LEZIONI DI ALGEBRA 2

Giuseppe Metere

(Bozza: ultima revisione del 2 ottobre 2023)

PREFAZIONE

Queste note si originano dalle lezioni di Algebra 2 che tengo dal 2013 per il Corso di Laurea in Matematica dell'Università degli Studi di Palermo. Esse non sono ancora nella loro forma definitiva (e forse mai lo saranno...) e non hanno alcuna pretesa di originalità. L'esposizione deve molto ai testi che ho adottato in questi anni, in particolare a due di essi: l'accurato manuale di Aluffi: *Algebra, chapter* 0, di impostazione contemporanea e piacevole lettura ([1]), e il più classico *Algebra* di Hungerford ([4]).

I prerequisiti sono quelli previsti dall'attuale ordinamento didattico del corso di laurea, cioè gli argomenti trattati nel corso di algebra del primo anno. Questi comprendono le basi della teoria de gruppi e degli anelli, inclusi i domini, gli anelli di polinomi e i campi. Tuttavia, qualche nozione di Algebra Lineare potrà essere utile per inquadrare più proficuamente le nozioni presentate.

Il corso, e di conseguenza questo testo, si compone di tre parti.

La prima parte è una introduzione al linguaggio della Teoria delle Categorie. Essa ha l'obiettivo di presentare la nozione di *universale*, e di dare un'idea di come tale nozione sia pervasiva in matematica. A questo scopo, si rivedranno alcune costruzioni e alcuni risultati elementari dal punto di vista categoriale, come i prodotti, i quozienti e le loro proprietà.

La seconda parte tratta argomenti di teoria dei gruppi. Si comincia con la nozione di gruppo libero, che viene introdotta principalmente per definire e giustificare le presentazioni di gruppi. Poi si studiano le azioni di gruppi su insiemi che vengono introdotte *geometricamente* come G-insiemi. Le proprietà dei G-insiemi vengono utilizzate per presentare e dimostrare i teoremi di Sylow. Conclude il capitolo la classificazione dei gruppi abeliani finiti e dei gruppi finiti con meno di 16 elementi.

Infine, nella terza parte vengono presentate le basi della teoria dei campi e delle estensioni di campi. La trattazione, in questo caso è quella classica, anche se spesso si fa uso delle proprietà universali, come ad esempio nel caso dell'omomorfismo caratteristico, del campo dei quozienti, degli anelli di polinomi. Un argomento centrale è lo studio delle radici di equazioni algebriche, e relativi campi di estensione. Il capitolo si conclude con la classificazione dei campi finiti e lo studio dei polinomi ciclotomici.

Questa pagina è lasciata volutamente vuota.
Anzi, non proprio, visto che contiene queste due righe.

INDICE

1

CATEGORIE E PROPRIETÀ UNIVERSALI

La teoria delle categorie nasce nel 1945 dal lavoro di Samuel Eilenberg e Saunders Mac Lane sul rapporto tra spazi topologici e loro invarianti algebrici [3]. Sebbene si sia originata in un ambito specifico, la teoria ha una vocazione universale, e ha fornito negli anni un punto di vista originale e fecondo. Il punto di vista categoriale, infatti, come una sorta di *lingua franca*, è uno strumento che permette di mettere in relazione le diverse discipline della matematica.

Se nel secolo scorso questo approccio è stato appannaggio soprattutto degli specialisti del settore, a nostro avviso, il tempo è oramai maturo per proporre fin dai primi anni di università i concetti e le tematiche più rilevanti della teoria. Cosa sono, dunque, le *categorie*? Vediamolo in qualche esempio concreto, prima di fornire una vera e propria definizione.

Come primo esempio, consideriamo qualcosa che conosciamo tutti molto bene: l'atto del contare. Cosa vuol dire contare? Sapere *contare* vuol dire essere in grado di mettere in relazione ogni insieme finito con un preciso numero naturale: il numero dei suoi elementi. Tale processo definisce la ben nota funzione *cardinalità*:

$$\{\text{insiemi finiti}\} \xrightarrow{\text{cardinaltà}} \{\text{numeri naturali}\}\,.$$

Da un certo punto di vista, il concetto di numero naturale nasce e trova giustificazione proprio in questa relazione. Osserviamo incidentalmente che il nostro approccio permette di rispondere senza indugio *affermativamente* alla domanda: *zero è un numero naturale?* In effetti, l'insieme vuoto è sicuramente un insieme finito, e conta esattamente *zero* elementi. Continuiamo con la nostra disamina del contare. Alla scuola primaria ci hanno insegnato che, dati due insiemi A e B, scriviamo $A \subseteq B$ se tutti gli elementi di A sono anche elementi di B. La relazione di *inclusione insiemistica* dà alla collezione degli insiemi finiti una struttura di preordine – una relazione si dice di preordine se soddisfa le proprietà *riflessiva* e *transitiva*.

Possiamo notare che la corrispondenza tra insiemi finiti e numeri naturali rispetta la struttura di preordine. Difatti, anche l'insieme dei numeri naturali è dotato della ben nota relazione "$\leqslant$" di *minore o uguale*. Ora, tutti sappiamo che se un insieme A è contenuto in un insieme finito B, la cardinalità di A è minore o uguale alla cardinalità di B. In simboli:

$$A \subseteq B \quad \Rightarrow \quad |A| \leqslant |B|\,.$$

La *cardinalità* stabilisce una corrispondenza tra gli insiemi finiti e i numeri naturali che rispetta la relazioni di preordine. Una corrispondenza siffatta è chiamata dagli algebristi *omomorfismo di preordini*.

Riflettiamoci un momento: la classe di tutti gli insiemi finiti è un ente matematico ricco e complesso, sicuramente più ricco e più complesso dell'insieme dei numeri naturali. Ebbene, la nozione di cardinalità è un collegamento fra questi due mondi, ed è in grado di far emergere molte proprietà rilevanti degli insiemi proprio per il fatto che rispetta la relazione di preordine data dall'inclusione insiemistica. Lo studio di tale connessione è proprio l'oggetto della *matematica combinatoria*.

Il secondo esempio riguarda l'algebra lineare, il cui studio viene di solito proposto al primo anno di università. Fissato un numero naturale n, ad ogni anello commutativo unitario R possiamo associare l'insieme $\mathrm{Mat}_n(R)$ delle matrici quadrate $n \times n$ a valori in R. Nei corsi di geometria del primo anno, in genere, si prende come R il campo dei reali, ma nulla vieta di considerare un generico anello commutativo unitario. $\mathrm{Mat}_n(R)$ è dotato della operazione di moltiplicazione righe per colonne che lo rende un monoide. L'identità è la matrice identica I_n (per i più distratti, ricordiamo che un monoide è un insieme dotato di una operazione binaria associativa e unitaria).

Abbiamo stabilito una corrispondenza tra anelli commutativi e monoidi:

$$\{\text{anelli commutativi unitari}\} \xrightarrow{\mathrm{Mat}_n} \{\text{monoidi}\}\ .$$

che associa a ogni anello commutativo unitario R, il monoide moltiplicativo $\mathrm{Mat}_n(R)$. È naturale chiedersi se questa corrispondenza si possa estendere agli omomorfismi. Supponiamo allora che

$$f\colon R \to S$$

sia un omomorfismo di anelli. Immediatamente osserviamo che f induce un omomorfismo di monoidi

$$\mathrm{Mat}_n(f)\colon \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(S)\,,$$

definito nel modo più naturale possibile: se A è la matrice

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots \\ \vdots & \ddots & \\ a_{n1} & & a_{nn} \end{bmatrix}$$

allora $\mathrm{Mat}_n(f)(A)$ è la matrice che si ottiene applicando f a ogni componente di A:

$$\mathrm{Mat}_n(f)(A) = \begin{bmatrix} f(a_{11}) & f(a_{12}) & \dots \\ \vdots & \ddots & \\ f(a_{n1}) & & f(a_{nn}) \end{bmatrix}$$

Inoltre, se

$$g\colon S \to T\,.$$

è un altro omomorfismo di anelli commutativi unitari, si ha che

$$\mathrm{Mat}_n(g \circ f) = \mathrm{Mat}_n(g) \circ \mathrm{Mat}_n(f)\,.$$

Riassumendo, la relazione tra gli anelli commutativi unitari e i monoidi si estende agli omomorfismi ed è compatibile con la composizione di omomorfismi.

Le situazioni che abbiamo descritto nei due esempi esemplificano in modo elementare, ma non banale, la nozione di *categoria* e quella di *funtore* fra due categorie. Nel primo caso, il funtore *cardinalità* mette in relazione gli insiemi finiti con i numeri naturali, mentre nel secondo caso, il funtore Mat_n mette in relazione la categoria degli anelli commutativi unitari con quella dei monoidi.

Per chiarire meglio il nesso fra i due esempi, è arrivato il momento di introdurre e formalizzare la nozione di categoria.

1.1 CATEGORIE

Una categoria, è costituita da due entità distinte: gli oggetti e i morfismi.

Di solito, gli oggetti di una categoria sono *oggetti matematici*, come ad esempio gli insiemi, gli anelli o gli spazi topologici. Essi possono essere rappresentati da punti disegnati sul foglio:

Tra oggetti di una categoria possono essere definiti dei *morfismi*. Questi sono rappresentati come frecce che collegano gli oggetti:

L'idea da cui si parte è quella secondo cui due oggetti collegati da una freccia debbano avere dei caratteri astratti comuni, una stessa μορφή, o forma. Ad esempio, in algebra, i morfismi tra insiemi dotati di una struttura algebrica sono le funzioni che rispettano tale struttura – di solito vengono chiamati *omo*morfismi. Analogamente, in geometria, i morfismi tra entità geometriche sono quelle mappe che ne preservano la *forma*, in un qualche senso precisato, come ad esempio le applicazioni lineari tra spazi vettoriali.

Un'idea chiave dell'approccio categoriale è che sia possibile studiare certe proprietà importanti di un oggetto matematico osservando le relazioni che possono essere stabilite tra esso e gli oggetti che lo circondano. Proprio per questa ragione abbiamo rappresentato un oggetto di una categoria con un punto •, perché è nostra intenzione studiarne le proprietà senza *guardare dentro di esso.*

La prima categoria che si incontra è di solito la categoria degli insiemi. In essa, gli oggetti sono gli insiemi stessi, i morfismi sono le funzioni tra insiemi. Prendiamo un insieme A, e rappresentiamolo così

$$\bullet^{A}$$

Se l'insieme A è diverso dal vuoto, allora A contiene degli elementi. Ci chiediamo se sia possibile studiare A, con i suoi elementi, senza guardarci dentro. La risposta è affermativa, e per questo possiamo utilizzare i morfismi della categoria: in questo caso le funzioni, che *partono da* o *arrivano in* A. Ad esempio, se $\{*\}$ è l'insieme singoletto, una funzione $a\colon \{*\} \to A$ consiste precisamente nella *scelta* di un elemento di A. Se possiamo identificare gli elementi di A con le funzioni che hanno come dominio il singoletto, allora possiamo identificare lo stesso A con l'insieme delle funzioni

$$\{\, f\colon \{*\} \to A \,\}$$

cioè possiamo studiare gli *elementi* di A senza guardare dentro A, utilizzando delle funzioni opportune.

Per quanto riguarda i sottoinsiemi, o parti, di A, anche in questo caso possiamo studiarli mediante delle funzioni, le cosiddette *funzioni caratteristiche*, attraverso le quali identifichiamo ciascun sottoinsieme $U \subseteq A$ con la funzione

$$\chi_U\colon A \to \{0,1\}$$

definita, per $x \in A$, dai casi $\chi_U(x) = 1$ se $x \in U$, e $\chi_U(x) = 0$ se $x \notin U$.

1.1.1 *La definizione di categoria*

È data la seguente definizione.

Definizione 1.1.1. *Una categoria* C *è data da*

- *una collezione* C_0 *di* ***oggetti****:* $A, B, C, \ldots$
- *una collezione* C_1 *di* ***morfismi****, o* ***frecce****:* $f, g, h, \ldots$

Inoltre,

- *a ogni morfismo sono assegnati due oggetti, chiamati* ***dominio*** *e* ***codominio*** *del morfismo. Con la notazione* $f\colon A \to B$ *intendiamo che il morfismo* f *ha per dominio l'oggetto* A*, e per codominio l'oggetto* B*;*
- *a ogni oggetto* A *è associato un morfismo* $\mathrm{id}_A\colon A \to A$*, chiamato* ***identità*** *di* A*;*
- *a ogni coppia di morfismi* f *e* g*, per i quali il codominio di* f *coincida con il dominio di* g*, è associato il* ***morfismo composto*** $g \circ f$*, o più semplicemente* gf*, avente lo stesso dominio di* f *e lo stesso codomino di* g*; ad esempio, per* $f\colon A \to B$ *e* $g\colon B \to C$*, si ha* $g \circ f\colon A \to C$*.*

Oggetti e morfismi di una categoria devono verificare i seguenti assiomi:

- *(**identità**) per ogni morfismo* $f\colon A \to B$*, valgono le uguaglianze*

$$f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f\,;$$

- *(**associatività**) per ogni tripla di morfismi* $f\colon A \to B$*,* $g\colon B \to C$ *e* $h\colon C \to D$*, vale l'uguaglianza*

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

Notazione 1.1.2. *Fissati due oggetti di una categoria* C*, indichiamo con*

$$\mathrm{Hom}_{\mathsf{C}}(A, B)$$

la classe di tutti i morfismi $A \to B$*; fissato un oggetto* A*, indichiamo con*

$$\mathrm{End}_{\mathsf{C}}(A)$$

la classe di tutti gli endomorfismi *di* A*, ossia dei morfismi* $A \to A$*. Si usano anche le notazioni* $\mathrm{Hom}(A, B)$*,* $\mathsf{C}(A, B)$ *e* $\mathrm{End}(A)$ *rispettivamente, quando ciò non generi ambiguità.*

Esercizio 1.1.3. Verificare che, data una categoria C, $\mathrm{End}_{\mathsf{C}}(A)$ ammette una struttura di monoide[1], con moltiplicazione data dalla composizione dimorfismi e elemento neutro id_A.

1.1.2 *Esempi di categorie*

Il primo esempio di categoria che presentiamo è fondamentale in tutti i rami della matematica: la *categoria degli insiemi*.

Esempio 1.1.4. **La categoria degli insiemi** è denotata Set. Essa ha per oggetti gli insiemi, e per morfismi le funzioni, o applicazioni, tra insiemi. Le identità sono le funzioni identiche, la composizione è l'usuale composizione di funzioni. La verifica della validità degli assiomi di identità e associatività è un facile esercizio.

Seguono alcuni esempi di categorie di *insiemi strutturati*, e morfismi che preservano la loro struttura. La verifica degli assiomi di categoria è lasciata al lettore.

Esempio 1.1.5. **La categoria dei gruppi** Gp ha per oggetti i gruppi, e per morfismi gli omomorfismi di gruppo.

Prima del prossimo esempio, forniamo la definizione di *sottocategoria*.

1 In realtà, come vedremo più avanti, $\mathrm{End}(A)$ potrebbe non essere un *insieme*, ma una *classe propria*. L'esercizio è da intendersi estendendo alle classi proprie la definizione di monoide, nozione che normalmente viene data in un contesto insiemistico (vedi Nota 1.1.3).

Definizione 1.1.6. *Data una categoria* C*, una sua sottocategoria* D *è costituita da una sottoclasse di oggetti di* C *e da una sottoclasse di morfismi di* C *tali che:*

i. *se* $f\colon A \to B$ *sta in* D*, allora anche* A *e* B *sono in* D*;*

ii. *se* $f\colon A \to B$ *e* $g\colon B \to C$ *stanno in* D*, allora anche* $g \circ f\colon A \to C$ *sta in* D*;*

iii. *se* A *sta in* D*, allora anche il morfismo identità* $\mathrm{id}_A\colon A \to A$ *sta in* D*.*

Notiamo come le tre condizioni *i.-iii.* garantiscano il fatto che D soddisfi a sua volta gli assiomi di categoria.

Esempio 1.1.7. **La categoria degli insiemi finiti** FinSet, che ha per oggetti gli insiemi finiti e per frecce le funzioni tra insiemi finiti è una sottocategoria della categoria degli insiemi Set.

Esempio 1.1.8. **La categoria dei gruppi abeliani** Ab ha per oggetti i gruppi abeliani, e per morfismi gli omomorfismi di gruppo. Si verifica facilmente che Ab è una sottocategoria di Gp.

Esempio 1.1.9. **La categoria dei monoidi** Mon ha per oggetti i monoidi, e per morfismi gli omomorfismi di monoide. Si verifica facilmente che Gp e Ab sono sottocategorie di Mon.

Esempio 1.1.10. **Le categorie degli anelli.** La categoria Rng ha per oggetti gli anelli, e per morfismi gli omomorfismi di anelli. La categoria Ring ha per oggetti gli anelli unitari, e per morfismi gli omomorfismi di anelli che preservano le unità. Si verifica facilmente che Ring è una sottocategoria di Rng.

Esercizio 1.1.11. Sia I un ideale proprio di un anello commutativo unitario A. Allora I è un sottoanello di A in Rng, mentre non è un sottoanello di A in Ring.

Esempio 1.1.12. **La categoria dei campi** Fld verrà studiata nel dettaglio nel seguito.

Esempio 1.1.13. Fissato un campo K, **la categoria dei** K**-spazi vettoriali** $K\text{-}\mathsf{Vect}$ ha per oggetti gli spazi vettoriali, e per morfismi le applicazioni lineari.

Esercizio 1.1.14. Dati due gruppi abeliani G e H, verificare che vale

$$\mathrm{Hom}_{\mathsf{Ab}}(G,H) = \mathrm{Hom}_{\mathsf{Gp}}(G,H) = \mathrm{Hom}_{\mathsf{Mon}}(G,H)\,,$$

mentre, per A e B anelli unitari, vale solamente

$$\mathrm{Hom}_{\mathsf{Ring}}(A,B) \subseteq \mathrm{Hom}_{\mathsf{Rng}}(A,B)\,.$$

Mostrare con un esempio che l'ultima inclusione può non essere stretta.

1.1.3 *Insiemi e classi*

A questo punto, è opportuno spiegare brevemente il perché si è utilizzato il termine *classe*, e non il termine *insieme*, per descrivere le collezioni degli oggetti e dei morfismi di una categoria.

In effetti, anche i pochi esempi visti fin qui mostrano come gli oggetti di una categoria possano non costituire un insieme. Nel caso di Set, infatti, ben sappiamo che l'*insieme di tutti gli insiemi* non può essere considerato, o per lo meno non può essere considerato all'interno della teoria degli insiemi *classsica*, detta ZFC, dai nomi dei matematici Zermelo e Fraenkel, e dall'assioma della scelta, *choice* in inglese. Di conseguenza, per la teoria delle categorie, dobbiamo basarci su quella che i logici chiamano una *estensione conservativa* di ZFC, ossia di una teoria che contenga ZFC, e all'interno della quale, tutte le proposizioni dimostrabili in ZFC, lo siano ancora, e tale che ogni proposizione di ZFC dimostrabile nell'estensione, sia già dimostrabile in ZFC. Un estensione conservativa di ZFC è ad esempio la teoria degli insiemi di NBG, dai nomi dei matematici von Neumann, Bernays, Gödel, dove oltre agli insiemi vengono introdotte le cosiddette *classi*. Una intuizione su cosa siano le classi si può avere pensando a una classe come a un insieme *molto grande*, più grande di qualunque altro insieme. Più precisamente, vale il fatto che tutti gli insiemi sono delle classi, mentre una classe in generale non è un insieme. Chiamiamo *classi proprie* precisamente le classi che non siano insiemi, cioè che non siano elementi di altre classi. Ad esempio, la classe di tutti gli insiemi è una classe propria.

La teoria delle classi non è l'unico modo di risolvere i paradossi come quello dell'insieme di tutti gli insiemi. Un approccio diverso è costituito, ad esempio, dalla teoria degli *universi di Grothendieck*. Di questa, però, non ci occuperemo. Attenzione! Il termine classe è spesso usato in matematica anche con altri significati; addirittura, talvolta, come sinonimo di insieme. Nel caso di una relazione di equivalenza, per esempio, parleremo di *classi di equivalenza*. Per non confondersi è necessario considerare attentamente il contesto del discorso.

Definizione 1.1.15. *Una categoria* C *è detta* ***localmente piccola*** *se, per ogni coppia di suoi oggetti* A, B*, la classe* $\mathrm{Hom}_{\mathsf{C}}(A, B)$ *è un insieme.*

Una categoria C *è detta* ***piccola*** *se la classe* C_0 *dei suoi oggetti è un insieme. Ogni categoria piccola è ovviamente anche localmente piccola.*

Esercizio 1.1.16. Le categorie riportate negli esempi sopra sono tutte localmente piccole, ma nessuna di esse è piccola.

1.1.4 *Diagrammi commutativi*

Uno strumento molto efficace fornito dal linguaggio delle categorie è l'uso di diagrammi per rappresentare, ed eventualmente svolgere, calcoli e dimostrazioni.

Consideriamo il seguente diagramma

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[k]{} & D \end{array} \tag{1}$$

dove cioè A, B, C e D sono insiemi, f, g, h e k sono funzioni, con i domini e i codomini indicati secondo la convenzione adottata. Le seguenti affermazioni sono equivalenti:

i. per ogni elemento $x \in A$, si ha $g(f(x)) = k(h(x))$;

ii. La funzione composta $g \circ f$ è uguale alla funzione composta $k \circ h$.

Se immaginiamo ora di considerare lo stesso diagramma, riferito però ad una categoria nella quale A, B, C e D potrebbero non essere insiemi, e f, g, h e k potrebbero non essere funzioni, l'affermazione (i.) potrebbe non avere significato, mentre la (ii.), poiché è stata formulata senza adoperare gli elementi, può essere ancora presa in considerazione: diremo che il diagramma (1) nella categoria C è un *diagramma commutativo* se vale l'uguaglianza

$$g \circ f = k \circ h\,.$$

Si noti come il termine *commutativo* in questo contesto assuma un significato diverso da quello che già conosciamo riferito alle operazioni.

Più in generale, un diagramma in una categoria C è detto commutativo se, comunque presi due suoi oggetti X e Y, tutte le coppie di frecce da X a Y, che si ottengono per composizione di frecce del diagramma, sono uguali.

Esempio 1.1.17 (Operazioni associative). Prima di presentare l'esempio, ricordiamo che, date due funzioni $f\colon X \to Y$ e $g\colon Z \to W$, il loro prodotto[2] $f \times g\colon X \times Z \to Y \times W$ si ottiene ponendo $(f \times g)(x, z) = (f(x), g(z))$, dove $x \in X$ e $z \in Z$. Ciò premesso, consideriamo un insieme M su cui sia definita una operazione binaria

$$*\colon M \times M \to M$$

dove, come è consuetudine, indichiamo l'applicazione di $*$ alla coppia (x, y) scrivendo $x * y$. Ora prendiamoci qualche minuto per contemplare il diagramma seguente

$$\begin{array}{ccc} M \times M \times M & \xrightarrow{*\times \mathrm{id}_M} & M \times M \\ {\scriptstyle \mathrm{id}_M \times *}\downarrow & & \downarrow{\scriptstyle *} \\ M \times M & \xrightarrow[*]{} & M \end{array} \tag{2}$$

2 Nel seguito, analizzeremo più nel dettaglio la nozione di prodotto in una categoria. Per il momento assumiamo la nozione insiemistica.

e chiediamoci che significato abbia la sua commutatività.

Formalmente, essa consiste nell'uguaglianza delle due composizioni:

$$*(* \times \mathrm{id}_M) = *(\mathrm{id}_M \times *)\,,$$

ma probabilmente questo punto di vista non è molto illuminante. Proviamo allora a esplicitare l'uguaglianza sugli elementi. Consideriamo un elemento $(x, y, z) \in M \times M \times M$, e valutiamo la composizione di sinistra su tale elemento:

$$*(\mathrm{id}_M \times *)(x, y, z) = *(x, *(y, z)) = *(x, y * z) = x * (y * z)\,,$$

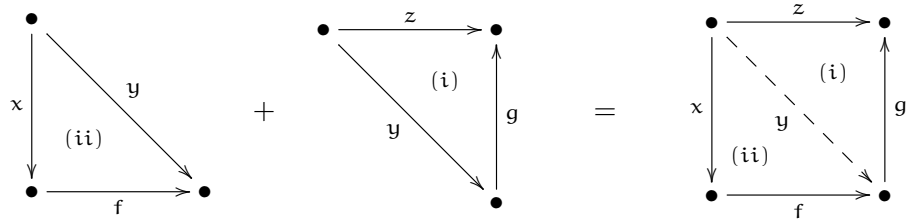
poi passiamo alla composizione a destra:

$$*(* \times \mathrm{id}_M)(x, y, z) = *(*(x, y), z) = *(x * y, z) = (x * y) * z\,.$$

Dire che il diagramma (2) commuta, vuol dire che, per ogni scelta di x, y e z in M, le due espressioni scritte sopra danno lo stesso risultato. In altre parole, la commutatività del diagramma esprime il fatto che l'operazione $*$ è associativa.

I diagrammi commutativi possono essere anche un modo conveniente per svolgere calcoli e operazioni. Infatti, *incollando* due diagrammi commutativi si ottiene ancora un diagramma commutativo. Questo ci permette di rappresentare graficamente l'operazione algebrica di *sostituzione* di una variabile, come mostrato nell'esempio che segue.

Esempio 1.1.18 (Composizione di diagrammi). In una categoria C, consideriamo il diagramma seguente:



Gli oggetti sono rappresentati con lo stesso simbolo $\bullet$, tuttavia non necessariamente essi sono uguali fra loro. In questo modo, vogliamo soltanto evidenziare come essi non siano poi così importanti nell'esempio che stiamo presentando. Il diagramma sulla destra può essere ottenuto incollando in due diagrammi sulla sinistra. Il primo, indicato con (i), ci dice che la freccia z è uguale alla composizione gy; il secondo, indicato con (ii), che y è uguale a alla composizione fx. Accostando questi due diagrammi, e identificando la freccia y, si ottiene un unico diagramma commutativo $(i) + (ii)$. In particolare, la commutatività del suo contorno, equivale all'uguaglianza delle frecce z e gfx (omettiamo volutamente il simbolo $\circ$ della composizione). Il calcolo che abbiamo fatto può essere rappresentato dalla catena di uguaglianze:

$$z = gy = g(fx)) = (gf)x\,.$$

Utilizzando la classica notazione funzionale, invece, avremmo dovuto scrivere:

$$z = g(y) = g(f(x)) = (g \circ f)(x)\,.$$

Questo esempio ci suggerisce come il *linguaggio dei diagrammi commutativi* possa aggiungere una dimensione alle nostre capacità di calcolo.

Esercizio 1.1.19. Esprimere gli assiomi di identità e associatività della definizione di categoria mediante dei diagrammi commutativi.

1.1.5 *Categorie preordine*

In algebra, un **preordine** (S, ρ) è un insieme S dotato di una relazione $\rho \subseteq S \times S$ che soddisfa le proprietà *riflessiva* e *transitiva*.

Sono esempi di preordine tutte le relazioni di equivalenza; esse, oltre alle proprietà summenzionate, soddisfano anche la proprietà *simmetrica*. Analogamente, sono esempi di preordine tutti gli ordini parziali (**poset**); essi oltre alle proprietà summenzionate, soddisfano anche la proprietà *antisimmetrica*.

Come ci accingiamo a mostrare, il preordine (S, ρ) può essere visto come una categoria, che denotiamo S. La categoria S ha per oggetti tutti gli elementi di S; inoltre, dati due oggetti $x, y \in S$, si ha esattamente una freccia $x \to y$ se e solo se x è in relazione ρ con y. Formalmente, quindi, poniamo $S_0 = S$ e $S_1 = \rho$.

La struttura di categoria si ottiene facilmente dalle considerazioni seguenti.

- Poiché la relazione ρ è riflessiva, ogni oggetto x è in relazione con sé stesso; questo ci permette di definire le frecce identità $x \to x$, per ogni $x \in S$.
- Poiché la relazione ρ è transitiva, possiamo definire la composizione. Infatti, se abbiamo due frecce $x \to y$ e $y \to z$, questo vuol dire precisamente che $x \rho y$ e $y \rho z$; per la proprietà transitiva, allora $x \rho z$, cioè esiste un'unica freccia $x \to z$ che definiamo essere la composizione delle due frecce da cui siamo partiti.

La verifica degli assiomi di categoria è lasciata al lettore.

Attenzione: la categoria di questo esempio è una entità astratta: ci serve a capire che gli oggetti di una categoria non sono necessariamente insiemi, e che i morfismi non sono necessariamente funzioni.

Osservazione 1.1.20. In una categoria preordine, ogni diagramma è commutativo.

Di seguito alcuni esempi di categorie preordine. Si noti che si tratta di categorie piccole.

Esempio 1.1.21. La categoria $(\mathbb{Z}, \leqslant)$. L'insieme degli interi $\mathbb{Z}$ è un insieme totalmente ordinato per la relazione d'ordine naturale $\leqslant$ definita da

$$n \leqslant m \text{ se e solo se esiste } k \in \mathbb{N} \text{ tale che } m = n + k\,.$$

Possiamo interpretare $(\mathbb{Z}, \leqslant)$ come una categoria: gli oggetti sono i numeri interi, e un si ha un morfismo $n \to m$ precisamente quando $n \leqslant m$.

Esempio 1.1.22. La categoria $(\mathbb{Z}, |\,)$. L'insieme degli interi $\mathbb{Z}$ è un insieme preordinato per la relazione di *divisibilità* $|$ definita da

$$n|m \text{ se e solo se esiste } k \in \mathbb{Z} \text{ tale che } m = nk\,.$$

Possiamo interpretare $(\mathbb{Z}, |\,)$ come una categoria: gli oggetti sono i numeri interi, e un si ha un morfismo $n \to m$ precisamente quando $n|m$.

Esempio 1.1.23. La categoria $(\mathcal{P}(X), \subseteq)$. Dato un insieme X, le sue parti formano un ordine parziale rispetto alla relazione $\subseteq$ di inclusione insiemistica. Gli oggetti della categoria $(\mathcal{P}(X), \subseteq)$ sono i sottoinsiemi di X; dati due sottoinsiemi U e V di X, si ha una freccia $U \to V$ precisamente quando $U \subseteq V$.

Esempio 1.1.24. Ogni insieme S può essere visto come categoria preordine $(S, =)$, dove la relazione di preordine è l'uguaglianza.

1.1.6 *La categoria lineare* Lin

Come abbiamo visto, dato un campo K, è possibile definire la categoria K-Vect degli spazi vettoriali su K, con morfismi le mappe lineari. L'esempio che segue riguarda gli spazi vettoriali di dimensione finita.

Introduciamo la categoria Lin_K, o più semplicemente Lin, quando il campo K è sottointeso.

- Oggetti di Lin sono i numeri naturali $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- Dati $m, n \in \mathbb{N}$, una freccia $A\colon m \to n$ è una matrice $n \times m$. In altre parole poniamo:

$$\mathrm{Hom}_{\mathsf{Lin}}(m, n) := \mathrm{Mat}_K(n, m)$$

- La composizione è l'usuale prodotto di matrici. Esplicitamente, data $A\colon m \to n$ e $B\colon n \to k$, la composizione $B \circ A\colon m \to k$ è l'usuale prodotto righe per colonne BA.
- Le identità sono le matrici identiche.

Si noti come la il fatto che due frecce siano componibili si traduce con la condizione di compatibilità richiesta dal prodotto di matrici,

ossia che il numero di colonne di B sia uguale al numero di righe di A. Gli assiomi di categoria sono facilmente verificati, poiché il prodotto di matrici è associativo, e le matrici identiche sono neutre rispetto al prodotto di matrici.

Osservazione 1.1.25. Le matrici si introducono nei corsi di Algebra Lineare per rappresentare le mappe lineari tra spazi vettoriali. È allora naturale chiedersi quale sia la relazione tra la categoria Lin e la categoria K-Vect vista in precedenza. Possiamo pensare a Lin come a una una sottocategoria di K-Vect che descrive in modo accurato e sintetico gli spazi vettoriali di dimensione finita su K. In effetti, ricordiamo dell'algebra lineare, un'applicazione lineare $f\colon V \to W$ tra due spazi vettoriali di dimensione finita m e n rispettivamente, si può rappresentare con una matrice $n \times m$ a patto di scegliere una base di V una base di W. Questo equivale a dire che stiamo fissando due isomorfismi $V \cong K^m$ e $W \cong K^n$, in modo tale che f possa essere ricondotta a una applicazione lineare $K^m \to K^n$. Quest'ultima può essere a sua volta descritta dalla moltiplicazione di una opportuna matrice A per un vettore colonna:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \cong\downarrow & & \downarrow\cong \\ K^m & \xrightarrow[\mathbf{v}\mapsto A\cdot\mathbf{v}]{} & K^n \end{array}$$

In conclusione, la categoria Lin è una versione più *magra* della categoria degli spazi vettoriali su K di dimensione finita, dove per ogni spazio W consideriamo solo il prototipo K^n, e poiché il campo K è chiaro dal contesto, ci limitiamo a rappresentare tale spazio con il numero naturale n, la sua dimensione.

1.1.7 *Categorie* (co)slice

Nello studio dell'algebra e di altre discipline matematiche, non è raro imbattersi in costruzioni *standard* che, data una certa struttura, permettono di costruirne delle nuove. È questo il caso delle *categorie slice* (dall'inglese *slice category*[3]) che sono l'oggetto di questa sezione.

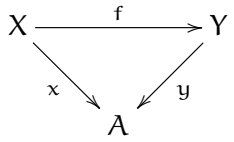
Abbiamo già insistito sul fatto che gli oggetti di una categoria non sono necessariamente degli insiemi. Nella costruzione che riportiamo qui, vedremo come gli oggetti di una categoria possano servire da frecce di un altra categoria.

Sia allora C una categoria data, e sia A un suo oggetto fissato. Definiamo una nuova categoria: la categoria slice di C su A, in simboli C/A.

- Gli oggetti di C/A sono le frecce di C di codominio A.

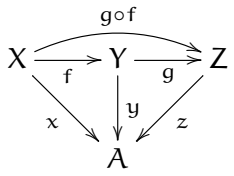
3 Al meglio della mia conoscenza, non esiste in italiano una terminologia consolidata per l'inglese *slice category*.

- Un morfismo dall'*oggetto* $\begin{smallmatrix} X \\ \downarrow x \\ A \end{smallmatrix}$ all'*oggetto* $\begin{smallmatrix} Y \\ \downarrow y \\ A \end{smallmatrix}$ è una freccia $f\colon X \to Y$ in C tale che $y \circ f = x$, ovvero tale che il seguente diagramma commuti in C:



  Scriveremo $f\colon (X,x) \to (Y,y)$ per rimarcare che la freccia f della categoria C è da intendersi come morfismo della categoria slice.

- Composizione. Dati due morfismi $f\colon (X,x) \to (Y,y)$ e $g\colon (Y,y) \to (Z,y)$, la loro composizione in C/A si fa esattamente come nella categoria ambiente C. Infatti, con riferimento al diagramma



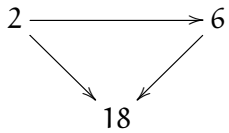
  poiché f è tale che $y \circ f = x$, e g è tale che $z \circ g = y$, si vede subito che la composta gf è tale che $z \circ g \circ f = x$, e quindi rappresenta un morfismo $(X,x) \to (Z,z)$ in C/A.

- Identità. Per un oggetto (X,x) di C/A, il morfismo identico $\mathrm{id}_{(X,x)}$ è dato dal morfismo identico id_X di X in C.

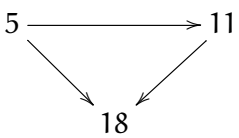
Esercizio 1.1.26. Dimostrare che i dati descritti sopra definiscono una categoria.

Negli esempi che seguono, la costruzione della categoria slice viene applicata ad alcune categorie introdotte negli esempi precedenti.

Esempio 1.1.27 (La categoria $(\mathbb{Z},|)/n$ dei divisori di $n \in \mathbb{Z}$.). Ha come oggetti i divisori di n, come frecce la relazione di divisibilità. Ad esempio, $2|6$ può essere interpretata come freccia $2 \to 6$ in $(\mathbb{Z},|)/18$:



Esempio 1.1.28 (La categoria $(\mathbb{Z},\leqslant)/n$ degli interi minori o uguali a $n \in \mathbb{Z}$.). Ha come oggetti gli interi minori o uguali a n, come frecce la relazione d'ordine naturale. Ad esempio, $5 \leqslant 11$ può essere interpretata come freccia $5 \to 11$ in $(\mathbb{Z},\leqslant)/18$:



Esempio 1.1.29. Sia I un insieme. Una applicazione $f\colon X \to I$ può essere sempre interpretata come una famiglia di insiemi indicizzati da I: basta considerare, per ogni $i \in I$, la controimmagine $f^{-1}(i)$. Se poniamo, per ogni i,

$$X_i := f^{-1}(i)$$

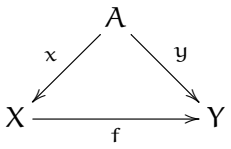
ecco che abbiamo definito la famiglia di insiemi $\{X_i\}_{i\in I}$, di cui I è il cosiddetto *insieme di indici*; dato $i \in I$, l'insieme X_i è detto *fibra di* f *sopra* i. Si verifica che la famiglia $\{X_i\}_{i\in I}$ costituisce una *partizione* dell'insieme X.

Siamo ora pronti a descrivere la categoria Set/I. Gli oggetti, abbiamo già visto, sono proprio le famiglie di insiemi indicizzate da i; inoltre, dati due oggetti (X, f) e (Y, g), si vede subito che che un morfismo $\phi\colon (X, f) \to (Y, g)$ è una funzione $X \to Y$ compatibile con le partizioni determinate da f e g. Concludiamo che ϕ corrisponde a una collezione di funzioni $\phi_i\colon X_i \to Y_i$, un morfismo di famiglie di insiemi.

Se invertiamo il ruolo di dominio e codominio nella costruzione precedente otteniamo ancora una categoria.

Data una categoria C e un suo oggetto fissato A, possiamo definire la categoria coslice di A su C, in simboli A/C.

- Gli oggetti di A/C sono le frecce di C di dominio A.
- Un morfismo dall'*oggetto* $\begin{smallmatrix} A \\ \downarrow x \\ X \end{smallmatrix}$ all'*oggetto* $\begin{smallmatrix} A \\ \downarrow y \\ Y \end{smallmatrix}$ è una freccia $f\colon X \to Y$ in C tale che $f \circ x = y$, ovvero tale che il seguente diagramma commuti in C:



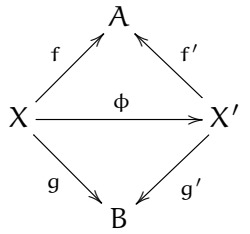
Esercizio 1.1.30. Completare la definizione di categoria coslice e verificare che soddisfa gli assiomi di categoria.

Esempio 1.1.31. Descriviamo la categoria $\mathsf{Set}^* := \{*\}/\mathsf{Set}$.

Dalla definizione sappiamo che un oggetto di questa categoria è una funzione $x\colon \{*\} \to X$. Ma una funzione dal singoletto a un insieme può essere identificata semplicemente con un elemento $x \in X$. Sempre dalla definizione, ricaviamo che un morfismo $f\colon (X, x) \to (Y, y)$ deve soddisfare $f \circ x = y$, che, sfruttando l'identificazione riportata sopra, scriviamo semplicemente $f(x) = y$. In conclusione, la categoria Set^* risulta essere quella che è comunemente detta *categoria degli insiemi puntati*, ossia la categoria che ha per oggetti gli insiemi con un elemento scelto (punto base) e morfismi le funzioni che preservano tale elemento.

La costruzione della categoria slice può essere raddoppiata. Data una categoria C, e due suoi oggetti A e B, chiameremo *bislice* la

categoria $C_{A,B}$ che descriviamo subito. Gli oggetti di $C_{A,B}$ sono triple (X, f, g), dove X è un oggetto di C, e $f\colon X \to A$ e $g\colon X \to B$ sono frecce di C. Un morfismo $\phi\colon (X, f, g) \to (X, f', g')$ è una freccia $\phi\colon X \to X'$ di C tale che $f' \circ \phi = f$ e $g' \circ \phi = g$; ovvero tale che il seguente diagramma commuti:



Esercizio 1.1.32. Completare la definizione di $C_{A,B}$ e verificare che soddisfa gli assiomi di categoria.

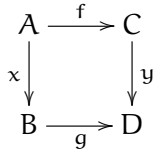
1.1.8 *Categorie di frecce*

Avvertenza 1.1.33. *Questa sezione ha lo scopo di introdurre delle costruzioni che verranno utilizzate nel seguito, ad esempio, per descrivere le estensioni di campi. Pertanto, essa può essere tranquillamente tralasciata ad una prima lettura del testo, per essere poi recuperata quando sarà necessaria.*

Le categorie slice e coslice viste nella sezione precedente, sono particolari categorie di frecce, cioè categorie i cui oggetti sono le frecce di una categoria fissata. Più in generale, fissata una categoria C, si può definire la categoria $\mathsf{Arr}(C)$ delle frecce di C. Essa ha per oggetti tutte le frecce di C; inoltre, dati due *oggetti*:

$$x\colon A \to B \qquad y\colon C \to D$$

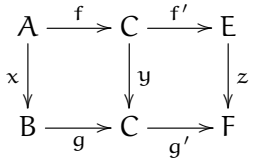
una morfismo $x \to y$ in $\mathsf{Arr}(C)$ è dato da una coppia di frecce $f\colon A \to C$ e $g\colon B \to D$ tale che il seguente diagramma sia commutativo:



La composizione di morfismi in $\mathsf{Arr}(C)$ si calcola componente per componente, ovvero, dati i morfismi

$$(f, g)\colon x \to y \qquad \text{e} \qquad (f', g')\colon y \to z$$

si definisce $(f', g') \circ (f, g) = (f' \circ f, g' \circ g)$, come si può vedere nel diagramma seguente:



L'identità di $x\colon A \to B$ è la coppia $(\mathrm{id}_A, \mathrm{id}_B)$.

Esercizio 1.1.34. Completare la definizione di $\mathsf{Arr}(C)$ e verificare che soddisfa gli assiomi di categoria.

1.1.9 *La categoria opposta*

Data una categoria C, consideriamo la categoria C^{op} così definita:

- Gli oggetti di C^{op} sono gli stessi oggetti di $\mathcal{C}$.
- Per A e B oggetti di C, si ha che

$$\mathrm{Hom}_{C^{op}}(A, B) := \mathrm{Hom}_C(B, A)$$

- La composizione di frecce si fa come in C. Più precisamente, date le frecce componibili

$$A \xrightarrow{f^{op}} B \xrightarrow{g^{op}} C \qquad \text{in } C^{op}$$

  esse corrispondono a frecce

$$A \xleftarrow{f} B \xleftarrow{g} C \qquad \text{in } C$$

  Allora possiamo definire $g^{op} \circ f^{op}$ in C^{op} come $(f \circ g)^{op}$.

- Le identità sono sostanzialmente le stesse di C.

Riassumendo, l'opposta di una categoria C si ottiene invertendo (formalmente) le frecce della categoria. Vediamo subito due casi estremi che si rifanno agli esempi visti in precedenza. La categoria $(\mathbb{Z}, \leqslant)^{op}$ corrisponde al preordine $(\mathbb{Z}, \geqslant)$. La categoria $(S, \sim)^{op}$ è invece isomorfa a $(S, \sim)$ (non abbiamo ancora visto la nozione di isomorfismo di categorie, ma in questo caso, dovrebbe essere chiaro dal contesto).

Nel caso di categorie preordine, allora, la categoria opposta non è altro che la relazione opposta sullo stesso insieme. Per le categorie più complesse, la situazione non è così semplice. Da un punto di vista tecnico, la costruzione della categoria opposta è un fatto puramente formale. Se ad esempio consideriamo la categoria Set degli insiemi e delle funzioni, si ha che un morfismo $f\colon A \to B$ Set^{op} è definito da una funzione $B \to A$. In altre parole, *dico* che ho un morfismo f come sopra se, in realtà, ho una funzione $\hat{f}$ che va nella direzione opposta. Ad esempio, per ogni insieme A c'è esattamente un morfismo $A \to \emptyset$, in Set^{op}, quello che corrisponde all'inclusione del vuoto in A (questo ovviamente non implica che ci sia una qualche funzione $A \to \emptyset$). Diventa allora interessante cercare una interpretazione della categoria opposta, interessante ma lontano dagli scopi di questo corso. Per completezza, precisiamo che nel caso preso in esame, Set^{op} può essere descritta come la categoria delle Algebre di Boole Atomiche Complete [**?**].

Esercizio 1.1.35. Sia C una categoria e A un oggetto di C. Mostrare che la categoria coslice A/C può essere descritta dalla categoria slice $(C^{op}/A)^{op}$. Analogamente, C/A può essere descritta da $(A/C^{op})^{op}$.

L'esercizio precedente ci fornisce almeno una buona ragione per introdurre la nozione di categoria opposta. La prima affermazione, infatti, ci dice che in realtà la nozione di categoria coslice può essere ottenuta a partire da quella di slice, cioè non è una nozione *nuova*. Questo è un fenomeno ricorrente, che ha meritato per la sua importanza un nome: *Principio di Dualità*. Informalmente, data una proposizione che riguarda oggetti e frecce di C, la proposizione duale si ottiene scambiando domini e codomini delle frecce e invertendo le composizioni nella proposizione originaria. Non è difficile provare che una certa proprietà sia vera in C, se e solo se la proprietà duale è vera in C^{op}.

1.1.10 *Isomorfismi*

Introduciamo ora la nozione di isomorfismo, o freccia iso. Nel caso dei gruppi o degli anelli, sappiamo bene che un omomorfismo

$$A \xrightarrow{f} B$$

è un *isomorfismo* quando la funzione f tra gli insiemi sostegno di A e B è una funzione biiettiva, ossia:

(i) f è una funzione: per ogni $x \in A$, esiste un unico $y \in B$ tale che $f(x) = y$

(ii) f è biiettiva: per ogni $y \in B$ esiste un unico $x \in A$ tale che $f(x) = y$

Scritta così, la definizione manifesta subito una proprietà delle funzioni biiettive: se (i) ci dice che che f è una funzione, (ii) testimonia il fatto che anche la relazione inversa f^{-1} è una funzione. Più precisamente, possiamo dare la seguente caratterizzazione, la cui dimostrazione è lasciata come esercizio.

Proposizione 1.1.36. *Una funzione* $f\colon A \to B$ *è biiettiva se e solo se esiste una funzione* $g\colon B \to A$ *tale che* $f \circ g = \mathrm{id}_B$ *e* $g \circ f = \mathrm{id}_A$.

Notiamo che la proposizione sopra non non si riferisce in alcun modo agli elementi di A o B, ma utilizza semplicemente la nozione di composizione e le funzioni identiche. Essa si presta quindi a diventare una definizione valida in una categoria qualunque.

Definizione 1.1.37. *Una freccia* $f\colon A \to B$ *di una categoria* C *è un iso(morfismo) se esiste una freccia* $g\colon B \to A$ *tale che* $f \circ g = \mathrm{id}_B$ *e* $g \circ f = \mathrm{id}_A$.

Possiamo allora interpretare la proposizione sopra come segue: nella categoria Set, gli iso sono precisamente le biiezioni.

La domanda che ci si può porre a questo punto, è la seguente: quanto la definizione di isomorfismo in una categoria riesce a catturare delle proprietà delle biiezioni? Ad esempio, è ben noto che data una biiezione f, la sua inversa è unica. Possiamo affermare lo stesso per una generica freccia iso? La risposta affermativa segue dalla prossima proposizione.

Proposizione 1.1.38. *Data una freccia* $f\colon A \to B$ *di una categoria* C, *se* f *è iso, la sua inversa è unica.*

Dimostrazione. Supponiamo di avere due frecce $g_1, g_2\colon B \to A$ tali che

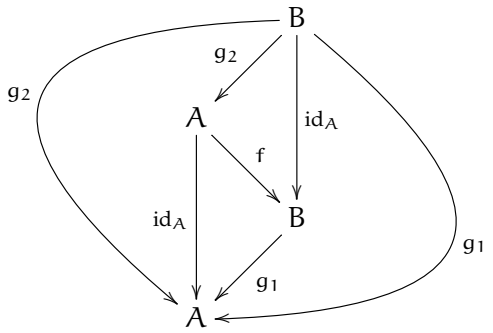
$$f \circ g_1 = \mathrm{id}_B \quad \text{e} \quad g_1 \circ f = \mathrm{id}_A$$

$$f \circ g_2 = \mathrm{id}_B \quad \text{e} \quad g_2 \circ f = \mathrm{id}_A$$

Allora si ha:

$$g_1 = g_1 \circ 1_B = g_1 \circ f \circ g_2 = \mathrm{id}_A \circ f \circ g_2 = g_2$$

dove abbiamo usato soltanto il fatto che g_1 è inverso sinistro e che g_2 è inverso destro di f. Osserviamo che la dimostrazione è essenzialmente quella che si utilizza per dimostrare l'unicità degli inversi nei gruppi (nei monoidi). La catena di uguaglianze può essere istruttivamente seguita sul diagramma commutativo riportato qui sotto:



□

Esercizio 1.1.39. Dimostrare le seguenti proprietà degli isomorfismi in una data categoria C:

1. Per ogni oggetto A, l'identità id_A e un iso, con inverso id_A.
2. Se f è un iso, anche f^{-1} è un iso.
3. Date due frecce componibili $A \xrightarrow{f} B \xrightarrow{g} C$, se entrambe f e g sono iso, allora $g \circ f$ è un iso; inoltre si ha $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Esercizio 1.1.40. Descrivere gli isomorfismi delle categorie Gp, Rng, $(\mathbb{Z}, \leqslant)$, $(\mathbb{Z}, |\,)$, Lin, C/A.

Dato un oggetto A di una categoria C, denotiamo con $\mathrm{Aut}_{\mathsf{C}}(A)$ la classe di tutti gli isomorfismi $A \to A$. Possiamo interpretare $\mathrm{Aut}_{\mathsf{C}}(A)$ come un gruppo, in particolare, un sottomonoide di $\mathrm{End}_{\mathsf{C}}(A)$.

Definizione 1.1.41. *Chiamiamo* gruppoide *una categoria* C *in cui tutte le frecce siano iso.*

In particolare, è possibile identificare un gruppoide con un solo oggetto con un gruppo. Viceversa, dato un gruppo G, denotiamo con $\mathsf{B}G$ la categoria (gruppoide) avente un unico oggetto $*$, e con le frecce, necessariamente $* \to *$ etichettate dagli elementi di G; la freccia identica è l'identità e del gruppo.

1.2 PROPRIETÀ UNIVERSALI

Lo scopo di questa sezione è introdurre il concetto di *proprietà universale*. Come vedremo, molte costruzioni che abbiamo già incontrato in algebra sono universali.

Le proprietà universali sono proprietà degli oggetti, e li caratterizzano a meno di isomorfismi.

1.2.1 *Oggetti terminali e oggetti iniziali*

I primi *universali* che incontreremo sono gli oggetti terminali e gli oggetti iniziali. Essi sono caratterizzati dalla proprietà descritta nella prossima definizione.

Definizione 1.2.1. *Un oggetto* T *di una categoria* C *è detto* terminale *se, per ogni altro oggetto* A *di* C*, esiste uno e un solo morfismo* $A \to \mathsf{T}$.
Un oggetto I *di una categoria* C *è detto* iniziale *se, per ogni altro oggetto* A *di* C*, esiste uno e un solo morfismo* $\mathsf{I} \to A$.

Analizziamo la situazione in alcune delle categorie introdotte in precedenza.

Esempio 1.2.2. In $(\mathbb{Z}, \leqslant)$ non esistono né oggetto iniziale, né terminale. Infatti, se ci fosse un oggetto iniziale, esisterebbe un $i \in \mathbb{Z}$ tale che $i \leqslant n$, per ogni numero intero n, il che è falso. Analogamente, se ci fosse un oggetto terminale, allora esisterebbe $t \in \mathbb{Z}$ tale che $n \leqslant t$, per ogninumero intero n, il che è falso.

Esempio 1.2.3. In $(\mathbb{N}, \leqslant)$ 0 è iniziale, non esiste terminale. Chiaramente, $0 \leqslant n$, per ogni numero naturale n. Questo si traduce nell'esistenza di una freccia $0 \to n$, per ogni n. L'unicità è ovvia, e dipende dal fatto che $(\mathbb{N}, \leqslant)$ è una categoria preordine. Per quanto riguarda l'oggetto terminale, esso non esiste, come nell'esempio precedente.

Esempio 1.2.4. In $(\mathbb{Z}, |)$ 1 è iniziale, 0 è terminale. Banalmente, $1|n$ e $n|0$, per ogni intero n. L'unicità si ottiene come sopra.

Esempio 1.2.5. In $(\mathcal{P}(X), \subseteq)$ $\emptyset$ è iniziale, X è terminale.

Esempio 1.2.6. In Set, l'insieme vuoto $\emptyset$ è iniziale, il singoletto $\{*\}$ è terminale. Infatti, è ben noto che per ogni insieme S, esiste un'unica funzione $\emptyset \to S$, ovvero l'inclusione dell'insieme vuoto. Inoltre, esiste una unica funzione $S \to \{*\}$, quella che assegna tutti gli elementi di S all'unico elemento $*$ dell'insieme singoletto.

Esempio 1.2.7. Per quanto riguarda la categoria Gp dei gruppi, è facile verificare che il gruppo banale è allo stesso tempo oggetto terminale e iniziale. Analogamente, nella categoria Rng degli anelli, lo zero-anello 0 è terminale e iniziale, mentre nella categoria K-Vect, lo spazio banale è terminale e iniziale.

Definizione 1.2.8. *Una categoria* C *è detta* puntata *se essa ammette sia oggetto iniziale* I *che oggetto terminale* T*, e l'unica freccia* $I \to T$ *è un iso. L'oggetto iniziale/terminale di una categoria puntata è spesso denotato* 1 *oppure* 0*. In una categoria puntata, dati due oggetti* X *e* Y*, esiste sempre una freccia da* X *a* Y *che fattorizza per* 0*:*

$$X \longrightarrow 1 \longrightarrow Y \quad , \qquad X \xrightarrow{\tau_{X,Y}} Y$$

Questa freccia è denotata $\tau = \tau_{X,Y}$ *ed è chiamata freccia* banale*.*

- La categoria Ring degli anelli unitari si comporta in modo alquanto diverso da Rng. Se infatti lo zero-anello è oggetto terminale anche di Ring, la situazione cambia se analizziamo il caso dell'oggetto iniziale. In effetti, dato un anello unitario A, l'omomorfismo di anelli $0 \to A$ non è un omomorfismo di anelli unitari, per il semplice fatto che non preserva l'unità moltiplicativa.

Esempio 1.2.9. L'anello $\mathbb{Z}$ degli interi è l'oggetto iniziale della categoria Ring degli anelli unitari.

Dimostrazione. Per ogni anello unitario A, è facile definire un omomorfismo $f\colon \mathbb{Z} \to A$ di anelli unitari. In effetti, $f(0) = 0$ e $f(1) = 1$ per definizione, per cui siamo forzati a definire $f(n) = n \cdot f(1)$; questo ci dà automaticamente anche l'unicità. □

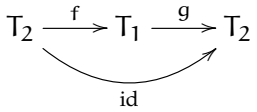
Normalmente, gli oggetti terminali sono definiti, e conseguentemente determinati, a meno di isomorfismi. Ad esempio, l'insieme singoletto è di solito indicato con $\{*\}$, ma ogni insieme con un solo elemento può andare bene. Più in generale, vale la seguente proposizione.

Proposizione 1.2.10. *Se* T_1 *e* T_2 *sono terminali nella categoria* C*, allora* $T_1 \cong T_2$*, e questo isomorfismo è univocamente determinato.*

Dimostrazione. Poiché T_1 è terminale, esiste una unica freccia $f\colon T_2 \to T_1$; analogamente poiché anche T_2 è terminale, esiste una unica freccia $g\colon T_1 \to T_2$. Ora consideri il seguente diagramma:

$$T_1 \xrightarrow{g} T_2 \xrightarrow{f} T_1 \qquad (\text{id})$$

Poiché I_1 è terminale, deve esistere una unica freccia $T_1 \to T_1$, e questo forza il diagramma a essere commutativo: $f \circ g = \mathrm{id}_{T_1}$. Analogamente, si considera il diagramma:



Questa volta si usa il fatto che T_2 è terminale, e quindi l'unicità della freccia $T_2 \to T_2$ implica di nuovo la commutatività del diagramma: $g \circ f = \mathrm{id}_{T_2}$. Concludiamo che f e g sono iso, con $g = f^{-1}$, e che tali isomorfismi sono univocamente determinati. In particolare vale $T_1 \cong T_2$. □

Osservazione 1.2.11. Si verifica facilmente che un oggetto T è terminale in C se e solo se è iniziale in C^{op}. In altre parole, iniziale e terminale sono concetti duali.

L'osservazione precedente ci permette di vedere all'opera per la prima volta il principio di dualità. Infatti, la Proposizione 1.2.10 è stata enunciata per l'oggetto terminale, ma la dimostrazione, vale anche per l'enunciato duale. Più precisamente, la dimostrazione duale si ottiene invertendo tutte le frecce nella dimostrazione originaria. Vale quindi la seguente proposizione.

Proposizione 1.2.12. *Se* I_1 *e* I_2 *sono iniziali nella categoria* C*, allora* $I_1 \cong I_2$*, e questo isomorfismo è univocamente determinato.*

Concludiamo la sezione con la seguente definizione molto generale di *universale*, definizione che applicheremo subito dopo nella definizione di prodotti, coprodotti, nuclei, conuclei e quozienti.

Definizione 1.2.13 (Proprietà Universale)**.** *Una costruzione si dice che* soddisfa una proprietà universale *se essa può essere interpretata come l'oggetto terminale (o l'oggetto iniziale) di una opportuna categoria.*

Come conseguenza, un universale è unico, a meno di isomorfismi.

Osservazione 1.2.14. Il concetto di proprietà universale in una categoria si si può formalizzare in diversi modi, e di solito si utilizza la nozione di cono limite. In queste pagine introduttive, abbiamo scelto di presentare gli universali come iniziali e/o terminali. È un modo questo che ha il pregio di essere sufficientemente compatto e rigoroso, tuttavia, nasconde sotto il tappeto le difficoltà: come faccio a trovare l'*opportuna categoria* a cui la definizione si riferisce? Lasciamo al lettore volenteroso il piacere di consultare uno dei testi in bibliografia per rispondere a questa domanda.

1.2.2 *Prodotti*

Dati due insiemi A e B, il loro prodotto cartesiano $A \times B$ è definito

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

In realtà la nozione di coppia ordinata è una nozione piuttosto delicata. Infatti, implicitamente, la possibilità di formare delle coppie ordinate presuppone la capacità di estrarre da tali coppie il primo e il secondo elemento. Questo si traduce con l'esistenza, accanto al prodotto cartesiano, di due funzioni, le cosiddette *proiezioni canoniche*,

$$\pi_1 : A \times B \to A\,, \qquad \pi_2 : A \times B \to B\,,$$

così definite:

$$\pi_1(a, b) = a\,, \qquad \pi_2(a, b) = b\,.$$

Osserviamo che il prodotto cartesiano di due insiemi, insieme con le sue proiezioni canoniche, soddisfa la seguente proprietà universale:

Per ogni insieme X *e per ogni coppia di funzioni*

$$f_1 : X \to A\,, \qquad f_2 : X \to B\,,$$

esiste un'unica funzione $\phi : X \to A \times B$ *tale che, per ogni* $x \in X$ *si abbia*

$$\pi_1(\phi(x)) = f_1(x)\,, \qquad \pi_2(\phi(x)) = f_2(x)\,.$$

In effetti, per convincersi della correttezza di quanto affermato, è sufficiente considerare la funzione ϕ così definita:

$$\phi(x) = (f_1(x), f_2(x))\,,$$

e la verifica dell'unicità è immediata.

Una costruzione analoga si può realizzare ad esempio se gli insiemi A e B sostengono una struttura di gruppo. In tale caso, il prodotto cartesiano $A \times B$ può essere naturalmente dotato di una struttura di gruppo a sua volta, con l'operazione definita componente per componente. Nei corsi di algebra, è quello che viene comunemente chiamato il *prodotto diretto di* A *e* B. Da notare, che in questo caso, le proiezioni canoniche sono automaticamente degli omomorfismi di gruppo, e vale una proprietà universale del tutto simile a quella enunciata sopra.

La nozione di prodotto di due oggetti può essere espressa all'interno di una generica categoria, a patto di liberarci degli elementi nella sua definizione. È facile convincersi allora della correttezza della prossima definizione.

Definizione 1.2.15 (Proprietà Universale del Prodotto)**.** *Dati due oggetti* A *e* B *di una categoria* C*, il loro prodotto (se esiste) è una tripla*

$$A \xleftarrow{\pi_1} P \xrightarrow{\pi_2} B$$

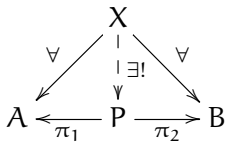
tale che per ogni altra tripla

$$A \xleftarrow{f_1} X \xrightarrow{f_2} B$$

esiste una unica freccia $\phi\colon X \to P$ *tale che*

$$\pi_1 \circ \phi = f_1 \qquad \pi_2 \circ \phi = f_2\,. \tag{3}$$

La situazione può essere rappresentata dal seguente diagramma commutativo:



L'oggetto P *è di solito denotato* $A \times B$.

Diremo che la categoria C ammette prodotti *se, presi comunque due oggetti* A *e* B*, il loro prodotto esiste in* C.

Osserviamo subito che il prodotto di due oggetti non è un oggetto, ma va sempre considerato insieme alle due proiezioni.

Illustriamo ora la definizione mediante alcuni esempi relativi alle categorie introdotte in precedenza, lasciando le verifiche al lettore.

Esempio 1.2.16. Come abbiamo appena osservato, nella categoria Gp dei gruppi il prodotto diretto è un prodotto categoriale, nel senso che, insieme alle proiezioni canoniche, soddisfa la relativa proprietà universale. Lo stesso per la categoria dei gruppi abeliani.

Esempio 1.2.17. Nella categoria Rng degli anelli, la somma diretta di anelli è un prodotto categoriale, sempre considerando anche le proiezioni canoniche. Lo stesso per la categoria degli anelli unitari, commutativi e commutativi unitari.

Esempio 1.2.18. La somma diretta di spazi serve da prodotto nella categoria K-Vect degli spazi vettoriali su K.

Non sempre in una categoria è possibile formare il prodotto di due suoi oggetti. Il prossimo esempio presenta proprio questa situazione.

Esempio 1.2.19. La categoria Fld dei campi non ha prodotti. Questa affermazione, per ora, non la dimostriamo. Ci limitiamo a osservare che il candidato naturale del prodotto di due campi non è un campo. Infatti, dati i campi K e L, possiamo considerare il loro prodotto $K \times L$ nella categoria Ring degli anelli unitari. Come è facile vedere, l'anello $K \times L$ non è un campo, in quanto possiede divisori dello zero: $(1,0)\cdot(0,1) = (0,0)$.

Vediamo ora qualche esempio nelle categorie preordine.

Esempio 1.2.20. In $(\mathbb{Z}, \leqslant)$ il prodotto di due oggetti (= numeri interi) n, m esiste sempre ed è $p = \min(m,n)$. Nello specifico, se $p = \min(m,n)$, si ha

$$p \leqslant m\,, \qquad p \leqslant n\,,$$

che si traduce nell'esistenza delle *proiezioni*

$$p \to m\,, \qquad p \to n\,.$$

Inoltre, se per un numero intero q si hanno le frecce

$$q \to m\,, \qquad q \to n\,,$$

questo vuol dire semplicemente che

$$q \leqslant m\,, \qquad q \leqslant n\,.$$

Ora, essendo p il minimo tra m e n, segue che $q \leqslant p$ e quindi vi è una (necessariamente unica) freccia $q \to p$. Le condizioni (3) sono automaticamente soddisfatte per il fatto che in un preordine, se esite una freccia tra due oggetti, essa è necessariamente unica.

Esempio 1.2.21. In $(\mathbb{Z}, |\,)$ il prodotto di due oggetti (= numeri interi) n, m esiste sempre ed è $p = \mathrm{MCD}(m, n)$. La verifica si ottiene in maniera analoga all'esempio precedente.

Esempio 1.2.22. In $(\mathcal{P}(X), \subseteq)$ il prodotto di due oggetti (= sottoinsiemi di X) U, V esiste sempre ed è $P = U \cap V$. Anche in questo caso, la verifica si ottiene in maniera analoga gli esempi precedenti.

La proposizione che segue fornisce almeno una buona ragione per avere introdotto la costruzione della categoria bislice.

Proposizione 1.2.23. *Data una categoria* C *e due suoi oggetti* A, B*, il loro prodotto, se esiste, è l'oggetto terminale di* $C_{A,B}$*.*

Dimostrazione. Sia P il prodotto di A e B, e π_1, π_2 le relative proiezioni. Ovviamente, la tripla (P, π_1, π_2) è un oggetto di $C_{A,B}$; verifichiamo che sia terminale. A questo scopo, consideriamo un qualunque altro oggetto (X, f_1, f_2) di $C_{A,B}$. Poiché P è un prodotto, esiste un'unica freccia di C, $\phi\colon X \to P$ che soddisfa le condizioni (3), ma queste condizioni garantiscono che ϕ sia anche una freccia di $C_{A,B}$. □

Come conseguenza diretta della proposizione precedente, e della Proposizione 1.2.12, deduciamo che il prodotto di due oggetti è unico, a meno di un unico isomorfismo (che commuta con le proiezioni). Per questo sarebbe opportuno parlare di *un* prodotto, piuttosto che *del* prodotto, tuttavia, spesso nel linguaggio corrente si dice il prodotto, sottintendendo il fatto che stiamo considerando una qualche versione canonica del prodotto.

Esercizio 1.2.24. Nella categoria degli insiemi, dati due insiemi A e B, verificare che ognuno dei seguenti insiemi è il prodotto di A con B, e in ciascun caso, descrivere le proiezioni.

(i) $P = \{(a, b) \mid a \in A, b \in B\}$

(ii) $Q = \{(b, a) \mid a \in A, b \in B\}$

(iii) $R = \{(a, b, a) \mid a \in A, b \in B\}$

(iv) $S = \{(a, *, b) \mid a \in A, b \in B\}$

Determinare inoltre le biiezioni $P \simeq Q$, $P \simeq R$ e $P \simeq S$ che commutano con le proiezioni, cioè che soddisfano la (3).

Delle diverse versioni del prodotto di A e B, la (i) è quella che chiameremo *canonica*, come chiameremo canoniche le proiezioni ad essa associate.

Esercizio 1.2.25. Verificare che la categoria Lin ha prodotti, e descriverli.

Svolgimento. Il prodotto di due oggetti m e n di Lin è rappresentato dalla loro somma $n + m$ come numeri naturali. Le due proiezioni sono le matrici

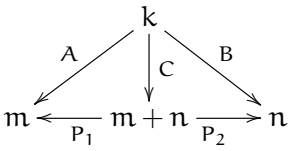
$$P_1 = \left[\begin{array}{c|c} I_m & 0 \end{array}\right] \in \mathrm{Mat}_K(m, m+n)$$

$$P_2 = \left[\begin{array}{c|c} 0 & I_n \end{array}\right] \in \mathrm{Mat}_K(n, m+n)$$

Verifichiamo la proprietà universale. Data due frecce $A\colon k \to m$ e $B\colon k \to n$ in Lin, queste sono due matrici $A \in \mathrm{Mat}_K(m, k)$ e $B \in \mathrm{Mat}_K(n, k)$. La matrice

$$C = \left[\begin{array}{c} A \\ \hline B \end{array}\right]$$

è proprio la freccia $k \to m + n$ determinata dalla proprietà universale del prodotto. Infatti, è facile vedere che $P_1 C = A$ e $P_2 C = B$, come rappresentato nel diagramma:



Inoltre, per ogni altra matrice D tale che $P_1 D = A$ e $P_2 D = B$, la prima relazione ci dice precisamente che le prime m righe di D coincidono con la matrice A, la seconda relazione ci dice che le ultime n coincidono con B. Concludiamo $C = D$, e l'unicità è dimostrata. □

1.2.3 *Coprodotti*

La nozione di coprodotto è la nozione duale a quella di prodotto.

Definizione 1.2.26 (Proprietà universale del coprodotto)**.** *Dati due oggetti A e B di una categoria C, il loro coprodotto (se esiste) è una tripla*

$$A \xrightarrow{\iota_1} Q \xleftarrow{\iota_2} B$$

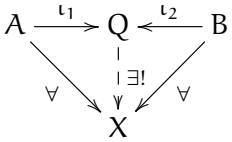
tale che per ogni altra tripla

$$A \xrightarrow{f_1} X \xleftarrow{f_2} B$$

esiste un'unica freccia $\phi\colon Q \to X$ *tale che*

$$\phi \circ \iota_1 = f_1 \qquad \phi \circ \iota_2 = f_2 \tag{4}$$

La situazione può essere rappresentata dal seguente diagramma commutativo:



L'oggetto Q *è di spesso denotato* $A \amalg B$*, oppure* $A + B$*.*

Diremo che la categoria C ammette coprodotti *se, presi comunque due oggetti* A *e* B*, il loro coprodotto esiste in* C*.*

Anche per il coprodotto, come già per il prodotto, rimarchiamo che il coprodotto di due oggetti non è semplicemente un oggetto, ma una tripla composta da un oggetto e due frecce.

Illustriamo la definizione mediante alcuni esempi relativi alle categorie già introdotte, lasciando le verifiche al lettore.

Esempio 1.2.27. Nella categoria Set degli insiemi, il coprodotto è l'unione disgiunta. Ricordiamo che, dati due insiemi A e B, la loro unione disgiunta può essere descritta come

$$A \amalg B = (A \times \{0\}) \cup (B \times \{1\})$$

Le funzioni ι_1 e ι_2 sono allora le *iniezioni canoniche*

$$\iota_1\colon a \mapsto (a, 0) \qquad \iota_2\colon b \mapsto (b, 1)$$

Esempio 1.2.28. La somma diretta di spazi funge anche da coprodotto nella categoria K-Vect degli spazi vettoriali su K: dati gli spazi vettoriali V e W si hanno le *iniezioni canoniche*

$$V \xrightarrow{\iota_1} V \times W \xleftarrow{\iota_2} W$$

così definite:

$$\iota_1(v) = (v, 0) \qquad \iota_2(w) = (0, w)\,.$$

Analogamente, il prodotto di gruppi abeliani funge anche da coprodotto in Ab. In questi casi, quando prodotto e coprodotto coincidono, si parla di *biprodotto*, e si usa il simbolo $\oplus$.

Esempio 1.2.29. Per quanto riguarda la categoria Gp dei gruppi, il coprodotto di due gruppi esiste sempre ed è il cosiddetto *prodotto libero* dei due gruppi. La sua descrizione, un po' più complicata rispetto al caso dei gruppi abeliani, viene rimandata alla sezione relativa ai gruppi liberi (vedi la Sezione 2.2.6).

Esempio 1.2.30. In $(\mathbb{Z}, \leqslant)$ il coprodotto di due oggetti (= numeri interi) n, m esiste sempre ed è $p = \max(m, n)$.

Esempio 1.2.31. In $(\mathbb{Z}, |)$ il coprodotto di due oggetti (= numeri interi) n, m esiste sempre ed è $p = \mathrm{mcm}(m, n)$.

Esempio 1.2.32. In $(\mathcal{P}(X), \subseteq)$ il coprodotto di due oggetti (= sottoinsiemi di X) U, V esiste sempre ed è $P = U \cup V$.

Esercizio 1.2.33. Verificare che la categoria Lin ha coprodotti, e descriverli.

Proposizione 1.2.34. *Data una categoria C e due suoi oggetti A, B, il loro coprodotto, se esiste, è l'oggetto iniziale di $\mathsf{C}^{A,B}$.*

Dimostrazione. Si ottiene per dualità, osservando che $(\mathsf{C}^{A,B})^{\mathsf{op}} = \mathsf{C}^{\mathsf{op}}_{A,B}$. Infatti, l'oggetto iniziale di $\mathsf{C}^{A,B}$ è precisamente l'oggetto terminale di $(\mathsf{C}^{A,B})^{\mathsf{op}}$, ovvero l'oggetto terminale di $\mathsf{C}^{\mathsf{op}}_{A,B}$, cioè il prodotto in C^{op}, che altri non è che il coprodotto in C. □

Il coprodotto è quindi un universale, e pertanto è unico, a meno di isomorfismi.

1.2.4 *Quozienti*

Sia X un insieme. Data una relazione di equivalenza $R \subseteq X \times X$, l'insieme quoziente X/R è definito come l'insieme delle classi di equivalenza di X determinate da R. Per $x \in X$, denotiamo la classe di x con $[x]_R$, o più semplicemente $[x]$. Si ha, per definizione,

$$[x] = \{x' \in X \mid x' R x\}$$

Ora, contestualmente all'insieme quoziente, si definisce una funzione, la proiezione canonica,

$$p_R \colon X \to X/R$$

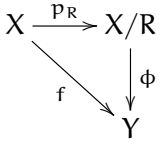
data dalla posizione $x \mapsto [x]$. La proiezione canonica p_R è universale rispetto a tutte le funzioni $f \colon X \to Y$ che assumono valori uguali su elementi che sono in relazione tra loro.

È questa la cosiddetta *proprietà universale del quoziente*, declinata nella categorie degli insiemi.

Data una funzione $f \colon X \to Y$ tale che

$$f(x) = f(x') \quad \Rightarrow \quad x R x' \tag{5}$$

esiste un unica funzione $\phi \colon R/X \to Y$ tale che $\phi \circ p_R = f$, cioè tale che il seguente diagramma commuti:



Per verificare la validità della proprietà universale del quoziente, è sufficiente definire $\phi([x]) = f(x)$. La definizione è ben posta: se

$x'Rx$, allora $f(x') = f(x)$ per ipotesi. Inoltre, per ogni $x \in X$, si ha $\phi(p_R(x)) = \phi([x]) = f(x)$. L'unicità è evidente.

Osservazione 1.2.35. Osserviamo che il termine *universale* è utilizzato in modo appropriato. Infatti, è possibile considerare la sottocategoria piena della categoria coslice X/Set, avente come oggetti le funzioni $f\colon X \to Y$ che soddisfano la condizione (5), e verificare che p_R è oggetto iniziale di tale categoria.

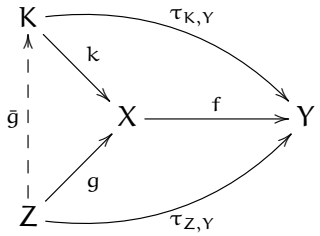
Per generalizzare a una categoria qualunque la nozione di *quoziente* dovremmo trovare un modo per non riferirci agli elementi x e x' nella condizione (5). Questo si può ottenere ricorrendo alla nozione di coequalizzatore, che però non introdurremo in queste note elementari. Lo studente interessato può riferirsi a qualunque testo introduttivo di Teoria delle Categorie, come ad esempio [6].

1.2.5 *Nuclei e conuclei*

Dopo aver presentato i quozienti in Set, siamo pronti a studiare i quozienti nella categoria dei gruppi e in altre situazioni di interesse. Seguendo la tradizione algebrica, essi verranno introdotti in relazione alla nozione di sottogruppo normale, o più in generale, in relazione alle nozioni di nucleo e di conucleo.

Definizione 1.2.36 (Proprietà universale del nucleo)**.** *Sia* C *una categoria puntata,* 1 *oggetto terminale (e iniziale) e* $f\colon X \to Y$ *un morfismo. Il* nucleo di f *è una coppia* $(K, k\colon K \to X)$*, con* $f \circ k = \tau_{K,Y}$*, tale che per ogni* $g\colon Z \to X$ *tale che* $f \circ g = \tau_{Z,Y}$*, esiste un unico* $\bar{g}\colon Z \to K$ *tale che* $k \circ \bar{g} = g$*.*

In altre parole, la freccia k è universale (terminale) tra tutte le frecce di C/X che precomposte con f danno una freccia banale:



Illustriamo la definizione mediante alcuni esempi relativi alle categorie già introdotte, lasciando le verifiche al lettore.

Esempio 1.2.37. In Gp, il nucleo di un omomorfismo $f\colon G \to H$ può essere identificato con il sottogruppo normale N formato dagli elementi di G che f manda nell'elemento neutro di H, i.e. $N = f^{-1}(1_H)$. Più precisamente, il nucleo è la coppia (N, j), dove j è l'inclusione $N \hookrightarrow G$.

Come sappiamo, le proprietà universali determinano gli oggetti a meno di omomorfismi: è facile verificare che qualunque omomorfismo iniettivo $k\colon K \to G$ che abbia immagine N è ancora nucleo di f.

Esempio 1.2.38. In Ab il nucleo di un omomorfismo è definito esattamente come in Gp.

Esempio 1.2.39. In Rng il nucleo di un omomorfismo di anelli $f\colon R \to S$ è l'ideale bilatero I formato dagli elementi di R che f manda in $0 \in S$. Si noti che I è sottoanello di R.

Esempio 1.2.40. La categoria Ring non è puntata, pertanto non ammette nuclei nel senso della Definizione 1.2.36. Infatti, dato un omomorfismo di anelli unitari $f\colon R \to S$, l'ideale bilatero I, formato sempre dagli elementi che f manda in $0 \in S$, non è un sottoanello unitario di R, e quindi non è un oggetto della categoria Ring.

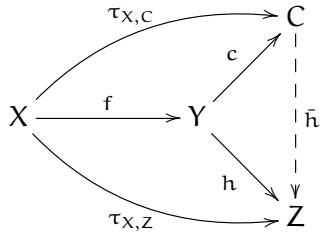
Esempio 1.2.41. In K-Vect, il nucleo di una applicazione lineare $f\colon V \to W$ è il sottospazio di V dei vettori che f manda nel vettore nullo, la *nullità* di f.

Dagli esempi possiamo concludere che se è vero che i nuclei sono sottostrutture (sottogruppi, sottoanelli, sottospazi...) non tutte le sottostrutture sono nuclei. Ad esempio, non tutti i sottogruppi sono nuclei, ma solo i sottogruppi normali possono esserlo.

Di seguito, riportiamo anche la nozione duale a quella di nucleo: il conucleo.

Definizione 1.2.42 (Proprietà universale del conucleo)**.** *Sia* C *una categoria puntata,* 1 *oggetto terminale (e iniziale) e* $f\colon X \to Y$ *un morfismo. Il* conucleo di f *è una coppia* $(C, c\colon Y \to C)$*, con* $c \circ f = \tau_{X,C}$*, tale che per ogni* $h\colon Y \to Z$ *tale che* $h \circ f = \tau_{X,Z}$*, esiste un unico* $\bar{h}\colon C \to Z$ *tale che* $\bar{h} \circ c = h$*.*

In altre parole, la freccia c è universale (iniziale) tra tutte le frecce di Y/C che composte con f danno una freccia banale:



In Ab i conuclei esistono e ammettono una descrizione particolarmente semplice: dato un omomorfismo di gruppi abeliani $f\colon A \to B$, il conucleo si ottiene come gruppo quoziente $B/f(A)$, e l'omomorfismo $c\colon B \to B/f(A)$ è la proiezione canonica. Questo succede perché in Ab tutti i sottogruppi sono normali. Nella categoria dei gruppi, invece, la descrizione esplicita di un conucleo può essere abbastanza complicata.

Esercizio 1.2.43. Dato un omomorfismo di gruppi $f\colon G \to H$, si consideri la chiusura normale $N = \overline{f(G)}$. Verificare che H/N con la proiezione canonica soddisfa la proprietà universale del conucleo.

La forma particolare in cui spesso incontreremo la proprietà universale del conucleo è la seguente.

Proposizione 1.2.44 (Proprietà universale del quoziente in Gp)**.** *Sia* N *sottogruppo normale di un gruppo* G*, e* $p\colon G \to G/N$ *la proiezione canonica. Per ogni omomorfismo* $h\colon G \to Z$ *tale che* $h(N) = 1$*, esiste un unico omomorfismo* $\bar{h}\colon G/N \to Z$ *tale che* $\bar{h} \circ p = h$*.*

In altre parole, la proiezione canonica p è universale (iniziale) tra tutte le frecce di G/Gp che *uccidono* N.

Dimostrazione. Per $gN \in G/N$, definiamo $\bar{h}(gN) = h(g)$. La definizione è ben posta, perché se $g'N = gN$, allora $g'g^{-1} \in N$, e quindi:

$$\bar{h}(g'N) = h(g') = h(g'g^{-1}g) = h(g'g^{-1})h(g) = hg = \bar{h}(gN)\,.$$

Chiaramente $\bar{h}$ è omomorfismo: per $g_1N, g_2N \in G/H$, si ha:

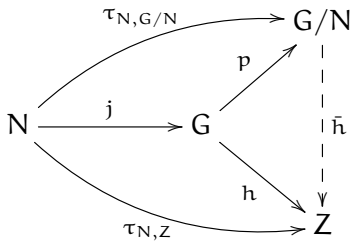
$$\bar{h}(g_1N)\bar{h}(g_2N) = h(g_1)h(g_2) = h(g_1g_2) = g_1g_2N\,.$$

Infine, tale $\bar{h}$ è unica che soddisfi le condizioni. Infatti, se $\phi\colon G/N \to Z$ soddisfa $\phi \circ p = h$, per ogni $gN \in G/N$ si ha:

$$\phi(gN) = \phi(p(g)) = h(g) = \bar{h}(gN)\,.$$

□

È facile verificare che la proprietà universale del quoziente è un caso particolare di proprietà universale del conucleo, dove l'omomorfismo j è l'inclusione di N in G. Ci si convince facilmente di quanto si è affermato analizzando il diagramma seguente:



Osservazione 1.2.45. Il lettore attento si starà domandando quale sia la relazione con la *proprietà universale del quoziente* descritta nella Sezione 1.2.4. In effetti, nella categoria dei gruppi, la nozione di sottogruppo normale serve proprio a descrivere le relazioni di equivalenza interne, chiamate *congruenze*. Più precisamente, se N è normale in G, e $g, h \in G$, possiamo definire la relazione R come gRh se $gh^{-1} \in N$. La relazione R è *interna* alla categoria dei gruppi, nel senso che R è un sottogruppo del prodotto $G \times G$, e il sottogruppo normale N è la classe di equivalenza dell'elemento neutro di G.

2

TEORIA DEI GRUPPI

2.1 GRUPPI E ALTRI ANIMALI DELLO ZOO ALGEBRICO

Le strutture algebriche (gruppi, anelli, campi) verranno qui solo richiamate, per fissare la notazione e inquadrarle in un contesto più generale. Maggiori dettagli si possono trovare su [1, 4].

Definizione 2.1.1. *Sia A un insieme. Una operazione n-aria su A è una funzione (o applicazione)*

$$\omega\colon A \times A \times \cdots \times A \longrightarrow A \ ,$$

dove il dominio è dato dal prodotto cartesiano ripetuto n volte. Il numero n è detto arietà *dell'operazione.*

Molte delle operazioni che si studiano in algebra sono operazioni *binarie*:

$$*\colon\ A \times A \longrightarrow A \ ,$$

In tale caso, per $a, b \in A$, piuttosto che la notazione funzionale (prefissa) $*(a, b)$, si utilizza la più leggibile notazione infissa $a * b$. Sono operazioni binarie le operazioni di addizione, sottrazione e moltiplicazione dell'aritmetica elementare.

Un altro tipo di operazioni che si incontrano spesso sono le operazioni *zerarie*, ovvero di arietà 0. Esse determinano le cosiddette *costanti*. Per comprendere questa affermazione, ricordiamo che, per $n = 0$ il prodotto cartesiano di un insieme eseguito 0 volte è l'insieme singoletto $\{\star\}$, oggetto terminale della categoria degli insiemi. Ora, per la Definizione 2.1.1, un'operazione zeraria è una funzione

$$e\colon\ A^0 = \{\star\} \longrightarrow A \ ,$$

e pertanto può essere identificata con l'immagine dell'unico elemento dell'insieme singoletto: $e(\star) \in A$. Per alleggerire la notazione, identificheremo il nome della funzione con l'unico elemento che essa determina, e scriveremo più semplicemente $e \in A$.

Definizione 2.1.2. *Una struttura algebrica, o insieme strutturato, è dato da un insieme A, detto sostegno o supporto, da un insieme Ω_A di operazioni su A, e da un insieme Σ_A di assiomi che tali operazioni devono soddisfare.*

Ci riferiremo a una determinata struttura algebrica con la notazione (A, Ω_A); più semplicemente, se Ω_A è un insieme finito $\{\omega_1, \ldots, \omega_n\}$, scriveremo

$$(A, \omega_1, \ldots, \omega_n)\,.$$

Se l'insieme delle operazioni è chiaro dal contesto, scriveremo semplicemente A.

Illustriamo la definizione con alcuni esempi.

Esempio 2.1.3. La struttura algebrica più semplice che possa essere imposta su un insieme è... nessuna struttura! Certamente si tratta di un caso limite, ma importante da considerare: un insieme S con un insieme vuoto di operazioni che non devono rispettare alcun assioma.

Esempio 2.1.4. Un insieme M dotato di un operazione binaria $\cdot\colon M \times M \to M$, che non debba soddisfare alcun assioma, si chiama *magma*. Scriviamo $(M, \cdot)$.

Esempio 2.1.5. Un magma $(M, \cdot)$ è chiamato *semigruppo*, se vale la proprietà associativa: per ogni $a, b, c \in M$, si ha che $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Esempio 2.1.6. Un *monoide* $(M, \cdot, e)$ è un magma associativo unitario. Questo vuol dire che, oltre all'operazione binaria $\cdot$ per cui vale la proprietà associativa, è presente un'operazione zeraria, i.e. un elemento $e \in M$, per cui vale $a \cdot e = a = e \cdot a$, per ogni $a \in M$.

Esempio 2.1.7. Un *gruppo* è un monoide $(G, \cdot, e)$ dotato di una ulteriore operazione unaria $(-)^{-1}\colon G \to G$ per cui vale $a \cdot a^{-1} = e = a^{-1} \cdot a$, per ogni $a \in G$.

In modo analogo agli esempi visti sopra si definiscono i gruppi abeliani, gli anelli, gli anelli unitari, etc.

Esercizio 2.1.8. La *morra cinese* è quel gioco in cui i due giocatori devono dichiarare ad ogni turno "carta", "forbici" o "sasso". La carta (c) vince sul sasso(s), che vince sulle forbici (f), le quali a loro volta vincono sulla carta. Gli altri casi consistono in dei pareggi, per cui possiamo dire che, ad esempio, carta contro carta vince carta, e così via. Verificare che, considerando l'insieme $M = \{c, f, s\}$ e interpretando le regole del gioco come operazioni (ad esempio $c * s = c$, $c * c = c$ e così via), la coppia $(M, *)$ ha la struttura di magma commutativo, non associativo.

Esercizio 2.1.9. Spesso si definisce un gruppo come un insieme G dotato di una operazione binaria associativa $\cdot\colon G \times G \to G$ tale che

- $\exists e \in G$ tale che $\forall g \in G, e \cdot g = g = g \cdot e$,
- $\forall g \in G, \exists g^{-1} \in G$ tale che $g \cdot g^{-1} = e = g^{-1} \cdot g$.

Verificare che questa definizione è equivalente a quella data nell'Esempio 2.1.7.

Due insiemi strutturati (A, Ω_A) e (B, Ω_B) sono della stessa specie se esiste una biezione tra i loro insiemi di operazioni, tale che operazioni corrispondenti abbiano la stessa arietà e soddisfino gli *stessi* assiomi, o meglio, assiomi corrispondenti.

Esercizio 2.1.10. A partire dall'Esempio 1.1.17, esprimere gli assiomi di monoide utilizzando diagrammi commutativi in Set.

Suggerimento: si ricordi che, dato un insieme M e un suo elemento $e \in M$, la proprietà universale del prodotto definisce le funzioni:

$$M \ni m \mapsto (e, m) \in M \times M\,,$$
$$M \ni m \mapsto (m, e) \in M \times M\,.$$

Esercizio 2.1.11. Esprimere gli assiomi di gruppo utilizzando diagrammi commutativi in Set.

Suggerimento: si ricordi che, dato un insieme G, la proprietà universale del prodotto definisce la funzione (chiamata diagonale):

$$G \ni g \mapsto (g, g) \in G \times G\,.$$

Definizione 2.1.12. *Date due insiemi strutturati della stessa specie A e B, un omomorfismo è una funzione $f\colon A \to B$ che preserva le operazioni. In altre parole, se ω è un'operazione n-aria di A e ω' la corrispondente operazione n-aria di B, si ha*

$$f(\omega(a_1, \ldots, a_n)) = \omega'(f(a_1), \ldots, f(a_n))\,.$$

Proposizione 2.1.13. *La classe di tutti gli insiemi strutturati di una stessa specie, insieme ai loro omomorfismi, forma una categoria.*

Dimostrazione. Oggetti della categoria sono gli insiemi strutturati di una stessa specie, morfismi gli omomorfismi definiti sopra. La composizione è ben definita. Infatti, dati due omomorfismi $f\colon A \to B$ e $g\colon B \to C$, se ω un operazione n-aria in A, ω' la corrispondente operazione in B e ω'' la corrispondente operazione in C, per ogni n-upla $a_1, \ldots a_n$ di elementi di A, si ha:

$$\begin{aligned}(g \circ f)(\omega(a_1, \ldots, a_n)) &= g(f(\omega(a_1, \ldots, a_n))) \\ &= g(\omega'(f(a_1), \ldots, f(a_n))) \\ &= \omega''(g(f(a_1)), \ldots, g(f(a_n))) \\ &= \omega''((g \circ f)(a_1), \ldots, (g \circ f)(a_n))\end{aligned}$$

Inoltre, dato un insieme strutturato A, è evidente che l'applicazione identica $\mathrm{id}_A\colon A \to A$ è un omomorfismo. La verifica degli assiomi di categoria è immediata. □

2.2 GRUPPI LIBERI

La nozione di struttura liberamente generata è una nozione fondamentale in tutta l'algebra. Il caso dei gruppi ci interessa da vicino, ed è l'oggetto in questo capitolo. Prima di entrare nel vivo della trattazione, vediamo qualche esempio motivante.

2.2.1 *Una motivazione dall'algebra lineare*

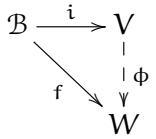
Dall'algebra lineare insegnata nei corsi di geometria, sappiamo che vale il seguente teorema.

> *Dati due spazi vettoriali V e W di dimensione finita, con $\mathcal{B} = \{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ base di V, e data una qualunque funzione $f\colon \mathcal{B} \to W$, esiste una unica applicazione lineare $\phi\colon V \to W$ che estende f, ossia, tale che:*
>
> $$\phi|_{\mathcal{B}} = f.$$

Infatti, dato $\mathbf{a} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$, per la linearità di ϕ si ha:

$$\phi(\mathbf{a}) = \phi(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = a_1 f(\mathbf{v}_1) + \cdots + a_n f(\mathbf{v}_n)\,.$$

Possiamo rappresentare la situazione descritta sopra con il diagramma seguente:



dove la freccia i rappresenta la funzione inclusione della base $\mathcal{B}$ in V, sicché la condizione $\phi|_{\mathcal{B}} = f$ può essere riscritta nella forma

$$\phi \circ i = f.$$

Il significato del teorema è chiaro: il valore di ϕ su un generico vettore è determinato dal valore che f assume sugli elementi di una base di V. Questo succede perché i vettori di $\mathcal{B}$ generano *liberamente* V.

Ma cosa vuol dire esattamente liberamente?

Nel caso in esame, quello che intendiamo affermare è che tra i vettori della base non vi è alcuna *relazione lineare*: nessuno di essi può essere espresso come combinazione lineare dei rimanenti, o equivalentemente, nessuna loro combinazione lineare non banale dà il vettore nullo.

In questo capitolo proveremo a dare una risposta più generale alla domanda posta sopra.

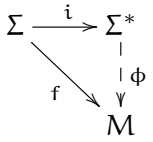
Ma prima vediamo un altro esempio.

2.2.2 *Una motivazione dall'informatica teorica*

Una delle costruzioni classiche per lo studio dei linguaggi formali è quella del *monoide libero*. Dato un alfabeto (di solito, finito) Σ, si indica con Σ^* l'insieme delle *parole* che si possono formare con gli elementi di Σ, dove per *parola* intendiamo una sequenza finita di tali elementi, i caratteri del nostro alfabeto.

L'insieme Σ^* ha una ovvia struttura di monoide, quando consideriamo l'operazione data dalla concatenazione di parole, e per elemento neutro la parola vuota, qui denotata ϵ. Chiamiamo i l'inclusione di Σ in Σ^*, o più precisamente la funzione che associa a ogni carattere di Σ la parola formata da quell'unico carattere. Possiamo enunciare la seguente proprietà universale che caratterizza la coppia (Σ^*, i):

> *Per ogni monoide* $M = (M, \bullet, e)$*, e per ogni funzione* $f\colon \Sigma \to M$*, esiste un unico omomorfismo di monoidi* $\phi\colon \Sigma^* \to M$ *tale che* $\phi \circ i = f$*:*



La dimostrazione è un facile esercizio: per un elemento $\sigma_1 \cdots \sigma_n$ di Σ^*, è sufficiente porre

$$\phi(\sigma_1 \cdots \sigma_n) = f(\sigma_1) \bullet \cdots \bullet f(\sigma_n)$$

e fare le necessarie verifiche.

Osservazione 2.2.1. Poiché la proprietà universale fornisce una caratterizzazione del monoide libero, essa può essere intesa come la sua definizione astratta. Come già osservato in precedenza, in questo modo possiamo definire l'*oggetto monoide libero* solo a meno di isomorfismi. D'altro canto, questo punto di vista ci permette di declinare la definizione di *oggetto libero* anche in altre categorie.

2.2.3 *Gruppi liberi*

Consideriamo il problema seguente:

> dato un insieme A, costruire un gruppo G che contenga gli elementi di A *nel modo più generale possibile*. Il più piccolo gruppo con tale proprietà verrà denotato $F(A)$.

Certo, detto così, è difficile capire anche solo cosa venga richiesto: cosa vuol dire *nel modo più generale possibile*? Quello che intendiamo è che nessun elemento di A è speciale come elemento di $F(A)$. L'idea è che,

- nessun elemento di A sia l'elemento neutro di $F(A)$,
- nessuna sua potenza dia l'elemento neutro,
- nessun prodotto tra potenze di elementi distinti di A dia l'elemento neutro.

Vediamo qualche esempio che ci aiuterà a formalizzare il problema.

Esempio 2.2.2. Sia $A = \emptyset$. Allora chiaramente $F(A) \cong \mathbf{1} = \{e\}$, il gruppo banale. Infatti, $\emptyset \subseteq \mathbf{1}$ e ogni altro gruppo contiene (una copia isomorfa di) $\mathbf{1}$; pertanto, esso è anche *il più piccolo*.

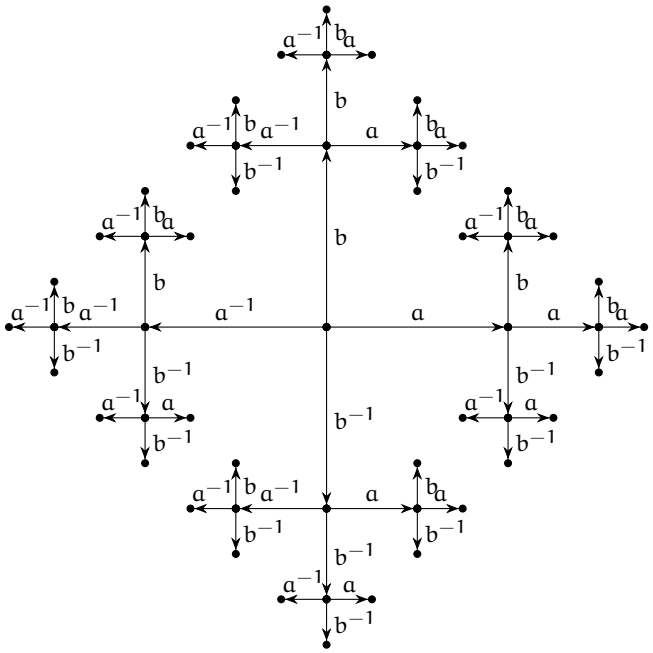
Esempio 2.2.3. Sia ora A un insieme con un solo elemento, ad esempio $A = \{a\}$. Escludiamo $a = 1$, l'identità del gruppo, perché ciò renderebbe l'elemento a speciale, ma abbiamo detto che vogliamo che $F(A)$ contenga a nel modo più generale possibile. Dal fatto che $a \in F(A)$, ed essendo quest'ultimo un gruppo, abbiamo che anche $a^2 \in F(A)$, con $a^2 \neq 1$ perché questo renderebbe a speciale. Analogamente, $1 \neq a^n \in F(A)$, per ogni $n \geqslant 0$. Inoltre, poiché $F(A)$ è un gruppo, anche $a^{-1} \in F(A)$, e ancora $(a^{-1})^n = a^{-n} \in F(A)$. In conclusione, se $F(A)$ contiene a nel modo più generale possibile, allora sicuramente conterrà

$$\{a^n \mid n \in \mathbb{Z}\},$$

Ma questo, che a priori è semplicemente un sottoinsieme di $F(A)$, risulta essere un gruppo, il gruppo ciclico infinito, e quindi per la minimalità di $F(A)$, si ha $F(A) = \langle a \rangle \cong (\mathbb{Z}, +, 0)$.

Esempio 2.2.4. A questo punto, si potrebbe pensare che, se l'insieme A è appena un po' più grande, ad esempio se A è un insieme di due elementi, $F(A)$ risulti essere solo un po' più complicato del caso precedente. In realtà non affatto è così. Consideriamo allora $A = \{a, b\}$; vale tutto il ragionamento precedente, sia per l'elemento a che per b, pertanto questa volta $F(A)$ contiene, come sottogruppi, i gruppi ciclici infiniti $\langle a \rangle$ e $\langle b \rangle$. Tuttavia sicuramente $F(A)$ non è isomorfo al prodotto diretto $\langle a \rangle \times \langle b \rangle$. Infatti, in tale caso sarebbe un gruppo abeliano, da cui avremmo che $ab = ba$, o equivalentemente, $aba^{-1}b^{-1} = 1$, e questo renderebbe a e b elementi speciali.

Per avere una idea di come sia fatto $F(A)$ in questo caso, riportiamo un diagramma che lo descrive fino agli elementi di lunghezza 3:



Qui i segmenti orizzontali rappresentano la moltiplicazione per a (o per a^{-1} a seconda del verso in cui vengono percorsi), quelli verticali

la moltiplicazione per b (o per b^{-1}). L'idea è che $F(A)$ sia costituito da tutte le sequenze finite di caratteri a, b, a^{-1}, b^{-1}, che non contengano sottosequenze del tipo xx^{-1} o $x^{-1}x$, per $x = a, b$. Ovviamente, al legge di composizione deve tenere conto delle possibili semplificazioni. Ad esempio,

$$aba^{-1}bb \cdot b^{-1}b^{-1}ab = ab \not{a}^{-1} \not{b} \not{b} \cdot \not{b}^{-1} \not{b}^{-1} \not{a}b = abb\,,$$

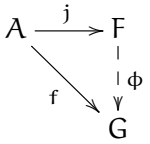
o più semplicemente

$$aba^{-1}b^2 \cdot b^{-2}ab = ab^2\,.$$

Siamo finalmente pronti a formalizzare la definizione generale di gruppo libero. Essa verrà dapprima espressa come un oggetto definito da una certa proprietà universale; successivamente studieremo la costruzione esplicita del gruppo libero su un dato insieme.

Definizione 2.2.5. *Sia A un insieme. Diciamo che la coppia $(F, j\colon A \to F)$, dove F è un gruppo e j è una funzione, è il gruppo libero su A, se soddisfa la seguente proprietà universale:*

> per ogni altra coppia $(G, f\colon A \to G)$, con G gruppo e f funzione, esiste un unico omomorfismo di gruppi $\phi\colon F \to G$ tale che $\phi \circ j = f$:



Il gruppo F viene di solito denotato $F(A)$ per sottolineare la sua dipendenza dall'insieme A. Inoltre, al fine di evidenziare il ruolo di j, si potrà anche dire che:

la coppia (F, j) presenta F come gruppo libero su A.

Esempio 2.2.6. Riprendiamo l'esempio visto sopra con $A = \{a\}$, e verifichiamo la proprietà universale. Considero il gruppo degli interi $\mathbb{Z}$, e la funzione $j\colon \{a\} \to \mathbb{Z}$ definita da $j(a) = 1$.

La coppia $(\mathbb{Z}, j)$ presenta $\mathbb{Z}$ come gruppo libero su $\{a\}$.

Infatti, per ogni altro gruppo G, e per ogni funzione $f\colon \{a\} \to G$, c'è un solo omomorfismo di gruppi $\phi\colon \mathbb{Z} \to G$ che estende f, quella che manda $1 \mapsto f(a)$, e quindi, per ogni $n > 0$, manda

$$n = n \cdot 1 \mapsto f(a)^n \qquad -n = n \cdot (-1) \mapsto (f(a)^{-1})^n = f(a)^{-n}$$

2.2.4 *Costruzione di* $F(A)$

Fissato l'insieme A, denotiamo con $W(A)$ il monoide libero $(A \amalg A)^*$ (vedi Sezione 2.2.2), dove interpretiamo l'unione disgiunta $A \amalg A$ come l'unione dell'insieme $A = \{a_1, a_2, \dots, a_i, \dots\}$ con l'insieme degli *inversi formali degli elementi di A*, ossia $\{a_1^{-1}, a_2^{-1}, \dots, a_i^{-1}, \dots\}$. Chiameremo *parole* gli elementi di $W(A)$. Definiamo la funzione $\ell\colon W(A) \to \mathbb{N}$, che restituisce la lunghezza di una parola; poniamo $\ell(\epsilon) = 0$.

Attenzione: inversi formali significa che non si comportano come inversi per l'operazione di monoide. Ad esempio, se $a, b \in A$, si ha che $abb^{-1} \neq a$ in $W(A)$, perché $bb^{-1} \neq \epsilon$, l'elemento neutro del monoide.

Per ottenere un gruppo dal monoide $W(A)$ dovremmo quindi introdurre delle *regole di riduzione* che permettano di semplificare espressioni come quella scritta sopra. A questo fine, introduciamo la funzione *riduzione elementare*

$$r\colon W(A) \to W(A)\,,$$

che data una parola $w \in W(A)$, cerca la prima occorrenza della sottosequenza xx^{-1} o di $x^{-1}x$, e se la trova, la rimuove. Ad esempio si ha

$$r(aaa^{-1}bb^{-1}c) = abb^{-1}c\,.$$

Diciamo che la parola $w \in W(A)$ è una *parola ridotta* se $r(w) = w$, ossia se applicando a w la riduzione elementare si ottiene ancora w. Vale il seguente risultato.

Lemma 2.2.7. *Se $w \in W(A)$ ha lunghezza $\ell(w) = n$, allora $r^{\lfloor n/2 \rfloor}(w)$ è una parola ridotta.*

Dimostrazione. Ad ogni iterazione di r ho due possibilità, o $\ell(r(w)) = \ell(w) - 2$, oppure $\ell(r(w)) = \ell(w)$. Di conseguenza, l'applicazione di r può effettivamente ridurre la lunghezza della parola al più $\lfloor n/2 \rfloor$ volte. □

Confortati dal lemma appena dimostrato, definiamo la funzione *riduzione*

$$R\colon W(A) \to W(A)$$

mediante la posizione $R(w) = r^{\lfloor n/2 \rfloor}(w)$ con $n = \ell(w)$, e finalmente definiamo

$$F(A) = R(W(A))\,.$$

Proposizione 2.2.8. *L'insieme delle parole ridotte $F(A)$ è un gruppo; per $w, w' \in F(A)$, la legge di composizione è data da*

$$w \cdot w' = R(ww')\,,$$

l'elemento neutro è $\epsilon \in F(A)$, l'inverso di una parola $w = a_1^{\sigma_1} \cdots a_k^{\sigma_k}$, con $a_i \in A$ e $\sigma_i \in \{+1, -1\}$, è la parola $w^{-1} = a_k^{-\sigma_k} \cdots a_1^{-\sigma_1}$.

Dimostrazione. La parola vuota ϵ è chiaramente elemento neutro, poiché se w è una parola ridotta, lo sono anche $w\epsilon = w = \epsilon w$. Inoltre, segue immediatamente dalla definizione che $R(ww^{-1}) = \epsilon = R(w^{-1}w)$. L'unica difficoltà è allora verificare che l'operazione così definita sia associativa, ossia che, per $w, w', w'' \in F(A)$, si abbia:

$$R(wR(w'w'')) = R(R(ww')w'') .$$

Una dimostrazione di questo fatto si può ottenere studiando i diversi modi di operare le cancellazioni su una generica parola di $W(A)$. Questo porta a una meticolosa (e tediosa) analisi dei casi possibili.

Una dimostrazione più elegante è dovuta a Van der Waerden [**?**]. Si procede costruendo una funzione iniettiva $\phi\colon F(A) \to \mathsf{Sym}(A)$ tale che $\phi(w \cdot w') = \phi(w) \circ \phi(w')$. In questo modo, l'associatività dell'operazione in $F(A)$ viene riflessa dall'associatività della composizione in $\mathsf{Sym}(A)$. □

Notazione 2.2.9. *Poiché scriviamo gli elementi del gruppo libero come sequenze di caratteri (parole), di solito seguiremo la convenzione di omettere il segno di* moltiplicazione *per indicare l'operazione di gruppo. Tuttavia, nel caso ci sia il rischio di ambiguità (ad esempio perché si ha a che fare con diversi gruppi con diverse operazioni), ricorreremo al segno ; per indicare l'operazione del gruppo libero. Così, se $w_1, w_2 \in F(A)$ scriveremo*

$$w_1; w_2$$

per il loro prodotto in $F(A)$. In questo caso, anche la singola parola, in quanto concatenazione di caratteri, potrà essere scritta nella forma

$$w = a_1^{\alpha_1}; \cdots ; a_k^{\alpha_k} .$$

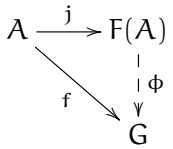
Sia ora j la funzione $A \to F(A)$ che associa a ogni elemento $a \in A$, l'elemento a stesso, considerato però come una parola di lunghezza 1. Vale la seguente proposizione.

Proposizione 2.2.10. *La coppia $(F(A), j\colon A \to F(A))$ soddisfa la proprietà universale del gruppo libero.*

Dimostrazione. Dato un gruppo $G = (G, *, 1)$, consideriamo una funzione $f\colon A \to G$. Sia $w = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ una parola ridotta di $F(A)$; definiamo:

$$\phi(w) = \phi(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) = f(a_1)^{\alpha_1} * \cdots * f(a_n)^{\alpha_n} .$$

Chiaramente si ha $\phi \circ j = f$:



Si noti che ϕ è in realtà definito su tutto $W(A)$, e che commuta con la riduzione, nel senso che vale $\phi \circ R = \phi$. Allora ϕ è un omomorfismo di gruppi. Infatti, per $w, w' \in F(A)$, si ha:

$$\phi(w \cdot w') = \phi(R(ww')) = \phi(ww') = \phi(w) * \phi(w')\,.$$

Per quanto riguarda l'unicità, supponiamo sia dato un omomorfismo ψ tale che $\psi \circ j = f$. Possiamo calcolare

$$\begin{aligned}
\psi(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) &= (\psi(a_1))^{\alpha_1} \cdots (\psi(a_n))^{\alpha_n} \\
&= (\psi(j(a_1)))^{\alpha_1} \cdots (\psi(j(a_n)))^{\alpha_n} \\
&= (f(a_1))^{\alpha_1} \cdots (f(a_n))^{\alpha_n} \\
&= (\phi(j(a_1)))^{\alpha_1} \cdots (\phi(j(a_n)))^{\alpha_n} \\
&= \phi(a_1^{\alpha_1} \cdots a_n^{\alpha_n})
\end{aligned}$$

per cui $\psi = \phi$, e l'unicità è dimostrata. □

Nella costruzione esplicita del gruppo libero, abbiamo visto che la funzione $j \to F(A)$ è iniettiva. In realtà, con abuso di linguaggio, essa è considerata spesso un'inclusione insiemistica, a patto di identificare i *caratteri* (elementi di A) con le parole di lunghezza 1 (elementi di $F(A)$). In realtà, l'iniettività di j non dipende da come abbiamo costruito $F(X)$, ma esclusivamente dalla sua proprietà universale.

Lemma 2.2.11. *Se la coppia* $(F, j\colon A \to F)$ *soddisfa la proprietà universale del gruppo libero,* j *è iniettiva.*

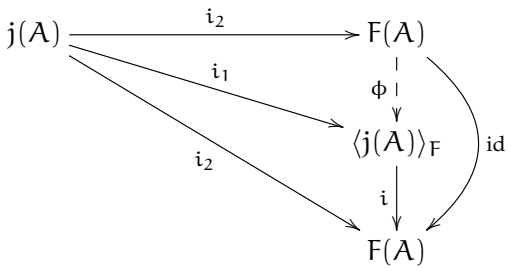
Dimostrazione. Se $|A| < 2$ è ovvio. Sia allora $|A| \geqslant 2$, e siano $a_1 \neq a_2 \in A$. Definisco la funzione $f\colon A \to \mathbb{Z}_2$, con $f(x) = 1$ se e solo se $x = a_1$. Per la proprietà universale del gruppo libero, esiste un'unico omomorfismo $\phi\colon F \to \mathbb{Z}_2$ che estende f. Allora si ha che $f(a_1) \neq f(a_2)$, ovvero $\phi(j(a_1)) \neq \phi(j(a_2))$, e dunque $j(a_1) \neq j(a_2)$. □

Dal lemma precedente si ha che $A \cong j(A)$, ed è facile dedurre che la coppia $(F, j(A) \hookrightarrow F)$ presenta F come gruppo libero su $j(A)$, sicché l'abuso di linguaggio a cui si faceva riferimento sopra è pienamente giustificato.

Concludiamo mostrando che $j(A)$ genera F *internamente*, ovvero che F coincide con il sottogruppo $\langle j(A)\rangle_F$ generato dall'insieme $j(A)$. A questo scopo, consideriamo le inclusioni:

$$i_1\colon j(A) \to \langle j(A)\rangle_F\,, \qquad i_2\colon j(A) \to F(A)\,, \qquad i\colon \langle j(A)\rangle_F \to F(A)\,.$$

e osserviamo che $i \circ i_1 = i_2$. Questa equazione è rappresentata dalla commutatività del triangolo in basso nel diagramma seguente:



Ora, poiché i_2 presenta $F(A)$ come gruppo libero su $j(A)$, esiste un unico omomorfismo ϕ tale che $\phi \circ i_2 = i_1$, equazione rappresentata dal triangolo in alto. Mettiamo insieme queste informazioni e calcoliamo:

$$(i \circ \phi) \circ i_2 = i \circ (\phi \circ i_2) = i \circ i_1 = i_2 \,,$$

ma anche:

$$\mathrm{id} \circ i_2 = i_2 \,.$$

Quindi, per l'unicità prevista dalla proprietà universale, deve essere $i \circ \phi = \mathrm{id}$, ed essendo i un'inclusione, essa deve necessariamente essere l'identità. Concludiamo $\langle j(A)\rangle_F = F(A)$.

Confortati dalla discussione svolta qui sopra, d'ora in poi, identificheremo anche senza esplicitarlo $j(A)$ con A.

Le prossime due proposizioni prendono in esame alcune proprietà analoghe a quelle che caratterizzano la base di uno spazio vettoriale. La prima fornisce un criterio molto utile nelle applicazioni, per stabilire se un gruppo è generato liberamente da un suo sottoinsieme. La seconda mostra che la cardinalità dell'insieme dei generatori di un gruppo libero è un invariante per isomorfismi. Possiamo considerarle delle nozioni analoghe a quelle di indipendenza lineare di un sistema di generatori e di dimensione di uno spazio vettoriale.

Proposizione 2.2.12. *Sia* $(G, *, 1)$ *un gruppo, e* $A \subseteq G$ *un sottoinsieme. Allora* G *è libero su* A *se e solo se ogni elemento* $1 \neq g \in G$ *può essere scritto in uno, e in un solo modo, nella forma:*

$$g = a_1^{\alpha_1} * \cdots * a_k^{\alpha_k} \,, \tag{6}$$

dove $k \geqslant 1$, $a_i \in A$, $\alpha_i \neq 0$ *intero* $(i = 1, \ldots, k)$ *e* $a_i \neq a_{i+1}$ *se* $i < k$.

Questa scrittura è detta *forma normale* di g, relativamente a A.

Dimostrazione. È sufficiente mostrare che l'unico omomorfismo $\phi\colon F(A) \to G$ tale che $\phi(a) = a$ per ogni $a \in A$ è un isomorfismo. Esso è suriettivo, perché, come abbiamo appena visto, A genera $F(A)$. Inoltre è iniettivo, perché altrimenti avremmo un elemento (non banale) $a_1^{\alpha_1} \cdots a_n^{\alpha_n} \in F(X)$ tale che

$$\phi(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) = a_1^{\alpha_1} * \cdots * a_n^{\alpha_n} = 1 \,,$$

e quindi, ad esempio, a_1 e $a_1^{\alpha_1+1} * \cdots * a_n^{\alpha_n}$ sarebbero due scritture distinte nella forma (6) dello stesso elemento non banale di G. □

Proposizione 2.2.13. *Siano A e B due insiemi. Si ha che* $|A| = |B|$ *se e solo se* $F(A) \cong F(B)$.

Dimostrazione. La dimostrazione dell'implicazione diretta è una facile applicazione della proprietà universale, che lasciamo come esercizio.

Per dimostrare l'implicazione inversa, consideriamo gli insiemi

$$V = \mathrm{Hom}_{\mathsf{Gp}}(F(A), \mathbb{Z}_2)\,, \qquad W = \mathrm{Hom}_{\mathsf{Gp}}(F(B), \mathbb{Z}_2)\,.$$

Ciascuno di essi supporta evidentemente una struttura di spazio vettoriale su $\mathbb{Z}_2$, con basi A e B rispettivamente. Sia ora $f\colon F(A) \to F(B)$ un isomorfismo di gruppi. Esso si estende naturalmente a un isomorfismo lineare $V \cong W$. Quindi, essendo V e W spazi vettoriali isomorfi, le loro basi avranno la stessa cardinalità. □

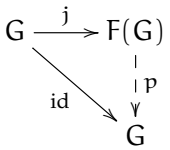
2.2.5 *Presentazioni di gruppi*

Per introdurre la nozione di gruppo libero, abbiamo considerato il caso degli spazi vettoriali di dimensione finita. Un limite di questa analogia è che, mentre in quel caso è sempre possibile trovare un sottoinsieme di vettori che genera liberamente lo spazio, nel caso dei gruppi non sempre è possibile trovare un sottoinsieme che generi liberamente un dato gruppo: essere libero è una proprietà di cui godono solo certi gruppi. D'altro canto, come vedremo in questa sezione, ogni gruppo può essere *presentato* come quoziente di un gruppo libero su un opportuno insieme di generatori.

Cominciamo con un risultato preliminare.

Proposizione 2.2.14. *Ogni gruppo è isomorfo al quoziente di un gruppo libero*

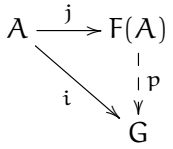
Dimostrazione. Dato un gruppo G, consideriamo il suo insieme supporto (che indichiamo sempre con G) e il gruppo libero $F(G)$ su tale insieme. Esso è costruito a partire dagli elementi di G che hanno però *dimenticato* di essere elementi di G. Gli elementi di $F(G)$ sono pertanto sequenze di elementi di G e loro inversi formali. Consideriamo ora il diagramma



dove j è l'inclusione di G in $F(G)$. Per la proprietà universale del gruppo libero, esiste un unico omomorfismo di gruppi $p\colon F(A) \to G$ che fa commutare il triangolo. Quindi p, vista come funzione, è una retrazione, e come tale, è suriettiva. Di conseguenza, poiché p è un omomorfismo di gruppi, per il teorema fondamentale di omomorfismo, si ha che $G \cong F(G)/\mathrm{Ker}(p)$. □

L'omomorfismo p è di un certo interesse. Infatti, se, come abbiamo detto, gli elementi di $F(G)$ sono sequenze di elementi di G e di loro inversi formali, p risulta essere la funzione che *interpreta* tali sequenze utilizzando proprio la moltiplicazione e gli inversi forniti dalla struttura di gruppo di G.

A dispetto della sua semplicità, la dimostrazione non ci fornisce in generale un modo efficiente per descrivere G come quoziente di un gruppo libero. Cerchiamo di illustrare questo punto. Sia dato un *sistema di generatori* A di G, ossia un sottoinsieme $A \subseteq G$ tale che $\langle A \rangle_G = G$ (abbiamo messo G a pedice della parentesi acuta per enfatizzare il fatto che A genera G internamente, i.e. come sottogruppo di G). Possiamo considerare il diagramma seguente:



dove i è l'inclusione di A in G. Ancora, p risulta essere definita come sopra, ed è suriettiva, poiché la sua immagine contiene A. È chiaro allora che, tanto più A è *piccolo*, quanto più la descrizione di G come quoziente di un gruppo libero potrà essere semplice.

Una volta che si sia fissato un sistema minimale A di generatori, poiché $G \cong F(A)/\mathrm{Ker}(p)$, e poiché $F(A)$ è noto, l'interesse si sposta la descrizione di $\mathrm{Ker}(p)$, o equivalentemente, sulla descrizione dei sottogruppi normali di dei gruppi liberi. Una trattazione approfondita di questo argomento esula dagli scopi di queste note. Tuttavia, non possiamo non citare un importante risultato, conosciuto come *Teorema di Nielsen-Schreier*. Esso afferma che ogni sottogruppo di un gruppo libero $F(A)$ è a sua volta libero, nel senso che è generato internamente, ma liberamente, da un sottoinsieme di elementi di $F(A)$.

Definizione 2.2.15 (Chiusura normale)**.** *Sia G un gruppo, e $R \subseteq G$ un suo sottoinsieme. La chiusura normale di R in G è il più piccolo sottogruppo normale di G che contiene R come sottoinsieme. Più precisamente, è un sottogruppo normale $N_R \trianglelefteq G$ tale che, se esiste H normale in G con $R \subseteq H$, allora $N_R \leqslant H$.*

La seguente caratterizzazione fornisce un'utile descrizione della chiusura normale.

Proposizione 2.2.16. *Sia G un gruppo e R un sottoinsieme di G. Le seguenti affermazioni sono equivalenti per un sottogruppo di G:*

1. *esso è la chiusura normale di R in G;*

2. *esso è l'intersezione di tutti i sottogruppi normali che contengono R;*

3. *esso è il sottogruppo di* G *generato da tutti gli elementi della forma*

$$grg^{-1},$$

dove $r \in R$ *e* $g \in G$.

Dimostrazione. $1 \Rightarrow 2$. Consideriamo l'intersezione

$$M = \bigcap_{R \subseteq H \trianglelefteq G} H$$

di tutti i sottogruppi normali che contengono R. È sufficiente mostrare che M è un sottogruppo normale di G; ma questo è ovvio, poiché per $g \in G$ e $x, y \in M$, si ha $xy^{-1} \in H$ e $gxg^{-1} \in H$ per ogni H normale in G contenente R, e sia M definito come sopra.

$2 \Rightarrow 3$. Sia

$$K = \langle grg^{-1} \mid g \in G, r \in R \rangle_G$$

il sottogruppo di G generato dai coniugati degli elementi di R, e sia M definito come sopra. Ovviamente, $K \subseteq M$, poiché i generatori di K sono elementi di M. D'altro canto, dati $g \in G$ e $g_1 r_1 g_1^{-1} g_2 r_2 g_2^{-1} \cdots g_k r_k g_k^{-1} \in K$, si ha

$$g(g_1 r_1 g_1^{-1} g_2 r_2 g_2^{-1} \cdots g_k r_k g_k^{-1}) g^{-1} =$$

$$= (gg_1 r_1 g_1^{-1} g^{-1})(gg_2 r_2 g_2^{-1} g^{-1}) \cdots (gg_k r_k g_k^{-1} g^{-1}) \in K.$$

Quindi, K è normale in G e, poiché contiene R per definizione, si ha $M \subseteq K$.

$3 \Rightarrow 1$. Sia H un sottogruppo normale di G, con $R \subseteq H$. È immediato verificare che $K \leqslant H$, dove K è definito come sopra. Per l'arbitrarietà di H, concludiamo che K è la chiusura normale di R. □

Definizione 2.2.17. *Una presentazione di un gruppo* G *è data da un insieme* A *di* generatori*, un insieme* $R \subseteq F(A)$ *di* relazioni*, e un isomorfismo* $G \cong \frac{F(A)}{N_R}$*, dove* N_R *è la chiusura normale di* R *in* $F(X)$.

Utilizzeremo la notazione $G \cong \langle A \mid R \rangle$ per riferirci al gruppo G presentato dall'insieme di generatori A, con relazioni R. Se possibile si ometteranno le parentesi non strettamente necessarie. Così, ad esempio. piuttosto che $\langle \{a_1, a_2, \ldots\} | \{r_1, r_2, \ldots\} \rangle$, si scriverà: $\langle a_1, a_2, \ldots \mid r_1, r_2 \ldots \rangle$. Analogamente, gli elementi del gruppo quoziente $\frac{F(A)}{N_R}$ verranno denotati $[w]_R$, o semplicemente w, con $w \in F(A)$.

La Proposizione 2.2.14 può essere così riformulata:

Corollario 2.2.18. *Ogni gruppo ammette una presentazione.*

Riportiamo degli esempi di presentazioni di gruppi, alcuni senza dimostrazione.

Esempio 2.2.19. Dato un insieme A, si ha che il gruppo libero su A ammette presentazione

$$F(A) \cong \langle A \,|\, \emptyset \rangle .$$

Infatti, la chiusura normale dell'insieme vuoto è il sottogruppo banale. In particolare avremo:

$$F(a, b) \cong \langle a, b \,|\, \emptyset \rangle = \langle a, b \rangle .$$

Esempio 2.2.20 (Gruppi ciclici). Come abbiamo già osservato, il gruppo libero su un solo generatore è isomorfo al gruppo ciclico infinito, ovvero al gruppo $\mathbb{Z}$ dei numeri interi, in notazione additiva. E' facile provare che gruppo ciclico C_n di ordine n, ovvero il gruppo $\mathbb{Z}_m$ delle classi di resto modulo m, in notazione additiva, ammette presentazione:

$$C_n \cong \langle c \,|\, c^n \rangle$$

Esempio 2.2.21. Il prodotto diretto $\mathbb{Z} \times \mathbb{Z}$ può essere presentato come segue:

$$\mathbb{Z} \times \mathbb{Z} \cong \langle a, b \,|\, aba^{-1}b^{-1} \rangle .$$

Il prodotto diretto $\mathbb{Z}_n \times \mathbb{Z}_m$ può essere presentato come segue:

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \langle a, b \,|\, a^n, b^m, aba^{-1}b^{-1} \rangle .$$

Notazione 2.2.22. *Talvolta le relazioni vengono scritte sotto forma di equazioni. Ad esempio, con riferimento agli esempi precedenti, si potrà anche scrivere:*

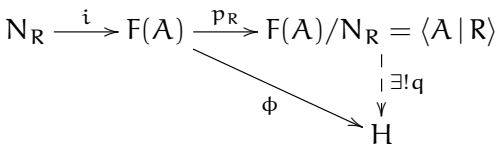
$$C_n \cong \langle c \,|\, c^n = 1 \rangle ,$$

$$\mathbb{Z} \times \mathbb{Z} \cong \langle a, b \,|\, ab = ba \rangle ,$$

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \langle a, b \,|\, a^n = 1, b^m = 1, ab = ba \rangle .$$

Proposizione 2.2.23 (Proprietà universale delle presentazioni di gruppi)**.** *Dato il gruppo* $\langle A \,|\, R \rangle = \frac{F(A)}{N_R}$*, e data una funzione* $f \colon A \to H$ *tale che, per ogni* $b_1^{\beta_1} \cdots b_m^{\beta_m} \in R$ *si abbia* $f(b_1)^{\beta_1} \cdots f(b_m)^{\beta_m} = 1$*, allora esiste un unico omomorfismo* $q \colon \langle A \,|\, R \rangle \to H$ *tale che* $q(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) = f(a_1)^{\alpha_1} \cdots f(a_n)^{\alpha_n}$.

Dimostrazione. Sia $\phi \colon F(A) \to H$ l'unico omomorfismo che ristretto a A dia f (dato dalla proprietà universale del gruppo libero). Si consideri il diagramma seguente:



Vogliamo dimostrare che $\phi \circ i = \omega_{N_R,H}$, ovvero l'omomorfismo banale. In effetti, è sufficiente verificarlo sui generatori di N_R. Sia $w \in R$ e $g \in F(A)$, si ha:

$$\phi(gwg^{-1}) = \phi(g) \cdot \phi(w) \cdot \phi(g^{-1}) = \phi(g) \cdot 1 \cdot \phi(g)^{-1} = \phi(g) \cdot \phi(g)^{-1} = 1\,.$$

Quindi, per la proprietà universale del quoziente, esiste un unico omomorfismo di gruppi $q\colon F(A)/N_R \to H$ tale che $q \circ p_R = \phi$, e dunque

$$\begin{aligned} q(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) &= q \circ p_R(a_1^{\alpha_1}; \cdots ; a_n^{\alpha_n}) \\ &= q\big(p_R(a_1^{\alpha_1}; \cdots ; a_n^{\alpha_n})\big) \\ &= \phi(a_1^{\alpha_1}; \cdots ; a_n^{\alpha_n}) \\ &= f(a_1)^{\alpha_1} \cdots f(a_n)^{\alpha_n} \end{aligned}$$

□

Corollario 2.2.24 (Teorema di von Dyck)**.** *Sia H un gruppo e $A \subseteq H$ un insieme di generatori di H, e supponiamo che $R \subseteq F(A)$ sia un insieme di relazioni soddisfatte dagli elementi di A, cioè tale che $w = 1$ in H, per ogni $w \in R$. Allora esiste un omomorfismo suriettivo $q\colon \langle A \,|\, R\rangle \to H$ tale che $q(a) = a$, per ogni $a \in A$.*

Dimostrazione. Per la proprietà universale del gruppo libero, esiste un unico omomorfismo $p\colon F(A) \to H$ che, ristretto a A, dia l'inclusione di A in H. Si può applicare allora la proposizione precedente ed ottenere l'unico omomorfismo di gruppi $q\colon F(A)/N_R \to H$ tale che $q \circ p_R = p$; pertanto, per $a \in A$, si ha $q([a]_R) = q(p_R(a)) = p(a) = a$. La dimostrazione si conclude osservando che l'omomorfismo p è suriettivo perché A genera H (vedi Proposizione 2.2.14), e quindi necessariamente anche q è suriettivo. □

Nell'applicare il Teorema di von Dyck, si considera spesso un insieme di generatori $A' \subseteq H$ in biezione con l'insieme A, piuttosto che A stesso. Il prossimo esempio chiarisce questo punto.

Esempio 2.2.25 (Gruppo simmetrico S_3). Il gruppo simmetrico su tre oggetti ha presentazione

$$S_3 \cong \langle x, y \,|\, x^2, y^3, xyxy\rangle\,.$$

Dimostrazione. Poniamo $A = \{x, y\}$ e $R = \{x^2, y^3, xyxy\}$. Il gruppo S_3 è generato, ad esempio, dall'insieme $A' = \{(13), (123)\}$. Gli insiemi A e A' possono essere messi in corrispondenza biunivoca identificando x con (13) e y con (123). Si verifica immediatamente che i generatori di S_3 verificano le relazioni di R:

$$\begin{aligned} x^2 &\leftrightarrow (13)^2 = \mathrm{id}\,, \\ y^3 &\leftrightarrow (123)^3 = \mathrm{id}\,, \\ xyxy &\leftrightarrow (13)(123)(13)(123) = \mathrm{id}\,. \end{aligned}$$

Pertanto, per il Teorema di von Dyck, l'assegnamento

$$x \mapsto (13) \qquad y \mapsto (123)$$

si estende a un omomorfismo suriettivo $q\colon \langle x, y \,|\, x^2, y^3, xyxy\rangle \to S_3$. Vogliamo dimostrare che tale isomorfismo è anche iniettivo. A questo scopo, notiamo che le tre relazioni ci forniscono la regola di riscrittura $yx = xy^2$, e quindi possiamo trasformare ogni parola di $\langle x, y \,|\, x^2, y^3, xyxy\rangle$, in una del tipo $x^\alpha y^\beta$, dove $\alpha = 0, 1$ e $\beta = 0, 1, 2$. Quindi, $\langle x, y \,|\, x^2, y^3, xyxy\rangle$ ha al più 6 elementi. Ora, poiché p e suriettiva su S_3 che ha ordine 6, questo implica che il dominio di q abbia almeno 6 elementi, e quindi ne ha esattamente 6, e q è un isomorfismo. □

La dimostrazione del prossimo esempio si ottiene in modo analogo quella che abbiamo appena visto, pertanto essa viene lasciata come esercizio.

Esempio 2.2.26 (Gruppi diedrali). Una presentazione standard per il diedrale di ordine n è data qui sotto:

$$D_n = \langle \rho, \sigma \,|\, \rho^n, \sigma^2, \rho\sigma\rho\sigma\rangle\,.$$

Le presentazioni di un gruppo, in generale, non sono uniche, né il numero di generatori è univocamente determinato. Vediamo due esempi.

Esempio 2.2.27. Si ha la seguente presentazione alternativa del gruppo degli interi:

$$\mathbb{Z} \cong \langle a, b \,|\, ab^{-1}\rangle\,.$$

Dimostrazione. Da $ab^{-1} = 1$ si ottiene immediatamente la regola di riscrittura $a = b$. Mediante questa, il generico elemento di $\langle a, b \,|\, ab^{-1}\rangle$, ovvero $a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_k} b^{\beta_k}$, si può riscrivere come $a^{\alpha_1+\beta_1\cdots\alpha_k+\beta_k}$. Pertanto, $\langle a, b \,|\, ab^{-1}\rangle \cong \langle a\rangle \cong \mathbb{Z}$. □

Esempio 2.2.28. Si ha la seguente presentazione alternativa del gruppo diedrale di ordine $2n$:

$$D_n \cong \langle x, y \,|\, x^2, y^2, (xy)^n\rangle\,.$$

Dimostrazione. La dimostrazione si ottiene applicando più volte la proprietà universale delle presentazioni di gruppi. Per evitare di far confusione tra le due presentazioni, poniamo:

$$G = \langle \rho, \sigma \,|\, \rho^n, \sigma^2, \rho\sigma\rho\sigma\rangle\,, \qquad H = \langle x, y \,|\, x^2, y^2, (xy)^n\rangle\,.$$

Sia $p\colon F(x, y) \to H$ l'omomorfismo tale che $p(x) = \sigma$ e $p(y) = \sigma\rho$. Si ha che le immagini di x e y soddisfano le relazioni di H:

$$\begin{aligned} \big(p(x)\big)^2 &= \sigma^2 = 1\,, \\ \big(p(y)\,,\big)^2 &= (\sigma\rho)^2 = \sigma\rho\sigma\rho = \sigma(\rho\sigma)\sigma = 1 \\ \big(p(x)p(y)\big)^n &= (\sigma\sigma\rho)^n = \rho^n = 1\,. \end{aligned}$$

Pertanto p passa al quoziente, i.e. esiste un unico omomorfismo $q\colon G \to H$ tale che $q(x) = \sigma$ e $q(y) = \sigma\rho$.

Sia ora $p'\colon F(\rho,\sigma) \to G$ l'omomorfismo tale che $p'(\rho) = xy$ e $p'(\sigma) = x$. Si ha che le immagini di ρ e σ soddisfano le relazioni G:

$$\begin{aligned} \big(p'(\rho)\big)^n = (xy)^n = 1\,, \\ \big(p'(\sigma)\big)^2 = x^2 = 1\,, \\ p'(\rho)p'(\sigma)p'(\rho)p'(\sigma) = xyxxyx = 1\,. \end{aligned}$$

Pertanto p' passa al quoziente, i.e. esiste un unico omomorfismo $q'\colon H \to G$ tale che $q'(\rho) = xy$ e $q'(\sigma) = x$.

A questo punto è sufficiente verificare che q e q' sono due isomorfismi, l'uno inverso dell'altro. A questo scopo, è sufficiente verificare che le composizioni $q \circ q'$ e $q' \circ q$ diano l'identità sui generatori. In effetti si ha:

$$\begin{aligned} q(q'(\rho)) &= q(xy) = q(x)q(y) = \sigma\sigma\rho = \rho\,, \\ q(q'(\sigma)) &= q(x) = \sigma\,, \\ q'(q(x)) &= q'(\sigma) = x\,, \\ q'(q(y)) &= q'(\sigma\rho) = q'(\sigma)q'(\rho) = xxy = y\,. \end{aligned}$$

□

2.2.6 *Prodotto libero (coprodotto) di gruppi*

La discussione sin qui svolta, su gruppi liberi e presentazioni, ci fornisce tutti gli ingredienti per trattare la nozione di *prodotto libero* di due gruppi. Più precisamente, chiameremo così la costruzione esplicita di quello che altro non è che il coprodotto nella categoria dei gruppi. Vediamo come la sua definizione emerga naturalmente.

Seguendo la Definizione 1.2.26, dati due gruppi G e H, il loro coprodotto (se esiste) è una tripla universale:

$$G \xrightarrow{\iota_1} G * H \xleftarrow{\iota_2} H\,.$$

Possiamo pensare che, per ogni $g \in G$, l'elemento $\bar{g} = \iota_1(g)$ appartenga a $G * H$; analogamente, per ogni $h \in H$, anche l'elemento $\bar{\bar{h}} = \iota_2(h)$ apparterrà a $G * H$. Prendiamo allora come generatori di $G * H$ l'insieme dei simboli

$$X = \{\bar{g}, \bar{\bar{h}} \mid g \in G, h \in H\}\,.$$

Resta da capire quali relazioni dobbiamo imporre su questi simboli. Per prima cosa, dobbiamo garantire che ι_1 e ι_2 siano omomorfismi. Per questo sarà necessario imporre le relazioni R:

$$\begin{aligned} \overline{g_1 \cdot g_2} &= \bar{g}_1 \cdot \bar{g}_2\,, && \text{per ogni } g_1, g_2 \in G \\ \overline{\overline{h_1 \cdot h_2}} &= \bar{\bar{h}}_1 \cdot \bar{\bar{h}}_2\,. && \text{per ogni } h_1, b_h \in H \end{aligned}$$

È immediato verificare che il gruppo definito come

$$G * H = \langle X \mid R \rangle$$

insieme a ι_1 e ι_2 soddisfi la proprietà universale del coprodotto.

Esercizio 2.2.29. Dimostrare quanto si è appena affermato.

Esercizio 2.2.30. Siano dati i gruppi con presentazioni:

$$G = \langle X \mid R \rangle \qquad H = \langle Y \mid S \rangle$$

Verificare che

$$\langle X \amalg Y \mid R \amalg S \rangle$$

con

$$\iota_1 : x \mapsto \bar{x} \qquad \iota_2 : y \mapsto \bar{y}$$

è il coprodotto di G e H (si ricordi che il simbolo $\amalg$ denota l'unione disgiunta di insiemi, vedi Esempio 1.2.27).

Esempio 2.2.31. Siano

$$G = \mathbb{Z}_5 = \langle x \mid x^5 \rangle \qquad H = \mathbb{Z}_6 = \langle x \mid x^6 \rangle .$$

Il loro prodotto libero può essere presentato come

$$\mathbb{Z}_5 * \mathbb{Z}_6 = \langle x, y \mid x^5, y^6 \rangle .$$

Si noti come si sia provveduto a cambiare il nome della variabile nel gruppo H (y al posto di x) nel rappresentare l'unione disgiunta $\{x\} \amalg \{x\}$. Infatti, se avessimo scritto $\langle x \mid x^5, x^6 \rangle$, avremmo ottenuto il gruppo banale, poiché da $x^5 = 1 = x^6$ si ottiene immediatamente $x = 1$.

2.3 AZIONI DI GRUPPI SU INSIEMI

Groups really shine when you let them act on something.
Paolo Aluffi.

2.3.1 *La categoria* G-Set

In questa sezione introduciamo la categoria dei G-insiemi.

Definizione 2.3.1. *Dato un gruppo* G*, un* G*-insieme* (X, φ) *è un omomorfismo*

$$G \xrightarrow{\varphi} \mathsf{Sym}(X) \tag{7}$$

dove $\mathsf{Sym}(X)$ *è il gruppo simmetrico delle permutazioni dell'insieme* X*. Dato* $g \in G$*, indichiamo con* φ_g *la permutazione ad esso associata.*

Un G-insieme è quindi sostanzialmente una *rappresentazione* di G nella categoria degli insiemi. Tuttavia, i G-insiemi nascono nella forma di gruppi che operano su insiemi, come chiarisce la seguente proposizione.

Proposizione 2.3.2. *Dare un* G*-insieme* (X, φ) *equivale a dare una funzione*

$$G \times X \xrightarrow{*} X \tag{8}$$

che soddisfi i seguenti assiomi:

i. $1_G * x = x$*, per ogni* $x \in X$*;*

ii. $g_1 * (g_2 * x) = (g_1 g_2) * x$*, per ogni* $g_1, g_2 \in G$ *e* $x \in X$*.*

Dimostrazione (traccia). Dato il G-insieme (X, φ), l'operazione è definita dalla posizione $g * x = \varphi_g(x)$. Data l'operazione $*$ come in (8), l'omomorfismo φ_* ad essa associato determina per il generico $g \in G$ la permutazione

$$g * - \colon x \mapsto g * x\,.$$

La dimostrazione si conclude verificando che gli assegnamenti descritti sopra sono uno l'inverso dell'altro. □

La proposizione precedente ci suggerisce di chiamare l'operazione $*$ *azione (sinistra) di* G *su* X. Nel seguito, le espressioni *azione di* G e G*-insieme* saranno considerate come sinonimi, e le notazioni (X, φ) e $(X, *)$ intercambiabili.

Esempio 2.3.3. Sia $S_n = \mathrm{Sym}(\underline{n})$ il gruppo delle permutazioni dell'insieme

$$\underline{n} = \{1, 2, \ldots, n\}\,.$$

È definita una azione canonica di S_n su $\underline{n}$ data dalla posizione

$$\sigma * k = \sigma(k)$$

per $\sigma \in S_n$ e $k \in \underline{n}$.

Esempio 2.3.4. Azione di traslazione (o di moltiplicazione) sinistra. Sia G un gruppo. Una azione di G sull'insieme degli elementi di G

$$G \times G \longrightarrow G$$

è data dalla posizione $g * x = gx$, con $g \in G$ e $x \in G$.

Esempio 2.3.5. Azione di coniugio. Sia G un gruppo. Una azione sinistra di G sull'insieme degli elementi di G

$$G \times G \longrightarrow G$$

è data dalla posizione $g * x = gxg^{-1}$, con $g \in G$ e $x \in G$.

Osserviamo che nei due esempi precedenti, abbiamo azioni di G su G. Il *primo* G è il gruppo che agisce, il *secondo* G è invece considerato come un semplice insieme. Esso è in effetti *l'insieme soggiacente* il gruppo G.

Esempio 2.3.6. Azione di traslazione sui sottoinsiemi. Sia G un gruppo, e sia $X = 2^G$ l'insieme delle parti dell'insieme degli elementi di G. Una azione sinistra di G su X è data dalla posizione $g * S = gS$, dove $g \in G$, $S \subseteq G$ e $gS = \{gs \mid s \in S\}$.

Esempio 2.3.7. Azione di coniugio per i sottogruppi. Sia G un gruppo, e sia $X \subseteq 2^G$ l'insieme dei sottogruppi di G. Una azione sinistra di G su X è data dalla posizione $g * H = gHg^{-1}$, dove $g \in G$, $H \leqslant G$ e $gH = \{gh \mid h \in H\}$.

Esempio 2.3.8. Azione indotta. Data una azione sinistra di G su X, e un omomorfismo di gruppi $f\colon G' \to G$, l'azione indotta da f

$$G' \times X \longrightarrow X$$

è data dalla posizione $g' * x = f(g') * x$, con $g' \in G'$ e $x \in X$. Un caso particolare si ha quando f è l'inclusione di un sottogruppo $H \hookrightarrow G$. In questo caso parleremo di *restrizione dell'azione di* G *all'azione del sottogruppo* H.

Ad esempio, se $D_n \leqslant S_n$ è il gruppo diedrale su n elementi, dall'Esempio 2.3.3 ricaviamo la classica azione di D_n su $\underline{n}$, che possiamo qui identificare con l'insieme dei vertici di un n-agono regolare.

Nel seguito, ci riferiremo alle azioni sinistre chiamandole semplicemente *azioni*.

Dati due G-set $(X, *)$ e $(X', *')$, un morfismo tra essi è una funzione $f\colon X \to X'$ compatibile con le azioni. Più precisamente, la funzione f rende commutativo il seguente diagramma in Set:

$$\begin{array}{ccc} G \times X & \xrightarrow{*} & X \\ {\scriptstyle \mathrm{id}_G \times f}\downarrow & & \downarrow{\scriptstyle f} \\ G \times X' & \xrightarrow[*']{} & X' \end{array}$$

i.e. per ogni $g \in G$ e $x \in X$ si ha

$$f(g * x) = g *' f(x)\,. \tag{9}$$

La condizione espressa dall'equazione (9) è chiamata *equivarianza di* f *rispetto all'azione.*

Proposizione 2.3.9. *I* G*-insiemi e i loro morfismi formano una categoria, denotata* G-Set.

Dimostrazione (traccia). Dati due morfismi di G-insiemi

$$(X, *) \xrightarrow{f} (X', *') \xrightarrow{g} (X'', *'')$$

la loro composizione in G-Set è data dalla composta di f e g in Set:

$$(X, *) \xrightarrow{g \circ f} (X'', *'')$$

L'identità del G-insieme $(X, *)$ è semplicemente id_X. La verifica delle condizioni di equivarianza e degli assiomi di categoria è lasciata al lettore. □

Lemma 2.3.10. *Un isomorfismo in* G-Set *è un morfismo*

$$(X, *) \xrightarrow{f} (X', *')$$

di G*-insiemi dove* f *è una biezione tra gli insiemi* X *e* X'*.*

Dimostrazione. Poiché $f \circ f^{-1} = \mathrm{id}_{X'}$ e $f^{-1} \circ f = \mathrm{id}_X$, basterà verificare che f^{-1} è equivariante. A questo scopo, si consideri $x' \in X'$. Essendo f biettiva, esiste $\bar{x} \in X$ tale che $f(\bar{x}) = x'$. Quindi si ha:

$$f^{-1}(g *' x') = f^{-1}(g *' f(\bar{x})) = f^{-1}(f(g * \bar{x})) = g * \bar{x} = g * f^{-1}(x')\,.$$

Si noti che nella seconda uguaglianza si è usata l'equivarianza di f. □

Esercizio 2.3.11. Dati i G-insiemi $(X, *_X)$ e $(Y, *_Y)$ verificare che l'unione disgiunta $X \amalg Y$ è un G-insieme, con azione $*$ definita da

$$g * z = g *_X z \qquad \text{per } z \in X\,,$$

$$g * z = g *_Y z \qquad \text{per } z \in Y\,.$$

Dette ι_1 e ι_2 le inclusioni canoniche di X e Y in $X \amalg Y$, provare che

$$(X, *_X) \xrightarrow{\iota_1} (X \amalg Y, *) \xleftarrow{\iota_2} (Y, *_Y)$$

è coprodotto di $(X, *)$ e $(X', *')$ in G-Set.

2.3.2 *Azioni fedeli*

Definizione 2.3.12. *Una azione di* G *su* X *viene chiamata* fedele (o effettiva) *se l'omomorfismo* φ *ad essa associato è un monomorfismo.*

Il concetto di azione fedele può essere caratterizzato nella proposizione seguente, la cui dimostrazione è lasciata come esercizio.

Proposizione 2.3.13. *Una azione di* G *su* X *è fedele se e solo se elementi diversi di* G *agiscono in modo diverso: se* $g_1 \neq g_2$*, allora esiste* $x \in X$ *tale che* $g_1 * x \neq g_2 * x$*.*

In altre parole, una azione è fedele se l'unico elemento di G che agisce in modo banale è l'identità.

Proposizione 2.3.14. *Ogni gruppo agisce fedelmente su qualche insieme.*

Dimostrazione. Per ogni gruppo G, l'azione descritta nell'Esempio 2.3.4 è una azione fedele. □

Corollario 2.3.15 (Teorema di Cayley)**.** *Ogni gruppo* G *è isomorfo a un sottogruppo di un opportuno gruppo di permutazioni.*

Dimostrazione. Si prenda ad esempio l'immagine dell'omomorfismo

$$G \xrightarrow{\tau} \mathrm{Sym}(G)$$

associato all'azione (fedele) di traslazione. □

Osserviamo che l'importanza del teorema di Cayley è soprattutto teorica. Infatti non è detto che il monomorfismo ottenuto dalla traslazione sinistra sia un modo efficiente di rappresentare G. Si prenda ad esempio il gruppo diedrale D_{10}. Esso è composta da 20 elementi, e pertanto, per quanto appena visto, può essere considerato come un sottogruppo di $\mathrm{Sym}(D_{10}) \cong S_{20}$, ma come è ben noto, D_{10} può essere visto come sottogruppo del gruppo simmetrico su 10 elementi. Ora, S_{20} conta ben $20! = 2\,432\,902\,008\,176\,640\,000$ elementi, mentre S_{10} appena $3\,628\,800$. Un tema interessante sviluppato dai teorici dei gruppi consiste proprio nel determinare delle rappresentazioni combinatorie più efficienti di un dato gruppo finito G.

Definizione 2.3.16. *Sia data una azione di un gruppo* G *su un insieme* X*, e sia* x *un elemento di* X*.*

- *L'orbita di* x *è il sottoinsieme di* X

$$\mathrm{Orb}_G(x) = \{g * x \mid g \in G\}.$$

- *Lo stabilizzatore di* x *è il sottoinsieme di* G

$$\mathrm{Stab}_G(x) = \{g \in G \mid g * x = x\}.$$

Proposizione 2.3.17. $\mathrm{Stab}_G(x)$ *è un sottogruppo di* X*.*

Dimostrazione. Dato $x \in X$, consideriamo una coppia di elementi $g_1, g_2 \in \mathrm{Stab}_G(x)$. Si ha

$$(g_1 g_2^{-1}) * x = g_1 * (g_2^{-1} * x) = g_1 * (g_2^{-1} * (g_2 * x)) =$$

$$= g_1 * (g_2^{-1} g_2 * x) = g_1 * (1_G * x) = g_1 * x = x$$

dove si sono usati gli assiomi di azione e il fatto che g_1 e g_2 fissano x. Concludiamo $g_1 g_2^{-1} \in \mathrm{Stab}_G(x)$. □

Le orbite di una azione di G su X formano una partizione dell'insieme X. Denotiamo con $\sim$ la relazione di equivalenza ad essa associata, per cui, $x, y \in X$ $x \sim y$ indica il fatto che x e y appartengono alla stessa orbita.

Definizione 2.3.18. *Una azione di* G *sull'insieme* X *viene chiamata* transitiva *se soddisfa la seguente proprietà: per ogni* $x, y \in X$*, esiste* $g \in G$ *tale che* $y = g * x$*.*

Osservazione 2.3.19. Dalla definizione si deduce che una azione è transitiva se e solo se $\mathrm{Orb}_G(x) = X$. Per questo, nel linguaggio dei G-insiemi, una azione transitiva determina un G-insieme *conesso*.

Esempio 2.3.20. Consideriamo l'azione canonica del gruppo S_n sull'insieme $\underline{n}$ (Esempio 2.3.3). Preso $i \in \underline{n}$ si ha che

$$\mathrm{Orb}_{S_n}(i) = \underline{n},$$

cioè l'azione è transitiva. Per quanto riguarda lo stabilizzatore, si tratta di selezionare in S_n tutte le permutazioni che fissano i. In altre parole, le permutazioni dell'insieme di $n-1$ elementi: $\underline{n} \setminus \{i\}$; di conseguenza,

$$\mathsf{Stab}_{S_n}(i) \cong S_{n-1}\,.$$

Esempio 2.3.21. Consideriamo l'azione di moltiplicazione sinistra del gruppo G sull'insieme soggiacente G (Esempio 2.3.4). L'azione è transitiva: dati $x, y \in G$, l'elemento $g = yx^{-1}$ è tale che

$$g * x = yx^{-1} * x = yx^{-1}x = y1_G = y\,.$$

Inoltre, dato $x \in G$, $g * x = x$ se e solo se $g = 1_G$, per cui concludiamo:

$$\mathsf{Orb}_G(x) = G\,, \qquad \mathsf{Stab}_G(x) = \{1_G\}\,.$$

Esempio 2.3.22. Consideriamo l'azione di coniugio del gruppo G sull'insieme soggiacente G (Esempio 2.3.5). Non si tratta in generale di un'azione transitiva (l'azione è transitiva se e solo se G è il gruppo banale). Le orbite dell'azione sono le classi di coniugio di G, mentre lo stabilizzatore di un generico elemento $x \in G$ è il suo *centralizzante* in G:

$$Z_G(x) = \{g \in G : gxg^{-1} = x\}\,.$$

Esempio 2.3.23. Consideriamo l'azione di coniugio del gruppo G sull'insieme X dei sottogruppi di G (Esempio 2.3.7). Anche in questo caso, non si tratta in generale di un'azione transitiva. Preso un sottogruppo $H \leqslant G$, l'orbita di H è l'insieme di tutti i sottogruppi coniugati a H, mentre lo stabilizzatore di H è il suo *normalizzante* in G:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}\,.$$

Osserviamo che il normalizzante di un sottogruppo è il più grande sottogruppo di G in cui H è normale.

Un altro esempio notevole di azione transitiva di un gruppo G è l'azione di moltiplicazione sinistra sui laterali. La proposizione che segue mostra come tali azioni possano essere considerate il prototipo di tutte le azioni transitive.

Esempio 2.3.24. Sia G un gruppo, e H un suo sottogruppo. Una azione transitiva di G sull'insieme G/H dei laterali sinistri di H in G

$$G \times G/H \longrightarrow G/H$$

è data dalla posizione $g * xH = gxH$. Infatti, dati $xH, yH \in G/H$, si ha $g * xH = yH$, per $g = yx^{-1}$.

Teorema 2.3.25. *Ogni azione transitiva di un gruppo G su un insieme X è isomorfa all'azione di moltiplicazione sinistra di G sull'insieme G/H dei laterali sinistri di H in G, dove $H = \mathsf{Stab}_G(x)$ e $x \in X$.*

Dimostrazione. Sia data una azione transitiva di G su X, con H e x come sopra.

Definiamo una funzione $\phi\colon G/H \to X$, con $\phi(gH) = g * x$. La funzione è ben definita. Infatti, se $g_1H = g_2H$, si ha che $g_1^{-1}g_2H = H$, i.e. $g_1^{-1}g_2 \in H$. Quindi $(g_1^{-1}g_2) * x = x$, ovvero $g_1 * x = g_2 * x$.

Definiamo poi una funzione $\psi\colon X \to G/H$, con $\psi(g * x) = gH$. Anche questa funzione è ben definita. Infatti, da $g_1 * x = g_2 * x$, subito deduciamo $(g_1^{-1}g_2) * x = x$, e ripercorrendo a ritroso il ragionamento svolto in precedenza, otteniamo $g_1H = g_2H$.

Ora, è evidente che ϕ e ψ siano reciprocamente inverse, per cui in particolare ϕ è una biezione. Infine, ϕ è equivariante rispetto alle azioni. Infatti:

$$\phi(g' * gH) = \phi(g'gH) = (g'g) * x = g' * (g * x) = g' * \phi(gH)\,.$$

□

Si noti che nel teorema la scelta di H non è unica, perché dipende dalla scelta arbitraria di $x \in X$. Tuttavia, x diversi nella stessa orbita hanno stabilizzatori coniugati, e quindi isomorfi.

Esercizio 2.3.26. Data una azione di G su X, e $x, y \in X$, $g \in G$ tali che $y = g * x$ si ha

$$\mathsf{Stab}_G(y) = g\,\mathsf{Stab}(x)_G\,g^{-1}$$

Corollario 2.3.27. *(Teorema orbita/stabilizzatore) Data una azione di* G *su* X *finito,* $x \in X$*, si ha*

$$|\mathsf{Orb}_G(x)| = [G : \mathsf{Stab}_G(x)]$$

Dimostrazione. L'azione di G ristretta al sottoinsieme $\mathsf{Orb}_G(x) \subseteq X$ è transitiva. Pertanto dal teorema otteniamo una biezione

$$\mathsf{Orb}_G(x) \simeq \frac{G}{\mathsf{Stab}_G(x)}$$

Prendendo le cardinalità si ottiene il risultato. □

Poiché ogni azione diventa transitiva, se ristretta a una singola orbita, è possibile scomporre ogni azione in azioni transitive sulle singole orbite. Questa affermazione è precisata dal prossimo teorema.

Teorema 2.3.28. *Ogni* G*-insieme* X *ammette una scomposizione canonica nel coprodotto delle sue componenti transitive*

$$X \simeq \coprod_{x \in \Omega} \frac{G}{\mathsf{Stab}_G(x)}$$

con $\Omega \subseteq X$ *contenente esattamente un singolo elemento per ogni orbita dell'azione.*

Dimostrazione. Le orbite dell'azione di G su X formano una partizione di X:

$$X = \coprod_{x \in \Omega} \mathrm{Orb}_G(x)$$

Generalizzando l'Esercizio 2.3.11 al coprodotto di una famiglia di G-insiemi, il risultato segue dallo stesso argomento utilizzato per provare il Corollario 2.3.27. □

Si noti che nel teorema si è preferito il termine G-insieme al termine azione. Questa scelta vuole mettere in luce un punto di vista più prettamente geometrico della categoria G-Set, cioé il fatto che ogni G-insieme è isomorfo al coprodotto delle sue componenti connesse.

2.3.3 *Equazione delle classi*

Quella che viene normalmente chiamata *equazione delle classi* di una azione, altro non è che la versione *numerica* del Teorema 2.3.28. Questa sezione è dedicata ad essa.

Definizione 2.3.29. *Data una azione di* G *su* X*, è definito l'insieme (eventualmente vuoto) dei punti fissi dell'azione:*

$$X_0 = \{x \in X \mid g * x = x, \textit{per ogni } g \in G\}$$

L'insieme X_0 comprende quindi esattamente tutte e sole le orbite costituite da un solo elemento. Dal Teorema 2.3.28 e dalla definizione di X_0, segue immediatamente il prossimo risultato.

Corollario 2.3.30 (Equazione delle classi)**.** *Data una azione di* G *su un insieme* X *finito, si ha:*

$$|X| = |X_0| + \sum_{x \in \Omega'} [G : \mathrm{Stab}_G(x)] \tag{10}$$

dove l'insieme $\Omega' \subseteq X$ *contiene esattamente un rappresentante per ogni orbita non banale dell'azione.*

Nel caso di un'azione in cui il gruppo ad agire abbia ordine una potenza di p, l'equazione delle classi fornisce un importante condizione sulla cardinalità dell'insieme dei punti fissati dall'azione.

Lemma 2.3.31 (dei punti fissi)**.** *Sia* p *primo e* G *gruppo di ordine* p^n*. Data un'azione di* G *su un insieme* X *finito, si ha*

$$|X_0| \equiv |X| \mod p$$

Dimostrazione. Consideriamo l'equazione (10) delle classi dell'azione. Per ogni $x \in \Omega'$, essendo l'orbita di x non banale, per il Teorema orbita/stabilizzatore, $\mathrm{Stab}_G(x)$ è contenuto *propriamente* in G. Pertanto, per l'ipotesi sulla cardinalità di G, si ha che p divide l'indice $[G : \mathrm{Stab}_G(x)]$. Il risultato segue dall'equazione delle classi. □

Come applicazione del Lemma 2.3.31, anticipando un tema che verrà sviluppato più approfonditamente nella sezione relativa ai teoremi di Sylow, presentiamo il prossimo risultato.

Proposizione 2.3.32 (Teorema di Cauchy)**.** *Dato un gruppo finito* G *e un numero primo* p *che divida l'ordine di* G*, esiste un sottogruppo* $H \leqslant G$ *di ordine* p*.*

Dimostrazione. Sia X l'insieme delle p-uple $(x_1, \dots, x_p)$ di elementi di G tali che $x_1 \cdots x_p = 1$. Osserviamo che una p-upla appartiene a X se e solo se $x_p = (x_1 \cdots x_{p-1})^{-1}$; pertanto la cardinalità di X è precisamente $|G|^{p-1}$. Definiamo ora l'azione del gruppo $\mathbb{Z}_p$ su X data dalla permutazione ciclica:

$$m * (x_1, \dots, x_p) = (x_{m+1}, \dots, x_p, x_1, \dots, x_m)\,.$$

Si osservi che l'azione è ben definita, poiché se è vero che $x_1 \cdots x_p = 1$, allora anche $x_{m+1} \dots x_p x_1 \dots x_m = 1$. Per il Lemma 2.3.31, si ha che $|X_0| \equiv |X| \mod p$, ma $|X_0| \neq 0$, perché almeno $(1, \dots, 1) \in X_0$. Inoltre, $|X_0| \neq 1$, perché $|X| \equiv 0 \mod p$. Quindi deve esistere $g \in G$ tale che $(g, \dots, g) \in X_0$, i.e. $g^p = 1$. □

Una classe di gruppi di notevole interesse è costituita dai cosiddetti p-gruppi.

Definizione 2.3.33. *Sia* p *un numero primo. Un gruppo* G *è detto* p-gruppo *se ogni suo elemento ha periodo una potenza di* p*.*

Proposizione 2.3.34 (Caratterizzazione p-gruppi finiti)**.** *Sia* G *un gruppo finito.* G *è un* p*-gruppo se, e solo se,* $|G| = p^k$*, per un certo intero positivo* k*.*

Dimostrazione. Se G è p-gruppo finito e q è un numero primo che divide $|G|$, il teorema di Cauchy ci assicura che esiste un elemento $g \in G$ di periodo q, quindi $q = p$. Il viceversa segue immediatamente dal teorema di Lagrange. □

L'equazione delle classi di un gruppo finito G si ottiene dall'equazione delle classi dell'azione di coniugio di G su G.

Dato un gruppo G, denotiamo con χ l'omomorfismo

$$G \xrightarrow{\chi} \mathsf{Sym}(G)$$

associato all'azione di coniugio (Esempio 2.3.5). È immediato verificare che il centro del gruppo

$$Z(G) = \ker(\chi)$$

è precisamente l'insieme degli elementi di G fissati da tale azione, i.e. l'insieme degli elementi che commutano con tutti gli elementi del gruppo.

Come anticipato dall'Esempio 2.3.22, le nozioni di *orbita* e di *stabilizzatore* per l'azione di coniugio producono due nozioni fondamentali in teoria dei gruppi. Dato $x \in G$, l'orbita di x non è altro che la classe di coniugio di x, e verrà denotata $[x]_G$, o più semplicemente $[x]$. Lo stabilizzatore di x è invece il *centralizzante* di x, e verrà denotato $Z_G(x)$, o più semplicemente $Z(x)$. Si noti che se si restringe l'azione di coniugio a un sottogruppo $H \leqslant G$, la notazione $Z_H(x)$ sarà riservata al centralizzante di x relativo a H, i.e. l'insieme degli elementi di H che commutano con x.

Corollario 2.3.35 (Equazione delle classi di un gruppo)**.** *Sia* G *un gruppo finito. Vale l'uguaglianza:*

$$|G| = |Z_G(G)| + \sum_{x \in \Omega'} [G : Z_G(x)] \tag{11}$$

con $\Omega' \subseteq X$ *contenente esattamente un singolo elemento del gruppo per ogni classe di coniugio non banale.*

Dimostrazione. Si scriva l'equazione delle classi per l'azione del coniugio. □

L'equazione delle classi di un p-gruppo ha una immediata applicazione.

Corollario 2.3.36. *Se* G *è un* p*-gruppo finito (non banale), allora il suo centro non è banale.*

Dimostrazione. Se $G = Z(G)$ la proposizione è vera. Supponiamo allora $G \neq Z(G)$. In questo caso, per $x \in G \setminus Z(G)$, i sottogruppi $Z_G(x)$ sono sottogruppi propri di G. Pertanto i termini $[G : Z_G(x)]$ nell'equazione (11), sono divisi da p. Ma p divide anche $|G|$, e di conseguenza p divide $|Z(G)| \neq 0$, che pertanto non può essere banale. □

2.3.4 *Applicazioni*

Analizziamo le classi di coniugio di alcuni gruppi notevoli e verifichiamo le relative equazioni delle classi.

Classi di coniugio di S_n

Definizione 2.3.37. *Data una permutazione* $\sigma \in S_n$*, la* struttura ciclica[1] *di* σ *si ottiene scrivendo* σ *come prodotto di cicli disgiunti, e considerando è la sequenza di interi positivi*

$$[k_1, k_2, \ldots, k_t]$$

con $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_t$*, corrispondente ai* k_i*-cicli di tale scrittura, con* $i = 1, \ldots, t$.

1 *cycle type*, in inglese.

Ad esempio, $(1234)(567) \in S_7$ ha struttura ciclica $[4,3]$, mentre $(1234)(567) \in S_{10}$ ha struttura ciclica $[4,3,1,1,1]$.

Lemma 2.3.38. *Dati $\tau \in S_n$ e $\alpha = (a_1, \ldots, a_k) \in S_n$, si ha*

$$\tau\alpha\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k)) .$$

Dimostrazione. Vogliamo provare che la permutazione $\tau\alpha\tau^{-1}$ manda

$$\tau(a_i) \mapsto \tau(a_{i+1}) ,$$

dove $i+1$ è preso *modulo* k. Basta calcolare:

$$\tau\alpha\tau^{-1}(\tau(a_i)) = \tau(\alpha(\tau^{-1}(\tau(a_i)))) = \tau(\alpha(a_i)) = \tau(a_{i+1}) .$$

□

Data una permutazione $\sigma \in S_n$, la proposizione seguente ci mostra che la sua classe di coniugio in S_n, denotata $[\sigma]_{S_n}$, è determinata esclusivamente dalla struttura ciclica di σ.

Proposizione 2.3.39. *Date $\sigma, \sigma' \in S_n$, la permutazione σ è coniugata alla permutazione σ' se e solo se σ e σ' hanno la stessa struttura ciclica.*

Dimostrazione. Sia $\alpha_1\alpha_2\cdots\alpha_t$ una scrittura di σ come prodotto di cicli disgiunti. Si ha che

$$\tau\sigma\tau^{-1} = (\tau\alpha_1\tau^{-1})(\tau\alpha_2\tau^{-1})\cdots(\tau\alpha_t\tau^{-1})$$

sono ancora cicli disgiunti, per il lemma precedente. □

Osservazione 2.3.40. Data una permutazione $\sigma \in S_n$ con struttura ciclica

$$[k_1, k_2, \ldots, k_t] ,$$

è chiaro che vale

$$k_1 + k_2 + \cdots + k_t = n$$

Quindi, le classi di coniugio di S_n sono in corrispondenza biunivoca con le *partizioni* dell'intero positivo n.

Per applicare le nozioni appena introdotte, vediamo le classi di coniugio di S_n, per $n = 3, 4, 5$.

Esempio 2.3.41 (Classi di coniugio di S_3). Analizziamo le strutture cicliche degli elementi. In S_3 abbiamo i 3-cicli, i 2-cicli e l'identità. La terza colonna della tabella riportata qui sotto conta quanti elementi ci sono per ogni struttura ciclica.

elemento tipo	struttura ciclica	n. elementi di quel tipo	parità
(abc)	$[3]$	$\frac{3\cdot2\cdot1}{3} = 2$	0
(ab)	$[2,1]$	$\frac{3\cdot2}{2} = 3$	1
id	$[1,1,1]$	1	0

Pertanto, l'equazione delle classi di S_3 è

$$|S_3| = 6 = 1 + 3 + 2\,.$$

Esempio 2.3.42 (Classi di coniugio di S_4). Analizziamo ora le strutture cicliche degli elementi di S_4. Ci sono i 4-cicli, i 3-cicli, le coppie di 2-cicli, i 2-cicli e l'identità. La terza colonna della tabella riportata qui sotto conta quanti elementi ci sono per ogni struttura ciclica.

elemento tipo	struttura ciclica	n. elementi di quel tipo	parità
$(abcd)$	$[4]$	$\frac{4\cdot3\cdot2\cdot1}{4} = 6$	1
(abc)	$[3,1]$	$\frac{4\cdot3\cdot2}{3} = 8$	0
$(ab)(cd)$	$[2,2]$	$\frac{4\cdot3}{2}\cdot\frac{2\cdot1}{2}\cdot\frac{1}{2} = 3$	0
(ab)	$[2,1,1]$	$\frac{4\cdot3}{1}\cdot\frac{1}{2} = 6$	1
id	$[1,1,1,1]$	1	0

Pertanto, l'equazione delle classi di S_4 è

$$|S_4| = 24 = 1 + 6 + 3 + 8 + 6\,.$$

Esempio 2.3.43 (Classi di coniugio di S_5). Analizziamo ora le strutture cicliche degli elementi di S_5. Ci sono i 5-cicli, i 4-cicli, le coppie 3-ciclo / 2-ciclo, i 3-cicli, le coppie di 2-cicli, i 2-cicli, e l'identità. La terza colonna della tabella riportata qui sotto conta quanti elementi ci sono per ogni struttura ciclica.

elemento tipo	struttura ciclica	n. elementi di quel tipo	parità
$(abcde)$	$[5]$	$\frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$	0
$(abcd)$	$[4,1]$	$\frac{5\cdot4\cdot3\cdot2}{4} = 30$	1
$(abc)(de)$	$[3,2]$	$\frac{5\cdot4\cdot3}{3}\cdot\frac{2\cdot1}{2} = 20$	1
(abc)	$[3,1,1]$	$\frac{5\cdot4\cdot3}{3} = 20$	0
$(ab)(cd)$	$[2,2,1]$	$\frac{5\cdot4}{2}\cdot\frac{3\cdot2}{2}\cdot\frac{1}{2} = 15$	0
(ab)	$[2,1,1,1]$	$\frac{5\cdot4}{2} = 10$	1
id	$[1,1,1,1,1]$	1	0

Pertanto, l'equazione delle classi di S_5 è

$$|S_5| = 120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$$

Classi di coniugio di A_n

Ricordiamo che la funzione di parità $p\colon S_n \to \mathbb{Z}_2$ (definita da $p(\sigma) = 0$ se σ può essere scritta come un prodotto di un numero pari di 2-cicli, $p(\sigma) = 1$ altrimenti) è un omomorfismo di gruppi, il cui nucleo è il cosiddetto *gruppo alterno* A_n. A_n è quindi sottogruppo normale di S_n, con indice $[S_n : A_n] = 2$.

Di seguito riportiamo una proprietà elementare di cui godono tutti i sottogruppi normali.

Lemma 2.3.44. *Sia* G *gruppo, e* H *sottogruppo di* G*. Allora* H *è normale in* G *se e solo se esso è unione di classi di coniugio di* G*.*

Dimostrazione. Sia H normale in G, e $x \in H$. Allora, per ogni $g \in G$, si ha $gxg^{-1} \in H$, e di conseguenza $[x]_G \subseteq H$. In altre parole, ogni elemento di H appartiene a una classe di coniugio che è contenuta totalmente in H, da cui

$$H = \bigcup_{x \in H} [x]_G \,.$$

Viceversa, se H è unione di classi di coniugio di G, per ogni $x \in H$ e $g \in G$ si ha $gxg^{-1} \in [x]_G \subseteq H$. □

Il lemma appena dimostrato ci pone una questione che è opportuno indagare subito. Poiché i sottogruppi A_n sono normali nei rispettivi S_n, essi sono composti dall'unione di un certo numero di classi di coniugio di S_n. Ad esempio si ha

$$A_3 = [\mathrm{id}]_{S_3} \cup [(123)]_{S_3}$$

$$A_4 = [\mathrm{id}]_{S_4} \cup [(123)]_{S_4} \cup [(12)(34)]_{S_4}$$

$$A_5 = [\mathrm{id}]_{S_5} \cup [(123)]_{S_5} \cup [(12)(34)]_{S_5} \cup [(12345)]_{S_5}$$

È naturale chiedersi se tali classi di coniugio restino classi di coniugio anche relativamente ai gruppi A_n. Chiaramente la risposta è no, in generale, visto che, ad esempio, A_3 è abeliano, e pertanto le sue classi di coniugio sono dei singoletti. Tuttavia la questione è interessante. Ad esempio, è facile vedere che

$$[(12)(34)]_{A_4} = [(12)(34)]_{S_4} \,.$$

Infatti, $(234)\,(12)(34)\,(243) = (13)(24)$ e $(243)\,(12)(34)\,(234) = (14)(23)$, e $(234) \in A_4$. D'altro canto, sicuramente

$$[(123)]_{A_4} \neq [(123)]_{S_4} \,.$$

Infatti, per il Teorema orbita/stabilizzatore, la cardinalità dell'orbita deve dividere l'ordine del gruppo, e invece

$$|[(123)]_{S_4}| = 8 \nmid 12 = |A_4| \,.$$

Coniugando mediante tutti gli elementi di A_4, è possibile verificare direttamente che le classi di coniugio dei 3-cicli in A_4 sono precisamente due

$$[(123)]_{A_4} = \{(123), (134), (243), (124)\}$$

$$[(132)]_{A_4} = \{(132), (143), (234), (142)\}$$

ma il lavoro può essere reso più semplice da considerazioni sull'ordine degli stabilizzatori per l'azione di coniugio. Questo tema è sviluppato nella proposizione seguente, che non si limita al caso $n = 4$.

Lemma 2.3.45. *Data una permutazione $\sigma \in A_n$, ci sono due casi possibili:*

(1) $|[\sigma]_{A_n}| = |[\sigma]_{S_n}|$;

(2) $|[\sigma]_{A_n}| = \frac{1}{2}|[\sigma]_{S_n}|$.

Nel primo caso, si ha che $[\sigma]_{A_n} = [\sigma]_{S_n}$; nel secondo caso, fissata $\sigma' \in A_n$ che abbia la stessa struttura ciclica di σ ma non sia coniugata a σ in A_n, gli insiemi $[\sigma]_{A_n}$ e $[\sigma']_{A_n}$ formano una partizione di $[\sigma]_{S_n}$.

Dimostrazione. Dal teorema orbita/stabilizzatore sappiamo che valgono le uguaglianze:

$$|S_n| = |[\sigma]_{S_n}| \cdot |Z_{S_n}(\sigma)| \qquad |A_n| = |[\sigma]_{A_n}| \cdot |Z_{A_n}(\sigma)|$$

Poiché $Z_{S_n}(\sigma)$ e A_n sono sottogruppi di S_n, si presentano i due casi che analizziamo di seguito.

(1) Se $Z_{S_n}(\sigma)$ è un sottogruppo di A_n, si ha $Z_{S_n}(\sigma) = Z_{A_n}(\sigma)$, e pertanto,

$$|[\sigma]_{A_n}| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|S_n|/2}{|Z_{S_n}(\sigma)|} = \frac{1}{2}|[\sigma]_{S_n}|.$$

(2) Se $Z_{S_n}(\sigma)$ non è un sottogruppo di A_n, allora $Z_{A_n} = Z_{S_n} \cap A_n$, e poiché $[S_n : A_n] = 2$, allora anche $[Z_{S_n} : Z_{A_n}] = 2$. Quindi:

$$|[\sigma]_{A_n}| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|S_n|/2}{|Z_{S_n}(\sigma)|/2} = |[\sigma]_{S_n}|.$$

Per concludere basta osservare che per ogni $\sigma \in A_n$, $[\sigma]_{A_n} \subseteq [\sigma]_{S_n}$. □

Esempio 2.3.46 (Classi di coniugio di A_3). Come già detto, $A_3 = \{\mathrm{id}, (123), (132)\}$ è abeliano. Le sue classi di coniugio sono tre, e ognuna contiene esattamente uno degli elementi di A_3. In conclusione, l'equazione delle classi di A_3 è

$$3 = 1 + 1 + 1.$$

Esempio 2.3.47 (Classi di coniugio di A_4). Si ha che $|[(12)(34)]_{S_4}| = 3$; poiché $2 \nmid 3$, siamo nel caso (2), e dunque anche $|[(12)(34)]_{A_4}| = 3$. Si ha $|[(123)]_{S_4}| = 8$, tuttavia $8 \nmid 12$ (ovvero la cardinalità di A_4) e dunque le classi di coniugio dei 3-cicli devono necessariamente essere due, come previsto dal caso (1). Si verifica facilmente che esse sono $[(123)]_{A_4}$ e $[(132)]_{A_4}$. In conclusione, l'equazione delle classi di A_4 è

$$12 = 1 + 3 + 4 + 4\,.$$

Esempio 2.3.48 (Classi di coniugio di A_5). Ci riferiamo alla tabella dell'esempio 2.3.43, dove sono riportate le classi di coniugio degli elementi di S_5. Per quanto riguarda i 5-cicli, essi sono 24. Ma $24 \nmid 60$ (ovvero la cardinalità di A_5), e quindi siamo necessariamente nel caso (1): la classe dei 5-cicli si spezza in due classi di coniugio da 12 elementi. Per quanto riguarda i 3-cicli, si vede facilmente che $(45) \in Z_{S_5}((123))$, ma $(45) \notin A_5$; quindi siamo nel caso (2), e concludiamo che la classe $[(123)]_{A_5} = [(123)]_{S_5}$ ha 20 elementi. Venendo alle coppie di 2-cicli, la loro classe di coniugio in S_5 è composta da 15 elementi. Pertanto essa non può essere suddivisa in due sottoclassi della stessa cardinalità, e quindi $[(12)(34)]_{A_5} = [(12)(34)]_{S_5}$ ha precisamente 15 elementi. L'equzione delle classi di A_5 è la seguente:

$$60 = 1 + 12 + 12 + 20 + 15\,.$$

In conclusione, presentiamo un semplice corollario che illustra come i vincoli numerici introdotti dall'equazione delle classi siano uno strumento molto efficace per risolvere problemi anche complessi.

Corollario 2.3.49. *Il gruppo alterno A_5 è un gruppo semplice.*

Dimostrazione. Sia H normale in A_5. Per il teorema di Lagrange la cardinalità di H divide 60, che è l'ordine di G. Per il Lemma 2.3.44, tale numero è anche la somma di alcuni degli addendi che compaiono nella sua equazione delle classi. Inoltre sappiamo con certezza che vi è 1, perché H sottogruppo contiene necessariamente l'identità del gruppo. Ora, nessuna di tali somme divide 60, se non 1 e 60. Pertanto, le uniche possibilità per H sono $H = 1$ oppure $H = A_5$. □

Si può dimostrare che anche tutti gli altri gruppi alterni sono semplici. Questo fatto è utilizzato nella dimostrazione del teorema di Abel-Ruffini, per mostrare che per $n > 4$ vi sono equazioni algebriche che non si possono risolvere per radicali.

Classi di coniugio di D_n

In questa sezione studieremo le classi di coniugio del gruppo diedrale, con presentazione:

$$D_n = \langle \rho, \sigma \mid \rho^n, \sigma^2, \rho\sigma\rho\sigma \rangle\,.$$

Come sappiamo, le relazioni ci permettono scrivere gli elementi di D_n come segue:

$$D_n = \{1, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma\}$$

Con riferimento all'azione canonica del gruppo diedrale sull'n-agono regolare, i primi n elementi corrispondono alle rotazioni in senso antiorario, e gli altri le riflessioni assiali.

Prima coniughiamo le rotazioni. Per i, j interi, si ha:

$$\rho^i\rho^j\rho^{-i} = \rho^j$$

$$(\rho^i\sigma)\rho^j(\rho^i\sigma)^{-1} = \rho^i\sigma\rho^j\sigma\rho^{-i} = \rho^i\sigma\sigma\rho^{-j}\rho^{-i} = \rho^{-j}$$

Quindi, la classe di coniugio di ρ^j è l'insieme $\{\rho^j, \rho^{-j}\}$.

Ora coniughiamo le riflessioni. Per i, j interi, si ha:

$$\rho^i(\rho^j\sigma)\rho^{-i} = \rho^{2i+j}\sigma = \rho^{2i}(\rho^j\sigma)$$

$$(\rho^i\sigma)(\rho^j\sigma)(\rho^i\sigma)^{-1} = \rho^i\sigma\rho^j\sigma\sigma\rho^{-i} = \rho^{2(i-j)}(\rho^j\sigma)$$

Quindi la classe (le classi) di coniugio di $\rho^j\sigma$ è (sono):

$$\{\rho^{2k}(\rho^j\sigma) \mid k = 0, 1, 2 \ldots, n-1\}.$$

Siamo ora nelle condizioni di descrivere le classi di coniugio di D_n. Distinguiamo due casi.

- Se n è dispari. Per quanto riguarda le rotazioni, le potenze di ρ formano
  - la classe $\{\mathrm{id}\}$ di un solo elemento, che costituisce il centro di D_n,
  - $\frac{n-1}{2}$ classi $\{\rho^j, \rho^{-j}\}$ di due elementi ciascuna.

  Per quanto riguarda le riflessioni, poiché con n dispari ogni potenza distinta di ρ può essere messa nella forma ρ^{2i}, esse formano
  - un'unica classe $\{\sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma\}$ di n elementi distinti.

  In conclusione, l'equazione delle classi di D_n quando n è dispari è:
  $$2n = 1 + 2 + \cdots + 2 + n.$$
- Se n è pari. Per quanto riguarda le rotazioni, le potenze di ρ formano
  - 2 classi di un solo elemento: $\{\mathrm{id}\}$ e $\{\rho^{\frac{n}{2}}\}$, che insieme formano il centro di D_n,
  - $\frac{n-2}{2}$ classi $\{\rho^j, \rho^{-j}\}_{j=0,\ldots,\frac{n-2}{2}}$ di due elementi ciascuna.

  Per quanto riguarda le riflessioni, esse formano:

* 2 classi distinte di $\frac{n}{2}$ elementi ciascuna:

$$\{\rho^{2j}\sigma\}_{j=0,\dots,\frac{n-2}{2}}\,, \qquad \{\rho^{2j+1}\sigma\}_{j=0,\dots,\frac{n-2}{2}}\,.$$

In conclusione, l'equazione delle classi di D_n quando n è pari è:

$$2n = 1 + 1 + 2 + \cdots + 2 + \frac{n}{2} + \frac{n}{2}\,.$$

Osservazione 2.3.50. Il diverso comportamento degli elementi di D_n rispetto all'azione di coniugio nel caso pari e nel caso dispari ha una semplice interpretazione geometrica.

Riferendoci ancora all'azione canonica del gruppo diedrale sull'n-agono regolare, nel caso dispari gli assi delle riflessioni passano per un vertice e il punto medio del lato opposto. Come conseguenza, le riflessioni sono tutte *dello stesso tipo* e ciò si riflette nel fatto che sono tutte coniugate tra loro. Nel caso pari, invece, gli assi delle riflessioni sono le $n/2$ diagonali gli $n/2$ assi dei lati del poligono. In questo caso formano due classi di coniugio distinte proprio perché non sono più tutte *dello stesso tipo*, sotto l'azione del gruppo diedrale.

2.4 TEOREMI DI SYLOW E APPLICAZIONI

Il cosiddetto *Teorema fondamentale dell'aritmetica* afferma che ogni numero intero $n > 1$ si può scrivere, in modo essenzialmente unico, come prodotto di potenze di numeri primi:

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

C'è da chiedersi se questa formula così elegante possa essere interpretata come la relazione numerica relativa a qualche proprietà dei gruppi.

Nel caso dei gruppi abeliani, in effetti, la formula è proprio la versione numerica del teorema di classificazione dei gruppi abeliani finiti. Come vedremo nel seguito, se A è un gruppo abeliano finito, con $|A| = n$, si ha

$$A \simeq A_{p_1} \times \cdots \times A_{p_k}$$

ossia A è isomorfo al prodotto diretto di p-gruppi, con $p = p_1, \dots, p_k$. Prendendo le cardinalità dei due membri si ottiene la formula sopra.

Nel caso di un gruppo G non necessariamente abeliano, con $|G| = n$, un risultato analogo non è disponibile. Infatti, benché come vedremo per ogni $p|n$ vi siano p-sottogruppi p-massimali, il loro prodotto diretto non è in generale isomorfo a G. Tuttavia lo studio dei p-sottogruppi di G continua a fornire importanti informazioni strutturali sul gruppo. Il risultato più rilevante che vedremo su questo argomento sono i tre teoremi di Sylow.

2.4.1 *I teoremi di Sylow*

Il matematico norvegese Peter Ludwig Mejdell Sylow è ricordato soprattutto per il suo importante contributo allo sviluppo teoria dei gruppi. Sylow pubblicò i teoremi che ora portano il suo nome sul giornale tedesco Mathematische Annalen, nel suo articolo *Theorems sur les groupes de substitucions* (1872). Tuttavia, nel lavoro citato, Sylow considera solo il caso dei gruppi di permutazioni; la dimostrazione del caso più generale dei gruppi astratti è successiva, ed è dovuta al matematico tedesco Ferdinand Frobenius (1887). In questa sezione presentiamo e dimostriamo i tre teoremi; il nostro approccio è basato prevalentemente sulle proprietà della categoria dei G-insiemi.

Teorema 2.4.1 (Teoremi di Sylow)**.** *Sia* G *un gruppo finito di ordine* $p^k m$*, con* p *primo, e* $(m, p) = 1$*. Valgono i seguenti tre teoremi di Sylow.*

(I) G *ha sottogruppi di ordine* p^k*, chiamati* p*-sottogruppi di Sylow.*

(II) I p*-sottogruppi di Sylow sono tutti coniugati tra loro.*

(III) Il numero n_p *dei* p*-sottogruppi di Sylow di* G *è tale che*

$$n_p \equiv 1 \mod p\,, \qquad n_p | m\,.$$

Vi sono diverse dimostrazioni dei teoremi di Sylow disponibili in letteratura, così come vi sono anche diverse formulazioni di detti teoremi. In queste note abbiamo adottato un approccio basato prevalentemente sulle proprietà delle azioni. La strategia che seguiremo è la seguente: per ognuno dei tre teoremi sceglieremo una specifica azione di G o di un suo sottogruppo su un opportuno insieme. Successivamente il risultato discenderà dalle proprietà dell'azione scelta.

Premettiamo alla dimostrazione dei tre teoremi il lemma seguente. Si tratta di una nota relazione della combinatoria elementare. Questa ci interessa non solo per il risultato che fornisce, ma anche perché la sua dimostrazione introduce alcune idee che utilizzeremo per provare il primo teorema di Sylow.

Lemma 2.4.2. *Sia* $n = p^k m$*, con* p *primo, e* $(p, m) = 1$*. Allora si ha*

$$\binom{n}{p^k} \equiv m \mod p$$

Dimostrazione. Sia X l'insieme delle parti dell'insieme supporto del gruppo $\mathbb{Z}_n$ che hanno cardinalità p^k e sia H il sottogruppo di $\mathbb{Z}_n$ generato dalla classe m. Consideriamo l'azione di traslazione di H su X definita da

$$h * S = h + S = \{h + x \,|\, x \in S\}, \qquad \text{per } h \in H, S \in X\,.$$

L'insieme X_0 degli elementi di X fissati dall'azione coincide con l'insieme delle classi laterali $\mathbb{Z}_n/H$, e di conseguenza, ha cardinalità m.

Infatti, $S \in X$ è fissato dall'azione se e solo se è un'unione di classi laterali, e poiché $|S| = p^k$, questo implica che S coincida con una di esse. Concludiamo osservando che $|X| = \binom{n}{p^k}$. Quindi, per il Lemma 2.3.31 sui punti fissi di una azione di un p-gruppo, si ottiene il risultato. □

Procediamo con la dimostrazione dei tre teoremi.

Dimostrazione di Sylow (I). Si consideri l'azione di traslazione sinistra del gruppo G sull'insieme X delle parti dell'insieme supporto di G che hanno cardinalità p^k:

$$g * S = gS = \{gx \,|\, x \in S\}, \qquad \text{per } g \in G,\ S \in X.$$

Per il Lemma 2.4.2, si ha che p non divide $\binom{|G|}{p^k}$. Poiché le orbite dell'azione formano una una partizione di X, si ha

$$\binom{|G|}{p^k} = |X| = \sum_{S \in \Omega} |\mathsf{Orb}_G(S)|$$

Quindi deve esistere almeno un $S \in X$ tale che

$$p \nmid |\mathsf{Orb}_G(S)| = [G : \mathsf{Stab}_G(S)].$$

da cui p^k divide $|\mathsf{Stab}_G(S)|$. Ora, è facile vedere che $|\mathsf{Stab}_G(S)| \leqslant p^k$. A questo fine, si scelga un elemento $x \in S$ e si consideri la funzione

$$\mathsf{Stab}_G(S) \xrightarrow{\phi} S$$

data da $\phi(g) = gx$. Essa è iniettiva, quindi $|\mathsf{Stab}_G(S)| \leqslant p^k$. Concludiamo allora che $|\mathsf{Stab}_G(S)| = p^k$. In altre parole, $P = \mathsf{Stab}_G(S)$ è il p-sottogruppo di Sylow cercato. □

Si osservi che l'ultimo argomento utilizzato nella dimostrazione dipende dal fatto che l'azione di traslazione puntuale di $\mathsf{Stab}_G(S)$ su S è una azione *libera*.

Dimostrazione di Sylow (II). Siano $Q \leqslant G$ un p-sottogruppo e $P \leqslant G$ un p-sottogruppo di Sylow; dimostreremo che vale

$$Q \leqslant xPx^{-1}, \qquad \text{per qualche } x \in G. \tag{12}$$

A questo fine, consideriamo l'azione di Q sull'insieme G/P delle classi laterali di P in G (traslazione sinistra):

$$g * xP = gxP, \qquad \text{per } g \in Q,\ xP \in G/P.$$

Denotato con $(G/P)_0$ l'insieme dei laterali fissati dall'azione, per il Lemma 2.3.31 si ha

$$|(G/P)_0| \equiv m \mod p.$$

In particolare, $(G/P)_0 \neq \emptyset$, cioé esiste (almeno) un laterale xP fissato dall'azione. Da $gxP = xP$ otteniamo $x^{-1}gxP = P$ e quindi $x^{-1}gx \in P$, per ogni $g \in Q$. Questo implica $x^{-1}Qx \subseteq P$, i.e. $Q \subseteq xPx^{-1}$. In particolare, se anche Q è p-sottogruppo di Sylow, si ha che Q e P sono coniugati. □

Notiamo che la validità di (12) è precisamente una delle formulazioni alternative del secondo teorema di Sylow disponibili in letteratura (vedi ad esempio...).

Dimostrazione di Sylow (III). Il p-sottogruppo di Sylow P opera tramite coniugio sull'insieme X dei p-sottogruppi di Sylow di G, essendo esso stesso fissato da tale azione. Dimostreremo che è l'unico. A tal fine, sia Q un altro p-sottogruppo di Sylow di G, con $gQg^{-1} = Q$ per ogni $g \in P$. Per definizione di normalizzante, questo vuol dire che P è un sottogruppo di $N_G(Q)$, o più precisamente, è un p-sottogruppo di Sylow di $N_G(Q)$. D'altro canto, anche Q stesso è sottogruppo di $N_G(Q)$, ed essendo normale in $N_G(Q)$, si ha che coincide con il suo coniugato, i.e. $Q = P$. Dal Lemma 2.3.31, si ottiene $n_p \equiv 1 \mod p$. Infine, considerando l'azione di coniugio di G sugli elementi di X, per il Teorema orbita/stabilizzatore si ha che $n_p = |\mathrm{Orb}_G(P)|$ divide $|G| = p^k m$, ed essendo $(n_p, p) = 1$ per quanto appena visto, si ha che n_p divide m. □

I risultati che seguono vengono talvolta incorporati nell'enunciato dei teoremi di Sylow.

Lemma 2.4.3. *Sia $H \leqslant G$ un p-sottogruppo di un gruppo finito G. Allora vale:*

$$[N_G(H) : H] = [G : H] \mod p\,.$$

Dimostrazione. Se H è banale, i due valori sono uguali, quindi non c'è niente da dimostrare. Supponiamo allora che H non sia banale, e consideriamo l'azione di H sull'insieme G/H dei laterali di H in G, data dalla posizione

$$h * xH = hxH\,.$$

Osserviamo che un laterale xH è fissato dall'azione se e solo se, per ogni $h \in H$ si ha $hxH = xH$. Ragionando come nella dimostrazione del terzo teorema di Sylow, concludiamo che questo è vero se e solo se $x^{-1}hx \in H$, per ogni $h \in H$, i.e. se e solo se $x \in N_G(H)$. Il risultato segue dal solito lemma sui punti fissi delle azioni dei p-gruppi. □

Proposizione 2.4.4. *Sia G un gruppo finito, e H un p-sottogruppo di G non di Sylow. Allora esiste un altro p-sottogruppo H' di G che contiene H come sottogruppo normale, tale che $[H' : H] = p$.*

Dimostrazione. Poiché il p-sottogruppo H non è Sylow, per il lemma precedente p divide l'indice $[N_G(H) : H]$. Quindi, per il teorema di Cauchy, esiste un sottogruppo

$$H_1 \leqslant N_G(H)/H$$

di ordine p. La sua controimmagine rispetto alla proiezione canonica

$$N_G(H) \longrightarrow N_G(H)/H$$

è un sottogruppo H' di $N_G(H)$ che contiene H come suo sottogruppo normale, con $[H' : H] = p$. □

Corollario 2.4.5. *Sia G un gruppo finito di ordine $p^k m$, con p primo, e $(m, p) = 1$. Allora, per ogni $i = 1, \dots, k$ vi è un p-sottogruppo di G di ordine p^i, e se $i < k$ esso è contenuto come sottogruppo normale in un p-sottogruppo di G di ordine p^{i+1}.*

Dimostrazione. Si procede per induzione, dove la base dell'induzione è fornita dal teorema di Cauchy, e il passo induttivo dalla proposizione precedente. □

2.4.2 *Esempi di sottogruppi di Sylow*

Come esempio di applicazione dei teoremi di Sylow, studiamo i sottogruppi di Sylow del gruppo simmetrico S_5, del gruppo alterno A_5 e del gruppo diedrale D_6.

Sottogruppi di Sylow di S_5

Il gruppo simmetrico S_5 è composto da $5! = 120 = 2^3 \cdot 3 \cdot 5$ elementi, quindi dovremo studiare i p sottogruppi di Sylow, per $p = 2, 3, 5$. Scriviamo n_p per il numero di p-sottogruppi di Sylow.

I 5-sottogruppi di Sylow hanno ordine 5. Dal terzo teorema di Sylow, si osserva che n_5 divide 24 e $n_5 \equiv 1 \pmod 5$. I valori possibili sono 1 e 6. Si vede immediatamente che $n \neq 1$. Infatti, gli elementi di periodo 5 di S_5 sono tutti e soli i 5-cicli, ed essi sono esattamente $(5 \cdot 4 \cdot 3 \cdot 2)/5 = 24$. Quindi i 5-sottogruppi di Sylow sono 6, e, per il secondo teorema di Sylow, sono tutti e soli i sottogruppi di S_5 coniugati con gruppo ciclico

$$P_5 = \langle (12345) \rangle \leqslant S_5 \,.$$

I 3-sottogruppi di Sylow hanno ordine 3. Dal terzo teorema di Sylow, si osserva che n_3 divide 40 e $n_3 \equiv 1 \pmod 3$. I valori possibili sono 1, 4, 10 e 40. Per il teorema di Lagrange, presi due 3-sottogruppi di Sylow, essi hanno sicuramente intersezione banale. Pertanto, per averne 40, sarebbero necessari 80 elementi di periodo 3, e questo chiaramente non può essere vero. D'altro canto, se i 3-sottogruppi di Sylow fossero

al più 4, vi dovrebbero essere al più 8 elementi di periodo 3, e anche questo non è vero. Infatti, gli elementi di periodo 3 sono tutti e soli i 3-cicli di S_5, ed essi sono esattamente $(5 \cdot 4 \cdot 3)/3 = 20$. Con questi si formano i 10 3-sottogruppi di Sylow, coniugati con gruppo ciclico

$$P_3 = \langle (123) \rangle \leqslant S_5 \, .$$

Infine, i 2-sottogruppi di Sylow hanno ordine $2^3 = 8$. Dal terzo teorema di Sylow, si osserva che n_2 divide 15 e $n_2 \equiv 1 \pmod 2$. I valori possibili sono 1, 3, 5 e 15. Ora, gli elementi non banali di questi sottogruppi potranno avere periodo 2 o 4, poiché chiaramente non vi sono elementi di periodo 8 in S_5. Gli elementi di periodo 2 sono quelli con struttura ciclica (ab) o $(ab)(cd)$, quelli di periodo 4 sono necessariamente dei 4-cicli come $(abcd)$. Si calcola facilmente che vi sono più di 35 elementi di periodo 2 o 4, pertanto n_2 non potrà essere 5, né meno di 5. Infatti, se i 2-Sylow fossero 5, e se pure avessero intersezione banale, vi sarebbero 35 elementi di periodo 2 o 4. Quindi i 2-sottogruppi di Sylow sono 15. Per determinarli, basti osservare che

$$P_2 = \langle (1234), (12)(34) \rangle \leqslant S_5 \, .$$

ha esattamente 8 elementi. Esso è isomorfo al diedrale D_4. Ora, per il secondo teorema di Sylow, i 15 2-sottogruppi di Sylow si possono ottenere prendendo tutti i sottogruppi coniugati con P_2.

Sottogruppi di Sylow di A_5

Il gruppo alterno A_5 è composto da $5!/2 = 60 = 2^2 \cdot 3 \cdot 5$ elementi, quindi dovremo studiare i p sottogruppi di Sylow, per $p = 2, 3, 5$. Scriviamo n_p per il numero di p-sottogruppi di $Sylow$.

Per quanto riguarda i 5-sottogruppi di Sylow, procediamo in maniera del tutto analoga al caso di S_5. Dal terzo teorema di Sylow, si ha che n_5 divide 24 e $n_5 \equiv 1 \pmod 5$, da cui $n_5 \in \{1, 6\}$. Considerando ancora i 24 5-cicli, si formano i sei 5-sottogruppi di Sylow, ciclici di ordine 5, coniugati con P_5.

Anche per quanto riguarda i 3-sottogruppi di Sylow, si ha che n_3 divide 20 e $n_3 \equiv 1 \pmod 3$, da cui $n_3 \in \{1, 4, 10\}$. Considerando i 20 3-cicli, si formano i dieci 3-sottogruppi di Sylow, ciclici di ordine 3, coniugati con P_3.

Concludiamo la nostra analisi con i 2-sottogruppi di Sylow. Questi hanno ordine 4, e il loro numero è un numero dispari che divide 15, ovvero $n_2 \in \{1, 3, 5, 15\}$. Si osserva immediatamente che le permutazioni pari di S_5 di periodo 2 sono quelle che hanno struttura ciclica $(ab)(cd)$. Esse sono

$$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \cdot \frac{1}{2} = 30 \, .$$

con cui si formano quindici 3-sottogruppi di Sylow, coniugati con, e pertanto isomorfi al, gruppo di Klein:

$$K = \{id, (12)(34), (13)(24), (14)(23)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2, \, .$$

Sottogruppi di Sylow di D_6

Consideriamo il gruppo diedrale di ordine $12 = 2^2 \cdot 3$ dato dalla presentazione

$$D_6 = \langle \rho, \sigma \mid \rho^6, \sigma^2, \rho\sigma\rho\sigma \rangle .$$

Per quanto riguarda i 2-sottogruppi di Sylow, essi hanno ordine 4. Sappiamo che il loro numero n_2 divide 3 ed è $n_1 \equiv 1 \pmod 2$; pertanto $n_2 \in \{1, 3\}$. Si verifica facilmente che non vi sono elementi di ordine 4 in D_6, quindi i 2-sottogruppi di Sylow sono isomorfi al gruppo di Klein $K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, e ognuno di essi è generato da due elementi di periodo 2. Gli elementi di periodo 2 sono ρ^3, che commuta con tutti gli altri elementi di D_6, e le riflessioni $\sigma\rho^i$, con $i = 0, 1, \ldots, 5$. In conclusione, troviamo i tre 2-sottogruppi di Sylow:

$$\begin{aligned} \langle \rho^3, \sigma \rangle &= \{\mathrm{id}, \rho^3, \sigma, \sigma\rho^3\}, \\ \langle \rho^3, \sigma\rho \rangle &= \{\mathrm{id}, \rho^3, \sigma\rho, \sigma\rho^4\}, \\ \langle \rho^3, \sigma\rho^2 \rangle &= \{\mathrm{id}, \rho^3, \sigma\rho^2, \sigma\rho^5\}. \end{aligned}$$

Per quanto riguarda i 3-sottogruppi di Sylow, essi hanno ordine 3, e sono pertanto gruppi ciclici. Sappiamo che il loro numero n_3 divide 4 ed è $n_3 \equiv 1 \pmod 3$; pertanto $n_3 \in \{1, 4\}$. Gli elementi di ordine 3 in D_6 sono ρ^2 e ρ^4, che formano quindi l'unico 3-sottogruppo di Sylow:

$$\langle \rho^2 \rangle = \langle \rho^4 \rangle = \{\mathrm{id}, \rho^2, \rho^4\},$$

che per il secondo teorema di Sylow, è normale in D_6.

2.4.3 *Sottogruppi di Sylow normali*

Come si accennava nell'introduzione, un gruppo abeliano finito può essere espresso come prodotto diretto dei suoi p-sottogruppi massimali. Questo dipende solo dal fatto che nel caso abeliano, ogni sottogruppo è normale. Infatti, il risultato analogo vale anche per un gruppo finito G non necessariamente abeliano, a patto che tutti i suoi sottogruppi di Sylow siano normali (e di conseguenza unici, cfr. secondo teorema di Sylow). Nel caso finito, questa condizione caratterizza i cosiddetti *gruppi nilpotenti*, la cui trattazione esula dagli scopi di queste note.[2]

Lemma 2.4.6. *Sia* G *un gruppo finito, e siano* $p \neq q$ *sono fattori primi dell'ordine di* G*, con il numero dei* p*-Sylow e dei* q*-Sylow uguali a* 1*. Allora gli elementi del* p*-Sylow* P *commutano con gli elementi del* q*-Sylow* Q*.*

Dimostrazione. Per il teorema di Lagrange, l'intersezione di P e Q è banale. Consideriamo allora due elementi $x \in P$ e $y \in Q$. Poiché P è normale in G si ha: $x(yx^{-1}y^{-1}) \in P$, e poiché Q è normale in G si ha: $(xyx^{-1})y^{-1} \in Q$. Quindi $xyx^{-1}y^{-1}$ sta nell'intersezione di P e Q, da cui $xyx^{-1}y^{-1} = 1_G$. □

2 Si veda ad esempio [**?**, II.7].

Teorema 2.4.7. *Se tutti i sottogruppi di Sylow del gruppo finito* G *sono normali in* G*, allora* G *è isomorfo al loro prodotto diretto.*

Dimostrazione. Qui dimostreremo che G è isomorfo al prodotto diretto esterno, ma è anche facile vedere che G coincide con il prodotto diretto interno dei suoi sottogruppi di Sylow.

Siano $P_1, \cdots P_k$ i sottogruppi di Sylow di G e consideriamo la mappa

$$P_1 \times \cdots \times P_k \xrightarrow{\phi} G$$

che associa alla k-upla $(x_1, \ldots, x_k)$ il prodotto (in G) $x_1 \cdots x_k$. Grazie al lemma precedente, ϕ è chiaramente un omomorfismo di gruppi ed è facile vedere che è iniettivo. Infine, le cardinalità (finite) di dominio e codominio coincidono, da cui ϕ è anche suriettivo. □

Esercizio 2.4.8. Siano H e K sottogruppi normali di un gruppo G tali che $H \cap K = 1$. Allora il prodotto diretto $H \times K$ è isomorfo al sottogruppo HK.

2.4.4 *Classificazione dei gruppi abeliani finiti*

In questa sezione ci occupiamo della classificazione dei gruppi abeliani finiti. L'approccio classico alla classificazione dei gruppi abeliani utilizza metodologie proprie dell'algebra commutativa. Noi, in questo contesto, preferiamo sviluppare l'argomento dal punto di vista dello studio dei p-sottogruppi come caso particolare del caso non abeliano.

Cominciamo con un facile corollario del Teorema 2.4.7.

Corollario 2.4.9. *Sia* A *un gruppo abeliano finito, con*

$$|A| = n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Allora esiste un isomorfismo di gruppi

$$A \simeq A_{p_1} \times \cdots \times A_{p_k}$$

con $A_{p_i} \leqslant A$ p_i*-sottogruppi di Sylow di* A*, e* $|A_{p_i}| = p_i^{\alpha_i}$*, per ogni* $i = 1, \ldots, k$.

Dimostrazione. Poiché A è abeliano, ogni sottogruppo di A è normale. La tesi segue immediatamente dal teorema. □

Per classificare i gruppi abeliani finiti è allora sufficiente classificare i suoi p-sottogruppi di Sylow, A_{p_i} i.e. le sue componenti primarie. Per questo motivo, il resto della sezione è dedicato allo studio dei p-gruppi abeliani finiti.

Per un gruppo ciclico finito, è noto che i suoi sottogruppi sono univocamente determinati dal loro ordine. Per i p-gruppi abeliani finiti vale una sorta di viceversa.

Lemma 2.4.10. *Se A è un p-gruppo abeliano finito che ammette un unico sottogruppo H con $|H| = p$, allora A è ciclico.*

Dimostrazione. Procediamo per induzione su $|A| = p^\alpha$.

Per $\alpha = 1$, $|A| = p$ e quindi $A \cong \mathbb{Z}_p$. Sia allora $\alpha > 1$. Considero l'omomorfismo $\phi\colon A \to A$ dato dalla posizione $\phi(a) = a^p$. Immediatamente, per la condizione di unicità fornita nell'ipotesi, si ha che $\mathrm{Ker}(\phi) = H$. Di conseguenza, l'immagine $\phi(A)$ è un sottogruppo proprio non banale di A isomorfo a $\frac{A}{H}$. Per il teorema di Cauchy, $\phi(A)$ ammette un sottogruppo di ordine p, e quindi, per ipotesi di induzione, $\frac{A}{H} \cong \phi(A)$ è ciclico.

Sia $\bar{a}H$ un generatore di $\frac{A}{H}$, dimostreremo che $\bar{a}$ è un generatore di A, che pertanto risulterà anch'esso ciclico. In effetti, $H \leqslant \langle \bar{a} \rangle$, perché $\langle \bar{a} \rangle$ contiene un sottogruppo di ordine p, che, essendo anche sottogruppo di A, per l'unicità deve coincidere con H. Dato allora $a \in A$, esiste un intero i tale che $a \in \bar{a}^i H$. Ma, come visto, anche gli elementi di H sono potenze di $\bar{a}$, pertanto si ha

$$a = \bar{a}^i h = \bar{a}^i \bar{a}^j = \bar{a}^{i+j},$$

per un intero j, e questo conclude la dimostrazione. □

Dal lemma appena visto si ottiene una procedura per scomporre A in un prodotto diretto con il primo fattore costituito da un suo p-sottogruppo ciclico di ordine massimale.

Lemma 2.4.11. *Se A è un p-gruppo abeliano finito, e $C \leqslant A$ ciclico di ordine massimale, allora esiste $H \leqslant A$ tale che la funzione*

$$C \times H \xrightarrow{\phi} A$$

definita dalla posizione $\phi(c, h) = ch$ sia un isomorfismo di gruppi.

Dimostrazione. Procediamo per induzione su $|A|$.

Se $|A| = 1$, non c'è niente da dimostrare. Supponiamo allora che sia $|A| > 1$. Se A è ciclico, ancora non c'è niente da dimostrare. Sia quindi A non ciclico, e necessariamente $|A| \geqslant p^2$ (perché?). Esiste allora un sottogruppo $K \leqslant A$ non contenuto C di ordine p (altrimenti ci sarebbe un unico sottogruppo di A di ordine p, quindi A sarebbe ciclico per il lemma precedente).

Consideriamo il gruppo quoziente $\frac{A}{K}$ con la proiezione canonica

$$A \xrightarrow{\pi} \frac{A}{K}.$$

Si ha che π ristretta a C è un monomorfismo. Infatti, se $\pi(c) = 1$ per $c \in C$, allora $c \in C \cap K = \{1\}$. Quindi, chiaramente, la sua immagine isomorfa $\pi(C)$ è un sottogruppo di $\frac{A}{K}$ ciclico di ordine massimale.

Applico l'ipotesi di induzione ad $\frac{A}{K}$, che stabilisce che esiste $H' \leqslant \frac{A}{K}$ tale che la funzione

$$\pi(C) \times H' \xrightarrow{\phi'} \frac{A}{K}$$

definita dalla posizione $\phi'(\bar{c}, h') = \bar{c}h'$ sia un isomorfismo.

Sia allora $H = \pi^{-1}(H')$, e sia ϕ definito come nell'enunciato del lemma. Poiché i gruppi sono abeliani, ϕ è chiaramente un omomorfismo di gruppi. Si verifica facilmente che è in effetti un monomorfismo. Infatti, consideriamo una coppia (c, h) tale che $\phi(c, h) = ch = 1$. Si ha che $1 = \pi(ch) = \pi(c)\pi(h) = \phi'(\pi(c), \pi(h))$. Ma ϕ' è un isomorfismo (e dunque iniettivo), per cui $(\pi(c), \pi(h)) = (1, 1)$. Come già osservato, π ristretta a C è un iniettiva, da cui $c = 1$. Immediatamente deduciamo $1 = ch = 1h = h$, i.e. ϕ è un monomorfismo. La suriettività di ϕ segue dall'osservare che, poiché $|C \cap H| = 1$, $|A| = |C| \cdot |H|$. □

Proposizione 2.4.12. *Se A è un p-gruppo abeliano finito, allora A è isomorfo un prodotto diretto di p-gruppi ciclici. Tale scomposizione è essenzialmente unica.*

Dimostrazione. Se A non è già ciclico, il lemma precedente garantisce che vi sia un isomorfismo $A \cong C \times A'$. Poiché $|A'| < |A|$, posso procedere per induzione su $|A|$. Per quanto l'unicità a meno di isomorfismi, se considero un differente sottogruppo $\bar{C}$ di ordine massimale, poiché $|C| = |\bar{C}|$, si ha che $C \cong \bar{C}$, e, ancora, si procede per induzione su $|A|$. □

Teorema 2.4.13 (Classificazione dei gruppi abeliani finiti)**.** *Ogni gruppo abeliano finito A è isomorfo al prodotto diretto di p-gruppi ciclici; più esplicitamente, esistono k numeri primi non necessariamente distinti $p_1, \cdots, p_k$, insieme a k numeri interi positivi $\alpha_1, \cdots, \alpha_k$ tali che A ammette una scomposizione*

$$A \cong C_{p_1^{\alpha_1}} \times \cdots \times C_{p_k^{\alpha_k}}$$

dove i $C_{p_i^{\alpha_i}}$ sono gruppi ciclici di ordine $p_i^{\alpha_i}$. Tale scomposizione è essenzialmente unica.

La dimostrazione per induzione è un facile esercizio di applicazione dei risultati esposti sopra.

2.4.5 *Classificazione dei gruppi con al più 15 elementi*

Per quanto riguarda i gruppi abeliani finiti, come abbiamo visto, è abbastanza semplice enunciare e dimostrare un teorema di classificazione. Questo non deve indurci a pensare che la classificazione dei gruppi finiti in genere sia un problema egualmente trattabile.

In effetti, al momento, la classificazione dei gruppi finiti è un problema di cui non si conosce la soluzione, né si sa se essa semplicemente esista... Un risultato in questa direzione è la classificazione dei gruppi

semplici finiti, ma per dare un'idea della complessità di questa, basti pensare che che essa è racchiusa in decine di migliaia di pagine, distribuite su parecchie centinaia di articoli scientifici pubblicate da un centinaio di autori a partire dagli anni cinquanta del secolo scorso. Inoltre, studiare i gruppi finiti è un'esperienza ricca di sorprese. Ad esempio, a quanto pare, la maggior parte dei gruppi finiti sembra avere ordine una potenza di 2. Ad esempio, in [2], gli autori studiano i gruppi G con $|G| \leqslant 2000$, e scoprono che, su un totale di 49 910 529 484 gruppi, ben 49 487 365 422 hanno ordine $2^{10} = 1\,024$, ben il 92, 2% del totale. Il lettore capirà quindi il perché, nel classificare i gruppi finiti, ci fermeremo a $15 < 16 = 2^4$, e la classificazione è già abbastanza involuta così.

Sia allora dato un gruppo G, con $|G| = n \leqslant 15$.

Se $n = 1$.

In questo caso, G è necessariamente il gruppo banale.

Se n *è un numero primo.*

Anche in questo caso la soluzione è semplice. Sappiamo infatti che se $|G| = p$ primo, G è necessariamente ciclico. Le classi di isomorfismo sono quindi i gruppi $\mathbb{Z}_p$:

$$\mathbb{Z}_2\,,\ \mathbb{Z}_3\,,\ \mathbb{Z}_5\,,\ \mathbb{Z}_7\,,\ \mathbb{Z}_{11}\,,\ \mathbb{Z}_{13}\,.$$

Restano da analizzare i valori di $n = 4, 6, 8, 9, 10, 12, 14, 15$.

Se $n = 4$.

Se G ha un elemento di periodo 4, $G \cong \mathbb{Z}_4$. Supponiamo allora che tutti gli elementi non banali di G abbiano periodo 2. Vale il seguente lemma, la cui dimostrazione è immediata.

Lemma 2.4.14. *Se in un gruppo* G *tutti gli elementi hanno periodo* 2*, il gruppo è abeliano.*

Dalla classificazione dei gruppi abeliani finiti (Proposizione 2.4.12) concludiamo che $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Se $n = 6, 10, 14, 15$.

In questo caso ci viene in aiuto una proposizione.

Proposizione 2.4.15. *Siano* p *e* q *due numeri primi, con* $p > q$*, e sia* G *un gruppo con* $|G| = p \cdot q$*. Si studiano due casi:*

(i) *Se* $q \nmid (p-1)$*, allora* $G \cong \mathbb{Z}_{pq}$.

(ii) *Se* $q \mid (p-1)$, *allora esistono esattamente due classi di isomorfismo: o* $G \cong \mathbb{Z}_{pq}$, *oppure* $G \cong K_{pq}$,

$$K_{pq} = \langle c, d \mid c^p, d^q, c^s d c^{-1} d^{-1} \rangle$$

dove $S \not\equiv 1 \pmod{p}$ *e* $s^q \equiv 1 \pmod{p}$

Dimostrazione. Vedi [4, Proposition 6.1]. □

Quindi, per $|G| = 6 = 3 \cdot 2$, poiché $2 \mid (3-1)$ siamo nel secondo caso. Di conseguenza abbiamo due possibilità: o $G \cong \mathbb{Z}_6$ è ciclico, oppure $G \cong K_6$. Ma è facile notare che

$$K_6 = \langle c, d \mid c^3, d^2, c^2 d c^{-1} d^{-1} \rangle \cong \langle \rho, \sigma \mid \rho^3, \sigma^2, \rho\sigma\rho\sigma \rangle = D_3 .$$

Per provarlo, si consideri la posizione $c \mapsto \rho^2$ e $d \mapsto \sigma$ e, mediante la proprietà universale delle presentazioni di gruppi (Proposizione 2.2.23) si mostri che tale posizione si estende a un isomorfismo.

Procedendo in modo analogo, si prova che

- se $|G| = 10$, poiché $2 \mid (5-1)$, si ha che $G \cong \mathbb{Z}_{10}$ o $G \cong D_5$,
- se $|G| = 14$, poiché $2 \mid (7-1)$, si ha che $G \cong \mathbb{Z}_{14}$ o $G \cong D_7$,
- se $|G| = 15$, poiché $3 \nmid (5-1)$, si ha solo il caso $G \cong \mathbb{Z}_{10}$.

Se $n = 9$.

Anche in questo caso, ci viene in aiuto una proposizione.

Proposizione 2.4.16. *Sia* G *un gruppo, con* $|G| = p^2$, *dove* p *è un numero primo. Allora* G *è abeliano.*

Dimostrazione. Per il Corollario 2.3.36, il centro $Z(G)$ di G non è banale; per il teorema di Lagrange ci sono due casi possibili: o $|Z(G)| = p$, oppure $|Z(G)| = p^2$. Verifichiamo che il primo caso non si verifica mai, e concludiamo che $G = Z(G)$ è abeliano. Se fosse $|Z(G)| = p$, potrei considerare il gruppo quoziente $G/Z(G)$, che avrebbe ordine $p^2/p = p$, e sarebbe pertanto ciclico. Sia $wZ(G)$ un suo generatore. Poiché i laterali formano una partizione del gruppo, presi due elementi $x, y \in G$, esisteranno $z_1, z_2 \in Z(G)$ e $n_1, n_2 \in \{0, 1, \dots, p-1\}$ tali che $x = w^{n_1} \cdot z_1$ e $y = w^{n_2} \cdot z_2$. Ma allora si avrebbe

$$x \cdot y = w^{n_1} \cdot z_1 \cdot w^{n_2} \cdot z_2 = w^{n_1+n_2} \cdot z_1 \cdot z_2 = w^{n_2} \cdot z_2 \cdot w^{n_1} \cdot z_1 = y \cdot x ,$$

i.e. G abeliano, da cui $Z(G) = G$, contraddizione. □

La proposizione ci permette ora di utilizzare il teorema di classificazione dei gruppi abeliani finiti per classificare i gruppi di ordine 9, concludere che i casi possibili sono due: o $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ oppure $G \cong \mathbb{Z}_9$.

Se $n = 12$.

Se G è abeliano, si hanno i casi:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \qquad e \qquad G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}\,.$$

Se G non abeliano, si hanno i casi:

$$G \cong A_4\,, \qquad G \cong D_6 \qquad e \qquad T\,,$$

dove $T = \langle a, b \mid a^6, a^3b^{-2}, abab^{-1}\rangle$.

Per una descrizione più esplicita del gruppo T, si risolva il prossimo esercizio.

Esercizio 2.4.17. Dimostrare che il gruppo T presentato sopra è isomorfo al sottogruppo di $S_3 \times \mathbb{Z}_4$ generato dagli elementi $((123), [2])$ e $((12), [1])$.

Per una dimostrazione del fatto che non vi sono altri gruppi di ordine 12, si possono consultare i testi [4] e [1].

Se $n = 8$.

Dulcis in fundo, il caso $n = 8 = 2^3$. Se G è abeliano, si hanno i casi:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_s \qquad G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \qquad G \cong \mathbb{Z}_8\,.$$

Se G non è abeliano, sicuramente abbiamo i casi $G \cong D_4$, il gruppo diedrale, e $G \cong Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, il gruppo moltiplicativo dei quaternioni. Un utile esercizio è verificare che

$$Q_8 \cong \langle a, b \mid a^4, a^2b^{-2}, abab^{-1}\rangle$$

Non vi sono altri gruppi non abeliani di ordine 8.

Dimostrazione. Sia G gruppo non abeliano, con $|G| = 8$. G, ha almeno un elemento di periodo 4. Infatti, non può avere elementi di periodo 8 perché sarebbe ciclico, e quindi abeliano, e non può avere tutti gli elementi non banali di periodo 2, perché, come già visto nel caso $n = 4$, ancora sarebbe abeliano.

Sia allora $a \in G$ di periodo 4. Chiaramente si ha che $\langle a\rangle$ è normale in G, perché ha indice 2. Considero $b \notin G$; si ha che $b^2 \in \langle a\rangle$, poiché il gruppo quoziente $G/\langle a\rangle$ ha ordine 2.

Ora, poiché le classi laterali formano una partizione di G, per ogni $x \in G$, $x = b^i \cdot a^j$, con $i = 0, \ldots 3$ e $j = 0, 1$, i.e. a, b generano G.

Poiché $b^2 \in \langle a\rangle$, analizziamo le possibilità:

$$b^2 = 1\,, \quad b^2 = a \quad b^2 = a^2 \quad b^2 = a^3\,.$$

Si vede immediatamente che il secondo e il quarto caso non so possono verificare. Infatti, se fosse $b^2 = a$, il periodo di b sarebbe 8, e il gruppo

G abeliano. Analogamente, se fosse $b^2 = a^3$, si avrebbe $b^6 = a^9 = a$, da cui il periodo di b^3 sarebbe ancora 8, e G ancora abeliano.

Un'ultima considerazione: poiché $\langle a \rangle$ normale, si ha che $bab^{-1} = a^h$, per un certo h. Procedendo in una analisi dei casi, si evince immediatamente che $h = 3$.

Possiamo riassumere quanto visto fin qui considerando due soli casi.

Caso 1

$$\begin{aligned} G &\cong \langle a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^3 \rangle \\ &= \langle a, b \mid a^4, a^2 b^{-2}, abab^{-1} \rangle \\ &\cong Q_8 \end{aligned}$$

Caso 2

$$\begin{aligned} G &\cong \langle a, b \mid a^4 = 1, b^2 = 1, bab^{-1} = a^3 \rangle \\ &= \langle a, b \mid a^4, b^2, abab \rangle \\ &\cong D_4 \end{aligned}$$

La verifica è una facile applicazione della proprietà universale delle presentazioni di gruppi.

□

2.4.6 *Provare che un gruppo finito non è semplice*

Ricordiamo che un gruppo G viene detto *semplice* se i suoi unici sottogruppi normali sono il gruppo banale $\{1\} \leqslant G$ e G stesso. In questa sezione analizziamo alcune tecniche per dimostrare che un gruppo finito non sia semplice. Si tratta di diverse applicazioni dei teoremi di Sylow.

Mostrare che esiste un unico p*-sottogruppo di Sylow*

Il secondo teorema di Sylow implica che se per un certo divisore p dell'ordine $|G|$ del gruppo, esiste un unico p-sottogruppo di Sylow, allora tale sottogruppo è normale. Quindi, una strategia per dimostrare che un gruppo finito G non è semplice consiste nel dimostrare che ammette un unico p-sottogruppo di Sylow. Questa tecnica si applica di solito più facilmente quando l'ordine $|G|$ del gruppo è abbastanza grande, ed è spesso conveniente cominciare con il calcolo del numero n_p di p-sottogruppi di Sylow a partire dai primi p più grandi.

Esempio 2.4.18. *Se* G *è un gruppo con 28 elementi, allora* G *non può essere semplice.*

Poiché $28 = 2^2 \cdot 7$, per il terzo teorema di Sylow, il numero n_7 dei 7-sottogruppi di Sylow deve essere congruo a 1 (mod7) e deve dividere 4. Quindi, l'unica possibilità è $n_7 = 1$, ovvero c'è un unico 7-sottogruppo di Sylow, che pertanto è normale.

Esempio 2.4.19. *Se* G *è un gruppo con 56 elementi, allora* G *non può essere semplice.*

Poiché $56 = 2^3 \cdot 7$, per il terzo teorema di Sylow, il numero n_7 dei 7-sottogruppi di Sylow deve essere congruo a 1 (mod7) e deve dividere 8. Quindi si ha $n_7 \in \{1, 8\}$. Se $n_7 = 1$, l'unico 7-sottogruppo di Sylow è normale, e G non è semplice. Supponiamo allora che $n_7 \neq 1$. Gli otto 7-sottogruppi di Sylow hanno ordine 7. Quindi sono sicuramente ciclici, e hanno intersezione banale per il teorema di Lagrange. Quindi G contiene esattamente $6 \cdot 8 = 48$ elementi di ordine 7. Con i restanti $56 - 48 = 8$ elementi, è possibile produrre esattamente un 2-sottogruppo di Sylow, che pertanto è normale.

Mostrare che $Ker(\varphi)$ *non è banale, per l'omomorfismo* $\varphi\colon G \to \mathsf{Sym}(X)$ *determinato da una opportuna azione*

Azione di traslazione. Sia H un sottogruppo di G, con $[G : H] = n$, tale che $|G| \nmid n!$. Consideriamo l'azione di traslazione di G sull'insieme delle classi laterali $X = G/H$ descritta nell'Esempio 2.3.24. A tale azione corrisponde canonicamente l'omomorfismo $\varphi\colon G \to \mathsf{Sym}(X) \cong S_n$, che assegna all'elemento $g \in G$ la permutazione $\varphi(g)$ che manda il laterale xH nel laterale gxH. E' facile verificare che

$$\mathrm{Ker}(\varphi) = \bigcap_{x \in G} xHx^{-1},$$

Di conseguenza,

- $\mathrm{Ker}(\varphi) \neq \{1\}$, altrimenti φ sarebbe iniettiva, e poiché $|G| \nmid n!$, si avrebbe una contraddizione.
- $\mathrm{Ker}(\varphi) \neq G$, altrimenti $|G| = |\bigcap_{x \in G} xHx^{-1}| \leqslant |H|$, ancora una contraddizione.

Una possibile applicazione si ha quando si considera un gruppo finito G, e H p-sottogruppo di Sylow. In questo caso, l'ultima ipotesi può essere riformula chiedendo $|G| > n!$, piuttosto che $|G| \nmid n!$.

Esempio 2.4.20. Sia G gruppo, con $|G| = 36 = 2^2 \cdot 3^2$, e sia $P \leqslant G$ un 3-sottogruppo di Sylow di G. Poiché l'indice di P in G è 4, l'azione di traslazione sui laterali determina un omomorfismo

$$\varphi\colon G \to S_4$$

Il nucleo $\ker(\varphi) \leqslant G$ non può essere banale, perché in tal caso φ sarebbe iniettiva, il che implicherebbe $36 = |G| \leqslant |S_4| = 24$, assurdo. Quindi $\ker(\varphi) \neq \{1\}$. D'altro canto, dobbiamo anche escludere che

$\ker(\varphi)$ coincida con l'intero gruppo G, perché in tal caso si avrebbe $36 = |G| = |\bigcap_{x\in G} xPx^{-1}| \leqslant |P| = 9$, assurdo. Quindi $\ker(\varphi) < G$ è un sottogruppo normale proprio di G, e G non è semplice.

Azione di coniugio. Consideriamo l'azione del gruppo finito G sull'insieme X dei suoi p-sottogruppi di Sylow. Anche in questo caso, l'idea è studiare il nucleo dell'omomorfismo associato all'azione.

Esempio 2.4.21. Sia G gruppo, con $|G| = 72 = 2^3 \cdot 3^2$, e sia n_3 il numero dei suoi 3-sottogruppi di Sylow. Per il terzo teorema di Sylow, $n_3 \equiv 1 \mod 3$, e poiché n_3 divide l'ordine di G, le uniche possibilità sono 1 e 4. Se $n_3 = 1$ allora c'è un unico sottogruppo di Sylow di ordine 9, che pertanto è normale. Se invece $n_3 = 4$ l'azione di coniugio sull'insieme dei 3-sottogruppi di Sylow fornisce un omomorfismo

$$\varphi\colon G \to S_4\,.$$

Chiaramente φ non può essere un monomorfismo, perché $|G|$ non divide $4! = 24$. D'altro canto, non può neanche essere $\ker(\varphi) = G$, perché questo implicherebbe che, per ogni 3-sottogruppo di Sylow P, $gPg^{-1} = P$, che non può essere perché P non è un sottogruppo normale. Quindi $\ker(\varphi) < G$ è un sottogruppo normale proprio di G, e G non è semplice.

Trovare un sottogruppo di H di G che abbia indice il più piccolo divisore primo di $|G|$

Un tale sottogruppo, infatti, è sempre normale in G. Per dimostrarlo, consideriamo l'azione di G sull'insieme dei laterali di H in G, e l'omomorfismo a essa associato $\varphi\colon G \to S_p$, dove $p = [G : H]$. Sia $K = \ker(\varphi)$; poiché $kH = H$ per ogni $k \in K$, si ha che $K \subseteq H$. Poniamo ora $[H : K] = m$. Per il primo teorema di isomorfismo, il gruppo G/K è isomorfo a un sottogruppo di S_n, e pertanto il suo ordine divide l'ordine di S_p, cioè $p!$. Poiché inoltre

$$[G : K] = [G : H][H : K] = pm$$

si ha che $pm \mid p!$, da cui $m \mid (p-1)!$. Se indichiamo con q un fattore primo di m, si ha che $p < m$ e $p \,||G|$, da cui m non ha fattori primi, i.e. $m = 1$. Allora $H = K$ è normale in G.

Esempio 2.4.22. Per ogni intero $n > 2$, S_n non è semplice. Infatti contiene un sottogruppo normale A_n, con $[S_n : A_n] = 2$.

3

TEORIA DEI CAMPI

In questo capitolo introdurremo le basi della teoria delle estensioni di campi.

3.1 QUALCHE RICHIAMO DI TEORIA DEGLI ANELLI COMMUTATIVI UNITARI

Ricordiamo che CRing è la categoria degli anelli commutativi unitari e omomorfismi di anelli unitari (laddove Ring denotava la categoria degli anelli unitari).

In questo contesto, gli ideali destri e sinistri coincidono, e gli ideali principali ammettono una descrizione semplificata. Riportiamo, senza dimostrazione, alcuni risultati.

Lemma 3.1.1. *Sia* $I \neq (1)$ *un ideale di un anello commutativo unitario* R. *Le seguenti affermazioni sono equivalenti:*

(i) L'anello quoziente R/I *è un dominio;*

(ii) Per ogni coppia $a, b \in R$ *si ha:*

$$ab \in I \qquad \Rightarrow \qquad a \in I \text{ } \textit{oppure} \text{ } b \in I\,.$$

Un ideale che soddisfi queste due condizioni equivalenti è chiamato ideale primo.

Ricordiamo che per *dominio* (di integrità) intendiamo un anello commutativo unitario privo di divisori dello 0.

Lemma 3.1.2. *Sia* $I \neq (1)$ *un ideale di un anello commutativo unitario* R. *Le seguenti affermazioni sono equivalenti:*

(i) L'anello quoziente R/I *è un campo;*

(ii) Per ogni altro ideale J *di* R *si ha:*

$$I \subseteq J \qquad \Rightarrow \qquad J = I \text{ } \textit{oppure} \text{ } J = R\,.$$

Un ideale che soddisfi queste due condizioni equivalenti è chiamato ideale massimale.

Dai due lemmi segue immediatamente che se I è ideale massimale, allora è ideale primo.

L'oggetto terminale della categoria Ring degli anelli unitari (così come della categoria CRing degli anelli commutativi unitari) è lo 0-anello; l'oggetto iniziale della categoria Ring degli anelli unitari (così

come della categoria CRing degli anelli commutativi unitari) è l'anello $\mathbb{Z}$ degli interi. In effetti, per ogni altro anello commutativo unitario R, vi è un solo modo di definire un omomorfismo di anelli unitari

$$\phi_R \colon \mathbb{Z} \to R$$

poiché una volta assegnati $\phi_R(0) = 0_R$ e $\phi_R(1) = 1_R$, l'omomorfismo ϕ_R si estende univocamente a tutti gli interi.

Per studiare efficacemente i campi, conviene spesso considerare la categoria Fld dei campi come una sottocategoria della categoria CRing degli anelli commutativi unitari. In effetti, per quello che riguarda i morfismi, un *omomorfismo* di campi è semplicemente un omomorfismo di anelli unitari, poiché tali morfismi preservano automaticamente sia la commutatività che gli inversi moltiplicativi. Tuttavia il lettore difficilmente avrà sentito parlare di *omomorfismi* di campi. La ragione sarà chiara immediatamente dopo il prossimo lemma.

Lemma 3.1.3. *Sia $f \colon K \to R$ un omomorfismo di anelli unitari, dove R non è lo 0-anello e K è un campo. Allora f è iniettivo.*

Dimostrazione. Il nucleo di f è un ideale del campo K, e diverso da K perché in tal caso avrei $0_R = f(0_K) = f(1_K) = 1_R$, che non può essere poiché R non è lo 0-anello. Quindi, necessariamente è $\ker(f) = (0)$, i.e. f è iniettivo. □

Quindi, in particolare, ogni morfismo nella categoria Fld è un monomorfismo.

Definizione 3.1.4. *Un monomorfismo di campi $F \to E$ è chiamato* estensione E *di* F.

Una nozione che useremo diffusamente nel seguito è quella di sottocampo generato da un insieme.

Definizione 3.1.5. *Sia E un campo e $S \subseteq E$ un suo sottoinsieme. Il sottocampo di E generato da S è l'intersezione di tutti i sottocampi di E che contengono S.*

In particolare, se E è un campo, $S \subseteq E$ un suo sottoinsieme e $F \hookrightarrow E$ un sottocampo, il sottocampo $F(S)$ di E generato da S su F è l'intersezione di tutti i sottocampi di E che contengono $S \cup F$.

Se $S = \{s_1, \ldots, s_n\}$ è un insieme finito, per indicare $F(S)$ scriveremo $F(s_1, \ldots, s_n)$. In questo caso si dirà che tale campo è finitamente generato *su F.*

Talvolta, è utile avere una descrizione esplicita del sottocampo generato.

Proposizione 3.1.6. *Se E è un campo, $S \subseteq E$ un suo sottoinsieme e $F \hookrightarrow E$ un sottocampo, il sottocampo $F(S)$ di E generato da S coincide con l'insieme E di tutti gli elementi della forma $f(s_1, \ldots, s_k)/g(s_1, \ldots, s_k)$, dove k è un intero positivo, $f, g \in F[x_1, \ldots, x_k]$ sono polinomi, e $g(s_1, \ldots, s_k) \neq 0$.*

Dimostrazione. È chiaro che valgono le inclusioni

$$(F \cup S) \subseteq E \subseteq F(S)\,.$$

Sarà quindi sufficiente mostrare che E è un campo per dedurre $E = F(S)$. La prova di questo fatto è lasciata come esercizio. *Suggerimento: la somma e il prodotto si definiscono nello stesso modo in cui di definiscono somma e prodotto di frazioni algebriche.* □

3.1.1 *Campo dei quozienti di un dominio*

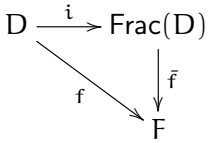
Dato un dominio D, cerchiamo un modo di immergere D in un campo, cioè di definire un monomorfismo anelli unitari da D verso un campo. Questo ci permetterebbe di considerare D sottoanello di tale campo, ovvero di attribuire a ogni elemento di D un inverso moltiplicativo. La soluzione universale di questo problema è detta *campo dei quozienti di* D.

Definizione 3.1.7 (Proprietà universale del campo dei quozienti)**.** *Sia* D *un dominio. Il* campo dei quozienti di D*, detto anche* campo delle frazioni *di* D*, è una coppia* $(\mathsf{Frac}(D), i)$ *dove*

(i) $\mathsf{Frac}(D)$ *è un campo,*

(ii) $i\colon D \to \mathsf{Frac}(D)$ *è un monomorfismo di anelli unitari*

universale rispetto a (i) *e* (ii)*, cioè tale che se* (f, F) *è un'altra coppia con* F *campo e* $f\colon D \to F$ *monomorfismo di anelli unitari, allora esiste un unico monomorfismo* $\bar{f}\colon \mathsf{Frac}(D) \to F$ *tale che* $\bar{f} \circ i = f$



Definire un oggetto attraverso la sua proprietà universale non ne garantisce l'esistenza. Tuttavia, il campo dei quozienti di un dominio può essere facilmente costruito imitando la costruzione dei numeri razionali a partire dall'anello degli interi.

Costruzione 3.1.8*.* Forniamo una traccia della costruzione del campo dei quozienti di un dominio. Lo studente diligente potrà completare i dettagli mancanti.

Sia D un dominio. Consideriamo prima l'insieme $D \times D^\times$, e poi, su questo insieme, la relazione di equivalenza

$$(a, b) \sim (a', b') \text{ se e solo se } ab' - ba' = 0\,.$$

Denotiamo la classe di equivalenza di (a, b) con la frazione $\frac{a}{b}$, e l'insieme quoziente $(D \times D^\times)/\sim$ con $\mathsf{Frac}(D)$. Possiamo definire somma e prodotto:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}\,, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}\,,$$

che insieme a $0 = \frac{0}{1}$ e $1 = \frac{1}{1}$ rendono $\mathsf{Frac}(D)$ un campo. Infine, l'assegnamento $i\colon a \mapsto \frac{a}{1}$ è un omomorfismo iniettivo di anelli unitari:

$$i\colon D \to \mathsf{Frac}(D)$$

che ci permette di identificare D con la sua immagine in $\mathsf{Frac}(D)$. Quest'ultima è costituita dalle frazioni con denominatore uguale a 1. Ovviamente, gli elementi di D diversi da 0 sono invertibili nel campo $\mathsf{Frac}(D)$, con $b^{-1} = \frac{1}{b}$.

Per verificare che la coppia $(\mathsf{Frac}(D), i)$ sia proprio il campo dei quozienti di D, dobbiamo provare che tale coppia è universale, nel senso della Definizione 3.1.7. A questo scopo, consideriamo un'altra coppia (f, F), con F campo e $f\colon D \to F$ omomorfismo iniettivo di anelli unitari. L'assegnamento

$$\bar{f}\colon \mathsf{Frac}(D) \to F \qquad \frac{a}{b} \mapsto f(a)f(b)^{-1}$$

è ben posto e definisce un omomorfismo iniettivo di anelli unitari, con $\bar{f} \circ i = f$. Infine, dato un altro omomorfismo iniettivo di anelli unitari

$$g\colon \mathsf{Frac}(D) \to F\,,$$

tale che $g \circ i = f$, per ogni $\frac{a}{b} \in \mathsf{Frac}(D)$

$$\bar{f}\left(\frac{a}{b}\right) = f(a)f(b)^{-1} = g(i(a))g(i(b))^{-1} = g\left(\frac{a}{1}\right) g\left(\frac{b}{1}\right)^{-1} = g\left(\frac{a}{b}\right).$$

È istruttivo verificare gli esempi che seguono, utilizzando la proprietà universale del campo dei quozienti.

1. Come già accennato, il prototipo del campo dei quozienti di un dominio è la classica costruzione del campo dei razionali a partire dall'anello degli interi:

   $$i\colon \mathbb{Z} \to \mathsf{Frac}(\mathbb{Z}) = \mathbb{Q}$$

   con $i(n) = \frac{n}{1}$.

2. Se F è un campo, si ha $\mathsf{Frac}(F) \cong F$.

3. Se F è un campo, l'anello di polinomi $F[x]$ è un dominio. Il suo campo dei quozienti è chiamato *campo delle funzioni razionali su* F, e viene denotato $F(x)$.[1] Esplicitamente, esso consiste nel campo delle frazioni algebriche $\frac{p(x)}{q(x)}$ dove $p(x)$ e $q(x)$ sono polinomi a coefficienti in F, e $q(x)$ non è il polinomio nullo.

1 La notazione utilizzata è consistente con la Definizione 3.1.5. Questo fatto sarà reso evidente nella trattazione delle estensioni trascendenti semplici.

4. Se D è un dominio, l'anello di polinomi $D[x]$ è a sua volta un dominio, e si ha

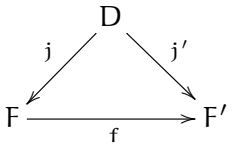
$$\mathsf{Frac}(D[x]) \cong \mathsf{Frac}(D)(x)$$

   i.e. il campo dei quozienti dell'anello di polinomi su un dominio non è altro che il campo delle funzioni razionali sul campo delle frazioni del dominio. Ad esempio $\mathsf{Frac}(\mathbb{Z}[x]) = \mathbb{Q}(x)$.

5. Gli ultimi due esempi si estendono facilmente a un numero finito di variabili, a dare i campi delle funzioni razionali: $F(x, y)$, $F(x, y, z)$, $F(x_1, \cdots, x_n)$ etc.

Osservazione 3.1.9. Il campo dei quozienti può essere definito come oggetto iniziale di una opportuna categoria.

Dato un dominio D, sia Fld^D la categoria avente come oggetti le coppie (F, j), dove F è un campo, e $j\colon D \to F$ è un omomorfismo iniettivo di anelli unitari. Una freccia $f\colon (F, j) \to (F', j')$ è un morfismo (estensione) di campi $F \to F'$ tale che $f \circ j = j'$, o diagrammaticamente:



È sufficiente rileggere la Definizione 3.1.7 per concludere che il campo dei quozienti $(\mathsf{Frac}(D), i)$ è oggetto iniziale di Fld^D.

3.1.2 *Anelli di polinomi*

Dato un anello commutativo unitario R, l'anello di polinomi $R[x_1, \ldots, x_n]$ ha come elementi le combinazioni R-lineari finite di *monomi*

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

dove $\alpha_1, \ldots, \alpha_n$ sono interi non-negativi.

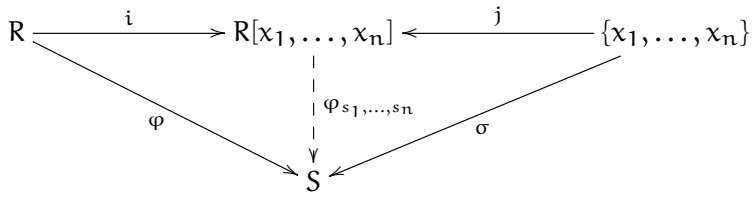
Dal punto di vista categoriale, è più naturale definire $R[x_1, \ldots, x_n]$ come R-algebra libera sull'insieme delle indeterminate $\{x_1, \ldots, x_n\}$, tuttavia, la teoria delle R-algebre non viene affrontata nei primi anni dei corsi universitari, e pertanto formalizziamo la proprietà universale degli anelli di polinomi, nel linguaggio degli anelli commutativi unitari.

Proposizione 3.1.10 (Proprietà universale anelli di polinomi)**.** *Sia* $\varphi\colon R \to S$ *un omomorfismo di anelli commutativi unitari, e* $R[x_1, \ldots, x_n]$ *l'anello di polinomi a coefficienti in* R *con indeterminate* $x_1, \ldots, x_n$*. Dati* n *elementi* $s_1, \ldots, s_n$ *di* S*, esiste un unico omomorfismo*

$$\varphi_{s_1,\ldots,s_n}\colon R[x_1, \ldots, x_n] \to S$$

che estende φ*, e tale che, per ogni* $k = 1, \ldots, n$*, si abbia* $\varphi(x_k) = s_k$*.*

La proprietà universale si traduce nella commutatività del diagramma:



(13)

dove i e j sono le inclusioni canoniche. Si noti che il triangolo commutativo a sinistra vive nella categoria degli anelli, mentre quello di destra, nella categoria degli insiemi.

Dimostrazione (traccia). Dato il polinomio

$$f(x_1, \dots, x_n) = \sum_{\epsilon \in E} f_\epsilon x_1^{\alpha_{\epsilon,1}} \cdots x_n^{\alpha_{\epsilon,n}}$$

in $R[x_1, \dots, x_n]$, con E insieme finito di indici e $f_\epsilon \in R$, per ogni $\epsilon \in E$, definiamo $\varphi_{s_1,\dots,s_n}$ come segue:

$$\varphi_{s_1,\dots,s_n}(f(x_1, \dots, x_n)) = \sum_{\epsilon \in E} \varphi(f_\epsilon) s_1^{\alpha_{\epsilon,1}} \cdots s_n^{\alpha_{\epsilon,n}} = \bar{\varphi}(f)(s_1, \dots, s_n),$$

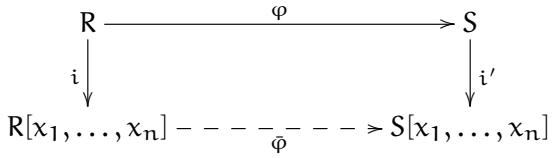
dove abbiamo introdotto la notazione:

$$\bar{\varphi}(f)(x_1, \dots, x_n) = \sum_{\epsilon \in E} \varphi(f_\epsilon) x_1^{\alpha_{\epsilon,1}} \cdots x_n^{\alpha_{\epsilon,n}}. \tag{14}$$

□

La Proposizione 3.1.10 sarà molto utile nel seguito. Nel prossimo esempio vediamo come essa possa essere utilizzata per estendere un omomorfismo tra due anelli commutativi ai rispettivi anelli di polinomi.

Esempio 3.1.11. Consideriamo il diagramma

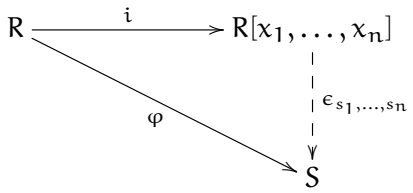


(15)

dove φ è un omomorfismo di anelli unitari e i e i' sono le inclusioni canoniche. Allora esiste un unico omomorfismo di anelli unitari $\bar{\varphi}$ che fa commutare il diagramma e tale che, per ogni $k = 1, \dots, n$, si abbia $\bar{\varphi}(x_k) = x_k$. L'omomorfismo $\bar{\varphi}$ è definito come nella dimostrazione della Proposizione 3.1.10: dato un polinomio $f \in R[x_1, \dots, x_n]$, si considera il corrispondente polinomio avente come coefficienti le immagini tramite φ dei coefficienti di f. La notazione è consistente con quella introdotta in (14).

3.1.3 *Omomorfismo di valutazione*

Una applicazione particolarmente rilevante della Proposizione 3.1.10 si ha quando φ è l'inclusione di un sottoanello unitario di S. In tal caso, la mappa $\varphi_{s_1,\dots,s_n}$ viene denotata $\epsilon_{s_1,\dots,s_n}$:



(16)

e chiamata *omomorfismo di valutazione* in $s_1, \dots, s_n$. Si vede facilmente che

$$\epsilon_{s_1,\dots,s_n}(f(x_1, \dots, x_n)) = f(s_1, \dots, s_n),$$

e fornisce il valore dell'espressione che si ottiene sostituendo al posto delle incognite x_k, i valori s_k. Si può facilmente vedere che l'immagine di $\epsilon_{s_1,\dots,s_n}$ è il sottoanello $R[s_1, \dots, s_n]$ generato da R e dall'insieme $\{s_1, \dots, s_n\} \subseteq S$. Quest'ultima considerazione apre alla prossima proposizione.

Proposizione 3.1.12. *Data una estensione di campi $F \to E$ e un sottoinsieme $\{s_1, \dots, s_n\} \subseteq E$. Allora, il sottocampo generato da $\{s_1, \dots, s_n\}$ su F è (isomorfo a) il campo dei quozienti del sottoanello generato da $\{s_1, \dots, s_n\}$ su F:*

$$F(s_1, \dots, s_n) \cong \mathsf{Frac}(F[s_1, \dots, s_n]) .$$

Dimostrazione. Per la Proposizione 3.1.6, possiamo definire un isomorfismo $\phi\colon \mathsf{Frac}(F[s_1, \dots, s_n]) \to F(s_1, \dots, s_n)$. Infatti, se indichiamo con $[f(s_1, \dots, s_n), g(s_1, \dots, s_n)]$ il generico elemento di $\mathsf{Frac}(F[s_1, \dots, s_n])$ (che ricordiamo essere una classe di equivalenza per la relazione di equivalenza descritta nella Costruzione 3.1.8), è naturale definire:

$$\phi([f(s_1, \dots, s_n), g(s_1, \dots, s_n)]) = f(s_1, \dots, s_n) \cdot g(s_1, \dots, s_n)^{-1} .$$

Si verifica facilmente che tale definizione è ben posta e che, invero, dà un isomorfismo di campi. □

3.2 LA CATEGORIA Fld DEI CAMPI

Come già detto, gli omomorfismi di campi non sono altro che omomorfismi di anelli unitari. Poiché ogni omomorfismo di campi è un monomorfismo (vedi Lemma 3.1.3), è possibile identificare il dominio di un omomorfismo con la sua immagine, e, di conseguenza, considerare il codominio come un modo di estendere il dominio. Per questo, nel resto del testo, non parleremo di omomorfismi di campi, ma piuttosto di *estensioni* di campi (Definizione 3.1.4), intendendo con questo sottolineare come gli omomorfismi di campi siano un modo di estendere un campo a un altro campo che lo contenga.

Esempio 3.2.1. Consideriamo l'estensione

$$\mathbb{R} \to \mathbb{C}$$

Essa è data dalla funzione che associa al numero reale α il numero complesso $\alpha + 0i$. Non è difficile mostrare che tale funzione è un omomorfismo di anelli unitari, la cui immagine

$$\tilde{\mathbb{R}} = \{\alpha + 0i \mid \alpha \in \mathbb{R}\}$$

è un sottocampo di $\mathbb{C}$ isomorfo al campo dei reali.

Esempio 3.2.2. Il campo $F(x)$ delle funzioni razionali a coefficienti nel campo F si può vedere in modo naturale come estensione di F. Infatti, è possibile definire un isomorfismo di campi $F \cong \bar{F}$, dove

$$\bar{F} = \left\{ \frac{a}{1} \mid a \in F \right\}.$$

Le due estensioni di campi trattate negli esempi precedenti sono chiamate *semplici*. Viene data, infatti, la definizione che segue.

Definizione 3.2.3. *L'estensione di campi* $F \to E$ *è detta* semplice *se esiste* $\alpha \in E$ *tale che* $E = F(\alpha)$.

Riferendoci agli esempi riportati sopra, nel primo caso si ha $\mathbb{C} = \mathbb{R}(i)$; il secondo è evidente.

Segue immediatamente dalla Proposizione 3.1.12, il fatto che, per un'estensione semplice

$$F \to F(\alpha),$$

si abbia $F(\alpha) = \mathsf{Frac}(F[\alpha])$, dove $F[\alpha]$ è l'immagine di $F[x]$ attraverso l'omomorfismo di valutazione $\epsilon_\alpha \colon F[x] \to E$.

3.2.1 *Caratteristica e sottocampo primo*

La nozione di *caratteristica* di un campo è definita in modo naturale quando consideriamo i campi come oggetti della categoria CRing. A questo scopo, per ogni campo F, consideriamo l'omomorfismo iniziale in CRing:

$$\phi_F \colon \mathbb{Z} \to F$$

anche chiamato *omomorfismo caratteristico*.

Definizione 3.2.4. *Diremo che il campo* F *ha caratteristica* n

$$\mathsf{chr}(F) = n$$

se $\ker(\phi_F) = (n)$.

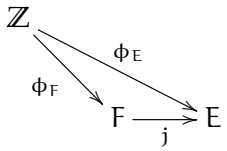
L'immagine $\phi_F(\mathbb{Z})$ è un sottoanello di F, e pertanto è un dominio di integrità. Inoltre, il primo teorema di isomorfismo ci dice che esso è isomorfo all'anello quoziente $\mathbb{Z}/\ker(\phi_F)$. Quindi, per il Lemma 3.1, $\ker(\phi_F)$ è un ideale primo di $\mathbb{Z}$. Questo ci lascia con due opzioni: se tale ideale non è massimale, esso è l'ideale nullo (0), se invece è massimale, esso è l'ideale principale (p) con p numero primo. In conclusione, la caratteristica di un campo è 0, oppure è un numero primo p.

Osservazione 3.2.5. La caratteristica del campo F può essere introdotta anche con una definizione *ad hoc*, come il più piccolo intero positivo n tale che $na = 0$, per ogni $a \in F$, o 0 se tale n non esiste. Questo approccio ha il vantaggio di poter essere applicato anche al caso più generale degli anelli. In queste note tuttavia, coerentemente con l'approccio che abbiamo voluto sviluppare, preferiamo definire la nozione di caratteristica per mezzo di un universale.

Proposizione 3.2.6. *Data una estensione* $F \to E$ *si ha*

$$\mathsf{chr}(F) = \mathsf{chr}(E)$$

Dimostrazione. Si consideri il diagramma seguente in CRing.



Si ha $j\phi_F = \phi_E$ perché $\mathbb{Z}$ è oggetto iniziale. Inoltre, poiché j è un monomorfismo, $\ker(\phi_F) = \ker(\phi_E)$. □

Una conseguenza della proposizione è che possiamo *scomporre* la categoria Fld nelle sue componenti connesse

$$\mathsf{Fld}_0,\ \mathsf{Fld}_2,\ \mathsf{Fld}_3,\ \mathsf{Fld}_5, \ldots,\ \mathsf{Fld}_p, \ldots$$

indicizzate dalla caratteristica. Ognuna di esse è una sottocategoria di Fld con un suo specifico oggetto iniziale.

Analizziamo prima il caso in cui la caratteristica sia 0. Sia F un oggetto di Fld_0. L'immagine $\phi_F(\mathbb{Z})$ è un sottoanello di F, isomorfo a $\mathbb{Z}$ poiché $\ker(\phi_F) = (0)$. Il campo dei quozienti di tale immagine è allora (isomorfo a) il campo $\mathbb{Q}$ dei razionali. Diciamo che $\mathbb{Q}$ è il *sottocampo primo* di F. La proprietà universale del campo dei quozienti garantisce che esiste un unico morfismo (estensione) di campi

$$\mathbb{Q} \to F.$$

Concludiamo che $\mathbb{Q}$ è l'oggetto iniziale della categoria Fld_0.

Nel caso in cui la caratteristica di F sia p, l'immagine $\phi_F(\mathbb{Z})$ è (isomorfa a) l'anello $\mathbb{Z}/(p) = \mathbb{Z}_p$. Questo anello è in effetti un campo

(e quindi è isomorfo al suo campo dei quozienti), e pertanto, per distinguerlo dal gruppo abeliano $\mathbb{Z}_p$, viene denotato $\mathbb{F}_p$. Diciamo che $\mathbb{F}_p$ è il *sottocampo primo* di F. Anche in questo caso, esiste un unico morfismo (estensione) di campi

$$\mathbb{F}_p \to F.$$

Concludiamo che $\mathbb{F}_p$ è l'oggetto iniziale della categoria Fld_p.

3.2.2 *Le categorie delle estensioni*

Nel seguito, dovremo considerare diverse versioni di categorie di estensioni di campi e di anelli. In effetti, si tratterà di specifiche sottocategorie della categoria $\mathsf{Arr}(\mathsf{CRing})$ delle frecce della categoria CRing degli anelli commutativi unitari (per la costruzione della categorie delle frecce di una categoria, si rimanda alla Sezione 1.1.8). Seguono gli esempi rilevanti per nostra trattazione.

Esempio 3.2.7. La categoria degli estensioni di campi in anelli. Oggetti sono gli omomorfismi (necessariamente iniettivi) di anelli commutativi unitari $F \to R$, dove F è un campo e R un anello commutativo unitario, morfismi di estensioni sono i quadrati commutativi:

$$\begin{array}{ccc} F & \xrightarrow{f} & F' \\ \downarrow & & \downarrow \\ R & \xrightarrow[g]{} & R' \end{array}$$

dove f è un monomorfismo di campi, e g un omomorfismo di anelli.

Esempio 3.2.8. Se nell'esempio precedente, consideriamo R e R' campi, otteniamo la categoria delle estensione di campi. In questo caso, g risulta essere un monomorfismo.

3.2.3 *Grado di una estensione*

L'estensione di campi $i\colon F \to E$ dota il campo E della struttura di F-spazio vettoriale. Infatti, E è un gruppo abeliano rispetto all'operazione di somma, mentre il prodotto *esterno* degli scalari di F si ottiene per restrizione della moltiplicazione in E: per $\lambda \in F$ e $v \in E$, si ha

$$\lambda \cdot v = i(\lambda)\, v \qquad (\text{moltiplicazione in } E).$$

Definizione 3.2.9. *Il grado* $[F : K]$ *dell'estensione* $F \to E$ *è la dimensione di* E *come spazio vettoriale su* F. *Se* $[F : K] < +\infty$, *l'estensione* $F \to E$ *si dirà* di grado finito, *o più semplicemente* finita, *altrimenti parleremo di* estensione infinita.

L'avere ricondotto le estensioni di campi a spazi vettoriali può sembrare bizzarro: un campo E ha più struttura di uno spazio vettoriale,

perché ha una moltiplicazione interna. Tuttavia, proprio l'esserci *dimenticati* di una parte della struttura, ci permetterà di applicare efficacemente i metodi dell'algebra lineare alla teoria dei campi.

Esempi 3.2.10.

1. Il grado dell'estensione $\mathbb{R} \to \mathbb{C}$ è $[\mathbb{C} : \mathbb{R}] = 2$, poiché $\mathbb{C}$ ha dimensione reale 2. Infatti, ogni numero complesso si scrive in un solo modo come combinazione lineare degli elementi della base $\{1, i\}$.

2. Se F è un campo, il grado dell'estensione banale $F \to F$ è $[F : F] = 1$. Ad esempio, il campo $\mathbb{C}$ come spazio vettoriale su se stesso ha dimensione complessa 1, e un qualunque numero complesso $z \neq 0$ costituisce da solo una base.

3. L'estensione $\mathbb{R} \to \mathbb{R}(x)$ delle funzioni razionali reali ha grado $+\infty$. Infatti, l'insieme $\{1, x, x^2, \dots, x^n, \dots\} \subseteq \mathbb{R}(x)$, è un sistema di vettori linearmente indipendenti su $\mathbb{R}$.

4. Sia $\mathbb{Q}(\sqrt{3})$ il sottoanello di $\mathbb{R}$ generato da $\mathbb{Q}$ e $\sqrt{3}$. Esso può essere descritto come segue:

$$\mathbb{Q}(\sqrt{3}) = \{\alpha + \sqrt{3}\beta \mid \alpha, \beta \in \mathbb{Q}\}$$

   e si verifica facilmente essere campo. Infatti, per $\alpha + \sqrt{3}\beta \neq 0$, si ha:

$$(\alpha + \sqrt{3}\beta) \cdot \left(\frac{\alpha}{\alpha^2 - 3\beta^2} - \sqrt{3}\frac{\beta}{\alpha^2 - 3\beta^2} \right) = 1$$

   Inoltre l'insieme $\{1, \sqrt{3}\}$ è una base di $\mathbb{Q}(\sqrt{3})$ su $\mathbb{Q}$, per cui l'estensione $\mathbb{Q} \to \mathbb{Q}(\sqrt{3})$ ha grado 2.

La prossima proposizione mette in evidenza la natura moltiplicativa del grado delle estensioni.

Proposizione 3.2.11 (Legge dei gradi)**.** *Siano date le estensioni di campi*

$$F \to E \to L$$

Allora:

(i) *Il grado* $[L : F]$ *è finito se e solo se i gradi* $[L : E]$ *e* $[E : F]$ *sono finiti.*

(ii) *Vale la formula:*

$$[L : F] = [L : E] \cdot [E : F]$$

(iii) *Se* $\mathcal{X} = \{x_1, \dots, x_m\}$ *è una base di* L *su* E*, e* $\mathcal{Y} = \{y_1, \dots, y_n\}$ *è una base di* E *su* F*, allora* $\mathcal{B} = \{x_i y_j\}_{i=1,\dots,m,\, j=1,\dots,n}$ *è una base di* L *su* F.

Dimostrazione. Poiché (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i), dimostreremo solamente (iii). Per prima cosa mostriamo che $\mathcal{B}$ è un sistema di generatori di L

su F. Infatti, per un generico $\ell \in L$, poiché $\mathcal{X}$ è un sistema di generatori di L su E, si ha:

$$\ell = \sum_{i=1}^{m} e_i x_i \,, \qquad \text{con } e_i \in E \,.$$

Inoltre, poiché $\mathcal{Y}$ è un sistema di generatori di E su F, per ogni $i = 1, \ldots, m$ si ha:

$$e_i = \sum_{j=1}^{n} f_{i,j} y_j \,, \qquad \text{con } f_{i,j} \in F \,.$$

Sostituendo si ottiene:

$$\ell = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} f_{i,j} y_j \right) x_i = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{i,j} x_i y_j \,.$$

Ora facciamo vedere che l'insieme di generatori $\mathcal{B}$ è linearmente indipendente su F. A questo scopo consideriamo una combinazione lineare:

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{i,j} x_i y_j \,, \qquad \text{con } \lambda_{i,j} \in F \,.$$

L'espressione può essere riscritta come segue:

$$0 = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \lambda_{i,j} y_j \right) x_i \,.$$

Poiché $\mathcal{X}$ è una base di L su E, si ha che per ogni i fissato deve valere:

$$\sum_{j=1}^{n} \lambda_{i,j} y_j = 0 \,,$$

e poiché $\mathcal{Y}$ è una base di E su F, si ha che per ogni j fissato deve valere:

$$\lambda_{i,j} = 0$$

In conclusione, per ogni $i = 1, \ldots, m$ e $j = 1, \ldots, n$ si ha $\lambda_{i,j} = 0$, il che conclude la dimostrazione. □

Il prossimo facile corollario della *Legge dei gradi* ha conseguenze rilevanti.

Corollario 3.2.12. *Data l'estensione $F \to E$, con $[E : F] = p$ numero primo, allora non vi sono estensioni intermedie proprie tra F e E.*

Dimostrazione. Data l'estensione intermedia

$$F \to E' \to E$$

per la legge dei gradi si ha $p = [E : F] = [E : E'] \cdot [E' : F]$. Essendo p primo, ci sono due possibilità: o $[E : E'] = 1$ da cui $E' \cong E$, oppure $[E' : F]$, da cui $E' \cong F$. □

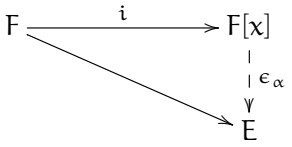
Esempio 3.2.13. Inserire esempio $\mathbb{Q} \to \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$

3.3 ESTENSIONI ALGEBRICHE E TRASCENDENTI

Consideriamo l'estensione di campi

$$F \to E$$

con $\alpha \in E$. Possiamo specializzare il caso trattato nella Sezione 3.1.3. Il diagramma che segue illustra la situazione



(17)

dove i è l'inclusione canonica, ϵ_α è l'omomorfismo di valutazione di α, cioè la legge che associa a ogni polinomio $f(x) \in F[x]$ il valore $f(\alpha) \in E$.

Formuliamo le definizioni seguenti.

Definizione 3.3.1. *Si fissi una estensione di campi* $F \to E$.

(i) *L'elemento* $\alpha \in E$ *è* algebrico *su* F *se* $\mathsf{Ker}(\epsilon_\alpha) \neq (0)$.

(ii) *L'elemento* $\alpha \in E$ *è* trascendente *su* F *se* $\mathsf{Ker}(\epsilon_\alpha) = (0)$.

(iii) *L'estensione* $F \to E$ *è algebrica se ogni* $\alpha \in E$ *è algebrico su* F.

(iv) *L'estensione* $F \to E$ *è trascendente se esiste* $\alpha \in E$ *trascendente su* F.

Proposizione 3.3.2 (Caratterizzazione elementi algebrici)**.** *Data l'estensione di campi* $F \to E$, $\alpha \in E$ *è algebrico su* F *se e solo se esiste un polinomio non nullo* $f(x)$ *a coefficienti in* F, *tale che* $f(\alpha) = 0$.

Dimostrazione. Si ha che $f(\alpha) = 0$ se e solo se $\epsilon_\alpha(f(x)) = 0$ se e solo se $f(x) \in \mathsf{Ker}(\epsilon_\alpha)$. □

Esempi 3.3.3.

1. Sono elementi algebrici su $\mathbb{Q}$ tutti i radicali semplici reali, quali $\sqrt{2}, \sqrt{3}, \sqrt[3]{5}, \sqrt[n]{m}, \ldots$, i radicali multipli quali $\sqrt{1+\sqrt{5}}, \sqrt{\sqrt[3]{2}+3}, \ldots$ e loro somme, prodotti etc. Ad esempio, $\sqrt{1+\sqrt{5}}$ è radice del polinomio $x^4 - 2x^2 - 4$.

2. L'unità immaginaria $i \in \mathbb{C}$ è algebrica su $\mathbb{Q}$, in quanto è radice del polinomio $x^2 + 1$. Di conseguenza, sono algebriche su $\mathbb{Q}$ anche le espressioni radicali complesse.

3. I cosiddetti *numeri trascendenti*, sono numeri reali o complessi trascendenti su $\mathbb{Q}$. Ad esempio, π è trascendente (su $\mathbb{Q}$) perché non vi è alcun polinomio a coefficienti razionali $f(x)$ tale che $f(\pi) = 0$, e discorso analogo può essere fatto per la costante di Nepero e.[2]

2 Per una dimostrazione elementare di queste asserzioni si veda ad esempio [7].

4. Attenzione: l'algebricità (e la trascendenza) sono concetti relativi. Ad esempio, π è trascendente su $\mathbb{Q}$, ma è algebrico su $\mathbb{R}$. Infatti, è radice del polinomio $x - \pi$ di $\mathbb{R}[x]$.

5. Data l'estensione $F \to F(x)$ del campo delle funzioni razionali su F, si ha che $x \in F(x)$ è trascendente su F. Infatti, l'unico polinomio f a coefficienti in F tale che $f(x)$ sia il polinomio nullo è proprio il polinomio nullo.

3.3.1 *Estensioni trascendenti semplici*

Un'estensione trascendente semplice è un'estensione semplice

$$F \to F(\alpha)$$

tale che α sia trascendente su F. La proposizione seguente fornisce una caratterizzazione degli elementi trascendenti su un campo F, e allo stesso tempo dà una descrizione delle estensioni trascendenti semplici di F.

Proposizione 3.3.4. *Data l'estensione di campi $F \to E$, e dato un elemento $\alpha \in E$, le seguenti condizioni sono equivalenti:*

(i) *α è trascendente su F;*

(ii) *esiste un isomorfismo $F(\alpha) \cong F(x)$ che fissa F e manda α in x.*

In questo caso, il grado $[F(\alpha) : F]$ dell'estensione $F \to F(\alpha)$ è infinito.

Dimostrazione. Sia

$$\begin{array}{ccccc} F[x] & \xrightarrow{\epsilon'_\alpha} & F[\alpha] & \xhookrightarrow{\iota} & E \\ & \searrow^{\epsilon_\alpha} & & \nearrow & \end{array}$$

la fattorizzazione canonica dell'omomorfismo di valutazione ϵ_α sull'immagine $F[\alpha]$. Poiché ι è iniettivo, si ha che il nucleo di ϵ'_α coincide con il nucleo di ϵ_α, l'ideale nullo (0). Pertanto, ϵ'_α è iniettivo. Poiché esso è anche suriettivo per definizione, stabilisce un isomorfismo $F[x] \cong F[\alpha]$. Tale isomorfismo, che fissa F e manda x in α, passa al quoziente: anche rispettivi i campi dei quozienti sono isomorfi

$$F(x) = \mathrm{Frac}(F[x]) \cong \mathrm{Frac}(F[\alpha]) = F(\alpha)\,.$$

Viceversa, dato un isomorfismo $F(x) \cong F(\alpha)$, la tesi segue immediatamente dall'Esempio 3.3.3 numero 5.

Nel caso siano verificate le condizioni equivalenti della proposizione, l'insieme $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n, \ldots\}$ è un sistema linearmente indipendente su F. Infatti, essendo α trascendente, per la Proposizione 3.3.2, $f(\alpha) \neq 0$, per ogni polinomio $f(x) \in F[x] \setminus \{0\}$. Di conseguenza, lo spazio vettoriale $F(\alpha)$ ha dimensione infinita su F. □

3.3.2 *Estensioni algebriche semplici*

Un'estensione algebrica semplice è un'estensione semplice

$$F \to F(\alpha)$$

tale che α sia algebrico su F. La proposizione seguente fornisce una caratterizzazione delle estensioni algebriche semplici su un campo F, e allo stesso tempo dà una descrizione di tali estensioni.

Proposizione 3.3.5. *Data l'estensione di campi $F \to E$, e un elemento $\alpha \in E$ algebrico su F, le seguenti asserzioni sono vere.*

1. *Il nucleo dell'omomorfismo di valutazione*

$$\epsilon_\alpha \colon F[x] \to E$$

   è un ideale principale di $F[x]$ generato da un polinomio monico irriducibile. Tale polinomio, univocamente determinato, è chiamato polinomio minimo di α su F, *ed è di solito denotato $m_\alpha(x)$, o $\min_\alpha(x)$.*

2. *Dato il polinomio $0 \neq f(x) \in F[x]$, si ha che $f(\alpha) = 0$ se e solo se $m_\alpha(x)$ divide $f(x)$.*

3. $F(\alpha) = F[\alpha]$ *e* $F(\alpha) \cong \dfrac{F[x]}{(m_\alpha(x))}$.

4. *Se il grado di $m_\alpha(x)$ è n, allora si ha che $[F(\alpha) : F] = n$, e l'insieme $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ è una base di $F(\alpha)$ su F.*

Dimostrazione. Punto 1. Dal teorema fondamentale di omomorfismo per gli anelli, sappiamo che l'immagine $F[\alpha]$ dell'omomorfismo di valutazione ϵ_α è canonicamente isomorfa all'anello quoziente $F[x]/\mathrm{Ker}(\epsilon_\alpha)$. Ora, tale immagine è sicuramente un dominio, in quanto sottoanello di un campo, e pertanto $\mathrm{Ker}(\epsilon_\alpha)$ è un ideale primo. Esso è inoltre diverso dall'ideale banale, perché α è algebrico su F, e quindi è ideale massimale. Poiché $K[x]$ è un PID, tale ideale è generato da un polinomio irriducibile, unico, se preso monico.

Punto 2. È una conseguenza immediata del punto appena dimostrato. $f(\alpha) = 0$ vuol dire precisamente che $\epsilon_\alpha(f(x)) = 0$, i.e. $f(x) \in \mathrm{Ker}(\epsilon_\alpha)$. Ma il nucleo è generato da $m_\alpha(x)$, e pertanto $f(x) = m_\alpha(x) \cdot g(x)$, per un certo $g(x) \in F[x]$.

Punto 3. Poiché $0 \neq m_\alpha(x)$ è irriducibile, l'ideale $(m_\alpha(x))$ è massimale, e quindi $F[\alpha] \cong \dfrac{F[x]}{(m_\alpha(x))}$ è (già) un campo, e per la Proposizione 3.1.6, esso coincide con il suo campo dei quozienti $F(\alpha)$.

Punto 4. Dimostriamo direttamente che l'insieme $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ è una base di $F(\alpha) \cong \dfrac{F[x]}{(m_\alpha(x))}$. Infatti, dati $a_0, \dots a_{n-1} \in F$ tali che

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0\,,$$

basta considerare il polinomio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$, e poiché $f(\alpha) = 0$, dal punto (2) deduciamo $m_\alpha(x) \mid f(x)$. Quindi, poiché $\deg(f(x)) < \deg(m_\alpha(x))$, $f(x)$ deve essere il polinomio nullo, il che significa $a_i = 0$, per ogni $i = 1, \ldots, n-1$. In altre parole, le potenze di α considerate sono indipendenti su F. Vediamo ora che esse sono anche dei generatori di $F(\alpha)$ su F. Poiché per il punto (3) sappiamo che $F(\alpha) = F[\alpha]$, consideriamo un generico $t \in F[\alpha]$:

$$t = t_0 + t_1\alpha + \cdots + t_k\alpha^k, \qquad t_i \in F$$

e definiamo il polinomio $g(x) = t_0 + t_1x + \cdots + t_kx^k$. Ora, $F[x]$ è un anello euclideo, pertanto possiamo dividere $g(x)$ per il polinomio minimo e ottenere:

$$f(x) = q(x) \cdot m_\alpha(x) + \bar{f}(x)$$

con $\deg(\bar{f}(x)) < \deg(m_\alpha(x))$. Quindi, calcoliamo:

$$t = \epsilon_\alpha(f(x)) = \epsilon_\alpha\left(q(x) \cdot m_\alpha(x) + \bar{f}(x)\right) = q(\alpha) \cdot m_\alpha(\alpha) + \bar{f}(\alpha)$$

$$= q(\alpha) \cdot 0 + \bar{f}(\alpha) = \bar{f}(\alpha) = \bar{a}_0 + \bar{a}_1\alpha + \cdot + \bar{a}_{n-1}\alpha^{n-1},$$

per certi $\bar{a}_0, \ldots, \bar{a}_{n-1}$. □

Esempio 3.3.6. *Determinare il polinomio minimo di* $\sqrt{2}\sqrt{6+\sqrt{3}}$ *su* $\mathbb{Q}$.

Poniamo

$$x = \sqrt{2}\sqrt{6+\sqrt{3}}.$$

Segue che

$$x^2 = 12 + 2\sqrt{3},$$

così

$$x^2 - 12 = 2\sqrt{3},$$

ed elevando entrambi i membri nuovamente al quadrato

$$x^4 - 24x^2 + 144 = 12.$$

Dunque considero il polinomio $p(x) = x^4 - 24x^2 + 132 \in \mathbb{Q}[x]$. Esso è monico ed ammette $\sqrt{2}\sqrt{6+\sqrt{3}}$ come radice. Infine $p(x)$ è irriducibile su $\mathbb{Q}$ in quanto, ponendo $t = x^2$, l'equazione

$$t^2 - 24t + 132 = 0$$

ammette due soluzioni distinte non razionali $t_{1,2} = 12 \pm 2\sqrt{3}$ e la fattorizzazione in $\mathbb{R}[x]$ è unica. Così $p(x)$ è proprio il polinomio minimo di $\sqrt{2}\sqrt{6+\sqrt{3}}$ su $\mathbb{Q}$.

Esempio 3.3.7. *Si consideri l'estensione* $\mathbb{Q}(\pi^3) \hookrightarrow \mathbb{Q}(\pi)$. *Dopo aver verificato che* $\pi^2 \notin \mathbb{Q}(\pi^3)$, *determiniamo il polinomio minimo di* π^2 *su* $\mathbb{Q}(\pi^3)$.

Se fosse $\pi^2 \in \mathbb{Q}(\pi^3)$, allora si avrebbe che

$$\pi^2 = \frac{a_n(\pi^3)^n + ... + a_1\pi^3 + a_0}{b_m(\pi^3)^m + ... + b_1\pi^3 + b_0},$$

dove $a_0, ..., a_n, b_0, ..., b_m \in \mathbb{Q}$ e $a_n \neq 0 \neq b_m$. Così si otterrebbe un'equazione polinomiale a coefficienti razionali

$$b_m\pi^{3m+2} + ... + b_1\pi^5 + b_0\pi^2 - (a_n\pi^{3n} + ... + a_1\pi^3 + a_0) = 0$$

e dunque π sarebbe radice del polinomio a coefficienti razionali

$$p(x) = b_m x^{3m+2} + ... + b_1 x^5 + b_0 x^2 - (a_n x^{3n} + ... + a_1 x^3 + a_0),$$

il che è un assurdo.

Quindi, il polinomio $p(x) = x^3 - \pi^6 = x^3 - (\pi^3)^2 \in \mathbb{Q}(\pi^3)[x]$ ammette π^2 come radice. Inoltre, esso è irriducibile su $\mathbb{Q}(\pi^3)$ in quanto la sua fattorizzazione su $\mathbb{R}[x]$ è

$$p(x) = x^3 - (\pi^2)^3 = (x - \pi^2)(x^2 + \pi^2 x + \pi^4).$$

In conclusione, il polinomio minimo di π^2 su $\mathbb{Q}(\pi^3)$ è proprio $p(x)$.

Il risultato seguente ci da immediatamente una caratterizzazione degli elementi algebrici e di quelli trascendendenti.

Corollario 3.3.8. *Data l'estensione $F \to E$, e un elemento $\alpha \in E$, si ha che*

- *α è algebrico su F se e solo se $[F(\alpha) : F]$ è finito.*
- *α è trascendente su F se e solo se $[F(\alpha) : F]$ è infinito.*

3.3.3 *Radici del polinomio minimo*

Consideriamo il polinomio a coefficienti razionali $x^3 - 2$. Esso è (monico e) irriducibile su $\mathbb{Q}$, e ha la radice reale $\sqrt[3]{2}$. Per quanto visto nella Proposizione 3.3.5, il polinomio $x^3 - 2$ è il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$. In realtà, $x^3 - 2$ ammette altre due radici, non reali, ma complesse coniugate. Per convincersene basta scomporre

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + x\sqrt[3]{2} + \sqrt[3]{4})$$

e risolvere il secondo fattore. È naturale allora domandarsi quale sia il polinomio minimo di queste altre radici. Il risultato seguente risponde in generale a tale domanda.

Lemma 3.3.9. *Consideriamo l'estensione $F \to E$, un elemento $\alpha \in E$ algebrico e $m_\alpha(x)$, polinomio minimo di α su F. Sia inoltre dato $\beta \in E$ tale che $m_\alpha(\beta) = 0$. Allora $m_\alpha(x)$ è anche il polinomio minimo di β su F.*

Dimostrazione. Poiché $m_\alpha(\beta) = 0$, per la Proposizione 3.3.5, si ha che $m_\beta(x)$, polinomio minimo di β su F, divide $m_\alpha(x)$ in $F[x]$. Ma i due polinomi sono entrambi irriducibile e monici. Concludiamo $m_\alpha(x) = m_\beta(x)$. □

Tornando all'esempio con cui abbiamo aperto, concludiamo che $x^3 - 2$ è il polinomio minimo anche delle radici complesse coniugate: $(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)\sqrt[3]{2}$ e $(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)\sqrt[3]{2}$.

3.3.4 *Estensioni algebriche*

Proposizione 3.3.10. *Data l'estensione $F \to E$, se il grado $[E : F]$ è finito, allora l'estensione è algebrica.*

Dimostrazione. Supponiamo per assurdo che $[E : F] = n$ finito e che $\alpha \in E$ sia trascendente su F. Allora, riferendoci all'estensione intermedia $F(\alpha)$, si ha la contraddizione:

$$n = [E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F] \geqslant [F(\alpha) : F] = +\infty .$$

□

Teorema 3.3.11 (Transitività delle estensioni algebriche)**.** *Si considerino le estensioni di campi:*

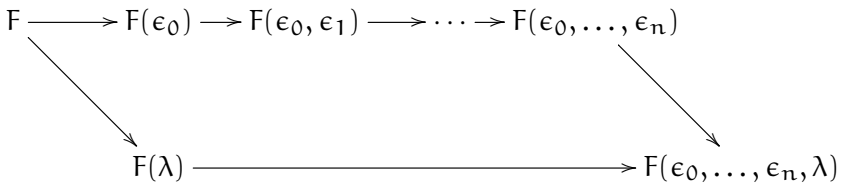
$$F \to E \to L .$$

Se E è estensione algebrica di F, e L è estensione algebrica di E, allora L è anche estensione algebrica di F.

Dimostrazione. Si vuole dimostrare che ogni $\lambda \in L$ è algebrico su F. A questo scopo, poiché λ è algebrico su E per ipotesi, esiste un polinomio

$$f(x) = \epsilon_0 + \epsilon_1 x + \epsilon_2 x^2 + \cdots + \epsilon_n x^n \in E[x]$$

tale che $f(\lambda) = 0$. Ora, poiché E è algebrico su F, tutti i coefficienti $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ sono elementi algebrici su F. Possiamo allora considerare il seguente diagramma commutativo e applicare ripetutamente il Corollario 3.3.8.



Si ha

$$[F(\epsilon_0) : F] = k_0 < +\infty ,$$

perché $F(\epsilon_0)$ è estensione algebrica semplice di F,

$$[F(\epsilon_0, \epsilon_1) : F(\epsilon_0)] = k_1 < +\infty ,$$

perché $F(\epsilon_0, \epsilon_1) = (F(\epsilon_0))(\epsilon_1)$ è estensione algebrica semplice di $F(\epsilon_0)$, e così via, fino a

$$[F(\epsilon_0, \ldots, \epsilon_n) : F(\epsilon_0, \ldots, \epsilon_{n-1})] = k_n < +\infty .$$

Inoltre,

$$[F(\epsilon_0, \dots, \epsilon_n, \lambda) : F(\epsilon_0, \dots, \epsilon_n)] < n$$

perché $f(x) \in F(\epsilon_0, \dots, \epsilon_n)[x]$, e $f(\lambda) = 0$. Per la legge dei gradi allora

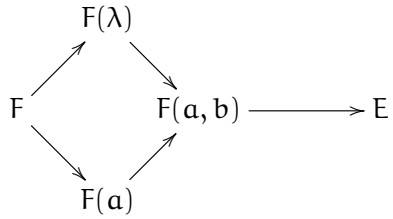
$$[F(\lambda) : F] \leqslant [F(\epsilon_0, \dots, \epsilon_n, \lambda) : F] \leqslant k_0 \cdots k_n \cdot n < +\infty$$

e λ è algebrico su F.

□

Proposizione 3.3.12. *Sia $F \to E$ una estensione di campi. L'insieme $A \subseteq E$ degli elementi algebrici su F è un sottocampo di E.*

Dimostrazione. Dati $a, b \in A$ diversi da zero, vogliamo provare che anche $a + b$, $a - b$, ab e a/b appartengono ad A. Sia allora $\lambda \in \{a + b, a - b, ab, a/b\}$, e sia a di grado n su F e b di grado k su F. Consideriamo il diagramma:



Si ha che

$$[F(\lambda) : F] \leqslant [F(a, b) : F] = [F(a) : F] \cdot [F(a) : F]$$

Ma $[F(a) : F] = n$ per ipotesi, e, poiché il polinomio minimo di b su $F(a)$ divide il polinomio minimo di b su F, per il punto 2 della Proposizione 3.3.5, si ha $[F(a) : F] \leqslant k$. Quindi il grado di λ su F è al più $n \cdot k$; in particolare tale grado è finito, per cui, per il Corollario 3.3.8, λ è algebrico su F. □

Esempio 3.3.13. Il campo $\mathbb{A}$ dei cosiddetti *numeri algebrici* è il sottocampo di $\mathbb{C}$ degli elementi algebrici su $\mathbb{Q}$:

$$\mathbb{Q} \to \mathbb{A} \to \mathbb{C}$$

La Proposizione 3.3.10 chiarisce che le estensioni di grado finito sono necessariamente algebriche. È allora naturale chiedersi se valga il viceversa. La risposta è negativa, come si deduce dal prossimo risultato.

Proposizione 3.3.14. *L'estensione $\mathbb{A}$ di $\mathbb{Q}$ è algebrica, ma non è di grado finito.*

Dimostrazione. Supponiamo per assurdo che $[\mathbb{A} : \mathbb{Q}] = n < +\infty$, e consideriamo il polinomio:

$$m(x) = x^{n+1} - 2 \in \mathbb{Q}[x]\,.$$

Per il criterio di Eisenstein (per $p = 2$), esso è irriducibile. Sia allora $\alpha \in \mathbb{C}$ una sua radice. Si ha che $\alpha \in \mathbb{A}$, per cui possiamo osservare la catena di estensioni:

$$\mathbb{Q} \to \mathbb{Q}(\alpha) \to \mathbb{A}$$

Per la legge dei gradi, calcoliamo:

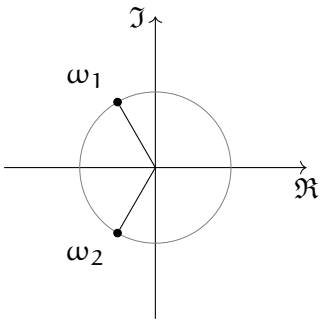
$$n = [\mathbb{A} : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \geqslant [\mathbb{Q}(\alpha) : \mathbb{Q}] = n + 1$$

il che è una contraddizione. □

3.4 ESTENSIONI E POLINOMI

3.4.1 *Aggiunzione formale di radici*

Consideriamo il polinomio $f(x) = x^2 + x + 1$ a coefficienti in $\mathbb{Q}$. Essendo di secondo grado, esso è irriducibile poiché non ammette radici razionali. Tuttavia è immediato calcolare le sue radici complesse:



$$\omega_{1,2} = \frac{-1 \pm \sqrt{1-4}}{2} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$$

In effetti, la descrizione delle radici di $f(x)$ si basa sul fatto che $\mathbb{Q}$ è un sottocampo di $\mathbb{C}$, e che ω_1 e ω_2 appartengono a $\mathbb{C}$. Tuttavia, il campo dei complessi è di gran lunga sovrabbondante, se il nostro scopo è semplicemente quello di descrivere le radici di $f(x)$. Per questo, per trattare le radici di $f(x)$, basta considerare il campo generato dalle radici del polinomio, ovvero: $\mathbb{Q}(\omega_1, \omega_2) = \mathbb{Q}(\omega_1)$.

È naturale chiedersi come si possa affrontare il problema analogo, se il polinomio $f(x)$ lo considerassimo a coefficienti in $\mathbb{F}_2$, dove $\mathbb{F}_2 = \{0, 1\}$ è il campo con due elementi (con sostegno il gruppo abeliano $\mathbb{Z}_2$).

In questo caso, non abbiamo già un'estensione del campo di base in cui andare a cercare le radici di $f(x)$. Inoltre, la formula che abbiamo usato per calcolare le radici di un polinomio di secondo grado perde significato in caratteristica 2, perché, qui, dividere per 2 equivale a dividere per 0. Tuttavia, già nel caso precedente, possiamo osservare come il campo $\mathbb{Q}(\omega_1)$ ammetta anche una descrizione alternativa e più formale: esso è canonicamente isomorfo al quoziente $\mathbb{Q}[x]/(f(x))$, mediante l'isomorfismo che manda l'elemento ω_1 nella classe $x + (f(x))$ avente come rappresentante il monomio x. Questo punto di vista può essere riportato anche nel secondo caso.

Per prima cosa, desriviamo l'estensione:

$$\mathbb{F}_2 \xrightarrow{\iota} \frac{\mathbb{F}_2[x]}{(x^2+x+1)} \ .$$

Gli elementi del campo quoziente sono le classi laterali di (x^2+x+1) in $\mathbb{F}_2[x]$. Come rappresentanti, possiamo come sempre considerare i resti della divisione euclidea per x^2+x+1, ovvero da polinomi di grado minore di 2 a coefficienti in $\mathbb{F}_2$. La somma si esegue come al solito, sommando i monomi dello stesso grado, mentre il prodotto si moltiplicano i polinomi, riducendo il risultato *modulo* x^2+x+1, ovvero si prende il reso della divisione euclidea per x^2+x+1. Per evitare confusione, introduciamo il simbolo ξ per indicare la classe determinata da x, e otteniamo la descrizione seguente:

$$\frac{\mathbb{F}_2[x]}{(x^2+x+1)} = \{a+b\xi \mid a,b \in \mathbb{F}_2,\ \xi^2+x+1=0\}$$

Si tratta quindi dell'insieme $\{0,1,\xi,1+\xi\}$ con le operazioni descritte nelle tabelle che seguono:

$+$	0	1	ξ	$1+\xi$
0	0	1	ξ	$1+\xi$
1	1	0	$1+\xi$	ξ
ξ	ξ	$1+\xi$	0	1
$1+\xi$	$1+\xi$	ξ	1	0

$\cdot$	0	1	ξ	$1+\xi$
0	0	0	0	0
1	0	1	ξ	$1+\xi$
ξ	0	ξ	$1+\xi$	1
$1+\xi$	0	$1+\xi$	1	ξ

Osserviamo che in tale campo, il polinomio x^2+x+1 ha radice $x=\xi$. Infatti basta sostituire, e ottenere $\xi^2+\xi+1=0$ (per definizione!). Quindi, possiamo legittimamente denotare questo campo $\mathbb{F}_2(\xi)$, essendo l'estensione di $\mathbb{F}_2$ generata dalla radice ξ. Dividendo il nostro polinomio iniziale per $(x+\xi)$ si trova immediatamente la scomposizione in fattori lineari del polinomio

$$f(x) = x^2+x+1 = (x+\xi)(x+\xi+1)\,.$$

Vedremo in seguito che quello che abbiamo trovato è l'unico campo con quattro elementi, a meno di isomorfismi. Per questo, esso viene comunemente denotato $\mathbb{F}_4$.

Il prossimo lemma generalizza la discussione precedente.

Lemma 3.4.1 (Aggiunzione formale di radici)**.** *Sia* $p(x) \in F[x]$ *di grado* $n > 0$*, irriducibile su* F*; allora esiste un'estensione* $F \to E$*, con* $[E : F] = n$ *tale che* $p(x)$ *abbia una radice in* E*.*

Dimostrazione. Sia E l'anello quoziente $F[x]/(p(x))$. Chiaramente E è un campo, poiché l'ideale principale $(p(x))$ è massimale. Inoltre E estende F, poiché

$$F \simeq \{(p(x)) + a \mid a \in F\} \hookrightarrow E\,.$$

Dato che

$$\{1 + (p(x)), x + (p(x)), \ldots, x^{n-1} + (p(x))\}$$

è una base di E su F, si ha $[E : F] = n$.

Infine, l'elemento $x + (p(x)) \in E$ è la radice di $p(x)$ cercata. Infatti, sia $p(x) = p_0 + p_1 x + \cdots p_n x^n$. Si calcola:

$$p(x + (p(x))) = p_0 + p_1 \cdot (x + (p(x))) + \cdots p_n \cdot (x + (p(x)))^n\,.$$

Poiché negli sviluppi delle potenze $(x + (p(x)))^j$, tutti gli addendi tranne il primo contengono il fattore $(p(x))$ l'espressione precedente diventa

$$p_0 + p_1 x + \cdots p_n x^n + (p(x)) = p(x) + (p(x)) = (p(x)) = 0\,.$$

□

3.4.2 *Campi algebricamente chiusi*

Trattiamo solo le nozioni più elementari di un argomento che meriterebbe sicuramente più spazio.

Una delle proprietà rilevanti del campo $\mathbb{C}$ dei numeri complessi è che in esso ogni equazione algebrica ammette delle soluzioni.[3] In altre parole, $\mathbb{C}$ contiene tutti gli elementi algebrici che si possono definire a partire da polinomi a coefficienti nello stesso $\mathbb{C}$. Possiamo allora dare la definizione seguente.

Definizione 3.4.2. *Un campo* F *si dice* algebricamente chiuso *se non ammette estensioni algebriche proprie.*

La seguente caratterizzazione fornisce due altri punti di vista sulla nozione di campo algebricamente chiuso.

Proposizione 3.4.3. *Sia* F *un campo. Le seguenti affermazioni sono equivalenti:*

(i) F *è algebricamente chiuso.*

3 Tale proprietà va sotto il nome di *Teorema Fondamentale dell'Algebra*. Per una dimostrazione si veda, ad esempio [7]

(ii) *Ogni* $f(x) \in F[x] \setminus F$ *può essere scritto nella forma*

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)\,,$$

con $a, \alpha_1, \ldots, \alpha_n \in F$.

(iii) *Ogni* $f(x) \in F[x] \setminus F$ *ammette almeno una radice in* F.

Dimostrazione. (i) $\Rightarrow$ (ii). Per induzione sul grado n di $f(x)$. Se $n = 1$, il polinomio $f(x)$ è del tipo $ax + b$, e può essere ovviamente riscritto come

$$a\left(x + \frac{b}{a}\right)\,.$$

Sia allora $n > 1$. Supponiamo che α sia una radice di $f(x)$. Si ha che $\alpha \in F$, perché altrimenti $F(\alpha)$ sarebbe un'estensione algebrica propria di F. Per il teorema di Ruffini, si ha che $f(x) = (x - \alpha)g(x)$, con $g(x) \in F(x) \setminus F$ e $\deg(g(x)) = n - 1$. Possiamo allora applicare l'induzione e scrivere:

$$g(x) = a(x - \alpha_1) \cdots (x - \alpha_{n-1})\,,$$

e quindi sostituendo

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_{n-1})(x - \alpha)\,.$$

(ii) $\Rightarrow$ (iii). Se vale (ii) è chiaro che, ad esempio, $f(\alpha_1) = 0$.

(iii) $\Rightarrow$ (i). Sia E un'estensione algebrica di F, e $\alpha \in E$. Il polinomio minimo $m_\alpha(x) \in F[x]$ è irriducibile. Tuttavia, per (iii), esso ammette una radice in F, pertanto è di primo grado, e quindi $[E : F] = 1$. □

Esempio 3.4.4. Il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso. È una riformulazione del Teorema Fondamentale dell'Algebra.

Esempio 3.4.5. Il campo $\mathbb{A}$ dei numeri algebrici è algebricamente chiuso. Infatti, dato il polinomio:

$$f(x) = a_0 + a_1 x + \cdots a_n x^n \in \mathbb{A}[x]\,,$$

sia una radice α di $f(x)$. Ora, consideriamo la catena di estensioni algebriche semplici, dove l'estensione più a sinistra è algebrica perché $f(x) \in \mathbb{Q}(a_0, \ldots, a_n)[x]$:

$$\mathbb{Q} \longrightarrow \mathbb{Q}(a_0) \longrightarrow \mathbb{Q}(a_0, a_1) \longrightarrow \mathbb{Q}(a_0, \ldots, a_n) \longrightarrow \mathbb{Q}(a_0, \ldots, a_n)(\alpha)\,.$$

Per il Teorema 3.3.11, la loro composizione è un'estensione algebrica di $\mathbb{Q}$, e quindi $\alpha \in \mathbb{A}$.

3.4.3 *Campo di spezzamento di un polinomio*

Definizione 3.4.6. *L'estensione* $F \to \Sigma$ *è il* campo di spezzamento *del polinomio* $f(x) \in F[x]$ *se:*

1. $f(x)$ *spezza in* Σ*, i.e. si scompone nel prodotto di fattori lineari in* $\Sigma[x]$*;*
2. $f(x)$ *non spezza in alcun sottocampo proprio di* Σ*.*

Lemma 3.4.7. *Sia* $f(x) \in F[x]$ *di grado* $n > 0$*; allora esiste un'estensione* $F \to E$*, con* $[E : F] \leqslant n$ *tale che* $f(x)$ *abbia una radice in* E*.*

Dimostrazione. Basta considerare un fattore irriducibile $p(x)$ di $f(x)$, e applicare il Lemma 3.4.1. □

Teorema 3.4.8 (di esistenza del campo di spezzamento)**.** *Sia* $f(x) \in F[x]$ *di grado* $n > 0$*; allora esiste un'estensione* $F \to E$ *tale che* $f(x)$ *spezzi in* E*, con* $[E : F] \leqslant n!$*.*

Dimostrazione. Procediamo per induzione sul grado n di $f(x)$. Se $n = 1$, f è lineare. Pertanto $E = F$ e $[E : F] = 1! = 1$. Assumiamo ora che l'enunciato del teorema valga per $n-1$ e dimostriamolo per n. Per il Lemma 3.4.7, esiste un'estensione $F \to E_1$, con $[E : F] \leqslant n$, tale che $f(x)$ ammetta una radice in E_1. Sia α tale radice. In $E_1[x]$, $f(x) = (x-\alpha)f_1(x)$, con $f_1(x)$ di grado $n-1$. Pertanto, per l'ipotesi di induzione, esiste un'estensione $E_1 \to E$ tale che $f_1(x)$ spezzi in E, con $[E : F] \leqslant (n-1)!$. Allora anche $f(x) = (x-\alpha)f_1(x)$ spezza in E. Per la legge dei gradi, si ha:

$$[E : F] = [E : E_1] \cdot [E_1 : F] \leqslant n \cdot (n-1)! = n!$$

□

Corollario 3.4.9. *Sia* $f(x) \in F[x] \setminus F$ *di grado* n*; allora esiste un campo di spezzamento* $F \to \Sigma$ *di* $f(x)$ *su* F*.*

Dimostrazione. Poiché il campo di spezzamento di $f(x)$ è il minimo sottocampo di E che contiene tutte le radici di $f(x)$, se $\alpha_1, \dots \alpha_n$ sono tali radici, è sufficiente porre $\Sigma = F(\alpha_1, \dots \alpha_n)$. □

Osservazione 3.4.10. Nella dimostrazione del teorema, è indicata una procedura per costruire il campo E, e quindi Σ. Tuttavia, tale procedura presenta una certa arbitrarietà poiché si deve decidere da quale delle componenti irriducibili di $f(x)$ cominciare ad estendere F. Chi ci garantisce dunque che, cominciando da componenti irriducibili diverse di $f(x)$, si pervenga allo stesso risultato? In altre parole, supponiamo di procedere in un diverso ordine, e di costruire un altro campo di spezzamento Σ' di $f(x)$ su F. Che rapporto c'è tra Σ e Σ'? Vedremo che non solo Σ e Σ' sono isomorfi, ma che esiste un isomorfismo tra Σ e Σ' che fissa il campo F.

Per affrontare il problema dell'unicità (a meno di isomorfismi) del campo di spezzamento, è opportuno considerare una situazione un po' più generale. Per questo, riportiamo di seguito la definizione della *categoria delle estensioni*.

Definizione 3.4.11. *La categoria* ExtnFR *delle estensioni di campi in anelli è costituita dai seguenti dati:*

- oggetti: *monomorfismi di anelli commutativi unitari*

$$F \xrightarrow{i} R$$

  dove F *è un campo.*

- frecce: *dati due oggetti* $i\colon F \to R$ *e* $i'\colon F' \to R'$ *una freccia da* i *a* i' *è una coppia di omomorfismi di anelli commutativi unitari* $f\colon F \to F'$ *e* $g\colon R \to R'$ *tali che* $i' \circ f = g \circ i$*, cioè tali che il diagramma seguente commuti:*

$$\begin{array}{ccc} F & \xrightarrow{i} & R \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ F' & \xrightarrow[i']{} & R' \end{array}$$

Osserviamo che, poiché F, F' sono campi, f è sicuramente un monomorfismo. Se i e i' sono inclusioni, diremo che g estende f, e scriveremo $g|_F = f$. Nel resto di questa sezione, ci occuperemo esclusivamente del caso in cui f e g siano isomorfismi.

Prima di provare il prossimo lemma, ricordiamo una importante conseguenza della proprietà universale dell'anello di polinomi $F[x]$ (vedi Esempio 3.1.11): dato un (iso)morfismo di campi $\tau\colon F \to F'$, si considera l'(iso)morfismo indotto $\bar{\tau}$ tra i rispettivi anelli di polinomi nell'indeterminata x, con

$$\bar{\tau}(a_0 + a_1 x + \cdots a_n x^n) = \tau(a_0) + \tau(a_1)x + \cdots \tau(a_n)x^n\,.$$

Ovviamente tale (iso)morfismo è tale che $\bar{\tau}_{|_F} = \tau$, pertanto determina la freccia $(\tau, \bar{\tau})$ di Extn rappresentata di seguito:

$$\begin{array}{ccc} F & \xrightarrow{j} & F[x] \\ {\scriptstyle \tau}\downarrow & & \downarrow{\scriptstyle \bar{\tau}} \\ F' & \xrightarrow[j']{} & F'[x] \end{array}$$

Lemma 3.4.12. *Siano dati un polinomio* $p(x) \in F[x] \setminus F$ *irriducibile su* F*, due estensioni* $i\colon F \to E$ *e* $i'\colon F' \to E'$ *e un isomorfismo di campi* $\tau\colon F \to F'$*. Se* α *è un elemento di* E *tale che* $p(\alpha) = 0$ *e* α' *un elemento di* E' *tale che* $\bar{\tau}p(\alpha') = 0$*, allora esiste un isomorfismo* $\varphi\colon F(\alpha) \to F(\alpha')$ *tale che*

$\varphi(\alpha) = \alpha'$, *e che il seguente diagramma commuti (le frecce orizzontali siano le inclusioni canoniche):*

$$\begin{array}{ccc} F & \longrightarrow & F(\alpha) \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\varphi} \\ F' & \longrightarrow & F'(\alpha') \end{array}$$

In particolare, se $\alpha, \beta \in E$ *sono radici di un polinomio irriducibile* $p(x) \in F[x] \setminus F$, *esiste un isomorfismo* $\varphi\colon F(\alpha) \to F(\beta)$ *tale che*

$$\varphi(\alpha) = \beta \quad e \quad \varphi_{|_F} = \mathrm{id}_F\,.$$

Dimostrazione. Possiamo supporre, senza perdere in generalità, che il polinomio $p(x)$ sia monico. Consideriamo la restrizione alle immagini degli omomorfismi di valutazione:

$$\epsilon_\alpha\colon F[x] \to F(\alpha) \quad \text{dato da} \quad \epsilon_\alpha(f(x)) = f(\alpha)$$

$$\epsilon_{\alpha'}\colon F'[x] \to F'(\alpha') \quad \text{dato da} \quad \epsilon_{\alpha'}(g(x)) = g(\alpha')$$

Chiaramente, $\mathrm{Ker}(\epsilon_\alpha) = (p(x))$. Considerato il generico elemento

$$f(x)p(x) \in (p(x))$$

si ha

$$\epsilon_{\alpha'} \circ \bar\tau\big((f(x)p(x))\big) = \epsilon_{\alpha'}\big((\bar\tau f(x)\,\bar\tau p(x))\big) = \bar\tau f(\alpha')\,\bar\tau p(\alpha') = \bar\tau f(\alpha')\,0 = 0$$

Quindi, per la proprietà universale del quoziente, esiste un unico omomorfismo di anelli unitari φ che rende commutativo il diagramma seguente:

$$\begin{array}{ccc} F[x] & \xrightarrow{\epsilon_\alpha} & F(\alpha) \\ & {\scriptstyle\epsilon_{\alpha'}\circ\bar\tau}\searrow & \downarrow{\scriptstyle\varphi} \\ & & F'(\alpha') \end{array}$$

Inoltre, φ è iniettivo perché $F(\alpha)$ e $F'(\alpha')$ sono campi, ed è anche suriettivo perché anche $\epsilon_{\alpha'} \circ \bar\tau$ lo è: in conclusione φ è un isomorfismo di campi, che si restringe a τ per costruzione.

Infine, se $\alpha, \beta \in E$ sono radici di $p(x) \in F[x] \setminus F$, l'ultima affermazione si ottiene considerando il caso $\tau = \mathrm{id}_F$. □

Teorema 3.4.13. *Sia* $\tau\colon F \to F'$ *un isomorfismo di campi, e siano* $f(x) \in F[x]$ *e* $g(x) \in F'[x]$ *tali che* $\bar\tau(f(x)) = g(x)$. *Se* $F \to \Sigma$ *è un campo di spezzamento di* $f(x)$ *e* $F' \to \Sigma'$ *è un campo di spezzamento di* $g(x)$, *allora l'isomorfismo* τ *si estende a un isomorfismo* $\sigma\colon \Sigma \to \Sigma'$.

Dimostrazione. Per induzione su $n = \deg(f(x))$. Se $n = 1$, Σ (risp. Σ') è isomorfo a F (risp. F'), e non c'è null'altro da dimostrare.

Supponiamo allora che il teorema valga per $n-1$, dimostriamolo per n. Senza perdere in generalità, possiamo supporre $f(x)$ e $g(x)$ monici. Consideriamo la fattorizzazione

$$f(x) = p_1(x) \cdot \cdots \cdot p_m(x)$$

dove i polinomi $p_j(x)$ sono monici e irriducibili in $F[x]$, per $j = 1, \ldots, m$. Ovviamente

$$\bar{\tau}(f(x)) = \bar{\tau}(p_1(x)) \cdot \cdots \cdot \bar{\tau}(p_m(x))$$

è una fattorizzazione di $g(x)$ nel prodotto di polinomi monici irriducibili in $F'[x]$. Se $\alpha \in \Sigma$ è una radice di $p_1(x)$, e $\alpha' \in \Sigma'$ è una radice di $\bar{\tau}(p_1(x))$, per il lemma precedente, esiste un isomorfismo di campi $\varphi\colon F(\alpha) \to F'(\alpha')$ che estende τ. La situazione è descritta dal diagramma seguente:

$$\begin{array}{ccccc} F & \longrightarrow & F(\alpha) & \longrightarrow & \Sigma \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\varphi} & & \\ F' & \longrightarrow & F'(\alpha') & \longrightarrow & \Sigma' \end{array}$$

Ora, per il teorema di Ruffini, $f(x) = (x-\alpha)f_1(x)$ in $F(\alpha)[x]$, con $\deg(f_1(x)) = n-1$. Chiaramente Σ risulta essere un campo di spezzamento per $f_1(x)$ su $F(\alpha)$, e analogamente Σ' è un campo di spezzamento per $g_1(x) = \bar{\tau}(f_1(x))$ su $F'(\alpha')$. Quindi possiamo applicare l'ipotesi di induzione a $f_1(x)$ e $g_1(x)$, ed estendere l'isomorfismo φ ad un isomorfismo $\sigma\colon \Sigma \to \Sigma'$, come mostrato di seguito:

$$\begin{array}{ccccc} F & \longrightarrow & F(\alpha) & \longrightarrow & \Sigma \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\sigma} \\ F' & \longrightarrow & F'(\alpha') & \longrightarrow & \Sigma' \end{array}$$

Ovviamente si ha:

$$\sigma_{|F} = (\sigma_{|F(\alpha)})_{|F} = \varphi_{|F} = \tau\,.$$

□

Corollario 3.4.14. *Dato $f(x) \in F[x] \setminus F$, siano $F \to \Sigma$ e $F \to \Sigma'$ due campi di spezzamento di $f(x)$. Allora esiste un isomorfismo di campi $\sigma\colon \Sigma \to \Sigma'$ che fissa F, i.e. tal che $\sigma_{|F} = \mathrm{id}$.*

Dimostrazione. Basti applicare il teorema al caso particolare $\tau = \mathrm{id}$. □

Esempio 3.4.15. Vogliamo calcolare il campo di spezzamento Σ del polinomio $f(x) = x^6 - 5$ sul campo $\mathbb{Q}[x]$. Si osserva subito che

$$x^6 - 5 = (x^3 - \sqrt{5})(x^3 + \sqrt{5}) = (x - \sqrt[6]{5})(x^2 + \sqrt[6]{5}x + \sqrt[3]{5})(x + \sqrt[6]{5})(x^2 - \sqrt[6]{5}x + \sqrt[3]{5})\,.$$

Inoltre, i polinomi di secondo grado $x^2 + \sqrt[6]{5}x + \sqrt[3]{5}$ e $x^2 - \sqrt[6]{5}x + \sqrt[3]{5}$ sono irriducibili su $\mathbb{Q}(\sqrt[6]{5})$ in quanto non hanno radici in tale campo.

Il campo di spezzamento Σ si ottiene estendendo il campo $\mathbb{Q}(\sqrt[6]{5})$ con una radice sesta primitiva dell'unità, ad esempio $\omega = e^{\frac{\pi i}{3}}$, la quale soddisfa la relazione $\omega^2 - \omega + 1 = 0$. Infatti risulta che $\sqrt[6]{5}\omega$ è radice del polinomio $x^2 - \sqrt[6]{5}x + \sqrt[3]{5}$ e $\sqrt[6]{5}\omega^2$ è radice di $x^2 + \sqrt[6]{5}x + \sqrt[3]{5}$. Inoltre si ha che

$$[\Sigma : \mathbb{Q}(\sqrt[6]{5})] = 2,$$

in quanto il polinomio $x^2 - x + 1$ è un polinomio monico, irriducibile su $\mathbb{Q}(\sqrt[6]{5})$ ed ammette ω come radice, ovvero è il polinomio minimo di ω sul campo $\mathbb{Q}(\sqrt[6]{5})$. Infine, sfruttando il Teorema dei Gradi, si osserva che

$$[\Sigma : \mathbb{Q}] = [\Sigma : \mathbb{Q}(\sqrt[6]{5})][\mathbb{Q}(\sqrt[6]{5}) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

Proposizione 3.4.16 (Teorema dell'elemento primitivo in caratteristica 0)**.** *Ogni estensione finita di un campo con caratteristica* 0 *è una estensione semplice.*

3.5 CAMPI FINITI

Nella trattazione della teoria dei campi, ci siamo tenuti sin qui su di un livello generalmente astratto, indulgendo solo qualche volta a analizzare in modo specifico i campi in caratteristica 0. Per questo, la maggior parte dei risultati presentati si applicano (anche) ai campi finiti, che necessariamente hanno caratteristica positiva.

In questa sezione si affronterà *prevalentemente* il caso finito, e si analizzeranno alcune sue peculiarità.

3.5.1 *Polinomi separabili*

Definizione 3.5.1. *Sia* F *campo. Un polinomio* $f(x) \in F[x]$ *è* separabile *se non ha radici multiple nel suo campo di spezzamento.*

Studiare la separabilità usando solo la definizione è un'opzione di solito poco praticabile, poiché il campo di spezzamento di un polinomio può essere difficile da determinare. Il lemma che segue ci fornisce una caratterizzazione della separabilità che si traduce in un criterio molto più semplice e veloce.

Lemma 3.5.2. *Il polinomio* $f(x) \in F[x]$ *ha qualche radice multipla se e solo se*

$$\deg(\mathrm{MCD}(f(x), f'(x))) > 0$$

dove $f'(x)$ *è la derivata (formale) di* $f(x)$*.*

Dimostrazione. Se $f(x)$ ha almeno una radice multipla α appartenente a qualche estensione di F, allora, per il Teorema di Ruffini, possiamo scrivere

$$f(x) = (x - \alpha)^2 g(x)\,,$$

da cui

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\,.\big)$$

Concludiamo che $(x-\alpha)$ divide $\mathsf{MCD}(f(x), f'(x))$, che pertanto ha grado almeno 1.

Viceversa, sia

$$d(x) = \mathsf{MCD}(f(x), f'(x))\,.$$

e sia α una radice di $d(x)$. A maggior ragione, α è radice anche di $f(x)$, per cui possiamo scrivere

$$f(x) = (x-\alpha)g(x)\,,$$

$$f'(x) = g(x) + (x-\alpha)g'(x)\,.$$

Dall'ultima espressione ricaviamo

$$g(x) = f'(x) - (x-\alpha)g'(x)\,,$$

e poiché $(x-\alpha)$ divide anche $f'(x)$, si ottiene immediatamente che $(x-\alpha)$ divide $g(x)$, e di conseguenza $(x-\alpha)^2$ divide $f(x)$. □

Osservazione 3.5.3. Per capire la rilevanza del corollario appena dimostrato, presentiamo un'utile analogia con la nozione di curvatura di una superficie immersa in $\mathbb{R}^3$. Consideriamo ad esempio la Terra, la cui superficie, come ben sappiamo, è curva. Per verificare questo fatto, abbiamo due possibilità

1. Andiamo nello spazio e, rivolgendo lo sguardo verso il nostro pianeta e costatiamo che si tratta di una superficie curva.

2. Misuriamo, ad esempio, la somma degli angoli di un triangolo disegnato sulla sua superficie. Se sceglieremo un triangolo sufficiente grande, sarà facile constatare che la somma degli angoli sia maggiore di 180 gradi, testimoniando così il fatto che la superficie è curva.

In effetti, senza entrare nei dettagli tecnici (per i quali si rimanda a un qualunque buon manuale di geometria) la curvatura di una superficie in un punto P è un numero reale che misura di quanto la superficie si discosti dal piano tangente in quel punto[4]. Se la curvatura è 0, la superficie è piatta, altrimenti avremo curvature positive o negative, per superfici, rispettivamente, concave o convesse.

Tornando alla nozione di separabiltà, utilizzando solo la definizione, non possiamo determinare se un polinomio sia separabile restando

4 Più precisamente, se ruotiamo la superficie (che deve essere almeno due volte differenziabile) in modo che il piano tangente in P sia orizzontale, la cosiddetta *curvatura gaussiana* in $P = (x_0, y_0, f(x_0, y_0))$ è il determinante dell'hessiano di f in (x_0, y_0). Il fatto che la curvatura sia una proprietà intrinseca di una superficie è il cosiddetto *Teorema Egregium* dimostrato da Carl Friedrich Gauss (1827).

nel campo in cui esso è definito (*sulla superficie)*, ma dobbiamo andare nel suo campo di spezzamento (*nello spazio*). Utilizzando invece il lemma, la nozione diventa intrinseca, propria dell'anello $F[x]$ in cui il polinomio è definito.

Il corollario seguente sarà utile nel seguito.

Corollario 3.5.4. *Sia* F *un campo, e* $f(x) \in F[x] \setminus F$.

(i) Se la caratteristica di F *è zero, e* $f(x)$ *è irriducibile, allora* $f(x)$ *è separabile.*

(ii) Se la caratteristica di F *è* p*, e* $(p, n) = 1$*, il polinomio*

$$x^n - 1$$

è separabile.

Dimostrazione. (i) Ovvio per il Lemma 3.5.2.

(ii) Anche in questo caso, il risultato segue dal lemma precedente. Infatti, se $f(x) = x^n - 1$, si ha $f'(x) = nx^{n-1}$, che non è il polinomio nullo, perché $(p, n) = 1$. Quindi $\mathrm{MCD}(f(x), f'(x)) = 1$. □

3.5.2 *Endomorfismo di Frobenius*

Proposizione 3.5.5. *Sia* F *un campo di caratteristica* p*. L'applicazione*

$$\Phi \colon F \to F, \qquad a \mapsto a^p$$

è un monomorfismo di campi, detto monomorfismo di Frobenius*, che fissa il sottocampo primo di* F.

Dimostrazione. Poiché i multipli di p fanno zero in F, per ogni $a, b \in F$ si ha

$$\Phi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k} = a^p + b^p = \Phi(a) + \Phi(b)$$

Infine, è semplice verificare che

$$\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b), \qquad \Phi(0) = 0^p = 0, \qquad \Phi(1) = 1^p = 1.$$

Inoltre, poiché l'ordine del gruppo moltiplicativo di $\mathbb{F}_p$ è $p-1$, per ogni $a \in \mathbb{F}_p$ si ha:

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

□

Il monomorfismo di Frobenius non è necessariamente suriettivo. Vale infatti la seguente definizione.

Definizione 3.5.6. *Un campo* F *si dice* perfetto *se il monomorfismo di Frobenius* Φ_F *è suriettivo.*

Sono perfetti, ovviamente, tutti i campi finiti. Il prossimo esempio dimostra tuttavia che non tutti i campi in caratteristica positiva sono perfetti.

Esempio 3.5.7. Consideriamo il campo

$$F = \mathbb{F}_p(t)$$

delle funzioni razionali a coefficienti in $\mathbb{F}_p$. Non è difficile verificare che

$$t \notin \Phi_F(F)\,.$$

Infatti, se così fosse, ci sarebbero due polinomi $f(x), g(x) \in F[x]$ tali che

$$t = \left(\frac{f(x)}{g(x)}\right)^p\,.$$

Uguagliando i gradi, si ottiene

$$1 = p \cdot \deg(f) - p \cdot \deg(g) = p \cdot (\deg(f) - \deg(g))$$

che è assurdo, poiché p non divide 1.

3.5.3 *Classificazione dei campi finiti*

Lemma 3.5.8. *Se* F *è un campo finito con* q *elementi, allora* $q = p^n$*, dove* p *è la caratteristica di* F*.*

Dimostrazione. La tesi deriva immediatamente dal fatto che F è spazio vettoriale sul suo sottocampo primo $\mathbb{F}_p$. □

Teorema 3.5.9 (di classificazione dei campi finiti)**.** *Sia* F *un campo finito. Allora* $|F| = q = p^n$ *se e solo se* F *è il campo di spezzamento del polinomio* $x^q - x$ *su* $\mathbb{F}_p$*.*

Dimostrazione. Sia F un campo finito con esattamente $q = p^n$ elementi. Poiché $q-1$ è l'ordine del gruppo moltiplicativo di F, per ogni $a \in F^\times$ si ha che $a^{q-1} = 1$, da cui $a^q = a$. Quindi abbiamo $q-1$ radici non nulle distinte di $x^q - x$. A queste possiamo aggiungere $0 \in F$, in modo da ottenere esattamente q radici distinte di $x^q - x$. Poiché esse formano un campo, F, esso è il campo di spezzamento di $x^q - x$, sul sottocampo primo $\mathbb{F}_p$ di F.

Viceversa, sia F il campo di spezzamento di $x^q - x$ su $\mathbb{F}_p$. Ovviamente, F contiene l'insieme E delle radici di $x^q - x$. Dimostreremo che E è un campo, e che $|E| = p^q$. In effetti, la seconda asserzione segue immediatamente dal Lemma 3.5.2, poiché $x^q - x = x(x^{q-1} - 1)$,

e $(p, q-1) = 1$. Per quanto riguarda la prima asserzione, supponiamo che a e b siano due radici di $x^q - x$. Ragionando come per la definizione del monomorfismo di Frobenius, si ha:

$$(a-b)^q - (a-b) = a^q - b^q - a + b = a^q - a - (b^q - b) = 0 - 0 = 0\,.$$

(Si osservi che q è pari se e solo se $p = 2$, e in questo caso $1 = -1$.) Inoltre, se $b \neq 0$, si ha:

$$(ab^{-1})^q = a^q (b^{-1})^q = a^q (b^q)^{-1} = ab^{-1}\,,$$

da cui anche ab^{-1} è radice di $x^q - x$. Ovviamente, $0^q = 0$ e $1^q = 1$, per cui concludiamo che E è un campo che contiene le radici di $x^q - x$, e poiché $E \subseteq F$, concludiamo $E = F$, e di conseguenza $|F| = |E| = q = p^n$. □

In particolare, il teorema ci dice che, per ogni potenza di p e per ogni $n > 0$, esiste, ed è essenzialmente unico, un campo di ordine p^n. L'unicità è data dall'unicità a meno di isomorfismi del campo di spezzamento.

Poiché sono definiti dalla loro cardinalità, i campi finiti di ordine q meritano un nome. D'ora un poi, indicheremo con $\mathbb{F}_q$ (o con $\mathsf{GF}(q)$) il campo finito di ordine $q = p^n$.

Proposizione 3.5.10. *Sia F campo finito. Il suo gruppo moltiplicativo $(F^\times, \cdot, 1)$ è un gruppo ciclico.*

Dimostrazione. $F^\times$ è gruppo abeliano finito di ordine $p^n - 1$. Considero la sua scomposizione primaria, i.e. nel prodotto di p_i-sottogruppi massimali:

$$F^\times \cong P_{p_1} \times \cdots \times P_{p_r}$$

dove, per $i = 1, \ldots, r$, indichiamo con p_i i primi distinti che compaiono nella fattorizzazione di $p^n - 1$. Per dimostrare che $F^\times$ è ciclico, sarà sufficiente dimostrare che P_{p_i} è ciclico, per ogni i.

Fissato i, sia $|P_{p_i}| = p_i^\alpha$. Per il teorema di classificazione dei gruppo abeliani finiti (Teorema 2.4.13), si ha che ogni gruppo P_{p_i} è isomorfo a un prodotto di gruppi ciclici $C_{p_i^{\alpha_1}} \times \cdots \times C_{p_i^{\alpha_t}}$, con $\alpha_1 + \cdots + \alpha_t = \alpha$. Supponiamo, per assurdo, che il massimo ordine di un elemento di P_{p_i} sia $p_i^{\alpha_1} < p_i^\alpha$. Allora, per ogni $a \in P_{p_i}$, si ha

$$a^{p_i^{\alpha_1}} = 1\,,$$

e questo implica che il polinomio $x^{p_i^{\alpha_1}} - 1$ ha un numero di radici superiore al suo grado, fatto, questo, impossibile in un campo. □

Corollario 3.5.11. *Per ogni primo p, e per ogni intero positivo n, esiste un polinomio di grado n, irriducibile su $\mathbb{F}_p$.*

Dimostrazione. Sia $q = p^n$. Come visto, il gruppo $\mathbb{F}_q^\times$ è ciclico. Pertanto, esiste un elemento $\alpha \in \mathbb{F}_q^\times$ tale che

$$\mathbb{F}_q^\times = \{1 = \alpha^0, \alpha, \alpha^2, \dots, \alpha^{q-2}\}.$$

Dunque, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, con $[\mathbb{F}_q : \mathbb{F}_p] = n$. In particolare, α è algebrico su $\mathbb{F}_p$, con un certo polinomio minimo $m_\alpha(x)$ irriducibile su $\mathbb{F}_p$. □

Il prossimo corollario è un altro caso particolare del *Teorema dell'elemento primitivo*, che abbiamo già visto in caratteristica 0 (Proposizione 3.4.16). Più in generale, esso è così formulato: che ogni estensione finita *separabile* è semplice[5].

Corollario 3.5.12. *Ogni estensione finita di $\mathbb{F}_p$ è semplice.*

Vale un risultato più generale della Proposizione 3.5.10. Omettiamo la dimostrazione, che può essere trovata in [**?**].

Proposizione 3.5.13. *Sia F un campo, e sia A un sottogruppo finito di $(F^\times, \cdot, 1)$. Allora A è un gruppo ciclico.*

Osserviamo che l'ipotesi di finitezza è essenziale. Infatti, $\mathbb{R}^\times$ è sicuramente un sottogruppo di $\mathbb{C}^\times$, ma non è ciclico (perché?).

3.6 POLINOMI CICLOTOMICI E RADICI DELL'UNITÀ

Abbiamo visto che per costruire il campo $\mathbb{F}_q$, con $q = p^m$ elementi, siamo portati a considerare le radici $(q-1)$-esime di 1. Infatti, $\mathbb{F}_q$ può essere costruito come campo di spezzamento del polinomio:

$$x^q - x = x(x^{q-1} - 1).$$

Più in generale, anche in caratteristica 0, se n è un numero positivo, le radici n-esime dell'unità formano un gruppo moltiplicativo finito, che denotiamo Γ_n. Esso è necessariamente ciclico per la Proposizione 3.5.13; inoltre, se la caratteristica del campo è 0, o se la caratteristica è coprima con n, il Corollario 3.5.4 garantisce che $x^n - 1$ sia separabile, e di conseguenza Γ_n ha ordine n.

D'ora in poi assumeremo tacitamente che $x^n - 1$ sia separabile.

Definizione 3.6.1. *Sia ξ una radice n-esima dell'unità. Diremo che ξ è* radice primitiva n-esima *se essa è un generatore di Γ_n.*

Proposizione 3.6.2. *Sia ξ radice primitiva n-esima di $1 \in F$, con $x^n - 1 \in F[x]$ separabile. Dato $k \in \mathbb{Z}$, si ha che ξ^k è primitiva se e solo se $(n, k) = 1$. Più in generale, il periodo di ξ^k è*

$$\frac{n}{MCD(n,k)}.$$

5 Ricordiamo che in caratteristica 0, la separabilità è gratis!

Dimostrazione (traccia). È sufficiente osservare che la funzione $\Gamma_n \to \mathbb{Z}_n$ data dalla posizione $\xi^k \mapsto k$, definisce un isomorfismo tra Γ_n e il gruppo additivo degli interi modulo n. □

Le radici primitive n-esime sono quindi esattamente $\phi(n)$, dove

$$\phi\colon \mathbb{N}^\times \to \mathbb{N}^\times$$

è la funzione *totiente* di Eulero, che dato un numero n, restituisce il numero dei valori positivi minori di n, coprimi con n. Richiamiamo di seguito qualche proprietà della funzione totiente.

- (Teorema di Eulero). Se $(a, n) = 1$, si ha che

  $$a^{\phi(n)} \equiv 1 \mod n,.$$

  La dimostrazione è una applicazione immediata del teorema di Lagrange.

Le prossime proprietà sono utili, nello specifico, per calcolare il valore di $\phi(n)$.

- Se $(a, b) = 1$, si ha che

  $$\phi(ab) = \phi(a) \cdot \phi(b)$$

  La dimostrazione si ottiene osservando che, se $(a, b) = 1$, *si ha un isomorfismo di anelli* $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$, *e che questo si restringe ovviamente ai rispettivi gruppi degli elementi unitari.*

- Se p è un numero primo,

  $$\phi(p) = p - 1\,.$$

- Più in generale, sempre con p primo

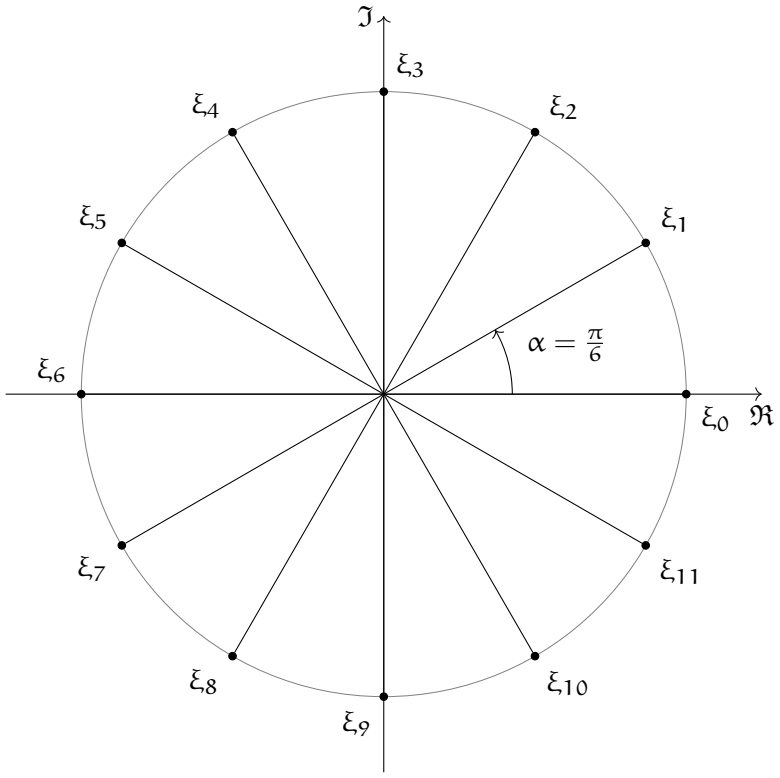
  $$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)\,.$$

3.6.1 *Case study: radici* 12*-esime dell'unità in* $\mathbb{C}$

Descriviamo le radici 12-esime dell'unità nel piano complesso, individuando quelle primitive. Iniziamo cercando le soluzioni dell'equazione $\xi^n = 1$ in $\mathbb{C}$. Poiché $1 = e^{2k\pi i}$ con $k \in \mathbb{Z}$, esse si ottengono immediatamente:

$$\xi_k = e^{\frac{2k\pi}{n} i} \qquad \text{con} \qquad k = 0, \ldots, 11\,.$$

I valori di ξ_k giacciono sulla circonferenza unitaria nel piano complesso, come si può osservare nel grafico riportato di seguito:



In effetti, se poniamo $\xi = \xi_1$, si osserva che, per ogni intero k, vale $\xi^k = \xi_k$. Quindi possiamo definire un isomorfismo di gruppi $\Gamma_{12} \to \mathbb{Z}_{12}$ dato dalla posizione $\xi_k \mapsto k$. Concludiamo che le radici primitive 12-esime dell'unità corrispondono ai generatori del gruppo additivo $\mathbb{Z}_{12}$, e quindi sono $\xi_1, \xi_5, \xi_7, \xi_{11}$.

È anche interessante indagare le proprietà delle altre radici 12-esime dell'unità. Se le quattro che abbiamo individuato sono infatti primitive 12-esime, anche le altre saranno primitive relativamente ai diversi divisori di 12. Classifichiamo allora tutte le radici 12-esime in base al loro periodo d come elementi di Γ_{12}.

$d = 1$ L'unico elemento di periodo 1 di un gruppo è l'identità del gruppo. Pertanto, si ha $\xi_0 = \xi^0 = 1$.

$d = 2$ Il valore $\xi_6 = -1$ ha periodo 2, ovvero -1 è la radice quadrata primitiva dell'unità.

$d = 3$ I valori $\xi_4 = e^{\frac{2\pi}{3}i}$ e $\xi_8 = e^{\frac{4\pi}{3}i}$ hanno periodo 3. Essi rappresentano le due radici cubiche primitive dell'unità. Sono complesse coniugate, e in forma cartesiana si rappresentano $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$ rispettivamente. Di solito si pone $\xi_4 = \omega$, per cui si ha $\xi_8 = \omega^2 = \overline{\omega}$.

$d = 4$ I valori $\xi_3 = e^{\frac{\pi}{2}i}$ e $\xi_9 = e^{\frac{3\pi}{2}i}$ hanno periodo 4. Essi rappresentano le due radici quarte primitive dell'unità. La prima è l'unità immaginaria i, la seconda è $-i$.

$d = 6$ I valori $\xi_2 = e^{\frac{\pi}{3}i}$ e $\xi_{10} = e^{\frac{5\pi}{3}i}$ hanno periodo 6. Essi rappresentano le due radici seste primitive dell'unità. Sono complesse coniugate, e in forma cartesiana si rappresentano $\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e $\frac{1}{2} - i\frac{\sqrt{3}}{2}$ rispettivamente. Con la notazione vista sopra, $\xi_2 = -\omega^2 = -\overline{\omega}$ e $\xi_{10} = -\omega$.

$d = 12$ Le radici restanti sono primitive 12-esime. Come abbiamo già osservato, esse sono:

$$\xi_1 = e^{\frac{\pi}{6}i}, \quad \xi_5 = e^{\frac{5\pi}{6}i}, \quad \xi_7 = e^{\frac{7\pi}{6}i}, \quad \xi_{11} = e^{\frac{11\pi}{6}i},$$

o in notazione cartesiana, rispettivamente:

$$\frac{\sqrt{3}}{2} + \frac{1}{2}i, \quad -\frac{\sqrt{3}}{2} + \frac{1}{2}i, \quad -\frac{\sqrt{3}}{2} - \frac{1}{2}i, \quad \frac{\sqrt{3}}{2} - \frac{1}{2}i.$$

Ora, avendo esplicitato le dodici radici distinte del polinomio $x^{12} - 1$, possiamo scomporre quest'ultimo nel prodotto di fattori lineari:

$$\begin{aligned} x^{12} - 1 \;=\; & (x - \xi_0)(x - \xi_1)(x - \xi_2)(x - \xi_3)(x - \xi_4)(x - \xi_5)(x - \xi_6) \cdot \\ & \cdot (x - \xi_7)(x - \xi_8)(x - \xi_9)(x - \xi_{10})(x - \xi_{11}). \end{aligned}$$

È interessante raggruppare i fattori in base al periodo d delle radici.

- Per $d = 1$ si ha: $(x - \xi_0) = (x - 1)$.
- Per $d = 2$ si ha: $(x - \xi_6) = (x + 1)$.
- Per $d = 3$ si ha: $(x - \xi_4)(x - \xi_8) = x^2 + (\xi_4 + \xi_8)x + \xi_4\xi_8 = x^2 + x + 1$.
- Per $d = 4$ si ha: $(x - \xi_3)(x - \xi_9) = (x - i)(x + i) = x^2 + 1$.
- Per $d = 6$ si ha: $(x - \xi_2)(x - \xi_{10}) = x^2 + (\xi_2 + \xi_{10})x + \xi_2\xi_{10} = x^2 - x + 1$.
- Per $d = 12$ si ha: $(x - \xi_1)(x - \xi_5)(x - \xi_7)(x - \xi_{11}) = x^4 - x^2 + 1$.

Si verifica che i polinomi ottenuti sono irriducibili su $\mathbb{Q}$. Pertanto, possiamo effettuare la scomposizione:

$$x^{12} - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1),$$

dove ogni fattore ha come radici tutte e sole le radici primitive d-esime dell'unità, per ogni divisore d di 12.

I polinomi che abbiamo trovato si chiamano cicolotomici[6], e sono l'oggetto della prossima sezione.

6 La *ciclotomia* è un problema classico della geometria, che consiste nella divisione di una circonferenza in n archi della stessa ampiezza, con l'uso di riga e compasso.

3.6.2 *Polinomi ciclotomici*

Definizione 3.6.3. *L'n-esimo polinomio ciclotomico a coefficienti nel campo F è*

$$\Phi_n(x) = (x-\rho_1)(x-\rho_2)\cdots\left(x-\rho_{\phi(n)}\right)$$

dove $\rho_1, \rho_2, \ldots, \rho_{\phi(n)}$ sono le radici primitive n-esime di $1 \in F$.

Osserviamo che $\deg(\Phi_n) = \phi(n)$.

Lemma 3.6.4. *Per ogni n positivo,*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)\,.$$

Dimostrazione. Siano $\xi_0, \ldots, \xi_{n-1}$ le n radici di $x^n - 1$, allora:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \xi_i)\,.$$

Quindi, posso cambiare l'ordine dei fattori ed ottenere:

$$x^n - 1 = \prod_{d|n} \left(\prod_{o(\xi_\alpha)=d} (x-\xi_\alpha) \right) = \prod_{d|n} \Phi_n(x)\,.$$

dove con $o(\xi_\alpha)$ si è indicato il periodo di ξ_α. □

Proposizione 3.6.5. *Per ogni intero positivo n si ha:*

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\, d\neq n} \Phi_d(x)}$$

Inoltre, $\Phi_n(x)$ ha i coefficienti in R, sottoanello fondamentale del campo F.

Dimostrazione. Per induzione (forte) su n. Per $n = 1$, si ha $\Phi_1(x) = x - 1 \in R[x]$. Sia allora $n > 1$. Dalla proposizione precedente possiamo scrivere

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{d|n,\, d\neq n} \Phi_d(x)$$

da cui si ottiene la formula cercata. Ora, per ipotesi di induzione, per ogni $d < n$, $\Phi_d(x) \in R[x]$, quindi necessariamente anche il rapporto tra $x^n - 1$ e il prodotto dei diversi $\Phi_d(x)$ ha i coefficienti in R. □

La Proposizione 3.6.5 ci permette di calcolare ricorsivamente i polinomi ciclotomici.

Esempio 3.6.6. Sia p un numero primo. Si ha che

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1\,.$$

Infatti,

$$\Phi_1(x) \cdot \Phi_p(x) = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$$

$$= x^p + x^{p-1} + \cdots + x^2 + x - (x^{p-1} + x^{p-2} + \cdots + x + 1) = x^p - 1$$

È facile verificare che il polinomio ciclotomico $\Phi_p(x)$, calcolato nell'esempio precedente, è irriducibile su $\mathbb{Q}$. Infatti, è sufficiente operare la sostituzione $x \mapsto x+1$ e calcolare

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p-1}{(x+1)-1} = \frac{1}{x}\sum_{i=1}^{p}\binom{p}{i}x^i \\ &= p+\binom{p}{2}x+\cdots+\binom{p}{p-1}x^{p-2}+x^{p-1}\,.\end{aligned}$$

Quest'ultimo polinomio, $\Phi_p(x+1)$, è irriducibile per il criterio di Eisenstein, e dunque necessariamente anche $\Phi_p(x)$ lo è.

La prossima proposizione mostra che quanto si è dimostrato per $\Phi_p(x)$ vale ben più in generale.

Proposizione 3.6.7. *Per ogni intero positivo n, $\Phi_n(x)$ è irriducibile su $\mathbb{Q}$.*

Dimostrazione. Vedi [4]. □

In caratteristica positiva, la situazione è molto diversa. L'esempio che segue illustra proprio questo punto.

Esempio 3.6.8. Il polinomio ciclotomico $\Phi_8(x) = x^4+1$ è *riducibile* in tutti i campi di caratteristica positiva.

In effetti, possiamo dimostrare che $\Phi_8(x)$ è riducibile su $\mathbb{F}_p$, per ogni primo p. Per cominciare, $x^4+1 = (x+1)^4$ in $\mathbb{F}_2[x]$. Sia allora p un numero primo dispari. Il grado del campo di spezzamento di $\Phi_8(x)$ su $\mathbb{F}_p$ è dato dal minimo numero naturale k tale per cui $8|(p^k-1)$, in quanto le radici di $\Phi_8(x)$ sono le radici primitive ottave dell'unità e la parte moltiplicativa di un campo finito è un gruppo ciclico. Ora, se $p \equiv 1 \mod 8$, si ha $k=1$, per cui $\Phi_8(x)$ spezza in fattori lineari già in $\mathbb{F}_p[x]$. Se invece $p \not\equiv 1 \mod 8$, si ha $k=2$, per cui $\Phi_8(x)$ spezza in due fattori quadratici in $\mathbb{F}_p[x]$. Il caso $k=4$ (i.e. $\Phi_8(x)$ irriducibile) non si verifica mai.

BIBLIOGRAFIA

[1] P. Aluffi, Algebra: chapter 0, GSM Amer Mathematical Society (2009).

[2] H. U. Besche, B. Eick and E. A. O'Brien, The groups of order at most 2000, Electron. Res. Announc. Amer. Math. Soc. 7 (2001), pp. 1–4.

[3] S. Eilenberg and S. MacLane, General Theory of Natural Equivalences, Transactions of the American Mathematical Society, Vol. 58, No. 2 (1945), pp. 291–394.

[4] T. W. Hungerford, Algebra. Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

[5] S. Mac Lane, Categories for the working mathematician. Second ed. Graduate Texts in Mathematics, 5. Springer-Verlag, New York (1998).

[6] E. Riehl, Category Theory in Context, Aurora: Dover Math Original (2016).

[7] I. Stewart, Galois Theory (first edition). Chapman and Hall, 1973.