 \times G_2 \times \ldots \times G_n$ il prodotto diretto esterno dei gruppi G_i e sia, per $i = 1, 2, \ldots, n$,*

$$H_i = \{(1_{G_1}, 1_{G_2}, \ldots, g_i, \ldots, 1_{G_n}) |\ g_i \in G_i\}.$$

Allora:

(1) $H_i \trianglelefteq G$

(2) $G = H_1H_2 \ldots H_n$

(3) $H_i \cap H_1H_2 \ldots H_{i-1}H_{i+1} \ldots H_n = \{1_G\}$, *per ogni* $i \in \{1, 2, \ldots, n\}$

(4) $H_i \simeq G_i$, *per ogni* $i \in \{1, 2, \ldots, n\}$.

Definizione. Sia G un gruppo e $H_1, H_2, \ldots, H_n$ sottogruppi di G che verificano le condizioni (1), (2) e (3) della Proposizione 4.6. Allora G si dice **prodotto diretto (interno)** dei sottogruppi $H_1, H_2, \ldots, H_n$.

Osservazioni

1) Nel seguito non distingueremo tra prodotto diretto esterno ed interno e parleremo semplicemente di "prodotto diretto".

2) La condizione (3) non puo' essere indebolita richiedendo semplicemente $H_j \cap H_j = \{1\}$ per ogni $i \neq j$. Sia infatti, ad esempio, $G = C_1 \times C_2$ il prodotto diretto di due gruppi ciclici di ordine 2, $C_1 =< x_1 >$ e $C_2 =< x_2 >$. Il gruppo G, che è abeliano, ha tre sottogruppi normali di ordine 2, $H_1 =< (x_1, 1) >$, $H_2 =< (1, x_2) >$ e $H_3 =< (x_1, x_2) >$. H_1, H_2 e H_3 si intersecano a due a due trivalmente, ma ognuno di essi è contenuto nel prodotto degli altri due, che è G stesso.

3) Nel caso di gruppi in notazione additiva, si usa di solito l'espressione "somma diretta" al posto di "prodotto diretto".

Esempio. Il gruppo additivo $(\mathbb{R}^n, +)$ dello spazio vettoriale $\mathbb{R}^n$ di dimensione n sul campo reale è isomorfo alla somma diretta di n "copie" del gruppo additivo $(\mathbb{R}, +)$.

Automorfismi

Ricordiamo che un **automorfismo** di un gruppo G è un isomorfismo di G in se stesso. Abbiamo osservato (pagina 13) che

L'insieme degli automorfismi di G con l'operazione di composizione è un gruppo.

Tale gruppo, il cui elemento identico è l'identità ι_G, si denota con $Aut(G)$.

Particolari automorfismi di un gruppo G sono i coniugi. Dato $g \in G$, si definisce una applicazione

$$\begin{aligned} \sigma_g : \ G &\to G \\ x &\mapsto g^{-1}xg \end{aligned}$$

che si chiama **coniugio** tramite l'elemento g.

Proposizione 0.3.17 *Sia G un gruppo, allora per ogni $g \in G$, $\sigma_g \in Aut(G)$.*

Dimostrazione. Fiassato $g \in G$, siano $x, y \in G$; allora

$$\sigma_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \sigma_g(x)\sigma_g(y) \ ,$$

quindi σ_g è un omomorfismo. Verifichiamo che è iniettivo; sia $x \in Ker(\sigma_g)$, allora $g^{-1}xg = 1_G$ da cui, moltiplicando a sinistra per g e a destra per g^{-1} si ottiene $x = 1_G$, quindi $Ker(\sigma_g) = \{1_G\}$ e per il Teorema 4 σ_g è iniettiva. Infine, σ_g è suriettiva perchè per ogni $y \in G$, $y = g^{-1}gyg^{-1}g = \sigma_g(gyg^{-1}$. Dunque σ_g è biettiva e quindi un automorfismo di G.

Sia $g \in G$ e $S \subseteq G$. L'immagine di S tramite l'automorfismo σ_G si chiama **coniugato** di S tramite g, e si denota con $g^{-1}Sg$ o, più comodamente, con S^g. Quindi

$$S^g = \{\ g^{-1}xg \mid x \in S\ \} \ .$$

Questo concetto è particolarmente rilevante nel caso in cui S sia un sottogruppo di G. Ad esempio, si provi per esercizio la seguente importante osservazione

Proposizione 0.3.18 *Sia H un sottogruppo del gruppo G. Allora $H \trianglelefteq G$ se e solo se H coincide con tutti i suoi coniugati (cioè $H = H^g$ per ogni $g \in G$).*

Osserviamo che se G è commutativo, allora per ogni $x, g \in G$, $g^{-1}xg = g^{-1}gx = x$. Quindi se G è commutativo ogni coniugazione è l'identità. Le coniugazioni sono quindi rilevanti solo per i gruppi non commutativi, nel qual caso sono gli automorfismi più importanti.
Sia G un gruppo e ϕ un automorfismo di G. L'insieme degli elementi di G che sono mandati in se stessi da ϕ si dice insieme dei **punti fissi** di ϕ. Chiaramente 1_G è un punto fisso per ogni automorfismo; il prossimo Lemma asserisce che l'insieme dei punti fissi è sempre un sottogruppo di G. La dimostrazione è immediata e la lasciamo per esercizio.

Lemma 0.3.19 . *Sia G un gruppo e $\phi \in Aut(G)$; allora l'insieme $\{ x \in G \mid \phi(x) = x \}$ è un sottogruppo di G.*

Sia G un gruppo e $g \in G$. L'insieme degli elementi di G che commutano con g si chiama **centralizzante** di g e si denota con $C_G(g)$. Quindi

$$C_G(g) = \{ x \in G \mid gx = xg \} .$$

Ora, $gx = xg$ se e solo se $x = g^{-1}xg = \sigma_g(x)$. Quindi il centralizzante di g non è altro che l'insieme dei punti fissi di σ_g, dunque per il Lemma precedente,

$$\text{per ogni } g \in G,\ C_G(g) \leq G.$$

(Si dimostri questo fatto direttamente dalla definizione di centralizzante)

Definizione. Sia G un gruppo. Il **centro** di G è l'insieme degli elementi che commutano con tutti gli elementi di G. Esso si denota con $Z(G)$.

Quindi $Z(G) = \{ x \in G \mid xg = gx \text{ per ogni } g \in G \}$, e anche

$$Z(G) = \bigcap_{g \in G} C_G(g) .$$

Chiaramente $1_G \in Z(G)$, e G è commutativo se e solo se $G = Z(G)$.

Esercizio. Si provi che per ogni gruppo G si ha $Z(G) \trianglelefteq G$.

Esercizio. Sia G un gruppo e $x, y \in G$. Si provi che $\sigma_x = \sigma_y$ se e solo se $x^{-1}y \in Z(G)$.

Osserviamo che può bene verificarsi il caso che $Z(G)$ si riduca al sottogruppo banale; ad esempio, verificate che $Z(S_3) = \{\iota\}$.

Il resto di questa sezione è di carattere complementare, ma è una interessante e istruttiva applicazione del Teorema di omomorfismo.

Dato un gruppo G denotiamo con $Inn(G) = \{ \sigma_G \mid g \in G \}$ l'insieme di tutte le coniugazioni di G.

Proposizione 0.3.20 *Sia G un gruppo. Allora $Inn(G) \trianglelefteq Aut(G)$.*

Dimostrazione. Innanzi tutto osserviamo che, per ogni $g, x \in G$,

$$\sigma_{g^{-1}} \circ \sigma_g(x) = \sigma_{g^{-1}}(g^{-1}xg) = gg^{-1}xgg^{-1} = x = \iota_G(x)$$

quindi $\sigma_{g^{-1}} = \sigma_g^{-1}$. Proviamo ora che $Inn(G)$ è un sottogruppo di $Aut(G)$. Abbiamo appena visto che $Inn(G)$ contiene l'inverso di ogni suo elemento. Verifichiamo quindi la chiusura: siano $\sigma_g,\ \sigma_h \in Inn(G)$; allora per ogni $x \in G$,

$$\sigma_g \circ \sigma_h(x) = \sigma_g(h^{-1}xh) = g^{-1}h^{-1}xhg = (hg)^{-1}x(hg)\sigma_{hg}$$

quindi $\sigma_g \circ \sigma_h = \sigma_{hg} \in Inn(G)$. Poichè $\iota_G = \sigma_{1_G} \in Inn(G)$, si ha quindi $Inn(G) \leq Aut(G)$. Verifichiamo ora la normalità. Siano $\sigma_g \in Inn(G)$ e $\phi \in Aut(G)$. Allora, per ogni $x \in G$,

$$\phi^{-1} \circ \sigma_g \circ \phi(x) = \phi^{-1} \circ \sigma_g(\phi(x)) = \phi^{-1}(g^{-1}\phi(x)g) =$$

$$= \phi^{-1}(g^{-1})\phi^{-1}(\phi(x))\phi^{-1}(g) = \phi^{-1}(g)^{-1}x\phi^{-1}(g) = \sigma_{\phi^{-1}(g)} \ ,$$

quindi $\phi^{-1} \circ \sigma_g \circ \phi = \sigma_{\phi^{-1}(g)} \in Inn(G)$. Per il criterio di normalità, $Inn(G) \trianglelefteq Aut(G)$.

Teorema 0.3.21 *Sia G un gruppo. Allora $Inn(G) \simeq G/Z(G)$.*

Dimostrazione. Consideriamo la applicazione

$$\Phi \ : \ G \ \rightarrow \ Inn(G)$$

$$g \mapsto \ \sigma_{g^{-1}}$$

Φ è un omomorfismo di gruppi; infatti dalla dimostrazione della Proposizione precedente segue che, per ogni $g, h \in G$,

$$\Phi(g)\Phi(h) = \sigma_{g^{-1}} \circ \sigma_{h^{-1}} = \sigma_{h^{-1}g^{-1}} = \sigma_{(gh)^{-1}} = \Phi(gh) \ .$$

Ora, $g \in Ker(\Phi)$, se e solo se $\sigma_{g^{-1}} = \iota_G$, se e solo se $gxg^{-1} = x$ per ogni $x \in G$, se e solo se $gx = xg$ per ogni $x \in G$, se e solo se $g \in Z(G)$. Quindi $Ker(\Phi) = Z(G)$. Poichè Φ è suriettiva per definizione di $Inn(G)$, per il primo Teorema di omomorfismo si conclude che

$$\frac{G}{Z(G)} \simeq Inn(G)$$

come si voleva dimostrare.

Esercizio. Si provi che $Aut(S_3) = Inn(S_3) \simeq S_3$.

ESERCIZI

1. Sia G un gruppo tale che $(xy)^3 = x^3y^3$ per ogni $x, y \in G$. Si provi che $\{x^3 \mid x \in G\}$ è un sottogruppo normale di G.

2. Sull'insieme $W = \mathbb{R}^* \times \mathbb{R}$ si definisca una operazione ponendo, per ogni $(a, b), (a_1, b_1) \in W$:

$$(a, b)(a_1, b_1) = (aa_1, ab_1 + b) \ .$$

Si provi che, con tale operazione, W è un gruppo. Si dimostri che $K = \{\ (1, b) \mid b \in \mathbb{R}\ \}$ è un sottogruppo normale, e che $W/K \simeq \mathbb{R}^*$.

3. Siano N, M sottogruppi normali del gruppo G tali che $N \cap M = \{1_G\}$. Si provi che, per ogni $x \in N,\ y \in M$ si ha $xy = yx$.

4. Si provi che per ogni elemento x del gruppo (additivo) $G = \mathbb{Q}/\mathbb{Z}$ esiste un $n \geq 1$ tale che $nx = 0_G$.

5. Sia H un sottogruppo proprio del gruppo additivo dei razionali $\mathbb{Q}$. Si provi che $[\mathbb{Q} : H] = \infty$.

6. Sia $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ il gruppo moltiplicativo delle radici n-esime dell'unità. Si provi che $\mathbb{C}^*/U_n$ è isomorfo a $\mathbb{C}^*$. [Si usi il fatto che per ogni $z \in \mathbb{C}^*$ esiste $a \in \mathbb{C}^*$ tale che $a^n = z$].

7. Sia G un gruppo finito e siano $H, K \leq G$ tali che $|H|^2 > |G|$ e $|K|^2 > |G|$. Si provi che $H \cap K \neq \{1_G\}$.

8. Siano G, N i gruppi definiti nell'esempio a pagina 31. Si provi che $G/N \simeq \mathbb{R}^* \times \mathbb{R}^*$. [Si cominci col trovare un omomorfismo suriettivo da G in $\mathbb{R}^* \times \mathbb{R}^*$.]

9. Sia P l'insieme dei numeri reali strettamente maggiori di 0. Si provi che $\mathbb{R}^* = \{1, -1\} \times P$.

10. Si provi che il gruppo $\mathbb{Z} \times \mathbb{Z}$ non è ciclico.

11. Si determinino tutti i coniugati in S_3 del sottogruppo $T =< \tau_1 >$.

12. Sia G un gruppo e $H \leq G$. Il *normalizzatore* di H in G è l'insieme

$$N_G(H) = \{\ g \in G \mid g^{-1}Hg = H\ \}$$

(si osservi che $H \trianglelefteq G$ se e solo se $N_G(H) = G$). Si dimostri che $H \leq N_G(H) \leq G$.

13. Nel gruppo $G = GL(2, \mathbb{R})$ si determini il centralizzante $C_G(g)$ dell'elemento $g = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$. Si determini quindi $Z(GL(2, \mathbb{R}))$

14. Sia $G =< g >$ un gruppo ciclico.
i) Si provi che se α, β sono omomorfismi di G nel medesimo gruppo H, e $\alpha(g) = \beta(g)$, allora $\alpha = \beta$.
ii) Si provi che per ogni $\psi \in Aut(G)$, $\psi(g)$ è un generatore di G.
iii) Si provi che se $|G| = n$ allora $|Aut(G)| = \phi(n)$, dove ϕ è la funzione di Eulero.

15. Si determini $Aut(\mathbb{Z})$.

0.4 Azioni di Gruppi

Il concetto di azione di un gruppo è molto importante in matematica. Abbiamo visto nelle sezioni precedenti che l'insieme di tutte le permutazioni di un insieme è un gruppo, l'insieme di tutti gli automorfismi di un gruppo è un gruppo, e che l'insieme delle simmetrie di un sistema di punti del piano è un gruppo. Questi gruppi possono essere visti come costituiti dall'insieme delle biezioni che conservano una certa "struttura" (gli automorfismi di un gruppo G sono biezioni che conservano l'operazione, le simmetrie di una figura piana sono biezioni del piano che conservano la figura stessa - che possiamo intendere come una struttura geometrica, le permutazioni semplicemente conservano una struttura "nulla"). Questo è un fenomeno molto generale; un altro esempio è dato dall'insieme di tutti gli automorfismi di uno spazio vettoriale, che costituisce un gruppo. Detto in modo informale, una *azione* di un gruppo G significa un omomorfismo del gruppo G nel gruppo delle biezioni su una certa struttura. Ad esempio, sia V uno spazio vettoriale di dimensione n sui reali e $\mathcal{B}$ una sua base fissata, allora ad ogni matrice quadrata reale invertibile di ordine n si associa una applicazione lineare definita rispetto alla base $\mathcal{B}$, e ciò definisce un isomorfismo del gruppo $GL(n,\mathbb{R})$ nel gruppo $Aut_{\mathbb{R}}(V)$ di tutte le applicazioni lineari invertibili di V in se stesso; questa è una azione di $GL(n,\mathbb{R})$ come gruppo di applicazioni lineari.
In questa sezione studieremo alcuni tipi di azione; come gruppi di permutazioni (si chiamano azioni su un insieme), come gruppi di simmetrie di una figura piana, e come gruppi di automorfismi di un gruppo. Le azioni come gruppi di permutazioni sono in un certo senso quelle fondamentali e sottendono a tutti gli altri tipi di azione; inizieremo quindi con esse. Per prima cosa introdurremo qualche strumento generale per lavorare con i gruppi simmetrici.

Permutazioni

Ricordiamo che, se I è un insieme, si dice *permutazione* su I una qualunque applicazione biunivoca di I in sè e si denota con $Sym(I)$ il gruppo, rispetto alla composizione, delle permutazioni su I. Se I e J sono due insiemi della stessa cardinalità, allora $Sym(I) \simeq Sym(J)$. Se I è un insieme finito di n elementi possiamo quindi assumere che sia $I = \{1, 2, \ldots, n\}$. Di solito, invece di $Sym(\{1, 2, \ldots, n\})$, viene usato il simbolo S_n.
Ogni $\pi \in S_n$ può essere rappresentata nel modo seguente:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(i) & \ldots & \pi(n) \end{pmatrix}$$

Esiste però una rappresentazione per molti aspetti più conveniente:

Esempio. Sia $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 7 & 6 \end{pmatrix} \in S_7$. Osserviamo che $\pi(1) = 3$, $\pi(3) = 5$ e $\pi(5) = 1$ ovvero $1 \xrightarrow{\pi} 3 \xrightarrow{\pi} 5 \xrightarrow{\pi} 1$. Inoltre, $2 \xrightarrow{\pi} 2$, $4 \xrightarrow{\pi} 4$ e $6 \xrightarrow{\pi} 7 \xrightarrow{\pi} 6$. Scriviamo allora

$\pi = (1\ 3\ 5)(6\ 7)$.

Cominciamo introducendo il concetto di *permutazione ciclica* (o *ciclo*) :

Definizione. ¡: Una permutazione $\sigma \in S_n$ si dice un **ciclo di lunghezza k** (o un **k-ciclo**), per k intero, $k > 1$, se esiste un sottoinsieme di ordine k $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ tale che

(a) $\pi(i_1) = i_2$, $\pi(i_2) = i_3$, ..., $\pi(i_{k-1}) = i_k$, $\pi(i_k) = i_1$;

(b) $\pi(j) = j$ per ogni $j \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$.

Scriviamo allora

$$\sigma = (i_1\ i_2\ \ldots\ i_k).$$

Osservazioni. 1) Se σ è un k-ciclo, $\sigma = (i_1\ i_2\ \ldots\ i_k)$, possiamo anche scrivere in modo equivalente

$$\sigma = (i_2\ i_3\ \ldots\ i_k\ i_1) = (i_3\ i_4\ \ldots\ i_k\ i_1\ i_2) = \ \ldots.$$

2) Se $\sigma = (i_1\ i_2\ \ldots\ i_k)$ è un k-ciclo, allora $\sigma^2(i_1) = i_3$, $\sigma^2(i_2) = i_4$, ..., $\sigma^2(i_k) = i_2$ e, più in generale, per $1 \leq r \leq k$

$$\sigma^r(i_j) = i_{j+r} \ \ se\ \ j + r \leq k$$

$$\sigma^r(i_j) = i_{j+r-k} \ \ se\ \ j + r > k\ .$$

Notazione. A differenza di quanto convenuto per le applicazioni, da questo momento scriveremo le permutazioni *a destra* degli elementi cui vengono applicate e cambieremo di conseguenza anche la notazione della composizione di due permutazioni. Se $\sigma_1, \sigma_2 \in S_n$ e $i \in \{1, 2, \ldots, n\}$, denoteremo con $i\sigma_1$ l'immagine di i tramite σ_1 e con $\sigma_1\sigma_2$ la permutazione ottenuta componendo *prima* σ_1 e *poi* σ_2. Pertanto, per ogni $i \in \{1, 2, \ldots, n\}$, $i\sigma_1\sigma_2 = (i\sigma_1)\sigma_2$.

Esempio. Consideriamo in S_5 le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} \ \ e\ \ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

α è un 3-ciclo, $\alpha = (2\ 4\ 3)$, e β è un 2-ciclo, $\beta = (1\ 3)$. La composizione $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$ è un 4-ciclo: $\alpha\beta = (1\ 3\ 2\ 4)$.

Definizione. Data una permutazione $\pi \in S_n$, si dice **supporto** di π l'insieme

$$supp(\pi) = \{i |\ i \in \{1, 2, \ldots, n\},\ \ i\pi \neq i\ \}$$

degli elementi "mossi" dalla π.

Esempi. 1) Se $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix} \in S_7$, $supp(\pi) = \{1, 2, 4, 6\}$.
2)Se $\sigma = (i_1\ i_2\ \ldots\ i_k)$ è un k-ciclo ($k > 1$), allora $supp(\sigma) = \{i_1, i_2, \ldots, i_k\}$.

Se $\sigma = \iota$, $supp(\sigma) = \emptyset$.

Osserviamo che, come segue subito dalla definizione, per ogni permutazione π vale

$$supp(\pi^{-1}) = supp(\pi) \ .$$

Definizione. Due cicli $\sigma_1, \sigma_2 \in S_n$ si dicono **disgiunti** se $supp(\sigma_1) \cap supp(\sigma_2) = \emptyset$.

Proposizione 0.4.1 *1) Se $\sigma = (i_1\ i_2\ \ldots\ i_k)$ allora $\sigma^{-1} = (i_k\ i_{k-1}\ \ldots\ i_1)$.*
2) Se σ e' un k-ciclo, allora $|\sigma| = k$.
3) Se σ_1, σ_2 sono cicli disgiunti, allora sono permutabili : $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Dimostrazione. 1) Sia $\tau = (i_k\ i_{k-1}\ \ldots\ i_1)$. Se $j \notin \{i_1, i_2, \ldots, i_k\}$ chiaramente $j\sigma\tau = j = j\tau\sigma$. Se $j \in \{i_1, i_2, \ldots, i_k\}$, si verifica immediatamente che vale ancora $j\sigma\tau = j = j\tau\sigma$.
2) Se σ e' un k-ciclo, allora $\sigma^k = \iota$. D'altra parte, se h e' un intero positivo, $h < k$, abbiamo $i_1\sigma^h = i_{h+1}$, dato che $h + 1 \leq k$. Quindi $i_1\sigma \neq i_1$ e $\sigma^h \neq \iota$.
3) Siano $\sigma_1, \sigma_2 \in S_n$ tali che $supp(\sigma_1) \cap supp(\sigma_2) = \emptyset$ e sia $j \in \{1, 2, \ldots, n\}$. Se $j \notin supp(\sigma_1) \cup supp(\sigma_2)$, allora $j\sigma_1\sigma_2 = j = j\sigma_2\sigma_1$. Se $j \in supp(\sigma_1)$ e $i = j\sigma_1$, allora $i \in supp(\sigma_1)$ e dunque $i, j \notin supp(\sigma_2)$. Quindi $j\sigma_1\sigma_2 = i\sigma_2 = i = j\sigma_1 = j\sigma_2\sigma_1$. Se $j \in supp(\sigma_2)$ si procede analogamente. Dunque $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Teorema 0.4.2 *Ogni permutazione $\pi \in S_n$, $\pi \neq \iota$, si può esprimere come prodotto*

$$\pi = \sigma_1\sigma_2 \ldots \sigma_t$$

di cicli disgiunti $\sigma_1, \sigma_2, \ldots, \sigma_t \in S_n$. Tale decomposizione è unica, a meno dell'ordine dei fattori.

Dimostrazione. Procediamo per induzione sull'ordine di $supp(\pi)$. Scegliamo $i \in supp(\pi)$ e sia $J = \{i\pi^m |\ m$ intero positivo $\}$. Poichè $J \subseteq \{1, 2, \ldots, n\}$, esistono sicuramente due interi positivi a e b, $b > a$, tali che $i\pi^b = i\pi^a$ e quindi $i\pi^{b-a} = i$. Denotiamo con k il minimo dell'insieme $\{h |\ h \in \mathbb{N}_0, i\pi^h = i\}$, non vuoto per quanto appena osservato, e siano $i_1 = i$, $i_2 = i\pi$, $\ldots$, $i_k = i\pi^{k-1}$. Dunque $J = \{i_1, i_2, \ldots, i_k\}$ e, considerando il k-ciclo $\sigma = (i_1\ i_2\ \ldots\ i_k)$, abbiamo $j\sigma^{-1}\pi = j$ per ogni $j \in J$. Quindi $supp(\sigma^{-1}\pi) = supp(\pi) \setminus J$. Se $\sigma^{-1}\pi = \iota$ allora $\pi = \sigma$ è un ciclo. Altrimenti, applicando l'ipotesi di induzione, abbiamo $\sigma^{-1}\pi = \sigma_2\sigma_3 \ldots \sigma_t$ con $\sigma_2, \sigma_3, \ldots, \sigma_t \in S_n$ cicli disgiunti. Dunque $\pi = \sigma\sigma_2 \ldots \sigma_t$ è prodotto di cicli disgiunti, dato che $supp(\sigma) = J$ e $supp(\sigma_u) \subseteq supp(\pi) \setminus J$ per ogni $2 \leq u \leq t$. Supponiamo infine che $\pi = \sigma_1\sigma_2 \ldots \sigma_t$ e $\pi = \tau_1\tau_2 \ldots \tau_u$ siano due decomposizioni di π in prodotto di cicli disgiunti e sia $i \in supp(\sigma_1)$. Poiche', in particolare, $i \in supp(\pi)$, esiste un τ_j per cui $i \in supp(\tau_j)$. Dato che le τ_j sono permutabili, possiamo supporre $i \in supp(\tau_1)$. Allora, come si verifica facilmente, deve essere $\sigma_1 = \tau_1$. Dunque, procedendo per induzione come sopra, segue $t = u$ e $\sigma_j = \tau_j$ per ogni $1 \leq j \leq t$.

Esercizio. Sia $\pi = \sigma_1\sigma_2 \ldots \sigma_t$ con σ_i k_i-cicli disgiunti, per $1 \leq i \leq t$.
Provare che $supp(\pi) = \bigcup_{i=1}^{t} supp(\sigma_i)$ e che $|\pi| = m.c.m(k_1, k_2, \ldots, k_i)$.

Vediamo ora come la decomposizione in cicli fornisca un semplice criterio per stabilire se due permutazioni in S_n sono coniugate. Premettiamo una definizione:

Definizione. Siano $\pi, \rho \in S_n$. Diciamo che π e ρ hanno lo stesso **tipo ciclico** se, date le decomposizioni $\pi = \sigma_1\sigma_2 \dots \sigma_t$ e $\rho = \tau_1\tau_2 \dots \tau_u$ in prodotto di cicli disgiunti, vale $t = u$ e, a meno di rinumerazione, σ_i e τ_i sono cicli della stessa lunghezza, per ogni $1 \leq i \leq t$.

Ad esempio, le permutazioni (1 2)(3 5 4)(6 7) e (1 3 2)(4 6)(5 7) hanno lo stesso tipo ciclico.

Lemma 0.4.3 *1) Sia $\sigma = (i_1\ i_2\ \dots\ i_k)$ un k-ciclo in S_n e $\pi \in S_n$. Allora $\pi^{-1}\sigma\pi = (i_1\pi\ i_2\pi\ \dots\ i_k\pi)$.*
2) Se $\gamma, \pi \in S_n$ e $\gamma = \sigma_1\sigma_2 \dots \sigma_t$ è la decomposizione in prodotto di cicli disgiunti di γ, allora $\pi^{-1}\gamma\pi = (\pi^{-1}\sigma_1\pi)(\pi^{-1}\sigma_2\pi) \dots (\pi^{-1}\sigma_t\pi)$ è la decomposizione in prodotto di cicli disgiunti della coniugata $\pi^{-1}\gamma\pi$.

Dimostrazione. 1) Osserviamo che $supp(\pi^{-1}\sigma\pi) = supp(\sigma)\pi$. Infatti, per $j \in \{1, 2, \dots, n\}$, vale $j = j(\pi^{-1}\sigma\pi)$ se e solo se $j\pi^{-1} = j\pi^{-1}\sigma$ ovvero $j\pi^{-1} \notin supp(\sigma)$ cioe' $j \notin supp(\sigma)\pi$. Per $j < k$, $(i_j\pi)(\pi^{-1}\sigma\pi) = i_j\sigma\pi = i_{j+1}\pi$. Inoltre, $(i_k\pi)(\pi^{-1}\sigma\pi) = i_k\sigma\pi = i_1\pi$. Dunque $\pi^{-1}\sigma\pi$ è il k-ciclo $(i_1\pi\ i_2\pi\ \dots\ i_k\pi)$. La 2) segue da 1), osservando che la $supp(\pi^{-1}\sigma_i\pi) \cap supp(\pi^{-1}\sigma_j\pi) = supp(\sigma_i)\pi \cap supp(\sigma_j)\pi = \emptyset$ per ogni $i \neq j$, $1 \leq i, j \leq t$.

Esempio. Consideriamo in S_6 gli elementi $\pi = (1\ 2\ 3\ 4\ 5)$ e $\gamma = (1\ 3)(2\ 5\ 4\ 6)$. Allora $\pi^{-1}\gamma\pi = (2\ 4)(3\ 1\ 5\ 6)$.

Proposizione 0.4.4 *Due permutazioni γ e δ sono coniugate in S_n se e solo se hanno lo stesso tipo ciclico.*

Dimostrazione. Supponiamo che, per $\pi \in S_n$, sia $\delta = \pi^{-1}\gamma\pi$. Allora per il Lemma 4.3, γ e δ hanno lo stesso tipo ciclico.
Supponiamo viceversa che γ e δ abbiano lo stesso tipo ciclico. Sia $\gamma = (a_1\ a_2\ \dots\ a_h)(b_1\ b_2\ \dots\ b_k)\dots$ e $\delta = (\hat{a}_1\ \hat{a}_2\ \dots\ \hat{a}_h)(\hat{b}_1\ \hat{b}_2\ \dots\ \hat{b}_k)\dots$ e siano $\{f_1, f_2, \dots, f_m\} = \{1, 2, \dots, n\} \setminus supp(\gamma)$ e $\{\hat{f}_1, \hat{f}_2, \dots, \hat{f}_{\hat{m}}\} = \{1, 2, \dots, n\} \setminus supp(\delta)$ gli insiemi degli elementi fissati γ e δ rispettivamente. Osserviamo che $m = \hat{m}$, poiche' $|supp(\gamma)| = |supp(\delta)|$. Consideriamo quindi la permutazione

$$\pi = \begin{pmatrix} a_1 & a_2 & \dots & a_h & b_1 & b_2 & \dots & b_k & \dots & f_1 & f_2 & \dots & f_m \\ \hat{a}_1 & \hat{a}_2 & \dots & \hat{a}_h & \hat{b}_1 & \hat{b}_2 & \dots & \hat{b}_k & \dots & \hat{f}_1 & \hat{f}_2 & \dots & \hat{f}_m \end{pmatrix}.$$

Per il Lemma 4.3 segue allora $\delta = \pi^{-1}\gamma\pi$.

Prendiamo ora in considerazione un altro modo di decomporre una permutazione in prodotto di cicli. Questa volta i fattori ciclici avranno tutti lunghezza 2, ma non più, in generale, supporti disgiunti.

Definizione. Un ciclo di lunghezza 2 si dice **trasposizione**.

Lemma 0.4.5 *Ogni ciclo di lunghezza k si può esprimere come prodotto di $k-1$ trasposizioni.*

Dimostrazione. Vale infatti $(i_1\ i_2\ \dots\ i_k) = (i_1\ i_2)(i_1\ i_3)\dots(i_1\ i_k)$, come si verifica facilmente per induzione su k.

Osserviamo come la decomposizione in prodotto di cicli di lunghezza due del lemma precedente *non* sia più però costituita da cicli *disgiunti*. Anche l'unicità di decomposizione viene a cadere: in S_4, ad esempio $(1\ 2\ 3) = (1\ 2)(1\ 3) = (1\ 2)(4\ 3)(1\ 3)(1\ 4)$. Inoltre, $(1\ 2)(1\ 3) \neq (1\ 3)(1\ 2)$.

Corollario. *Ogni permutazione $\pi \in S_n$, $\pi \neq \iota$, si può scrivere come prodotto di trasposizioni. Dunque*

$$S_n = < \{\tau |\ \tau \in S_n,\ \tau \ \text{ trasposizione } \} > .$$

Esercizio. Provare che, dati $a, b, c \in \{1, 2, \dots, n\}$, vale $(b\ c) = (a\ b)(a\ c)(a\ b)$ in S_n. Provare quindi che

$$S_n = < (1\ 2), (1\ 3), \dots, (1\ n) > .$$

Tutte le decomposizioni di una data permutazione in prodotto di trasposizioni hanno una proprietà in comune, la *parità* del numero di fattori:

Proposizione 0.4.6 *Sia $\pi \in S_n$ e siano*

$$\pi = \tau_1\tau_2\dots\tau_n = \theta_1\theta_2\dots\theta_m$$

due decomposizioni di π come prodotto di trasposizioni $\tau_i, \theta_j \in S_n$.
Allora $n \equiv m (mod\ \ 2)$, ovvero n è pari (risp. dispari) se e solo se m è pari (risp. dispari).

Dimostrazione. Supponiamo, per assurdo, che sia $\pi = \tau_1\tau_2\dots\tau_n = \theta_1\theta_2\dots\theta_m$ con τ_i, θ_j trasposizioni e n pari, m dispari. Allora $\iota = \tau_1\dots\tau_n\theta_m^{-1}\dots\theta_1^{-1} = \tau_1\dots\tau_n\theta_m\dots\theta_1$ ovvero l'identità ι di S_n si decompone nel prodotto di un numero dispari di trasposizioni. Sia d il minimo intero positivo dispari per cui valga

$$\iota = \gamma_1\gamma_2\dots\gamma_d \tag{1}$$

con γ_i trasposizioni e sia $a \in \{1, 2, \dots, n\}$ un elemento "mosso" da almeno una γ_i. Chiaramente γ_i commuta con ogni γ_j tale che $|supp(\gamma_i) \cap supp(\gamma_j)| = 0, 2$ e inoltre, come è facile verificare, per ogni $b, c \in \{1, 2, \dots, n\}$ vale $(a\ b)(b\ c) = (b\ c)(a\ c)$.
Possiamo dunque trasformare la decomposizione (1) in

$$\iota = \delta_1\delta_2\dots\delta_t\beta_1\beta_2\dots\beta_v \tag{2}$$

con $t + v = d$, $a \notin supp(\delta_i)$ e $\beta_j = (a\ b_j)$, $b_j \in \{1, 2, \dots, n\}$, per ogni $1 \leq i \leq t$, $1 \leq j \leq v$. Osserviamo ora che se gli elementi b_j sono tutti distinti, allora $\beta_1\beta_2\dots\beta_v = (a\ b_1)(a\ b_2)\dots(a\ b_v) = (a\ b_1\ b_2\ \dots\ b_v)$ e quindi $a\beta_1\beta_2\dots\beta_v = b_1 \neq a$. Ma $\beta_1\beta_2\dots\beta_v = (\delta_1\delta_2\dots\delta_t)^{-1} = \delta_t\delta_{t-1}\dots\delta_1$ e $a\delta_t\delta_{t-1}\dots\delta_1 = a$, contraddizione. Esistono quindi $1 \leq$

$r, s \leq v$, $r \neq s$, tali che $b_r = b_s = b$. Poichè, per ogni $c \in \{1, 2, \ldots, n\}$, $(a\ b)(a\ c) = (b\ c)(a\ b)$ possiamo trasformare la (2) in

$$\iota = \delta_1\delta_2 \ldots \delta_t\delta_{t+1} \ldots \delta_{d-2}(a\ b)(a\ b) = \delta_1\delta_2 \ldots \delta_{d-2}$$

contraddicendo la minimalità di d.

In virtù del risultato precedente è ben posta la seguente

Definizione. Una permutazione si dice **pari** (risp. **dispari**) se si può scrivere come prodotto di un numero pari (risp. dispari) di trasposizioni.

Proposizione 0.4.7 *L'applicazione* $sgn : S_n \to \{+1, -1\}$ *definita ponendo, per ogni* $\pi \in S_n$,

$$sgn(\pi) = \begin{cases} +1 & \textit{se } \pi \textit{ e' pari} \\ -1 & \textit{se } \pi \textit{ è dispari} \end{cases}$$

è, per ogni $n > 1$, *un omomorfismo suriettivo del gruppo simmetrico* S_n *nel gruppo moltiplicativo* $\{+1, -1\}$. *(*$sgn(\pi)$ *si dice* **segno** *della permutazione* π*).*

Dimostrazione. Date $\pi_1, \pi_2 \in S_n$, scriviamo $\pi_1 = \alpha_1\alpha_2 \ldots \alpha_{n_1}$, $\pi_2 = \beta_1\beta_2 \ldots \beta_{n_2}$ con α_i, β_j trasposizioni. Allora $sgn(\pi_1) = (-1)^{n_1}$, $sgn(\pi_2) = (-1)^{n_2}$ e

$$sgn(\pi_1\pi_2) = sgn(\alpha_1\alpha_2 \ldots \alpha_{n_1}\beta_1\beta_2 \ldots \beta_{n_2}) = (-1)^{n_1+n_2} = sgn(\pi_1)sgn(\pi_2).$$

La suriettività segue osservando, ad esempio, che $sgn(\iota) = 1$ e $sgn((1\ 2)) = -1$.

Definizione. Denotiamo con

$$A_n = \{\pi \in S_n | \ \pi \text{ è pari}\}$$

l'insieme delle permutazioni pari di S_n. Per la Proposizione 4.7, A_n è un sottogruppo normale di S_n, detto **gruppo alterno** su n oggetti.

Enunciamo, senza dimostrazione, il seguente fondamentale risultato:

Teorema 0.4.8 *Il gruppo alterno* A_n *è semplice per ogni* $n \geq 5$.

Concludiamo mostrando che ogni gruppo finito si può immergere in un gruppo simmetrico :

Teorema (Cayley). *Sia* G *un gruppo finito di ordine* n. *Allora* G *è isomorfo ad un sottogruppo del gruppo simmetrico* S_n.

Dimostrazione. Siano, tramite opportuna numerazione, $g_1, g_2, \ldots g_n$ gli elementi del gruppo G. Fissato un elemento $g \in G$, consideriamo l'applicazione $\phi_g : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ definita ponendo, per ogni $i \in \{1, 2, \ldots, n\}$, $\phi(i) = j$ se vale $gg_i = g_j$.

Dato che, per ogni $j \in \{1, 2, \ldots, n\}$, $gg_i = g_j$ se e solo se $g_i = g^{-1}g_j$, l'applicazione ϕ_g è biettiva ovvero $\phi_g \in S_n$. Sia quindi $\omega : G \to S_n$ definita, per ogni $g \in G$, da $\omega(g) = \phi_g$. Verifichiamo che ω è un omomorfismo: per $g, h \in G$, $i \in \{1, 2, \ldots, n\}$,

$$g_{\phi_{gh}(i)} = (gh)g_i = g(hg_i) = g(g_{\phi_h(i)}) = g_{\phi_g(\phi_h(i))}$$

e quindi $\phi_{gh} = \phi_g \circ \phi_h$.
Infine, ω è iniettiva: se $\phi_g = \phi_h$ allora, per ogni $i \in \{1, 2, \ldots, n\}$, $gg_i = hg_i$ e quindi $g = h$. Dunque G è isomorfo al sottogruppo $\omega(G)$ di S_n.

Abbiamo dimostrato questo Teorema per un gruppo finito, perchè in questo caso il legame con le permutazioni è particolarmente trasparente. Tuttavia il teorema di Cayley vale per qualunque gruppo. Se il gruppo G in questione è infinito, non si può in generale "enumerare" gli elementi di G, come abbiamo fatto nel caso finito; allora si prende come insieme su cui definire le permutazioni, il gruppo G stesso. La dimostrazione la suggeriamo mediante una coppia di esercizi.

Teorema di Cayley. *Sia G un gruppo. Allora G è isomorfo ad un sottogruppo del gruppo simmetrico $Sym(G)$.*

Dimostrazione. Sia G un gruppo.
1) Si provi che per ogni $g \in G$ la applicazione

$$\begin{array}{rccc} \rho_g : & G & \to & G \\ & x & \mapsto & gx \end{array}$$

è una permuatzione di G.
2) Si provi che la applicazione

$$\begin{array}{rccc} \Phi : & G & \to & Sym(G) \\ & x & \mapsto & \rho_g \end{array}$$

è un omomorfismo iniettivo del gruppo G nel gruppo $Sym(G)$. Da ciò si conclude che $G \simeq \Phi(G) \leq Sym(G)$.

ESERCIZI

1. Siano I, J insiemi tali che $|I| = |J|$. Provare che $Sym(I) \simeq Sym(J)$.

2. Date le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 2 & 6 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$$

scrivere α, β, $\alpha\beta$, $\beta\alpha$, $\beta^{-1}\alpha\beta$ e $\alpha^{-1}\beta\alpha$ come prodotto di cicli disgiunti.

3. Scrivere la permutazione $\pi = (1\ 2\ 3)(2\ 4\ 5)(3\ 2\ 4)(1\ 2\ 5)$ come prodotto di cicli disgiunti e come prodotto di trasposizioni. Dire se π appartiene al gruppo alterno A_5.

4. Determinare il numero dei coniugati della permutazione

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

nel gruppo simmetrico S_5.

5. Determinare il massimo ordine di un elemento nei seguenti gruppi:
a) S_7 ; b) S_{10} ; c) A_{10} .

6. Scrivere gli elementi del gruppo alterno A_4.

7. Determinare un sottogruppo del gruppo simmetrico S_8 isomorfo al gruppo Q dei quaternioni.

Azioni di un gruppo su un insieme

Definizione. Sia G un gruppo e S un insieme non vuoto. Una **azione** di G su S è un omomorfismo

$$\Phi \ : \ G \ \to \ Sym(S)$$

di G nel gruppo delle permutazioni di S (e si dice che G *opera* su S).

Se un tale omomorfismo è iniettivo l'azione si dice *fedele*. In tal caso l'immagine $\Phi(G)$ è un sottogruppo di $Sym(S)$ isomorfo a G; si dice in questo caso che G è un *gruppo di permutazioni* su S (e si identifica G con $\Phi(G)$).
Ad esempio, il Teorema di Cayley descrive una azione fedele di un gruppo G su se stesso.

Se $\Phi : \ G \ \to \ Sym(X)$ è una azione di G su S, allora, per ogni $g \in G$ e ogni $s \in S$ si scrive

$$g \cdot s = \phi(g)(s) \ .$$

Si hanno quindi le seguenti proprietà, per ogni $g, h \in G$ e ogni $s \in S$:

$$(gh) \cdot s = g \cdot (h \cdot s) \ , \qquad 1_G \cdot s = s \ .$$

Questa notazione suggerisce un altro modo per definire il concetto di azione di un gruppo su un insieme. Se G è un gruppo e S un insieme, una azione di G su S è una applicazione

$$\begin{array}{ccc} G \times S & \to & S \\ (g, s) & \mapsto & g \cdot s \end{array}$$

tale che per ogni per ogni $g, h \in G$ e ogni $s \in S$, $(gh) \cdot s = g \cdot (h \cdot s)$ e $1_G \cdot s = s$.
Allora, per ogni $g \in G$ la applicazione

$$\begin{array}{rccc} \phi(g) : & S & \to & S \\ & s & \mapsto & g \cdot s \end{array}$$

è una biezione di S, e (lo si verifichi per esercizio) la applicazione che associa ad ogni $g \in G$ la permutazione $\phi(g)$ è un omomorfismo di G in $Sym(S)$.

Esempio. Su $G = \mathbb{R}^* \times \mathbb{R}$ si definisca una operazione ponendo, per ogni $(a,b),(c,d) \in G$

$$(a,b)(c,d) = (ac, ad+b) \ .$$

Si verifichi che, rispetto a tale operazione, G è un gruppo con elemento identico $(1,0)$. Ora, la regola

$$(a,b) \cdot s = as + b$$

per ogni $(a,b) \in G$ e ogni $s \in \mathbb{R}$, definisce una azione del gruppo G sull'insieme $\mathbb{R}$. Infatti, per ogni $s \in \mathbb{R}$:

$$1_G \cdot s = (1,0) \cdot s = 1s + 0 = s$$

e, per ogni $(a,b),(c,d) \in G$:

$$(a,b) \cdot ((c,d)) \cdot s) = (a,b) \cdot (cs+d) = a(cs+d)+b = acs+ad+b = (ac, ad+b) \cdot s = ((a,b)(c,d)) \cdot s.$$

Supponiamo di avere data una azione del gruppo G sull'insieme S. Per ogni $s \in S$ si definiscono:

- l'**orbita** $O_G(s)$ di s (rispetto alla azione di G)

$$O_G(s) = \{ \ g \cdot s \mid g \in G \ \} \ ,$$

ovvero l'insieme dei trasformati di s tramite tutti gli elementi di G.

- lo **stabilizzatore** G_s (o anche $Stab_G(s)$) di s in G:

$$G_s = \{ \ g \in G \mid g \cdot s = s \ \}$$

ovvero l'insieme degli elementi di G la cui corrispondente permutazione fissa s.

Definizione. Una azione si dice **transitiva** se esiste $s \in S$ tale che $O_G(s) = S$; ciò avviene se per ogni $t \in S$ esiste $g \in G$ tale che $g \cdot s = t$.

Ad esempio, l'azione descritta nell'esempio di sopra è transitiva: infatti, per ogni $a \in \mathbb{R}$: $(a,0) \cdot 1 = a1 + 0 = a$ se $a \neq 0$, e $(1,-1) \cdot 1 = 1 \cdot 1 + (-1) = 0$; quindi $O_G(1) = \mathbb{R}$. Calcoliamo lo stabilizzatore di un punto $s \in \mathbb{R}$. Sia $(a,b) \in G$; allora $(a,b) \in G_s$ se e solo se $s = (a,b) \cdot s = as+b$, se e solo se $b = s - as$; quindi $G_s = \{ \ (a, s-as) \mid : a \in \mathbb{R}^* \ \}$ (ad esempio, $G_1 = \{ \ (a, 1-a) \mid a \in \mathbb{R}^* \ \}$).

Esercizio Si provi che una azione di un gruppo G su un insieme S è transitiva se e solo se $O_G(x) = S$ per ogni $x \in S$.

Proposizione 0.4.9 *Sia data una azione del gruppo G sull'insieme S. Allora l'insieme delle orbite è una partizione di S.*

Dimostrazione. Poichè, per ogni $s \in S$, $s = 1_G \cdot s \in O_G(s)$, si ha che le orbite sono non vuote e che la loro unione è tutto S.
Siano ora $s,t \in S$ tali che $O_G(s) \cap O_G(t) \neq \emptyset$; allora esiste $u \in O_G(s) \cap O_G(t)$ e quindi esistono $g,h \in G$ tali che $u = g \cdot s = h \cdot t$. Allora, per ogni $x \in G$,

$$x \cdot s = (xg^{-1}g) \cdot s = (xg^{-1}) \cdot (g \cdot s) = (xg^{-1}) \cdot (h \cdot t) = (xg^{-1}h) \cdot t \in O_G(t) \ .$$

Dunque $O_G(s) \subseteq O_G(t)$. Allo stesso modo si prova che $O_G(t) \subseteq O_G(s)$, e quindi $O_G(s) = O_G(t)$; il che dimostra che orbite distinte sono disgiunte e completa la dimostrazione. (Per esercizio si verifichi che la partizione in orbite è l'insieme quoziente rispetto alla equivalenza $\sim_G$ definita su S da $s \sim_G t \ \Leftrightarrow \ \exists g \in G : \ g \cdot s = t$).

Teorema 0.4.10 *Sia data una azione del gruppo G sull'insieme S, e sia $s \in S$. Allora:*

1) *G_s è un sottogruppo di G.*

2) *$|O_G(s)| = [G : G_s]$.*

Dimostrazione. 1) Poichè $1_G \cdot s = s$, si ha $1_G \in G_s$ per qualunque $s \in S$. Fissato ora un tale punto s, siano $g, h \in G_s$. Allora $g \cdot s = s = h \cdot s$ e quindi

$$(gh^{-1}) \cdot s = (gh^{-1}) \cdot (h \cdot s) = (gh^{-1}h) \cdot s = g \cdot s = s,$$

dunque $gh^{-1} \in G_s$ e, per il criterio dei sottogruppi, $G_s \leq G$.

2) Sia $\mathcal{C} = \{\ xG_s \mid x \in G\ \}$ l'insieme delle classi laterali sinistre di G modulo G_s e consideriamo la applicazione

$$\begin{array}{rcl} \eta\ :\ \mathcal{C} & \to & O_G(s) \\ xG_s & \mapsto & x \cdot s \end{array}$$

essa è ben definita, infatti se $x, y \in G$ sono tali che $xG_s = yG_s$ allora $y^{-1}x \in G_s$, cioè $(y^{-1}x) \cdot s = s$ e quindi $y \cdot s = y \cdot ((y^{-1}x) \cdot s) = (yy^{-1}x) \cdot s = x \cdot s$. Dunque η è ben definita.
Proviamo ora che η è biettiva. Essa è suriettiva per definizione di orbita di s. Siano ora $xG_s, yG_s \in \mathcal{C}$ tali che $\eta(xG_s) = \eta(yG_s)$; allora $x \cdot s = y \cdot s$, e quindi

$$(y^{-1}x) \cdot s = y^{-1} \cdot (x \cdot s) = y^{-1} \cdot (y \cdot s) = (y^{-1}y) \cdot s = 1_G \cdot s = s\ ;$$

dunque $y^{-1}x \in G_s$, cioè $xG_s = yG_s$. Quindi η è iniettiva e pertanto è una biezione.
In particolare si ha $[G : G_s] = |\mathcal{C}| = |O_G(s)|$, come si voleva.

Se il gruppo G è finito allora, in congiunzione con il Teorema di Lagrange, segue dal Teorema precedente la seguente importante osservazione.

Corollario. *Se il gruppo finito G opera sull'insieme S, allora per ogni $s \in S$, $|O_G(s)|$ divide $|G|$. In particolare, se l'azione è transitiva, allora $|S|$ divide $|G|$.*

Consideriamo ora il caso in cui sia G che S sono finiti, ed è data una azione di G su S. Siano $O_G(s_1)$, $O_G(s_2)$, $\ldots$, $O_G(s_n)$ le orbite distinte di G su S (l'insieme $\{s_1, s_2, \ldots, s_n\}$ si dice un insieme di rappresentanti per le orbite di G su S). Per la Proposizione 4.9 esse costituiscono una partizione di S, quindi

$$|S| = |O_G(s_1)| + |O_G(s_2)| + \ldots + |O_G(s_n)|\ .$$

Ora, per il Teorema 4.10, per ogni $i = 1, \ldots, n$ si ha $|O_G(s_i)| = [G : G_{s_i}]$; quindi si ricava l'importante:

Equazione delle orbite. *Sia $\{s_1, s_2, \ldots, s_n\}$ un insieme di rappresentanti per le orbite di G su S. Allora*

$$|S| = \sum_{i=1}^{n} [G : G_{s_i}]\ .$$

Definizione. Se G opera sull'insieme S ed $s \in S$ è tale che $O_G(s) = \{s\}$, allora s si dice un **punto fisso** l'azione di G su S. In altri termini, $s \in S$ è un punto fisso se e solo se $g \cdot s = s$ per ogni $g \in G$, ovvero se e solo se $G_s = G$.

Come applicazione dell'equazione delle orbite, vediamo un criterio sufficiente all'esistenza di un punto fisso. Sia p un numero primo e sia P un gruppo di ordine p^m (si dice che P è un *p-gruppo finito*), e sia data una azione di P su un insieme finito S. Sia $\{s_1, s_2, \ldots, s_n\}$ un insieme di rappresentanti per le orbite di G su S. Per il teorema di Lagrange, per ogni $i = 1, \ldots, n$, l'indice $[G : G_{s_i}]$ divide $|P| = p^m$. Assumiamo che non vi siano punti fissi per l'azione di P su S; allora, per ogni $i = 1, \ldots, n$, G_{s_i} è un sottogruppo proprio di P, quindi $[G : G_{s_i}] = p^{k(i)}$ con $k(i) \geq 1$; in particolare p divide $[G : G_{s_i}]$. Applicando la formula delle orbite si ha che p divide $\sum_{i=1}^{n} [G : G_{s_i}] = |S|$. Abbiamo quindi dimostrato

Teorema 0.4.11 *Sia P un p-gruppo finito che opera su un insieme S. Se $(|S|, p) = 1$ allora esiste almeno un punto fisso di P su S.*

Esercizio. Sia data una azione del gruppo G su un insieme S. Siano $s \in S$, $g \in G$ e poniamo $t = g \cdot s$. Si provi che $G_s = g^{-1}(G_t)g$.

Vediamo ora un esempio interessante di azione transitiva di un gruppo G. Sia H un sottogruppo fissato di G e denotiamo con $G\backslash H$ l'insieme delle classi laterali sinistre di G modulo H; su questo insieme definiamo una azione di G ponendo, per ogni $g \in G$ e ogni $xH \in G\backslash H$,

$$g \cdot xH = gxH \ .$$

Si verifica immediatamente che ciò definisce una azione, e che tale azione è transitiva. Infatti, per ogni xH, $yH \in G\backslash H$ si ha

$$(yx^{-1}) \cdot xH = yx^{-1}xH = yH \ .$$

Supponiamo ora che l'indice $[G : H] = n$ sia finito. Allora $|G\backslash H| = [G : H] = n$, e l'azione di G su $G\backslash H$ sopra descritta da luogo ad un omomorfismo $G \to Sym(G\backslash H) = S_n$. Sia N il nucleo di questo omomorfismo, allora

$$N = \{\ g \in G \mid g \cdot xH = xH \ \ \forall xH \in G\backslash H\ \} = \{\ g \in G \mid gxH = xH \ \ \forall x \in G\ \} =$$

$$= \{\ g \in G \mid x^{-1}gxH = H \ \ \forall x \in G\ \}$$

osservando che

$$x^{-1}gxH = H \quad \Leftrightarrow \quad x^{-1}gx \in H \quad \Leftrightarrow \quad \exists h \in H : \ x^{-1}gx = h \quad \Leftrightarrow \quad g \in xHx^{-1} = H^{x^{-1}}$$

possiamo concludere che

$$N = \{\ g \in G \mid g \in H^{x^{-1}} \ \ \forall x \in G\ \} = \bigcap_{x \in G} H^x \ .$$

Questo sottogruppo normale di G si denota con H_G. Chiaramente $H_G \leq H$. Inoltre, per il Teorema di omomorfismo, G/H_G è isomorfo ad un sottogruppo di S_n; in particolare $[G : H_G]$ divide $n!$.

Questo tipo di azioni di G è importante perchè si può dimostrare che ogni azione transitiva di G è equivalente (secondo una naturale definizione di equivalenza di azioni, vedi gli esercizi 5 e 6) ad una azione di G sulle classi laterali di un suo opportuno sottogruppo.

ESERCIZI

1. Sia data una azione transitiva del gruppo S_3 su un insieme S. Quanti elementi può avere S ?

2. Sia G un gruppo di ordine 1998 e S un insieme di ordine 14. Si provi che ogni azione di G su S ha almeno tre orbite.

3. Sia $I_n = \{1, 2, \ldots, n\}$ (con $n \geq 2$) e sia X l'insieme costituito dai sottoinsiemi di ordine 2 di I_n. Allora il gruppo simmetrico S_n opera su X in modo naturale: per ogni $\sigma \in S_n$ e ogni $\{i, j\} \in X$, $\sigma \cdot \{i, j\} = \{i\sigma, j\sigma\}$.

a) Si provi che tale azione è transitiva, e si calcoli l'ordine dello stabilizzatore di $\{1, 2\}$.

b) Posto $n = 5$, si determini $Stab_{S_5}(\{1, 2\}) \cap A_5$.

4. Sia $G = GL(2, \mathbb{R})$ e consideriamo l'azione di G sull'insieme dei vettori colonna reali non nulli $S = \{ \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{R}\ (a, b) \neq (0, 0) \}$ definita da

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} .$$

Si dica se tale azione è transitiva, e si determini lo stabilizzatore del punto $\mathbf{e_1} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

5. Sia G un gruppo. Due azioni di G su insiemi S e S' si dicono *equivalenti* se esiste una biezione $f : S \to S'$ tale che, per ogni $g \in G$, $s \in S$

$$g \cdot (f(s)) = f(g \cdot s)$$

Si provi che se due azioni di G su S e S' sono equivalenti, allora per ogni $s \in S$ si ha $O_G(f(s)) = f(O_G(s))$ e $G_{f(s)} = G_s$.

6. Sia data una azione transitiva del gruppo G sull'insieme S; fissato un $s \in S$, si ponga $H = G_s$. Si provi che l'azione di G su S è equivalente all'azione di G sull'insieme delle classi laterali sinistre modulo H.

7. Sia G un gruppo finito, e sia p il minimo numero primo che divide $|G|$. Si provi che se $H \leq G$ e $[G : H] = p$, allora $H \trianglelefteq G$.

8. Sia G un gruppo e $H \leq G$. Si provi che H_G è il massimo sottogruppo normale di G contenuto in H.

Classi di coniugio

In questo paragrafo applicheremo i risultati del paragrafo precedente al caso dell'azione di un gruppo G su se stesso mediante coniugio. Ricordiamo che se x, g sono elementi di un gruppo G, il *coniugato* di x tramite g è l'elemento $g^{-1}xg$, che si denota con x^g.
Il coniugio definisce una azione di G su G ponendo, per ogni $g, x \in G$: $g \cdot x = x^{g^{-1}}$.
Infatti, per ogni $x \in G$, $x^{1_G} = x$, e per ogni $x, g, h \in G$:

$$(gh) \cdot x = x^{(gh)^{-1}} = (gh)x(h^{-1}g^{-1}) = g(hxh^{-1})g^{-1} = (x^{h^{-1}})^{g^{-1}} = (h \cdot x)^{g^{-1}} = g \cdot (h \cdot x) .$$

In questo caso, la notazione "a destra" risulta più conveniente. Infatti per ogni $x, g, h \in G$ si ha

$$x^{gh} = (x^g)^h \ .$$

(La permutazione di G associata ad ogni elemento $g \in G$ rispetto a questa azione è - come abbiamo visto nell'ultimo paragrafo della sezione precedente - l'automorfismo σ_g di G. Quindi l'omomorfismo da G in $Sym(G)$ associato all'azione per coniugio è di fatto un omomorfismo da G in $Aut(G)$. Potremo dire che l'azione per coniugio è una azione di G come gruppo di automorfismi su se stesso. Da questo punto di vista è stata trattata nell'ultimo paragrafo della sezione precedente; ora ci interessa piuttosto il punto di vista delle permutazioni, in modo da applicare i concetti che abbiamo esposto su questo tipo di azioni.)

L'orbita di un elemento $x \in G$ rispetto all'azione per coniugio si chiama **classe di coniugio** di x ed è

$$\{ \ x^g \mid g \in G \ \} \ .$$

Lo stabilizzatore in G di x si denota con $C_G(x)$ e si chiama centralizzante di x in G:

$$C_G(x) = \{ \ g \in G \mid x^g = x \ \} = \{ \ g \in G \mid g^{-1}xg = x \ \} = \{ \ g \in G \mid xg = gx \ \} \ .$$

Il centralizzante di un elemento x è quindi l'insieme degli elementi di G che commutano con x. Se G è un gruppo finito si ha, per il Teorema 4.10

$$|\{ \ x^g \mid g \in G\}| = [G : C_G(x)] \ .$$

Inoltre G (come insieme) si ripartisce nelle sue classi di coniugio distinte (che sono le orbite dell'azione per coniugio).
Dopo aver ricordato la definizione di **centro** di G:

$$Z(G) = \{ \ x \in G \mid xg = gx \ \text{ per ogni } \ g \in G \ \},$$

osserviamo che un elemento $x \in G$ appartiene al centro $Z(G)$ se e solo se $gx = xg$ per ogni $g \in G$, ovvero se e solo se $x^g = g^{-1}xg = x$ per ogni $g \in G$, cioè se e solo se la classe di coniugio di x consiste del solo elemento x.

Prima di andare avanti con la teoria delle classi di coniugio, vediamo una interessante applicazione del Teorema 4.11

Teorema 0.4.12 *Sia p un numero primo e G un p-gruppo finito. Allora $Z(G) \neq \{1_G\}$.*

Dimostrazione. Sia G un gruppo di ordine p^n, dove p è un numero primo. Poniamo $S = G \setminus \{1_G\}$; chiaramente l'azione per coniugio di G su se stesso induce una azione per coniugio su S. Ora $|S| = p^n - 1$, quindi per il Teorema 4.11, G ha punto fisso su S, cioè esiste un elemento $1_G \neq x \in G$ tale che la sua classe di coniugio è $\{x\}$. Per quanto osservato sopra, $x \in Z(G)$ e quindi $Z(G) \neq \{1_G\}$.

Sia ora G un gruppo finito, denotiamo con $K_1, K_2, \ldots, K_n$ le sue classi di coniugio distinte e, per ogni $i = 1, 2, \ldots, n$ fissiamo un elemento $x_i \in K_i$ (l'insieme $\{x_1, x_2, \ldots, x_n\}$

è detto allora un insieme di rappresentanti delle classi di coniugio di G). Allora la formula delle orbite si scrive

$$|G| = \sum_{i=1}^{n} |K_i| = \sum_{i=1}^{n} [G : C_G(x_i)] \ .$$

Una classe di coniugio si dice *centrale* se consiste di un solo elemento; per quanto abbiamo osservato prima, una classe è centrale se e solo se è la classe di un elemento appartenente al centro di G. Il numero di classi centrali è dunque $|Z(G)|$. Se, nella somma di sopra, raccogliamo gli addendi corrispondenti alle classi centrali, il loro contributo alla somma è ancora $|Z(G)|$, a cui va sommato il contributo delle classi non centrali. Possiamo enunciare questa importante osservazione con la seguente

Formula delle Classi. *Sia G un gruppo finito, e siano $y_1, y_2, \ldots, y_m$ rappresentanti delle classi non centrali di G. Allora*

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(y_i)] \ .$$

Come esempio, consideriamo il gruppo S_4. Per la Proposizione 4.4, due elementi di S_4 sono coniugati se e solo se hanno lo stesso tipo ciclico. Per oottenere un insieme di rappresentanti delle classi di coniugio di S_4 è quindi sufficiente considerare un lemento per ciascun tipo ciclico; ad esempio possiamo prendere $\{ \ x_1 = \iota, \ x_2 = (1\,2), \ x_3 = (1\,2)(3\,4), \ x_4 = (1\,2\,3), \ x_5 = (1\,2\,3\,4) \ \}$. Indichiamo con n_i il numero di elementi coniugati a x_i (ovvero $n_i = [S_4 : C_{S_4}(x_i)]$). Allora, $n_1 = 1$, $n_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix} = 6$ (infatti ogni coppia di elementi di $\{1,2,3,4\}$ da luogo ad una trasposizione), $n_3 = 3$, $n_4 = 2\begin{pmatrix} 4 \\ 3 \end{pmatrix} = 8$ (infatti ogni terna di elementi di $\{1,2,3,4\}$ da luogo a due 3-cicli). Possiamo ora calcolare n_5 usando la formula delle classi:

$$n_5 = |S_4| - (n_1 + n_2 + n_3 + n_4) = 24 - 18 = 6 \ .$$

Esercizio. Si dimostri il Teorema 4.12 utilizzando la Formula delle Classi.

La serie di esercizi svolti che segue tratta alcune interessanti applicazioni dei concetti e delle formule introdotte in questo paragrafo. Naturalmente, cercate di discuterli da voi prima di controllarne la soluzione. Ricordiamo che il centro di un gruppo è sempre un sottogruppo normale.

Esercizio A. Sia G un gruppo. Dimostrare che se $G/Z(G)$ è ciclico allora G è commutativo (quindi $Z(G) = G$).

Soluzione. Sia $G/Z(G)$ un gruppo ciclico. Allora esiste un elemento $gZ(G) \in G/Z(G)$ tale che

$$G/Z(G) = < gZ(G) > = \{(gZ(G))^z \mid z \in \mathbb{Z}\} = \{ \ g^z Z(G) \mid z \in \mathbb{Z}\} \ .$$

Quindi, se $x, y \in G$, esistono $a, b \in \mathbb{Z}$ tali che $xZ(G) = g^a Z(G)$ e $yZ(G) = g^b Z(G)$; cioè esistono $h, k \in Z(G)$ tali che $x = g^a h$ e $y = g^b k$. Poichè h, k commutano con ogni elemento di G, abbiamo

$$xy = g^a h g^b k = g^a g^b hk = g^{a+b} kh = g^b g^a kh = g^b k g^a h = yx \ .$$

Dunque G è commutativo.

Esercizio B. Sia p un numero primo. Dimostrare che ogni gruppo di ordine p^2 è commutativo.

Soluzione. Sia G un gruppo con $|G| = p^2$. Allora, per il Teorema 4.12, $Z(G) \neq \{1_G\}$, e quindi, per il Teorema di Lagrange, $|Z(G)| = p, p^2$. Se $|Z(G)| = p^2$, allora $G = Z(G)$ è commutativo. Se invece $|Z(G)| = p$, allora $|G/Z(G)| = p$; ma allora, per la Proposizione 13 della sezione precedente, $G/Z(G)$ è ciclico, e quindi, per Esercizio A, G è commutativo (quindi, a posteriori, possiamo dire che il caso $|Z(G)| = p$ non si verifica se $|G| = p^2$).

Esercizio C. Sia G un gruppo di ordine 6. Si dimostri che se G non è commutativo allora G è isomorfo a S_3.

Soluzione. Sia G un gruppo non commutativo di ordine 6. Allora $G \neq Z(G)$. Poichè $Z(G)$ è un sottogruppo di G, il suo ordine è un divisore di 6. Se fosse $|Z(G)| = 2$, allora $|G/Z(G)| = 3$ e quindi $G/Z(G)$ sarebbe ciclico e pertanto, per l'esercizio A, G sarebbe commutativo. Similmente si esclude il caso $|Z(G)| = 3$. Quindi si ha $|Z(G)| = 1$.
Ora, se $y \in G \setminus Z(G)$ allora $[G : C_G(y_i)]$ non è uguale ad 1, e quindi, sempre per il Teorema di Lagrange, deve essere 2 o 3. Se $y_1, \ldots, y_m$ sono rappresentanti delle classi non centrali di G, abbiamo, per la Formula delle Classi,

$$6 = |Z(G)| + [G : C_G(y_1)] + \ldots + [G : C_G(y_m)] = 1 + [G : C_G(y_1)] + \ldots + [G : C_G(y_m)] \ ,$$

dove gli addendi $[G : C_G(y_i)]$ appartengono tutti all'insieme $\{2, 3\}$. La sola possibilità è: $6 = 1 + 2 + 3$.
In particolare, segue che G ha una classe di coniugio K di ordine 3. Ora, G opera per coniugio, transitivamente, su K, e tale azione determina un omomorfismo $\phi : G \to S_K$. Sia $N = Ker(\phi)$. Non può essere $|N| = 2$, perchè un sottogruppo normale di ordine 2 è sempre contenuto nel centro (questo è facile e lo lasciamo), contro il fatto che $Z(G) = \{1_G\}$. Quindi (poichè l'azione è transitiva) si ha $N = \{1_G\}$. Dunque ϕ è un omomorfismo iniettivo; siccome $|G| = 6 = |S_K|$, ϕ è allora un isomorfismo. Dunque G è isomorfo a S_K che è isomorfo a S_3.

L'idea di azione per coniugio si può estendere in modo naturale considerando l'azione, invece che sugli elementi, su sottoinsiemi del gruppo G.
Se G è un gruppo, $\emptyset \neq S \subseteq G$ e $g \in G$, il coniugato di S tramite g è l'insieme

$$S^g = \{ \ x^g \mid x \in S \ \} \ .$$

Si verifica facilmente che $S^{1_G} = S$ e che $S^{gh} = (S^g)^h$ per ogni $g, h \in G$. Lo stabilizzatore di S è (il sottogruppo) $\{ \ g \in G \mid S^g = S \ \}$.
Se $H \leq G$ allora $H^g \leq G$ per ogni $g \in G$, e lo stabilizzatore di H rispetto alla azione di coniugio si chiama **normalizzatore** di H in G, e si denota con $N_G(H)$. Allora $H \leq N_G(H) \leq G$ (vedi esercizio 13 alla fine della sezione precedente), ed il numero di coniugati distinti di H in G è uguale all'indice

$$[G : N_G(H)]$$

in particolare, $H \trianglelefteq G$ se e soltanto se $N_G(H) = G$.

Naturalmente, non è necessario considerare l'azione per coniugio di un gruppo G sulla famiglia di tutti i suoi sottoinsiemi non vuoti. L'azione per coniugio si può definire su una particolare famiglia di sottoinsiemi, purchè essa contenga tutti i coniugati di ogni suo elemento. Ad esempio, si può considerare l'azione sulla famiglia dei sottogruppi di G, oppure sulla famiglia dei sottogruppi di un ordine fissato.
Utilizzeremo l'azione per coniugio su sottogruppi nel prossimo paragrafo, per dimostrare gli importanti Teoremi di Sylow.

Concludiamo con una osservazione che sarà anch'essa utilizzata nel prossimo paragrafo. La dimostrazione è lasciata per esercizio, perchè ricalca quella del Lemma 1 della sezione precedente.

Lemma 0.4.13 *Siano G un gruppo, e $H, K \leq G$. Se $K \subseteq N_G(H)$ allora $HK \leq G$.*

ESERCIZI

1. Sia G un gruppo di ordine 21. Si provi che se $Z(G) \neq \{1_G\}$ allora G è commutativo.

2. Si provi che un gruppo di ordine p^2 (p un numero primo) è ciclico oppure è il prodotto diretto di due gruppi ciclici di ordine p.

3. Si scriva la formula delle classi per il gruppo S_5.

4. Si provi che il gruppo S_6 ha un sottogruppo di indice 90 (sugg.: si consideri la classe dell'elemento $(1\,2\,3\,4)$).

5. Si provi che ogni gruppo di ordine 6 è ciclico oppure isomorfo a S_3.

6. Sia G un gruppo di ordine dispari. Si provi che G ha un numero dispari di classi di coniugio.

7. Sia G un gruppo di ordine dispari, e sia $x \in G$. Si provi che se x è coniugato a x^{-1} allora $x = 1_G$.

8. Sia G un gruppo di ordine 15. Si provi che G è commutativo.

9. Sia H un sottogruppo del gruppo G e sia

$$C_G(H) = \{\ g \in G \mid gx = xg \ \ \forall x \in H\ \}\ .$$

Si provi che $C_G(H) \leq G$ e che $C_G(H) \trianglelefteq N_G(H)$.

Teoremi di Sylow

Insieme al Teorema di Lagrange, i Teoremi di Sylow sono lo strumento fondamentale per lo studio dei gruppi finiti. La dimostrazione che daremo non è quella originaria di L. Sylow (1832 - 1918), ma è ispirata a quella scoperta molti anni più tardi (1959) da H. Wielandt, ed è una ingegnosa applicazione della azione su sottoinsiemi.

Primo Teorema di Sylow. *Sia p un numero primo, e sia G un gruppo finito tale che p^k divide $|G|$. Allora esistono sottogruppi di G di ordine p^k.*

Se G è un gruppo di ordine $p^m a$, con p un numero primo e $(p, a) = 1$, allora il Primo Teorema di Sylow assiscura l'esistenza di sottogruppi di G di ordine p^k per ogni $1 \leq k \leq m$ (per il Teorema di Lagrange, G non ha certo sottogruppi di ordine p^s con $s \geq m+1$). I sottogruppi di G di ordine p^m si chiamano *p-sottogruppi di Sylow* di G.

Dimostreremo il Primo Teorema di Sylow procedendo per induzione su $|G|$. Per comodità, isoliamo in un Lemma un caso molto particolare (e già noto a Cauchy).

Lemma 0.4.14 *Sia G un gruppo finito commutativo, e p un primo che divide l'ordine di G. Allora G ha un elemento di ordine p.*

Dimostrazione. Sia G un gruppo commutativo il cui ordine è diviso da p. Allora $|G| = pr$, e procediamo per induzione su r. Se $r = 1$, G è ciclico ed è generato da un elemento di ordine p.
Sia quindi $|G| = pr > p$ e supponiamo l'affermazione vera per ogni gruppo il cui ordine è diviso da p ed è strettamente minore dell'ordine di G. Sia $1_G \neq a \in G$, e sia $A =< a >$. Se p divide l'ordine di a allora A contiene un elemento di ordine p (se n è l'ordine di a, $a^{n/p}$ ha ordine p).
Supponiamo quindi che p non divida $|a| = |A|$. Poichè G è commutativo, $A \trianglelefteq G$ ed il quoziente G/A ha ordine $|G/A| = |G|/|A|$ diviso da p e minore dell'ordine di G. Per ipotesi induttiva G/A contiene un elemento bA di ordine p, cioè tale che $bA \neq 1_{G/A} = A$ e $A = (bA)^p = b^pA$. Ora, se s è l'ordine di b, si ha $(bA)^s = b^sA = A = 1_{G/A}$, quindi $p = |bA|$ divide s; e quindi $< b >$ ha un elemento di ordine p, completando la dimostrazione.

Dimostrazione (del Primo Teorema di Sylow). Procediamo per induzione sull'ordine di G. Se $|G| = 1$ non c'è nulla da provare. Sia $|G| > 1$ e supponiamo il Teorema vero per ogni gruppo di ordine strettamente minore di $|G|$, e sia p^k (con $k \geq 1$) un divisore di $|G|$. Consideriamo l'equazione delle classi per G:

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(y_i)] \ .$$

Supponiamo che per un indice $i \in \{1, 2, \ldots, m\}$, $, p$ non divida $[G : C_G(y_i)]$, allora per il Teorema di Lagrange, p^k divide $|C_G(y_i)| = |G|/[G : C_G(y_i)]$. Poichè y_i è un elemento non centrale di G, $C_G(y_i)$ è un sottogruppo proprio di G, e quindi, per ipotesi induttiva, contiene un sottogruppo di ordine p^k, e siamo a posto.
Supponiamo quindi che p divida ogni indice $[G : C_G(y_i)]$; allora p divide anche $|Z(G)|$. Per il Lemma precedente, $Z(G)$ ha un elemento a di ordine p. Sia $A =< a >$. Poichè $A \leq Z(G)$ si ha $A \trianglelefteq G$. Ora $|G/A| = |G|/p$; quindi p^{k-1} divide $|G/A|$ e, per ipotesi induttiva, G/A ha un sottogruppo H/A (ove, per il Teorema di Corrispondenza, $A \leq H \leq G$) di ordine p^{k-1}. Ma allora H è il sottogruppo di G cercato; infatti $|H| = [H : A]|A| = |H/A||A| = p^{k-1}p = p^k$.

Secondo Teorema di Sylow. *Sia G un gruppo finito, e $|G| = p^m a$, dove p è un numero primo e $(p, a) = 1$. Allora i p-sottogruppi di Sylow G sono tra loro coniugati, e se n_p denota il numero di p-sottogruppi di Sylow di G si ha*

$$n_p \equiv 1 \,(\mathrm{mod}\ p) \qquad e \qquad n_p | a \ .$$

Dimostrazione. Sia Σ l'insieme di tutti i p-sottogruppi di Sylow di G (quindi $n_p = |\Sigma|$). Osserviamo che, se $U \in \Sigma$ allora, per ogni $x \in G$, $U^g \in \Sigma$; quindi G opera per coniugio sull'insieme Σ. Sia P un fissato p-sottogruppo di Sylow di G, e consideriamo l'azione di

P per coniugio su Σ. Poichè $P \in \Sigma$ e $P^x = P$ per ogni $x \in P$, P è (come elemento di Σ) un punto fisso per l'azione di P. Vediamo che non ci sono altri punti fissi. Infatti, se $Q \in \Sigma$ è un punto fisso, allora $Q^x = Q$ per ogni $x \in P$, cioè $P \subseteq N_G(Q)$; quindi, per il Lemma 4.13, $PQ \leq G$. Ora, $P \leq PQ$ e, per il Lemma 3(b) della sezione precedente

$$|PQ| = \frac{|P||Q|}{|P \cap Q|}$$

è una potenza di p, da cui segue $P = Q$ perchè P è un p-sottogruppo di Sylow e quindi il suo ordine è la massima potenza di p che divide G. Quindi P è l'unico punto fisso nella azione di P su Σ. Ciò significa che $\{P\}$ è un orbita di P su Σ, e che se $\mathcal{O}$ è un'altra orbita diversa da $\{P\}$, allora $1 \neq |\mathcal{O}|$; poichè $|\mathcal{O}|$ è uguale all'indice dello stabilizzatore in P di un elemento di $\mathcal{O}$, e P è un p-gruppo, si ha che p divide $|\mathcal{O}|$. La formula delle orbite si scrive quindi

$$n_p = |\Sigma| = |\{P\}| + \sum_{\mathcal{O} \neq \{P\}} |\mathcal{O}| = 1 + \sum_{\mathcal{O} \neq \{P\}} |\mathcal{O}| \equiv 1 \,(\text{mod } p)$$

dimostrando una delle affermazioni dell'enunciato.

Proviamo ora che tutti i p-sottogruppi di Sylow sono tra loro coniugati in G; ovvero che Σ è una classe di coniugio di sottogruppi di G. Consideriando l'azione per coniugio di tutto il gruppo G su Σ, si tratta di verificare che c'è una sola orbita. Fissiamo un p-sottogruppo di Sylow P e sia $\mathcal{A} = O_G(P)$ la sua orbita. Considerando, l'azione di P su $\mathcal{A}$ e ragionando come sopra, si ha $|\mathcal{A}| \equiv 1 \,(\text{mod } p)$. Supponiamo, per assurdo, che esista $Q \in \Sigma$ tale che $Q \notin \mathcal{A}$, e consideriamo l'azione di Q su $\mathcal{A}$. Ora, Q ha un solo punto fisso nella sua azione su Σ, che è Q stesso. Poichè Q non appartiene ad $\mathcal{A}$, ne segue che Q non ha punti fissi su $\mathcal{A}$, e quindi, per il Teorema 4.11, p divide $|\mathcal{A}|$, una contraddizione. Dunque $\mathcal{A} = \Sigma$, e quindi, per ogni coppia di p-sottogruppi di Sylow P, Q di G, esiste $x \in G$ tale che $Q = P^x$.
Infine, stabilito che l'azione di G per coniugio su Σ è transitiva, abbiamo che il numero di elementi di Σ coincide con l'indice dello stabilizzatore in G di un suo elemento. Quindi, per quanto osservato nel paragrafo precedente, se P è un p-sottogruppo di Sylow di G, allora

$$n_p = |\Sigma| = [G : N_G(P)] \ .$$

Ora, $P \leq N_G(P) \leq G$, e quindi

$$a = [G : P] = [G : N_G(P)][N_G(P) : P] = n_p[N_G(P) : P]$$

in particolare , n_p divide $a = [G : P]$, e questo completa la dimostrazione del Teorema.

Terzo Teorema di Sylow. *Sia G un gruppo finito, e sia p un numero primo che divide $|G|$. Allora ogni sottogruppo di G il cui ordine è una potenza di p è contenuto in almeno un p-sottogruppo di Sylow di G.*

Dimostrazione. Sia $H \leq G$ tale che $|H| = p^k$ per qualche $k \geq 1$. Sia Σ l'insieme di tutti i p-sottogruppi di Sylow di G e consideriamo l'azione per coniugio di H su Σ. Poichè $(|\Sigma|, |H|) = (n_p, p^k) = 1$, per il Teorema 4.11, H ha almeno un punto fisso su Σ; cioè esiste un $P \in \Sigma$ tale che $P^x = P$ per ogni $x \in H$, ovvero $H \subseteq N_G(P)$. Allora,

ragionando come nella dimostrazione del Secondo Teorema di Sylow, $PH \leq G$ e, di conseguenza, $H \leq P$, che è quello che si voleva dimostrare.

Concludiamo questo paragrafo illustrando con alcuni esempi come i teoremi di Sylow possano fornire molte informazioni su un gruppo finito. Gli esempi che considereremo sono molto specifici, ma danno un idea dei metodi che si possono applicare in molte circostanze. Negli esercizi verranno suggeriti anche alcuni casi più generali, non complicati, che si possono affrontare mediante queste tecniche. Un fatto banale ma fondamentale da tener presente è che se $H \leq G$ allora per ogni $g \in G$ il coniugato H^g è un sottogruppo dello stesso ordine di H; quindi se avviene che H è il solo sottogruppo di un certo ordine, allora $H \trianglelefteq G$. In particolare, se per qualche primo p il numero di p-sottogruppi di Sylow di G è 1, l'unico p-sottogruppo di Sylow è normale.

Esempio 1. Sia G un gruppo di ordine $45 = 3^2 \cdot 5$; proviamo che G è commutativo. Ora, i 3-sottogruppi di Sylow di G hanno ordine $3^2 = 9$ ed i 5-sottogruppi di Sylow hanno ordine 5. Indichiamo con $n_3,\ n_5$, rispettivamente il numero di 3-sottogruppi di Sylow e di 5-sottogruppi di Sylow di G. Allora, per il secondo Teorema di Sylow, $n_3 \equiv 1 \pmod 3$ e $n_3|5$; quindi $n_3 = 1$ e dunque G ha un solo 3-sottogruppo di Sylow T ed è $T \trianglelefteq G$. Similmente, $n_5 \equiv 1 \pmod 5$ e $n_5|9$; quindi $n_5 = 1$ e G ha un solo 5-sottogruppo di Sylow Q che è normale in G. Ora, $T \cap Q$ è sottogruppo sia di T che di Q e dunque il suo ordine deve dividere sia $|T| = 9$ che $|Q| = 5$; quindi $T \cap Q = \{1_G\}$. Si ha quindi

$$|TQ| = \frac{|T||Q|}{|T \cap Q|} = \frac{9 \cdot 5}{1} = 45$$

quindi $TQ = G$. Dunque $G = T \times Q$. Poichè T e Q sono commutativi (perche il loro ordine è una potenza di esponente al più 2 di un numero primo), concludiamo che G è commutativo.

Ricordiamo che un gruppo G si dice *semplice* se i soli suoi sottogruppi normali son $\{1_G\}$ e G.

Esempio 2. Sia G un gruppo di ordine $72 = 2^3 \cdot 3^2$; proviamo che G non è semplice. Sia n_3 il numero di 3-sottogruppi di Sylow di G. Se $n_3 = 1$ allora G ha un 3-sottogruppo di Sylow normale e quindi G non è semplice. Supponiamo quindi $n_3 \neq 1$. Allora, per il secondo Teorema di Sylow, si ha $n_3 = 4$. Siano P, Q due distinti 3-sottogruppi di Sylow di G. Poichè $|P| = |Q| = 9 = 3^2$, P e Q sono commutativi. Consideriamo il loro prodotto $PQ \subseteq G$, e sia $H = P \cap Q$, si ha

$$72 = |G| \geq |PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{81}{|H|}$$

e quindi $H \neq \{1_G\}$. Poichè $P \neq Q$, deve essere, per il Teorema di Lagrange, $|H| = 3$, e $|PQ| = 27$. Sia ora $1 \neq x \in H$. Poichè P e Q sono commutativi, $C_G(x)$ contiene sia P che Q; quindi $PQ \subseteq C_G(x)$. In particolare $|C_G(x)| \geq |PQ| = 27$. Poichè $|C_G(x)|$ divide $|G|$, deve essere $|C_G(x)| = 36, 72$. Se $|C_G(x)| = 72$ allora $C_G(x) = G$, e quindi $x \in Z(G)$, cioè $Z(G) \neq \{1_G\}$ e quindi G non è semplice. Sia quindi $|C_G(x)| = 36 = 2^2 \cdot 3^2$; poichè $C_G(x)$ contiene almeno due distinti 3-sottogruppi di Sylow (i nostri P e Q), applicando il secondo Teorema di Sylow al gruppo $C_G(x)$ si ha che esso contiene quattro 3-sottogruppi di Sylow; questi sono necessariamente anche tutti i 3-sottogruppi di Sylow di G. Da ciò segue che $H =< x >$ è contenuto in ogni 3-sottogruppo di Sylow di G. Allora, se $g \in G$, $H^g = (P \cap Q)^g = P^g \cap Q^g = H$ e quindi $H \trianglelefteq G$, e G non è semplice.

Esempio 3. Sia G un gruppo di ordine 408; proviamo che G contiene un sottogruppo di indice 3. Abbiamo $408 = 2^3 \cdot 3 \cdot 17$. Per il secondo teorema di Sylow, il numero n_{17} di 17-sottogruppi di Sylow di G è congruo ad 1 modulo 17, e divide $2^3 \cdot 3 = 24$; quindi $n_{17} = 1$, G ha un unico 37-sottogruppo di Sylow N e $N \trianglelefteq G$. Consideriamo ora il gruppo quoziente G/N. Ora, $|G/N| = |G|/|N| = 24$ e quindi G/N ha un sottogruppo di ordine 2^3; per il Teorema di Corrispondenza, esiste un sottogruppo H di G tale che $N \leq H$ e $|H/N| = 2^3$. Quindi $|H| = |H/N||N| = 2^3 \cdot 17$ e dunque $[G : H] = |G|/|H| = 3$ e H è il sottogruppo cercato.

ESERCIZI

1. Si determinino tutti i sottogruppi di Sylow (per ogni primo che divide l'ordine del gruppo) dei gruppi S_3 e S_4.

2. Sia G un gruppo finito, $N \trianglelefteq G$ e p un divisore primo dell'ordine di G. Sia P un p-sottogruppo di Sylow di G. Si provi che NP/N è un p-sottogruppo di Sylow di G/N, e che $P \cap N$ è un p-sottogruppo di Sylow di N.
Si faccia un esempio di un gruppo finito G, un p-sottogruppo di Sylow P di G, e di un sottogruppo (non normale) H di G, tali che $P \cap H$ non è un p-sottogruppo di Sylow di H.

3. Sia G un gruppo finito, e p un divisore primo dell'ordine di G. Sia $N \trianglelefteq G$ tale che $|N| = p^k$. Si provi che il numero di p-sottogruppi di Sylow di G è uguale al numero di p-sottogruppi di Sylow di G/N.

4. Sia G un gruppo di ordine pq, con p e q numeri primi. Si provi che G non è semplice. Si provi quindi che se $p < q$ e $p \not| q - 1$ allora G è commutativo (anzi ciclico).

5. Siano p, q primi distinti. Si provi che un gruppo di ordine p^2q non è semplice.

6. Si provi che un gruppo di ordine 120 ha almeno 6 classi di coniugio.

7. Sia G un gruppo di ordine 224. Si provi che G non è semplice.

8. Sia G un gruppo di ordine 1998. Si provi che G ha un unico sottogruppo di indice 2.

9. Sia G un gruppo di ordine 63. Si provi che $Z(G) \neq \{1_G\}$.

10. Sia G un gruppo di ordine pq^2, con p, q primi distinti. Si provi che se $|Z(G)| = p$ allora G è commutativo.

11. Sia G un gruppo di ordine 12. Si provi che si verifica uno dei casi seguenti.
a) G è commutativo; in tal caso G è ciclico oppure isomorfo al prodotto diretto di un gruppo non ciclico di ordine 4 per un gruppo ciclico di ordine 3.
b) $|Z(G)| = 3$ e $G/Z(G)$ è isomorfo a S_3.
c) $|Z(G)| = 1$ e G è isomorfo a A_4.

VI - TEORIA DEI CAMPI

0.5 Estensioni di campi

Siano F, E campi. E si dice *estensione* di F (e si scrive $E|F$) se esiste un omomorfismo iniettivo di campi (detto immersione):

$$\phi \ : \ F \ \longrightarrow \ E.$$

In tal caso, l'immagine $\phi(F)$ è un sottocampo di E *isomorfo* ad F. Risulta allora spesso più agevole pensare di identificare ogni elemento a di F con la sua immagine $\phi(a)$, e di vedere quindi F "contenuto" in E come suo sottocampo.

Esempi fondamentali di estensioni di campi sono $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{R}$ e $\mathbb{C}|\mathbb{Q}$ (con le immersioni naturali - ovvero la restrizione dell'identità).
Un altro esempio che è utile tener presente è il seguente. Se F è un campo, allora l'anello dei polinomi $F[x]$ è un dominio d'integrità. Denotiamo con $F(x)$ il campo delle frazioni di $F[x]$. Quindi

$$F(x) = \left\{ \ \frac{f}{g} \ | \ f, g \in F[x], \ g \neq 0 \ \right\}$$

si chiama *campo delle frazioni algebriche* su F. Allora $F(x)|F$ è un'estensione di campi (l'immersione è quella che associa ad ogni elemento a di F il polinomio "costante" a).

Ancora, sia F un campo, e I un ideale massimale di $F[x]$; allora $E = F[x]/I$ è un campo, e $E|F$ è una estensione mediante l'omomorfismo (definito da F in E)

$$a \ \mapsto \ a + I.$$

(Ricordo che se $I \neq \{0\}$ è un ideale di $F[x]$ (con F un campo) allora, per quanto visto in precedenza, I è principale e $I = (f)$, dove f è un polinomio di grado minimo tra i polinomi non nulli contenuti in I. Inoltre I è massimale se e soltanto se f è irriducibile in $F[x]$.)

Inffine, osserviamo che se $E|F$ e $L|E$ sono estensioni di campi ottenute mediante, rispettivamente, gli omomorfismi ϕ e ψ, allora $L|F$ è un'estensione, ottenibile mediante l'omomorfismo composto $\psi \circ \phi$.

Grado di una estensione.

Sia F un sottocampo del campo E (o più in generale, sia $E|F$ un'estensione di campi). Allora è possibile vedere in modo naturale E come uno spazio vettoriale su F (ovvero su $\phi(F)$): i vettori sono gli elementi di E, gli scalari quelli di F e il prodotto di un vettore per uno scalare è effettuato mediante la moltiplicazione dei due elementi nel campo E. Si verifica facilmente che tutti gli assiomi di spazio vettoriale sono soddisfatti.

Definizione. Sia $E|F$ un'estensione di campi. La *dimensione* di E come spazio vettoriale su F si chiama **grado** di E su F, e si denota con $[E : F]$.

Ad esempio, ogni numero complesso si scrive in modo unico nella forma $a + ib = a1 + bi$ con $a, b \in \mathbb{R}$, cioè come combinazione lineare (a coefficienti nel campo degli scalari $\mathbb{R}$) di 1 e i (visti come vettori). Quindi $\{1, i\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$ e dunque $[\mathbb{C} : \mathbb{R}] = 2$ (mentre $[\mathbb{R} : \mathbb{Q}] = \infty$, come sarà chiaro più avanti).
Osserviamo anche che $[E : F] = 1$ se e solo se $E = F$.

Questo semplice punto di vista è di fatto molto utile. Ecco una prima applicazione.

Proposizione 0.5.1 *Sia L un campo finito. Allora $|L| = p^n$ con p un numero primo e $1 \leq n \in \mathbb{N}$.*

Dimostrazione. Poichè L è un campo ed è finito la sua caratteristica deve essere un numero primo p (Proposizione 7.2 Cap. IV). Quindi, se F è il suo sottoanello fondamentale, allora $F \simeq \mathbb{Z}_p$ è un campo, e possiamo vedere L come estensione di F. Sia $[L : F] = n$ il grado di questa estensione. Allora L è uno spazio vettoriale su F di dimensione n; quindi, *come spazio vettoriale*, L è isomorfo allo spazio $F^{(n)}$ delle n-uple a coefficienti in F. In particolare, $|L| = |F^{(n)}| = |F|^n = p^n$. ■

Dimostreremo più avanti che per ogni primo p ed ogni $n \geq 1$ esiste un campo di ordine p^n, e che due campi finiti dello stesso ordine sono isomorfi.

Ricordiamo (Proposizione 8.2, Cap. IV) che se F è un campo, e $I = (f)$ un ideale massimale dell'anello dei polinomi $F[x]$ con $n = \deg f$, allora ogni elemento del campo $E_f = F[x]/I$ si scrive in modo unico nella forma

$$a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + I = a_0 \cdot 1 + a_1 \cdot (x + I) + \ldots + a_{n-1} \cdot (x^{n-1} + I)$$

con $a_0, a_1, \ldots, a_{n-1} \in F$. Ne segue che l'insieme di elementi di E_f:

$$1,\ x + I,\ x^2 + I, \ldots, x^{n-1} + I$$

è una base di E_f come spazio vettoriale su F, e quindi $[E_f : F] = n = \deg f$.

Vediamo ora un importante strumento per lo studio dei gradi di un'estensione.

Teorema 0.5.2 (Formula dei Gradi) *Siano F, L, M campi con $F \leq L \leq M$. Allora $[M : F] = [M : L][L : F]$.*

Dimostrazione. Il fatto è ovvio se $[M : L] = \infty$ oppure $[L : F] = \infty$ (qui, adottiamo la convenzione $\infty \cdot n = \infty \cdot \infty = \infty$). Quindi assumiamo che $[M : L] = n,\ [L : F] = m$ siano entrambi finiti.
Sia $a_1, a_2, \ldots, a_n$ una base di M su L, e sia $b_1, b_2, \ldots, b_m$ una base di L su F. Proviamo che gli elementi $b_j a_i$ $(1 \leq j \leq m,\ 1 \leq i \leq n)$ costituiscono una base di M su F.
(generazione). Sia $u \in M$, allora esistono $x_1, x_2, \ldots, x_n$ in L tali che

$$u = x_1 a_1 + x_1 a_2 + \ldots + x_n a_n = \sum_{i=1}^{n} x_i a_i \ .$$

Ora ogni $x_i \in L$ è a sua volta una combinazione a coefficienti in F della base (b_j):

$$x_i = y_{1i} b_1 + y_{2i} b_2 + \ \ldots \ + y_{mi} b_m = \sum_{j=1}^{m} y_{ji} b_j \ .$$

Quindi

$$u = \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} y_{ji} b_j \right) a_i = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{ji} b_j a_i)$$

quindi ogni $u \in M$ è combinazione a coefficienti in F degli elementi $b_j a_i$.
(indipendenza). Proviamo ora che il sistema $(b_j a_i)$ è linearmente indipendente. Sia $I = \{1, \ldots, m\} \times \{1, \ldots, n\}$ e siano, per $(j, i) \in I$, $y_{ji} \in F$ tali che

$$\sum_{(j,i) \in I} y_{ji} b_j a_i = 0 \ .$$

Allora

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{ji} b_j a_i) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} y_{ji} b_j \right) a_i$$

dove, per ogni $1 \leq i \leq n$, $\sum_{j=1}^{m} y_{ji} b_j \in L$. Poichè gli elementi a_i sono linearmente indipendenti su L, si ha, per ogni $1 \leq i \leq n$,

$$\sum_{j=1}^{m} y_{ji} b_j = 0$$

e, poichè gli elementi b_j sono indipendenti su F, si conclude che $y_{ji} = 0$ per ogni $(j, i) \in I$, provando così l'indipendenza del sistema $(b_j a_i)$.
Dunque $(b_j a_i)_{(j,i) \in I}$ è una base di M come spazio vettoriale su F e quindi

$$[M : F] = nm = [M : L][L : F] \ . \qquad \blacksquare$$

Elementi algebrici e trascendenti.

Sia F un sottocampo del campo E (se $E|F$ è estensione, F è identificato con la sua copia isomorfa in E), e sia $b \in E$. Denotiamo con

– $F[b]$ il minimo *sottoanello* di E che contiene $F \cup \{b\}$;

– $F(b)$ il minimo *sottocampo* di E che contiene $F \cup \{b\}$ (come al solito, esso esiste perché l'intersezione di sottocampi di E è un sottocampo). Chiaramente $F[b] \subseteq F(b)$.

Ricordo (limitandolo ai campi) il contenuto del Teorema 8.3 (Cap. IV):

Sia $E|F$ un'estensione di campi, e sia $b \in E$. Allora

$$F[b] = \left\{ \sum_{i=0}^{n} a_i b^i \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in F \right\} .$$

E, in generale, $F(b)$ risulterà isomorfo al campo delle frazioni di $F[b]$.
Queste notazioni si estendono nella maniera naturale. Siano $b_1, b_2, \ldots, b_n$ elementi di E; allora $F[b_1, b_2, \ldots, b_n]$ è il minimo sottoanello di E che contiene $F \cup \{b_1, b_2, \ldots, b_n\}$; mentre $F(b_1, b_2, \ldots, b_n)$ è il minimo sottocampo di E che contiene $F \cup \{b_1, b_2, \ldots, b_n\}$. Risulta immediato verificare che

$$F(b_1, b_2, \ldots, b_n) = (F(b_1, \ldots, b_{n-1}))(b_n) = F(b_1) \ldots (b_{n-1})(b_n).$$

In particolare

$$F(b_1)(b_2) = F(b_1, b_2) = F(b_2)(b_1).$$

Definizione. Sia $E|F$ un'estensione di campi, e sia $b \in E$.

(1) b si dice **algebrico** su F se esiste un polinomio $f \neq 0$ in $F[x]$ tale che $f(b) = 0$.

(2) b si dice **trascendente** su F se per ogni polinomio $f \neq 0$ in $F[x]$ si ha $f(b) \neq 0$.

Esempi. 1) Per ogni $n, m \in \mathbb{N}$, con $m \geq 1$, $\sqrt[m]{n}$ è un numero reale algebrico su $\mathbb{Q}$, essendo radice del polinomio $x^m - n \in \mathbb{Q}[x]$. Similmente, $i \in \mathbb{C}$ è algebrico su $\mathbb{Q}$ essendo radice del polinomio $x^2 + 1$.

2) Esistono numeri reali che sono trascendenti su $\mathbb{Q}$. Esempi sono i numeri π ed e. La dimostrazione di questo fatto è stata ottenuta da F. Lindemann nel 1882, ed è piuttosto complicata. Tuttavia, non è difficile provare che l'insieme dei numeri reali che sono algebrici su $\mathbb{Q}$ è un insieme numerabile; poichè l'insieme dei reali non è numerabile, da ciò segue che devono esistere numeri reali trascendenti su $\mathbb{Q}$ (anzi, che l'insieme di essi è più che numerabile).

3) L'elemento $x \in F(x)$ è trascendente su F (nell'estensione $F(x)|F$). Più in generale, si provi per esercizio che ogni $f/g \in F(x) \setminus F$ (con f, g polinomi su F, $g \neq 0$) è trascendente su F.

Esercizio. Si provi che $u = \sqrt{2} - \sqrt{3}$ è algebrico su $\mathbb{Q}$.

Soluzione. Occorre trovare un polinomio non nullo in $\mathbb{Q}[x]$ che ammette u come radice. Cominciamo con elevare u al quadrato

$$u^2 = 2 - 2\sqrt{2}\sqrt{3} + 3 = 5 - 2\sqrt{6}$$

da cui $2\sqrt{6} = 5 - u^2$ ed elevando ancora al quadrato

$$24 = u^4 - 10u^2 + 25$$

quindi u è radice del polinomio $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ e dunque è algebrico su $\mathbb{Q}$.

Osserviamo i seguente fatti banali. 1) Se $b \in F$ allora b è algebrico su F (è radice del polinomio $x - b \in F[x]$).

2) Siano $F \leq E \leq L$ campi, e sia $b \in L$: se b è algebrico su F, allora b è algebrico su E; mentre se b è trascendente su E allora è trascendente su F.

Veniamo ora ad una osservazione fondamentale. Sia $E|F$ un'estensione di campi, e sia $b \in E$. Abbiamo allora l'omomorfismo di sostituzione

$$\begin{array}{rccc} \sigma_b : & F[x] & \to & E \\ & f & \mapsto & f(b) \end{array}$$

la cui immagine è $F[b]$ ed il cui nucleo è $I_b = \ker(\sigma_b) = \{\ f \in F[x] \mid f(b) = 0\ \}$. Dal Teorema fondamentale di omomorfismo discende allora che

$$F[b] \simeq \frac{F[x]}{I_b}\ .$$

Vale dunque il seguente importante risultato.

Teorema 0.5.3 *Sia $E|F$ un'estensione di campi, e sia $b \in E$. Allora $F[b] \simeq F[x]/I_b$, dove $I_b = \{f \in F[x] \mid f(b) = 0\}$.*

Supponiamo che l'elemento $b \in E$ sia trascendente su F; allora, per definizione, l'ideale $I_b = \{f \in R[x] \mid f(b) = 0\}$ coincide con $\{0\}$; dunque, in questo caso, l'omomorfismo di sostituzione σ_b è iniettivo. Quindi $F[b]$ è isomorfo all'anello dei polinomi $F[x]$ (e non è un campo).
Se invece b è algebrico su F, per definizione esiste almeno un polinomio non nullo a coefficienti in F che ammette b come radice. Dunque l'ideale $\ker(\sigma_b) = I_b$ non è l'ideale nullo. Poiché F è un campo, I_b è un ideale principale, e sappiamo che un generatore f di I_b è un polinomio di grado *minimo* tra i polinomi non nulli di I_b. Fra i generatori di I_b ne esiste dunque uno e uno solo *monico* (ovvero con coefficiente direttivo uguale a 1): esso è detto **polinomio minimo** di b (su F).
Chiamiamo f il polinomio minimo di b su F ($b \in E$ algebrico su F), e supponiamo che f si fattorizzi in $F[x]$ come il prodotto di due polinomi, cioè che $f = gh$ con $g, h \in F[x]$ (ed, essendo $f \neq 0$, è anche $g \neq 0 \neq h$). Allora, applicando l'omomorfismo di sostituzione:

$$0 = f(b) = g(b)h(b)\ ;$$

poiché E è un campo, si deve avere $g(b) = 0$ oppure $h(b) = 0$. Sia $g(b) = 0$, allora, poiché $g \neq 0$, deve essere $\deg g = \deg f$, quindi $\deg h = 0$, che significa $h \in F^*$; similmente, se $h(b) = 0$ si ha $\deg h = \deg f$ e $g \in F^*$. Abbiamo quindi concluso che il polinomio f è **irriducibile** (vedi la Proposizione 8.6 del Cap. IV e gli esempi che seguono). [Viceversa, se $f \in F[x]$ è un polinomio monico irriducibile che ammette b come radice nel campo K, allora f è il polinomio minimo di b su F; infatti il polinomio minimo g di b divide f e quindi $\deg g = \deg f$ da cui $g = f$ (essendo entrambi monici).]
Ora, poiché f è irriducibile, per una proprietà fondamentale dei P.I.D. (e $F[x]$ è tale), $I_b = (f)$ è un ideale massimale, e pertanto $F[b] \simeq F[x]/(f)$ è un campo (Teorema 8.7 del Cap. IV).

Ricapitolando, se $b \in E$ è **algebrico** su F, allora $F[b]$ è un campo; quindi, in questo caso $F(b) = F[b]$.

Se invece b è **trascendente** su F, allora $F[b]$ è isomorfo all'anello dei polinomi $F[x]$. Poiché $F(b)$ è un campo che contiene $F[b] \simeq F[x]$, per la proprietà del campo delle frazioni, esiste un campo $K \simeq F(x)$ tale che $F[b] \leq K \leq F(b)$; ma $F(b)$ è il minimo sottocampo di E che contiene $F \cup \{b\}$ e quindi $K = F(b)$. In conclusione, abbiamo dunque provato il seguente risultato.

Teorema 0.5.4 *Sia $E|F$ un'estensione di campi e sia $b \in E$. Allora*

(1) *Se b è algebrico su F, allora $F(b) = F[b] \simeq F[x]/(f)$, dove f è il polinomio minimo di b su F. Inoltre, $[F[b] : F] = \deg f$.*

(2) *Se b è trascendente su F, allora $F(b) \simeq F(x)$. In tal caso $[F(b) : F] = \infty$.*

Corollario 0.5.5 *Sia $E|F$ un'estensione di campi e sia $b \in E$. Allora b è trascendente su F se e soltanto se $F(b) \neq F[b]$.*

In effetti, dobbiamo ancora chiarire compiutamente l'ultima affermazione al punto (1) del Teorema 5.4.
Sia $b \in E$ un elemento algebrico su F, e $f \in F[x]$ il suo polinomio minimo. Allora per quanto ricordato a proposito degli elementi dell'anello quoziente $F[x]/(f)$, e mediante l'isomorfismo $F[x]/(f) \to F[b]$ (dato da $g + (f) \mapsto g(b)$), otteniamo infatti la seguente descrizione degli elementi di $F[b]$.

Proposizione 0.5.6 *Sia $E|F$ un'estensione di campi, $b \in E$ un elemento algebrico su F, e $f \in F[x]$ il suo polinomio minimo. Allora ogni elemento di $F[b]$ si scrive in modo unico nella forma*

$$a_0 + a_1 b + \ldots + a_{n-1} b^{n-1}$$

dove $n = \deg f$ e $a_0, a_1, \ldots, a_{n-1} \in F$.

Da ciò segue che $(1, b, b^2, \ldots, b^{n-1})$ è una base di $F[b]$ come spazio vettoriale su F, e che quindi $[F[b] : F] = \dim_F(F[b]) = n = \deg f$.

Esempio. Abbiamo visto che $b = \sqrt{2} - \sqrt{3}$ è algebrico su $\mathbb{Q}$, e il suo polinomio minimo è $f = x^4 - 10x^2 + 1$; quindi $\mathbb{Q}[b] = \mathbb{Q}(b)$ è un campo di grado 4 su $\mathbb{Q}$. Troviamo l'espressione di $(b^2 + b - 1)^{-1} \in \mathbb{Q}(b)$ come combinazione a coefficienti razionali di $1, b, b^2, b^3$. Si può procedere brutalmente determinando i coefficienti $a_i \in \mathbb{Q}$ con l'imporre l'uguaglianza

$$(b^2 + b - 1)(a_0 + a_1 b + a_2 b^2 + a_3 b^3) = 1,$$

oppure si pone $g = x^2 + x - 1$ e poiché $(g, f) = 1$ (dato che f è irriducibile) mediante l'algoritmo di Euclide si determinano $h, t \in \mathbb{Q}[x]$ tali che $hg + tf = 1$; a questo punto, sostituendo b, si ha $1 = h(b)g(b) + t(b)f(b) = h(b)(b^2 + b - 1)$, per cui $b^{-1} = h(b)$. Così procedendo si trova che

$$1 = -\frac{x+2}{7} \cdot f + \frac{x^3 + x^2 - 10x - 9}{7} \cdot g$$

e pertanto $b^{-1} = \frac{1}{7}(b^3 + b^2 - 10b - 9)$.

Estensioni semplici.

Un'estensione $E|F$ di campi si dice si dice **estensione semplice** se esiste $b \in E$ tale che $E = F(b)$. In tal caso, b si dice un *elemento primitivo* di $E|F$. Ad esempio, $\mathbb{C} = \mathbb{R}[i]$ è una estensione semplice di $\mathbb{R}$. Il Teorema 5.4 fornisce una descrizione delle estensioni semplici. In particolare, notiamo il fatto seguente.

Proposizione 0.5.7 *Sia $E|F$ un'estensione semplice di campi. Allora $[E : F]$ è finito, oppure $E \simeq F(x)$.*

Esempi. 1) Sia $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$; allora $L|\mathbb{Q}$ è una estensione semplice. Proviamo infatti che $L = \mathbb{Q}[\sqrt{2} - \sqrt{3}]$. L'inclusione $\mathbb{Q}[\sqrt{3} - \sqrt{2}] \subseteq L$ è ovvia. Viceversa, osserviamo che

$$\sqrt{3} + \sqrt{2} = (\sqrt{3} - \sqrt{2})^{-1} \in \mathbb{Q}[\sqrt{3} - \sqrt{2}],$$

e quindi $\sqrt{2} = \frac{1}{2}[(\sqrt{3} + \sqrt{2}) - (\sqrt{3} - \sqrt{2}) \in \mathbb{Q}[\sqrt{3} - \sqrt{2}]$. Analogamente $\sqrt{3} \in \mathbb{Q}[\sqrt{3} - \sqrt{2}]$, e dunque $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} - \sqrt{3}]$.

2) $\mathbb{Q}(\pi, \sqrt{2})$ non è un'estensione semplice di $\mathbb{Q}$. Infatti, poiché π è trascendente su $\mathbb{Q}$, $[\mathbb{Q}(\pi, \sqrt{2}) : \mathbb{Q}] = \infty$, e dunque $\mathbb{Q}(\pi, \sqrt{2})$ non può essere un'estensione di $\mathbb{Q}$ ottenuta mediante l'aggiunzione di un elemento algebrico. Se fosse $\mathbb{Q}(\pi, \sqrt{2}) \simeq \mathbb{Q}(x)$, allora (vedi esercizio 1) ogni elemento di $\mathbb{Q}(\pi, \sqrt{2}) \setminus \mathbb{Q}$ sarebbe trascendente su $\mathbb{Q}$, e ciò è in contraddizione con il fatto che $\sqrt{2} \in \mathbb{Q}(\pi, \sqrt{2}) \setminus \mathbb{Q}$ è algebrico su $\mathbb{Q}$.

Osservazione. $\mathbb{R}$ non è una estensione semplice di $\mathbb{Q}$. Questo si può provare dimostrando che ogni estensione semplice di un campo numerabile è numerabile. Poichè $\mathbb{R}$ non è numerabile, non può essere una estensione semplice di $\mathbb{Q}$.

Citaimo, senza dimostrarlo, il seguente risultato di Steinitz.

Teorema 0.5.8 *Sia $E|F$ un'estensione di grado finito. Allora $E|F$ è semplice se e solo se il numero di campi intermedi tra F ed E è finito.*

Estensioni algebriche.

Un'estensione di campi $E|F$ si dice **algebrica** se ogni elemento di E è algebrico su F.

Proposizione 0.5.9 *Sia $E|F$ una estensione di campi di grado finito n. Allora ogni elemento di E è algebrico su F, e di grado $\leq n$ (e quindi $E|F$ è algebrica).*

Dimostrazione. Sia $E|F$ estensione con $[E : F] = n < \infty$, e sia $b \in E$. Ora, E è uno spazio vettoriale di dimensione n su F. Quindi gli $n + 1$ elementi $1, b, b^2, b^3, \ldots, b^n$ di E sono linearmente *dipendenti* su F, cioè esistono $a_0, a_1, a_2, \ldots, a_n$ in F non tutti nulli tali che

$$a_0 \cdot 1 + a_1 b + a_2 b^2 + \ldots + a_n b^n = 0$$

e dunque b è radice del polinomio non nullo $f = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$. Quindi, b è algebrico su F, ed il suo polinomio minimo divide f e pertanto ha grado al più $\deg f \leq n$. ∎

Corollario 0.5.10 *Sia $E|F$ un'estensione di campi, e sia $b \in E$ algebrico su F. Allora $F[b]$ è estensione algebrica di F*

DIMOSTRAZIONE. Sia $f \in F[x]$ il polinomio minimo di b su F, e sia $n = \deg f$. Allora $[F[b] : F] = n$, e si applica la Proposizione precedente. ∎

Un estensione $E|F$ tale che $[E : F] < \infty$ si dice estensione **finita**.

Proposizione 0.5.11 *Sia $E|F$ una estensione di campi. Allora $E|F$ è finita se e solo se esistono elementi $b_1, \ldots, b_m \in E$, algebrici su F, tali che $E = F[b_1, \ldots, b_m]$.*

DIMOSTRAZIONE. Sia $E = F[b_1, \ldots, b_m]$. Allora $b_1, \ldots, b_m$ sono algebrici su F (dire perché). Una ripetuta applicazione del punto (1) del Teorema 5.4 e della formula dei gradi porta a $[E : F] < \infty$; infatti:

$$\begin{aligned} [E : F] &= [F[b_1, \ldots, b_{n-1}][b_n] : F[b_1, \ldots, b_{n-1}]] \ldots\ldots [F[b_1][b_2] : F[b_1]]\, [F[b_1] : F] \leq \\ &\leq [F[b_n] : F] \cdot \ldots \cdot [F[b_2] : F] \cdot [F[b_1] : F] < \infty. \end{aligned}$$

Viceversa, sia $[E : F] = n < \infty$, e procediamo per induzione su n. Se $n = 1$, $E = F$ e non c'è nulla da provare. Sia $n \geq 2$, e sia $b_1 = b \in E \setminus F$. Allora $2 \leq [F(b) : F] = k \leq n$ per la Proposizione 5.9. Se $F(b) = E$ siamo a posto; altrimenti, applichiamo la formula dei gradi $n = [E : F] = [E : F(b)][F(b) : F]$, e quindi $[F(b) : F] = n/k < n$. Per ipotesi induttiva, esistono $b_2, \ldots, b_m \in E$ tali che $E = F(b)(b_2, \ldots, b_m)$, e quindi $E = F(b_1, b_2, \ldots, b_m)$ e abbiamo concluso. ∎

Teorema 0.5.12 *Sia $E|F$ una estensione di campi. Allora l'insieme degli elementi di E algebrici su F è un sottocampo di E (che ovviamente contiene F).*

DIMOSTRAZIONE. Siano $a, b \in E$ algebrici su F. Allora $[F(a) : F] = n$ e $[F(b) : F] = m$ con $1 \leq n, m \in \mathbb{N}$. Sia f il polinomio minimo di b su F. Allora, in particolare, $0 \neq f \in F(a)[x]$, e $f(b) = 0$. Pertanto b è algebrico su $F(a)$ e si ha $[F(a, b) : F(a)] \leq \deg f = m$. Quindi, per la formula dei gradi

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] \leq nm < \infty.$$

Dunque, per il Lemma 5.9, ogni elemento di $F(a, b)$ è algebrico su F. In particolare, sono quindi algebrici su F gli elementi $a - b,\ ab, a^{-1},\ b^{-1}$. Dunque somme, prodotti e inversi di elementi algebrici sono ancora elementi algebrici, provando così l'asserto. ∎

Se $E|F$ è una estensione di campi, il campo costituito da tutti gli elementi algebrici di E su F si chiama **chiusura algebrica** di F in E (la denoteremo con $\overline{F}_E$). Un caso molto importante, è quello dell'estensione $\mathbb{C}|\mathbb{Q}$. I numeri complessi che sono algebrici su $\mathbb{Q}$ si chiamano *numeri algebrici* e l'insieme di essi (ovvero la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$), che denotiamo con $\overline{\mathbb{Q}}$, si chiama il **campo dei numeri algebrici**. Osserviamo che $\mathbb{R} \not\subseteq \overline{\mathbb{Q}}$, infatti $\mathbb{R}$ contiene elementi trascendenti su $\mathbb{Q}$ (ad esempio $\pi \notin \overline{\mathbb{Q}}$).

Proposizione 0.5.13 $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$.

DIMOSTRAZIONE. Per ogni intero $n \geq 2$, sia $\delta_n = \sqrt[n]{2}$. δ_n è algebrico su $\mathbb{Q}$, ed il suo polinimio minimo è $x^n - 2$ (che è irriducibile per il Criterio di Eisenstein - Ccriterio 2 del Cap. IV). Dunque $\overline{\mathbb{Q}}$ contiene elementi il cui grado su $\mathbb{Q}$ è grande quanto si vuole, e dunque, per la Proposizione 5.9, $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$. ∎

Quest'ultimo fatto riconferma, in particolare, che il grado di $\mathbb{R}$ su $\mathbb{Q}$ è ∞.
Usando metodi del genere, possiamo infine fare la seguente osservazione.

Proposizione 0.5.14 *Siano $E|F$ e $L|E$ estensioni algebriche di campi. Allora l'estensione $L|F$ è algebrica.*

DIMOSTRAZIONE. Siano $E|F$ e $L|E$ estensioni algebriche, e sia $b \in L$. Poiché b è algebrico su E esistono elementi non tutti nulli $a_0, a_1, \ldots, a_m$ di E tali che

$$a_0 + a_1 b + \ldots + a_m b^m = 0.$$

Quindi b è algebrico su $K = F(a_1, a_2, \ldots, a_m)$, e $[K(b) : K] \leq m$. Poiché ciascun a_1 $(i = 1, 2, \ldots, m)$ è algebrico su F, K ha grado finito su F. Dunque

$$[K(b) : F] = [K(b) : K][K : F] < \infty.$$

Dalla Proposizione 5.9 segue che b è algebrico su F, così provando che l'estensione $L|F$ è algebrica. ∎

Commenti e trucchi.

$\mathbb{R}$ *contiene elementi trascendenti su* $\mathbb{Q}$. Iniziamo osservando che $\mathbb{Q}[x]$ è numerabile: infatti, se denotiamo con P_n l'insieme di tutti polinomi razionali di grado n, allora P_n è numerabile; poiché $\mathbb{Q}[x] = \bigcup_{n\in\mathbb{N}} P_n$, $\mathbb{Q}[x]$ è un'unione numerabile di insiemi numerabili, ed è pertanto numerabile. Ora, ogni elemento di $\mathbb{R}$ che sia algebrico su $\mathbb{Q}$ è radice di qualche polinomio non nullo in $\mathbb{Q}[x]$. Poiché un polinomio non nullo ha al più un numero finito di radici, l'insieme degli elementi di $\mathbb{R}$ algebrici su $\mathbb{Q}$ (la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{R}$) è unione numerabile di insiemi finiti, ed è dunque numerabile. Siccome $\mathbb{R}$ non è numerabile, questo significa che esistono elementi di $\mathbb{R}$ che non sono algebrici su $\mathbb{Q}$. (Osserviamo che ciò implica, in particolare, che $\mathbb{R}$ contiene un sottocampo isomorfo a $\mathbb{Q}(x)$.)

Formula dei gradi. La formula dei gradi risulta molto utile per eliminare i conti in diverse situazioni. Vediamo alcuni esempi.

1) Sia $F \leq L$ una estensione di campi. Proviamo che se $b \in L$ è algebrico su F di grado dispari allora $F[b] = F[b^2]$. Poichè b è algebrico, $F[b]$ e $F[b^2]$ sono campi. L'inclusione $F[b^2] \subseteq F[b]$ è ovvia. Supponiamo per assurdo $F[b] \not\subseteq F[b^2]$; ciò equivale a $b \notin F[b^2]$. Ora, b è radice del polinomio $g = x^2 - b^2 \in F[b^2][x]$, e siccome $b \notin F[b^2]$, g è il polinomio minimo di b sul campo $F[b^2]$. Poichè chiaramente $F[b^2, b] = F[b]$ si ha allora $[F[b] : F[b^2]] = 2$ e quindi, per la formula dei gradi,

$$[F[b] : F] = [F[b] : F[b^2]][F[b^2] : F] = 2[F[b^2] : F]$$

contro l'ipotesi che $[F[b] : F]$ sia dispari.

2) Calcolare il grado di $L = \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}]$ su $\mathbb{Q}$. $\sqrt[3]{3}$ è algebrico su $\mathbb{Q}$ ed il suo polinomio minimo su $\mathbb{Q}$ è $x^3 - 3$. Quindi $\mathbb{Q}[\sqrt[3]{3}]$ è un campo e $[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}] = 3$. Ora, $\sqrt{2} \notin \mathbb{Q}[\sqrt[3]{3}]$, perché, se così fosse, allora $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{3}]$ e per la formula dei gradi si avrebbe la conclusione assurda che $2 = [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$ divide $[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}] = 3$. Dunque $x^2 - 2$ è il polinomio minimo di $\sqrt{2}$ anche sul campo $\mathbb{Q}(\sqrt[3]{3})$. Applicando ancora la formula dei gradi si ha in conclusione

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{2}) : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

3) Siano $\zeta, \omega \in \mathbb{C}$, rispettivamente, una radice 7-ima ed una radice quinta dell'unità, diverse da 1. Proviamo che $\omega \notin \mathbb{Q}[\zeta]$. Infatti (vedi la Proposizione 4.7 del Cap. IV ed il commento seguente) i polinomi minimi su $\mathbb{Q}$ di ζ e ω sono, rispettivamente

$$x^6 + x^5 + \ldots + x + 1 \quad \text{e} \quad x^4 + x^3 + x^2 + x + 1.$$

Quindi $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 6$ e $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$; se fosse $\omega \in \mathbb{Q}[\zeta]$ allora $\mathbb{Q}[\omega] \subseteq \mathbb{Q}[\zeta]$ che, applicando la formula dei gradi come negli esempi precedenti, conduce ad una contraddizione.

Esercizio. Sia $f = x^3 - x + 1 \in \mathbb{Q}[x]$, e sia $b \in \mathbb{C}$ una radice di f. Si provi che $\mathbb{Q}(b)$ non contiene altre radici di f. Il facile studio del grafico della funzione reale $y = x^3 - x + 1$ associata al polinomio f, mostra che esso interseca l'asse delle ascisse in un solo punto. Dunque, f ha una sola radice reale α, e due radici complesse e non reali ζ e $\bar{\zeta}$, tra loro coniugate. Se $b = \alpha$, allora $\mathbb{Q}(b) \subseteq \mathbb{R}$, e dunque $\zeta \notin \mathbb{Q}(b)$ e $\bar{\zeta} \notin \mathbb{Q}(b)$. Sia allora $b = \zeta$. Poiché f è irriducibile su $\mathbb{Q}$ (è monico di terzo grado e non ha radici intere), esso è il polinomio minimo di ogni sua radice in $\mathbb{C}$. In particolare

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg f = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Se fosse $\alpha \in \mathbb{Q}(\zeta)$, allora $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$, e dunque, per la formula dei gradi $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$. Ciò è assurdo perché $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, mentre $\zeta \in \mathbb{C} \setminus \mathbb{R}$. Si osservi anche che $\bar{\zeta} \notin \mathbb{Q}(\zeta)$.

ESERCIZI

1. Sia F un campo e $F(x)$ il campo delle frazioni algebriche su F. Si provi che ogni elemento in $F(x) \setminus F$ è trascendente su F.

2. Calcolare $[\mathbb{Q}(\sqrt{5}, \sqrt{11}) : \mathbb{Q}]$.

3. Calcolare $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ con $\alpha \in \mathbb{C}$ tale che $\alpha^7 = 2$. Stessa domanda con α tale che $\alpha^6 = 4$.

4. Sia $a = \sqrt[3]{3} + 1313$. Qual è il grado del polinomio minimo di a su $\mathbb{Q}$? Qual è il grado del polinomio minimo di $a + i$ su $\mathbb{Q}$?

5. Siano $a, b \in \mathbb{C}$ elementi algebrici su $\mathbb{Q}$ tali che $[\mathbb{Q}(a) : \mathbb{Q}] = n$, $[\mathbb{Q}(b) : \mathbb{Q}] = m$ con $(n, m) = 1$. Si provi che $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$.

6. Sia $E = \mathbb{Q}(\sqrt[3]{2})$. Si provi che il polinomio $x^2 + x + 1$ è irriducibile in $E[x]$.

7. provare che i campi $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{5})$ non sono isomorfi.

8. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $x^3 - x + 1$, e in $\mathbb{Q}(\alpha)$ si consideri l'elemento $\beta = 2 - 3\alpha + 2\alpha^2$. Si provi che β è algebrico su $\mathbb{Q}$ e si trovi il suo polinomio minimo.

9. Sia $E|F$ un'estensione di grado finito e tale che per ogni coppia F_1, F_2 di campi intermedi tra F ed E si ha $F_1 \subseteq F_2$ oppure $F_2 \subseteq F_1$. Provare che $E|F$ è un'estensione semplice.

10. Sia A il campo dei numeri algebrici. Provare che ogni $z \in \mathbb{C} \setminus A$ è trascendente su A. Assumendo quindi il fatto che $\mathbb{C}$ è algebricamente chiuso, provare che A è un campo algebricamente chiuso.

11. Sia $E|F$ un'estensione algebrica. Si provi che se R è un sottoanello di E contenente F, allora R è un campo.

12. Siano $a, b \in \mathbb{C}$ algebrici su $\mathbb{Q}$, con $[\mathbb{Q}(a) : \mathbb{Q}] = p$, $[\mathbb{Q}(b) : \mathbb{Q}] = q$, p, q primi distinti e $p > q$. Sia f il polinomio minimo di a su $\mathbb{Q}$, e h il polinomio minimo di $a + b$ su $\mathbb{Q}$.

1) Provare che $[\mathbb{Q}(a, b) : \mathbb{Q}] = pq$.

2 Provare che f è il polinomio minimo di a su $\mathbb{Q}(b)$.

3) Provare che $\deg h \geq p$ e che $\deg h | pq$.

4) Sia, per assurdo, $\deg h = p$. Posto $h_1 = h(x + b) \in \mathbb{Q}(b)[x]$, provare che $h_1 = f \in \mathbb{Q}[x]$, e confrontando i coefficienti di grado $p - 1$ arrivare ad una contraddizione.

5) Concludere che $\deg h = pq$, e quindi che $\mathbb{Q}(a, b) = \mathbb{Q}(a + b)$.

0.6 Campi di spezzamento

Un omomorfismo iniettivo è detto **monomorfismo**.

Sia $f = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio irriducibile sul campo F. Allora l'ideale (f) di $F[x]$ è massimale; quindi $E = F[x]/(f)$ è un campo, ed è in modo naturale (mediante il monomorfismo definita da $a \mapsto a + (f)$, per ogni $a \in F$) un'estensione di F. Identificando gli elementi di F con le loro immagini in E, il polinomio f può essere visto come un polinomio a coefficienti in E. In E sia $\alpha = x + (f)$; allora

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \ldots + a_n\alpha^n = a_0 + a_1(x + (f)) + \ldots + a_n(x + (f))^n = \\ &= a_0 + (a_1 x + (f)) + \ldots + (a_n x^n + (f)) = \\ &= a_0 + a_1 x + \ldots + a_n x^n + (f) = f + (f) = (f) = 0_E. \end{aligned}$$

Dunque E è un'estensione di F che *contiene una radice di* f (e osserviamo che risulta $E = F[\alpha]$). Abbiamo dunque provato il seguente fatto fondamentale.

Proposizione 0.6.1 *Sia f un polinomio irriducibile sul campo F. Allora esiste un'estensione E di F che contiene una radice α di F, ed è tale che $E = F[\alpha]$.*

La situazione descritta da questa proposizione si chiama "aggiunzione" ad F di una radice di f.

Definizione. Sia F un campo, e $0 \neq f \in F[x]$. Un'estensione E di F si dice **campo di spezzamento** per f su F, se esistono elementi $a_1, \ldots, a_n \in E$ tali che

1) $f = a(x - a_1) \cdots (x - a_n)$ in $E[x]$ (dove a è il coefficiente direttivo di f);

2) $E = F[a_1, \ldots, a_n]$.

In altre parole, un campo di spezzamento per f su F è una estensione di F che contiene tutte le radici di f, ed è da queste generata su F. Il risultato che segue mostra come, in sostanza mediante aggiunzione successiva di radici, sia sempre possibile estendere F ad un campo di spezzamento per f.

Teorema 0.6.2 *Sia F un campo, e $0 \neq f \in F[x]$, con $\deg f = n$. Allora esiste un campo di spezzamento E per f su F, tale che $[E : F]$ divide $n!$.*

DIMOSTRAZIONE. Sia F un campo, e $0 \neq f \in F[x]$, con $\deg f = n$. Procediamo per induzione su n. Se $n = 1$ allora F è esso stesso campo di spezzamento. Sia $n \geq 2$. Supponiamo che f sia riducibile in $F[x]$. Dunque $f = f_1 f_2$ con $f_1, f_2 \in F[x]$ e, ponendo $d = \deg f_1$, $1 \geq d \leq n-1$ e $\deg f_2 = n - d < n$. Per ipotesi induttiva, esistono allora un campo di spezzamento E_1 per f_1 su F, ed un campo di spezzamento E per f_2 su E_1, inoltre $[E - 1 : F]$ divide $d!$ e $[E : E_1]$ divide $(n-d)!$. Si verifica facilmente dalla definizione che E è un campo di spezzamento per f su F; infine per la formula dei gradi si ha che $[E : F] = [E : E_1][E_1 : E]$ divide $d!(n-d)!$ che, a sua volta, divide $n!$. Supponiamo quindi che f si irriducibile in $F[x]$. Per la Proposizione 6.1, esiste allora un'estensione E_1 di F tale che $E_1 = F[\alpha]$ con α radice di f; inoltre, per il Teorema 5.4, $[E_1 : E] = n$. Ora, in $E_1[x]$, f si fattorizza come $(x-\alpha)g$, con $\deg g = n-1$. Per ipotesi induttiva, esiste un campo di spezzamento E per g su E_1, con $[E : E_1] | (n-1)!$. Come sopra, E è un campo di spezzamento per f su F, e si ha che $[E : F] = [E : E_1][E_1 : F]$ divide $(n-1)!n = n!$. ∎

Esempi. 1) Sia $1 \leq n \in \mathbb{N}$, e sia $\omega \in \mathbb{C}$ una radice *primitiva* n-esima dell'unità (quindi, $\omega = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$, con $0 \leq k \leq n-1$ e $(k, n) = 1$); sia $f = x^n - 1$. Allora, le radici in $\mathbb{C}$ di f sono tutte e sole le potenze ω^t con $t = 0, 1, \ldots, n-1$. Quindi $E = \mathbb{Q}(\omega) = \mathbb{Q}(1, \omega, \omega^2, \ldots, \omega^{n-1})$ è un campo di spezzamento per f su $\mathbb{Q}$. In $E[x]$,

$$x^n - 1 = (x-1)(x-\omega)\cdots(x-\omega^{n-1}).$$

Inoltre, se $n = p$ è un primo, allora sappiamo (come applicazione del criterio di Eisenstein) che il polinomio minimo di ω su $\mathbb{Q}$ è $1 + x + \ldots + x^{p-1}$, e pertanto $[E : \mathbb{Q}] = p - 1$. Se n non è un primo si può provare (lo vedremo più avanti) che $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$, dove ϕ è la funzione di Eulero (ed anche il numero di radici primitive n-esime dell'unità distinte).

2) Sia $f = x^3 - x + 1 \in \mathbb{Q}[x]$. Nell'esercizio a pag. 9 abbiamo osservato che f ha in $\mathbb{C}$ una redice reale α e due radici complesse e non reali ζ e $\bar{\zeta}$, tra loro coniugate. Abbiamo anche provato che l'aggiunzione a $\mathbb{Q}$ di una sola di queste radici non dà luogo ad un campo di spezzamento per f su $\mathbb{Q}$. Quindi un tale campo di spezzamento è dato da $E = \mathbb{Q}(\alpha, \zeta, \bar{\zeta}) = \mathbb{Q}(\alpha, \zeta)$. Ora, poiché f è irriducibile su $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. In $\mathbb{Q}(\alpha)[x]$ si ha $f = (x-\alpha)g$, dove g è un polinomio irriducibile di grado 2 (se g fosse riducibile allora $\mathbb{Q}(\alpha)$ conterrebbe tutte le radici di f) che ammette ζ e $\bar{\zeta}$ come radici. Dunque $[\mathbb{Q}(\alpha)(\zeta) : \mathbb{Q}(\alpha)] = 2$ e, per la formula dei gradi

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!.$$

Estensioni normali.

Siano $E|F$ e $M|\overline{F}$ estensioni di campi, e supponiamo che sia dato un isomorfismo di campi $^- : F \to \overline{F}$ (con $a \mapsto \bar{a}$ per ogni $a \in F$). Ci chiediamo sotto quali condizioni sia possibile estendere tale isomorfismo a un monomorfismo $E \to M$.
Osserviamo in primo luogo che è possibile estendere in modo canonico l'isomorfismo $^- : F \to \overline{F}$ ad un isomorfismo (che denoteremo ancora con $^-$) dall'anello dei polinomi $F[x]$ in $\overline{F}[x]$; definito da, se $g = a_0 + a_1x + \ldots + a_nx^n \in F[x]$,

$$\bar{g} = \bar{a}_0 + \bar{a}_1x + \ldots + \bar{a}_nx^n.$$

Lemma 0.6.3 *Sia $^- : F \to \overline{F}$ ad un isomorfismo di campi. Sia E estensione di F tale che $E = F[b]$ con b algebrico su F, e sia f il polinomio minimo di b. Sia M un'estensione di $\overline{F}$. Allora l'isomorfismo $^-$ si estende ad un monomorfismo $E \to M$ se e solo se M contiene qualche radice di $\bar{f}$. Inoltre, se c è una radice in M di $\bar{f}$, allora esiste un unico monomorfismo $\phi : E \to M$ che estende $^-$ e tale che $\phi(b) = c$; e si ha $\phi(E) = \overline{F}[c]$.*

Dimostrazione. Supponiamo che esista un monomorfismo $\phi : E \to M$ che estende l'isomorfismo $^-$ (cioè tale che $\phi(a) = \bar{a}$ per ogni $a \in F$). Allora, se $f = a_0+a_1x+\ldots+a_n$,

$$\bar{f}(\phi(b)) = \bar{a}_0 + \ldots + \bar{a}_n\phi(b)^n = \phi(a_0) + \ldots + \phi(a_n)\phi(b)^n = \phi(f(b)) = 0$$

e dunque $\phi(b) \in M$ è una radice di $\bar{f}$.
Viceversa, sia $c \in M$ una radice di $\bar{f}$, e ricordiamo che ogni elemento di $E = F[b]$ si scrive in modo unico nella forma $a_0 + a_1b + a_{n-1}b^{n-1}$, con $a_0, a_1, \ldots, a_n \in F$. Allora l'applicazione $\phi : E \to M$ definita da, per ogni $u = a_0 + a_1b + a_{n-1}b^{n-1} \in E$,

$$\phi(u) = \bar{a}_0 + \bar{a}_1c + \bar{a}_{n-1}c^{n-1},$$

definisce un monomorfismo da E in M che chiaranente estende $^-$. Infatti, l'isomorfismo $F[x] \to \overline{F}[x]$ (che manda f in $\bar{f}$, che quindi è il polinomio minimo di c su $\overline{F}$) manda l'ideale (f) nell'ideale $(\bar{f})$. Ne segue che $F[x]/(f)$ è isomorfo a $\overline{F}[x]/(\bar{f})$ (mediante l'applicazione $g + (f) \mapsto \bar{g} + (\bar{f})$). L'applicazione ϕ definita sopra è la composizione dei tre isomorfismi

$$E = F[b] \to \frac{F[x]}{(f)} \to \frac{\overline{F}[x]}{(\bar{f})} \to \overline{F}[c],$$

con l'inclusione di $\overline{F}[c]$ in M. ϕ è quindi un monomorfismo da E in M. Infine, è chiaro che ϕ è l'unico monomorfismo da E in M che estende $^-$ e manda b in c. ∎

Vediamo subito una applicazione del Lemma 6.3, che stabilisce l'unicità (a meno di isomorfismo) del campo di spezzamento di un polinomio.

Teorema 0.6.4 *Sia $^- : F \to \overline{F}$ ad un isomorfismo di campi, e $0 \neq f \in F[x]$. Siano, rispettivamente, E un campo di spezzamento per f su F, e M un campo di spezzamento per $\bar{f}$ su $\overline{F}$. Allora l'isomorfismo $^-$ si estende ad un isomorfismo $E \to M$.*

Dimostrazione. Procediamo per induzione su $[E : F]$. Se $[E : F] = 1$, allora $E = F$ e di conseguenza f si fattorizza in $F[x]$ come prodotto di polinomi lineari; ne segue che anche $\bar{f}$ si fattorizza in $\overline{F}[x]$ come prodotto di polinomi lineari e quindi $M = \overline{F}$.

Sia quindi $[E : F] \geq 2$. Allora, in $F[x]$, $f = gh$ dove g è un fattore irriducibile e non lineare. Di conseguenza, in $\overline{F}[x]$, $\bar{f} = \bar{g}\bar{h}$. Siano, rispettivamente, $b \in E$ una radice di g, e $c \in M$ una radice di $\bar{g}$. Per il Lemma 6.3, l'isomorfismo $F \to \overline{F}$ si estende ad un unico isomorfismo $\eta : F[b] \to \overline{F}[c]$ tale che $\eta(b) = c$. Ora, E è un campo di spezzamento per f su $F[b]$ e M è un campo di spezzamento per $\bar{f}$ su $\overline{F}[c]$. D'altra parte

$$[E : F] = [E : F[b]][F[b] : F] = [E : F[b]](\deg g) \geq [E : F[b]] \cdot 2,$$

e quindi $[E : F[b]] < [E : F]$. Per ipotesi induttiva esiste dunque un isomorfismo $\bar{\eta} : E \to M$ che estende η. Chiaramente, $\bar{\eta}$ estende anche l'isomorfismo $F \to \overline{F}$. ∎

Abbiamo enunciato e provato il Lemma 6.3 ed il Teorema 6.4 in forma generale, a partire cioè da un arbitrario isomorfismo $F \to \overline{F}$, questo (in particolare per il Teorema) per poter applicare con maggior facilità l'induzione; in molti casi (ma non sempre), saremo in seguito interessati alla situazione in cui $\overline{F} = F$ e l'isomorfismo di partenza è l'identità. Si tratta di un caso importante, che giustifica la seguente definizione.

Definizione. Siano E e M estensioni del medesimo campo F. Allora un monomorfismo $\phi : E \to M$ tale che $\phi(a) = a$ per ogni $a \in F$ si dice **F-monomorfismo**. Se ϕ è un isomorfismo, si chiama **F-isomorfismo**.

Corollario 0.6.5 *Sia F un campo, $0 \neq f \in F[x]$, e siano E e M campi di spezzamento per f su F. Allora esiste un F-isomorfismo di E in M.*

Dimostrazione. È un caso particolare del Teorema 6.4. ∎

Proviamo ora un'altra importante proprietà dei campi di spezzamento.

Proposizione 0.6.6 *Sia E un campo di spezzamento su F per il polinomio $f \in F[x]$, e sia g un polinomio irriducibile in $F[x]$ che ha una radice in E. Allora E contiene un campo di spezzamento per g su F.*

Dimostrazione. Poiché E è campo di spezzamento di f, $E = F(a_1, \ldots, a_n)$, dove $a_1, \ldots, a_n$ sono le radici di f. Sia g un polinomio irriducibile in $F[x]$ che abbia una radice $b \in E$. Sia M un campo di spezzamento per g su E.
Sia $b_1 \in M$ una radice di g. Ora, $E_1 = F(b_1, a_1, \ldots, a_n) = E(b_1)$ è un campo di spezzamento per f su $F(b_1)$, mentre $E = F(b, a_1, \ldots, a_n)$ è un campo di spezzamento per f su $F(b)$. Poiché g è il polinomio minimo su F sia di b che di b_1, per il Lemma 6.3 esiste un F-isomorfismo $\eta : F(b) \to F(b_1)$ tale che $\eta(b) = b_1$. Siccome g ha coefficienti in F, $\eta(g) = g$. Dunque, per il Teorema 6.4, η si può estendere ad un F-isomorfismo $\eta_1 : E \to E_1$. Siccome η_1 fissa F, si ha $[E : F] = [E_1 : F]$. Ma $E_1 \supseteq E$ e quindi, per la formula dei gradi, $[E_1 : E] = 1$, cioè $E_1 = E$. Questo implica che $b_1 \in E$. Poiché ciò vale per ogni radice b_1 di g in M, e M è generato su E da tali radici, si conclude che $M = E$ e pertanto che E contiene un campo di spezzamento per g su F. ∎

Un'estensione algebrica di campi $E|F$ che soddisfa la conclusione della Proposizione precedente si chiama estensione normale.

Definizione. Un'estensione algebrica di campi $E|F$ si dice **normale** se E contiene un campo di spezzamento di ogni polinomio irriducibile in $F[x]$ che ha almeno una radice in E.

La proposizione 6.6 viene completata col seguente risultato.

Teorema 0.6.7 *Sia $E|F$ un'estensione di campi. Allora sono equivalenti*

(1) $E|F$ è finita e normale;

(2) E è un campo di spezzamento per qualche polinomio in $F[x]$.

Dimostrazione. (2) $\Rightarrow$ (1) : è la Proposizione 6.6.
(1) $\Rightarrow$ (2). Sia E un'estensione finita e normale del campo F. Poiché $E|F$ è finita, per la Proposizione 5.11, esistono elementi $b_1, \ldots, b_n$ di E (algebrici su F) tali che $E = F[b_1, \ldots, b_n]$. Per ciascun $i = 1, \ldots, n$ sia $f_i \in F[x]$ il polinomio minimo di b_i su F, e poniamo $f = f_1 f_2 \ldots f_n$. Poiché $E|F$ è un'estensione normale, E contiene un campo di spezzamento su F per ciascuno dei polinomi f_i. Ne segue che E contiene un campo di spezzamento per f. Siccome poi E è generato su F da radici di f, si conclude che E è un campo di spezzamento per f su F. ∎

Radici multiple.

Sia F campo, $0 \neq f \in F[x]$, E un campo di spezzamento per f, e $\alpha \in E$ una radice di f. Allora dal teorema di Ruffini segue che, in $E[x]$, $(x-\alpha)$ divide f. Si chiama **molteplicità** (algebrica) della radice α il massimo intero positivo m_α tale che $(x-\alpha)^{m_\alpha}$ divide f (chiaramente, essa non dipende dal particolare campo di spezzamento). La radice α si dice radice *semplice* se $m_\alpha = 1$, e radice *multipla* se $m_\alpha \geq 2$.
Osserviamo che, ancora per il Teorema di Ruffini, α è una radice semplice se e soltanto se, in $E[x]$, $f = (x-\alpha)g$ con $g(\alpha) \neq 0$.

Ricordiamo ora la definizione di polinomio *derivato*: sia $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ un polinomio a coefficienti nel campo F. Il suo polinomio derivato f' è:

$$f' = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}.$$

Le seguenti regole di derivazione sono di immediata verifica.

Siano $f, g \in F[x]$. Allora

$$(f+g)' = f' + g'$$
$$(fg)' = f'g + g'f.$$

Lemma 0.6.8 *Sia F campo, $0 \neq f \in F[x]$, e α una radice di f (in un campo di spezzamento E). Allora α è una radice multipla se e solo se $f'(\alpha) = 0$.*

DIMOSTRAZIONE. Siano f ed α come nelle ipotesi. Supponiamo che α sia radice multipla di f; quindi, in $E[x]$, $f = (x-\alpha)^2 g$ (con $g \in E[x]$) e dunque, applicando la regola di derivazione riportata sopra,

$$f' = 2(x-\alpha)g + (x-\alpha)^2 g' = (x-\alpha)(2-(x-\alpha)g')$$

da cui segue che $f'(\alpha) = 0$.
Viceversa, sia α radice semplice di f. Allora, in $E[x]$, $f = (x-\alpha)g$ e $g(\alpha) \neq 0$. Dunque

$$f'(\alpha) = g(\alpha) + (\alpha-\alpha)g'(\alpha) = g(\alpha) \neq 0$$

concludendo la dimostrazione. ∎

Nella situazione che stiamo considerando, supponiamo che il polinomio monico $f \in F[x]$ sia irriducibile. Allora f è il polinomio minimo di ogni sua radice in qualche estensione di F. In particolare è il polinomio minimo della radice $\alpha \in E$. Poiché $f' \in F[x]$ e $\deg f' = degf - 1$, si osserva dunque che α è radice anche di f' (e quindi è radice multipla di f) se e soltanto se $f' = 0$. Assumiamo ulteriormente che $char(F) = 0$; allora, si verifica facilmente che, se f è un polinomio di grado ≥ 1 (non necessariamente irriducibile) in $F[x]$, si ha $f' \neq 0$.
Mettendo insieme queste due osservazioni abbiamo dunque la seguente

Proposizione 0.6.9 *Sia F un campo di caratteristica 0, e sia $f \in F[x]$ un polinomio irriducibile. Allora tutte le radici di f, in un campo di spezzamento E, sono semplici (quindi, se $\deg f = n$, f ha n radici distinte in E).*

I campi di caratteristica 0 non sono i soli a godere della proprietà stabilita dalla Proposizione precedente (tali campi sono detti *perfetti*). Ad esempio, essa sussiste anche per i campi finiti. Ma non tutti i campi sono perfetti. Ad esempio si consideri il campo delle frazioni algebriche su $\mathbb{Z}_p$ (p un primo), ovvero $F = \mathbb{Z}_p(t)$ (abbiamo chiamato t l'ideterminata per riservare x a denotare un'indeterminata su F). Nell'anello dei polinomi $F[x]$ si consideri $f = x^p - t$. Si può provare che f è irriducibile in $F[x]$, mentre d'altra parte $f' = px^{p-1} = 0$ (dato che, in un campo di caratteristica p moltiplicare per p dà sempre 0). Quindi, per il Lemma 6.8, le radici di f in un campo di spezzamento sono multiple (si può anche provare che, se α è una radice di f in E, allora, in $E[x]$, $f = (x-\alpha)^p$).

Un polinomio a coefficienti nel campo F si dice *separabile* se ogni suo fattore irriducibile ha tutte radici semplici in un suo campo di spezzamento (dunque, se $char(F) = 0$ ogni polinomio $0 \neq f \in F[x]$ è separabile).
Un'estensione di campi $E|F$ si dice **separabile** se è algebrica e per ogni $b \in E$ il polinomio minimo di b in $F[x]$ è separabile. Un'immediata conseguenza della Proposizione 6.9 è il seguente fatto

Teorema 0.6.10 *Sia F un campo di caratteristica 0. Allora ogni estensione algebrica $E|F$ è separabile.*

ESERCIZI

1. Sia F un campo, e siano $a \in F$ e $1 \leq n \in \mathbb{N}$, tali che il polinomio $f = x^n - a$ è irriducibile in $F[x]$. Sia u una radice di F in un'opportune estensione di F, e sia $m \geq 1$, $m|n$. Si provi che il grado di u^m su F è n/m, e si determini il polinomio minimo di u^m su F.

2. Sia F campo con $char(F) \neq 2$, e sia $f \in F[x]$ un polinomio irriducibile di grado 2. Sia E campo di spezzamento per f, ed $a \in E$ una radice di f. Si provi che $E = F[a]$, e che esiste $d \in E$ tale che $E = F[d]$ e $d^2 \in F$.

3. Si provi che $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ è il campo di spezzamento su $\mathbb{Q}$ di $x^3 - 2$.

4. Per ciascuno dei seguenti polinomi razionali si determini un campo di spezzamento contenuto in $\mathbb{C}$, e se ne calcoli il grado su $\mathbb{Q}$:

- $f = x^5 - 2$.
- $g = x^4 - x^2 + 4$.

5. Sia $E|F$ un'estensione normale, e sia L campo intermedio ($F \leq L \leq E$): si provi che $E|L$ è un'estensione normale.

6. Sia F un campo e sia $E|F$ estensione tale che $[E : F] = 2$. Si provi che $E|F$ è un'estensione normale.

7. Si provi che $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ è un'estensione normale.

8. Si provi che le estensioni $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ sono normali, mentre l'estensione $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ non lo è.

9. Sia E campo di spezzamento per un polinomio f sul campo F, e sia K un campo tale che $F \leq K \leq E$. Si provi che ogni F-monomorfiamo $K \to E$ si può estendere ad un F-automorfismo di E.

10. Sia F, e $0 \neq f \in F[x]$. Si provi che tutte le radici di f in un campo di spezzamento sono semplici se e solo se (in $F[x]$) $(f, f') = 1$.

11. In una opportuna estensione di $\mathbb{Z}_3$, si trovino le eventuali radici multiple del polinomio $x^7 + x^5 + x^4 - x^3 - x^2 - x + 1$.

12. Sia $E|F$ un'estensione separabile, e sia L un campo intermedio: si provi che $E|L$ e $L|F$ sono estensioni separabili.

0.7 Gruppo di Galois

Sia $E|F$ un'estensione di campi, e siano ψ, ϕ F-automorfismi di E (ovvero automorfismi del campo E che lasciano fisso ogni elemento del sottocampo F); è chiaro allora che anche

ϕ^{-1} e $\phi \circ \psi$ sono F-automorfismi di di E. Dunque l'insieme degli F-automorfismi di E è un sottogruppo del gruppo degli automorfismi di E: esso viene chiamato **Gruppo di Galois** dell'estensione $E|F$, e si denota con $Gal(E|F)$.

Esempi. 1) Sia F un campo di caratteristica diversa da 2, ed $E = F[b]$ dove $b \in E$ è tale che $b \notin F$ e $b^2 \in F$. Allora, il polinomio minimo di b su F è $x^2 - b^2$, le cui radici in E sono b e $-b$ (che sono distinte perché $\text{char}(F) \neq 2$). Poiché E è generato su F dall'elemento b (più esplicitamente: gli elementi di E sono tutti del tipo $a_0 + a_1 b$, con $a_0, a_1 \in F$), un F-automorfismo di E è univocamente determinato dall'immagine di b tramite esso. Dunque, segue dal Lemma 6.3, che $Gal(E|F) = \{\iota_E, \phi\}$ dove ϕ è l'unico F-automorfismo di E tale che $\phi(b) = -b$. Precisamente, ϕ è dato da $\phi(a_0 + a_1 b) = a_0 - a_1 b$, per ogni $a_0 + a_1 b \in E$.
In particolare, questo si applica al caso di $\mathbb{C} = \mathbb{R}(i)$, per cui deduciamo che $Gal(\mathbb{C}|\mathbb{R})$ è costituito dall'identità e dall'automorfismo di coniugio di $\mathbb{C}$.

2) $Gal(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = \{\iota\}$. Infatti, sempre per il Lemma 6.3, se ϕ è un $\mathbb{Q}$-automorfismo di $\mathbb{Q}(\sqrt[3]{2})$, allora $\phi(\sqrt[3]{2})$ deve di necessità essere una radice del polinomio minimo $g = x^3 - 2$ di $\sqrt[3]{2}$ su $\mathbb{Q}$; ma $\mathbb{Q}(\sqrt[3]{2})$ non contiene radici di g diverse da $\sqrt[3]{2}$, dato che queste ultime non sono reali mentre $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Dunque ogni $\mathbb{Q}$-automorfismo di $\mathbb{Q}(\sqrt[3]{2})$ deve mandare $\sqrt[3]{2}$ in se stesso. Poiché $\mathbb{Q}(\sqrt[3]{2})$ è generato su $\mathbb{Q}$ da $\sqrt[3]{2}$, si conclude che l'identità è l'unico elemento del gruppo di Galois di $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$.

3) Siano p un numero primo positivo, $\omega \in \mathbb{C}$ una radice primitiva p-esima dell'unità, e poniamo $E = \mathbb{Q}(\omega)$. Gli automorfismi di E che fissano i razionali sono chiaramente determinati dall'immagine di ω. Se σ è un tale $\mathbb{Q}$-automorfismo, allora $\sigma(\omega)$ deve essere una radice dell'unità diversa da 1, quindi $\sigma(\omega) = \omega^k$ per un $1 \leq k \leq p-1$, e pertanto $|Gal(E|\mathbb{Q})| \leq p-1$. D'altra parte, per ogni $1 \leq k \leq p-1$ si ha che $E = \mathbb{Q}(\omega^k)$, e ω^k (così come ω) è radice del polinomio irriducibile $1+x+\ldots+x^{p-1}$. Per il Lemma 6.3 esiste dunque un $\mathbb{Q}$-automorfismo σ_k di E tale che $\sigma_k(\omega) = \omega^k$. Dunque $Gal(E|\mathbb{Q}) = \{\iota = \sigma_1, \sigma_2, \ldots, \sigma_{p-1}\}$. In particolare, $|Gal(E|\mathbb{Q})| = p - 1 = [E : \mathbb{Q}]$ (osserviamo che, in questo esempio, E è un campo di spezzamento su $\mathbb{Q}$).

4) $Gal(\mathbb{R}|\mathbb{Q}) = \{\iota\}$. Infatti, l'identità è il solo automorfismo (di campo!) di $\mathbb{R}$. Sia ϕ automorfismo di $\mathbb{R}$, allora da $\phi(1) = 1$ segue che $\phi(z) = z$ per ogni $z \in \mathbb{Z}$, e da ciò che $\phi(u) = u$ per ogni $u \in \mathbb{Q}$ (lo si dimostri per bene). Inoltre se $0 \leq r \in \mathbb{R}$, allora $0 \leq \phi(r)$: infatti se $r \geq 0$, esiste $a \in \mathbb{R}$ tale che $r = a^2$ e, quindi, poiché ϕ è omomorfismo, $\phi(r) = \phi(a^2) = \phi(a)^2 \geq 0$. Supponiamo, per assurdo, che esista $r \in \mathbb{R}$ tale che $\phi(r) \neq r$; possiamo assumere che $\phi(r) > r$ (il ragionamento nel caso opposto è identico). Allora. per la densità dei razionali nei reali, esiste $u \in \mathbb{Q}$ con $r < u < \phi(r)$, e quindi, per quanto osservato sopra,

$$0 > \phi(u - r) = \phi(u) - \phi(r) = u - \phi(r) < 0,$$

che è una contraddizione. Quindi $\phi = \iota_{\mathbb{R}}$.

Sia $G = Gal(E|F)$ il gruppo di Galois dell'estensione di campi $E|F$, e sia H un sottogruppo di G. Si pone

$$Inv_E(H) = \{\ b \in E \mid \sigma(b) = b \ \text{ per ogni } \sigma \in H\ \}.$$

Dalle definizioni date, e mediante semplici verifiche, segue ora facilmente la seguente ossevazione.

Lemma 0.7.1 *Sia $E|F$ un'estensione di campi. Allora*

(1) se L è un campo intermedio (cioè $F \leq L \leq E$) allora $Gal(E|L) \leq Gal(E|F)$;

(2) se $H \leq Gal(E|F)$ allora $Inv_E(H)$ è un sottocampo di E contenente F.

DIMOSTRAZIONE. Per esercizio. ∎

Questo Lemma mostra che il funtore $Gal(E|\ \cdot\ )$ associa ad ogni campo intermedio dell'estensione $E|F$ un sottogruppo di $Gal(E|F)$; e viceversa il funtore $Inv_E(\ \cdot\ )$ associa ad ogni sottogruppo di $Gal(E|F)$ un campo intermedio dell'estensione $E|F$. Il teorema fondamentale della Teoria di Galois afferma che per certe estensioni (in particolare per i campi di spezzamento su $\mathbb{Q}$ di polinomi razionali), questi due funtori sono l'uno l'inverso dell'altro, e che vi è pertanto una corrispondenza biunivoca tra l'insieme dei sottogruppi di $Gal(E|F)$ e quello dei campi intermedi dell'estensione $E|F$.

Teorema 0.7.2 *Sia F un campo, ed E campo di spezzamento su F per il polinomio $0 \neq f \in F[x]$. Se le radici di f in E sono tutte semplici allora $|Gal(E|F)| = [E : F]$.*

DIMOSTRAZIONE. Procediamo per induzione su $[E : F]$. Se $[E : F] = 1$ allora $E = F$ e non c'è nulla da provare.
Sia quindi $[E : F] > 1$. Allora, in $F[x]$, f ha un fattore irriducibile g di grado $n = \deg g$ almeno 2. Per ipotesi, E contiene n radici distinte di g: $b = b_1, b_2, \ldots, b_n$. Per il Lemma 6.3, per ogni $i = 1, 2, \ldots, n$, esiste un unico F-isomorfismo $\tau_i : F[b] \to F[b_i]$ tale che $\tau_i(b) = b_i$. Ora, E è un campo di spezzameno per il polinomio f sia su $F[b]$ che su $F[b_i]$, e quindi, per il Teorema 6.4, ciascun τ_i $(i = 1, 2, \ldots, n)$ può essere esteso ad un isomorfismo $\eta_i : E \to E$. È chiaro che gli η_i sono F-automorfismi di E, cioè $\eta_i \in Gal(E|F)$ per ogni $i = 1, 2, \ldots, n$ (osserviamo che possiamo scegliere $\eta_1 = \iota_E$).
Sia ora $H = Gal(E|F[b])$. Per il Lemma 7.1, H è un sottogruppo di $G = Gal(E|F)$. Proviamo che G è l'unione disgiunta

$$G = \eta_1 H \cup \eta_2 H \cup \ldots \cup \eta_n H \tag{3}$$

(ovvero che $\{\eta_1, \eta_2, \ldots, \eta_n\}$ è un sistema di rappresentanti delle classi laterali sinistre di G modulo H). Proviamo innanzi tutto che tali classi sono distinte. Siano $1 \leq i, j \leq n$ tali che $\eta_i H = \eta_j H$; allora $\eta_j^{-1}\eta_i = \sigma \in H$, quindi $\eta_i = \eta_j \sigma$, e dunque

$$b_i = \eta_i(b) = \eta_j\sigma(b) = \eta_j(\sigma(b)) = \eta_j(b) = bj$$

da cui segue $i = j$. Proviamo ora che l'unione è tutto G. Sia $\alpha \in G$; poiché α fissa ogni elemento di F, $\alpha(b)$ deve essere una radice di g, dunque $\alpha(b) = b_i$, per un unico $i = 1, 2, \ldots, n$. Ne segue che $\eta_i^{-1}\alpha(b) = b$, e dunque che $\eta_i^{-1}\alpha \in Gal(E|F[b]) = H$, cioè $\alpha \in \eta_i H$, provando così l'uguaglianza (3). Dunque, applicando l'ipotesi induttiva $|H| = [E : F[b]]$ (che sussiste perché E è campo di spezzamento per f su $F[b]$), si ha

$$|G| = |H|n = [E : F[b]] \deg g = [E : F[b]][F[b] : F] = [E : F],$$

e la dimostrazione è completa. ∎

Definizione. Un'estensione di campi $E|F$ che sia *finita, normale e separabile* si dice **estensione di Galois**.

Segue quindi dai Teoremi 6.7 e 6.10 che se F è un campo di caratteristica 0, ed E è un campo di spezzamento per un polinomio $0 \neq f \in F[x]$, allora l'estensione $E|F$ è un'estensione di Galois.

Teorema 0.7.3 *Se $E|F$ è un'estensione di Galois allora $|Gal(E|F)| = [E : F]$.*

DIMOSTRAZIONE. Sia $E|F$ un'estensione di Galois. Poiché $[E : F] < \infty$, esistono $b_1, \ldots, b_n \in E$ tali che $E = F[b_1, \ldots, b_n]$. Per ogni $i = 1, 2, \ldots, n$, sia $f_i \in F[x]$ il polinomio minimo di b_i su F, e sia $f \in F[x]$ il prodotto degli f_i distinti. Poiché $E|F$ è normale, E contiene un campo di spezzamento per ciascuno degli f_i e quindi contiene un campo di spezzamento per f su F; ma $b_1, \ldots, b_n$ sono tutti radici di f, e dunque E è un campo di spezzamento per f. Ora, poiché $E|F$ è separabile, ciascun f_i ha solo radici semplici. Siccome polinomi monici irriducibili distinti non possono avere radici comuni, concludiamo che le radici di f sono tutte semplici. Dunque, per il Teorema 7.2, $|Gal(E|F)| = [E : F]$. ∎

Come esempio, determiniamo il gruppo di Galois dell'estensione $E|\mathbb{Q}$ dove E è il campo di spezzamento del polinomio $f = x^3 - x + 1$. Abbiamo visto che, in $\mathbb{C}$, f ha tre radici $\alpha, \zeta, \bar{\zeta}$, di cui α è reale e $\zeta, \bar{\zeta}$ sono complesse coniugate. Quindi, un campo di spezzamento per f è $E = \mathbb{Q}(\alpha, \zeta, \bar{\zeta}) = \mathbb{Q}(\alpha, \zeta)$ e, come abbiamo visto, $[E : F] = 6$. Sia $\Omega = \{\alpha, \zeta, \bar{\zeta}\}$, e sia $G = Gal(E|F)$. Se $\sigma \in G$, allora σ manda radici di f in radici di f, e dunque induce una permutazione dell'insieme Ω. Pertanto è possibile definire (semplicemente mediante restrizione) un'azione di G su Ω. Se $\sigma \in G$ fissa tutti gli elementi di Ω, allora, poiché E è da questi generato su F, σ deve essere l'identità su E. Dunque l'azione di G su Ω è fedele e pertanto G è isomorfo ad un sottogruppo di $Sym(\Omega) \simeq S_3$. Ma, per il Teorema 7.2, $|G| = [E : F] = 6$. Quindi $G \simeq S_3$. Descriviamo ora i campi degli invarianti $Inv_E(H)$ dei sottogruppi H di G. Osserviamo innanzi tutto che ogni $\sigma \in G$ è univocamente determinato dalla permutazione che esso induce sull'insieme Ω delle radici di f, e che (in questo caso! dato che $G \simeq S_3$) ogni permutazione di Ω è indotta da un elemento di G. Osserviamo anche (lo si provi usando la formula dei gradi) che $E \cap \mathbb{R} = \mathbb{Q}[\alpha]$. Chiaramente, $Inv_E(\{\iota\}) = E$. Sia $\tau_0 \in G$ tale che induce su Ω la permutazione che fissa α e scambia tra loro ζ e $\bar{\zeta}$; $H_0 = \langle \tau_0 \rangle$ è un sottogruppo di ordine 2 di G. Ora, τ_0 è la restrizione a E dell'automorfismo di coniugio, e quindi $Inv_E(H_0) = E \cap \mathbb{R} = \mathbb{Q}[\alpha]$. Sia $\tau_1 \in G$ tale che τ_1 fissa ζ e scambia α e $\bar{\zeta}$, e sia $H_1 = \langle \tau_1 \rangle$. Allora, chiaramente, $\mathbb{Q}[\zeta] \leq Inv_E(H_1)$; se fosse $Q[\zeta] < Inv_E(H_1)$ allora, per la formula dei gradi, $Inv_E(H_1) = E$, ma ciò non è perché $\alpha \notin Inv_E(H_1)$: dunque $Inv_E(H_1) = Q[\zeta]$. Allo stesso modo si prova che, posto $H_2 = \langle \tau_2 \rangle$, dove $\tau_2 \in G$ è tale che fissa $\bar{\zeta}$ e scambia α con ζ, allora $Inv_E(H_2) = Q[\bar{\zeta}]$. A questo punto, osserviamo che

$$Inv_E(G) \leq Inv_E(H_0) \cap Inv_E(H_1) = \mathbb{Q}[\alpha] \cap \mathbb{Q}[\zeta] = \mathbb{Q}$$

e dunque $Inv_E(G) = \mathbb{Q}$.
Infine, sia $\gamma \in G$ tale che $\gamma(\alpha) = \zeta,\ \gamma(\zeta) = \bar{\zeta},\ \gamma(\bar{\zeta}) = \alpha$. Allora $A = \langle \gamma \rangle = \{\iota, \gamma, \gamma^{-1}\}$ è un sottogruppo di ordine 3 di G (che corrisponde al sottogruppo alterno A_3 di S_3). Sia

$$d = (\alpha - \zeta)(\zeta - \bar{\zeta})(\bar{\zeta} - \alpha).$$

Allora $\gamma(d) = (\zeta - \bar{\zeta})(\bar{\zeta} - \alpha)(\alpha - \zeta) = d$, e dunque $d \in Inv_E(A)$. Ora, $d \notin \mathbb{Q}$, infatti: $\tau_0(d) = (\alpha - \bar{\zeta})(\bar{\zeta} - \zeta)(\zeta - \alpha) = -d$. Quindi $\mathbb{Q} < \mathbb{Q}[d] \leq Inv_E(A)$; e siccome $Inv_E(A) \neq E$, si deduce che $Inv_E(A) = \mathbb{Q}[d]$. Osserviamo che da $\tau_0(d) = -d$ segue $\tau_0(d^2) = d^2$, e similmente si verifica che $\tau_1(d^2) = d^2$; quindi $d^2 \in Inv_E(\tau_0) \cap Inv_E(\tau_1) = \mathbb{Q}[\alpha] \cap \mathbb{Q}[\zeta] = \mathbb{Q}$. Con un po' di conti, tenendo conto che $a^3 = \alpha - 1$ e delle identità fornite dal confronto dei coefficienti in

$$x^3 - x + 1 = (x - \alpha)(x - \zeta)(x - \bar{\zeta})$$

si trova che $d^2 = -23$. In particolare, $[\mathbb{Q}[d] : \mathbb{Q}] = 2$. Ricapitolando abbiamo trovato che

$$Inv_E(\{\iota\}) = E, \quad Inv_E(G) = \mathbb{Q}, \quad Inv_E(A) = \mathbb{Q}[i\sqrt{23}],$$

$$Inv_E(H_0) = Q[\alpha], \quad Inv_E(H_1) = Q[\zeta], \quad Inv_E(H_2) = Q[\bar{\zeta}]$$

Notiamo come per ogni sottogruppo H di G si abbia $[Inv_E(H) : \mathbb{Q}] = [G : H]$. Questo non è un caso, come vedremo più avanti col teorema fondamentale della teoria di Galois. Quello stesso Teorema garantisce che, poiché quelli che abbiamo esaminato sono tutti i sottogruppi di $G \simeq S_3$, i campi di invarianti che abbiamo trovato sono tutti i campi intermedi nell'estensione $E|\mathbb{Q}$.

Permutazioni delle radici. Concludiamo questo paragrafo col formalizzare esplicitamente un'osservazione che abbiamo già fatto nel corso dello svolgimento di alcuni degli esempi, che è semplice, ma fondamentale nella pratica.
Sia $E|F$ un'estensione di campi, sia $G = Gal(E|F)$, e $f \in F[x]$. Se $b \in E$ è una radice di f, allora, per ogni $\alpha \in G$, si ha (poiché α fissa i coefficienti di F),

$$f(\alpha(b)) = \alpha(f(b)) = \alpha(0) = 0.$$

Quindi, *gli elementi di $Gal(E|F)$ trasformano le radici in E di ciascun polinomio f a coefficienti in F in radici di f.* In altri termini, per ogni $f \in F[x]$, $Gal(E|F)$ opera come un gruppo di permutazioni sull'insieme delle radici di f in E. Particolarmente significativo è il caso in cui E è il campo di spezzamento di $f \in F[x]$. In questo caso, E è generato da F e dall'insieme $\mathbb{R} = \{b_1, \ldots, b_n\}$ delle radici di f. $G = Gal(E|F)$ oper su R come un gruppo di permutazioni; inoltre, poiché E è generato da R, un F-automorfismo di E che fissa ogni elemento di R è l'identità, pertanto l'azione di G su R è fedele, e quindi G è isomorfo ad un sottogruppo di $Sym(R) = S_n$. Osserviamo infine che se $f \in F[x]$ è irriducibile, F separabile, ed E è un campo di spezzamento, allora $Gal(E|F)$ opera transitivamente sull'insieme R delle radici in E di f; in generale, per campi di spezzamento, le orbite di $Gal(E|F)$ su R sono costituiscono gli insiemi delle radici dei fattori irriducibili di f (in $F[x]$).

ESERCIZI

1. Sia F un campo, ed E campo di spezzamento su F per il polinomio $0 \neq f \in F[x]$. Si provi che $|Gal(E|F)| \leq [E : F]$.

2. Se K e L sono sottocampi del medesimo campo E, denotiamo con $K \vee L$ il minimo sottocampo di E contenete $K \cup L$. Sia $E|F$ un'estensione di campi. Provare che:

i) Se K e L sono campi intermedi di $E|F$, allora $\mathrm{Gal}(E|K) \cap \mathrm{Gal}(E|L) = \mathrm{Gal}(E|K \vee L)$;

ii) Se H e T sono sottogruppi di $Gal(E|F)$, allora $\mathrm{Inv}_E(H) \cap \mathrm{Inv}_E(T) = \mathrm{Inv}_E(\langle H, T\rangle)$.

3. Sia F un campo infinito, e $F(x)$ il suo campo delle frazioni algebriche. Si provi che $\mathrm{Gal}(F(x)|F)$ è infinito.

4. Sia $E = \mathbb{Q}(\sqrt{3}5, \sqrt[3]{5})$. Dire se l'estensione $E|\mathbb{Q}$ è normale.

5. Provare che l'estensione $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ è di Galois, e provare che il gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q})$ è isomorfo al prodotto diretto di due gruppi ciclici di ordine 2.

6. Sia $E = \mathbb{Q}(r)$, dove $r \in \mathbb{C}$ è una radice del polinomio $g = x^3 + x^2 - 2x - 1$. Verificare che anche $r' = r^2 - 2$ è radice di g. Determinare quindi $\mathrm{Gal}(E|\mathbb{Q})$, e provare che $E|\mathbb{Q}$ è un'estensione normale.

7. Sia E il campo di spezzamento del polinomio $f = x^3+3x^2+3$ su $\mathbb{Q}$. Provare che $\mathrm{Gal}(E|\mathbb{Q}) \simeq S_3$.

8. Sia E il campo di spezzamento di $f = x^4 - 7x^3 + 2x - 14$ su $\mathbb{Q}$. Determinare l'ordine del gruppo di Galois $\mathrm{Gal}(E|\mathbb{Q})$. Stessa domanda con $f = x^4 + 2x^2 - 2$.

9. Determinare il gruppo $\mathrm{Gal}(E|\mathbb{Q})$, dove E è campo di spezzamento su $\mathbb{Q}$ per il polinomio $f = x^4 + 1$.

10. Determinare il gruppo $\mathrm{Gal}(E|\mathbb{Q})$, dove E è campo di spezzamento su $\mathbb{Q}$ per il polinomio $f = (x^3 - 2)(x^2 - 3)$.

11. Sia $f \in \mathbb{Q}[x]$, con $\deg f \geq 2$, e sia E campo di spezzamento per f su $\mathbb{Q}$, e sia $G = \mathrm{Gal}(E|\mathbb{Q})$. Provare che $|G| \leq n!$, e che se f non è irriducibile allora $|G| \leq (n-1)!$.

0.8 Campi finiti

In questo paragrafo descriveremo brevemente le principali caratteristiche dei campi finiti. Iniziamo col ricordare un'utile proprietà numerica dei coefficienti binomiali.
Sia p un primo (positivo) e sia $1 \leq i \leq p-1$. Allora p divide il numeratore ma non il denominatore di

$$\binom{p}{i} = \frac{p(p-1)(p-2)\dots(p-i+1)}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (i-1) \cdot i}$$

e quindi p divide $\binom{p}{i}$.

Lemma 0.8.1 *Sia F un campo di caratteristica prima p. Allora l'applicazione $\Phi : F \to F$ definita da $\Phi(a) = a^p$, per ogni $a \in F$, è un monomorfismo (di campi).*

Dimostrazione. Constatato che $\Phi(0) = 0$ e $\Phi(1) = 1$, siano $a, b \in F$. Allora, poiché F è commutativo, $\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b)$. Applicando lo sviluppo di Newton della potenza di un binomio (che vale ancora perché F è commutativo), si ha

$$\Phi(a+b) = (a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

Per quanto osservato sopra a proposito dei coefficienti binomiali, e ricordando che, in un anello di caratteristica p, i multipli $p \cdot a$ si annullano, si ricava che, per ogni $i = 1, \dots, p-1$, $\binom{p}{i} a^i b^{p-i} = 0$, e dunque

$$\Phi(a+b) = a^p + b^p = \Phi(a) + \Phi(b)$$

provando pertanto che Φ è un omomorfismo. Poiché F è un campo, $\ker(\Phi) = \{0\}$, e quindi Φ è iniettivo (cioè è un monomorfismo). ∎

Il monomorfismo Φ descritto nel Lemma precedente si chiama *endomorfismo di Frobenius* di F. Se F è finito allora Φ è biettiva (infatti è una applicazione iniettiva da un insieme finito in sé, ed è quindi suriettiva) e pertanto è un automorfismo di F. Osserviamo inoltre che per ogni $k \geq 0$, ed ogni $a \in F$

$$\Phi^k(a) = a^{p^k}.$$

Sia ora p un primo fissato e $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ il campo con p elementi. Per $1 \leq n \in \mathbb{N}$ denotiamo con $GF(p^n)$ il campo di spezzamento su $\mathbb{Z}_p$ del polinomio

$$f = x^{p^n} - x$$

(GF sta per Galois Field). Sia $D \subseteq GF(p^n)$ l'insieme delle radici di f. Ricordando che per il Teorema di Eulero-Fermat, $a^p = a$ per ogni $a \in \mathbb{Z}_p$, si osserva subito che $\mathbb{Z}_p \subseteq D$. Inoltre, poiché

$$f' = p^n x^{p^n-1} - 1 = -1$$

(infatti anche la caratteristica di $\mathbb{Z}_p[x]$ è p), il Lemma 6.8 assicura che le radici di f sono tutte semplici e dunque, per il teorema di Ruffini, $|D| = p^n$. Siano ora $a, b \in D$, con $b \neq 0$; allora, per il lemma 8.1 (opportunamente reiterato)

$$f(ab^{-1}) = (ab^{-1})^{p^n} - ab^{-1} = a^{p^n}(b^{-1})^{p^n} - ab^{-1} = ab^{-1} - ab^{-1} = 0$$

$$f(a-b) = (a-b)^{p^n} - (a-b) = a^{p^n} - b^{p^n} - (a-b) = (a^{p^n} - a) - (b^{p^n} - b) = 0.$$

Dunque, ab^{-1} e $a-b$ appartengono a D, e pertanto D è un sottocampo di $GF(p^n)$. Poiché $GF(p^n)$ è il campo generato da $\mathbb{Z}_p$ e da D, si conclude che $D = GF(p^n)$. In particolare, $|GF(p^n)| = p^n$. Abbiamo così provato la prima parte del seguente risultato.

Teorema 0.8.2

(1) Sia p un primo e sia $1 \leq n \in \mathbb{N}$. Allora esiste un campo di ordine p^n.

(2) Due campi finiti dello stesso ordine sono isomorfi.

Dimostrazione. Rimane da dimostrare il punto (2). Poiché (Proposizione 5.1) ogni campo finito ha ordine una potenza di un primo, è sufficiente provare che ogni campo F di ordine p^n (p primo e $1 \leq n \in \mathbb{N}$) è isomorfo a $GF(p^n)$. Innanzi tutto, poiché il sottoanello fondamentale di F è il campo $\mathbb{Z}_p$, si ha che F è un'estensione di $\mathbb{Z}_p$. Ora, il gruppo moltiplicativo F^* degli elemento non nulli di F ha ordine $|F| - 1 = p^n - 1$. Ricordando che se G è un gruppo finito e $g \in G$ allora $g^{|G|} = 1$, si ha $a^{p^n-1} = 1$ per ogni $a \in F^*$, e quindi (tenendo conto che $0^{p^n} = 0$),

$$a^{p^n} = a$$

per ogni $a \in F$. Quindi gli elementi di F sono tutti radici del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$. Poiché $|F| = p^n$ si conclude che F è un campo di spezzamento su $\mathbb{Z}_p$ per $x^{p^n} - x$, e dunque è isomorfo a $GF(p^n)$. ∎

Ci proponiamo ora di dire qualcosa a proposito dell'estensione $E|\mathbb{Z}_p$, dove $E = GF(p^n)$. Innanzi tutto, osserviamo che

$$[GF(p^n) : \mathbb{Z}_p] = n.$$

Infatti se $d = [GF(p^n) : \mathbb{Z}_p]$, allora $GF(p^n)$ *come spazio vettoriale su* $\mathbb{Z}_p$ è isomorfo a $\mathbb{Z}_p^{(d)}$ (l'insieme delle d-uple ordinate a coefficienti in $\mathbb{Z}_p$) e dunque, confrontando gli ordini, si ha $d = n$.
Sia Φ l'automorfismo di Frobenius di $E = GF(p^n)$. Poiché, per il Teorema di Eulero-Fermat, $\Phi(a) = a^p = a$ per ogni $a \in \mathbb{Z}_p$, Φ è un $\mathbb{Z}_p$-automorfismo, cioè $\Phi \in Gal(E|\mathbb{Z}_p)$. Ora, come abbiamo osservato sopra, per ogni $b \in E$,

$$\Phi^n(b) = b^{p^n} = b$$

e quindi $\Phi^n = \iota_E$. Mentre, se $1 \leq k < n$, esiste almeno un $b \in E$ tale che $\Phi^k(b) = b^{p^k} \neq b$ (dato che il polinomio $x^{p^k} - x$ ha al più p^k radici in E), e quindi $\Phi^k \neq \iota$. Dunque, nel gruppo $Gal(E|\mathbb{Z}_p)$, $|\langle\Phi\rangle| = n$.
D'altra parte, per il Teorema 7.2, $|Gal(E|\mathbb{Z}_p)| = [E : \mathbb{Z}_p] = n$. Quindi

$$Gal(E|\mathbb{Z}_p) = \langle\Phi\rangle = \{\iota, \Phi, \Phi^2, \ldots, \Phi^{n-1}\}.$$

La dimostrazione dell'esistenza di campi finiti di ordine p^n che abbiamo dato è abbastanza concettuale. Di fatto, per costruire un campo di tale ordine si procede nel modo seguente. Si trova un polinomio *irriducibile* $f \in \mathbb{Z}_p[x]$ di grado n, e uno c'è senz'altro tra i fattori irriducibili di $x^{p^n} - x$ (questa affermazione verrà chiarita tra poco). Quindi si considera il campo $E = \mathbb{Z}_p[x]/(f)$. Poiché gli elementi di E si scrivono tutti in modo unico nella forma

$$a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + (f) \qquad (a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_p)$$

si conclude che $|E| = p^n$.

Esempio. Poichè il polinomio $x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$ non ha radici in $\mathbb{Z}_5$, esso non ha fattori di grado 1 in $\mathbb{Z}_5[x]$, e quindi è irriducibile in $\mathbb{Z}_5[x]$. Dunque

$$E = \frac{\mathbb{Z}_5[x]}{(x^3 + x + \overline{1})}$$

è un campo di ordine $5^3 = 125$ (e pertanto coincide col campo di spezzamento del polinomio $x^{125} - x$ su $\mathbb{Z}_5$).

Gruppo moltiplicativo di un campo.

In questo paragrafo dimostriamo la seguente importante proprietà del gruppo moltiplicativo degli elementi non nulli di un campo.

Teorema 0.8.3 *Ogni sottogruppo* **finito** *del gruppo moltiplicativo di un campo è ciclico.*

Per la dimostrazione di questo Teorema abbiamo biosogna di una caratterizzazione dei gruppi ciclici, che è fornita dal seguente Lemma.

Lemma 0.8.4 *Sia G un gruppo commutativo finito di ordine n. Se per ogni divisore d di n, G ha al più un sottogruppo di ordine d, allora G è ciclico.*

DIMOSTRAZIONE. Sia G un gruppo di ordine n che soddisfa alle ipotesi del Lemma. Allora $G = P_1 \times P_2 \times \cdots \times P_s$, dove i P_i è (l'unico) p_i-sottogruppo di Sylow di G per ogni divisore primo p_i di n. Chiaramente ogni P_i soddisfa le ipotesi del Lemma e poichè il prodotto di gruppi ciclici di ordine coprimo è ciclico, è sufficiente provare il Lemma nel caso in cui G è un p-gruppo per un primo p. In tal caso, sia $g \in G$ un elemento del massimo ordine possibile $|g| = p^m$. Sia $y \in G$, con $|y| = p^s$; per la scelta di g si ha $s \leq m$. Ora $T =< g^{p^{m-s}} >$ è un sottogruppo di $< g >$ e quindi di G di ordine p^s. Poiché, per ipotesi, G ha un unico sottogruppo di ordine p^s, deve essere $T =< y >$ e quindi $y \in < g >$. Dunque $G =< g >$ è un gruppo ciclico, e il Lemma è provato. ∎

DIMOSTRAZIONE DEL TEOREMA 8.3. Sia F un campo, e sia G un sottogruppo finito del gruppo moltiplicativo F^*. Sia $|G| = n$; proviamo che G soddisfa le ipotesi del Lemma 8.4. G è commutativo perchè tale è il gruppo moltiplicativo di un campo. Sia d un divisore di n e sia $T \leq G$ con $|T| = d$. Allora, per ogni $a \in T$ si ha $a^d = 1$. Quindi ogni $a \in T$ è una radice in F del polinomio $x^d - 1 \in F[x]$. Poichè F è un campo, il numero di radici di tale polinomio è al più $d = |T|$. Quindi T coincide con l'insieme delle radici in F del polinomio $x^d - 1$. Questo prova che G ha al più un sottogruppo di ordine d. Per il Lemma 8.4, G è ciclico. ∎

Esempio 1. Sia $n \geq 2$ e sia U_n l'insieme delle radici complesse n-esime dell'unità. Allora U_n è un sottogruppo del gruppo moltiplicativo $\mathbb{C}^*$ e contiene esattamente n elementi. Dunque U_n è un gruppo ciclico di ordine n (rispetto alla moltiplicazione). Per quanto sappiamo sui gruppi ciclici, il numero di generatori di U_n è $\phi(n)$ dove ϕ è la funzione di Eulero. I generatori di U_n si sono le radici n-esime **primitive** dell'unità, ovvero i numeri complessi

$$cos\frac{2k\pi}{n} + i \cdot sin\frac{2k\pi}{n}$$

con $1 \leq k \leq n-1$ e $(k, n) = 1$.

Esempio 2. Consideriamo il campo di ordine 125

$$E = \frac{\mathbb{Z}_5[x]}{(x^3 + x + \overline{1})}$$

costruito in un precedente esempio. Il suo gruppo moltiplicativo E^* è un gruppo ciclico di ordine $124 = 4 \cdot 31$. Sia α un suo generatore; dunque $E^* =< \alpha >= \{1, \alpha, \alpha^2, \ldots, \alpha^{123}\}$. Notiamo che posto $\beta = \alpha^{31}$ allora $\langle\beta\rangle$ è un sottogruppo di E^* di ordine 4 e quindi i suoi elementi sono radici del polinomio $x^4 - 1$; d'altra parte, per il teorema di Fermat, ogni elemento non nullo $a \in \mathbb{Z}_5$ è tale che $a^4 = 1$; quindi si ha $\langle\beta\rangle = \mathbb{Z}_5 \setminus \{0\}$.

Naturalmente, l'esempio 2 si generalizza ad un qualsiasi campo finito. Se p è un primo e $E = GF(p^n)$, allora il gruppo moltiplicativo E^* degli elementi non nulli di E è ciclico ed ha ordine $p^n - 1$. I suoi generatori (ce ne sono in numero di $\phi(p^n - 1)$) si chiamano

elementi primitivi del campo finito E. Se α è un tale elemento primitivo, gli elementi non nulli di E sono quindi tutti potenze di α, e questo procura una rappresentazione degli elementi di E particolarmente utile in alcune applicazioni computazionali (ma, computazionalmente, trovare α non è una cosa facile).
Osserviamo infine che se α è un elemento primitivo del campo $GF(p^n)$, allora chiaramente $GF(p^n) = \mathbb{Z}_p(\alpha)$. Siccome $[GF(p^n) : \mathbb{Z}_p] = n$, il polinomio minimo f di α su $\mathbb{Z}_p$ ha grado n. Poiché α (in quanto elemento di $GF(p^n)$) è anche una radice di $g = x^{p^n} - x$, si ha che f divide g. Dunque, come avevamo già sostenuto in precedenza, $x^{p^n} - x$ ammette un fattore irriducibile di grado n.

Anche l'esempio 1 si può considerare a partire da un qualsiasi campo F. Sia $n \geq 1$, e supponiamo inoltre, se $charF = p$, che n sia coprimo con p. Allora le radici del polinomio $f = x^n - 1_F$ in un suo campo di spezzamento E sono tutte semplici, dato che $f' = nx^{n-1} \neq 0$ non ha radici in comune con f, e costituiscono un sottogruppo U di ordine n del gruppo moltiplicativo di E. Per il Teorema 8.3, U è un gruppo ciclico. I suoi generatori si chiamano *radici primitive n-esime* sul campo F.

ESERCIZI

1. Si determini il numero di fattori irriducibili di $x^{125} - x$ in $\mathbb{Z}_5$[x].

2. Dire quanti sono i polinomi irriducibili di grado 2 in $\mathbb{Z}_p[x]$ (p un primo).

3. Si costruiscano campi di ordine 8, 27, 81 e 121.

4. Siano $1 \leq m \leq n \in \mathbb{N}$, e sia p un numero primo. Si provi che esiste un monomorfismo $GF(p^m) \to GF(p^n)$ se e solo se $m|n$.

5. Sia E un campo di ordine p^n e sia $g \in \mathbb{Z}_p[x]$ un polinomio irriducibile di grado m, con $m|n$. Si provi che g ha una radice in E.

6. Si provi che ogni estensione di campi finiti è normale.

7. Sia E un campo di ordine 125. Dire quante radici hanno in E i seguenti polinomi:
$x^3 - 1,\ x^4 - 1,\ x^{31} - 1,\ x^7 - 1$. Provare che $x^2 + x + 1$ è irriducibile in $E[x]$.

8. Sia F un campo finito di caratteristica p, e sia $f \in F[x]$. Si provi che $f' = 0$ se e solo se $f \in F[x^p]$. Ricordando che se F è finito allora il suo endomorfismo di Frobenius è un automorfismo, e che quindi $F = F^p = \{a^p \mid a \in F\}$, dedurre che se $f \in F[x]$ ha grado almeno 1 e $f' = 0$, allora esiste $g \in F[x]$ tale che $f = g^p$. Concludere che se F è un campo finito ogni polinomio di $F[x]$ è separabile.

9. Sia F un campo di caratteristica p, e sia $a \in F$. Si provi che se $a \notin F^p$, allora $x^p - a$ è irriducibile in $F[x]$, ma ha un'unica radice in un suo campo di spezzamento. Si deduce che se $F = \mathbb{Z}_p(t)$ è il campo delle frazioni algebriche su $\mathbb{Z}_p$, allora $x^p - t \in F[x]$ è un polinomio irriducibile ma non separabile.

10. Sia F un campo finito di ordine $q = p^n$. Si provi che

i) se $p = 2$, ogni elemento di F è un quadrato;

ii) se $p > 2$, allora F contiene esattamente $\frac{q+1}{2}$ elementi che sono quadrati ;

iii) se $p > 2$, allora gli elementi di F che sono quadrati sono tutte e sole le radici del polinomio $x^{(q+1)/2} - x$. [sugg.: si studi la applicazione $F \to F$ definita da $a \mapsto a^2$ per ogni $a \in F$].

11. Si provi che in un campo finito ogni elemento é somma di due quadrati.

0.9 Connessione di Galois

In questo capitolo dimostreremo il teorema fondamentale della Teoria di Galois. Iniziamo con un risultato tecnico ma utile.

Lemma 0.9.1 (Lemma di Artin) *Sia G un gruppo finito di automorfismi del campo E, e sia $F = \mathrm{Inv}_E(G)$. Allora $[E : F] \leq |G|$.*

Dimostrazione. Sia $|G| = n$, e sia $G = \{g_1 = \iota, g_2, \ldots, g_n\}$. Siano $x_1, x_2, \ldots, x_{n+1}$ elementi di E, e consideriamo il sistema di equazioni lineari su E

$$\begin{cases} g_1(x_1)t_1 + g_1(x_2)t_2 + \ldots + g_1(x_{n+1})t_{n+1} = 0 \\ g_2(x_1)t_1 + g_2(x_2)t_2 + \ldots + g_2(x_{n+1})t_{n+1} = 0 \\ \cdot \\ \cdot \\ g_n(x_1)t_1 + g_n(x_2)t_2 + \ldots + g_n(x_{n+1})t_{n+1} = 0 \end{cases} \tag{4}$$

che è un sistema omogeneo con n equazioni e $n + 1$ incognite. Per la teoria generale dei sistemi di equazioni lineari (che vale sopra un campo qualunque), tale sistema ammette soluzione non nulla $(y_1, y_2, \ldots, y_{n+1}) \neq (0, 0, \ldots, 0)$ ad elementi in E. Tra queste soluzioni ne scegliamo una $(b_1, b_2, \ldots, b_{n+1})$ con il massimo numero possibile di zeri; osservando che, eventualmente riordinando gli x_i, possiamo suppore $b_1 \neq 0$, e moltiplicando poi per b^{-1} (dato che il sistema è omogeneo) possiamo supporre che $b_1 = 1$. Quindi, per ogni $1 \leq j \leq n$,

$$g_j(x_1)b_1 + g_j(x_2)b_2 + \ldots + g_j(x_{n+1})b_{n+1} = 0.$$

Sia $g \in G$. Applicando g all'identità di sopra

$$gg_j(x_1)g(b_1) + gg_j(x_2)g(b_2) + \ldots + gg_j(x_{n+1})g(b_{n+1}) = 0. \tag{5}$$

per ogni $1 \leq j \leq n$. Poiché G è un gruppo, $\{gg_1, gg_2, \ldots, gg_n\} = G$, e quindi le identità (5) significano che la $(n+1)$-upla di elementi di E $(g(b_1), g(b_2), \ldots, g(b_n))$ è una soluzione del sistema (4). Dunque, anche

$$(g(b_1) - b_1,\ g(b_2) - b_2,\ \ldots,\ g(b_{n+1}) - b_{n+1}) \tag{6}$$

è soluzione di (4). Ora, poiché g è isomorfismo di E, se $b_i = 0$ si ha $g(b_i) - b_i = 0$, e inoltre $g(b_1) - b_1 = g(1) - 1 = 1 - 1 = 0$. Dunque, la soluzione (6) ha un numero di zeri maggiore di $(b_1, \ldots, b_{n+1})$ e quindi, per la scelta di quest'ultima, la (6) deve essere la soluzione nulla; cioè, per ogni $i = 1, \ldots, n+1$,

$$g(b_i) = b_1.$$

Ciò vale per ogni $g \in G$, e quindi $b_i \in F = \mathrm{Inv}_E(G)$ per ogni $i = 1, \ldots, n+1$. Ricordando che avevamo posto $g_1 = \iota$ la prima equazione del sistema (4) dà allora

$$x_1 b_1 + x_2 b_2 + \ldots + x_{n+1} b_{n+1} = 0$$

con i $b_i \in F$ non tutti nulli. Questo prova che gli $n+1$ elementi $x_1, x_2, \ldots, x_{n+1}$ di E sono linearmente dipendenti su F. Quindi, come spazio vettoriale su F, la dimensione di E è al più n, ovvero $[E : F] \leq n$. ∎

Ricordiamo che un'estensione di campi $E|F$ si dice di Galois se è finita, normale e separabile. In particolare se $char(F) = 0$ ed E è un campo di spezzamento per un polinomio su F, allora $E|F$ è un'estensione di Galois.

Lemma 0.9.2 *Sia $E|F$ un'estensione di Galois e $F \leq L \leq E$ un campo intermedio. Allora $E|L$ è un'estensione di Galois.*

Dimostrazione. Sia $E|F$ di Galois e L campo con $F \leq L \leq E$. Poiché $[E : F] < \infty$, anche $[E : L] < \infty$. Sia $g \in L[x]$ un polinomio irriducibile monico che ha una radice $b \in E$. Sia $f \in F[x]$ il polinomio minimo di b su F. Poiché g è il polinomio minimo di b su L si ha che, in $L[x]$, g divide f. Siccome $E|F$ è normale, E contiene un campo di spezzamento per f su F, e quindi contiene un campo di spezzamento per g su L. Ciò prova che $E|L$ è un'estensione normale.
Infine, sia $u \in E$ e sia $g \in L[x]$ il polinomio minimo di u su L; mostriamo che g è separabile (cioè che ha tutte radici semplici in un suo campo di spezzamento). Come prima, sia f il polinomio minimo di u su F. Allora, in $L[x]$, $g|f$. Poiché $E|F$ è separabile, f è separabile, e di conseguenza g è separabile. Dunque $E|L$ è un'estensione separabile, e pertanto è un'estensione di Galois. ∎

Proposizione 0.9.3 *Sia $E|F$ un'estensione finita di campi, e sia $G = \mathrm{Gal}(E|F)$ un gruppo finito. Allora sono equivalenti*

(i) $E|F$ è un'estensione di Galois;

(ii) $F = \mathrm{Inv}_E(G)$.

Dimostrazione. (i) $\Rightarrow$ (ii). Sia $E|F$ estensione di Galois. Allora, per il Teorema 7.3, si ha $|G| = [E : F]$. D'altra parte, per definizione di F-isomorfismo, F è contenuto in $\mathrm{Inv}_E(G)$, e chiaramente $\mathrm{Gal}(E|\mathrm{Inv}_E(G)) = G$. Per il Lemma 9.2, anche $E|\mathrm{Inv}_E(G)$ è un'estensione di Galois, e quindi $[E : \mathrm{Inv}_E(G)] = |\mathrm{Gal}(E|\mathrm{Inv}_E(G))| = |G|$. Dunque $[E : F] = [E : \mathrm{Inv}_E(G)]$, e pertanto $\mathrm{Inv}_E(G) = F$.

(ii) $\Rightarrow$ (i). Sia $F = \mathrm{Inv}_E(G)$, e sia $G = \{\eta_1 = \iota_E, \eta_2, \ldots, \eta_n\}$. Sia $g \in F[x]$ un polinomio monico irriducibile su F che ha una radice $b \in E$. Consideriamo il polinomio

$$f = (x - \eta_1(b))(x - \eta_2(b)) \ldots (x - \eta_n(b)) \in E[x].$$

Per ogni $\eta \in G$, la moltiplicazione a sinistra per η è una permutazione di G, e quindi (considerando l'estensione canonica di η a $E[x]$,

$$\eta(f) = (x - \eta\eta_1(b))(x - \eta\eta_2(b)) \ldots (x - \eta\eta_n(b)) = f.$$

Dunque i coefficienti di f sono tutti elementi di E fissati da η; ciò vale per ogni $\eta \in G$, per cui i coefficienti di f appartengono a $\mathrm{Inv}_E(G) = F$, cioè $f \in F[x]$. Ma f ammette $b = \eta_1(b)$ come radice e dunque il polinomio minimo g di b divide f. Da ciò segue che g si fattorizza in $E[x]$ come prodotto di fattori lineari, e quindi che E contiene un campo di spezzamento per g. Pertanto $E|F$ è un'estensione normale.
Similmente procediamo per provare la separabilità. Sia $b \in E$, e sia $g \in F[x]$ il suo polinomio minimo. Per ogni $\eta \in G$, $g(\eta(b)) = \eta(g(b)) = 0$, cioè $\eta(b)$ è un radice di g. Sia $A = \{b = b_1, b_2, \ldots, b_k\}$ l'insieme di tutte le radici *distinte* di g che si ottengono come immagine di b tramite un elemento di G. Allora, per ogni $\eta \in G$, $\eta(A) \subseteq A$, e poiché η è iniettivo, $\eta(A) = A$. Poniamo $f = (x - b_1)(x - b_2) \ldots (x - b_k) \in E[x]$. Per il teorema di Ruffini $f|g$ in $E[x]$ e, per quanto osservato sopra, $\eta(f) = f$ per ogni $\eta \in G$. Dunque, come prima, i coefficienti di f sono invarianti per ogni $\eta \in G$, e quindi $f \in F[x]$. Siccome f ammette $b = b_1$ come radice si ha che $g|f$. Pertanto $g = f$, e dunque le radici di g sono semplici, provando così che $E|F$ è separabile. Poiché $E|F$ è finita per ipotesi, si conclude che $E|F$ è un'estensione di Galois. ∎

Teorema 0.9.4 (Fondamentale della Teoria di Galois) *Sia $E|F$ un'estensione di Galois, e sia $G = \mathrm{Gal}(E|F)$. Siano $\mathcal{S}$ l'insieme di tutti i sottogruppi di G, e $\mathcal{F}$ l'insieme di tutti i campi L con $F \leq L \leq E$. Allora le applicazioni:*

$$\begin{array}{rccc} \mathrm{Gal}(E, \cdot): & \mathcal{F} & \to & \mathcal{S} \\ & L & \mapsto & \mathrm{Gal}(E|L) \end{array} \qquad \begin{array}{rccc} \mathrm{Inv}_E: & \mathcal{S} & \to & \mathcal{F} \\ & H & \mapsto & \mathrm{Inv}_E(H) \end{array}$$

sono l'una l'inversa dell'altra. Inoltre, valgono le seguenti proprietà per ogni $H, K \in \mathcal{S}$,

(1) $H \leq K$ se e solo se $\mathrm{Inv}_E(H) \supseteq \mathrm{Inv}_E(K)$;

(2) $|H| = [E : \mathrm{Inv}_E(H)]$ e $[G : H] = [\mathrm{Inv}_E(H) : F]$;

(3) H è normale in G se e solo se $\mathrm{Inv}_E(H)|F$ è un'estensione normale. In tal caso, $\mathrm{Gal}(\mathrm{Inv}_E(H)|F) \simeq G/H$.

Dimostrazione. Sia H un sottogruppo di $G = \mathrm{Gal}(E|F)$, allora $\mathrm{Inv}_E(H) \in \mathcal{F}$. Poniamo $H' = \mathrm{Gal}(E|\mathrm{Inv}_E(H))$. Poiché, per definizione, ogni automorfismo in H fissa ogni elemento di $Inv_E(H)$, si ha $H \leq H'$. Ora, poiché per il Lemma 9.2, $E|\mathrm{Inv}_E(H)$ è un'estensione di Galois, dal Teorema 7.3 segue $|H'| = [E : \mathrm{Inv}_E(H)]$; d'altra parte, per il Lemma di Artin, $[E : \mathrm{Inv}_E(H)] \leq |H|$. Quindi $|H'| \leq |H|$, e siccome $H \leq H'$ si conclude che $H' = H$.

Sia ora L un campo intermedio di $E|F$, allora $\mathrm{Gal}(E|L) \leq G$. Sia $L' = \mathrm{Inv}_E(\mathrm{Gal}(E|L))$. Per definizione di $\mathrm{Gal}(E|L)$ si ha chiaramente $L \subseteq L'$. Ma, per il punto precedente,

$\mathrm{Gal}(E|L') = \mathrm{Gal}(E|L)$. Poiché $E|L$ ed $E|L'$ sono entrambe estensioni di Galois, per il Teorema 7.3 si ha $[E : L] = |\mathrm{Gal}(E|L)| = |\mathrm{Gal}(E|L')| = [E : L']$; dunque $[L' : L] = 1$, cioè $L' = L$.

Abbiamo così provato che le applicazioni $\mathrm{Gal}(E, \cdot\ )$ e Inv_E sono l'una l'inversa dell'altra, e quindi che esse stabiliscono una corrispondenza biunivoca tra gli insiemi $\mathcal{S}$ e $\mathcal{F}$. Proviamo ora gli altri punti dell'enunciato.

(1) Siano $H, K \leq G$. Se $H \leq K$ allora chiaramente $\mathrm{Inv}_E(H) \supseteq \mathrm{Inv}_E(K)$. Viceversa, sia $\mathrm{Inv}_E(H) \supseteq \mathrm{Inv}_E(K)$; allora $\mathrm{Gal}(E|\mathrm{Inv}_E(H)) \leq \mathrm{Gal}(E|\mathrm{Inv}_E(K))$, e per quanto provato sopra

$$H = \mathrm{Gal}(E|\mathrm{Inv}_E(H)) \leq \mathrm{Gal}(E|\mathrm{Inv}_E(K)) = K.$$

(2) Sia $H \leq G$. Per quanto già provato: $|G| = [E : F]$, $H = \mathrm{Gal}(E|\mathrm{Inv}_E(H))$ e quindi (poiché $E|\mathrm{Inv}_E(H)$ è di Galois) $|H| = [E : \mathrm{Inv}_E(H)]$. Applicando la formula dei gradi ed il Teorema di Lagrange per l'ordine dei sottogruppi di un gruppo finito si ha

$$[G : H] = \frac{|G|}{|H|} = \frac{[E : F]}{[E : \mathrm{Inv}_E(H)]} = [\mathrm{Inv}_E(H) : F].$$

(3) Sia N un sottogruppo normale di G, e poniamo $L = \mathrm{Inv}_E(N)$. Allora, per ogni $\eta \in N$ ed ogni $\sigma \in G$, si ha $\sigma^{-1}\eta\sigma \in N$. Quindi, se $b \in L$, $b = \sigma^{-1}\eta\sigma(b)$, da cui, applicando σ, si deduce che, per ogni $b \in L$ ed ogni $\eta \in N$, $\sigma(b) = \eta(\sigma(b))$, ovvero $\sigma(b) \in L$, e quindi $\sigma(L) \subseteq L$. Poiché, allo stesso modo, $\sigma^{-1}(L) \subseteq L$, si ha $\sigma(L) = L$. Dunque, la restrizione definisce un'applicazione

$$\begin{array}{rccc} \Phi: & G & \to & \mathrm{Gal}(L|F) \\ & \sigma & \mapsto & \sigma_{|L} \end{array}$$

che facilmente si verifica essere un omomorfismo di gruppi. Ora

$$\ker(\Phi) = \{\sigma \in G \mid \sigma_{|L} = \iota_L\} = \mathrm{Gal}(E|L) = \mathrm{Gal}(E|\mathrm{Inv}_E(N)) = N.$$

Per il teorema di omomorfismo per gruppi, si ha quindi $G/N \simeq Im(\Phi)$. Inoltre,

$$\mathrm{Inv}_L(\mathrm{Gal}(L|F)) \subseteq \mathrm{Inv}_L(\Phi(G)) = L \cap \mathrm{Inv}_E(G) = L \cap F = F,$$

quindi $\mathrm{Inv}_L(\mathrm{Gal}(L|F)) = F$, e per la Proposizione 9.3 si deduce che $L|F$ è un'estensione di Galois. In particolare è normale e

$$|\mathrm{Gal}(L|F)| = [L : F] = \frac{[E : F]}{[E : L]} = \frac{|\mathrm{Gal}(E|F)|}{|\mathrm{Gal}(E|L)|} = \frac{|G|}{|N|} = |G/Ker(\Phi))|$$

da cui segue che Φ è suriettiva, e $\mathrm{Gal}(L|F) \simeq G/N$.

Viceversa, sia $H \leq G$ tale che $L = \mathrm{Inv}_E(H)$ è estensione normale di F. Allora $L|F$ è di Galois dato che è sicuramente separabile, essendo L contenuto in E. Siano $\gamma \in G$ e $b \in L$. Sia $f \in F[x]$ il polinomio minimo di b su F. Poiché $L|F$ è normale L contiene un campo di spezzamento per f su F; in particolare contiene tutte le radici di f che appartengono ad E. Ora, essendo γ un F-isomorfismo, $f(\gamma(b)) = \gamma(f(b)) = 0$. Dunque, per quanto osservato sopra $\gamma(b) \in L$, e ciò vale per ogni $b \in L$. Pertanto, come prima, la restrizione $\gamma \mapsto \gamma_{|L}$ è un omomorfismo Φ del gruppo G nel gruppo $Gal(L|F)$, e chiaramente $H \leq Ker(\Phi)$; posto $K = Ker(\Phi)$, gli elementi di K sono gli automorfismi

di E che inducono l'identità su L, quindi per il punto (1), $L \subseteq \mathrm{Inv}_E(K) \subseteq \mathrm{Inv}_E(H) = L$. Dunque $L = \mathrm{Inv}_E(K)$ e, di conseguenza, $H = \mathrm{Gal}(E|L) = \mathrm{Gal}(E|\mathrm{Inv}_E(K)) = K$ che è un sottogruppo normale di G. ∎

Esempio 1. Sia $\omega \in \mathbb{C}$ una radice primitiva 11-esima dell'unità (e.g. $\omega = \cos\frac{2\pi}{11} + i\sin\frac{2\pi}{11}$), e sia $U = \{\omega^k \mid 0 \leq k \leq 10\}$ l'insieme di tutte le radici 11-esime dell'unità. U è un sottogruppo ciclico del gruppo moltiplicativo $\mathbb{C}^*$. Ora, il polinomio minimo di ω su $\mathbb{Q}$ è il polinomio *ciclotomico*

$$\Phi_{11}(x) = x^{10} + x^9 + \ldots + x^2 + x + 1.$$

Sia $E \leq \mathbb{C}$ il suo campo di spezzamento. Allora $E|\mathbb{Q}$ è un'estensione di Galois (detta estensione ciclotomica di grado 11); sia $G = \mathrm{Gal}(E|\mathbb{Q})$ il suo gruppo di Galois. Poiché l'insieme di tutte le radici complesse di $\Phi_{11}(x)$ è $U \setminus \{1\}$, si ha $E = \mathbb{Q}[\omega]$, e quindi

$$|G| = [E : \mathbb{Q}] = [\mathbb{Q}[\omega] : \mathbb{Q}] = \deg \Phi_{11}(x) = 10.$$

Se $\alpha \in G$, allora $\alpha(U) = U$, e quindi (essendo un automorfismo di campo), α induce un automorfismo $a_{|U}$ del gruppo ciclico U (che, come gruppo, è isomorfo a $\mathbb{Z}/11\mathbb{Z}$). Inoltre, è chiaro che α è univocamente individuato dall'immagine $\alpha(\omega) \in U \setminus \{1\}$. Siccome $|G| = 10 = |U \setminus \{1\}|$, concludiamo che per ogni $1 \leq k \leq 10$, esiste uno ed un solo $\eta_k \in G$ tale che $\eta_k(\omega) = \omega^k$ (cosa che si poteva anche direttamente dedurre dal Lemma 6.3).
Poniamo $\eta = \eta_2$ (ovvero l'automorfismo di E tale che $\omega \mapsto \omega^2$). Ora per $t \geq 1$,

$$\eta^t(\omega) = \omega^{2^t}.$$

Quindi, $\eta^n = \iota = 1_G$ se e solo se $\omega^{2^n} = 1$, ovvero se e solo se $2^n \equiv 1 \pmod{11}$. Poiché il minimo intero $n \geq 1$ per cui ciò si verifica è $n = 10$, concludiamo che l'ordine di η nel gruppo G è 10. Quindi $G = \langle\eta\rangle$, e G è un gruppo ciclico.
Per quanto conosciamo sui gruppi ciclici, per ogni divisore d di 10, G ammette uno ed un solo sottogruppo di ordine d. Precisamente, i sottogruppi di $G = \langle\eta\rangle$ sono

$$G_1 = G = \langle\eta\rangle \qquad G_2 = \langle\eta^2\rangle \qquad G_3 = \langle\eta^5\rangle \qquad G_4 = \{\iota\},$$

di ordine, rispettivamente, 10, 5, 2 e 1. Siano $F_i = \mathrm{Inv}_E(G_i)$ $(i = 1, 2, 3, 4)$ i corrispondenti campi degli invarianti. Per il Teorema 9.4, questi sono tutti e soli i campi intermedi dell'estensione $E|\mathbb{Q}$. Abbiamo poi, per ogni i,

$$[F_i : \mathbb{Q}] = [\mathrm{Inv}_E(G_i) : \mathbb{Q}] = [G : G_i] = 10/|G_i|.$$

In particolare $[F_2 : \mathbb{Q}] = 2$. In E sia

$$a = \omega + \omega^4 + \omega^5 + \omega^9 + \omega^3 = \omega + \eta^2(\omega) + \eta^4(\omega) + \eta^6(\omega) + \eta^8(\omega).$$

Per come è definito, $\eta^2(a) = a$, e quindi $a \in \mathrm{Inv}_E(\langle\eta^2\rangle) = F_2$. D'altra parte $a \notin \mathbb{Q}$ (altrimenti ω sarebbe radice del polinomio razionale $x^9 + x^5 + x^4 + x^3 + x - a$), e dunque (dato che $[F_2 : \mathbb{Q}]$ è un numero primo) $F_2 = \mathbb{Q}[a]$. Similmente, sia

$$b = \omega + \eta^5(\omega) = \omega + \omega^{10} = \omega + \omega^{-1} = \omega + \overline{\omega}.$$

Allora $b \in \mathrm{Inv}_E(\langle\eta^5\rangle) = F_3$, $b \notin \mathbb{Q}$ e, poiché $[F_3 : \mathbb{Q}] = 5$, $F_3 = \mathbb{Q}[b]$.
Concludendo, se ω è una radice primitiva 11-esima, i campi intermedi dell'estensione ciclotomica $\mathbb{Q}(\omega)|\mathbb{Q}$ di grado 11 sono

$$\mathbb{Q} \qquad \mathbb{Q}(\omega + \omega^3 + \omega^4 + \omega^5 + \omega^9) \qquad \mathbb{Q}(\omega + \omega^{-1}) \qquad \mathbb{Q}(\omega).$$

Osserviamo infine che, poiché in questo caso $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$ è un gruppo abeliano, e quindi tale che ogni suo sottogruppo è normale, per il punto (3) del Teorema 9.4 i campi che abbiamo elencato sopra sono estensioni normali di $\mathbb{Q}$.

Esempio 2. Determinaimo il gruppo di Galois G di $E|\mathbb{Q}$, dove $E \leq \mathbb{C}$ è il campo di spezzamento su $\mathbb{Q}$ del polinomio $f = x^5 - 2$. Innanzi tutto f è irriducibile per il criterio di Eisenstein; in particolare le sue radici in E sono tutte distinte. Inoltre, f ha una radice reale $a = \sqrt[5]{2}$, e

$$[\mathbb{Q}(a) : \mathbb{Q}] = 5.$$

In particolare 5 divide $[E : \mathbb{Q}] = |G|$. Sia $\omega = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ una radice primitiva quinta dell'unità. Allora le radici di f sono

$$a, \quad \omega a, \quad \omega^2 a, \quad \omega^3 a, \quad \omega^4 a \tag{7}$$

e quindi $E = \mathbb{Q}(a, \omega)$. Ora, il polinomio minimo di ω su $\mathbb{Q}$ è $g = x^4 + x^3 + x^2 + x + 1$. Poiché $\mathbb{Q}(\omega)$ è il campo di spezzamento di g su $\mathbb{Q}$, l'estensione $\mathbb{Q}(\omega)|\mathbb{Q}$ è normale, e quindi, per il punto (3) del Teorema 9.4, $N = \mathrm{Gal}(E|\mathbb{Q}(\omega))$ è un sottogruppo normale di G, e

$$G/N \simeq \mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$$

è un gruppo ciclico di ordine 4 (questo si vede anlalogamente a quanto fatto nell'esempio precedente con una radice 11-esima). In particolare 4 divide $|G|$, e quindi $5 \cdot 4 = 20$ divide $|G| = [E : \mathbb{Q}]$. Ora,

$$[E : \mathbb{Q}] = [\mathbb{Q}(\omega, a) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] \leq [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] \leq 5 \cdot 4 = 20.$$

Dunque, $|G| = [E : \mathbb{Q}] = 20$, e inoltre $[E : \mathbb{Q}(\omega)] = 5$. Pertanto $N = \mathrm{Gal}(E|\mathbb{Q}(\omega))$ ha ordine 5. Sia $H = \mathrm{Gal}(E|\mathbb{Q}(a))$; allora $|H| = [E : \mathbb{Q}(a)] = 4$. Quindi $N \cap H = \{1\}$, e $NH = G$. Per il secondo teorema di isomorfismo per gruppi,

$$\frac{G}{N} = \frac{NH}{N} = \frac{H}{N \cap H} = H,$$

e dunque H è un gruppo ciclico. Osserviamo che H non è normale in G; infatti, $\mathrm{Inv}_E(H) = \mathbb{Q}(a)$ che non è un'estensione normale di $\mathbb{Q}$ (dato che $\mathbb{Q}(a)$ contiene una sola radice del polinomio irriducibile f). Di fatto (lo si completi per esercizio) in G il sottogruppo H ha cinque coniugati distinti, che corrispondo ai campi intermedi $\mathbb{Q}(a)$, $\mathbb{Q}(\omega a)$, $\mathbb{Q}(\omega^2 a)$, $\mathbb{Q}(\omega^3 a)$, $\mathbb{Q}(\omega^4 a)$.
Possiamo ora descrivere piuttosto esplicitamente gli elementi di G. Innanazi tutto, osserviamo che un $\mathbb{Q}$-automorfismo di $E = \mathbb{Q}(a, \omega)$ è univocamente determinato dalle immagini di $a = \sqrt[5]{2}$ e di ω. Consideriamo per primo il sottogruppo $N = \mathrm{Gal}(E|\mathbb{Q}(\omega))$; esso è ciclico di ordine 5, sia σ un suo generatore; poiché $\mathrm{Inv}_E(N) = \mathbb{Q}(\omega)$, si ha $\sigma(\omega) = \omega$. Ora, ogni elemento di G manda radici di f in radici di f, ovvero induce una permutazione degli elementi in (7), e dunque $\sigma(a) = \omega^k a$ per qualche $1 \leq k \leq 4$; rimpiazzando eventualmente σ con una sua potenza, possiamo assumere $\sigma(a) = \omega a$. Prendiamo ora in esame $H = \mathrm{Gal}(E|\mathbb{Q}(a))$; anch'esso è ciclico, per cui sia η un suo generatore; allora η ha ordine 4, e poiché $\mathrm{Inv}_E(H) = \mathbb{Q}(a)$, $\eta(a) = a$. Ne segue che η "muove" ω, e siccome $\eta(\omega a) = \omega^t a$ per qualche $1 \leq t \leq 4$, si ha $\eta(\omega) = \omega^t$. Dal fatto che $|\eta| = 4$ segue $t = 2, 3$, e dunque, sostituendo eventualmente η con η^{-1}, possiamo porre $\eta(\omega) = \omega^2$. Poiché $G = NH$ concludiamo che gli elementi di G sono tutti del tipo $\sigma^u\eta^v$ con $0 \leq u \leq 4$ e $0 \leq v \leq 3$, dove

$$\sigma^u\eta^v(\sqrt[5]{2}) = \omega\sqrt[5]{2}$$
$$\sigma^u\eta^v(\omega) = \omega^{2^u}$$

Notiamo anche che $\sigma^\eta = \eta^{-1}\sigma\eta = \sigma^3$. Di passaggio, consideriamo a questo punto l'elemento $b = \sqrt[5]{2} + \omega \in E$, ed osserviamo che nessun $1 \neq \alpha \in G$ fissa b; da ciò segue che $E = \mathbb{Q}(b)$: infatti se fosse $\mathbb{Q}(b) < E$, allora $\mathbb{Q}(b)$ dovrebbe essere il campo degli invarianti di qualche sottogruppo non banale di G, il che non è.
Proviamo infine, a mo' di illustrazione della forza della connessione di Galois, come nell'estensione $E|\mathbb{Q}$ ci sia una sola estensione intermedia di grado 2 su $\mathbb{Q}$. Ciò corrisponde a provare che G ha un solo sottogruppo di indice 2. Sia T un tale sottogrupoo; allora T ha ordine 10 e dunque

contiene un sottogruppo di ordine 5; ma N è l'unico sottogruppo di ordine 5 di G (dato che N è un 5-sottogruppo di Sylow normale di G); dunque $N \leq T$; ma allora T/N è un sottogruppo di ordine 2 di G/N: poiché G/N è ciclico esiste un solo tale sottogruppo, e dunque T è unico (si provi che $T = N\langle\eta^2\rangle$). $L = \mathrm{Inv}_E(T)$ è quindi il solo campo intermedio in $E|\mathbb{Q}$ che ha grado 2 su $\mathbb{Q}$. Ancora $L \leq \mathbb{Q}(\omega)$, da cui segue facilmente che $L = \mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{5})$.

Gruppo di Galois di un polinomio.

Proposizione 0.9.5 *Sia F un campo, $f \in F[x]$, e E un campo di spezzamento per f su F. Se f è un polinomio separabile allora $E|F$ è un'estensione di Galois.*

Dimostrazione. Sia $f_1 \in F[x]$ il polinomio ottenuto moltiplicando i fattori irriducibili distinti di f in $F[x]$. Chiaramente, E è un campo di spezzamento per f_1 su F. Poiché f è separabile, e polinomi irriducibili distinti non possono avere radici comuni, le radici di f_1 sono tutte semplici e quindi, per il Teorema 7.2, $|\mathrm{Gal}(E|F)| = [E : F]$. Ma E è anche campo di spezzamento per f su $L = \mathrm{Inv}_E(G)$, e dunque $[E : L] = |\mathrm{Gal}(E|L)|$. Ma chiaramente $G = \mathrm{Gal}(E|L)$; dunque $[E : F] = [E : L]$, e quindi $F = L = \mathrm{Inv}_E(G)$. Poiché $E|F$ è finita, per la Proposizione 9.3 $E|F$ è un'estensione di Galois. ∎

Sia F un campo, $f \in F[x]$ un polinomio separabile ed E un suo campo di spezzamento su F. Allora $\mathrm{Gal}(E|F)$ si chiama **gruppo di Galois del polinomio** f. Ovviamente, esso non dipende dal particolare campo di spezzamento. Come abbiamo già più volte avuto modo di osservare, gli elementi di $G = \mathrm{Gal}(E|F)$ permutano le radici di f, e si verifica subito che ciò definisce un'azione di G sull'insieme Ω delle radici di f; ora, se $\sigma \in G$ fissa tutte le radici di f, siccome fissa anche tutti gli elementi di F, ed E è generato su F dall'aggiunzione delle radici di f, si conclude che σ è l'identità di E. Quindi l'azione di G sull'insieme Ω è un'azione fedele, e pertanto G è isomorfo ad un sottogruppo del gruppo simmetrico $\mathrm{Sym}(\Omega)$, Se $\deg f = n$, allora $|\Omega| \leq n$, e dunque G è isomorfo ad un sottogruppo di S_n.
Supponiamo a questo punto che il polinomio f sia irriducibile su F di grado n. Essendo separabile, le sue n radici nel cammpo di spezzamento E sono distinte. Siano a e b due di tali radici; allora, per il Lemma 6.3 esiste un F-isomorfismo $F[a] \to F[b]$ che manda a in b. Poiché E è campo di spezzamento per f sia su $F[a]$ che su $F[b]$, il Teorema 6.4 assicura che tale isomorfismo può essere esteso ad un F-isomorfismo η di E, cioè ad un elemento $\eta \in Gal(E|F)$. Dunque esiste η nel gruppo di Galois G di f su F tale che $\eta(a) = b$. Pertanto, come gruppo di permutazioni dell'insieme delle radici di f, G è transitivo. Dunque: *il gruppo di Galois di un polinomio irriducibile e separabile di grado n è isomofo ad un sottogruppo transitivo di S_n.*

Nel seguito di questa sezione, daremo un'idea di come trovare, fissato un primo p, polinomi a coefficienti razionali il cui gruppo di Galois (su $\mathbb{Q}$) sia isomorfo al gruppo simmetrico S_p. Iniziamo con un lemma sui gruppi di permutazioni.

Lemma 0.9.6 *Sia p un numero primo. Sia G un sottogruppo di S_p che contiene un ciclo di ordine p ed una trasposizione. Allora $G = S_p$.*

DIMOSTRAZIONE. Possiamo chiaramente supporre che G contenga la trasposizione $\tau = (1\,2)$. Sia σ un ciclo di ordine p contenuto in G; allora esiste una sua opprtuna potenza $\gamma = \sigma^k$ (con $1 \leq k \leq p-1$) tale che $\gamma(1) = 2$. Ora, poiché p è primo, γ è anch'essa un ciclo di ordine p, sia $\gamma = (1\,2\,i_3 \ldots\, i_p)$ (dove $\{i_3, i_4, \ldots\, i_p\} = \{3, 4, \ldots, p\}$). Quindi, eventualmente riordinando i punti $\{3, 4, \ldots, p\}$, possiamo supporre che $\gamma = (1\,2\,3\,\ldots\,p)$. Ora $\gamma^{-1}\tau\gamma = (2\,3)$, $\gamma^{-1}(2\,3)\gamma = (3\,4)$, e così via, portando a concludere che G contiene tutte le trasposizioni del tipo $(k\,k+1)$ (con $k = 1, \ldots, p-1$). Ma ancora, $(1\,2)(2\,3)(1\,2) = (1\,3)$, da cui iterando segue che G contiene tutte le trasposizioni del tipo $(1\,k)$. Ma allora, per ogni $1 \leq i, j \leq p$, $i \neq j$, si ha $(i\;j) = (1\,i)(1\,j)(1\,i) \in G$. Poiché le trasposizioni generano tutto S_p si conclude che $G = S_p$. ∎

Proposizione 0.9.7 *Sia p un primo, e f un polinomio irriducibile in $\mathbb{Q}[x]$ di gardo p. Supponiamo che f abbia esattamente due radici non reali nel campo $\mathbb{C}$. Allora il gruppo di Galois di f su $\mathbb{Q}$ è isomorfo a S_p.*

DIMOSTRAZIONE. Sia $E \leq \mathbb{C}$ il campo di spezzamento per f su $\mathbb{Q}$, e denotiamo con G il suo gruppo di Galois, che interpretiamo come un gruppo di permutazioni sull'insieme delle p radici (che sono tutte distinte) di f in E, dunque come sottogruppo del gruppo simmetrico S_p. Sia b una di tali radici; poiché f è irriducibile, $[\mathbb{Q}[b] : \mathbb{Q}] = \deg f = p$. Quindi

$$|G| = [E : \mathbb{Q}] = [E : \mathbb{Q}[b]][\mathbb{Q}[b] : \mathbb{Q}] = [E : \mathbb{Q}[b]] \cdot p.$$

Dunque p divide l'ordine di G, e pertanto (per il teorema di Sylow) G contiene un elemento γ di ordine p. Poiché l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti, si ha che γ (come permutazione delle radici di f) è un ciclo di ordine p. Siano ora u e v le sole due radici non reali di f. Allora $v = \bar{u}$ è il coniugato complesso di u (e $u = \bar{v}$). Dunque l'automorfismo di coniugio in $\mathbb{C}$ fissa tutte le radici reali di f e scambia tra di loro le due radici non reali. Poiché E è generato su $\mathbb{Q}$ dalle radici di f, ne segue che la restrizione τ ad E del coniugio complesso è un $\mathbb{Q}$-automorfismo di E, cioè un elemento di G. Come permutazione dell'insieme delle radici di f, τ fissa tutte le radici reali e scambia u e v, e dunque è una trasposizione in S_p. Quindi G è un sottogruppo di S_p che contiene una trasposizione ed un ciclo di ordine p e pertanto, per il Lemma precedente, $G = S_p$. ∎

Consideriamo ad esempio il polinomio razionale $f = x^5 - 10x + 2$ che, per il criterio di eisenstein, è irriducibile su $\mathbb{Q}$. Per verificare che f soddisfa le ipotesi della Proposizione 9.7 studiamo il garfico della funzione polinomiale reale $y = f(x)$. Siccome il termine di grado massimo nella x è di grado dispari si ha:

$$\lim_{x\to-\infty} f(x) = -\infty \qquad\qquad \lim_{x\to+\infty} f(x) = +\infty$$

Inoltre $y' = 5x^4 - 10 = 5(x^4 - 2)$, e si trova quindi che $y = f(x)$ ha un massimo relativo per $x = -\sqrt[4]{2}$, ed un minimo relativo per $x = \sqrt[4]{2}$. Ora $f(-\sqrt[4]{2}) = -2\sqrt[4]{2} + 10\sqrt[4]{2} + 2 > 0$, e $f(\sqrt[4]{2}) = 2\sqrt[4]{2} - 10\sqrt[4]{2} + 2 < 0$. Quindi il grafico di $y = f(x)$ attraversa una volta l'asse delle x nell'intervallo $(-\sqrt[4]{2},\ \sqrt[4]{2})$, e dunque, complessivamente, incontra esattamente in tre punti l'asse delle x. Pertanto il polinomio $f = x^5 - 10x + 2$ ha esattemente tre radici reali, e di conseguenza in $\mathbb{C}$ ha altre due radici complesse coniugate. Per la Proposizione precedente si ha che il gruppo di Galois di f su $\mathbb{Q}$ è isomnorfo a S_5.

Per ogni primo p è possibile trovare esplicitamente un polinomio irriducibile razionale di grado p che soddisfa alle ipotesi della Proposizione 9.7 (vedi Jacobson: Basica Algebra I, pag. 261)

ESERCIZI

1. Sia $E|F$ un estensione di campi finiti. Si provi che $E|F$ è un'estensione di Galois, e che il suo gruppo di Galois è ciclico.

2. Sia $\omega \in \mathbb{C}$ una radice primitiva 17-esima dell'unità, e sia $E = \mathbb{Q}[\omega]$. Si provi che $E|\mathbb{Q}$ è un'estensione di Galois e si dica qual è l'indice $[E : \mathbb{Q}]$. Si provi quindi che $E|\mathbb{Q}$ ha esattamente 5 campi intermedi (inclusi $\mathbb{Q}$ ed E), e si dimostri che (rispetto all'inclusione) essi formano una catena.

3. Sia $\omega \in \mathbb{C}$ una radice primitiva ottava dell'unità, e sia $E = \mathbb{Q}(\omega)$. Si determini il polinomio minimo di ω su $\mathbb{Q}$, si descriva il gruppo di Galois $\mathrm{Gal}(E|\mathbb{Q})$, e si determinino i campi intermedi dell'estensione $E|\mathbb{Q}$.

4. Si determinino i campi intermedi dell'estensione $E|\mathbb{Q}$, dove $E \leq \mathbb{C}$ è il campo di spezzamento del polinomio $x^7 - 1$ su $\mathbb{Q}$.

5. Sia $n \geq 1$, e siano $\zeta_1, \zeta_2, \ldots, \zeta_k$ tutte le radici *primitive* n-esime dell'unità in $\mathbb{C}$. Si provi che il polinomio

$$\Phi_n(x) = (x - \zeta_1)(x - \zeta_2) \ldots (x - \zeta_k)$$

è un polinomio a coefficienti razionali, è irriducibile su $\mathbb{Q}$, ed ha grado $\phi(n)$, dove ϕ è la funzione di Eulero ($\Phi_n(x)$ è detto polinomio ciclotomico n-esimo su $\mathbb{Q}$).

6. Sia $F = \mathbb{Z}_5$, sia ω una radice primitiva 13-esima dell'unità su F. Tenendo conto che $5^4 \equiv 1 \pmod{13}$, provare che $|F(\omega)| = 5^4$. Quindi descrivere il gruppo di Galois ed i campi intermedi dell'estensione $F(\omega)|F$.

7. Sia $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Si provi che $E|\mathbb{Q}$ è un'estensione di Galois, e si determinino i suoi sottocampi intermedi.

8. Trovare un polinomio in $\mathbb{Q}[x]$ tale che il suo gruppo di Galois su $\mathbb{Q}$ sia isomorfo al gruppo simmetrico S_7.

9. Sia $f \in \mathbb{Q}[x]$ un polinomio irriducibile di grado 3, e sia G il suo gruppo di Galois. Si provi che G è isomorfo a S_3 oppure ad A_3. Denotate con a, b, c le radici di f in un campo di spezzamento E per f, sia

$$d = (a - b)(b - c)(c - a).$$

Si provi che se $G \simeq S_3$ allora $d \in E \setminus \mathbb{Q}$, $\mathbb{Q}[d] = \mathrm{Inv}_E(A_3)$, e $[Q[d] : \mathbb{Q}] = 2$. Si provi che $G \simeq A_3$ se e solo se $d \in \mathbb{Q}$.

10. Si descriva il gruppo di Galois su $\mathbb{Q}$ del polinomio $f = x^4 - x^2 + 4$.

11. Si descriva il gruppo di Galois su $\mathbb{Q}$ del polinomio $f = x^4 - 2$. Si dica se, posto E il campo di spezzamento di f su $\mathbb{Q}$, l'estensione $E|\mathbb{Q}$ ammette campi intermedi che non sono estensioni normali di $\mathbb{Q}$.

12. Sia $E|F$ un'estensione di campi, con E campo di spezzamento di un polinomio irriducibile $f \in F[x]$. Siano $\alpha_1, \ldots, \alpha_n$ le radici di f in E, e si supponga che $\mathrm{Gal}(E|F)$ sia abeliano. Si provi che allora, per ogni $i = 1, \ldots, n$, $E = F[\alpha_i]$, e quindi che $[E : F] = \deg f$.

13. Sia F un campo di caratteristica 0, e sia $E|F$ un'estensione finita. Usando il Teorema di Steinitz (Teorema 1.8) si provi che $E|F$ è un'estensione semplice.

0.10 Epilogo

La vicenda delle idee di Galois (tra le più belle e feconde della storia della matematica) continua mostrando come le radici di un polinomio razionale f possano essere espresse, a partire dai coefficienti dello stesso, mediante radicali (ed ovviamente le usuali operazioni: si pensi alla formula risolutiva delle equazioni di secondo grado) se e soltanto se il gruppo di Galois di f su $\mathbb{Q}$ soddisfa una proprietà piuttosto restrittiva detta risolubilità. Questa è senz'altro soddisfatta se $\deg f \leq 4$ (ed infatti esistono "formule risolutive" per equazioni polinomiali di grado fino a 4), mentre per $n \geq 5$ si vede abbastanza facilmente che il gruppo simmetrico S_n non è risolubile. Poiché, come abbiamo visto, esistono polinomi razionali il cui gruppo di Galois è S_n, ne segue che le radici di un polinomio di grado 5, o maggiore, non sempre possono essere espresse mediante radicali a partire dai coefficienti del polinomio, ed in particolare che per $n \geq 5$ non esiste una "formula risolutiva" per le equazioni di grado n.
In tal modo, prima di morire all'età di ventuno anni, per un duello i cui pretesti rimangono misteriosi, Evariste Galois chiudeva un problema che per secoli aveva affascinato ed eluso molti tra i matematici migliori, e nel contempo apriva interi nuovi orizzonti alla matematica, dando vita, si può dire, a quella che sarebbe diventata l'algebra moderna.
Alla memoria di tal gigante, sopra le spalle del quale egli non solo è indegno ma anche incapace di salire, il sottoscritto dedica queste imperfette pagine.
Si capisce che ci vuole ben altro: siate felici.