TUTTO QUELLO CHE NON AVRESTE VOLUTO SAPERE DEL CORSO DI

INTRODUZIONE ALLA TEORIA DEI GRUPPI, DEGLI ANELLI E DEI CAMPI

MA CHE QUALCUNO VI HA VOLUTO INSEGNARE LO STESSO

CONTIENE

1. tutte le risposte alle domande che vi siete pentiti di aver fatto;
2. tutte le risposte alle domande che non avete proprio fatto;
3. una gran quantità di roba che non vi verrà mai chiesta all'esame;
4. niente di più di quello che potreste trovare in un qualsiasi libro appena decente sull'argomento "gruppi anelli e campi" (anche questo è vero).

Indice

Notazioni

La maggior parte delle notazioni seguono quelle classiche che ricordiamo qui solo per comodità .
$\mathbb{N}$ è l'insieme dei numeri naturali $\{0, 1, 2 \dots\}$ mentre $\mathbb{N}^+$ denota l'insieme dei numeri naturali positivi $\{1, 2, 3, \dots\}$.
$\mathbb{Z}$ è l'insieme degli interi, $\mathbb{Q}$ l'insieme dei numeri razionali, $\mathbb{R}$ l'insieme dei numeri reali e $\mathbb{C}$ l'insieme dei numeri complessi. Inoltre $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$ e $\mathbb{C}^* = \mathbb{C} - \{0\}$ (osservare che questa notazione non viene usata per $\mathbb{Z}$ in cui si avrà $\mathbb{Z}^* = \{1, -1\}$ per motivi che vedremo più avanti).
$\mathbb{Z}/n\mathbb{Z}$ è l'insieme delle classi resto modulo n, la classe resto di un intero a in $\mathbb{Z}/n\mathbb{Z}$ si indica con $[a]_n = \{b \in \mathbb{Z} \ t.c. \ b \equiv a \pmod{n}\}$, dunque, per esempio $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$. Spesso, se non si creano problemi di interpretazione, scriveremo solo a per indicare sia l'intero a che la sua classe resto modulo n, il contesto dovrebbe chiarire a quale dei due ci stiamo riferendo.
Dati due interi m ed n si indica con (m, n) il loro massimo comune divisore e con $[m, n]$ il loro minimo comune multiplo.
Dati due insiemi A e B il loro prodotto cartesiano si indica con $A \times B = \{(a, b) \ t.c. \ a \in A \ e \ b \in B\}$.
La cardinalità di un insieme E si indica con $\#E$.

Capitolo 1

Gruppi

1.1 Definizione ed esempi

Un gruppo è definito da un insieme G e da un'operazione $*$ su tale insieme. Se l'operazione verifica alcune proprietà la coppia $(G, *)$ ha una struttura di gruppo per definire la quale abbiamo quindi bisogno di partire dal concetto di operazione (cerchiamo di dare per scontato il concetto di insieme, non perché effettivamente lo sia, ma proprio per il motivo opposto: cercare di definirlo con precisione ci porterebbe troppo lontano dallo scopo di queste note).

Definizione 1.1.1 Una *legge di composizione* o *operazione* su un insieme E è una funzione $* : E \times E \longrightarrow E$. Una coppia insieme-operazione $(E, *)$ si dice *magma* (un bourbakismo in realtà poco usato).

Esempi:

1. La somma $+$ è un'operazione per $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Z}/n\mathbb{Z}$ per ogni $n > 0$.
2. Il prodotto $\cdot$ è un'operazione per gli stessi insiemi.
3. $a * b = \frac{a+b}{3}$ è un'operazione su $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ ma non lo è su $\mathbb{N}$ e $\mathbb{Z}$. Su $\mathbb{Z}/n\mathbb{Z}$ è un'operazione $\iff$ 3 è invertibile, cioè $(3, n) = 1$.
4. $a * b = a^b$ è un'operazione su $\mathbb{N}$ e $\mathbb{C}$ ma non lo è su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{Z}/n\mathbb{Z}$ in generale (perché ?).

Definizione 1.1.2 Un'operazione $* : E \times E \longrightarrow E$, data da $(a, b) \longrightarrow a * b$ si dice:

- *associativa* se $\forall\, a, b, c \in E$ si ha $(a * b) * c = a * (b * c)$;
- *commutativa* se $\forall\, a, b \in E$ si ha $a * b = b * a$.

Un elemento $e \in E$ si dice *elemento neutro* (di E rispetto a $*$) se $\forall\, a \in E$ si ha $a * e = e * a = a$.
Una terna insieme-operazione associativa-elemento neutro $(E, *, e)$ si dice *monoide*. Se, nella terna, l'operazione è anche commutativa si definisce *monoide commutativo*.

Esercizio Per ognuno degli esempi precedenti dire se l'insieme considerato è un monoide con l'operazione data. In particolare, verificare che le operazioni $a * b = \frac{a+b}{3}$ e $a * b = a^b$ non sono associative e non hanno elemento neutro. Tra quelli che sono monoidi dire quali sono commutativi.

Definizione 1.1.3 Sia $(E, *, e)$ un monoide. Un elemento $a \in E$ si dice *invertibile* se $\exists\, b \in A$ tale che $a * b = b * a = e$. In questo caso b si dice *inverso di* a e (quasi sempre) si indica con a^{-1}.

Osservazione 1.1.4 La notazione esponenziale può trarre in inganno, per questo bisogna sempre fare riferimento al monoide in cui si sta lavorando. Per esempio nel monoide $(\mathbb{R}, \cdot, 1)$ si ha $5^{-1} = \frac{1}{5}$ (e la notazione 5^{-1} non presenta ambiguità rispetto all'uso comune) mentre nel monoide $(\mathbb{R}, +, 0)$ si ha $5^{-1} = -5$.

Cercheremo di usare sempre la notazione esponenziale (salvo dove esplicitamente dichiarato). Dunque per a appartenente al monoide $(E, *, e)$ si ha

$$a^n = \begin{cases} e & \text{se } n = 0 \\ a * a * \cdots * a \ \ \text{(n volte)} & \text{se } n > 0 \end{cases} .$$

Gli esponenti negativi sono ben definiti solo per gli elementi invertibili di un monoide (per esempio, in $(\mathbb{Z}, \cdot, 1)$ non esiste 2^{-1}). Quindi se $a \in E$ è invertibile, per ogni $n < 0$ si definisce $a^n = a^{-1} * a^{-1} * \cdots * a^{-1}$ (n volte).
Ricordiamo di nuovo di fare attenzione alla notazione: in $(\mathbb{R}, +, 0)$ a^n rappresenta na per ogni $n \in \mathbb{Z}$.

Esempio Consideriamo tutte le funzioni da $\mathbb{R}$ in $\mathbb{R}$.
$E = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$;
$* = \circ$ la composizione di funzioni, cioè $(f * g)(x) = (f \circ g)(x) = f(g(x))$ per ogni $x \in \mathbb{R}$;
$e = id$ la funzione identica o identità , cioè $id(x) = x$ per ogni $x \in \mathbb{R}$.

Con queste definizioni $(E, *, e)$ è un monoide in cui gli elementi invertibili sono tutte e sole le funzione biunivoche (per esempio $f(x) = x^2$ non è invertibile mentre lo è $f(x) = x^3$).
Analogo discorso vale per $E = \{f : X \longrightarrow X\}$ con X insieme qualsiasi.

Definizione 1.1.5 Un monoide $(E, *, e)$ in cui ogni elemento è invertibile si dice *gruppo*. Se l'operazione è commutativa il gruppo si dice *commutativo* o *abeliano*.

Riassumendo: un insieme E con un'operazione $*$ è un gruppo se e solo se
1. $*$ *è associativa*, cioè $\forall\, a, b, c \in E$ si ha $(a * b) * c = a * (b * c)$;
2. *esiste un elemento neutro*, cioè $\exists\, e \in E$ tale che $\forall\, a \in E\ a * e = e * a = a$;
3. *ogni elemento è invertibile*, cioè $\forall\, a \in E\ \exists\, b \in E$ tale che $a * b = b * a = e$.

Esempi - Esercizi

1. Quali tra tutti i monoidi degli esempi precedenti sono gruppi ?

2. $(\mathbb{Z}/n\mathbb{Z}, \cdot, 1)$ non è un gruppo per nessun n. Il problema non è il solo 0 (come per esempio accade nei monoidi $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{R}, \cdot, 1)$ e $(\mathbb{C}, \cdot, 1)$), infatti $(\mathbb{Z}/n\mathbb{Z} - \{0\}, \cdot, 1)$ in generale continua a non essere un gruppo. Per quali n, $(\mathbb{Z}/n\mathbb{Z} - \{0\}, \cdot, 1)$ è un gruppo ?

3. Dimostrare che l'insieme degli elementi invertibili di un monoide è un gruppo. Per esempio l'insieme degli invertibili di $(\mathbb{Z}/n\mathbb{Z}, \cdot, 1)$ si indica con $(\mathbb{Z}/n\mathbb{Z})^*$ ed è un gruppo rispetto a $\cdot$ con elemento neutro 1.

Notazione In generale, se non si presta ad interpretazioni errate, trascureremo il segno dell'operazione scrivendo semplicemente ab invece di $a * b$. Inoltre (sempre a meno di ambiguità) scriveremo solo il gruppo G in luogo dell'intera terna $(G, *, e)$.

Proposizione 1.1.6 *Sia G un gruppo e sia $a \in G$, allora la funzione $f : G \longrightarrow G$ definita da $f(g) = ag$ $(\forall\, g \in G)$ è biunivoca. Lo stesso vale per la funzione $h : G \longrightarrow G$ definita da $h(g) = ga$ $(\forall\, g \in G)$.*

Dim. Se $f(x) = f(y)$ allora $ax = ay$ e quindi, moltiplicando a destra entrambi i membri per $a^{-1} \in G$, $a^{-1}ax = a^{-1}ay$ cioè $ex = x = ey = y$. Dunque f è iniettiva. Per la surgettività se $g \in G$ allora $a^{-1}g \in G$ e $g = f(a^{-1}g)$ appartiene all'immagine di f. Analoga dimostrazione per la funzione h. $\square$

Corollario 1.1.7 *In un gruppo G valgono le seguenti affermazioni:*

1. Leggi di Cancellazione*: $\forall\, a, x, y \in G$ si ha che $ax = ay \iff x = y$ (e $xa = ya \iff x = y$);*
2. *l'elemento neutro è unico;*
3. *l'inverso di un elemento è unico, in particolare, $\forall\, a, b \in G$ si ha $(a^{-1})^{-1} = a$ e $(ab)^{-1} = b^{-1}a^{-1}$.*

Dim. **1.** Equivale all'iniettività della Proposizione.
2. Se e ed e' sono elementi neutri di G allora (per definizione) $e = ee' = e'$.
3. Se $b, c \in G$ sono inversi di a allora (per definizione) $b = be = b(ac) = (ba)c = ec = c$. Le due formule seguono immediatamente. □

1.1.1 Esempi principali

Matrici

Sia $(G, *, e)$ un gruppo e sia $\mathscr{M}(n \times m, G)$ l'insieme delle matrici con n righe ed m colonne a coefficienti in G. Su tale insieme possiamo definire un'operazione (indotta da $*$ e che, per semplicità, chiamiamo ancora $*$)

$$* : \mathscr{M}(n \times m, G) \times \mathscr{M}(n \times m, G) \longrightarrow \mathscr{M}(n \times m, G)$$

$$(a_{ij}) * (b_{ij}) = (a_{ij} * b_{ij}) \ .$$

Si verifica facilmente che, con tale operazione e con elemento neutro la matrice E in cui ogni coefficiente è uguale ad e, $\mathscr{M}(n \times m, G)$ è un gruppo.
La definizione data è solo una banale generalizzazione dei classici gruppi $(\mathscr{M}(n \times m, \mathbb{R}), +, 0)$ già incontrati in algebra lineare.
Attenzione comunque all'ambiente in cui ci si muove: con la definizione appena data $(\mathscr{M}(n \times m, \mathbb{R} - \{0\}), \cdot, 1)$ (dove 1 è la matrice con tutti i coefficienti uguali a 1) è un gruppo in cui la moltiplicazione è fatta componente per componente e non righe per colonne come usuale per le matrici quadrate (notare che la moltiplicazione righe per colonne non è nemmeno ben definita come operazione su $\mathscr{M}(n \times m, \mathbb{R} - \{0\})$ nel caso in cui $n \neq m$).

Il gruppo lineare

Sia $GL_n(\mathbb{R}) = \{A \in \mathscr{M}(n \times n, \mathbb{R}) \ : \ \det(A) \neq 0\}$ il *gruppo lineare* (di dimensione n) su $\mathbb{R}$. Si verifica facilmente (usando il Teorema di Binet)

che $(GL_n, \cdot, I)$ (con I matrice identità e $\cdot$ la usuale moltiplicazione righe per colonne) è un gruppo.
Analoghe verifiche si possono fare sostituendo ad $\mathbb{R}$ altri insiemi di coefficienti, per esempio $\mathbb{Q}$, $\mathbb{C}$ e $\mathbb{Z}/p\mathbb{Z}$ per ogni p primo (non però $\mathbb{Z}$ o $\mathbb{Z}/n\mathbb{Z}$ per n non primo, perché ?).
Osserviamo che, per $n \geq 2$, $GL_n(\mathbb{R})$ è un gruppo non abeliano. Per esempio, per $n = 2$, si ha

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

mentre

$$\begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 7 \\ 0 & -3 \end{pmatrix} .$$

Gruppi di permutazioni (1)

Dato un insieme E siano:
$S(E) = \{f : E \longrightarrow E,\ f \text{ biunivoca}\}$;
$\circ$ la composizione di funzioni;
id la funzione identica di E.
Allora la terna $(S(E), \circ, id)$ si definisce *gruppo delle permutazioni* di E (verificare la definizione di gruppo, vd anche l'esempio precedente sulle funzioni da $\mathbb{R}$ in $\mathbb{R}$).
Se E è un insieme finito con n elementi, $E = \{a_1, \ldots, a_n\}$ per semplificare le notazioni si considera semplicemente l'insieme degli indici $\{1, \ldots, n\}$ (con cui E è in corrispondenza biunivoca) e si scrive $S(E) = S(n) = S_n$.

Osservazione 1.1.8 S_n ha $n!$ elementi.

Dim. Ogni permutazione $f : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ è determinata dalle immagini $f(1), \ldots, f(n)$.
$f(1)$ è un qualsiasi elemento di $\{1, \ldots, n\}$: n possibilità
$f(2)$ è un qualsiasi elemento di $\{1, \ldots, n\} - \{f(1)\}$: $n-1$ possibilità
$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$
$f(n-1)$ è un qualsiasi elemento di $\{1, \ldots, n\} - \{f(1), \ldots, f(n-2)\}$: 2 possibilità
$f(n)$ è uguale all'unico elemento di $\{1, \ldots, n\} - \{f(1), \ldots, f(n-1)\}$: 1 possibilità .
Dunque gli elementi di S_n sono $n(n-1)(n-2)\ldots 2 \cdot 1 = n!$. $\square$

Rappresentazione degli elementi di S_n . Per rappresentare una permutazione è essenziale mettere in relazione un elemento con la sua immagine. Per esempio ciò si può fare con una rappresentazione matriciale (2 righe, n colonne) del tipo

$$\begin{pmatrix} 1 & \dots & n \\ f(1) & \dots & f(n) \end{pmatrix}$$

in cui elemento ed immagine occupano la stessa colonna ("lettura verticale"). In generale useremo una notazione che, anche se può sembrare meno naturale e diretta, è tuttavia da preferirsi per la compattezza e la semplicità nei calcoli. La *rappresentazione ciclica* di una permutazione si ottiene partendo da un elemento (generalmente 1) e scrivendo, alla sua destra, la sua immagine (dunque $(1\, f(1)..)$). Si prosegue ancora scrivendo a destra l'immagine di $f(1)$ e si ripete il procedimento fino a quando si trova un elemento la cui immagine è 1 e che chiude il ciclo (perché siamo sicuri che un tale elemento esiste ?). Se tutti gli elementi sono presenti nel ciclo, abbiamo finito, altrimenti si apre un nuovo ciclo con il primo elemento non presente in quello appena concluso.

Esempi Per $n = 5$ vediamo per due permutazioni le due rappresentazioni descritte sopra.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \longleftrightarrow (1\,3\,2\,4\,5)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \longleftrightarrow (1\,3)(2\,5\,4)$$

Una scrittura del tipo $(i_1 \dots i_k)$ si dice *ciclo di lunghezza* k e rappresenta la permutazione $f(i_1) = i_2$, $f(i_2) = i_3 \dots f(i_{k-1}) = i_k$, $f(i_k) = i_1$. Nello scrivere le rappresentazioni cicliche di solito si omettono i cicli di lunghezza 1 (i "punti fissi"). La rappresentazione ciclica si adatta al calcolo della composizione di permutazioni, che si può vedere come un "prodotto" di cicli. Siano $f, g \in S_n$ per trovare la rappresentazione ciclica di $f \circ g$ si percorrono (sempre da destra verso sinistra, perché la prima applicazione da considerare è la g) le rappresentazioni cicliche di f e g (scritte in questo ordine), seguendo il "percorso" di ogni elemento. Se l'immagine di 1 nel primo ciclo è i_1 si prosegue cercando l'immagine di i_1 nel secondo ciclo e così via.

Esempio Consideriamo due cicli in S_6 .

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix} \longleftrightarrow (1\,3)(2\,4\,6)$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix} \longleftrightarrow (1\,2\,5)(3\,4)$$

Osserviamo che $f(g(1)) = 4$, $f(g(2)) = 5 \ldots f(g(6)) = 2$. Con il prodotto di cicli:

$$f \circ g = (1\,3)(2\,4\,6)(1\,2\,5)(3\,4) = (1\,4)(2\,5\,3\,6) \ .$$

Osserviamo anche che invertendo l'ordine del prodotto si ottiene:

$$g \circ f = (1\,2\,5)(3\,4)(1\,3)(2\,4\,6) = (1\,4\,6\,5)(2\,3) \neq f \circ g \ .$$

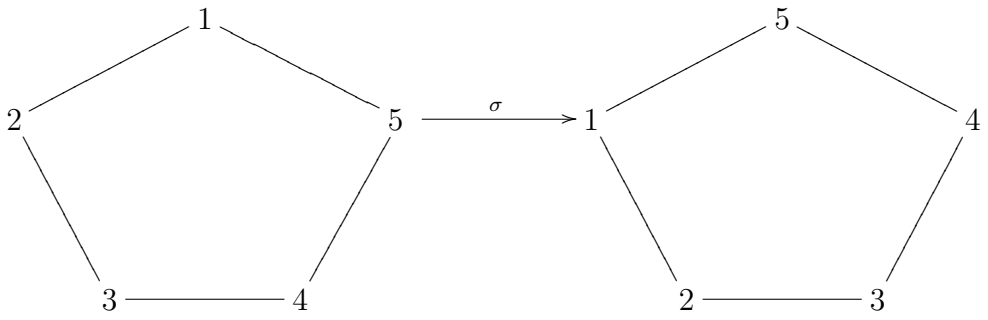
Osservazione 1.1.9 Per ogni $n \geq 3$ il gruppo S_n non è abeliano.
(Dimostrarlo)

Proposizione 1.1.10 *Ogni permutazione è prodotto di cicli disgiunti.*

Dim. Basta applicare l'algoritmo descritto precentemente per trovare i cicli. Il fatto che siano disgiunti (cioè che ogni elemento compaia in uno ed un solo ciclo) è una semplice conseguenza della biunivocità della funzione. □

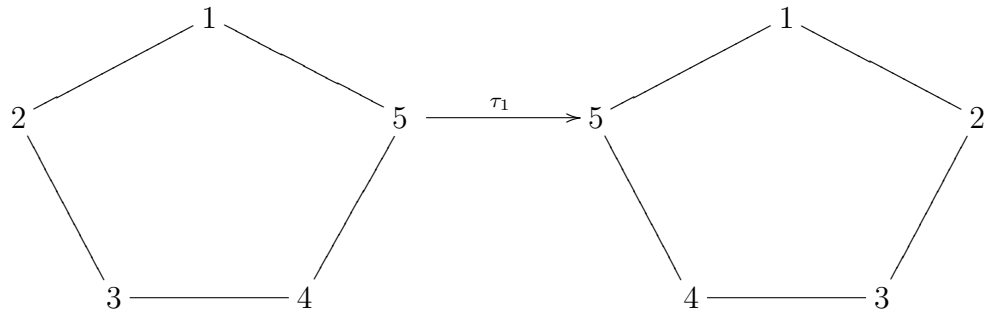
Gruppi diedrali

Consideriamo le isometrie di un poligono regolare ad $n \geq 3$ vertici. Le isometrie sono movimenti rigidi del piano che mandano un poligono dato in sé stesso. Prendiamo per esempio il pentagono e sia σ una rotazione antioraria di $\frac{2\pi}{5}$ radianti con centro nel centro del pentagono:



Ci sono 5 rotazione di questo tipo, esattamente σ, σ^2, σ^3, σ^4 e $\sigma^5 = id$ che sono, rispettivamente, di $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$ e 2π radianti. Osserviamo che tutte le rotazioni mantengono l'ordinamento antiorario della numerazione dei vertici. Sia adesso τ_1 la simmetria rispetto all'asse che va dal vertice 1 al punto medio

del lato opposto:



Ci sono 5 simmetrie di questo tipo τ_1 , τ_2 , τ_3 , τ_4 e τ_5 (una per ogni vertice) e osserviamo che tutte cambiano l'ordinamento della numerazione dei vertici.

Esercizio Verificare che l'insieme $D_5 = \{id, \sigma, \sigma^2, \sigma^3, \sigma^4, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5\}$ con l'operazione di composizione ed elemento neutro id è un gruppo di 10 elementi.
Per il calcolo delle composizioni e degli inversi può essere utile considerare un'isometria come una permutazione dei vertici (dunque un elemento di S_5). Per esempio

$$\sigma = (1\,2\,3\,4\,5) \quad \text{e} \quad \tau_1 = (2\,5)(3\,4)$$

dunque

$$\sigma\tau_1 = (1\,2\,3\,4\,5)(2\,5)(3\,4) = (1\,2)(3\,5) = \tau_4 \ ,$$

$$\tau_1\sigma = (2\,5)(3\,4)(1\,2\,3\,4\,5) = (1\,5)(2\,4) = \tau_3 \ \ , \ \text{ecc}\dots \ .$$

Inoltre $\sigma\sigma^4 = \sigma^5 = id$ implica $\sigma^{-1} = \sigma^4$ e ogni simmetria è inversa di sé stessa (cioè $\tau_i^2 = id$ per ogni $1 \leq i \leq 5$).

In generale per un poligono regolare ad n lati ci sono n rotazioni con centro nel centro del poligono: $\sigma, \sigma^2, \dots, \sigma^n = id$, dove σ è una rotazione di $\frac{2\pi}{n}$ radianti, ed n simmetrie. Indicheremo sempre con σ la rotazione "iniziale" e con τ una simmetria.

Osservazione 1.1.11 Se n è dispari gli n assi di simmetria vanno da un vertice al punto medio del lato opposto (come visto per il pentagono). Se n è pari gli assi di simmetria sono gli assi passanti per due vertici opposti rispetto al centro (le "diagonali" che sono $\frac{n}{2}$) e quelli passanti per i punti medi di due lati opposti (gli altri $\frac{n}{2}$).

Definizione 1.1.12 L'insieme $D_n = \{\text{simmetrie, rotazioni}\}$ con l'operazione di composizione ed elemento neutro id è un gruppo di $2n$ elementi e si dice *gruppo diedrale* (n-esimo).

Polinomi ? (per confondere le idee)

Definizione 1.1.13 Dato un monoide $(A, \cdot, e)$ denoteremo con $A[X]$ l'*insieme dei polinomi a coefficienti in A*. Dunque

$$A[X] = \{ \sum_{i \geq 0} a_i X^i \, : \, a_i \in A \text{ ed } a_i = e \text{ per quasi ogni } i \, \}$$

(dove "per quasi ogni" significa "per tutti, tranne un numero finito").

Possiamo definire su $A[X]$ un'operazione naturalmente indotta da quella su A (ma che può riservare comunque qualche sorpresa).
Definiamo $\cdot : A[X] \times A[X] \longrightarrow A[X]$ tramite la formula

$$\sum_{i \geq 0} a_i X^i \cdot \sum_{i \geq 0} b_i X^i = \sum_{i \geq 0} a_i b_i X^i$$

(dove, nell'ultimo termine, il prodotto $a_i b_i$ deriva dall'operazione in A).
Se G è un gruppo, è facile vedere che, con tale operazione, $G[X]$ è un gruppo:
- l'associatività segue dall'associatività dell'operazione in G;
- l'elemento neutro è $\sum_{i \geq 0} e X^i$;
- l'inverso di $\sum_{i \geq 0} a_i X^i$ è $\sum_{i \geq 0} a_i^{-1} X^i$.

Vediamo qualche esempio.

1. Con $G = \mathbb{Z}$, $(\mathbb{Z}[X], +, 0)$ è un gruppo (ovvio).

2. Con $G = \mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z}[X], +, 0)$ è un gruppo (analogo al precedente).

3. Con $A = (\mathbb{Z}, \cdot, 1)$, $(\mathbb{Z}[X], \cdot, 1)$ è un monoide il cui gruppo degli invertibili è dato da

$$\mathbb{Z}^*[X] = \{ \sum_{i \geq 0} a_i X^i \, : \, a_i = \pm 1, \ \forall \, i \, \}$$

dove con $\mathbb{Z}^*$ si indica l'insieme degli invertibili di $\mathbb{Z}$ rispetto al prodotto, cioè $\mathbb{Z}^* = \{\pm 1\}$.

4. Con $A = (\mathbb{R}, \cdot, 1)$, $(\mathbb{R}[X], \cdot, 1)$ è un monoide con gruppo degli invertibili

$$\mathbb{R}^*[X] = \{ \sum_{i \geq 0} a_i X^i \, : \, a_i \in \mathbb{R}^* = \mathbb{R} - \{0\}, \ \forall \, i \, \} \ .$$

5. Con $G = \mathbb{R}^*$ si ottiene il gruppo $\mathbb{R}^*[X]$ con elemento neutro $\sum_{i \geq 0} X^i$ ed un prodotto molto diverso da quello usuale tra polinomi. Per esempio con il prodotto usuale tra polinomi si ha $(1 + 2X)(2 - 3X) = 2 + X - 6X^2$ mentre la definizione appena data produce $(1 + 2X)(2 - 3X) = 2 - 6X$. $\mathbb{R}^*[X]$ è un gruppo solo rispetto a quest'ultima operazione, con il prodotto usuale non è un gruppo (perché ?).

Prodotto diretto

Dati due gruppi $(G_1, *, e_1)$ e $(G_2, \circ, e_2)$, vogliamo definire una struttura di gruppo sul loro prodotto cartesiano $G_1 \times G_2 = \{(a, b) : a \in G_1 \text{ e } b \in G_2\}$. Sia quindi $\cdot : (G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow G_1 \times G_2$ definita da

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2 \, , b_1 \circ b_2) \ .$$

Verificare che $(G_1 \times G_2, \cdot, (e_1, e_2))$ è un gruppo.
La costruzione si può generalizzare in maniera ovvia ad un qualsiasi numero di gruppi (è sufficiente definire il prodotto componente per componente).

1. In $\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/m\mathbb{Z})^*$ si ha $([a]_n, [b]_m)([c]_n, [d]_m) = ([a + c]_n, [bd]_m)$. Per esempio in $\mathbb{Z}/7\mathbb{Z} \times (\mathbb{Z}/11\mathbb{Z})^*$ si ha $([1]_7, [3]_{11})^4 = ([4]_7, [81]_{11}) = ([4]_7, [4]_{11})$.

2. Sia G un gruppo. Che differenze e/o analogie si possono trovare tra $\mathscr{M}(n \times m, G)$ (con l'operazione descritta nel primo esempio di questa sezione) e il prodotto di nm copie di G ?

1.2 Sottogruppi

Per ogni sottoinsieme H di un gruppo G si può considerare su H l'operazione indotta da G. Bisogna però ricordare che:
1. l'operazione può non essere ben definita su H;
2. anche se l'operazione è ben definita su H, il sottoinsieme H può non essere un gruppo rispetto a tale operazione.

Esempi
1. Sia $G = (\mathbb{Z}, +, 0)$ e siano

$$H_0 = \{a \in G \ t.c. \ a \equiv 0 \pmod 2\} \ , \ H_1 = \{a \in G \ t.c. \ a \equiv 1 \pmod 2\} \ .$$

Si verifica facilmente che $+$ è un'operazione su H_0 ma non su H_1, inoltre $(H_0, +, 0)$ è un gruppo.
2. Sia $G = (\mathbb{R}, +, 0)$ e sia $H = \mathbb{R}_{\geq 0} = \{a \in \mathbb{R} \ t.c. \ a \geq 0\}$. In questo caso $+$ è un'operazione su H ma $(H, +, 0)$ non è un gruppo.

Definizione 1.2.1 Un sottoinsieme non vuoto H di un gruppo G si dice *sottogruppo* di G se è un gruppo rispetto all'operazione indotta da G. In particolare $H \subset G$ è un sottogruppo se e solo se:

1. $H \neq \emptyset$ (spesso è utile e facile controllare se $e \in H$ o no);

2. $\forall\, a, b \in H$ si ha che $ab \in H$ (buona definizione dell'operazione);

3. $\forall\, a \in H$ si ha che $a^{-1} \in H$ (esistenza degli inversi).

Notazione: $H < G$ significa H sottogruppo di G.

Esempi - Esercizi

1. I sottogruppi *banali* di G che sono $\{e\}$ e G stesso.

2. Per ogni $n \in \mathbb{Z}$ l'insieme $n\mathbb{Z} = \{a \in \mathbb{Z} \ t.c.\ a \equiv 0 \pmod{n}\}$ è un sottogruppo di $(\mathbb{Z}, +, 0)$.
Per quali n si ottengono i sottogruppi banali ?

3. $H = \{0, 1, -1\}$ non è un sottogruppo di $(\mathbb{Z}, +, 0)$ (perché ?).

4. In $GL_2(\mathbb{R})$ il sottoinsieme

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\}$$

è un sottogruppo (verificarlo).

5. Sia $G = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ (p primo). Definiamo

$$SL_n(G) = \{M \in GL_n(G) \ t.c.\ \det M = 1\}\ .$$

Verificare che $SL_n(G) < GL_n(G)$.

6. Scrivendo le isometrie come particolari permutazioni è immediato osservare che $D_n < S_n$ per ogni n.

7. In D_n le rotazioni $\{id, \sigma, \ldots, \sigma^{n-1}\}$ formano un sottogruppo, mentre né l'insieme delle simmetrie $\{\tau_1, \ldots, \tau_n\}$ né l'insieme delle simmetrie con l'identità $\{id, \tau_1, \ldots, \tau_n\}$ sono sottogruppi (verificarlo).

Lemma 1.2.2 *I sottogruppi di $\mathbb{Z}$ sono tutti e soli gli insiemi della forma*

$$n\mathbb{Z} = \{\, a \in \mathbb{Z} \ t.c.\ a \equiv 0 \pmod{n}\,\} \quad n \in \mathbb{Z}\ .$$

Dim. Abbiamo visto tra gli esempi che gli insiemi $n\mathbb{Z}$ sono sottogruppi di $\mathbb{Z}$. Vediamo il viceversa: sia $H < \mathbb{Z}$, se $H = \{0\}$ allora $H = 0\mathbb{Z}$ e abbiamo finito. Se $H \neq \{0\}$ allora $\exists\, a \in H - \{0\}$, dunque $-a \in H$ ed H contiene almeno un elemento > 0. Per il principio del Buon Ordinamento (vd sezione 3.1)

possiamo definire $n = \min\{a \in H \,:\, a > 0\}$. Per definizione di sottogruppo si ha $n\mathbb{Z} \subset H$ e vogliamo dimostrare che sono uguali.
Sia $h \in H$ allora, per il Teorema di divisione, otteniamo $h = nq + r$ con $q, r \in \mathbb{Z}$ e $0 \leq r < n$. Dato che $h, nq \in H$ allora $r = h - nq \in H$ e la minimalità di n implica $r = 0$. Dunque $h = nq$ ed $H \subset n\mathbb{Z}$. $\square$

Proposizione 1.2.3 *L'intersezione (anche infinita) di sottogruppi è un sottogruppo.*

Dim. Esercizio. $\square$

In generale l'unione di sottogruppi non è un sottogruppo.

Esempi - Esercizi

1. $2\mathbb{Z} \bigcup 3\mathbb{Z}$ non è un sottogruppo di $\mathbb{Z}$.
2. Verificare che $2\mathbb{Z} \bigcap 3\mathbb{Z} = 6\mathbb{Z}$.
   In generale che sottogruppo è $m\mathbb{Z} \bigcap n\mathbb{Z}$?
3. Siano H e K due sottogruppi di un gruppo G. Dimostrare che $H \bigcup K$ è un sottogruppo di G se e solo se $H \subset K$ o $H \supset K$.
   Sugg.: ($\Longleftarrow$) è banale. Per dimostrare ($\Longrightarrow$) supporre, per assurdo, che $H \not\subset K$ e $H \not\supset K$. Prendere allora due elementi $h \in H - K$ e $k \in K - H$ e considerare il prodotto hk ... .

Definizione 1.2.4 Sia S un sottoinsieme non vuoto di un gruppo G. Il *sottogruppo generato da* S è il più piccolo (rispetto all'inclusione) sottogruppo di G contenente S e si indica con $< S >$.

Dato un sottoinsieme S il sottogruppo generato da S si può definire come l'intersezione di tutti i sottogruppi di G che contengono S. Più precisamente sia $\mathscr{F}_S = \{H < G \; t.c. \; S \subset H\}$ allora $\mathscr{F}_S \neq \emptyset$ perché $G \in \mathscr{F}_S$ e si ha

$$< S >= \bigcap_{H \in \mathscr{F}_S} H \; .$$

Una descrizione alternativa (e più "operativa") di $< S >$ si ottiene osservando che, per definizione di sottogruppo, $< S >$ deve contenere (almeno) tutti i prodotti finiti tra gli elementi di S ed i loro inversi. Non è difficile verificare che un insieme che contenga esattamente tutti i possibili prodotti finiti tra gli elementi di S ed i loro inversi è in effetti un sottogruppo di G ed è sicuramente il più piccolo che contenga S.

Definizione 1.2.5 Un gruppo che sia generato da un solo elemento si dice *ciclico*.

Esempi - Esercizi

1. In $\mathbb{Z}$ il sottogruppo $n\mathbb{Z}$ è generato da n, cioè $n\mathbb{Z} =< n >$. Tutti i sottogruppi di $\mathbb{Z}$ sono ciclici.

2. Le rotazioni di D_n sono il sottogruppo generato da σ. Verificare (per n piccolo) che $< \sigma, \tau >= D_n$ e che D_n non è mai ciclico.

3. Sia G un gruppo e sia $a \in G$. Allora $< a >= \{a^n : n \in \mathbb{Z}\}$.

4. $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ è ciclico per ogni n, generato dalla classe di equivalenza di 1. In generale un gruppo ciclico può avere più di un generatore. Per esempio $\mathbb{Z}/8\mathbb{Z}$ è uguale a $< 1 >$, $< 3 >$, $< 5 >$ e $< 7 >$ dunque ha 4 generatori distinti. I sottogruppi non banali di $\mathbb{Z}/8\mathbb{Z}$ sono $< 2 >= \{0, 2, 4, 6\} =< 6 >$ e $< 4 >= \{0, 4\}$.

5. Dimostrare che $\mathbb{Z}/n\mathbb{Z} =< m > \iff (m, n) = 1$. Dunque in generale $\mathbb{Z}/n\mathbb{Z}$ ha $\phi(n)$ generatori distinti (dove ϕ è la funzione di Eulero).

6. Gruppi infiniti possono contenere sottogruppi finiti (ciclici e non). Per esempio in $(\mathbb{R}^*, \cdot, 1)$ (dove $\mathbb{R}^* = \mathbb{R} - \{0\}$) abbiamo il sottogruppo $\{1, -1\} =< -1 >$.

7. $(\mathbb{Q}^*, \cdot, 1)$ (dove $\mathbb{Q}^* = \mathbb{Q} - \{0\}$) non ha un insieme finito di generatori, infatti abbiamo bisogno di tutti i numeri primi per generare i suoi elementi.

Definizione 1.2.6 Sia G un gruppo con elemento neutro e e sia $a \in G$.

1. L'*ordine* di G è il numero (finito o infinito) degli elementi di G e si indica con $o(G)$.

2. L'*ordine di* a è il più piccolo intero positivo n tale che $a^n = e$, se tale intero non esiste si dice che a ha ordine infinito. L'ordine di a (finito o infinito) si indica con $o(a)$.

Esempi - Esercizi

1. In ogni gruppo $o(e) = 1$.

2. In $\mathbb{Z}$ ogni elemento diverso da 0 ha ordine infinito.

3. In $\mathbb{Z}/8\mathbb{Z}$ abbiamo $o(1) = o(3) = o(5) = o(7) = 8$, $o(2) = o(6) = 4$ e $o(4) = 2$.

4. In $\mathbb{R}^*$ solo 1 e -1 hanno ordine finito.

5. In $\mathbb{C}^*$ hanno ordine finito tutte e sole le radici dell'unità, cioè tutte e sole le radici dei polinomi $X^n - 1$ per $n \geq 1$.

6. Verificare che in S_n un ciclo di lunghezza k ha ordine k.

7. Dimostrare che l'ordine di una permutazione è il minimo comune multiplo degli ordini dei cicli disgiunti di cui è il prodotto.

8. Si verifica facilmente che $o(a) = o(< a >)$ (l'ordine di un elemento è uguale all'ordine del sottogruppo da lui generato).

9. Sia $a \in G$ un elemento di ordine finito d. Allora $a^n = e \iff d|n$. Infatti se dividiamo n per d si ottiene $n = dq + r$ con $0 \leq r < d$, dunque $e = a^n = a^{dq+r} = (a^d)^q a^r = ea^r = a^r$. Quindi $a^r = e$ e, per la minimalità dell'ordine, deve essere $r = 0$ cioè $d|n$. Il viceversa è banale.

Gruppi di permutazione (2)

Abbiamo visto in precedenza che ogni permutazione è prodotto di cicli disgiunti (Proposizione 1.1.10), adesso ci concentriamo sui cicli di lunghezza 2 che si definiscono *trasposizioni*.

Teorema 1.2.7 *Per ogni n le trasposizioni generano S_n .*

Dim. È sufficiente dimostrare che ogni ciclo è un prodotto di trasposizioni. Questo si vede facilmente perché $(i_1 \ldots i_k) = (i_1\, i_2)(i_2\, i_3)\cdots(i_{k-1}\, i_k)$. □

In S_n ci sono $\binom{n}{2} = \frac{n(n-1)}{2}$ trasposizioni ma è possibile trovare insiemi di generatori più piccoli. Per esempio dimostriamo che S_5 può essere generato da $\tau = (1\,2)$ e $\sigma = (1\,2\,3\,4\,5)$.
Osserviamo che $\tau = \tau^{-1}$, $\sigma^2 = (1\,3\,5\,2\,4) = \sigma^{-3}$, $\sigma^3 = (1\,4\,2\,5\,3) = \sigma^{-2}$ e $\sigma^4 = (1\,5\,4\,3\,2) = \sigma^{-1}$ (perché $o(\sigma) = 5$), quindi tutti questi sono elementi di $< \tau, \sigma >$. Altri elementi sono:

$$\sigma\tau\sigma^{-1} = (2\,3)\ ,\ \sigma^2\tau\sigma^{-2} = (3\,4)\ ,\ \sigma^3\tau\sigma^{-3} = (4\,5)\ ,\ \sigma^4\tau\sigma^{-4} = (1\,5)\ .$$

Continuando con le combinazioni tra elementi di $< \tau, \sigma >$ si ottengono:

$$(2\,3)(1\,2)(2\,3) = (1\,3)\ ,\ (1\,5)(1\,2)(1\,5) = (2\,5)\ ,\ (1\,5)(4\,5)(1\,5) = (1\,4)\ ,$$
$$(3\,4)(2\,3)(3\,4) = (2\,4)\ ,\ (2\,3)(2\,5)(2\,3) = (3\,5)\ .$$

Abbiamo così ottenuto tutte le 10 trasposizioni di S_5 e, per il Teorema 1.2.7, queste generano tutto S_5. Dunque $< \tau, \sigma >= S_5$.

Esercizio Dimostrare che $\tau = (1\,2)$ e $\sigma = (1\,2\,\ldots\,n)$ generano S_n (farlo esplicitamente almeno per n piccolo e poi provare a generalizzare).

In generale un ciclo può avere diverse scritture come prodotto di trasposizioni, per esempio $(1\,2\,3) = (1\,2)(2\,3) = (1\,3)(1\,2)$. Comunque se una permutazione σ si può scrivere come prodotto di un numero pari (risp. dispari) di trasposizioni allora ogni altra scrittura di σ come prodotto di trasposizioni ne conterrà un numero pari (risp. dispari). Per dimostrarlo consideriamo il polinomio in n variabili

$$P(X_1, \ldots, X_n) = \prod_{1 \le i < j \le n} (X_i - X_j)$$

e, per ogni $\sigma \in S_n$ definiamo

$$\sigma P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \prod_{1 \le i < j \le n} (X_{\sigma(i)} - X_{\sigma(j)})\ .$$

Esaminando ogni fattore è facile vedere che se τ è una trasposizione allora $\tau P = -P$ (se $\tau = (i\,j)$ cambia segno $X_i - X_j$ mentre gli altri fattori si compensano). Dunque se $\sigma \in S_n$ allora

$$\sigma P = \begin{cases} P & \text{se } \sigma = \text{ prodotto di un numero pari di trasposizioni} \\ -P & \text{se } \sigma = \text{ prodotto di un numero dispari di trasposizioni} \end{cases}\ .$$

Comunque si scriva σ come prodotto di trasposizioni il suo effetto su P non può cambiare $\Longrightarrow$ la "parità" del numero di trasposizioni è invariante.

Possiamo quindi dare la seguente

Definizione 1.2.8 Una permutazione $\sigma \in S_n$ si dice *pari* (risp. *dispari*) se è prodotto di un numero pari (risp. dispari) di trasposizioni.

Osservazione 1.2.9 Se σ è un ciclo $(i_1\,i_2\,\ldots\,i_k)$ di lunghezza k allora $\sigma = (i_1\,i_2)(i_2\,i_3)\cdots(i_{k-1}\,i_k)$ è prodotto di $k-1$ trasposizioni. Dunque un ciclo è pari se e solo se la sua lunghezza è dispari (e viceversa).

Proposizione 1.2.10 *Le permutazioni pari in S_n formano un sottogruppo.*

Dim. Ovvio. □

Definizione 1.2.11 Il gruppo delle permutazioni pari di S_n si definisce *gruppo alterno* (n-esimo) e si indica con $\mathscr{A}_n$.

Qualche sottogruppo - Esercizi

1. Sia G un gruppo. Il *centro* di G è l'insieme $Z(G) = \{a \in G \ t.c. \ ag = ga \ \forall\, g \in G\}$. Dimostrare che $Z(G) < G$. Notare che se G è abeliano allora $Z(G) = G$.
Per un caso non banale si può verificare che in D_4 e D_6 le rotazioni di π radianti sono nel centro del gruppo. Per i calcoli è utile usare la rappresentazione in permutazioni in cui $\sigma = (1\,2\,3\,4) \in D_4$ e $\theta = (1\,2\,3\,4\,5\,6) \in D_6$ sono le rotazioni di $\frac{2\pi}{4}$ e $\frac{2\pi}{6}$ radianti rispettivamente. Allora le rotazioni di π radianti sono $\sigma^2 = (1\,3)(2\,4)$ e $\theta^3 = (1\,4)(2\,5)(3\,6)$.
In generale si può dimostrare che con n pari e $\sigma = (1\,2\,\ldots\,n) \in D_n$ la rotazione di $\frac{2\pi}{n}$ radianti, si ha $\sigma^{n/2} \in Z(D_n)$.

2. Sia G un gruppo ed $a \in G$. Il *centralizzante* (o *centralizzatore*) di a in G è l'insieme $C(a) = \{g \in G \ t.c. \ ag = ga\}$. Dimostrare che $C(a) < G$.

3. Sia G un gruppo ed $H < G$. Il *normalizzante* (o *normalizzatore*) di H in G è l'insieme $N(H) = \{g \in G \ t.c. \ gHg^{-1} = H\}$. Dimostrare che $N(H) < G$ e $H \subset N(H)$.

4. Sia G un gruppo, $H < G$ ed $a \in G$. Dimostrare che $aHa^{-1} < H$.
Dim. È ovvio che $e \in aHa^{-1}$, inoltre se $ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1}$ allora $ah_1a^{-1}ah_2a^{-1} = ah_1h_2a^{-1} \in aHa^{-1}$. Infine se $aha^{-1} \in aHa^{-1}$ allora il suo inverso $(aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$.

5. Sia G un gruppo finito ed H un sottoinsieme di G tale che:

i) $e \in H$;

ii) $a, b \in H \Longrightarrow ab \in H$.

Dimostrare che $H < G$.
Dim. Rimane solo da dimostrare l'esistenza degli inversi. Se $a \in H$ allora $a^n \in H$ per ogni $n \in \mathbb{Z}$. Dato che G è finito anche $o(H)$ è finito quindi devono esistere $n < m$ tali che $a^n = a^m \Longrightarrow a^{m-n} = e$. Dunque $a^{-1} = a^{m-n-1} \in H$.

6. Siano G_1 e G_2 due gruppi e siano $H_1 < G_1$, $H_2 < G_2$. Dimostrare che $H_1 \times H_2 < G_1 \times G_2$.

7. Trovare l'ordine di ogni elemento di $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^*$. Per esempio con $([1]_3, [2]_3)$ si ha:
$([1]_3, [2]_3)^2 = ([2]_3, [4]_3) = ([2]_3, [1]_3)$,
$([1]_3, [2]_3)^3 = ([3]_3, [8]_3) = ([0]_3, [2]_3)$,
$([1]_3, [2]_3)^4 = ([4]_3, [16]_3) = ([1]_3, [1]_3)$,
$([1]_3, [2]_3)^5 = ([5]_3, [32]_3) = ([2]_3, [2]_3)$,
$([1]_3, [2]_3)^6 = ([6]_3, [64]_3) = ([0]_3, [1]_3)$,
dunque $o(([1]_3, [2]_3)) = 6 = o(\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^*)$ e il gruppo è ciclico.

8. Trovare l'ordine di ogni elemento di $(\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$. Per esempio con $([2]_5, [2]_3)$ si ha:
$([2]_5, [2]_3)^2 = ([4]_5, [4]_3) = ([4]_5, [1]_3)$,
$([2]_5, [2]_3)^3 = ([8]_5, [8]_3) = ([3]_5, [2]_3)$,
$([2]_5, [2]_3)^4 = ([16]_5, [16]_3) = ([1]_5, [1]_3)$,
dunque $o(([2]_5, [2]_3)) = 4$.

1.2.1 Classi laterali - Teorema di Lagrange

Definizione 1.2.12 Sia G un gruppo ed $H < G$. Un *laterale destro* (risp. *sinistro*) *di* H in G è un sottoinsieme del tipo

$$Ha = \{ha \,:\, h \in H\} \quad (\text{risp. } aH = \{ah \,:\, h \in H\}\,)$$

per qualche $a \in G$.

Esempi -Esercizi

1. $H = eH = He$ è laterale destro e sinistro di sé stesso.
2. Siano $n\mathbb{Z} < \mathbb{Z}$ ed $m \in \mathbb{Z} - n\mathbb{Z}$ allora l'insieme

   $$m + n\mathbb{Z} = n\mathbb{Z} + m = \{m + nl \,:\, l \in \mathbb{Z}\} = \{a \in \mathbb{Z} \,:\, a \equiv m \pmod{n}\}$$

   è un laterale destro e sinistro di $n\mathbb{Z}$.
3. Scrivere la classi laterali destre e sinistre di $< \sigma >$ e $< \tau >$ in D_n (per n piccolo).

In generale le classi laterali di un sottogruppo non sono sottogruppi, inoltre nei gruppi abeliani le classi laterali destre e sinistre coincidono ma ciò non è vero in generale (vedere, per esempio, le classi laterali di $< \tau >$ in D_3).

Definizione 1.2.13 Sia G un gruppo e sia $H < G$. Per $a, b \in G$ definiamo $a \sim b \iff \exists\, h \in H$ tale che $b = ha$ (risp. $b = ah$). Tale relazione si dice *congruenza destra* (risp. *sinistra*) *modulo* H.

In generale parleremo solo di congruenza modulo un sottogruppo, intendendo la congruenza destra. Tutti i risultati che seguiranno possono essere dimostrati per la congruenza sinistra con banali modifiche.

Proposizione 1.2.14 *Sia $\sim$ la congruenza modulo il sottogruppo H di un gruppo G. Allora*

1. *$\sim$ è una relazione di equivalenza;*
2. *per ogni $a \in G$ la classe di equivalenza di a è $[a] = Ha$.*

Dim. **1.** Proprietà riflessiva: $e \in H$ ed $a = ea$ dunque $a \sim a$.
Proprietà simmetrica: se $a \sim b$ allora $\exists\, h \in H$ tale che $b = ha$; per la definizione di sottogruppo si ha $h^{-1} \in H$ e da $b = ha$ segue $h^{-1}b = a$, dunque $b \sim a$.
Proprietà transitiva: se $a \sim b$ e $b \sim c$ allora $\exists\, h_1, h_2 \in H$ tali che $b = h_1 a$ e $c = h_2 b$, ma allora $c = h_2 h_1 a$ e, per definizione di sottogruppo, $h_2 h_1 \in H$; dunque $a \sim c$.
2. Un elemento $b \in G$ appartiene ad Ha se e solo se $\exists\, h \in H$ tale che $b = ha$ cioè se e solo se $b \sim a$, dunque $Ha = [a]$. $\square$

Corollario 1.2.15 *Sia H un sottogruppo di un gruppo G. Sia R un insieme di rappresentanti per le classi laterali (destre) di H in G. Allora $G = \bigcup_{a \in R} Ha$ e classi laterali distinte sono disgiunte.*

Dim. Segue immediatamente dalla Proposizione precedente e dalle proprietà delle classi di equivalenza (Proposizione 3.2.3). $\square$

Esempio Sia $H = n\mathbb{Z} < \mathbb{Z} = G$, allora $b = ha$ significa $b = nl + a$ per qualche $l \in \mathbb{Z}$ (perché $h \in H$ significa $h = nl$ e l'operazione su $\mathbb{Z}$ è la somma). Dunque $a \sim b \iff \exists\, l \in \mathbb{Z}$ tale che $b = nl + a$, cioè $\iff n | a - b$. Quindi la congruenza modulo $n\mathbb{Z}$ non è altro che la solita congruenza modulo n.

Lemma 1.2.16 *Due classi laterali di H sono in corrispondenza biunivoca tra loro.*

Dim. Sia Ha una classe laterale di H in G. Definiamo $f : H \longrightarrow Ha$ con $f(h) = ha$. Si verifica facilmente che f è biunivoca dunque ogni classe laterale è in corrispondenza biunivoca con H. $\square$

Un'importante conseguenza è il seguente

Teorema 1.2.17 (Lagrange) *Se G è un gruppo finito ed $H < G$ allora $o(H)|o(G)$.*

Dim. Abbiamo visto che $G = \bigcup_{a \in R} Ha$ (dove R è un insieme di rappresentanti). Dato che l'unione è tra insiemi disgiunti si ha

$$o(G) = \sum_{a \in R} o(Ha) = (\text{Lemma 1.2.16}) = \sum_{a \in R} o(H) = o(H)\#R \; . \quad \square$$

Corollario 1.2.18 *Sia G un gruppo finito e sia $a \in G$. Allora*

1. *$o(a)|o(G)$;*
2. *$a^{o(G)} = e$;*
3. *se $o(G) = p$ è primo, allora G è ciclico.*

Dim. **1.** Nella malaugurata ipotesi che qualche studente pigro non abbia dimostrato che $o(a) = o(< a >)$ quando era il momento di farlo, ecco una breve dimostrazione. Sia $< a >= \{a^n : n \in \mathbb{Z}\}$, se $o(a) = \infty$ allora $a^n \neq a^m$ per ogni $n \neq m$ (altrimenti $a^n = a^m \Longrightarrow a^{n-m} = e \Longrightarrow o(a) \leq |n - m|$), dunque $< a >$ avrebbe infiniti elementi il che è impossibile perché $< a > \subset G$ che è un gruppo finito. Supponiamo allora $o(a) = n < \infty$. Per ogni $m \in \mathbb{Z}$ possiamo scrivere $m = nq + r$ per qualche $q, r \in \mathbb{Z}$ con $0 \leq r < n$. Dunque

$$a^m = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$$

e $< a >= \{a^0 = e, a, a^2, \ldots, a^{n-1}\}$. Gli elementi a^i, $0 \leq i \leq n-1$, sono tutti distinti perché se $a^i = a^j$ per qualche $o \leq i < j \leq n-1$ allora $a^{j-i} = e$ il che contraddice la minimalità di $o(a)$. Quindi $< a >$ ha $n = o(a)$ elementi e, per il Terema di Lagrange, $o(a) = o(< a >)|o(G)$.
2. Banale conseguenza di **1**.
3. Sia $a \in G - \{e\}$, allora $o(a) \neq 1$. Quindi, dato che $o(a)|o(G)$, deve essere $o(a) = p = o(G)$, cioè $< a >= G$. $\square$

Esempi - Teoremi di Eulero e Fermat Sia $G = ((\mathbb{Z}/n\mathbb{Z})^*, \cdot, 1)$ il gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$. Sappiamo che $o(G) = \phi(n)$ dove ϕ è la funzione di Eulero, cioè

$$\phi(n) = \#\{a \in \mathbb{N} \,:\, 0 < a < n \text{ e } (a, n) = 1\} \ .$$

Dunque $a^{o(G)} = e$ si traduce nel *Teorema di Eulero*:
$\forall\, a$ tale che $(a, n) = 1$ si ha $a^{\phi(n)} \equiv 1 \pmod{n}$.
Ricordiamo che, per convenzione, $\phi(1) = 1$ e inoltre
i) per ogni primo p ed ogni $k > 0$ si ha $\phi(p^k) = p^{k-1}(p-1)$;
ii) se $n = \prod_{i=1}^{d} p_i^{k_i}$ allora $\phi(n) = \prod_{i=1}^{d} \phi(p_i^{k_i})$.
Segue facilmente il (piccolo) *Teorema di Fermat*:
sia p un primo, allora $\forall\, a \in \mathbb{Z}$ si ha $a^p \equiv a \pmod{p}$.

Definizione 1.2.19 Sia G un gruppo ed $H < G$. L'*indice* di H in G è il numero di classi laterali (destre o sinistre) di H e si indica con $[G : H]$ o con $i_G(H)$.

Osservazione 1.2.20 La definizione non distingue tra classi laterali destre e sinistre perché il loro numero è lo stesso. Infatti la funzione

$$f : \{\text{Classi laterali destre di } H\} \longrightarrow \{\text{Classi laterali sinistre di } H\}$$

data da $f(Ha) = a^{-1}H$ è biunivoca (dimostrarlo).

Corollario 1.2.21 *Sia G un gruppo finito ed $H < G$. Allora $o(G) = o(H)[G : H]$.*

Dim. Segue banalmente dal Teorema di Lagrange osservando che $[G : H] = \#R$. $\square$

Nei gruppi infiniti invece si possono avere:

1. sottogruppi infiniti di indice finito, per esempio $n\mathbb{Z}$ in $\mathbb{Z}$ per $n \neq 0$;

2. sottogruppi infiniti di indice infinito, per esempio $< 2 >$ in $\mathbb{R}^*$;

3. sottogruppi finiti di indice infinito, per esempio $< -1 >$ in $\mathbb{R}^*$.

Gruppi ciclici

Vogliamo studiare più approfonditamente i gruppi ciclici per varie ragioni tra cui una immediata (sono facili da descrivere) ed una che sarà chiara più in là nel corso (sono importanti come "mattoni" con cui costruire tutti i gruppi abeliani, vd Teoremi 1.5.3 e 1.5.4). Osserviamo prima di tutto che un gruppo ciclico è abeliano.

1. Sia G un gruppo ciclico e sia $H < G$. Allora H è ciclico.
Dim. Sia $G =< a >$: se $H = \{e\}$ allora è ovviamente ciclico. Se $H \neq \{e\}$ allora $\exists\, m > 0$ tale che $a^m \in H$ (perché ?), dunque possiamo definire (per il principio del buon ordinamento) un intero $d = \min\{m > 0 \ t.c. \ a^m \in H\}$. Ovviamente $< a^d > \subset H$ e se $a^n \in H$ allora, dividendo n per d, possiamo scrivere $n = dq + r$ con $0 \leq r < d$. Dunque $a^n = a^{dq+r} \Longrightarrow a^r = a^n(a^{-d})^q \in H$ e la minimalità di $d \Longrightarrow r = 0$ cioè $a^n \in < a^d >$ e quindi $H =< a^d >$.

Faremo adesso una serie di esercizi che, oltre a descrivere precisamente la struttura dei gruppi ciclici, porteranno alla dimostrazione di una nota formula sulla ϕ di Eulero e precisamente $\sum_{d|n} \phi(d) = n$.

2. *Generatori di un gruppo ciclico.* Sia $G =< a >$ un gruppo ciclico.
Supponiamo $o(G) = \infty$: se a^n è un generatore allora $\exists\, m \in \mathbb{Z}$ tale che $(a^n)^m = a$ cioè $a^{nm-1} = e$. Dato che a ha ordine infinito deve essere $nm = 1$ cioè $n = \pm 1$ ed i generatori sono solo 2: a ed a^{-1}.
Supponiamo $o(G) = t < \infty$: come sopra se a^n è un generatore allora $\exists\, m \in \mathbb{Z}$ tale che $(a^n)^m = a$ cioè $a^{nm-1} = e$. Dato che $o(a) = t$ deve essere $nm - 1 \equiv 0 \pmod{t}$. Tale congruenza (nell'incognita m) ha soluzione se e solo se $(n, t) = 1$. Dunque ci sono $\phi(t)$ generatori, esattamente gli elementi a^n con $0 < n < t$ e $(n, t) = 1$.

3. Sia G un gruppo ed $a \in G$ un elemento di ordine finito, $o(a) = n$. Allora per ogni $m \in \mathbb{Z}$ si ha

$$o(a^m) = \frac{n}{(m, n)} = \frac{o(a)}{(m, o(a))} \ .$$

Dim. Ovviamente $(a^m)^{\frac{n}{(m,n)}} = a^{\frac{nm}{(m,n)}} = e$ perché $n | \frac{nm}{(m,n)} = [n, m]$, dunque $o(a^m) | \frac{n}{(m,n)}$. Inoltre se $o(a^m) = l$ allora $a^{ml} = e$. Dunque $n | ml$ e $\frac{n}{(m,n)} | l$. Possiamo concludere che $o(a^m) = \frac{n}{(m,n)}$.

4. Sia $G =< a >$ ciclico di ordine finito n. Allora per ogni d divisore di n $\exists!\, H < G$ tale che $o(H) = d$.
Dim. Se $n = md$ è facile vedere che $H =< a^m >$ ha ordine d. Sia adesso K un sottogruppo di ordine d, dato che K è ciclico deve essere $K =< a^l >$ per

qualche $l \in \mathbb{Z}$. Dunque

$$d = o(a^l) = \frac{n}{(n,l)} = \frac{md}{(n,l)} \Longrightarrow (n,l) = m \ .$$

Esiste quindi una soluzione t della congruenza $lx \equiv m \pmod{n}$, cioè t tale che $lt = m + nk$ per qualche $k \in \mathbb{Z}$. Dato che $o(a) = n$ si ha $a^m = a^{m+nk} = a^{lt} \in < a^l >= K \Longrightarrow H \subset K$, ma dato che hanno lo stesso ordine deve essere $H = K$. Dunque H è l'unico sottogruppo di G di ordine d.

5. Sia G ciclico di ordine finito n. Allora per ogni d divisore di n ci sono, in G, esattamente $\phi(d)$ elementi di ordine d.
Dim. Un elemento di ordine d genera un sottogruppo di ordine d e abbiamo visto che c'è un solo sottogruppo con tale ordine ed è ciclico. Dunque gli elementi di ordine d sono tutti e soli i generatori di quel sottogruppo $\Longrightarrow$ sono $\phi(d)$ = numero di generatori di un gruppo ciclico di ordine d.

6. *Formula per la ϕ di Eulero.* Per ogni $n \in \mathbb{N} - \{0\}$ si ha

$$\sum_{d|n} \phi(d) = n \ .$$

Dim. Sia G un gruppo ciclico di ordine n (per esempio $\mathbb{Z}/n\mathbb{Z}$). Per ogni d divisore di n sia $G_d = \{a \in G \ t.c. \ o(a) = d\}$. Gli insiemi (solo uno di loro è un sottogruppo, quale ?) G_d sono disgiunti perchè uno stesso elemento non può avere due diversi ordini e, per il Teorema di Lagrange, la loro unione è tutto G. Infine abbiamo visto che G_d ha $\phi(d)$ elementi e quindi

$$G = \bigcup_{d|n} G_d \text{ (disgiunti)} \Longrightarrow n = o(G) = \sum_{d|n} \#G_d = \sum_{d|n} \phi(d) \ .$$

7. Verificare i punti **2**, **3**, **4** e **5** per qualche gruppo $\mathbb{Z}/n\mathbb{Z}$.

1.2.2 Sottogruppi normali - Gruppi quoziente

Nel caso delle classi resto modulo n sappiamo che è possibile definire sulle classi di equivalenza (le classi laterali di $< n >$ in $\mathbb{Z}$) un'operazione di somma (indotta da $\mathbb{Z}$) rispetto alla quale tali classi formano un gruppo. Questo non è sempre possibile per sottogruppi H qualsiasi di un gruppo G. Prima di tutto perché l'operazione indotta da G sia ben definita sulle classi laterali di H è necessario che la relazione di equivalenza indotta da H (la congruenza) sia compatibile con l'operazione di G (Definizione 3.2.5), poi si deve verificare che

l'insieme delle classi di equivalenza (insieme quoziente) con tale operazione sia un gruppo. Affrontiamo separatamente i due problemi, vedremo che risolvere il primo significa risolvere automaticamente anche il secondo.

Proposizione 1.2.22 *Sia G un gruppo ed $H < G$. Sia $\sim$ la relazione di equivalenza indotta da H. Allora $\sim$ è compatibile con l'operazione di $G \iff$ per ogni $a \in G$, $aH = Ha$ (cioè se classi laterali destre e sinistre coincidono).*

Dim. ($\Longleftarrow$) Siano $a \sim b$ e $c \sim d$ elementi equivalenti di G, allora $\exists\, h_1\,, h_2 \in H$ tali che $b = h_1 a$ e $d = h_2 c$. Dunque $bd = h_1 a h_2 c$, ma $Ha = aH$ implica che $\exists\, h_3 \in H$ tale che $h_3 a = a h_2\,$. Quindi $bd = h_1 h_3 ac \Longrightarrow$ (dato che $h_1 h_3 \in H$) $ac \sim bd$ che è la condizione richiesta per la compatibilità di $\sim$ con l'operazione di G.
($\Longrightarrow$) Sia $ah \in aH$, allora per la relazione indotta da H si hanno le equivalenze $a \sim a$ ed $e \sim h$. Per la compatibilità di $\sim$ con l'operazione si ha $ae \sim ah$, cioè $\exists\, k \in H$ tale che $ah = kae = ka \in Ha$. Dunque $aH \subset Ha$ e l'inclusione opposta si dimostra nello stesso modo. $\square$

Esempio In S_3 siano $\tau = (2\,3)$ e $\sigma = (1\,2\,3)$ e definiamo $K =< \tau >$ e $H =< \sigma >$.

Laterali destri	Laterali sinistri
$K = \{id, (2\,3)\}$	$K = \{id, (2\,3)\}$
$K(1\,2) = \{(1\,2), (1\,3\,2)\}$	$(1\,2)K = \{(1\,2), (1\,2\,3)\}$
$K(1\,3) = \{(1\,3), (1\,2\,3)\}$	$(1\,3)K = \{(1\,3), (1\,3\,2)\}$
$H = \{id, (1\,2\,3), (1\,3\,2)\}$	$H = \{id, (1\,2\,3), (1\,3\,2)\}$
$H(1\,2) = \{(1\,2), (1\,3), (2\,3)\}$	$(1\,2)H = \{(1\,2), (2\,3), (1\,3)\}$

Dunque H verifica la condizione della proposizione e K no. In effetti per la relazione (destra) indotta da K si ha (per esempio) $(1\,2) \sim (1\,3\,2)$ e $(1\,3) \sim (1\,2\,3)$ ma $(1\,2)(1\,3) = (1\,3\,2) \in K(1\,2) \not\sim (1\,3\,2)(1\,2\,3) = id \in K$.

Osservazione 1.2.23 È *molto importante* ricordare che $aH = Ha$ *non implica* $ah = ha$ per ogni $h \in H$. Nell'esempio precedente abbiamo visto che $H(1\,2) = (1\,2)H$ ma $(1\,2\,3)(1\,2) = (1\,3) \in H(1\,2)$ è diverso da $(1\,2)(1\,2\,3) = (2\,3) \in (1\,2)H$.

I sottogruppi che inducono relazioni di equivalenza compatibili con l'operazione del gruppo sono particolarmente importanti nella costruzione degli insiemi quoziente (che, senza un'operazione, non sembrerebbero avere proprietà degne di attenzione).

Definizione 1.2.24 Un sottogruppo H di un gruppo G si dice *normale*, e si scrive $H \lhd G$, se verifica una delle seguenti proprietà equivalenti tra loro:

1. $\forall\, a \in G$ si ha $aH = Ha$;
2. $\forall\, a \in G$ si ha $aHa^{-1} = H$;
3. $\forall\, a \in G$ si ha $aHa^{-1} \subset H$.

Esercizio Verificare l'equivalenza delle proprietà dimostrando che **1** $\Longrightarrow$ **2** $\Longrightarrow$ **3** $\Longrightarrow$ **1**.

Teorema 1.2.25 *Sia G un gruppo e sia $H \lhd G$. Definiamo G/H l'insieme delle classi laterali di H in G (cioè l'insieme quoziente delle classi di equivalenza di G per la relazione indotta da H). Definiamo una funzione $G/H \times G/H \longrightarrow G/H$ data da $(Ha, Hb) \longrightarrow Hab$ (dove il prodotto ab è l'operazione di G). Allora:*

1. *la funzione è un'operazione ben definita su G/H, cioè è indipendente dai rappresentanti scelti per le classi di equivalenza;*
2. *con tale operazione G/H è un gruppo di ordine $o(G/H) = [G : H]$.*

Tale gruppo si definisce gruppo quoziente *di G rispetto ad H.*

Dim. **1.** Abbiamo già dimostrato nella Proposizione 1.2.22 che se H è normale in G allora $Ha = Hb$ e $Hc = Hd$ implicano $HaHc = Hac = Hbd = HbHd$.
2. L'associatività dell'operazione segue dall'associatività in G.
L'elemento neutro è dato dalla classe H.
L'inverso di Ha è Ha^{-1}.
Il fatto che $o(G/H) = [G : H]$ segue dalla definizione di indice. $\square$

Esempi

1. Il quoziente di $\mathbb{Z}$ rispetto a $n\mathbb{Z}$ è il gruppo delle classi resto $\mathbb{Z}/n\mathbb{Z}$.
2. Sia $H = \{x \in \mathbb{R}^* \,:\, x > 0\} \lhd \mathbb{R}^*$, allora $\mathbb{R}^*/H$ ha due soli elementi: H e $H(-1) = -H = \{x \in \mathbb{R}^* \,:\, x < 0\}$ e l'operazione è definita da $H(-H) = (-H)H = -H$ e $(-H)(-H) = H$.

Qualche sottogruppo normale - Esercizi

1. Sia $H =< \sigma >=< (1\,2\,3\,4) >$ un sottogruppo di S_4. Scriviamo le classi laterali destre e sinistre di H in S_4.
Sappiamo che $o(S_4) = 4! = 24$ e che $o(H) = 4$ dunque ci sono $[S_4 : H] = 6$ classi laterali.

Classi laterali destre	Classi laterali sinistre
$H = \{id, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$	$H = \{id, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$
$H(1\,2) = \{(1\,2), (1\,3\,4), (1\,4\,2\,3), (2\,4\,3)\}$	$(1\,2)H = \{(1\,2), (2\,3\,4), (1\,3\,2\,4), (1\,4\,3)\}$
$H(1\,3) = \{(1\,3), (1\,4)(2\,3), (2\,4), (1\,2)(3\,4)\}$	$(1\,3)H = \{(1\,3), (1\,2)(3\,4), (2\,4), (1\,4)(2\,3)\}$
$H(1\,4) = \{(1\,4), (2\,3\,4), (1\,2\,4\,3), (1\,3\,2)\}$	$(1\,4)H = \{(1\,4), (1\,2\,3), (1\,3\,4\,2), (2\,4\,3)\}$
$H(2\,3) = \{(2\,3), (1\,2\,4), (1\,3\,4\,2), (1\,4\,3)\}$	$(2\,3)H = \{(2\,3), (1\,3\,4), (1\,2\,4\,3), (1\,4\,2)\}$
$H(3\,4) = \{(3\,4), (1\,2\,3), (1\,3\,2\,4), (1\,4\,2)\}$	$(3\,4)H = \{(3\,4), (1\,2\,4), (1\,4\,2\,3), (1\,3\,2)\}$

2. Scrivere le classi laterali destre e sinistre di $H = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ e di $\mathscr{A}_4$ (le permutazioni pari) in S_4.

3. Verificare che $D_4 = \{id, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma = \sigma^3\tau, \tau\sigma^2 = \sigma^2\tau, \tau\sigma^3 = \sigma\tau\}$ dove $\sigma = (1\,2\,3\,4)$ e $\tau = (1\,4)(2\,3)$. Sia $H =< \sigma >$, verificare che $D_4 = H \bigcup H(1\,3) < S_4$. Scrivere le classi laterali destre e sinistre di D_4 in S_4. Scrivere le classi laterali di $K =< \sigma^2 >$ in D_4 ed in S_4 e verificare $K \lhd D_4$ ma $K \not\lhd S_4$.

4. Dimostrare che $Z(G) \lhd G$ ($Z(G)$ è il centro di G).

5. Sia A uno degli insiemi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{Z}/p\mathbb{Z}$ con p primo. Dimostrare che $SL_n(A) \lhd GL_n(A)$.

6. Sia G un gruppo e sia H un sottogruppo di G tale che $[G : H] = 2$. Dimostrare che $H \lhd G$.

7. Dimostrare che il sottogruppo $\mathscr{A}_n$ delle permutazioni pari di S_n è normale in S_n.

8. Sia G un gruppo e sia $G' =< aba^{-1}b^{-1} : a, b \in G >$ il sottogruppo generato da tutti gli elementi del tipo $aba^{-1}b^{-1}$. Si definisce G' il *sottogruppo dei commutatori* di G. Dimostrare che $G' \lhd G$ e che G/G' è abeliano. Dimostrare che se $N \lhd G$, allora G/N è abeliano $\iff N \supset G'$.
Dim. Per avere $G' \lhd G$ è sufficiente dimostrare che per ogni generatore $aba^{-1}b^{-1}$ e per ogni $g \in G$ si ha $g(aba^{-1}b^{-1})g^{-1} \in G'$. Infatti si ha

$$gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} =$$

$$= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in G'$$

per definizione di G'.
Per quanto riguarda G/G', per ogni $G'a, G'b \in G/G'$ si ha

$$G'aG'b = G'ab = G'(bab^{-1}a^{-1})ab = G'ba = G'bG'a \ .$$

Infine sia $N \lhd G$, allora G/N è abeliano $\iff$ per ogni $Na, Nb \in G/N$ si ha $NaNb = Nab = NbNa = Nba$ cioè $\iff$ $Nab = Nba$ $\iff$ $Naba^{-1}b^{-1} = N$ $\iff$ $aba^{-1}b^{-1} \in N$. Dunque N deve contenere tutti i generatori di G' e, quindi, anche G' stesso.

1.3 Omomorfismi

Definizione 1.3.1 Siano $(G, *, e)$ ed $(H, \circ, e')$ due gruppi. Una mappa $f : G \longrightarrow H$ si dice *omomorfismo* se $\forall\, a, b \in G$ si ha $f(a * b) = f(a) \circ f(b)$ (cioè l'immagine della composizione è la composizione delle immagini). Un omomorfismo biunivoco si dice *isomorfismo*. Due gruppi G ed H si dicono *isomorfi*, e si scrive $G \simeq H$, se esiste un isomorfismo $f : G \longrightarrow H$.

Esempi - Esercizi

1. Definiamo una relazione nell'insieme di tutti i gruppi: $G \sim G' \iff G \simeq G'$ (G è isomorfo a G'). Dimostrare che la relazione così definita è una relazione di equivalenza.

2. La mappa $f : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}^*, \cdot, 1)$ definita da $f(x) = e^x$ è un omomorfismo. Infatti $\forall\, a, b \in \mathbb{R}$ si ha $f(a+b) = e^{a+b} = e^a e^b = f(a)f(b)$.

3. La mappa $g : (\mathbb{R}^*, \cdot, 1) \longrightarrow (\mathbb{R}, +, 0)$ definita da $g(x) = ln|x|$ è un omomorfismo. Infatti $\forall\, a, b \in \mathbb{R}^*$ si ha $g(ab) = ln|ab| = ln|a| + ln|b| = g(a) + g(b)$.

4. Sia $\mathbb{R}_{>0} = \{x \in \mathbb{R} \,:\, x > 0\}$, allora $(\mathbb{R}_{>0}, \cdot, 1)$ è un gruppo. Le mappe $f : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}_{>0}, \cdot, 1)$ e $g : (\mathbb{R}_{>0}, \cdot, 1) \longrightarrow (\mathbb{R}, +, 0)$ definite da $f(x) = e^x$ e da $g(y) = ln(y)$ sono due isomorfismi uno inverso dell'altro. Dunque $\mathbb{R} \simeq \mathbb{R}_{>0}$.

5. Sia $f : G \longrightarrow G$ definita da $f(a) = a^2$.

   i) Se $G = \mathbb{R}^*$, f è un omomorfismo, infatti $f(ab) = (ab)^2 = a^2b^2 = f(a)f(b)$.

ii) Se $G = \mathbb{R}$, f è un omomorfismo, $f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b)$.

iii) Se $G = S_3$, f non è un omomorfismo, per esempio con $\sigma = (1\,2\,3)$ e $\tau = (1\,2)$ si ha $f(\sigma\tau) = f((1\,3)) = id \neq f(\sigma)f(\tau) = (1\,3\,2)id = (1\,3\,2)$.

6. Sia $U_n = \{\alpha \in \mathbb{C} \,:\, \alpha^n = 1\}$. Dimostrare che U_n è un sottogruppo di $\mathbb{C}^*$. Sia

$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\ ,$$

si può dimostrare che $U_n =< \zeta_n >$. Definiamo $f : \mathbb{Z} \longrightarrow U_n$ tramite la formula $f(a) = \zeta_n^a$. Dato che $f(a+b) = \zeta_n^{a+b} = \zeta_n^a\zeta_n^b = f(a)f(b)$, f è un omomorfismo.

7. Sia $f : G \longrightarrow G$ definita da $f(a) = a^{-1}$.

i) Se G è abeliano, f è un isomorfismo, infatti $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$ e la biunivocità è facile da verificare.

ii) Se $G = S_3$, f non è un omomorfismo, per esempio con σ e τ come al punto **5** *iii)* si ottiene $f(\sigma\tau) = f((1\,3)) = (1\,3) \neq f(\sigma)f(\tau) = (1\,3\,2)(1\,2) = (2\,3)$.

Definizione 1.3.2 Sia $f : G \longrightarrow H$ un omomorfismo di gruppi. Il *nucleo* di f è l'insieme

$$Ker\, f = \{a \in G \,:\, f(a) = e'\}$$

(dove e' è l'elemento neutro di H). L'*immagine* di f è l'insieme

$$Im\, f = \{\alpha \in H \,:\, \exists\, a \in G \text{ t.c. } f(a) = \alpha\}\ .$$

Proposizione 1.3.3 *Sia $f : G \longrightarrow H$ un omomorfismo di gruppi, allora*

1. $f(e) = e'$;

2. $f(a^{-1}) = f(a)^{-1}$ *e, in generale,* $f(a^n) = f(a)^n$ *per ogni* $n \in \mathbb{Z}$;

3. $Ker\, f \lhd G$;

4. $Im\, f < H$.

Dim. **1.** $f(a)e' = f(a) = f(ae) = f(a)f(e)$, cancellando $f(a)$ si ottiene $e' = f(e)$.
2. $f(aa^{-1}) = f(e) = e'$ ma anche $f(aa^{-1}) = f(a)f(a^{-1})$; dunque $e' = f(a)f(a^{-1})$ e quindi $f(a)^{-1} = f(a^{-1})$. La generalizzazione per $f(a^n)$, $n \in \mathbb{Z}$, è immediata
3. Abbiamo già dimostrato che $e \in Ker\, f \neq \emptyset$.
Siano $a, b \in Ker\, f$ allora $f(a) = f(b) = e'$, dunque $f(ab) = f(a)f(b) = e'e' = e' \Longrightarrow ab \in Ker\, f$.
Sia $a \in Ker\, f$ allora $f(a^{-1}) = f(a)^{-1} = (e')^{-1} = e' \Longrightarrow a^{-1} \in Ker\, f$.
Infine sia $a \in Ker\, f$ e sia $g \in G$ allora $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e'f(g)^{-1} = e' \Longrightarrow gag^{-1} \in Ker\, f$. Quindi, $\forall\, g \in G$, $g(Ker\, f)g^{-1} \subset Ker\, f$ che equivale a dire $Ker\, f \lhd G$.
4. Abbiamo visto che $e' = f(e) \in Im\, f$.
Siano $\alpha, \beta \in Im\, f$ allora $\exists\, a, b \in G$ tali che $f(a) = \alpha$ e $f(b) = \beta$. Quindi $\alpha\beta = f(a)f(b) = f(ab) \in Im\, f$.
Sia $\alpha \in Im\, f$ allora $\alpha = f(a)$ per qualche $a \in G$ e dunque $\alpha^{-1} = f(a)^{-1} = f(a^{-1}) \in Im\, f$. $\square$

Esempi - Esercizi

1. Sia σ la rotazione di $\frac{2\pi}{n}$ radianti in D_n. Sia $f : \mathbb{Z} \longrightarrow D_n$ data da $f(a) = \sigma^a$ per ogni $a \in \mathbb{Z}$. Verificare che f è un omomorfismo. L'immagine di f è l'insieme $\{\sigma^a : a \in \mathbb{Z}\} =< \sigma >$ che è un sottogruppo di D_n. Un intero a è in $Ker\, f$ se e solo se $\sigma^a = id$, cioè se e solo se $o(\sigma)|a$. Dato che $o(\sigma) = n$ si ha $Ker\, f = n\mathbb{Z}$.

2. Sia $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ la funzione definita da $f(a) = \frac{a}{|a|} = sgn(a)$. Verificare che è un omomorfismo con $Im\, f = \{1, -1\}$ e $Ker\, f = \{a \in \mathbb{R} : a > 0\}$.

3. Sia $f : \mathbb{Q}[X] \longrightarrow \mathbb{Q}$ definita da $f(P(X)) = P(1)$. La mappa è un omomorfismo, infatti $f(P+Q) = (P+Q)(1) = P(1) + Q(1) = f(P) + f(Q)$. Inoltre f è surgettiva perché per ogni $a \in \mathbb{Q}$ si ha $f(a) = a$ e infine $P \in Ker\, f \iff f(P) = P(1) = 0 \iff (X-1)|P$ (per il Teorema di Ruffini).

Per gli omomorfismi il nucleo serve a caratterizzare l'iniettività della mappa.

Proposizione 1.3.4 *Sia $f : G \longrightarrow H$ un omomorfismo di gruppi, allora f è iniettivo se e solo se $Ker\, f = \{e\}$.*

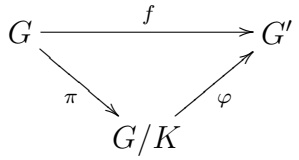
Dim. ($\Longrightarrow$) Ovvio dato che $f(e) = e'$.
($\Longleftarrow$) Se $f(a) = f(b)$ allora $f(a)f(b)^{-1} = e' \Longrightarrow f(ab^{-1}) = e'$ e dunque $ab^{-1} \in Ker\, f$. Quindi $ab^{-1} = e \Longrightarrow a = b$ ed f è iniettiva. $\square$

Esercizio Dimostrare che se $f : G \longrightarrow H$ è un omomorfismo di gruppi, allora $f(a) = f(b) \iff aKer\, f = bKer\, f$.

Esempio (fondamentale) Sia G un gruppo ed $H \lhd G$. Definiamo la *proiezione sul quoziente* $\pi : G \longrightarrow G/H$ tramite la formula $\pi(a) = Ha$. È un omomorfismo, infatti $\pi(ab) = Hab = HaHb = \pi(a)\pi(b)$ (ricordare la definizione del prodotto sul gruppo quoziente). La proiezione è ovviamente surgettiva ed il suo nucleo è esattamente $Ker\, f = H$. Dunque per ogni sottogruppo normale H di G esiste un omomorfismo surgettivo che ha per nucleo H.

1.3.1 I Teoremi di omomorfismo

Teorema 1.3.5 (1^o Teorema di omomorfismo) *Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi con nucleo K. Sia $\pi : G \longrightarrow G/K$ la proiezione, allora $\exists!$ omomorfismo iniettivo $\varphi : G/K \longrightarrow G'$ che rende commutativo il diagramma*



cioè tale che $\varphi \circ \pi = f$.

Dim. Per ottenere la commutatività del diagramma è necessario definire $\varphi(Ka) = f(a)$ per ogni $Ka \in G/K$. Prima di verificare che φ sia un omomorfismo dobbiamo accertarci che sia ben definita, cioè che $\varphi(Ka)$ non dipenda dal rappresentante scelto per la classe di equivalenza di a. Dunque supponiamo $Ka = Kb$, allora $\exists\, c \in K$ tale che $b = ca$ e quindi $\varphi(Kb) = f(b) = f(ca) = f(c)f(a) = ef(a) = f(a) = \varphi(Ka)$. Dimostrato questo (che non va mai dimenticato quando si definiscono strutture su un insieme quoziente) il resto è ordinaria amministrazione.
Infatti $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$, dunque φ è un omomorfismo. Infine $Ka \in Ker\, \varphi \iff \varphi(Ka) = f(a) = e'$, ma $f(a) = e' \iff a \in K$ dunque $Ka \in Ker\, \varphi \iff a \in K$ cioè $\iff Ka = K$ e K è l'elemento neutro di G/K, quindi (per la Proposizione 1.3.4) φ è iniettiva. $\square$

Corollario 1.3.6 *Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi, allora $G/Ker\, f$ è isomorfo a $Im\, f$.*

Dim. Sia $\varphi : G/Ker\, f \longrightarrow G'$ la mappa descritta dal Teorema. Tale mappa è iniettiva ed è ovviamente surgettiva sulla propria immagine che, per definizione, è $Im\, \varphi = Im\, f$. $\square$

Come applicazione possiamo dimostrare la seguente

Proposizione 1.3.7 *Sia G un gruppo ciclico allora*

$$G \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{se } o(G) = n \\ \mathbb{Z} & \text{se } o(G) = \infty \end{cases} .$$

Dim. Sia $G =< a >= \{a^n : a \in \mathbb{Z}\}$, definiamo $f : \mathbb{Z} \longrightarrow G$ tramite la formula $f(n) = a^n$. È facile verificare che f è un omomorfismo surgettivo. Il nucleo di f è un sottogruppo di $\mathbb{Z}$, dunque è del tipo $n\mathbb{Z}$ per qualche $n \in \mathbb{Z}$. Se $Ker\, f = \{0\}$ allora f è anche iniettiva e $G \simeq \mathbb{Z}$ è infinito. Se invece $Ker\, f = n\mathbb{Z}$ per qualche $n > 0$ allora il Corollario 1.3.6 implica che $\mathbb{Z}/n\mathbb{Z} \simeq G$. $\square$

Un omomorfismo tra due gruppi G e G' fornisce anche una corrispondenza tra i sottogruppi di G e G' che si può riassumere nel seguente

Lemma 1.3.8 *Sia $f : G \longrightarrow G'$ un omomorfismo surgettivo tra gruppi. L'applicazione indotta*

$$\tilde{f} : \{\, H < G \text{ t.c. } Ker\, f \subset H \,\} \longrightarrow \{\, H' < G' \,\}$$

definita da $\tilde{f}(H) = f(H)$ è biunivoca.

Dim. La prima cosa da verificare è che la definizione di $\tilde{f}$ abbia senso, cioè che $\tilde{f}(H)$ sia un sottogruppo di G' per ogni $H < G$ contenente $Ker\, f$. Ovviamente $e \in H \Longrightarrow e' = f(e) \in f(H)$, inoltre se $x = f(a), y = f(b) \in f(H)$ allora $xy = f(a)f(b) = f(ab) \in f(H)$. Infine se $x = f(a) \in f(H)$ allora $a^{-1} \in H$ e dunque $x^{-1} = f(a)^{-1} = f(a^{-1}) \in f(H)$.
Per l'iniettività supponiamo che $\tilde{f}(H) = \tilde{f}(K)$ (cioè $f(H) = f(K)$), allora, $\forall\, h \in H$, $\exists\, k \in K$ tale che $f(h) = f(k)$ e dunque $f(h)f(k)^{-1} = f(hk^{-1}) = e' \Longrightarrow hk^{-1} \in Ker\, f$. Quindi $h \in (Ker\, f)k \subset Ker\, fK \subset K$ (perché, per ipotesi, stiamo considerando solo sottogruppi di G che contengano $Ker\, f$) e $H \subset K$. Il viceversa è simmetrico, quindi $H = K$ e la funzione $\tilde{f}$ è iniettiva. Per la surgettività sia $H' < G'$ e definiamo $H = \{a \in G \text{ t.c. } f(a) \in H'\}$.

È facile verificare che $H < G$ e $Ker\, f \subset H$, inoltre, per definizione e per la surgettività di f, si ha $f(H) = H'$ quindi $\tilde{f}$ è anche surgettiva. $\square$

Esercizio Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi (non necessariamente surgettivo). Dimostrare che se $H' \lhd G'$ allora $f^{-1}(H') = \{a \in G \ t.c. \ f(a) \in H'\}$ è un sottogruppo normale di G. Il viceversa non è vero cioè $H \lhd G$ *non implica* $f(H) \lhd G'$ in generale. Per esempio, la mappa $f : \mathbb{Z} \longrightarrow S_3$ definita da $f(n) = (1\,2)^n$ è un omomorfismo e l'immagine del sottogruppo normale $3\mathbb{Z}$ è $\{id, (1\,2)\}$ che non è normale in S_3.

Esercizio Sia $f : G \longrightarrow G'$ un omomorfismo surgettivo tra gruppi. Dimostrare che se $H \lhd G$ allora $f(H) \lhd G'$.

Teorema 1.3.9 (2^o Teorema di omomorfismo) *Sia $f : G \longrightarrow G'$ un omomorfismo surgettivo tra gruppi con nucleo $Ker\, f = K$. Siano $N' \lhd G'$ ed $N = f^{-1}(N')$. Allora*

$$G/N \simeq G'/N' \simeq (G/K)/(N/K) \ .$$

Dim. Il Teorema 1.3.5 ed il suo Corollario 1.3.6 applicati agli omomorfismi $f : G \longrightarrow G'$ ed $f_{|N} : N \longrightarrow N'$ (f ristretto ad N) forniscono gli isomorfismi $G' \simeq G/K$ e $N' \simeq N/K$. È facile verificare che la mappa $\varphi : G \longrightarrow G'/N'$ definita da $\varphi(a) = N'f(a)$ è un omomorfismo surgettivo con nucleo N. Dunque ancora il 1^o Teorema di omomorfismo fornisce l'isomorfismo $G/N \simeq G'/N'$. $\square$

1.3.2 Automorfismi

Di particolare importanza sono gli omomorfismi di un gruppo in sé stesso.

Definizione 1.3.10 Sia G un gruppo, un omomorfismo $f : G \longrightarrow G$ si dice *endomorfismo* di G e l'insieme degli endomorfismi di G si indica con $End(G)$. Un endomorfismo biunivoco si dice *automorfismo* e l'insieme degli automorfismi di G si indica con $Aut(G)$.

Proposizione 1.3.11 *Sia G un gruppo, allora $(Aut(G), \circ, id)$ è un gruppo.*

Dim. Abbiamo già visto che le funzioni biunivoche formano un gruppo rispetto alla composizione, ma qui vogliamo limitarci solo agli omomorfismi. L'identità è ovviamente un isomorfismo dunque $id \in Aut(G)$ e l'associatività di

$\circ$ vale in $Aut(G)$ perché vale in generale per tutte le funzioni.
Siano $f, g \in Aut(G)$ allora $f \circ g$ è biunivoca (perché lo sono f e g) e $\forall\, a, b \in G$ $(f \circ g)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = (f \circ g)(a)(f \circ g)(b)$ dunque $f \circ g \in Aut(G)$.
Infine se $f \in Aut(G)$ allora f^{-1} è biunivoca, inoltre, $\forall\, a, b \in G$, $f(f^{-1}(ab)) = ab$ e $f(f^{-1}(a)f^{-1}(b)) = ff^{-1}(a)ff^{-1}(b) = ab$. Quindi per l'iniettività di f si ha $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ ed anche $f^{-1} \in Aut(G)$. $\square$

Esempio Sia $a \in G$ gruppo. Definiamo $\varphi_a : G \longrightarrow G$ tramite la formula $\varphi_a(g) = aga^{-1}$ per ogni $g \in G$. Dimostriamo che $\varphi_a \in Aut(G)$ per ogni $a \in G$.
Per ogni $g, h \in G$ si ha $\varphi_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \varphi_a(g)\varphi_a(h)$ dunque $\varphi_a \in End(G)$. Inoltre $\varphi_a(g) = \varphi_a(h) \Longrightarrow aga^{-1} = aha^{-1}$ e, cancellando a ed a^{-1}, si ottiene $g = h$ dunque φ_a è iniettiva. Infine, per ogni $h \in G$, abbiamo $a^{-1}ha \in G$ e $\varphi_a(a^{-1}ha) = h$ dunque φ_a è anche surgettiva e $\varphi_a \in Aut(G)$.

Definizione 1.3.12 Gli automorfismi come φ_a definito nell'esempio precedente si dicono *automorfismi interni* di G e l'insieme di tali automorfismi si indica con $Int(G) = \{\varphi_a : a \in G\}$.

Proposizione 1.3.13 *Sia G un gruppo. Allora*

1. *se G è abeliano $Int(G) = \{id\}$;*
2. *$Int(G) \lhd Aut(G)$;*
3. *$Int(G) \simeq G/Z(G)$ (dove $Z(G)$ è il centro di G).*

Dim. **1.** Ovvio.
2. L'elemento neutro $id = \varphi_e \in Int(G)$.
Siano $a, b, g \in G$ allora $\varphi_a\varphi_b(g) = \varphi_a(bgb^{-1}) = abgb^{-1}a^{-1} = (ab)g(ab)^{-1} = \varphi_{ab}(g)$ dunque $\varphi_a\varphi_b = \varphi_{ab} \in Int(G)$.
Con la formula appena dimostrata è facile vedere che $\varphi_a^{-1} = \varphi_{a^{-1}} \in Int(G)$.
Infine per ogni $\varphi_a \in Int(G)$, $\psi \in Aut(G)$ e $g \in G$ si ha

$$\psi\varphi_a\psi^{-1}(g) = \psi(a\psi^{-1}(g)a^{-1}) = \psi(a)\psi(\psi^{-1}(g))\psi(a^{-1}) =$$

$$= \psi(a)g\psi(a)^{-1} = \varphi_{\psi(a)}(g)\ .$$

Dunque $\psi\varphi_a\psi = \varphi_{\psi(a)} \in Int(G)$ e quindi $Int(G) \lhd Aut(G)$.
3. Definiamo $f : G \longrightarrow Int(G)$ tramite la formula $f(a) = \varphi_a$. Con quanto dimostrato in **2** è facile vedere che f è un omomorfismo surgettivo e che il suo nucleo è $Z(G)$ dunque, per il Teorema 1.3.5, si ha $G/Z(G) \simeq Int(G)$. $\square$

Definizione 1.3.14 Il gruppo quoziente $Aut(G)/Int(G)$ si dice gruppo degli *automorfsmi esterni* di G.

Applicazioni - Esercizi

1. Sia $\phi : \mathbb{N}^+ \longrightarrow \mathbb{N}$ la funzione di Eulero definita da $\phi(1) = 1$ e $\phi(n) = \#\{a \in \mathbb{N} \; t.c. \; 1 \leq a \leq n-1 \; e \; (n,a) = 1\}$ per ogni $n \geq 2$ (dunque in particolare per ogni $n \geq 2$ si ha $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$).
Dimostrare che per ogni primo p e per ogni $k \in \mathbb{N}^+$ si ha $\phi(p^k) = p^{k-1}(p-1)$.
Dimostrare che se $(m,n) = 1$ allora $\phi(mn) = \phi(n)\phi(m)$.
Dim. Sugg. Costruire un isomorfismo $(\mathbb{Z}/nm\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.

2. Sia A uno dei gruppi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{Z}/p\mathbb{Z}$ con p primo. Dimostrare che $\det : GL_n(A) \longrightarrow A^*$ (dove A^* è l'insieme degli elementi di A invertibili rispetto al prodotto) è un omomorfismo surgettivo con nucleo $SL_n(A)$.

3. Per calcolare $o(SL_2(\mathbb{Z}/p\mathbb{Z}))$ consideriamo l'omomorfismo appena visto $\det : GL_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$. È surgettivo ed ha nucleo $SL_2(\mathbb{Z}/p\mathbb{Z})$, dunque, per il primo Teorema di omomorfismo, $GL_2(\mathbb{Z}/p\mathbb{Z})/SL_2(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$. Allora

$$o(SL_2(\mathbb{Z}/p\mathbb{Z})) = \frac{o(GL_2(\mathbb{Z}/p\mathbb{Z}))}{o((\mathbb{Z}/p\mathbb{Z})^*)} = \frac{o(GL_2(\mathbb{Z}/p\mathbb{Z}))}{p-1} \; .$$

Per calcolare $o(GL_2(\mathbb{Z}/p\mathbb{Z}))$ è sufficiente osservare che per avere una matrice invertibile sono necessarie le righe linearmente indipendenti, dunque abbiamo $p^2 - 1$ possibilità per scegliere la prima riga (tutte tranne $(0\,0)$) e $p^2 - p$ possibilità per la seconda (tutte tranne i p multipli della prima). Quindi $o(GL_2(\mathbb{Z}/p\mathbb{Z})) = (p^2-1)(p^2-p)$ e

$$o(SL_2(\mathbb{Z}/p\mathbb{Z})) = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1) \; .$$

4. Generalizzare l'esercizio precedente calcolando $o(SL_n(\mathbb{Z}/p\mathbb{Z}))$, $n \in \mathbb{N}$.

5. Sia $\varphi : G \longrightarrow G'$ un omomorfismo di gruppi e sia $a \in G$ di ordine finito. Dimostrare che $o(\varphi(a))|o(a)$ e che, se φ è iniettiva, allora $o(\varphi(a)) = o(a)$.
Dim. Ovviamente

$$\varphi(a)^{o(a)} = \varphi(a^{o(a)}) = \varphi(e) = e'$$

dunque $o(\varphi(a))|o(a)$. Inoltre se φ è iniettiva allora

$$\varphi(e) = e' = \varphi(a)^{o(\varphi(a))} = \varphi(a^{o(\varphi(a))}) \Longrightarrow e = a^{o(\varphi(a))}$$

cioè $o(a)|o(\varphi(a))$. Insieme al precedente ciò $\Longrightarrow o(a) = o(\varphi(a))$.

6. Descriviamo tutti gli omomorfismi $\varphi : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z}$.
Osserviamo prima di tutto che è sufficiente definire $\varphi([1]_4)$ perché poi si avrà automaticamente $\varphi([i]_4) = i\varphi([1]_4)$. Inoltre $o(\varphi([1]_4))$ deve essere un divisore di 4 (cioè dell'ordine di $[1]_4$) e di 8 (cioè dell'ordine di $\mathbb{Z}/8\mathbb{Z}$ a cui $\varphi([1]_4)$ appartiene). Le uniche posibilità sono $\varphi([1]_4) = [0]_8\,, [2]_8\,, [4]_8\,, [6]_8\,.$

7. Sia $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}\ t.c.\ \varphi$ omomorfismo$\}$. Definiamo un'operazione su $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ data da $(\varphi + \psi)([a]_n) = \varphi([a]_n) + \psi([a]_n)$ per ogni $\psi, \varphi \in Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$. Dimostrare che, con questa operazione, $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ è un gruppo. Dimostrare inoltre che per ogni $n, m \in \mathbb{N}^+$ si ha

$$Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/(n, m)\mathbb{Z}\ .$$

Dim. La verifica del fatto che $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ è un gruppo è banale (elemento neutro la funzione nulla ed inverso di φ la funzione $-\varphi$ tale che $(-\varphi)([a]_n) = -\varphi([a]_n)$).
Un omomorfismo $\varphi \in Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ è determinato da $\varphi([1]_n)$ che deve avere ordine divisore di $n = o([1]_n)$ e di $m = o(\mathbb{Z}/m\mathbb{Z})$, dunque $o(\varphi([1]_n))|(n, m)$. Caraterizziamo le funzioni tramite la loro immagine. L'insieme $Im\,\varphi$ è un sottogruppo di $\mathbb{Z}/m\mathbb{Z}$ di ordine $d = o(\varphi([1]_n))$ (perché ?), e sappiamo che $\exists!$ sottogruppo di $\mathbb{Z}/m\mathbb{Z}$ di ordine d. Tale sottogruppo ha $\phi(d)$ generatori dunque ci sono $\phi(d)$ scelte possibili per $\varphi([1]_n)$ che danno $Im\,\varphi$ di ordine d. Quindi per ogni d divisore di (n, m) ci sono $\phi(d)$ elementi in $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \Longrightarrow$

$$o(Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})) = \sum_{d|(n,m)} \phi(d) = (n, m)$$

(ricordare la formula sulla ϕ di Eulero dimostrata nella sezione 1.2.1).
In particolare esistono, in $\mathbb{Z}/m\mathbb{Z}$, $\phi((n, m))$ elementi di ordine (n, m) ed uno di essi è $\left[\frac{m}{(n,m)}\right]_m$. Sia $\tilde{\varphi} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ definita da $\tilde{\varphi}([1]_n) = \left[\frac{m}{(n,m)}\right]_m$. Per tale funzione si ha $d\tilde{\varphi} = 0$ (l'elemento neutro di $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$) $\iff$ $d\tilde{\varphi}([1]_n) = [0]_m$ cioè $\iff$ $d\left[\frac{m}{(n,m)}\right]_m = [0]_m$ (ricordare che l'operazione in $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ è una "somma"). Quindi $o(\tilde{\varphi}) = (n, m)$ e $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ è un gruppo ciclico di ordine $(n, m) \Longrightarrow$ isomorfo a $\mathbb{Z}/(n, m)\mathbb{Z}$.

8. Sia $\varphi \in Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ tale che $\varphi([1]_n) = [h]_m$ con $o([h]_m) = d|(n, m)$. Trovare $x \in \mathbb{Z}$ tale che $\varphi = x\tilde{\varphi}$ (notazioni dell'esercizio precedente).

9. Sia $G =< a >$ un gruppo ciclico. Calcolare $Aut(G)$.
Dim. Prima consideriamo $o(G) = \infty$. Se $\varphi \in Aut(G)$ allora, dato che $Im\,\varphi$ è generata da $\varphi(a)$, è necessario che $\varphi(a)$ sia un generatore di G. Abbiamo già visto che in G ci sono solo 2 generatori a ed a^{-1}, dunque ci sono solo due automorfismi e $o(Aut(G)) = 2 \Longrightarrow Aut(G) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}^*$ (gli elementi di $\mathbb{Z}$ invertibili rispetto al prodotto).
Se $o(G) = n < \infty$ allora G ha $\phi(n)$ generatori che sono gli a^i con $0 < i < n$ e $(i, n) = 1$. Per ognuno di questi indici i sia allora $\varphi_i \in Aut(G)$ tale che $\varphi_i(a) = a^i$ e definiamo $f : Aut(G) \longrightarrow (\mathbb{Z}/n\mathbb{Z}^*)$ tramite la formula $f(\varphi_i) = i$. È facile verificare che f è un isomorfismo.

10. Sia $\mathscr{A}_n$ il sottogruppo delle permutazioni pari di S_n. Per calcolare $o(\mathscr{A}_n)$ si può considerale la mappa $f : S_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$ definita da

$$f(\sigma) = \begin{cases} 0 & \text{se } \sigma \in \mathscr{A}_n \\ 1 & \text{se } \sigma \notin \mathscr{A}_n \end{cases} .$$

È facile verificare che f è un omomorfismo surgettivo di nucleo $\mathscr{A}_n$, dunque, per il primo Teorema di omomorfismo, $S_n/\mathscr{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$ e infine

$$o(\mathscr{A}_n) = \frac{o(S_n)}{2} = \frac{n!}{2} .$$

11. Una delle ragioni per cui i gruppi di permutazioni tendono a comparire continuamente è il seguente

Teorema 1.3.15 (Cayley) *Sia G un gruppo e sia $S(G) = \{f : G \longrightarrow G\, t.c.\, f$ biunivoca$\}$ il gruppo delle permutazioni di G (per esempio se $o(G) = n < \infty$ allora $S(G) \simeq S_n$). Allora G è isomorfo ad un sottogruppo di $S(G)$.*

Dim. Definiamo $f : G \longrightarrow S(G)$ tramite la formula $f(a) = \tau_a$ dove $\tau_a(g) = ag$ per ogni $g \in G$. È facile verificare che, per ogni $a \in G$, $\tau_a \in S(G)$ (vd anche Proposizione 1.1.6).
Inoltre $f(ab) = \tau_{ab}$ e $\tau_{ab}(g) = (ab)g = a(bg) = \tau_a(bg) = \tau_a\tau_b(g)$, dunque $f(ab) = \tau_{ab} = \tau_a\tau_b = f(a)f(b)$ (ricordare che in $S(G)$ l'operazione è la composizione di funzioni) ed f è un omomorfismo.
Infine $a \in Ker\, f \iff f(a) = \tau_a = id$ cioè $\tau_a(g) = ag = id(g) = g$ per ogni $g \in G \iff a = e$ quindi f è iniettiva e, per il primo Teorema di omomorfismo,

$$G/Ker\, f = G \simeq Im\, f < S(G) . \quad \square$$

1.4 La formula delle classi

Definizione 1.4.1 Sia G un gruppo. Definiamo una relazione su G data da $a \sim b \iff \exists\, g \in G$ tale che $a = gbg^{-1}$. Tale relazione è detta *coniugio* e se $a \sim b$ si dice che a è *coniugato* a b.

Esercizio Verificare che il coniugio è una relazione di equivalenza.

Sia $[a] = \{b \in G \text{ } t.c. \text{ } a \sim b\}$ la classe di equivalenza di a (detta anche *classe di coniugio*), non è sempre facile individuarne gli elementi ma possiamo trovare una formula per $\#[a]$. Fatto questo, dato un sistema di rappresentanti R per $\sim$ in G, avremo $G = \bigcup_{a \in R} [a]$ (unione disgiunta) e quindi una formula per l'ordine di G

$$o(G) = \sum_{a \in R} \#[a] \ .$$

Teorema 1.4.2 *Sia G un gruppo finito e $\sim$ la relazione di coniugio. Sia $a \in G$, allora*

$$\#[a] = o(G)/o(C(a)) = [G : C(a)]$$

dove $C(a)$ è il centralizzante di a.

Dim. Definiamo $f : \{\text{Laterali sinistri di } C(a)\} \longrightarrow [a]$ tramite la formula $f(gC(a)) = gag^{-1}$. La funzione f è ben definita, infatti se $gC(a) = hC(a)$ allora $\exists\, k \in C(a)$ tale che $g = hk$ e dunque

$$f(gC(a)) = gag^{-1} = (hk)a(hk)^{-1} = hkak^{-1}h^{-1} = hah^{-1} = f(hC(a))$$

per la definizione di centralizzante.
Se $f(gC(a)) = f(hC(a))$ allora

$$gag^{-1} = hah^{-1} \Longrightarrow h^{-1}ga = ah^{-1}g$$

e dunque $h^{-1}g \in C(a)$, cioè $g \in hC(a)$. Di conseguenza $gC(a) = hC(a)$ ed f è iniettiva.
Infine se $b \in [a]$ allora $\exists\, g \in G$ tale che $b = gag^{-1}$ dunque $b = f(gC(a))$ ed f è surgettiva.
Quindi f biunivoca implica

$$\#[a] = \#\{\text{Laterali sinistri di } C(a)\} = [G : C(a)] \ . \quad \square$$

Corollario 1.4.3 (Formula delle classi: 1) *Sia R un sistema di rappresentanti per la relazione di coniugio su un gruppo finito G allora*

$$o(G) = \sum_{a \in R} o(G)/o(C(a)) = \sum_{a \in R} [G : C(a)] \ .$$

Dim. Ovvia. □

Corollario 1.4.4 (Formula delle classi: 2) *Sia R un sistema di rappresentanti per la relazione di coniugio su un gruppo finito G allora*

$$o(G) = o(Z(G)) + \sum_{a \in R - Z(G)} o(G)/o(C(a)) = o(Z(G)) + \sum_{a \in R - Z(G)} [G : C(a)] \ .$$

Dim. È sufficiente osservare che se $a \in Z(G)$ allora $C(a) = G$ e dunque $[a] = \{a\}$ ha un solo elemento. □

1.4.1 Applicazioni

Centro di un p-gruppo

Definizione 1.4.5 Sia p un primo. Un gruppo di ordine p^n (per qualche $n > 0$) si dice *p-gruppo.*

Proposizione 1.4.6 *Se G è un p-gruppo, il suo centro è non banale, cioè $Z(G) \neq \{e\}$.*

Dim. Per ogni $a \in R - Z(G)$ si ha $C(a) < G$ con $C(a) \neq G$, dunque $o(C(a)) = p^{n_a}$ per qualche $n_a < n$ (Teorema di Lagrange). Dalla seconda formula delle classi si ottiene

$$o(G) = p^n = o(Z(G)) + \sum_{a \in R - Z(G)} p^{n - n_a} \ .$$

Quindi

$$o(Z(G)) = p^n - \sum_{a \in R - Z(G)} p^{n - n_a}$$

è divisibile per p. □

Esercizio Sia p un primo. Dimostrare che un gruppo di ordine p^2 è abeliano.
Dim. Dato che $Z(G)$ è non banale deve essere $o(Z(G)) = p$ o p^2. Se

$o(Z(G)) = p^2$ allora G è abeliano, quindi supponiamo $o(Z(G)) = p$. Consideriamo $G/Z(G)$ che è ciclico perché ha ordine primo p. Siano $Z(G) =< a >$ e $G/Z(G) =< Z(G)b >$, allora ogni elemento di G è in una classe laterale di $Z(G)$ e quindi si può scrivere come $a^i b^j$ per qualche $1 \leq i, j \leq p$. Dunque siano $x = a^i b^j \, , y = a^k b^l \in G$, il prodotto è

$$xy = a^i b^j a^k b^l = b^j a^{i+k} b^l = b^{j+l} a^{i+k} = a^k b^{j+l} a^i = a^k b^l a^i b^j = yx$$

(dove si è usato ripetutamente il fatto che $a \in Z(G)$) ma allora G è abeliano il che contraddice $o(Z(G)) = p \Longrightarrow o(Z(G)) = p^2$ e G è abeliano. $\square$

Osservazione 1.4.7 La dimostrazione dell'esercizio precedente mostra che $G/Z(G)$ è ciclico se e solo se $Z(G) = G$ cioè se $G/Z(G)$ è banale. Dunque il gruppo degli automorfismi interni $Int(G)$ non è mai ciclico (a meno che non sia $= \{id\}$).

Teorema di Cauchy (1)

Teorema 1.4.8 (Teorema di Cauchy: 1) *Sia G un gruppo finito e p un primo che divide l'ordine di G. Allora $\exists\, a \in G$ tale che $o(a) = p$.*

Dim. Procediamo per induzione su $o(G)$. Per $o(G) = 1$ tutto è banale. Supponiamo il teorema vero per gruppi di ordine $< n$ e consideriamo un gruppo G di ordine n.
Se $\exists\, H < G$ tale che $H \neq G$ e $p | o(H)$ allora per induzione $\exists\, a \in H \subset G$ tale che $o(a) = p$ e abbiamo finito. Se invece p non divide l'ordine di nessun sottogruppo non banale di G allora $p \nmid o(C(a))$ per ogni $a \in G - Z(G)$ e questo implica che $p | [G : C(a)]$ per ogni $a \in G - Z(G)$. Dunque dalla seconda formula delle classi si ricava

$$p \Big| \left(o(G) - \sum_{a \in R - Z(G)} [G : C(a)] \right) = o(Z(G)) \; .$$

Quindi $Z(G)$ non è un sottogruppo proprio di G e l'unica possibilità è che sia $Z(G) = G$, cioè G è un gruppo abeliano.
La conclusione del teorema seguirà dal Teorema di struttura dei gruppi abeliani finiti (Teoremi 1.5.3 e 1.5.4). $\square$

Gruppi di permutazioni (3) - Coniugio

1. Sia $\sigma = (i_1 \ \dots \ i_k) \in S_n$ allora per ogni $\theta \in S_n$ si ha $\theta\sigma\theta^{-1} = (\theta(i_1) \ \dots \ \theta(i_k))$. Infatti

- se $l \notin \{\theta(i_1) \dots \theta(i_k)\}$ allora $\theta^{-1}(l) \notin \{i_1 \dots i_k\}$ dunque $\sigma\theta^{-1}(l) = \theta^{-1}(l)$ e $\theta\sigma\theta^{-1}(l) = \theta\theta^{-1}(l) = l$;
- invece per ogni $1 \leq j \leq k$ si ha

$$\theta\sigma\theta^{-1}(\theta(i_j)) = \theta\sigma(i_j) = \begin{cases} \theta(i_{j+1}) & \text{se } 1 \leq j \leq k-1 \\ \theta(i_1) & \text{se } j = k \end{cases} .$$

Dunque $\theta\sigma\theta^{-1}$ e $(\theta(i_1) \dots \theta(i_k))$ hanno lo stesso "effetto" su ogni indice $l \in \{1, \dots n\} \Longrightarrow$ sono uguali come elementi di S_n.

2. Siano $\sigma = (i_1 \ \dots \ i_k)$ e $\tau = (j_1 \ \dots \ j_k)$ due cicli di S_n della stessa lunghezza k. Allora $\exists\, \theta \in S_n$ tale che $\tau = \theta\sigma\theta^{-1}$. Infatti è sufficiente definire una funzione θ tale che $\theta(i_l) = j_l$ per ogni $1 \leq l \leq k$ e poi completare (a piacere) il resto della definizione di θ per ottenere (come visto in **1**) $\theta\sigma\theta^{-1} = \tau$.
Per esempio siano $\sigma = (1\,3\,5\,4\,8)$ e $\tau = (2\,5\,9\,4\,7)$ in S_9. Scrivendo θ in forma matriciale sappiamo che deve essere

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & & 5 & 4 & 9 & & & 7 & \end{pmatrix}$$

mentre il resto dell'immagine non ha vincoli (se non la biunivocità di θ). Due tra i possibili "completamenti" sono

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 5 & 4 & 9 & 3 & 6 & 7 & 8 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 5 & 4 & 9 & 8 & 6 & 7 & 1 \end{pmatrix} .$$

In forma ciclica sono $\theta_1 = (1\,2)(3\,5\,9\,8\,7\,6)(4)$ e $\theta_2 = (1\,2\,3\,5\,9)(4)(6\,8\,7)$. Verificare che in entrambi i casi si ha $\theta_1\sigma\theta_1^{-1} = \theta_2\sigma\theta_2^{-1} = \tau$.

Proposizione 1.4.9 *Due permutazioni in S_n sono coniugate se e solo se hanno la stessa struttura ciclica (cioè sono prodotto di cicli disgiunti della stessa lunghezza).*

Dim. Ogni permutazione è prodotto di cicli disgiunti (Proposizione 1.1.10), quindi due permutazioni sono coniugate se e solo se lo sono i loro cicli. Da **1** e **2** segue che due cicli sono coniugati se e solo se hanno la stessa lunghezza. □

3. Sia $\sigma = (1\,2\,3) \in S_6$. Trovare $C(\sigma) < S_6$ (dove $C(\sigma)$ è il centralizzante di σ).
Dim. Abbiamo vsto che $o(C(\sigma)) = \frac{o(S_6)}{\#[\sigma]}$ dove $[\sigma]$ è la classe di coniugio di σ. Sappiamo che σ è coniugato a tutti e soli i 3-cicli di S_6 che sono $\binom{6}{3}2! = 40$: il calcolo segue dal prendere tutti i sottoinsieme di 3 elementi in un insieme di 6 elementi (sono $\binom{6}{3}$) e poi considerare quanti 3-cicli si possono ottenere con 3 elementi (sono 2!, osserviamo che in generale con un insieme di k elementi si possono scrivere $(k-1)!$ cicli di lunghezza k). Dunque $o(C(\sigma)) = \frac{6!}{40} = 18$. Trovato l'ordine cominciamo a cercarne gli elementi: ci sono 3! permutazioni in S_6 che lasciano fissi 1, 2 e 3 e queste sicuramente commutano con σ. Inoltre σ commuta con le sue potenze id, σ e σ^2. Combinando questi elementi si ottengono già $3! \cdot 3 = 18$ permutazioni con cui σ commuta $\Longrightarrow$ abbiamo trovato tutti gli elementi di $C(\sigma)$.

4. Sia $\sigma = (1\,4\,2\,9)(5\,8\,3) \in S_9$. Trovare $C(\sigma) < S_9$.
Dim. Procediamo come nel precedente esercizio. In S_9 ci sono $\binom{9}{4}3!\binom{5}{3}2! = 15120$ elementi con la stessa struttura ciclica di σ (calcolo: (numero di 4-cicli possibili con 9 elementi)(numero di 3-cicli possibili con i 5 elementi rimasti)). Dunque $o(C(\sigma)) = \frac{9!}{15120} = 24$.
Ci sono 2 permutazioni in S_9 che non agiscono sugli indici presenti nei cicli (non banali) di σ e quindi commutano con σ. Inoltre σ ha ordine 12 (il minimo comune multiplo tra gli ordini dei cicli disgiunti che lo compongono), dunque commuta con le sue 12 potenze. Abbiamo così già trovato tutti i $12 \cdot 2 = 24$ elementi di $C(\sigma)$.

5. Sia $\sigma = (1\,2)(3\,4) \in S_6$. Trovare $C(\sigma) < S_6$.
Dim. Procediamo come nei precedenti esercizi. In S_6 ci sono $\binom{6}{2}\binom{4}{2}\frac{1}{2} = 45$ elementi con la stessa struttura ciclica di σ (calcolo: (numero di 2-cicli possibili con 6 elementi)(numero di 2-cicli possibili con i 4 elementi rimasti) diviso 2 perché in questo modo abbiamo considerato due volte le permutazioni $(i_1\,i_2)(j_1\,j_2)$, una volta nella scrittura data ed una volta come $(j_1\,j_2)(i_1\,i_2)$). Dunque $o(C(\sigma)) = \frac{6!}{45} = 16$.
La permutazione σ commuta con le sue potenze (sono 2), con le permutazioni che non agiscono su 1, 2, 3 e 4 (sono 2), con $(1\,2)$, con $(3\,4)$ ed infine con $(1\,3)(2\,4)$. Dai prodotti tra questi elementi si ricavano tutti i 16 elementi di $C(\sigma)$.

1.5 Gruppi abeliani finiti

Enunciamo prima di tutto un'importante Teorema che useremo in seguito senza darne la dimostrazione (vd per esempio [1] sezione 2.12).

Teorema 1.5.1 (Sylow) *Sia G un gruppo finito e sia p un numero primo tale che $p^n \parallel o(G)$ (cioè $p^n | o(G)$ e $p^{n+1} \nmid o(G)$). Allora $\exists P < G$ con $o(P) = p^n$, un tale sottogruppo si definisce* p-sottogruppo di Sylow *di G.*

Abbiamo già visto la costruzione del prodotto diretto "dall'esterno", cioè dati due gruppi G_1 e G_2, abbiamo definito il prodotto diretto $G_1 \times G_2$. È importante sapere quando tale costruzione può essere fatta "dall'interno" cioè quando, dato un gruppo G, esistono due (o più) sottogruppi H e K di G tali che $G \simeq H \times K$.

Proposizione 1.5.2 *Sia G un gruppo e siano $H, K \lhd G$ tali che:*

1. $H \bigcap K = \{e\}$;
2. $HK = G$ *cioè, per ogni $g \in G$, $\exists\, h \in H$ ed $\exists\, k \in K$ tali che $g = hk$.*

Allora $G \simeq H \times K$.

Dim. Prima dimostriamo che per ogni $h \in H$ e $k \in K$ si ha $hk = kh$. Infatti

$$hkh^{-1}k^{-1} = \begin{cases} (hkh^{-1})k^{-1} \in K & \text{dato che } K \lhd G \\ h(kh^{-1}k^{-1}) \in H & \text{dato che } H \lhd G \end{cases} .$$

Dunque $hkh^{-1}k^{-1} \in H \bigcap K$, cioè $hkh^{-1}k^{-1} = e \Longrightarrow hk = kh$.
Sia $f : H \times K \longrightarrow G$ data da $f(h,k) = hk$ che è surgettiva per l'ipotesi **2**.
Si ha

$$f((h_1,k_1)(h_2,k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 =$$

$$= h_1k_1h_2k_2 = f(h_1,k_1)f(h_2,k_2) ,$$

dunque f è un omomorfismo.
Infine $f(h,k) = e \iff hk = e \iff h = k^{-1}$, dunque $h = k^{-1} \in H \bigcap K = \{e\}$ e $(h,k) = (e,e)$ l'elemento neutro di $H \times K$. Quindi f è anche iniettiva ed è l'isomorfismo richiesto. □

Esercizi

1. Siano H e K sottogruppi di un gruppo G. Dimostrare che se $H \bigcap K = \{e\}$ allora $o(HK) = o(H)o(K)$.

2. Generalizzare la Proposizione 1.5.2 dimostrando che:
se G è un gruppo e $H_1, \ldots, H_n$ sono sottogruppi normali di G tali che:

a) $H_i \bigcap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$ per ogni $1 \leq i \leq n$;

b) $H_1 \cdots H_n = G$.

Allora $G \simeq H_1 \times \cdots \times H_n$.

Teorema 1.5.3 (Struttura dei gruppi abeliani: 1) *Sia G un gruppo abeliano finito di ordine $n = \prod_{i=1}^{k} p_i^{n_i}$ (dove i p_i sono primi distinti) e, per ogni i, sia P_i un sottogruppo di Sylow di G relativo al primo p_i . Allora $G \simeq P_1 \times \cdots \times P_k$.*

Dim. Dato che G è abeliano tutti i sottogruppi sono normali.
Sia $a \in P_i \bigcap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_k)$, allora $o(a) | o(P_i) = p_i^{n_i}$ e

$$o(a) | o(P_1 \cdots P_{i-1} P_{i+1} \cdots P_k) = \text{(vd esercizio 1 sopra)} =$$

$$= o(P_1) \cdots o(P_{i-1}) o(P_{i+1}) \cdots o(P_k) = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} \ .$$

Dato che tali ordini sono relativamente primi tra loro deve essere $o(a) = 1$ cioè $a = e$.
Infine, dato che le intersezioni sono banali, $o(P_1 \cdots P_k) = o(P_1) \cdots o(P_k) = o(G)$ e dunque $P_1 \cdots P_k = G$. Il teorema segue dalla generalizzazione della Proposizione 1.5.2. $\square$

NOTA La dimostrazione precedente manca di dettagli (anche importanti, per esempio sul calcolo degli ordini dei prodotti di sottogruppi), ma in questa sede volevamo solo dare le linee guida del ragionamento. Quello che manca sono dettagli tecnici, non "idee".

Per concludere dobbiamo solo descrivere la struttura dei p-gruppi (come sono i gruppi di Sylow).

Teorema 1.5.4 (Struttura dei gruppi abeliani: 2) *Sia G un p-gruppo abeliano di ordine p^n allora sono univocamente determinati degli interi positivi $a_1, \ldots, a_k$ tali che:*

1. $a_1 + \cdots + a_k = n$;

2. $G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$.

Dim. Vd Herstein sezione 2.14 (molto tecnica). □

Possiamo adesso concludere il seguente

Teorema 1.5.5 (Teorema di Cauchy: 2) *Sia G un gruppo abeliano finito e sia p un numero primo tale che $p|o(G)$. Allora $\exists a \in G$ tale che $o(a) = p$.*

Dim. Per il Teorema di struttura G è isomorfo ad un prodotto diretto di gruppi ciclici e l'ordine di almeno uno di questi è divisibile per p. Abbiamo già visto che in un gruppo ciclico esistono elementi di ordine d per ogni d divisore dell'ordine del gruppo. □

Applicazioni - Esercizi

1. Siano $m, n \in \mathbb{Z}$ tali che $(m, n) = 1$. Dimostrare che $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$.

2. Scriviamo, a meno di isomorfismi, tutti i gruppi abeliani di ordine 900.
La fattorizzazione di 900 è $2^2 \cdot 3^2 \cdot 5^2$ dunque se G è un gruppo abeliano di ordine 900 si ha $G \simeq P_2 \times P_3 \times P_5$ dove ogni P_p è un p-Sylow di G. Per un primo p

$$o(P_p) = p^2 \Longrightarrow P_p \simeq \begin{cases} \mathbb{Z}/p^2\mathbb{Z} \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \end{cases} .$$

Dunque le possibili combinazioni con i sottogruppi di Sylow di G sono:

$$G \simeq \begin{cases} \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{cases} .$$

3. Per ognuno dei gruppi del punto **2** calcolare il numero di elementi di ordine d per ogni d divisore di 900.
Lo facciamo esplicitamente solo per $G \simeq \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$, gli altri sono simili una volta capito il metodo da seguire. L'ordine di un elemento $([\alpha]_4, [\beta]_3, [\gamma]_3, [\delta]_{25}) \in G$ è il minimo comune multiplo degli ordini delle singole coordinate, dunque per ottenere, per esempio, un elemento di ordine 60, abbiamo bisogno di un elemento di ordine 4 in $\mathbb{Z}/2^2\mathbb{Z}$ (ce ne sono

$\phi(4) = 2$), un elemento di ordine 3 in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (che si può ottenere in vari modi: un elemento di ordine 3 ed uno di ordine 1 e sono $\phi(3)\phi(1) = 2$, un elemento di ordine 1 ed uno di ordine 3 e sono $\phi(1)\phi(3) = 2$ oppure un elemento di ordine 3 ed uno di ordine 3 e sono $\phi(3)\phi(3) = 4$) ed un elemento di ordine 5 in $\mathbb{Z}/5^2\mathbb{Z}$ (ce ne sono $\phi(5) = 4$). Quindi ci sono $2(2+2+4)4 = 64$ elementi di ordine 60 in G. Ecco la tabella complessiva:

Ordine	In $\mathbb{Z}/2^2\mathbb{Z}$	In $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	In $\mathbb{Z}/5^2\mathbb{Z}$	Totale
1	1	1	1	1
2	$\phi(2)$	1	1	1
3	1	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	1	8
4	$\phi(4)$	1	1	2
5	1	1	$\phi(5)$	4
6	$\phi(2)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	1	8
9	1	0	1	0
10	$\phi(2)$	1	$\phi(5)$	4
12	$\phi(4)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	1	16
15	1	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	$\phi(5)$	32
18	$\phi(2)$	0	1	0
20	$\phi(4)$	1	$\phi(5)$	8
25	1	1	$\phi(25)$	20
30	$\phi(2)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	$\phi(5)$	32
36	$\phi(4)$	0	1	0
45	1	0	$\phi(5)$	0
50	$\phi(2)$	1	$\phi(25)$	20
60	$\phi(4)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	$\phi(5)$	64
75	1	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	$\phi(25)$	160
90	$\phi(2)$	0	$\phi(5)$	0
100	$\phi(4)$	1	$\phi(25)$	40
150	$\phi(2)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	$\phi(25)$	160
180	$\phi(4)$	0	$\phi(25)$	0
225	1	0	$\phi(25)$	0
300	$\phi(4)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	$\phi(25)$	320
450	$\phi(2)$	0	$\phi(25)$	0
900	$\phi(4)$	0	$\phi(25)$	0
				Tot. 900

4. Scriviamo, a meno di isomorfismi, tutti i gruppi abeliani di ordine $6p^2$ con p primo.
Se $p \neq 2, 3$ allora abbiamo 3 distinti Sylow P_2, P_3 e P_p. I gruppi possibili

sono

$$G \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} & G_1 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & G_2 \end{cases} .$$

Se $p = 2$ il gruppo ha ordine 24 ed ha due Sylow P_2 e P_3. Si ottengono

$$G \simeq \begin{cases} \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & G_3 \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & G_4 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & G_5 \end{cases} .$$

Se $p = 3$ il gruppo ha ordine 54 ed ha due Sylow P_2 e P_3. Si ottengono

$$G \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} & G_6 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & G_7 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & G_8 \end{cases} .$$

5. In ognuno dei gruppi del punto **4** vogliamo contare il numero di elementi di ordine 6.

Gruppo	Ordine 2	Ordine 3	Totale
G_1	$\phi(2)$	$\phi(3)$	2
G_2	$\phi(2)$	$\phi(3)$	2
G_3	$\phi(2)$	$\phi(3)$	2
G_4	$\phi(2) + \phi(2) + \phi(2)\phi(2)$	$\phi(3)$	6
G_5	$3\phi(2) + 3\phi(2)\phi(2) + \phi(2)^3$	$\phi(3)$	14
G_6	$\phi(2)$	$\phi(3)$	2
G_7	$\phi(2)$	$\phi(3) + \phi(3) + \phi(3)\phi(3)$	8
G_8	$\phi(2)$	$3\phi(3) + 3\phi(3)\phi(3) + \phi(3)^3$	26

6. Scrivere esplicitamente gli elementi di ordine 6 dei gruppi del punto **4**.

7. *Teorema di Sylow per gruppi abeliani.* Sia G un gruppo abeliano finito e sia p un primo tale che $p^n \parallel o(G)$. Dimostrare che $\exists\, P < G$ tale che $o(P) = p^n$.
Dim. Sia $P = \{a \in G : \exists\, k \in \mathbb{Z} - \{0\} \text{ con } a^{p^k} = e\}$. È facile verificare che P è un sottogruppo di G, vediamo quale è il suo ordine. Se un primo $q \neq p$ divide l'ordine di P allora $\exists\, b \in P$ tale che $o(b) = q$ (Teorema di Cauchy 1.4.8 e 1.5.5). Per definizione $b \in P \Longrightarrow \exists\, k$ tale che $b^{p^k} = e$. Dato che $(p, q) = 1$ l'identità di Bezout fornisce $x, y \in \mathbb{Z}$ tali che $xp^k + yq = 1$, dunque $b = b^{xp^k+yq} = (b^{p^k})^x (b^q)^y = e$ il che contraddice $o(b) = q$. Dunque l'ordine di P deve essere una potenza di p ed è quindi $\leq p^n$. Se $o(P) = p^m$ con $m < n$ allora p divide l'ordine di $G/P \Longrightarrow$ (ancora il Teorema di Cauchy) $\exists\, Pa \in G/P$ tale che $o(Pa) = p$. Quindi $(Pa)^p = Pa^p = P$ l'elemento neutro di G/P, cioè $a^p \in P$ e, per definizione di P, $\exists\, k$ tale che $(a^p)^{p^k} = a^{p^{k+1}} = e$.

Ma allora $a \in P$ e $Pa = P$ che contraddice $o(Pa) = p$. Dunque $o(P) = p^n$ ed è il sottogruppo di Sylow cercato.

1.6 Esercizi di riepilogo

1. Sia G un gruppo di ordine p^3 con p primo. Dimostrare che se G non è abeliano allora $o(Z(G)) = p$.

2. Sia G un gruppo e sia $D = \{ (a, a) \in G \times G : a \in G \}$.

a) Dimostrare che $D < G \times G$.

b) Dimostrare (con un esempio) che, in generale, D non è un sottogruppo normale di $G \times G$.

c) Sia G abeliano. Dimostrare che $(G \times G)/D \simeq G$.

3. Dire quali tra le seguenti mappe sono omomorfismi di gruppi.

a) $Tr : \mathscr{M}(n, \mathbb{R}) \longrightarrow \mathbb{R}$ la traccia (cioè la somma degli elementi della diagonale della matrice).

b) $Tr : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}$ la traccia.

c) $\det : \mathscr{M}(n, \mathbb{R}) \longrightarrow \mathbb{R}$ il determinante.

d) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ il determinante.

e) $f : \mathscr{M}(n, \mathbb{R}) \times \mathscr{M}(n, \mathbb{R}) \longrightarrow \mathscr{M}(n, \mathbb{R})$ data da $f(A, B) = A - B$.

f) $f : GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow \mathscr{M}(n, \mathbb{R})$ data da $f(A, B) = A - B$.

g) $f : GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$ data da $f(A, B) = AB^{-1}$.

4. Siano H e K sottogruppi normali di un gruppo G.

a) Dimostrare che $H \bigcap K \lhd G$.

b) Dimostrare che $G/(H \bigcap K)$ è isomorfo ad un sottogruppo di $G/H \times G/K$.

c) Dimostrare (con un esempio) che, in generale, $G/(H \bigcap K)$ non è isomorfo a $G/H \times G/K$.

d) Sia $G = \mathbb{Z}/18\mathbb{Z}$ e siano $H =< 3 >$, $K =< 2 >$. Definire un isomorfismo $G/(H \bigcap K) \longrightarrow G/H \times G/K$.

5. Dimostrare che $Aut(S_3) \simeq S_3$.

6. Sia G un gruppo tale che per ogni $a \in G$ si ha $a^2 = e$ (e è l'elemento neutro di G). Dimostrare che G è abeliano. Se G è finito che forma può avere (a meno di isomorfismi) ?

7. Sia G un gruppo ed H un sottogruppo di G. Definiamo

$$K = \bigcap_{a \in G} aHa^{-1} \ .$$

Dimostrare che $K \lhd G$.

8. Siano G_1 e G_2 due gruppi. Dimostrare che $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

9. Sia G un gruppo di ordine 6. Dimostrare che G o è ciclico o è isomorfo ad S_3 .

10. Sia $\sigma = (5\ 2\ 9\ 1\ 3)(6\ 4) \in S_9$.

a) Trovare $\theta \in S_9$ tale che $\theta\sigma\theta^{-1} = (1\ 6\ 8\ 7\ 2)(5\ 9)$.

b) Trovare tutti gli elementi di S_9 che commutano con σ (cioè trovare $C(\sigma)$).

11. Consideriamo gruppi abeliani di ordine 200.

a) Scrivere (a meno di isomorfismi) tutti i gruppi abeliani di ordine 200.

b) Per ognuno dei gruppi del punto **a)** e per ogni d divisore di 200 calcolare il numero degli elementi di ordine d.

12. Trovare l'ordine di ogni elemento di $(\mathbb{Z}/7\mathbb{Z})^* \times S_3$.

13. Sia $H = \{\, M \in GL_2(\mathbb{Z}/7\mathbb{Z}) \,:\, \det M = 2 \text{ o } \det M = 4 \text{ o } \det M = 1 \,\}$.

a) Dimostrare che $H \lhd GL_2(\mathbb{Z}/7\mathbb{Z})$.

b) Dimostrare che $GL_2(\mathbb{Z}/7\mathbb{Z})/H \simeq \mathbb{Z}/2\mathbb{Z}$ e calcolare $o(H)$.

N.B. Negli esercizi **10, 11, 12** i dati numerici sono poco rilevanti. Potete sostituire 200, σ, S_9 , ecc... con altri interi (altre permutazioni ed altri S_n) per ottenere infinite variazioni del medesimo esercizio.

Capitolo 2

Anelli e Campi

2.1 Definizione ed esempi

Per descrivere la struttura di anello su un insieme E si richiedono due operazioni che, in generale, indicheremo con $+$ e $\cdot$ per non appesantire le notazioni, e alcune proprietà che le riguardano. Sempre per semplicità le operazioni verranno spesso chiamate *somma* e *prodotto* ed i rispettivi elementi neutri (se esistono) si indicheranno con 0 e 1.

Definizione 2.1.1 Una quaterna $(E, +, \cdot, 0)$ insieme - 1^a operazione - 2^a operazione - elemento neutro per la 1^a operazione, si dice *anello* se

1. $(E, +, 0)$ è un gruppo commutativo;
2. $\cdot$ (la 2^a operazione) è associativa;
3. $\forall\, a, b, c \in E$ si ha $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ cioè valgono le due simmetriche *leggi distributive*.

Notazione Come fatto per i gruppi, scriveremo sempre ab invece di $a \cdot b$.

Se la 2^a operazione verifica altre proprietà aggiuntive si definiscono particolari tipi di anelli.

Definizione 2.1.2 Sia $(E, +, \cdot, 0)$ un anello:

1. se $\cdot$ è commutativa, E si dice *anello commutativo*;

2. se $\exists 1 \in E$ elemento neutro per $\cdot$, E si dice *anello con unità*;

3. se $(E - \{0\}, \cdot, 1)$ è un gruppo, E si dice *corpo*;

4. se $(E - \{0\}, \cdot, 1)$ è un gruppo abeliano, E si dice *corpo commutativo* o *campo*.

Esempi - Esercizi

1. $\mathbb{Z}$ è un anello, mentre $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono campi.

2. Dimostrare che $\mathbb{Z}/n\mathbb{Z}$ è un anello per ogni $n \geq 1$ e che $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è primo.

3. $\mathscr{M}(n \times n, \mathbb{R})$ e $\mathscr{M}(n \times n, \mathbb{Z}/p\mathbb{Z})$ (con p primo) sono entrambi anelli rispetto alla somma ed al prodotto righe per colonne tra matrici. Entrambi hanno come unità la matrice identità I.

4. Sia X un insieme e sia $\mathcal{M}(X, \mathbb{R}) = \{f : X \longrightarrow \mathbb{R}\}$. Definiamo due operazioni su $\mathcal{M}(X, \mathbb{R})$ nel modo seguente:

$$+ : (f + g)(x) = f(x) + g(x), \, \forall\, x \in X \text{ e } \forall\, f, g \in \mathcal{M}(X, \mathbb{R});$$
$$\cdot : (f \cdot g)(x) = f(x)g(x), \, \forall\, x \in X \text{ e } \forall\, f, g \in \mathcal{M}(X, \mathbb{R})$$

(a destra abbiamo le operazioni in $\mathbb{R}$). Verificare che, con tali operazioni, $\mathcal{M}(X, \mathbb{R})$ è un anello commutativo con unità. Gli elementi invertibili rispetto a $\cdot$ sono le funzioni f tali che $f(x) \neq 0$, $\forall\, x \in X$.

5. Definizioni e dimostrazioni analoghe a quelle del punto **4** valgono per $\mathcal{M}(X, A)$ dove A è un qualsiasi anello. Dimostrare che $\mathcal{M}(X, A)$ "eredita" le proprietà di A cioè:
i) $\mathcal{M}(X, A)$ è commutativo se e solo se A lo è;
ii) $\mathcal{M}(X, A)$ ha unità (quale ?) se e solo se A ce l'ha.
Se A ha unità, quali sono gli elementi invertibili rispetto al prodotto di $\mathcal{M}(X, A)$?

Per definizione ogni anello è un gruppo abeliano rispetto alla somma, le distinzioni dipendono dalle proprietà del prodotto. Quindi invece di ripetere continuamente a quale operazione ci stiamo riferendo diamo la seguente

Definizione 2.1.3 Sia A un anello con unità. Un elemento $a \in A$ si dice *invertibile* se è invertibile rispetto al prodotto. L'insieme degli elementi invertibili di A si denota con A^*.

Lemma 2.1.4 *Sia A un anello con unità.*

1. $0 \notin A^*$;
2. $(A^*, \cdot, 1)$ *è un gruppo.*

Dim. **1.** Per ogni $a \in A$, $0a = (0+0)a = 0a + 0a$ e, sottraendo a destra ed a sinistra $0a$, si ottiene $0a = 0$. Dunque non esiste $b \in A$ tale che $0b = 1$.
2. Esercizio. $\square$

Esempi

1. $2\mathbb{Z}$ è un anello senza elemento unità quindi non ha senso parlare di invertibili in $2\mathbb{Z}$. In $\mathbb{Z}$ si ha $\mathbb{Z}^* = \{1, -1\}$.
2. Gli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$ sono tutte e sole le classi resto i cui rappresentanti sono primi con n.
3. Un anello commutativo con unità è un campo $\iff A^* = A - \{0\}$.

Definizione 2.1.5 Sia A un anello. Un elemento $a \in A - \{0\}$ si dice *divisore di zero* se $\exists\, b \in A - \{0\}$ tale che $ab = 0$. L'insieme dei divisori di zero di A si denota con $Div_0(A)$.
Un anello commutativo con unità si dice *dominio di integrità* (o semplicemente *dominio*) se non ha divisori di zero.

Esempio $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ sono domini di integrità mentre $\mathbb{Z}/n\mathbb{Z}$ è un dominio se e solo se n è primo.

Lemma 2.1.6 *Sia A un anello.*

1. $\forall\, a \in A$, $0a = a0 = 0$;
2. $\forall\, a, b \in A$, $a(-b) = (-a)b = -(ab)$;
3. $\forall\, a, b \in A$, $(-a)(-b) = ab$;
4. *se A ha unità,* $\forall\, a \in A$, $(-1)a = a(-1) = -a$;
5. *se A ha unità,* $(-1)(-1) = 1$;
6. *se A ha unità,* $Div_0(A) \bigcap A^* = \emptyset$.

Dim. **1.** Già visto.
2. $a(-b) + ab = a(-b + b) = a0 = 0 \Longrightarrow a(-b) = -(ab)$. Analoga dimostrazione per $(-a)b$.
3. $(-a)(-b) - (ab) = (-a)(-b) + a(-b) = (-a + a)(-b) = 0b = 0 \Longrightarrow (-a)(-b) = ab$.
4. Caso particolare di **2**.
5. Caso particolare di **4** con $a = -1$.
6. Sia $a \in Div_0(A) \bigcap A^*$ allora $\exists\, b \in A - \{0\}$ tale che $ab = 0$ ed $\exists\, c \in A$ tale che $ac = ca = 1$. Dunque $ab = 0 \Longrightarrow 0 = c0 = c(ab) = (ca)b = 1b = b$: contraddizione a $b \neq 0$, quindi $Div_0(A) \bigcap A^* = \emptyset$. $\square$

Proposizione 2.1.7 *Sia A un dominio di integrità. Se A è finito allora è un campo.*

Dim. Bisogna solo dimostrare che $a \in A - \{0\} \Longrightarrow a$ invertibile. Siano $a_1, \ldots, a_n$ gli elementi di A e consideriamo gli elementi $aa_1, \ldots, aa_n$. Tali elementi sono distinti perché $aa_i = aa_j \Longrightarrow a(a_i - a_j) = 0$, quindi $a \neq 0$ ed A dominio $\Longrightarrow a_i = a_j$. Dunque $A = \{aa_1, \ldots, aa_n\} \Longrightarrow \exists\, i$ tale che $aa_i = 1$ ed a è invertibile. $\square$

Esercizio È possibile dimostrare la Proposizione precedente considerando invece degli $aa_1, \ldots, aa_n$, solo le potenze a^i, $i \in \mathbb{N}$?

Osservazione 2.1.8 La legge di cancellazione vale in un anello A per la somma (ovvio), ma non vale in generale per il prodotto. Per esempio in $\mathbb{Z}/6\mathbb{Z}$ si ha $[2]_6[4]_6 = [2]_6$ ma $[4]_6 \neq [1]_6$. La condizione necessaria per far valere la legge di cancellazione per il prodotto è l'assenza di divisori di zero. Infatti in questo caso $a \neq 0$ e $ab = ac \Longrightarrow a(b - c) = 0 \Longrightarrow b - c = 0$ e $b = c$. La presenza di divisori di zero può causare anche altri fenomeni contrari "all'esperienza matematica comune" (qualsiasi cosa questo voglia dire visto che per molti significa fare le somme in $\mathbb{N}$ e poco più). Per esempio quante radici ha $X^2 - 1$ in $\mathbb{Z}/8\mathbb{Z}$?

Definizione 2.1.9 Sia A un dominio di integrità. La *caratteristica* di A è il minimo intero positivo p tale che $pa = a + \cdots + a = 0$, $\forall\, a \in A$. Se un tale intero non esiste allora si dice che A ha *caratteristica* 0. La caratteristica di A si indicherà con $char(A)$.

Esempi - Esercizi

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ hanno caratteristica 0, mentre $\mathbb{Z}/p\mathbb{Z}$ ha caratteristica p per ogni primo p.

2. Sia $M \in \mathscr{M}(n \times n, \mathbb{Z}/p\mathbb{Z})$ allora $pM = 0$. Sia $f \in \mathcal{M}(X, \mathbb{Z}/p\mathbb{Z})$ allora $(pf)(x) = p(f(x)) = 0$. Questi due anelli però non sono, in generale, domini di integrità (dimostrare che $\mathscr{M}(n \times n, \mathbb{Z}/p\mathbb{Z})$ è un dominio $\iff n = 1$ e che $\mathcal{M}(X, \mathbb{Z}/p\mathbb{Z})$ è un dominio $\iff \#X = 1$). Dunque per loro non si parla di caratteristica.

3. Dimostrare che un dominio di integrità finito A (cioè un campo finito) ha caratteristica > 0.
Dim. Sia $p = o(1)$ l'ordine dell'unità nel gruppo additivo A. Allora $0 = 1 + \cdots + 1$ (p volte) $\Longrightarrow \forall\, a \in A$, $pa = a + \cdots + a = a(1 + \cdots + 1) = a0 = 0$.

4. Sia A un dominio di caratteristica $n > 0$. Dimostrare che n deve essere un numero primo.
Dim. Sugg. se n non è primo si trovano dei divisori di zero.

Come corollario dell'esercizio **3** abbiamo

Corollario 2.1.10 *Sia A un dominio di integrità. Se $char(A) = 0$ allora A è infinito.*

2.1.1 Esempi principali

Polinomi e serie formali

Definizione 2.1.11 Sia A un anello. Definiamo l'*anello dei polinomi* a coefficienti in A come

$$A[X] = \left\{ \sum_{n \geq 0} a_n X^n \text{ } t.c. \text{ } a_n \in A \text{ e } a_n = 0 \text{ per quasi ogni } n \right\}$$

e l'*anello delle serie formali* a coefficienti in A come

$$A[[X]] = \left\{ \sum_{n \geq 0} a_n X^n \text{ } t.c. \text{ } a_n \in A \right\} .$$

Il *grado* di un polinomio $P = \sum_{n \geq 0} a_n X^n$, che si indica con $\deg P$, è definito da $\deg P = \max\{n \in \mathbb{N} : a_n \neq 0\}$ se $P \neq 0$ e, per convenzione, $\deg 0 = -\infty$.

Le operazioni che forniscono la struttura di anello sono le stesse per entrambi gli insiemi e sono le usuali somma e prodotto tra polinomi (e serie):

$$\sum_{n\geq 0} a_n X^n + \sum_{n\geq 0} b_n X^n = \sum_{n\geq 0} (a_n + b_n) X^n$$

$$\sum_{n\geq 0} a_n X^n \cdot \sum_{n\geq 0} b_n X^n = \sum_{n\geq 0} \left(\sum_{h+k=n} a_h b_k \right) X^n$$

(notare come X sia solo un segno formale e non abbia nessuna influenza sulle definizioni).

Molte delle proprietà di A vengono trasmesse agli anelli dei polinomi e delle serie come si vedrà risolvendo la seguente serie di esercizi.

Esempi - Esercizi

1. Dimostrare che $A[X]$ e $A[[X]]$ sono anelli.

2. Dimostrare che $A[X]$ e $A[[X]]$ sono commutativi se e solo se A lo è. Dimostrare che $A[X]$ e $A[[X]]$ hanno unità se e solo se A ce l'ha.

3. Dimostrare che $A[X]$ e $A[[X]]$ sono domini di integrità se e solo se A lo è .

4. Dimostrare che $\mathbb{Z}[X]^* = \mathbb{Z}^* = \{1, -1\}$. Dimostrare che $\mathbb{R}[X]^* = \mathbb{R}^*$.

5. Non è sempre vero che $A[X]^* = A^*$. La dimostrazione dell'esercizio **4** si basa (probabilmente, se avete trovato altre strade prendetelo come un tardivo suggerimento) sulla formula $\deg PQ = \deg P + \deg Q$. Tale formula non vale in generale, per esempio in $\mathbb{Z}/4\mathbb{Z}$ si ha $(2X+1)^2 = 1$, dunque $2X + 1 \in \mathbb{Z}/4\mathbb{Z}[X]^*$. Ancora una volta i divisori di zero sono responsabili di queste "stranezze", infatti si può dimostrare che se A è un dominio di integrità allora $\forall\, P, Q \in A[X]$ si ha $\deg PQ = \deg P + \deg Q$.

6. È invece abbastanza facile individuare gli elementi invertibili tra le serie formali.
Sia A un anello commutativo con unità. Dimostrare che

$$A[[X]]^* = \left\{ \sum_{n\geq 0} a_n X^n \ t.c.\ a_0 \in A^* \right\} .$$

Dim. Sia $a_0 \in A^*$ e sia $\sum_{n\geq 0} a_n X^n \in A[[X]]$, vogliamo risolvere

$$\sum_{n\geq 0} a_n X^n \cdot \sum_{n\geq 0} b_n X^n = \sum_{n\geq 0} \left(\sum_{h+k=n} a_h b_k \right) X^n = 1$$

per trovare la serie $\sum_{n\geq 0} b_n X^n$ inversa di $\sum_{n\geq 0} a_n X^n$.
Controllando i coefficienti si ottiene la seguente tabella

Grado	Equazione coeff.	Serie inversa
0	$a_0 b_0 = 1$	$b_0 = a_0^{-1}$
1	$a_0 b_1 + a_1 b_0 = 0$	$b_1 = -a_1 b_0 a_0^{-1}$
2	$a_0 b_2 + a_1 b_1 + a_0 b_2 = 0$	$b_2 = (-a_2 b_0 - a_1 b_1) a_0^{-1}$
$\vdots$	$\vdots$	$\vdots$
n	$a_0 b_n + \cdots + a_n b_0 = 0$	$b_n = (-a_n b_0 - \cdots - a_1 b_{n-1}) a_0^{-1}$

e si possono risolvere progressivamente tutte le equazioni per trovare i coefficienti b_n dell'inverso della serie data.

7. Per esempio, in $\mathbb{Z}[[X]]$, $1 - X$ è invertibile infatti

$$(1 - X) \sum_{n\geq 0} X^n = \sum_{n\geq 0} X^n - \sum_{n\geq 0} X^{n+1} = 1 \ .$$

Endomorfismi di un gruppo

Sia $(G, *, e)$ un gruppo abeliano, definiamo l'*anello degli endomorfismi* di G l'insieme $Hom(G, G) = \{f : G \longrightarrow G \ t.c. \ f$ omomorfismo$\}$ con le seguenti operazioni:

$(f+g)(a) = f(a) * g(a)$ e $(f \circ g)(a) = f(g(a)) \ \forall\, a \in G$ e $\forall\, f, g \in Hom(G, G)$.

Con queste operazioni $Hom(G, G)$ è un anello che si denota con $End(G)$, ha unità $1 = id$ (perchè il "prodotto" è la composizione di funzioni) ed inoltre $End(G)^* = Aut(G)$. Tutte queste sono facili verifiche.
Se $(A, +, \cdot, 0)$ è un anello, eliminando la restrizione agli omomorfismi, possiamo considerare l'insieme $\mathcal{M}(A, A) = \{f : A \longrightarrow A\}$. Su $\mathcal{M}(A, A)$ abbiamo adesso due diverse strutture di anello:

- $(\mathcal{M}(A, A), +, \circ, f_0)$ dove $f_0(a) = 0$ per ogni $a \in A$.
  In generale è un anello non commutativo con unità id_A ed invertibili le mappe biunivoche.

- $(\mathcal{M}(A,A),+,\cdot,f_0)$ con il prodotto già definito nelle pagine precedenti $(fg)(a)=f(a)g(a)$ per ogni $a\in A$.
  In generale tale anello
  i) è commutativo $\iff$ A è un anello commutativo;
  ii) ha unità $\iff$ A ha unità (e, in questo caso, l'unità è la funzione f_1 tale che $f_1(a)=1$, $\forall\, a\in A$);
  iii) (se A ha unità) ha per elementi invertibili quelli dell'insieme $\{f\in \mathcal{M}(A,A)\ t.c.\ f(a)\in A^*\ \forall\, a\in A\}$.

Esempio Sia V uno spazio vettoriale di dimensione n su $\mathbb{R}$ allora

$$End(V)\simeq(\mathscr{M}(n\times n,\mathbb{R}),+,\cdot,0)$$

(con la corrispondenza applicazione lineare $\leftrightarrow$ matrice, la composizione di funzioni corrisponde al prodotto tra matrici). Inoltre $End(V)^*\simeq GL_n(\mathbb{R})$.

Prodotto diretto

Siano $(A_1,+_1,\cdot_1,0_1)$ ed $(A_2,+_2,\cdot_2,0_2)$ due anelli. Sul prodotto cartesiano $A_1\times A_2$ definiamo due operazioni

$$(a_1,a_2)+(b_1,b_2)=(a_1+_1 b_1,a_2+_2 b_2)$$

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1\cdot_1 b_1,a_2\cdot_2 b_2)\ .$$

Dimostrare che, con tali operazioni, $A_1\times A_2$ è un anello. Inoltre
a) $A_1\times A_2$ è commutativo $\iff$ A_1 ed A_2 lo sono;
b) $A_1\times A_2$ ha unità $\iff$ A_1 ed A_2 ce l'hanno e, in tal caso, l'unità di $A_1\times A_2$ è $(1_1,1_2)$.
Infine $(A_1\times A_2)^*=A_1^*\times A_2^*$: infatti, se (a,b) è invertibile, allora $\exists\,(c,d)\in A_1\times A_2$ tale che $(a,b)(c,d)=(a\cdot_1 c,b\cdot_2 d)=(1_1,1_2)$. Dunque $a\cdot_1 c=1_1$ e $b\cdot_2 d=1_2$ cioè $a\in A_1^*$ e $b\in A_2^*$. Il viceversa è banale.

L'anello $A_1\times A_2$ non è mai un dominio di integrità anche se A_1 ed A_2 lo sono. Infatti in ogni caso si ha $(0_1,b)(a,0_2)=(0_1,0_2)$ per ogni $a\in A_1$ e $b\in A_2$.

2.2 Ideali e anelli quoziente

Cerchiamo adesso delle nozioni simili a quelle di sottogruppo e sottogruppo normale, la definizione potrà sembrare artificiosa all'inizio ma, in seguito,

vedremo che gli ideali negli anelli sono i nuclei di omomorfismi esattamente come lo erano i sottogruppi normali nei gruppi.

Definizione 2.2.1 Un sottoinsieme B di un anello A si dice *sottoanello* se

1. B è un sottogruppo additivo di A;
2. $\forall\, a, b \in B$ si ha $ab \in B$.

Un sottoinsieme I di un anello A si dice *ideale* (bilatero) se

1. I è un sottogruppo additivo di A;
2. $\forall\, a \in I$ e $\forall\, b \in A$ si ha $ab \in I$ e $ba \in I$.

Sia S un sottoinsieme di un anello A. L'*ideale generato da* S è il più piccolo (rispetto alla relazione di inclusione) ideale di A che contiene S, tale ideale si indica con (S).
Se $\mathscr{F}_S$ è l'insieme di tutti gli ideali di A che contengono S allora l'ideale generato da S è

$$(S) = \bigcap_{I \in \mathscr{F}_S} I \ .$$

Esempi - Esercizi

1. $\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$ che è un sottoanello di $\mathbb{R}$ che è un sottoanello di $\mathbb{C}$.
2. $\{0\}$ ed A sono ideali di A (ideali *banali* o *impropri*).
3. Un sottoanello di $\mathbb{Z}$ deve prima di tutto essere un sottogruppo additivo, dunque del tipo $n\mathbb{Z}$. È facile vedere che gli insiemi $n\mathbb{Z}$ sono sottoanelli di $\mathbb{Z}$, che sono ideali di $\mathbb{Z}$ e che $n\mathbb{Z} = (n)$.
4. Sia A un anello, allora A è un sottoanello di $A[X]$ che è un sottoanello di $A[[X]]$.
5. Sia I un ideale di A anello con unità. Dimostrare che $I = A \iff 1 \in I$. Dimostrare che questo non è vero per sottoanelli (cioè se B è un sottoanello di A e $1 \in B$ ciò non implica $B = A$).
6. In $\mathbb{Z}[X]$ l'ideale generato da un polinomio P è formato da tutti e soli i polinomi divisibili per P.

7. Sia A un anello e sia $a \in A$. Dimostrare che

$$I = \{P \in A[X] \text{ } t.c. \text{ } P(a) = 0\}$$

è un ideale di $A[X]$.

Lemma 2.2.2 *Sia A un anello e siano I e J due ideali di A.*

1. *$I \bigcap J$ è un ideale di A (*ideale intersezione*);*

2. *$I + J = \{a + b \text{ } t.c. \text{ } a \in I, \text{ } b \in J\}$ è un ideale di A (*ideale somma*).*

Dim. Esercizio. □

Esempio In $\mathbb{Z}$ abbiamo già visto che $n\mathbb{Z} \bigcap m\mathbb{Z} = [n, m]\mathbb{Z}$ (dove $[n, m]$ è il minimo comune multiplo). Inoltre per l'identità di Bezout $\exists\, x, y \in \mathbb{Z}$ tali che $(n, m) = xn + ym \in n\mathbb{Z} + m\mathbb{Z}$. Dunque $(n, m)\mathbb{Z} \subset n\mathbb{Z} + m\mathbb{Z}$, l'inclusione opposta è banale dato che entrambi $n\mathbb{Z}$ e $m\mathbb{Z}$ sono contenuti in $(n, m)\mathbb{Z}$, quindi $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$.

Dato che un ideale I di un anello A è un sottogruppo del gruppo abeliano $(A, +, 0)$ (quindi un sottogruppo normale) possiamo definire il gruppo quoziente A/I come fatto nel capitolo sui gruppi. In effetti tale gruppo è un anello con le operazioni indotte da A.

Proposizione 2.2.3 *Sia I un ideale di un anello A. Sia A/I il gruppo quoziente di A rispetto ad I. Definamo due operazioni tra le classi laterali di I:*

$$(a + I) + (b + I) = (a + b) + I \text{ e } (a + I)(b + I) = ab + I \text{ .}$$

Con tali operazioni A/I è un anello che si definisce anello quoziente *di A rispetto ad I.*

Dim. Dai risultati sui gruppi sappiamo che A/I è un gruppo abeliano rispetto alla somma. Dobbiamo dimostrare che il prodotto è ben definito cioè che $a + I = b + I$ e $c + I = d + I \Longrightarrow ac + I = bd + I$. In effetti $a + I = b + I \Longrightarrow \exists\, \alpha \in I$ tale che $b = a + \alpha$ e, analogamente, $c + I = d + I \Longrightarrow \exists\, \beta \in I$ tale che $d = c + \beta$. Dunque

$$bd + I = (a + \alpha)(c + \beta) + I = ac + a\beta + \alpha c + \alpha\beta + I = ac + I$$

per definizione di ideale.
Le altre verifiche delle proprietà del prodotto seguono dalle proprietà delle corrispondenti operazioni su A. □

Osservazione 2.2.4 Il quoziente di un anello modulo un suo sottoanello è un gruppo abeliano rispetto alla somma ma, in generale, non è un anello perché l'operazione prodotto può non essere compatibile con la relazione di equivalenza indotta da un sottoanello. Per esempio consideriamo $\mathbb{Z}$ come sottoanello di $\mathbb{Q}$: ovviamente $\frac{1}{2} \sim \frac{1}{2}$ e $1 \sim 2$ modulo $\mathbb{Z}$ ma $1 \cdot \frac{1}{2} = \frac{1}{2} \not\sim 1 = 2 \cdot \frac{1}{2}$ modulo $\mathbb{Z}$.

Esempio Sia P un polinomio di $\mathbb{Q}[X]$ (o, in generale, di $K[X]$ con K campo). Allora $\mathbb{Q}[X]/(P)$ è l'anello delle classi resto modulo P e dei rappresentanti sono i polinomi di grado $<$ deg P (si sfrutta l'algoritmo di divisione per trovare un rappresentante "canonico").
Per esempio se $P \in \mathbb{Z}/p\mathbb{Z}[X]$ (con p primo) e deg $P = d$ allora $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ ha p^d elementi.

Definizione 2.2.5 Un ideale I di un anello A si dice *primo* se dati $x, y \in A$ tali che $xy \in I$ si ha che $x \in I$ o $y \in I$. Un ideale I si dice *massimale* se non è contenuto in nessun ideale di A diverso da A ed I stesso (cioè: se esiste un ideale J tale che $I \subset J \subset A$ allora $J = I$ o $J = A$).

Proposizione 2.2.6 *Sia I un ideale di A anello commutativo con unità.*

1. *I è primo $\iff$ A/I è un dominio di integrità.*
2. *I è massimale $\iff$ A/I è un campo.*

Dim. **1.** ($\Longrightarrow$) Vogliamo vedere che A/I non ha divisori di zero, cioè che $(a+I)(b+I) = I$ (ricordare chi è lo "zero" di A/I) $\Longrightarrow a+I = I$ o $b+I = I$. Infatti $I = (a+I)(b+I) = ab+I \Longrightarrow ab \in I$ che è un ideale primo, dunque $a \in I$ o $b \in I$ che equivale a $a+I = I$ o $b+I = I$.
($\Longleftarrow$) Siano $x, y \in A$ tali che $xy \in I$ allora, nell'anello quoziente, $I = xy+I = (x+I)(y+I)$. Dato che A/I è un dominio, deve essere $x+I = I$ o $y+I = I$ cioè $x \in I$ o $y \in I$, dunque I è primo.
2. ($\Longrightarrow$) A/I è un anello commutativo con unità $1+I$, dunque è sufficiente dimostrare che ogni elemento di $A/I - \{I\}$ è invertibile. Sia $x \notin I$, allora l'ideale (x, I) (generato da x ed I) contiene propriamente I e, dunque, per definizione di ideale massimale, deve essere $(x, I) = A$. In particolare $1 \in (x, I)$, quindi $\exists\, y \in A$ ed $\exists\, \alpha \in I$ tali che $xy + \alpha = 1$. Allora $(x+I)(y+I) = xy + I = xy + \alpha + I = 1 + I$ ed $x + I$ è invertibile.
($\Longleftarrow$) Sia J un ideale di A diverso da I e tale che $I \subset J$. Sia $x \in J - I$, allora $x + I \neq I$ in $A/I \Longrightarrow x + I$ è invertibile ed $\exists\, y + I$ tale che $(x+I)(y+I) = xy + I = 1 + I$. Quindi $\exists\, \alpha \in I$ tale che $1 = xy + \alpha$ e dunque $(x, I) = A$. Dato che $I \subset (x, I) \subset J$ si ha $J = A$ ed I è massimale. $\square$

Corollario 2.2.7 *Ogni ideale massimale di un anello A è primo.*

Dim. Ovvio. □

Esempi - Esercizi

1. In $\mathbb{Z}$ gli ideali primi sono (0) e (p) per ogni p primo. Tra questi sono massimali solo i (p).

2. L'ideale (0) è primo se e solo se A è un dominio di integrità. L'ideale (0) è massimale se e solo se A è un campo.

3. Un ideale non banale (P) di $\mathbb{Q}[X]$ (o, in generale, di $K[X]$ con K campo) è primo (e massimale) se e solo se P è irriducibile.

2.3 Omomorfismi

I risultati di questa sezione saranno analoghi (anche nelle dimostrazioni) a quelli della corrispondente sezione nel capitolo sui gruppi, quindi (quasi sempre) trascureremo i dettagli delle dimostrazioni che possono essere facilmente ricavate da quelle già viste per i gruppi.

Definizione 2.3.1 Una funzione $\varphi : A \longrightarrow B$ tra due anelli si dice *omomorfismo* se:

1. $\forall\, a, b \in A$, $\varphi(a+b) = \varphi(a) + \varphi(b)$;

2. $\forall\, a, b \in A$, $\varphi(ab) = \varphi(a)\varphi(b)$.

Un omomorfismo biunivoco si dice *isomorfismo*.

Esempi - Esercizi

1. $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ definito da $\varphi(a) = na$ con $n \in \mathbb{Z}$ è un omomorfismo se e solo se $n = 0$ o $n = 1$. Infatti deve essere $\varphi(ab) = nab = \varphi(a)\varphi(b) = nanb = n^2ab\ \forall\, a, b \in \mathbb{Z}$. Dunque è un omomorfismo $\iff n^2 = n$.

2. $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ definito da $\varphi(a+ib) = a - ib$ il *coniugio* in $\mathbb{C}$, che si indica anche con $\varphi(a+ib) = \overline{a+ib}$. Verificare che è un isomorfismo.

3. La proiezione canonica $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ data da $\pi(a) = a + n\mathbb{Z}$. Sappiamo già che è un omomorfismo di gruppi, è facile verificare che è anche un omomorfismo di anelli. In generale per un anello A ed un suo ideale I la proiezione canonica sul quoziente $\pi : A \longrightarrow A/I$ data da $\pi(a) = a + I$ è un omomorfismo (surgettivo).

4. Sia A un anello e sia $a \in A$. La mappa $\varphi : A[X] \longrightarrow A$ definita da $\varphi(P) = P(a)$ è un omomorfismo di anelli.

Definizione 2.3.2 Sia $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Il *nucleo* di φ è l'insieme

$$Ker\,\varphi = \{a \in A \ t.c.\ \varphi(a) = 0\} \ .$$

L'*immagine* di φ è l'insieme

$$Im\,\varphi = \{b \in B \ t.c.\ \exists\, a \in A \text{ con } \varphi(a) = b\} \ .$$

Proposizione 2.3.3 *Sia $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Allora:*

1. *$Ker\,\varphi$ è un ideale di A;*

2. *$Im\,\varphi$ è un sottoanello di B.*

Dim. **1.** Dai risultati sui gruppi (Proposizione 1.3.3) sappiamo che $Ker\,\varphi$ è un sottogruppo additivo di A. Inoltre siano $a \in Ker\,\varphi$ ed $\alpha \in A$, allora $\varphi(a\alpha) = \varphi(a)\varphi(\alpha) = 0\varphi(\alpha) = 0$ e, analogamente, $\varphi(\alpha a) = 0$. Quindi $\alpha a, a\alpha \in Ker\,\varphi$ che è un ideale.
2. Dai risultati sui gruppi sappiamo che $Im\,\varphi$ è un sottogruppo additivo di B. Inoltre $\alpha, \beta \in Im\,\varphi \Longrightarrow \exists\, a, b \in A$ tali che $\varphi(a) = \alpha$ e $\varphi(b) = \beta$, dunque $\alpha\beta = \varphi(a)\varphi(b) = \varphi(ab) \in Im\,\varphi$. $\square$

Analogamente ai risultati sui gruppi (Proposizione 1.3.3) si può dimostrare il seguente

Lemma 2.3.4 *Sia $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Allora:*

1. *$\varphi(0) = 0$;*

2. *$\forall\, a \in A$, $\varphi(-a) = -\varphi(a)$;*

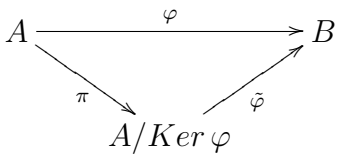
3. *se A e B hanno unità e se $\varphi(1_A) = 1_B$ allora $\forall\, a \in A^*$ si ha $\varphi(a) \in B^*$ e $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

Dim. Semplice applicazione delle definizioni. □

Proposizione 2.3.5 *Sia $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Allora φ è iniettivo se e solo se $Ker\,\varphi = \{0\}$.*

Dim. Analoga a quella per i gruppi (Proposizione 1.3.4). □

Teorema 2.3.6 *Sia $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Sia $\pi : A \longrightarrow A/Ker\,\varphi$ la proiezione canonica sul quoziente. Allora $\exists!$ omomorfismo iniettivo $\tilde{\varphi} : A/Ker\,\varphi \longrightarrow B$ che rende commutativo il diagramma*



cioè tale che $\tilde{\varphi} \circ \pi = \varphi$.
In particolare $\tilde{\varphi}$ induce un isomorfismo $A/Ker\,\varphi \simeq Im\,\varphi$.

Teorema 2.3.7 *Sia $\varphi : A \longrightarrow B$ un omomorfismo surgettivo di anelli. Allora c'è corrispondenza biunivoca tra gli ideali di B e gli ideali di A che contengono $Ker\,\varphi$ data da*

$$J \leftrightarrow \varphi^{-1}(J) = \{a \in A \text{ } t.c. \text{ } \varphi(a) \in J\} \quad \forall\, J \text{ ideale di } B\ .$$

Inoltre c'è un isomorfismo canonico $A/\varphi^{-1}(J) \simeq B/J$.

Le dimostrazioni ricalcano (con ovvie generalizzazioni) quelle già fatte per i gruppi (Teoremi 1.3.5 e 1.3.9 e Lemma 1.3.8). Può essere utile scriverle come esercizio da fare una volta nella vita (ovviamente, dato che la mia volta è stata nel secolo scorso, in queste note non troverete nessuna dimostrazione).

Esempio Sia $\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$ definita da $\varphi(P) = P(i)$. È facile vedere che φ è un omomorfismo surgettivo. Il suo nucleo è composto da tutti i polinomi di $\mathbb{R}[X]$ che si annullano in i cioè da tutti quelli divisibli per $X^2 + 1$, quindi $Ker\,\varphi = (X^2 + 1)$. Dunque $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$. Notare che, dato che $\mathbb{C}$ è un campo, $(X^2 + 1)$ è un ideale massimale in $\mathbb{R}[X]$.

Ideali e omomorfismi - Esercizi

1. *Nilpotenti*

Definizione 2.3.8 Sia A un anello. Un elemento $a \in A$ si dice *nilpotente* se $\exists\, n \in \mathbb{N}$ tale che $a^n = 0$. L'insieme degli elementi nilpotenti di A si indica con $Nil(A)$.

Proposizione 2.3.9 *Sia A un anello commutativo con unità, allora $Nil(A)$ è un ideale di A.*

Dim. È ovvio che $0 \in Nil(A)$, inoltre se $a \in Nil(A)$ allora $a^n = 0$ per qualche $n \in \mathbb{N} \Longrightarrow (-a)^n = (-1)^n a^n = 0$, dunque $-a \in Nil(A)$. Siano $a, b \in Nil(A)$ con $a^n = b^m = 0$ $(n, m \in \mathbb{N})$, allora

$$(a+b)^{n+m-1} = \sum_{i=1}^{n+m-1} \binom{n+m-1}{i} a^i b^{n+m-1-i} \ .$$

Nella somma a destra, per gli indici $i \geq n$, si ha

$$a^i b^{n+m-1-i} = a^n a^{i-n} b^{n+m-1-i} = 0 \ ,$$

mentre per gli indici $i \leq n-1$ si ha $n+m-1-i \geq n+m-1-(n-1) = m$ dunque

$$a^i b^{n+m-1-i} = a^i b^m b^{n-1-i} = 0 \ .$$

Quindi $(a+b)^{n+m-1} = 0 \Longrightarrow (a+b) \in Nil(A)$ e $Nil(A)$ è un sottogruppo additivo di A.
Infine se $a \in Nil(A)$ (con $a^n = 0$) e $b \in A$ si ha $(ab)^n = a^n b^n = 0$. $\square$

Osservazione 2.3.10 Se A non è commutativo $Nil(A)$ non è un ideale in generale. Per esempio con $A = \mathscr{M}(2 \times 2, \mathbb{R})$ siano

$$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ \text{ ed } \ L = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \ .$$

È facile verificare che $M^2 = L^2 = 0$ ma $M + L$ è tale che

$$(M+L)^n = \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{se } n \text{ dispari} \\ \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{se } n \text{ pari} \end{cases} \ .$$

Dunque $M, L \in Nil(A)$ ma $M + L \notin Nil(A)$.

Esercizio Trovare $Nil(A)$ per gli anelli $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/125\mathbb{Z}$ e $\mathbb{Z}/100\mathbb{Z}$. In generale sia $n = p_1^{a_1} \cdots p_k^{a_k}$ (con p_i primi distinti) la fattorizzazione di n. Dimostrare che $Nil(A) = (\prod_{i=1}^{k} p_i)$.

2. Sia A un anello commutativo con unità, $x \in A^*$ ed $a \in Nil(A)$. Dimostrare che $x + a \in A^*$.
Dim. Sia $y \in A$ tale che $xy = 1$ e sia $n \in \mathbb{N}$ tale che $a^n = 0$. Si ha $(x + a)y = 1 + ay$ ed ay è tale che $(ay)^n = 0$. È sufficiente dimostrare che $1 + ay$ è invertibile,

$$(1+ay)(1-ay+a^2y^2-\cdots+(-1)^{n-1}a^{n-1}y^{n-1}) = (1+ay)\sum_{i=0}^{n-1}(-1)^i(ay)^i =$$

$$= \sum_{i=0}^{n-1}(-1)^i(ay)^i + \sum_{i=0}^{n-1}(-1)^i(ay)^{i+1} = \sum_{i=0}^{n-1}(-1)^i(ay)^i + \sum_{i=1}^{n}(-1)^{i-1}(ay)^i =$$

$$= 1 + \sum_{i=1}^{n-1}((-1)^i + (-1)^{i-1})(ay)^i + (-1)^{n-1}(ay)^n = 1 \ .$$

3. Sia A un anello commutativo con unità. Allora A è un campo $\iff$ i suoi unici ideali sono quelli banali (A e (0)).
Dim. ($\Longrightarrow$) Se I è un ideale $\neq (0)$ allora contiene un elemento invertibile x, dunque contiene $xx^{-1} = 1$ ed è quindi $I = A$.
($\Longleftarrow$) Sia $x \in A - \{0\}$ e consideriamo l'ideale (x). Dato che $(x) \neq (0)$ deve essere $(x) = A \Longrightarrow 1 \in (x)$ cioè $\exists\, y \in A$ tale che $xy = 1$. Dunque $A^* = A - \{0\}$ ed A è un campo.

4. Dire se (X) è un ideale primo e massimale di $\mathbb{Z}[X]$ e di $\mathbb{Z}/n\mathbb{Z}[X]$.
Dim. Possiamo in generale definire, per ogni anello A, un omomorfismo $\varphi : A[X] \longrightarrow A$ dato da $\varphi(P) = P(0)$. È ovviamente surgettivo, con nucleo $Ker\,\varphi = (X)$. Dunque per il Teorema 2.3.6 si ha $A[X]/(X) \simeq A$ e (X) è primo $\iff$ A è un dominio di integrità (quindi, nei casi richiesti, per $\mathbb{Z}$ e $\mathbb{Z}/p\mathbb{Z}$ con p primo), mentre (X) è massimale $\iff$ A è un campo (quindi, nei casi richiesti, solo $\mathbb{Z}/p\mathbb{Z}$ con p primo).
Per esempio in $\mathbb{Z}/15\mathbb{Z}[X]$ l'ideale (X) non è primo, infatti $3+X, 5+X \notin (X)$ ma $(3 + X)(5 + X) = 8X + X^2 \in (X)$.

5. Dimostrare che per ogni primo p l'ideale (p, X) è massimale in $\mathbb{Z}[X]$.
Dim. Esercizio. (Sugg. Utilizzare la mappa $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}$ data da $\varphi(P) = [P(0)]_p$)

6. Sia $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5}\ t.c.\ a, b \in \mathbb{Z}\}$, dimostrare che è un sottoanello di $\mathbb{R}$ ed è un dominio di integrità ma non è un campo.

7. Sia $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \ t.c. \ a, b \in \mathbb{Q}\}$, dimostrare che è un campo.

8. Dire se l'ideale $(X^2 - 5)$ è primo e massimale in $\mathbb{Z}[X]$ e $\mathbb{Q}[X]$.
Dim. Verificare che la mappa $\varphi : A[X] \longrightarrow A[\sqrt{5}]$ (con $A = \mathbb{Z}$ o $\mathbb{Q}$) definita da $\varphi(P) = P(\sqrt{5})$ è un omomorfismo surgettivo, verificare che il nucleo è proprio l'ideale (X^2-5) ed utilizzare il Teorema 2.3.6 ed i precedenti esercizi **6** e **7**.

9. Sia $\varphi : A \longrightarrow B$ un omomorfismo di anelli commutativi con unità. Sia P un ideale primo di B, dimostrare che $\varphi^{-1}(P) = \{a \in A \ t.c. \ \varphi(a) \in P\}$ è un ideale primo di A. Vale la stessa cosa per un ideale massimale ?
Dim. È utile fare l'esercizio seguendo semplicemente la definizione di ideale primo. Se uno vuol fare il figo può anche notare che, per il Teorema 2.3.7, $A/\varphi^{-1}(P)$ è isomorfo ad un sottoanello di B/P che è un dominio $\Longrightarrow A/\varphi^{-1}(P)$ è un dominio e quindi P è primo.
La controimmagine di un ideale massimale non è sempre massimale, per esempio considerando l'inclusione $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ si ha $i^{-1}(0) = (0)$ e (0) è massimale in $\mathbb{Q}$ ma soltanto primo in $\mathbb{Z}$.

10. Sia $\mathcal{C}(\mathbb{Q})$ l'insieme di tutte le successioni di Cauchy definite su $\mathbb{Q}$, cioè le successioni di Cauchy $\{a_n\}_{n\in\mathbb{N}}$ tali che $a_n \in \mathbb{Q}$ per ogni $n \in \mathbb{N}$. Verificare che $\mathcal{C}(\mathbb{Q})$ con le operazioni $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ e $\{a_n\} \cdot \{b_n\} = \{a_n b_n\}$ è un anello commutativo con unità. Sia I l'insieme delle successioni in $\mathcal{C}(\mathbb{Q})$ il cui limite è 0. Dimostrare che I è un ideale massimale di $\mathcal{C}(\mathbb{Q})$.

2.4 Anelli di polinomi

In questa sezione A sarà sempre un dominio, $Q(A)$ sarà il suo campo dei quozienti (vd sezione 3.3) e K sarà un campo.
Dato un anello A abbiamo già definito $A[X]$ e ne abbiamo viste alcune proprietà. Adesso spostiamo l'attenzione sulla fattorizzazione degli elementi di $A[X]$.

Definizione 2.4.1 Sia A un dominio, un elemento non invertibile $a \in A$ si dice *irriducibile* se $a = bc \Longrightarrow b \in A^*$ o $c \in A^*$. Un elemento non invertibile $a \in A$ si dice *primo* se $a|bc \Longrightarrow a|b$ oppure $a|c$.

Esempi - Esercizi

1. In un dominio 0 è primo (ricordiamo che ogni elemento divide 0 ma 0 divide solo se stesso) ma non è mai irriducibile.

2. In $\mathbb{Z}$ ogni primo p è un elemento primo ed irriducibile.

3. In $\mathbb{R}[X]$ gli irriducibili sono tutti e soli i polinomi di grado 1 o di grado 2 con discriminante negativo. I primi sono gli stessi polinomi e lo 0. In $\mathbb{C}[X]$ gli irriducibili (e primi, aggiungendo lo 0) sono tutti e soli i polinomi di grado 1.

4. Sia A un dominio e sia $a \in A$ irriducibile. Dimostrare che a è irriducibile anche come elemento di $A[X]$.

Lemma 2.4.2 *Sia A un dominio e sia $a \in A - \{0\}$. Allora a primo $\Longrightarrow$ a irriducibile.*

Dim. Se $a = bc$ allora $a|b$ o $a|c$. Supponiamo $a|b$ (l'altro caso è simmetrico) allora $\exists\, d \in A$ tale che $b = ad$ e dunque $a = bc = adc \Longrightarrow a(dc - 1) = 0$. Dato che A è un dominio ed $a \neq 0$ si ottiene $dc = 1$ cioè c è invertibile. $\square$

Osservazione 2.4.3 Il viceversa non è sempre vero (ma vd Lemma 2.4.7). Per esempio in $\mathbb{Z}[\sqrt{-5}]$ si ha $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Dunque $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ ma $2 \nmid (1 + \sqrt{-5})$ e $2 \nmid (1 - \sqrt{-5})$ quindi 2 non è primo. Comunque 2 è irriducibile in $\mathbb{Z}[\sqrt{-5}]$ (la stessa cosa vale per 3, $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$).

Definizione 2.4.4 Sia A un dominio. Due elementi a e b di A si dicono *associati* se $\exists\, u \in A^*$ tale che $a = ub$.

Esercizio Verificare che $a \sim b \iff \exists u \in A^*$ tale che $a = ub$ è una relazione di equivalenza.

Andremo ad esaminare la possibilità di fattorizzare (in maniera sostanzialmente unica) gli elementi di alcuni anelli in prodotto di irriducibili (un esempio è la fattorizzazione degli interi in prodotto di primi). In realtà l'unicità dei fattori sarà garantita solo a meno di elementi tra loro associati. Per esempio in $\mathbb{Z}$ siamo abituati a fattorizzare con primi positivi ma una fattorizzazione come $6 = (-2)(-3)$ deve essere ammissibile (perchè sia -2 che -3 sono irriducibili secondo la Definizione 2.4.1) senza negare "l'unicità". Lo stesso per le fattorizzazioni in $\mathbb{Q}[X]$

$$X^2 + 3X + 2 = (X + 1)(X + 2) = (aX + a)\left(\frac{X + 2}{a}\right) \ \forall\, a \in \mathbb{Q}^* \ .$$

Dunque ogni volta che parleremo di "fattorizzazione unica" intenderemo sempre "a meno di elementi associati tra loro" cioè modulo la relazione di equivalenza appena descritta. Il fatto che nelle applicazioni si tenda ad affidarsi a convenzioni consolidate (tipo prendere i primi positivi in $\mathbb{Z}$ o i polinomi monici in $K[X]$) non deve far dimenticare il quadro teorico generale.

Definizione 2.4.5 Un ideale I in un anello A si dice *principale* se può essere generato da un solo elemento, cioè se $\exists\, a \in A$ tale che $I = (a)$. Un dominio di integrità A si dice *dominio ad ideali principali* (sigla *PID*) se ogni ideale di A è principale.
Un dominio di integrità A si dice *anello a fattorizzazione unica* (sigla *UFD*) se ogni elemento non invertibile di A si può scrivere in maniera unica (vd sopra) come prodotto di irriducibili.

Osservazione 2.4.6 In un UFD si possono definire le nozioni di massimo comune divisore (MCD) e minimo comune multiplo (mcm) analogamente a quelle classiche di $\mathbb{Z}$. Ovviamente l'algoritmo euclideo per il calcolo del MCD è applicabile solo negli anelli in cui sia definibile una qualche operazione di divisione (tali anelli sono appunto detti *euclidei*, vd [1] sezione 3.7) come per esempio $\mathbb{Z}$ e $K[X]$ come vedremo tra poco. Negli altri casi il calcolo può richiedere strumenti più sofisticati di algebra computazionale.

Esempio $\mathbb{Z}$ è un PID ed un UFD. Si può dimostrare che PID $\Longrightarrow$ UFD (vd, per esempio, [2] Chapter II Theorem 5.2) ma non è vero il viceversa. Per esempio $\mathbb{Z}[X]$ è un UFD (e lo dimostreremo) ma non un PID, infatti l'ideale $(3, X)$ non è principale. Se fosse $(3, X) = (P)$ allora $P|3$ e $P|X$ ma l'unico divisore comune in $\mathbb{Z}[X]$ è 1 e P non può essere uguale a 1 perché $(3, X) \neq \mathbb{Z}[X]$.

Lemma 2.4.7 *Sia A un PID e sia $a \in A$. Allora a è irriducibile $\Longleftrightarrow$ a è primo e diverso da* 0.

Dim. Abbiamo già visto (Lemma 2.4.2) che primo $\Longrightarrow$ irriducibile in generale. Sia adesso a irriducibile, supponiamo $a|bc$ e $a \nmid b$. Consideriamo l'ideale (a, b) che, dato che A è un PID, sarà generato da un elemento d. Allora $d|a$ e, dato che a è irriducibile, deve essere $d \in A^*$ oppure d associato ad a. Ma $(d) = (a, b) \Longrightarrow d|b$ e, dato che $a \nmid b$, d non può essere associato ad a (perché ?). Dunque $d \in A^* \Longrightarrow (a, b) = (d) = A$ e, in particolare, $1 \in (a, b)$. Siano allora $x, y \in A$ tali che $ax + by = 1$, moltiplicando per c si ottiene $acx + bcy = c$ e, dato che $a|acx$ ed $a|bcy$, si ha $a|c$: quindi a è primo. $\square$

Definizione - Esercizio Sia A un PID e siano $a, b \in A$. Definiamo il *massimo comune divisore* di a e b, indicato con $MCD(a, b)$, come l'elemento d (meglio come la classe di elementi associati a d) tale che

1. $d|a$ e $d|b$;
2. se $c|a$ e $c|b$ allora $c|d$.

Sia α un generatore dell'ideale (a, b) in A. Dimostrare che $\alpha = MCD(a, b)$.

Lemma 2.4.8 *Sia A un dominio e sia $a \in A$. Allora:*

1. *a è primo $\iff$ (a) è un ideale primo;*
2. *se A è un PID allora a è irriducibile $\iff$ (a) è un ideale massimale;*
3. *se A è un PID allora ogni ideale primo diverso da 0 è massimale.*

Dim. **1.** L'ideale (a) è primo $\iff$ per ogni $b, c \in A$ tali che $bc \in (a)$ si ha $b \in (a)$ o $c \in (a)$ $\iff$ $a|bc$ implica $a|b$ o $a|c$ $\iff$ a è primo.
2. ($\Longleftarrow$) segue dalla parte **1** e dal Lemma 2.4.2.
($\Longrightarrow$) Sia (b) un ideale che contiene (a) allora $a = bc$ per qualche $c \in A$. Ma a irriducibile $\Longrightarrow$ $b \in A^*$ o $c \in A^*$. Nel primo caso $(b) = (1) = A$ e nel secondo $a = bc \Longrightarrow ac^{-1} = b$ cioè $b \in (a)$ e $(b) = (a)$.
3. Segue dai punti precedenti e dal Lemma 2.4.7. $\square$

2.4.1 Polinomi a coefficienti in un campo

Sia K un campo allora sull'anello $K[X]$ è possibile definire un *algoritmo di divisione* (analogo a quello su $\mathbb{Q}[X]$ o $\mathbb{R}[X]$) che consiste nel seguente

Teorema 2.4.9 *Siano $f, g \in K[X]$, con $fg \neq 0$. Allora $\exists\, q, r \in K[X]$ tali che $f = gq + r$ e $\deg r < \deg g$.*

Dim. Procediamo per induzione su $\deg f$. Se $\deg f = 0$ allora o $\deg g = 0$ e dunque $f = \frac{f}{g} g$ con $q = \frac{f}{g}$ ed $r = 0$ (ricordare la convenzione per cui $\deg 0 = -\infty$) oppure $\deg g > 0$ e si ottiene $f = 0g + f$ con $q = 0$ e $r = f$.
Ipotesi induttiva: supponiamo vera la tesi per $\deg f < n$.
Consideriamo f di grado n e g di grado m qualsiasi,

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{e} \quad g = \sum_{i=0}^{m} b_i X^i$$

con $a_n b_m \neq 0$. Se $m > n$ allora $f = 0g + f$ come sopra. Se invece $m \leq n$ definiamo $f_1 = f - a_n b_m^{-1} g X^{n-m}$. Per costruzione deg $f_1 \leq n-1$, dunque per induzione $\exists\, q_1, r_1 \in K[X]$ tali che $f_1 = gq_1 + r_1$ e deg $r_1 <$ deg g. Quindi $f = g(a_n b_m^{-1} X^{n-m} + q_1) + r_1$ e la tesi è verificata con $q = a_n b_m^{-1} X^{n-m} + q_1$ ed $r = r_1$. $\square$

Teorema 2.4.10 *Sia K un campo. Allora $K[X]$ è un PID ed un UFD.*

Dim. Se I è un ideale banale (0) o $K[X]$ allora $I = (0)$ o $I = (1)$ dunque è principale. Se I non è banale allora $\exists\, Q \in I$ con deg $Q > 0$ (notare che se $a \in I$ e deg $a = 0$ allora $a \in K^*$, dunque è invertibile ed $aa^{-1} = 1 \in I \Longrightarrow I = K[X]$: quindi se I non è banale non può contenere elementi di grado 0). Definiamo $P \in I$ come il polinomio diverso da 0 di grado minimo in I, cioè deg $P = \min\{\text{deg } Q \,:\, Q \in I - \{0\}\}$. Per ogni $Q \in I$, l'algoritmo di divisione dà $Q = PS + R$ con deg $R <$ deg P. Allora $R = Q - PS \in I$ e, per la minimalità del grado di P, deve essere $R = 0$. Quindi $I \subset (P)$, l'altra inclusione è ovvia e $I = (P)$ è principale.
Per la fattorizzazione sia $P \in K[X]$ e procediamo per induzione su deg P. Se deg $P = 0$ allora P è invertibile e se deg $P = 1$ allora P è ovviamente irriducibile.
Ipotesi induttiva: supponiamo di avere una fattorizzazione per polinomi di grado $< n$.
Consideriamo P di grado n, se P è irriducibile abbiamo finito, se non è irriducibile allora $\exists\, Q, R \in K[X]$ tali che $P = QR$ e $Q, R \notin K[X]^*$. Dalla formula deg $P =$ deg $Q +$ deg R segue che deg Q, deg $R <$ deg $P = n \Longrightarrow$ per ipotesi induttiva esistono fattorizzazioni in irriducibili

$$Q = \prod_i Q_i^{a_i} \quad \text{ed} \quad R = \prod_j R_j^{b_j} \ .$$

Dunque

$$P = \prod_i Q_i^{a_i} \prod_j R_j^{b_j}$$

è prodotto di irriducibili.
Per l'unicità supponiamo di avere due diverse fattorizzazioni in irriducibili distinti

$$P = \prod_i P_i^{a_i} \quad \text{e} \quad P = \prod_j Q_j^{b_j} \ .$$

Dunque $P_1 | P$ cioè $P_1 | \prod_j Q_j^{b_j}$ e, dato che P_1 è primo (Lemma 2.4.7), $P_1 | Q_j$ per qualche j. Dato che sono entrambi irriducibili devono essere associati quindi $P_1 \sim Q_j$. Analogamente si procede con gli altri irriducibili per dimostrare che le due fattorizzazioni sono associate e, quindi, equivalenti. $\square$

2.4.2 Polinomi a coefficienti in un dominio

Sia A un dominio di integrità e sia $K = Q(A)$ il suo campo dei quozienti. Nella sezione precedente abbiamo dimostrato che $K[X]$ è un PID ed un UFD ma ancora non abbiamo visto nulla sulla fattorizzazione in $A[X]$. Per avere una fattorizzazione (unica a meno di associati anche in questo caso) in $A[X]$ è ovvio che bisogna cominciare da una fattorizzazione in A altrimenti i polinomi di grado zero non sarebbero fattorizzabili. Il nostro scopo sarà di dimostrare che se A è un UFD allora anche $A[X]$ è un UFD.

Definizione 2.4.11 Sia A un UFD e sia $P \in A[X]$. Il *divisore* di P o *contenuto* di P (che si indica con $d(P)$ o $cont(P)$) è il massimo comune divisore tra i coefficienti di P. Un polinomio P si dice *primitivo* se $d(P) = 1$.

Esempi

1. Ogni polinomio monico (cioè con coefficiente direttore 1) è primitivo.
2. In $\mathbb{Z}[X]$, $P = 2X^3 + 4X^2 - 6X + 5$ è primitivo, mentre per $Q = 3X^3 - 6X^2 + 12X - 9$ si ha $d(Q) = 3$.
3. In $(\mathbb{Q}[X])[Y]$ (anello dei polinomi nella variabile Y con coefficienti in $\mathbb{Q}[X]$) il polinomio $P = (X^2 - 1)Y^2 + (X + 1)^3Y + (X^3 + 1)$ non è primitivo. Quale è $d(P)$?

Lemma 2.4.12 (Gauss) *Sia A un UFD e siano $P, Q \in A[X]$ allora $d(PQ) = d(P)d(Q)$.*

Dim. Fissiamo un irriducibile $a \in A$ e supponiamo che $a^r \parallel d(P)$ e $a^s \parallel d(Q)$, vogliamo dimostrare che $a^{r+s} \parallel d(PQ)$ (il che equivale alla tesi). È facile vedere che $a^{r+s} | d(PQ)$ quindi cerchiamo un coefficiente di PQ che non sia divisibile per a^{r+s+1}. Siano $P = \sum a_n X^n$ e $Q = \sum b_n X^n$, definiamo $i = \min\{k : a^{r+1} \nmid a_k\}$ e $j = \min\{k : a^{s+1} \nmid b_k\}$. Il coefficiente di X^{i+j} in PQ è

$$\sum_{h+k=i+j} a_k b_h = a_i b_j + \sum_{\substack{h+k=i+j \\ k \neq i,\, h \neq j}} a_k b_h \ .$$

Nella sommatoria a destra ogni termine è divisibile per a^{r+s+1} (perché o $k < i$ o $h < j$) mentre $a^{r+s+1} \nmid a_i b_j$, quindi a^{r+s+1} non divide il coefficiente di $X^{i+j} \Longrightarrow a^{r+s+1}$ non divide $d(PQ)$. $\square$

Corollario 2.4.13 *Sia A un UFD, il prodotto di due polinomi primitivi in $A[X]$ è primitivo.*

Teorema 2.4.14 *Se A è un UFD allora $A[X]$ è un UFD.*

Dim. Sia $P \in A[X]$ allora possiamo scrivere $P = d(P)P_1$ con $d(P) \in A$ e $P_1 \in A[X]$ primitivo. L'elemento $d(P)$ ha una fattorizzazione (unica) in A e, quindi, in $A[X]$ (ricordare che gli irriducibili di A sono irriducibili anche in $A[X]$). Sia $K = Q(A)$ il campo dei quozienti di A allora $K[X]$ è un UFD per il Teorema 2.4.10 $\Longrightarrow \exists$ una fattorizzazione (unica) $P_1 = \prod Q_i^{e_i}$ con i $Q_i \in K[X]$ irriducibili. Prendendo i minimi comuni denominatori possiamo scrivere, per ogni i, $Q_i = \frac{a_i}{b_i} R_i$ dove $a_i\,, b_i \in A$, $b_i \neq 0$ e $R_i \in A[X]$ primitivo. Dunque

$$P_1 = \prod \frac{a_i}{b_i} R_i = \frac{a}{b} \prod R_i \Longrightarrow bP_1 = a \prod R_i \ .$$

Inoltre P_1 primitivo $\Longrightarrow d(bP_1) = b$ ed R_i primitivo per ogni $i \Longrightarrow \prod R_i$ primitivo (per il Corollario 2.4.13), dunque $d(a \prod R_i) = a$. Quindi $b = d(bP_1) = d(a \prod R_i) = a$ e $P_1 = \prod R_i$ è una fattorizzazione in $A[X]$. Unendo le fattorizzazioni di $d(P)$ e di P_1 si ottiene una fattorizzazione (unica perché le altre due lo sono) di P in $A[X]$. $\square$

Teorema dell'elemento primitivo

Procediamo con una serie di esercizi che porteranno alla fine alla dimostrazione del Teorema dell'elemento primitivo.

Definizione 2.4.15 Sia K un campo e sia $P \in K[X]$. Un elemento $\alpha \in K$ si dice *radice* di P se $P(\alpha) = 0$.

Osserviamo che anche se un polinomio $P \in K[X]$ non ha radici in K può essere riducibile in $K[X]$. Per esempio le radici di $X^4 - 4$ sono $\pm\sqrt{2}$ e $\pm\sqrt{-2}$ e nessuna di loro è in $\mathbb{Q}$, ma $X^4 - 4 = (X^2 + 2)(X^2 - 2)$ in $\mathbb{Q}[X]$. Se invece un polinomio ha una radice in K allora è sicuramente riducibile in $K[X]$ come mostra il seguente esercizio.

1. Sia K un campo e sia $P \in K[X]$. Dimostrare che $\alpha \in K$ è una radice di P se e solo se $X - \alpha$ divide P.

Definizione 2.4.16 Sia K un campo, sia $P \in K[X]$ e sia $\alpha \in K$ una radice di P. Si dice che α ha *molteplicità* m se $(X - \alpha)^m \parallel P$.

2. Sia K un campo e sia $P \in K[X]$ di grado $n \geq 0$. Dimostrare che P ha al più n radici distinte in K.
Dim. Per induzione su deg P. Se deg $P = 0$ tutto è banale.
Ipotesi induttiva: supponiamo la tesi vera per polinomi di grado $\leq n-1$. Sia adesso P di grado n, se P non ha radici in K abbiamo finito. Se $\exists \alpha \in K$ radice di P allora $P = (X-\alpha)Q$ e deg $Q = n-1$. Sia $\beta \in K$ un'altra radice ($\beta \neq \alpha$) allora $0 = P(\beta) = (\beta - \alpha)Q(\beta) \Longrightarrow Q(\beta) = 0$. Dunque le radici distinte di P sono α e le radici distinte di Q. Per ipotesi induttiva Q ha al più $n-1$ radici distinte $\Longrightarrow P$ ne ha al più n.

3. *Teorema dell'elemento primitivo.* Sia K un campo e sia U un sottogruppo finito di K^*. Allora U è ciclico.
Dim. Sia $o(U) = n$ e sia d il massimo tra gli ordini degli elementi di U, per il Corollario 1.2.18 si ha $d \leq n$ e vogliamo dimostrare che $d = n$. Sia $b \in U$ qualsiasi, per il Teorema di struttura dei gruppi abeliani finiti (vd Teoremi 1.5.3 e 1.5.4) si ha che $b^d = 1$, dunque ogni elemento di U è radice del polinomio $X^d - 1 \in K[X]$. Tale polinomio ha allora almeno n radici $\Longrightarrow d \geq n$ e quindi $d = n$.

4. Dal Teorema precedente segue, per esempio, che per ogni p primo $(\mathbb{Z}/p\mathbb{Z})^*$ è ciclico. Trovare almeno un generatore di $(\mathbb{Z}/p\mathbb{Z})^*$ per p=2, 3, 5, 7, 11, 13, 17, 19, 23,...

5. Sia K un campo che contenga tutte le radici di $P \in K[X]$. Dimostrare che P ha radici distinte (cioè tutte di molteplicità 1) se e solo se è relativamente primo con la sua derivata, cioè $MCD(P, P') = 1$.
Dim. ($\Longleftarrow$) Se $\alpha \in K$ è una radice di molteplicità $m \geq 2$ allora, per definizione, $P = (X-\alpha)^m Q$ dunque $P' = m(X-\alpha)^{m-1}Q + (X-\alpha)^m Q' \Longrightarrow (X-\alpha) | MCD(P, P')$: contraddizione.
($\Longrightarrow$) Sia $n = \deg P$ e siano $\alpha_1, \ldots, \alpha_n$ le radici distinte di P, allora

$$P = \prod_{i=1}^{n} (X - \alpha_i)$$

è la fattorizzazione di P in $K[X]$. Dunque

$$P' = \sum_{i=1}^{n} \left(\prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - \alpha_j) \right)$$

e

$$P'(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_i - \alpha_j) \neq 0 \ .$$

Quindi, per ogni i, $X - \alpha_i$ non divide P', cioè P e P' non hanno fattori comuni $\Longrightarrow (P, P') = 1$.

6. Dimostrare che per ogni $n \geq 1$ il polinomio $X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]$ ha radici distinte.
Dim. Sugg. Quale è la sua derivata ?

7. Sia p un primo. Dimostrare che $(p-1)! \equiv -1 \pmod{p}$.
Dim. Dal (piccolo) Teorema di Fermat segue che le classi di 0, 1,..., $p-1$ sono radici di $X^p - X$. Dunque in $\mathbb{Z}/p\mathbb{Z}[X]$ si ha la fattorizzazione $X^p - X = X(X-1)\cdots(X-p+1)$ e quindi $X^{p-1} - 1 = (X-1)\cdots(X-p+1)$. Dall'uguaglianza dei termini noti segue $(-1)(-2)\cdots(-p+1) \equiv -1 \pmod{p}$ cioè $(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}$. La tesi segue osservando che, se $p = 2$, $-1 \equiv 1 \pmod{2}$ e, se $p \neq 2$, allora p è dispari e quindi $(-1)^{p-1} = 1$.

8. Sia K un campo di caratteristica 0 e sia $P \in K[X]$ irriducibile. Dimostrare che P ha radici distinte.

2.5 Estensioni di campi

In questa sezione F e K saranno sempre campi. In generale un polinomio $P \in K[X]$ può non avere radici in K (per esempio X^2+1 non ha radici in $\mathbb{R}$) ma è sempre possibile definire un campo $F \supset K$ in cui sia presente almeno una radice di P (nell'esempio precedente $\mathbb{C} \supset \mathbb{R}$).

Definizione 2.5.1 Sia K un campo, un campo F contenente K si dice *estensione* di K. Un elemento $\alpha \in F \supset K$ si dice *algebrico* su K se $\exists\, P \in K[X] - \{0\}$ tale che $P(\alpha) = 0$. Un elemento $\alpha \in F \supset K$ che non sia algebrico su K si dice *trascendente* su K.

Esempi

1. $i = \sqrt{-1}$ è radice di $X^2 + 1$ ed è algebrico su $\mathbb{Q}$.
2. Sia K un campo, allora ogni $\alpha \in K$ è banalmente algebrico su K.
3. Si può dimostrare (vd per esempio [1] sezione 5.2) che e e π sono trascendenti su $\mathbb{Q}$.
4. $\sqrt{2} + \sqrt{3}$ è radice di $X^4 - 10X^2 + 1$ ed è dunque algebrico su $\mathbb{Q}$.

Cercheremo di trovare una risposta ai seguenti problemi:

1. dato α algebrico su un campo K, trovare $P \in K[X]$ irriducibile di grado minimo tale che $P(\alpha) = 0$;

2. dato P irriducibile in $K[X]$ trovare un campo in cui P abbia almeno una radice.

Il primo è (almeno nella teoria, il calcolo pratico è spesso molto complesso) semplice da risolvere. Sia $\alpha \in F$ algebrico su K. Definiamo $I_\alpha = \{P \in K[X] \; t.c. \; P(\alpha) = 0\}$, è facile verificare che I_α è un ideale di $K[X]$. Dato che $K[X]$ è un PID, $\exists\, P_\alpha \in K[X]$ tale che $I_\alpha = (P_\alpha)$. Dalla dimostrazione del Teorema 2.4.10 segue che P_α è un polinomio diverso da zero di grado minimo in I_α. Se $u \in K^*$ allora è ovvio che $(P_\alpha) = (uP_\alpha)$, dunque possiamo sempre scegliere un generatore che sia monico.

Definizione 2.5.2 Con le notazioni precedenti sia P_α il generatore monico di I_α, allora P_α si dice *polinomio minimo* di α su $K[X]$.

Esercizio Sia α algebrico su un campo K. Dimostrare che il polinomio minimo di α su K è irriducibile.
Dim. Sugg. se P_α non è irriducibile allora esiste un polinomio di grado inferiore a deg P_α che ha per radice α. Quale contraddizione ne segue ?

Esempi

1. $X^2 + 1$ è il polinomio minimo di i su $\mathbb{R}$ e su $\mathbb{Q}$.

2. $X^2 - 2$ è il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ ma non su $\mathbb{R}$.

3. Sia $\zeta_3 = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ una radice cubica dell'unità, allora ζ_3 è radice di X^3-1 quindi è algebrico su $\mathbb{Q}$ e il suo polinomio minimo è X^2+X+1.

Per quanto riguarda il secondo problema sia K un campo e $P \in K[X]$ (monico e) irriducibile, allora l'ideale (P) è massimale in $K[X]$ dunque $K[X]/(P)$ è un campo. Sia $\pi : K[X] \longrightarrow K[X]/(P)$ la proiezione canonica sul quoziente e definiamo $\pi(X) = \alpha$ la classe laterale di X. Per definizione $\pi(P) = 0$ ma, dato che π è un omomorfismo, si ha anche $\pi(P) = P(\alpha)$ dunque $P(\alpha) = 0$ e abbiamo trovato un campo (estensione di K perché K è isomorfo a $\pi(K)$ che è un sottocampo di $K[X]/(P)$) che contiene una radice di P.

Visto che i due problemi iniziali hanno offerto poca resistenza proviamo a "raffinare la ricerca" per analizzare più da vicino la struttura di queste estensioni.

Sia K un campo e sia $\alpha \in F \supset K$ algebrico su K, vogliamo cercare il più piccolo campo che contenga sia K che α. Un campo che li contenga entrambi si può trovare considerando l'anello

$$K(\alpha) = \left\{ \sum_{n \geq 0} a_i \alpha^i \ : \ a_i \in K \text{ e } a_i = 0 \text{ per quasi ogni } i \right\} .$$

Osserviamo che $K(\alpha)$ è il più piccolo anello contenente K ed α (perché ?) ed è un dominio. Dunque il suo campo delle frazioni $Q(K(\alpha))$ è un campo contenente K ed α. L'operazione di passaggio al campo dei quozienti è però superflua come dimostra il seguente

Teorema 2.5.3 *Se α è algebrico su K allora $K(\alpha)$ è un campo.*

Dim. Definiamo $\varphi : K[X] \longrightarrow K(\alpha)$ tramite la formula $\varphi(P) = P(\alpha)$. La mappa φ è un omomorfismo surgettivo di anelli, inoltre, se $P_\alpha \in K[X]$ è il polinomio minimo di α su K allora $Ker\, \varphi = (P_\alpha)$. Dunque per il Teorema 2.3.6 si ha un isomorfismo $K(\alpha) \simeq K[X]/(P_\alpha)$. Infine P_α è irriducibile $\Longrightarrow$ (P_α) è massimale e quindi $K[X]/(P_\alpha)$ è un campo. $\square$

L'isomorfismo del Teorema mostra concretamente la struttura di $K(\alpha)$ legando somme, prodotti e inversi di quel campo agli analoghi elementi di $K[X]/(P_\alpha)$, un campo nel quale (una volta conosciuto P_α) si possono fare i calcoli con le classi resto.

Esempio Sia $\alpha = \sqrt[3]{2} \in \mathbb{R}$ con polinomio minimo su $\mathbb{Q}$ dato da $P_\alpha = X^3 - 2$. Sia $\alpha^4 + \alpha^3 + 2\alpha^2 - \alpha + 1 \in \mathbb{Q}(\alpha)$, dato che $\alpha^3 = 2$ si ha

$$\alpha^4 + \alpha^3 + 2\alpha^2 - \alpha + 1 = 2\alpha + 2 + 2\alpha^2 - \alpha + 1 = 2\alpha^2 + \alpha + 3$$

e questa operazione corrisponde a prendere il polinomio $Q = X^4 + X^3 + 2X^2 - X + 1 \in \mathbb{Q}[X]$ modulo P_α . Infatti facendo la divisione si ottiene

$$Q = (X^3 - 2)(X + 1) + 2X^2 + X + 3 \equiv 2X^2 + X + 3 \pmod{P_\alpha} .$$

L'inverso di $2\alpha^2+\alpha+3$ si trova cercando l'inverso di $2X^2+X+3$ in $\mathbb{Q}[X]/(P_\alpha)$ (e ricordando che α corrisponde alla classe di X nel quoziente).
Procedendo con l'algoritmo di Euclide e l'identità di Bezout si ottiene

$$1 = \frac{1}{5}(X^3 - 2)(2X - 1) + \frac{1}{5}(2X^2 + X + 3)(-X^2 + X + 1) .$$

Dunque $(2\alpha^2 + \alpha + 3)^{-1} = \frac{1}{5}(-\alpha^2 + \alpha + 1)$.

In particolare ogni elemento di $K(\alpha)$ si può scrivere come $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ dove $a_i \in K$ ed $n = \deg P_\alpha$. Tramite la mappa $f : K(\alpha) \longrightarrow K^n$ definita da

$$f\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

si dimostra che $K(\alpha)$ è isomorfo ad uno spazio vettoriale di dimensione n su K.

Definizione 2.5.4 Siano $F \supset K$ due campi. Si dice *grado* di F su K, e si indica con $[F : K]$, la dimensione di F come spazio vettoriale su K. Se $\alpha \in F$ è algebrico su K con polinomio minimo P_α di grado n allora $[K(\alpha) : K] = n$ ed α si dice *algebrico di grado n* su K.

Proposizione 2.5.5 *Sia $\alpha \in F \supset K$. Allora α è algebrico su K se e solo se $[K(\alpha) : K] < \infty$ (equivalentemente α è algebrico su K se e solo se è contenuto in una estensione finita di K).*

Dim. ($\Longrightarrow$) Già visto che α algebrico $\Longrightarrow [K(\alpha) : K] = \deg P_\alpha$.
($\Longleftarrow$) Supponiamo che $[K(\alpha) : K] = n < \infty$, allora $1, \alpha, \alpha^2, \ldots, \alpha^n$ sono $n + 1$ elementi di $K(\alpha)$ (spazio vettoriale di dimensione n su K) $\Longrightarrow$ sono linearmente dipendenti su K. Quindi $\exists\, a_0, \ldots, a_n \in K$ non tutti nulli, tali che $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ e dunque α è radice del polinomio $a_0 + a_1X + \cdots + a_nX^n \in K[X]$. $\square$

Proposizione 2.5.6 *Siano $L \supset F$ ed $F \supset K$ due estensioni di campi di grado finito. Allora $L \supset K$ è un'estensione di grado $[L : K] = [L : F][F : K]$.*

Dim. Basta prendere una base di L come spazio vettoriale su F ed una base di F come spazio vettoriale su K. I prodotti tra gli elementi di queste due basi formano una base di L come spazio vettoriale su K (dimostrazione standard di algebra lineare, vd per esempio [1] Teorema 5.1.1). $\square$

Corollario 2.5.7 *Siano $F \supset K$ campi. Gli elementi di F che sono algebrici su K formano un sottocampo di F.*

Dim. Siano $\alpha, \beta \in F$ algebrici su K allora $[K(\alpha) : K]$ e $[K(\beta) : K]$ sono finiti. Dobbiamo dimostrare che anche $\alpha + \beta$, α^{-1} (se $\alpha \neq 0$) ed $\alpha\beta$ sono

algebrici su K. Osserviamo che β è anche algebrico su $K(\alpha)$ e, ovviamente, $[K(\alpha)(\beta) : K(\alpha)] \leq [K(\beta) : K]$. Dunque $[K(\alpha)(\beta) : K] \leq [K(\alpha) : K][K(\beta) : K]$ è finito ed ogni elemento di $K(\alpha)(\beta)$ è algebrico su K. Quindi $\alpha+\beta$, α^{-1} ed $\alpha\beta$ sono algebrici su K. $\square$

Esempio $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ perché $\sqrt{2}$ è radice di $X^2 - 2$ che è irriducibile in $\mathbb{Q}[X]$. In $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ non c'è nessun elemento α tale che $\alpha^2 = 3$ (dimostrarlo) dunque $X^2 - 3$ è irriducibile in $\mathbb{Q}(\sqrt{2})[X] \Longrightarrow [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ e quindi $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}] = 4$.

Il procedimento di estensione di un campo è utile anche per la fattorizzazione dei polinomi. In effetti trovare una radice α di un polinomio P significa trovarne un fattore (sicuramente irriducibile) $X - \alpha$. Per esempio $X^2 + 1$ è irriducibile in $\mathbb{Q}[X]$ ma si fattorizza in $(X + i)(X - i)$ in $\mathbb{Q}(i)[X]$.
Aggiungendo progressivamente le radici di un polinomio irriducibile (che, in caratteristica 0, sono tutte di molteplicità 1) si può trovare un'estensione del campo di partenza in cui il polinomio ha tutte le sue radici e, quindi, si fattorizza in prodotto di polinomi di grado 1.
Concretamente dato un polinomio $P \in K[X]$ irriducibile si considera $F_1 = K[X]/(P)$ dove P ha una radice α corrispondente alla classe di X. Allora in $F_1[X]$ il polinomio P si fattorizza come $(X - \alpha)^d P_1$. Se tutte le radici di P_1 (e quindi anche quelle di P) sono in F_1 allora abbiamo finito: la fattorizzazione di P in $F_1[X]$ contiene solo irriducibili di grado 1. Altrimenti P_1 avrà almeno un fattore irriducibile $Q \in F_1[X]$ di grado ≥ 2. Si considera il campo $F_2 = F_1[X]/(Q)$ dove troviamo una radice di P_1 (e quindi di P) e si itera il procedimento fino a quando non si riesce a fattorizzare P in polinomi di grado 1.

Definizione 2.5.8 Sia $P \in K[X]$, si dice *campo di spezzamento* di P su K la più piccola estensione di K che contiene tutte le radici di P o, equivalentemente, il più piccolo campo F tale che P si fattorizza in prodotto di polinomi di grado 1 in $F[X]$.

Osservazione 2.5.9 Vista l'arbitrarietà nell'aggiungere radici, può sorprendere il fatto che si sia usato l'articolo "il" per il campo di spezzamento di P. A priori un cambiamento nell'ordine in cui vengono aggiunte le radici potrebbe produrre un campo diverso. In realtà si può dimostrare (non lo faremo in queste note ma vd [1] Teorema 5.3.4) che due campi di spezzamento dello stesso polinomio P sono isomorfi.

Esempi

1. $P = X^3 - 2$ è irriducibile in $\mathbb{Q}[X]$ e le sue radici sono $\sqrt[3]{2} \in \mathbb{R}$, $\zeta_3\sqrt[3]{2}$ e $\zeta_3^2\sqrt[3]{2}$ dove ζ_3 è una radice cubica di 1. Osserviamo che $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ perché $\zeta_3 \in \mathbb{C} - \mathbb{R}$. Dunque il campo di spezzamento è $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Inoltre ζ_3 ha grado 2 su $\mathbb{Q} \Longrightarrow$ ha grado 2 anche su $\mathbb{Q}(\sqrt[3]{2})$ (sicuramente tale grado è ≤ 2, perché è $\neq 1$?) e dunque $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$.

2. Il polinomio $X^n - 1$ non è irriducibile in $\mathbb{Q}[X]$ per nessun $n \geq 2$. Le sue radici sono gli elementi dell'insieme

$$U_n = \{\alpha \in \mathbb{C} : \alpha^n = 1\} =< e^{\frac{2\pi i}{n}} >=< \zeta_n > ,$$

   quindi il campo $\mathbb{Q}(\zeta_n)$ contiene già tutte le radici del polinomio dato. Per $n = 1$ o 2 si ha $\mathbb{Q}(\zeta_n) = \mathbb{Q}$ ma per $n \geq 3$ il campo $\mathbb{Q}(\zeta_n)$ è un'estensione propria di $\mathbb{Q}$. Il campo di spezzamento di P si dice *campo ciclotomico* (n-esimo) e si può dimostrare che ha grado $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

3. Sia $P = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$. Calcolando le radici si ottiene $X^2 = 5 \pm 2\sqrt{6}$ e quindi $X = \pm(\sqrt{2} + \sqrt{3})$, $\pm(\sqrt{2} - \sqrt{3})$ e P è irriducibile in $\mathbb{Q}[X]$. Il suo campo di spezzamento deve contenere $\sqrt{2} + \sqrt{3}$ e deve avere grado almeno 4 su $\mathbb{Q} \Longrightarrow$ tale campo è $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2.6 Campi finiti

Sia K un campo finito (esempio: $\mathbb{Z}/p\mathbb{Z}$ per ogni p primo), allora la caratteristica di K deve essere > 0, dunque un numero primo p. Dato che $0, 1, 1+1 = 2, \ldots, 1 + \cdots + 1 = p - 1 \in K$ si ha un inclusione $\mathbb{Z}/p\mathbb{Z} \subset K$ e, quindi, K è un'estensione finita di $\mathbb{Z}/p\mathbb{Z}$. Il campo K è uno spazio vettoriale di dimensione finita $[K : \mathbb{Z}/p\mathbb{Z}]$ su $\mathbb{Z}/p\mathbb{Z}$ e dunque $o(K) = p^{[K:\mathbb{Z}/p\mathbb{Z}]}$.
Se K è un campo finito allora K^* è un gruppo finito di invertibili in un campo $\Longrightarrow$ per il Teorema dell'elemento primitivo, K^* è ciclico generato da un qualche $\alpha \in K^*$. Quindi $K = K^* \bigcup \{0\} =< \alpha > \bigcup \{0\}$ e, se $o(K) = p^n$, si ha $o(\alpha) = p^n - 1 = o(K^*)$.

Lemma 2.6.1 *Sia $X^{p^n} - X = P_n \in \mathbb{Z}/p\mathbb{Z}[X]$ con p primo e sia K un campo finito di caratteristica p con p^n elementi (cioè di grado n su $\mathbb{Z}/p\mathbb{Z}$). Allora*

1. *le radici di P_n formano un campo di caratteristica p con p^n elementi;*

2. *il campo K è il campo di spezzamento di P_n su $\mathbb{Z}/p\mathbb{Z}$.*

Dim. **1.** Sia F_n l'insieme delle radici di P_n (che sarà contenuto in un qualche campo L), ovviamente $0, 1 \in F_n$. Siano $x, y \in F_n$ dobbiamo dimostrare che $x + y, xy \in F_n$ e che, se $x \neq 0$, allora $x^{-1} \in F_n$. In effetti

$$(x+y)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} x^i y^{p^n - i} = x^{p^n} + y^{p^n} = x + y$$

perché p divide i coefficienti binomiali per $1 \leq i \leq p^n - 1$ e siamo in caratteristica p. Per il prodotto e gli inversi la verifica è banale.
2. Abbiamo già visto che il polinomio P_n ha radici distinte, dunque ha p^n radici. Sia $\beta \in K$, allora, se $\beta = 0$, è ovvio che è una radice di P_n . Se invece $\beta \neq 0$ allora $\beta \in K^* =< \alpha >$ cioè $\beta = \alpha^h$ per qualche $h \in \mathbb{N}$. Allora

$$\beta^{p^n} = (\alpha^h)^{p^n} = \alpha^{p^n}\alpha^{p^n} \cdots \alpha^{p^n} \ (h \text{ volte}) \ = \alpha\alpha \cdots \alpha \ (h \text{ volte}) \ = \alpha^h = \beta \ .$$

Quindi ogni elemento di K è radice di $P_n \Longrightarrow$ dato che le cardinalità sono le stesse, K è l'insieme di tutte e sole le radici di P_n ed è ovviamente il più piccolo campo che contiene tutte le radici di P_n , cioè il campo di spezzamento. $\square$

Ricordando che due campi di spezzamento dello stesso polinomio sono isomorfi si giunge al seguente

Teorema 2.6.2 *Siano p un primo ed n un intero positivo. Allora $\exists\,!$ campo con p^n elementi ed è il campo di spezzamento di $X^{p^n} - X$ su $\mathbb{Z}/p\mathbb{Z}$. Tale campo ha grado n su $\mathbb{Z}/p\mathbb{Z}$.*

Notazione Il campo con p^n elementi si indica con $\mathbb{F}_{p^n}$.

Corollario 2.6.3 *Siano p un primo ed n un intero positivo. Allora $\exists\, P \in \mathbb{Z}/p\mathbb{Z}[X]$ irriducibile di grado n.*

Dim. Sia $\mathbb{F}^*_{p^n} =< \alpha >$, è sufficiente considerare il polinomio minimo P di α su $\mathbb{Z}/p\mathbb{Z}[X]$. $\square$

Polinomi irriducibili

Da quanto visto fino ad adesso dovrebbe risultare chiara l'importanza dei polinomi irriducibili, non solo per le fattorizzazioni ma anche per la costruzione di estensioni di campi. Almeno in $\mathbb{Z}[X]$ abbiamo dei criteri che ci consentono di individuare alcuni polinomi irriducibili.

1. *Criterio di Eisenstein.* Sia A un UFD e sia $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polinomio primitivo. Se $\exists\, \alpha \in A$ primo tale che:

i) $\alpha \nmid a_n$;

ii) $\alpha | a_i$ per $0 \leq i \leq n-1$;

iii) $\alpha^2 \nmid a_0$,

allora P è irriducibile in $A[X]$.
Dim. Se $P = QR$ con $Q = b_0 + b_1 X + \cdots + b_k X^k$ ed $R = c_0 + c_1 X + \cdots + c_h X^h$ in $A[X]$ allora $b_k c_h = a_n \Longrightarrow \alpha \nmid b_k$ ed $\alpha \nmid c_h$, dunque esistono coefficienti di Q ed R non divisibili per α. Inoltre $\alpha \parallel a_0 = b_0 c_0 \Longrightarrow \alpha$ divide solo uno dei due. Supponiamo $\alpha | c_0$ ed $\alpha \nmid b_0$ (l'altro caso è simmetrico) e sia j il minimo indice per cui $\alpha \nmid c_j$ (notare $0 < j \leq h$). Il coefficiente di X^j in $QR = P$ è $b_0 c_j + b_1 c_{j-1} + \cdots + b_j c_0 = a_j$ ed è divisibile per α per l'ipotesi *ii)*. Ma $\alpha | b_1 c_{j-1} + \cdots + b_j c_0$ ed $\alpha \nmid b_0 c_j$ (entrambe per la definizione di j) $\Longrightarrow \alpha \nmid a_j$: contraddizione. Dunque P non può essere riducibile.

2. Sia A un UFD e sia $Q(A)$ il suo campo dei quozienti. Sia $P \in A[X]$ primitivo, allora P è irriducibile in $A[X] \iff P$ è irriducibile in $Q(A)[X]$.
Dim. ($\Longleftarrow$) Ovvio.
($\Longrightarrow$) Se $P = QR$ con $Q, R \in Q(A)[X]$ allora possiamo scrivere $Q = \frac{a}{b} Q_1$ ed $R = \frac{c}{d} R_1$ con $a, b, c, d \in A$, $bd \neq 0$ e $Q_1 , R_1 \in A[X]$ primitivi. Allora $bdP = acQ_1 R_1$ ed il Lemma di Gauss (Lemma 2.4.12) $\Longrightarrow bd = ac$, dunque $P = Q_1 R_1$ è riducibile in $A[X]$: contraddizione.

3. Sia p un primo allora $P(X) = X^{p-1} + X^{p-2} + \cdots + 1$ è irriducibile in $\mathbb{Z}[X]$.
Dim. È facile vedere che $P(X)$ è irriducibile $\iff P(X+1)$ è irriducibile, infatti se $P(X+1) = Q(X)R(X)$ allora $P(X) = Q(X-1)R(X-1)$ [1]. Osserviamo che $P(X) = \frac{X^p - 1}{X - 1}$ e si ha

$$P(X+1) = \frac{(X+1)^p - 1}{X} = \frac{1}{X} \left(\sum_{i=0}^{p} \binom{p}{i} X^i - 1 \right) =$$

$$= \frac{1}{X} \left(\sum_{i=1}^{p} \binom{p}{i} X^i \right) = X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots + \binom{p}{2} X + \binom{p}{1} .$$

Basta osservare che il polinomio è monico, $p | \binom{p}{i}$ per $1 \leq i \leq p-1$, il termine noto è p ed usare il Criterio di Eisenstein.

4. Sia p un primo e sia $\zeta_p = e^{\frac{2\pi i}{p}}$ una radice p-esima di 1 in $\mathbb{C}$. Trovare il polinomio minimo di ζ_p in $\mathbb{Z}[X]$.

[1] **IMPORTANTE** questo vale per cambi di varabile lineari, per esempio $P(X) = X - 1$ è irriducibile ma $P(X^2) = X^2 - 1$ non lo è in $\mathbb{Z}[X]$

5. *Riduzione modulo α.* Sia $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ con A un UFD. Sia $\pi_\alpha : A[X] \longrightarrow A/(\alpha)[X]$ la proiezione definita dalla riduzione dei coefficienti modulo α. Se esiste un primo α tale che:

i) $\alpha \nmid a_n$,

ii) $\pi_\alpha(P)$ è irriducibile in $A/(\alpha)[X]$,

allora P è irriducibile in $A[X]$.
Dim. La proiezione π_α è un omomorfismo (verificarlo), dunque se $P = QR$ in $A[X]$ allora $\pi_\alpha(P) = \pi_\alpha(Q)\pi_\alpha(R)$. Dato che $\alpha \nmid a_n$ si ha deg $P =$ deg $\pi_\alpha(P)$ e lo stesso vale per Q ed R, dunque $\pi_\alpha(P) = \pi_\alpha(Q)\pi_\alpha(R)$ è una fattorizzazione non banale in $A/(\alpha)[X]$ (ricordare chi sono gli elementi invertibili di $A[X]$): contraddizione.

6. L'ipotesi $p \nmid a_n$ è necessaria. Per esempio $P = 2X^2 + 3X + 1 = (2X + 1)(X + 1)$ è riducibile mentre la sua proiezione su $\mathbb{Z}/2\mathbb{Z}[X]$ è $\pi_2(P) = X + 1$ che è irriducibile.

7. Dimostrare che $P = X^5+8X^4-7X^3-6X^2+2X+9 \in \mathbb{Z}[X]$ è irriducibile.
Dim. Consideriamo il primo $p = 2$ e sia $\pi_2(P) = X^5 + X^3 + 1$. Dato che P non ha radici in $\mathbb{Z}/2\mathbb{Z}$ non ci sono fattori di grado 1 nella fattorizzazione di $\pi_2(P)$, l'unica altra possibilità quindi è che sia il prodotto di un polinomio di grado 2 ed uno di grado 3. Siano $X^3 + aX^2 + bX + c$ e $X^2 + dX + e$ tali polinomi. Il loro prodotto è

$$X^5 + (a + d)X^4 + (e + ad + b)X^3 + (ae + bd + c)X^2 + (be + cd)X + ce$$

e, per avere l'uguaglianza con $\pi_2(P)$, dobbiamo risolvere il sistema

$$\begin{cases} ce = 1 \\ be + cd = 0 \\ ae + bd + c = 0 \\ e + ad + b = 1 \\ a + d = 0 \end{cases} \implies \begin{cases} c = e = 1 \\ b + d = 0 \\ a + bd + 1 = 0 \\ 1 + ad + b = 1 \\ a + d = 0 \end{cases}$$

La seconda e la quinta equazione insieme danno $a = b = d$. Dunque:
• se $a = b = d = 0$ si ha dalla terza equazione $0 = 1$ assurdo;
• se $a = b = d = 1$ si ha dalla terza equazione $0 = 1$ assurdo.
Dato che non ci sono soluzioni $\pi_2(P)$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$ e P è irriducibile in $\mathbb{Z}[X]$.

Polinomi irriducibili in $\mathbb{Z}/p\mathbb{Z}[X]$

Vogliamo trovare una fattorizzazione di $X^{p^n} - X$ in $\mathbb{Z}/p\mathbb{Z}[X]$ (ricordiamo che non ha fattori multipli) perché ciò servirà anche a calcolare il numero di polinomi irriducibili di grado d di $\mathbb{Z}/p\mathbb{Z}[X]$ per ogni d (da ora in avanti useremo la notazione per i campi finiti $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$).

1. Sia $P \in \mathbb{F}_p[X]$ irriducibile di grado d. Allora $P|(X^{p^n} - X) \iff d|n$.
Dim. ($\Longleftarrow$) Sia α una radice di P, allora $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d \Longrightarrow \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$, dunque $\alpha^{p^d} = \alpha$. Se $n = dh$ allora

$$\alpha^{p^n} = (\alpha^{p^d})^{p^{(h-1)d}} = (\alpha)^{p^{(h-1)d}} = (\alpha^{p^d})^{p^{(h-2)d}} = (\alpha)^{p^{(h-2)d}} = \cdots = \alpha \ ,$$

cioè α è una radice di $X^{p^n} - X \Longrightarrow P|X^{p^n} - X$.
($\Longrightarrow$) Sia α una radice di P, allora $P|X^{p^n} - X \Longrightarrow \alpha^{p^n} = \alpha$ e $\alpha \in \mathbb{F}_{p^n}$. Ma $\alpha \in \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$ dunque $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Sia $h = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]$ allora $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{F}_p] = hd$ e $d|n$.

Corollario 2.6.4 *Sia p un primo ed n un intero positivo. Allora la fattorizzazione di $X^{p^n} - X$ in $\mathbb{F}_p[X]$ è data da*

$$X^{p^n} - X = \prod_{\substack{P \text{ irriducibile} \\ \deg P = d \text{ e } d|n}} P \ .$$

Per esempio abbiamo già visto che dal (piccolo) Teorema di Fermat segue $X^p - X = X(X-1)\cdots(X-p+1)$ cioè il prodotto di tutti i polinomi irriducibili di grado 1 in $\mathbb{F}_p[X]$.

2. Calcolare il numero di polinomi irriducibili di $\mathbb{F}_p[X]$ di grado ≤ 5.
Dim. Sia n_i il numero di polinomi irriducibili di grado i di $\mathbb{F}_p[X]$. Ovviamente $n_1 = p$. Dal Corollario 2.6.4 segue che

$$X^{p^2} - X = \prod_{\substack{P \text{ irriducibile} \\ \deg P = 1}} P \prod_{\substack{Q \text{ irriducibile} \\ \deg Q = 2}} Q \ .$$

Quindi, confrontando i gradi, $p^2 = n_1 + 2n_2 \Longrightarrow n_2 = \frac{p^2-p}{2}$.
Analogamente per $i = 3$ si ha

$$X^{p^3} - X = \prod_{\substack{P \text{ irriducibile} \\ \deg P = 1}} P \prod_{\substack{Q \text{ irriducibile} \\ \deg Q = 3}} Q \ .$$

Dunque $p^3 = n_1 + 3n_3 \Longrightarrow n_3 = \frac{p^3-p}{3}$.
Per $i = 4$ si ha

$$X^{p^4} - X = \prod_{\substack{P \text{ irriducibile} \\ \deg P=1}} P \prod_{\substack{Q \text{ irriducibile} \\ \deg Q=2}} Q \prod_{\substack{R \text{ irriducibile} \\ \deg R=4}} R \ .$$

Dunque $p^4 = n_1 + 2n_2 + 4n_4 \Longrightarrow n_4 = \frac{p^4-p^2}{4}$.
Per $i = 5$ si ha

$$X^{p^5} - X = \prod_{\substack{P \text{ irriducibile} \\ \deg P=1}} P \prod_{\substack{Q \text{ irriducibile} \\ \deg Q=5}} Q \ .$$

Dunque $p^5 = n_1 + 5n_5 \Longrightarrow n_5 = \frac{p^5-p}{5}$.
Ovviamente si può continuare per ogni i stando attenti a non dimenticarsi nessun divisore d di i.

3. Calcolare

$$\prod_{a \in \mathbb{F}_{p^n}^*} a \quad \text{e} \quad \sum_{a \in \mathbb{F}_{p^n}} a \ .$$

Dim. Sappiamo che gli elementi di $\mathbb{F}_{p^n}$ sono tutte e sole le radici di $X^{p^n} - X$, dunque

$$X^{p^n} - X = \prod_{a \in \mathbb{F}_{p^n}} (X - a) = X \prod_{a \in \mathbb{F}_{p^n}^*} (X - a) \ .$$

Quindi $\prod_{a \in \mathbb{F}_{p^n}^*} a$ è il coefficiente del termine di grado 1 e $\sum_{a \in \mathbb{F}_{p^n}} a$ è il coefficiente del termine di grado $p^n - 1 \Longrightarrow$

$$\prod_{a \in \mathbb{F}_{p^n}^*} a = -1 \quad \text{e} \quad \sum_{a \in \mathbb{F}_{p^n}} a = 0 \ .$$

Qualche campo di spezzamento - Esercizi

1. Sia $P = (X^2+1)^2+1 = X^4+2X^2+2$. Trovare il suo campo di spezzamento F su $\mathbb{Q}$ e su $\mathbb{F}_5$.
Dim. P è irriducibile su $\mathbb{Q}$ (Eisenstein con $p = 2$). Sia α una radice di P allora è facile vedere che $-\alpha$, $\overline{\alpha}$ e $-\overline{\alpha}$ (dove $\overline{\alpha}$ è il coniugato di α) sono radici di P, se sono distinte allora abbiamo tutte le radici di P. Sicuramente $\alpha \neq -\alpha$ perché $\alpha \neq 0$, si ha $\alpha = \overline{\alpha} \iff \alpha \in \mathbb{R}$ ma, $\alpha^4 + 2\alpha^2 + 2 = 0 \Longrightarrow \alpha^2 = -1 \pm i \Longrightarrow \alpha \notin \mathbb{R}$. Infine $\alpha = -\overline{\alpha} \iff \alpha = ib$ per qualche $b \in \mathbb{R}$, ma, anche in questo caso, non è possibile che $(ib)^2 = -b^2 = -1 \pm i$. Dunque

il campo $\mathbb{Q}(\alpha)$ è il campo di spezzamento di P su $\mathbb{Q}$ ed ha grado 4 su $\mathbb{Q}$ (perché P è irriducibile).
In $\mathbb{F}_5$, 1 e -1 sono radici di P, infatti $X^4+2X^2+2=(X^2-1)(X^2+3)$. Dunque, dato che X^2+3 è irriducibile in $\mathbb{F}_5[X]$, il campo di spezzamento di P su $\mathbb{F}_5$ è $\mathbb{F}_5(\sqrt{-3})$. Dato che $[\mathbb{F}_5(\sqrt{-3}):\mathbb{F}_5]=2$ deve essere $\mathbb{F}_5(\sqrt{-3})=\mathbb{F}_{25}$.

2. Sia $P=X^p-X+a\in\mathbb{F}_p[x]$. Dimostrare che è irriducibile per ogni $a\neq 0$ e trovare il campo di spezzamento F.
Dim. Sia α una radice di P dunque $\alpha^p-\alpha+a=0$. Per ogni $i=0,\dots,p-1$ si ha

$$(\alpha+i)^p-(\alpha+i)+a=\alpha^p+i^p-\alpha-i+a=i^p-i=0\ .$$

Dunque $\alpha,\dots,\alpha+p-1$ sono tutte le radici di P e, dato che α non è in $\mathbb{F}_p$ (perché ?), il campo di spezzamento è $\mathbb{F}_p(\alpha)$.
Inoltre, dato che $P=\prod_{i=0}^{p-1}(X-\alpha-i)$, se $P=QR$ con $Q,R\in\mathbb{F}_p[X]$ allora Q è del tipo $Q=\prod_{j=1}^{d}(X-\alpha-i_j)$ ed il coefficiente del termine di grado $d-1$ di Q è $\sum_{j=1}^{d}(-\alpha-i_j)=-d\alpha-(i_1+\cdots+i_d)$. Perché tale coefficiente sia in $\mathbb{F}_p$ deve essere $\alpha\in\mathbb{F}_p$: contraddizione. Dunque P è irriducibile e $F=\mathbb{F}_p(\alpha)=\mathbb{F}_{p^p}$.

3. Sia $P=X^n-a\in\mathbb{Q}[X]$ ($n\geq 3$), supponiamo sia irriducibile e con $a>0$. Trovare il suo campo di spezzamento F su $\mathbb{Q}$.
Dim. Sia $\zeta_n=e^{\frac{2\pi i}{n}}$ una radice primitiva n-esima di 1. Allora le radici di P sono $\alpha=\sqrt[n]{a}\in\mathbb{R}$, $\zeta_n\alpha$, $\zeta_n^2\alpha,\dots,\zeta_n^{n-1}\alpha$. Inoltre $\mathbb{Q}(\alpha)\subset\mathbb{R}$ e $\zeta_n\in\mathbb{C}-\mathbb{R}\Longrightarrow\zeta_n\notin\mathbb{Q}(\alpha)$. Dunque $F=\mathbb{Q}(\alpha,\zeta_n)$, per calcolarne il grado si deve tener conto del fatto che $[\mathbb{Q}(\alpha):\mathbb{Q}]=n$ e $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\phi(n)$, ma non è automaticamente vero che $[F:\mathbb{Q}]=n\phi(n)$, bisognerebbe dimostrare che il polinomio minimo di ζ_n su $\mathbb{Q}$ è ancora irriducibile in $\mathbb{Q}(\alpha)[X]$ (cosa assolutamente non banale, questa difficoltà viene superata dall'applicazione della teoria di Galois che però è al di là degli scopi di queste note).

4. Sia p un primo $p\equiv 1\pmod 4$. Dimostrare che X^4+1 è riducibile in $\mathbb{F}_p[X]$.
Dim. Sia α un generatore di $\mathbb{F}_p^*$, allora $o(\alpha)=p-1\Longrightarrow o(a^{\frac{p-1}{2}})=2$ e l'unico elemento di ordine 2 in $\mathbb{F}_p$ è -1 (perchè è unico ?). Dunque $a^{\frac{p-1}{2}}=-1$ e

$$(X-a^{\frac{p-1}{4}})(X+a^{\frac{p-1}{4}})=X^4-a^{\frac{p-1}{2}}=X^4+1\ .$$

5. Sia $P=X^4+6\in K[X]$. Trovare il suo campo di spezzamento F su K per $K=\mathbb{Q},\mathbb{F}_2,\mathbb{F}_3,\mathbb{F}_5,\mathbb{F}_7,\mathbb{F}_{11},\mathbb{F}_{13}$ e calcolare $[F:K]$.
Dim. **5. a)** $K=\mathbb{Q}$: il polinomio P è irriducibile (Eisenstein). Sia α una radice di P, allora le radici sono $\alpha,-\alpha,i\alpha,-i\alpha$ e quindi $F=\mathbb{Q}(\alpha,i)$. Dato

che P è irriducibile si ha $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. Gli elementi di $\mathbb{Q}(\alpha)$ sono tutti del tipo $a\alpha^3+b\alpha^2+c\alpha+d$ con $a,b,c,d\in\mathbb{Q}$, vogliamo dimostrare che $i\notin\mathbb{Q}(\alpha)$ cioè che un'equazione del tipo $(a\alpha^3+b\alpha^2+c\alpha+d)^2=-1$ non ha soluzioni in $\mathbb{Q}$. Svolgendo i conti si ottiene (ricordando $\alpha^4=-6$)

$$-1=(a\alpha^3+b\alpha^2+c\alpha+d)^2=$$

$$=(2ad+2bc)\alpha^3+(c^2+2bd-6a^2)\alpha^2+(2cd-12ab)\alpha+d^2-6b^2-12ac\ .$$

che equivale al sistema

$$\begin{cases} 2ad+2bc=0 & E1\\ c^2+2bd-6a^2=0 & E2\\ 2cd-12ab=0 & E3\\ d^2-6b^2-12ac=-1 & E4 \end{cases}$$

Se $a=0$ allora $E1\Longrightarrow b=0$ o $c=0$. Se $b=0$ allora $E4\Longrightarrow d^2=-1$ che non ha soluzioni. Se $c=0$ allora $E2\Longrightarrow b=0$ o $d=0$ e quindi $E4\Longrightarrow d^2=-1$ o $-6b^2=-1$ che non hanno soluzioni. Dunque deve essere $a\neq 0$ ed $E1\Longrightarrow d=-\frac{bc}{a}$ mentre $E3\Longrightarrow b=\frac{cd}{6a}$, quindi $d=b\left(-\frac{c}{a}\right)=-\frac{dc^2}{6a^2}$. Allora $-\frac{c^2}{6a^2}=1$ o $d=0\Longrightarrow -c^2=6a^2$ o (dall'equazione $E2$) $c^2=6a^2$ che non hanno soluzioni in $\mathbb{Q}$.
Dunque $i\notin\mathbb{Q}(\alpha)$ e $[F:\mathbb{Q}(\alpha)]=2$ (perché ?), quindi $[F:\mathbb{Q}]=[F:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=8$.
5. b) $K=\mathbb{F}_2$ e $K=\mathbb{F}_3$: in entrambi i casi P si riduce a X^4 dunque ha unica radice 0 ed $F=K$.
5. c) $K=\mathbb{F}_5$: il polinomio P si riduce a X^4+1 e, dato che $5\equiv 1\pmod 4$, abbiamo visto nel punto **4** che P è riducibile. Si verifica facilmente che $\mathbb{F}_5^*=<2>$ dunque $X^4+1=(X^2+2)(X^2-2)$. Non ci sono radici in $\mathbb{F}_5$ ma, se α è tale che $\alpha^2=2$, allora $\alpha,-\alpha,2\alpha,-2\alpha$ sono tutte le radici di $P\Longrightarrow F=\mathbb{F}_5(\alpha)$ e $[F:\mathbb{F}_5]=2$ cioè $F=\mathbb{F}_{25}$.
5. d) $K=\mathbb{F}_7$: il polinomio P si riduce a $X^4-1=(X^2-1)(X^2+1)=(X+1)(X-1)(X^2+1)$ e X^2+1 è irriducibile in $\mathbb{F}_7[X]$. Dunque $F=\mathbb{F}_7(i)$, $[F:\mathbb{F}_7]=2$ ed $F=\mathbb{F}_{49}$.
5. e) $K=\mathbb{F}_{11}$: il polinomio P ha radici 2 e -2 in $\mathbb{F}_{11}$ e, dividendo per X^2-4, si ottiene la fattorizzazione $X^4+6=(X-2)(X+2)(X^2+4)$. Dato che X^2+4 è irriducibile in $\mathbb{F}_{11}[X]$ si ha $F=\mathbb{F}_{11}(\sqrt{-4})=\mathbb{F}_{11}(i)$, $[F:\mathbb{F}_{11}]=2$ ed $F=\mathbb{F}_{121}$.
5. f) $K=\mathbb{F}_{13}$: il polinomio P non ha radici in $\mathbb{F}_{13}$, l'unica altra possibilità di fattorizzazione è data dal prodotto di due polinomi di grado 2. Per avere

$$X^4+6=(X^2+aX+b)(X^2+cX+d)=$$

$$= X^4 + (a+c)X^3 + (b+d+ac)X^2 + (ad+bc)X + bd$$

(perché ci si può limitare ai polinomi monici ?) si deve risolvere il sistema

$$\begin{cases} a+c=0 & E1 \\ b+d+ac=0 & E2 \\ ad+bc=0 & E3 \\ bd=6 & E4 \end{cases}$$

Se $a=0$ allora $E2 \Longrightarrow b=-d$ ed $E4 \Longrightarrow -b^2=6$ che non ha soluzione in $\mathbb{F}_{13}$. Dunque $a \neq 0$ ed $E1 \Longrightarrow a=-c$, quindi $E3 \Longrightarrow b=d$ e, sostituendo in $E4$, si ottiene $b^2=6$ che non ha soluzione in $\mathbb{F}_{13}$.
Allora P è irriducibile e, se α è una radice di P, le radici sono $\alpha, -\alpha, 5\alpha, -5\alpha$ (5 è una radice di -1 in $\mathbb{F}_{13}$) quindi $F=\mathbb{F}_{13}(\alpha)$, $[F:\mathbb{F}_{13}]=4$ ed $F=\mathbb{F}_{13^4}$.

2.7 Esercizi di riepilogo

1. Sia A un anello commutativo con unità. Supponiamo che $\forall a \in A$ esista $n \in \mathbb{N}$, $n>1$ (dipendente da a) tale che $a^n=a$. Dimostrare che un ideale I di A è primo $\iff$ è massimale.

2. Sia $\mathbb{Z}[i]$ l'anello degli *interi di Gauss*. Sia $I \neq 0$ un ideale di $\mathbb{Z}[i]$. Dimostrare che $\mathbb{Z}[i]/I$ ha cardinalità finita.

3. Sia $\mathcal{M}(\mathbb{N},\mathbb{Z}) = \{ f : \mathbb{N} \longrightarrow \mathbb{Z} \}$ l'insieme delle funzioni da $\mathbb{N}$ in $\mathbb{Z}$ con le operazioni indotte da $\mathbb{Z}$, cioè

$$(f+g)(n) = f(n)+g(n) \qquad (fg)(n) = f(n)g(n) \quad \forall n \in \mathbb{N}\ .$$

a) Dimostrare che $\mathcal{M}(\mathbb{N},\mathbb{Z})$ è un anello commutativo con unità.

b) Dimostrare che $\mathcal{M}(\mathbb{N},\mathbb{Z})$ non è un dominio di integrità.

c) Descrivere gli insiemi dei divisori di zero e degli elementi invertibili di $\mathcal{M}(\mathbb{N},\mathbb{Z})$. Dimostrare che nessuno dei due è un ideale di $\mathcal{M}(\mathbb{N},\mathbb{Z})$.

d) Per ogni sottoinsieme X di $\mathbb{N}$ definiamo

$$I(X) = \{ f \in \mathcal{M}(\mathbb{N},\mathbb{Z}) : f(x)=0\ \forall x \in X \}\ .$$

Dimostrare che $I(X)$ è un ideale di $\mathcal{M}(\mathbb{N},\mathbb{Z})$.

e) Dimostrare che se $I(X)$ è primo allora X ha al più un elemento.

f) $I(\{0\})$ è primo ? $I(\{0\})$ è massimale ?

4. Sia $\mathcal{M}(\mathbb{N},\mathbb{R})$ definito in maniera analoga ad $\mathcal{M}(\mathbb{N},\mathbb{Z})$ dell'esercizio precedente. Rispondere alle stesse domande **a**), ..., **f**) dell'esercizio precedente per l'insieme $\mathcal{M}(\mathbb{N},\mathbb{R})$, verificando inoltre che ogni elemento di $\mathcal{M}(\mathbb{N},\mathbb{R})$ o è un divisore dello zero o è invertibile.

5. Sia

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathscr{M}(2,\mathbb{Q}) \right\} .$$

a) Dimostrare che A è un anello commutativo con unità.

b) Trovare A^* e l'insieme dei divisori dello zero.

c) Dimostrare che $A \simeq \mathbb{Q}[X]/(X^2)$.

6. Sia

$$A = \mathbb{Q}[X]/(X^5 - 2X^4 + X^3 + 2X^2 - 4X + 2) .$$

a) Trovare l'ideale dei nilpotenti di A. È un ideale primo ?

b) Trovare l'insieme dei divisori dello zero e dimostrare che non è un ideale.

7. Sia $P(X) = X^4 + 3X + 1 \in \mathbb{Q}[X]$.

a) Dimostrare che $A = \mathbb{Q}[X]/(P)$ è un campo.

b) Sia α una radice di P. Trovare l'inverso di $\alpha^2 + 1$ in $\mathbb{Q}(\alpha)$.

8. Sia $P(X) = X^4 + 3X + 1$.

a) Rispondere alle stesse domande dell'esercizio precedente considerando P come polinomio in $\mathbb{F}_2[X]$.

b) Dimostrare che $\mathbb{F}_3[X]/(P)$ ed $\mathbb{F}_5[X]/(P)$ non sono campi.

9. (Definizioni in Appendice 3.3) Sia $S = \{\, P(X) \in \mathbb{Q}[X] \,:\, P(0) \neq 0 \text{ e } P(1) \neq 0 \,\}$.

a) Dimostrare che S è un sistema moltiplicativo.

b) Trovare gli ideali primi di $S^{-1}\mathbb{Q}[X]$.

10. Sia $P(X) = X^2 + 2$.

a) Dimostrare che $\mathbb{F}_7[X]/(P)$ è un campo.

b) Sia α una radice di P. Calcolare l'ordine di $\alpha + 1$ in $(\mathbb{F}_7(\alpha))^*$.

c) Calcolare l'inverso di $\alpha + 1$ in $\mathbb{F}_7(\alpha)$.

d) Rispondere alle domande **b)** e **c)** per altri elementi $a + \alpha b \in (\mathbb{F}_7(\alpha))^*$ scelti a piacere.

e) Per quali $a \in \mathbb{F}_7$ l'anello $\mathbb{F}_7[X]/(X^2 - a)$ è un campo ?

11. Sia $\zeta_n = e^{\frac{2\pi i}{n}}$ $(n \geq 1)$ una radice primitiva n-esima dell'unità e sia $\Phi_n(X)$ il suo polinomio minimo in $\mathbb{Q}(X)$.

a) Scrivere $\Phi_1(X)$, $\Phi_2(X)$, $\Phi_3(X)$ e $\Phi_4(X)$.

b) Calcolare $\Phi_p(X)$ per ogni primo p.

c) Dimostrare che

$$\prod_{d|n} \Phi_d(X) \quad \text{divide} \quad X^n - 1 \ .$$

d) Dimostrare che $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ dove ϕ è la funzione di Eulero. (Sugg. induzione)

12. Sia K un campo, sia H un sottogruppo di $Aut(K)$ (gli automorfismi di K) e sia F un sottocampo di K.

a) Sia $K^H = \{\, \alpha \in K \,:\, \sigma(\alpha) = \alpha \ \forall \sigma \in H \,\}$. Dimostrare che K^H è un sottocampo di K.

b) Sia $G_F = \{\, \sigma \in Aut(K) \,:\, \sigma(\alpha) = \alpha \ \forall \alpha \in F \,\}$. Dimostrare che $G_F < Aut(K)$.

Capitolo 3

Appendici

3.1 Buon Ordinamento ed Induzione

I due "principi" di cui ci occuperemo adesso sono equivalenti (nel senso che prendendone uno come ipotesi si può dimostrare l'altro e viceversa) quindi la denominazione di "principio" o "teorema" è, sostanzialmente, una convenzione.

Principio del Buon Ordinamento (B.O.) *Ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ha un elemento minimo.*

Principio di Induzione (P.I.) *Sia* $P(n)$ *un'affermazione che abbia senso per ogni* $n \geq n_0$ *(*$n, n_0 \in \mathbb{N}$*). Se*

1. $P(n_0)$ *è vera;*

2. *per ogni* $n \geq n_0$ *,* $P(n)$ *vera* $\Longrightarrow P(n+1)$ *vera,*

allora $P(n)$ *è vera per ogni* $n \geq n_0$ *.*

Nel Principio di Induzione si può sostituire l'ipotesi **2** con la seguente

2a. per ogni $n \geq n_0$, $P(k)$ vera per ogni $n_0 \leq k \leq n \Longrightarrow P(n+1)$ vera.

Esercizio Dimostrare che **2** $\Longleftrightarrow$ **2a**.

Per coloro che trovano inappropriata l'espressione "abbia senso", sappiate che siete in ottima e numerosa compagnia ma qui non c'è né spazio né tempo

per addentrarsi in una disputa del genere (il Dipartimento di Filosofia è al Cubo 14). Ci accontentiamo di dimostrare l'equivalenza tra i due principi.

B.O.$\Longrightarrow$P.I. Sia $S \subset \{n \in \mathbb{N} : n \geq n_0\}$ il sottoinsieme dei numeri naturali per i quali $P(n)$ è falsa. Se $S = \emptyset$ abbiamo finito. Se invece $S \neq \emptyset$ allora per il **B.O.** S ha un minimo che chiamiamo m. Per l'ipotesi **1**, $m > n_0$ e, per definizione di minimo, $P(m-1)$ è vera (notare quindi che $m - 1 \geq n_0$). Ma allora **2**$\Longrightarrow P(m)$ è vera: contraddizione. Dunque S deve essere vuoto e $P(n)$ è vera per ogni $n \geq n_0$. $\square$

P.I.$\Longrightarrow$B.O. Sia $S \subset \mathbb{N}$ un insieme che non ha un minimo e sia $P(n)$ l'affermazione "Nessun numero naturale $\leq n$ appartiene ad S". Vogliamo dimostrare che $S = \emptyset$ o, equivalentemente, che $P(n)$ è vera per ogni $n \geq 0$. L'affermazione $P(0)$ è vera perché $P(0)$ falsa $\Longrightarrow 0 \in S$ e dunque 0 sarebbe il minimo di S: contraddizione. Supponiamo che $P(n)$ sia vera e controlliamo $P(n+1)$. Se $P(n+1)$ è falsa allora $\exists\, m \leq n+1$ tale che $m \in S$ ma, $P(n)$ vera $\Longrightarrow a \notin S$ per ogni $a \leq n$, quindi $m = n+1$ ed è il minimo di S: contraddizione. Dunque $P(n)$ vera $\Longrightarrow P(n+1)$ vera ed il **P.I.**$\Longrightarrow S = \emptyset$. $\square$

Esempi - Esercizi

1. Dimostrare che, per ogni $n \geq 0$,

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \ .$$

2. Dimostrare che, per ogni $n \geq 0$,

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \ .$$

La formula si può ricavare dallo sviluppo del binomio $(i+1)^3 = i^3 + 3i^2 + 3i + 1$. Sommando da 0 ad n si ottiene

$$\sum_{i=0}^{n} (i+1)^3 = \sum_{i=0}^{n} i^3 + \sum_{i=0}^{n} (3i^2 + 3i + 1) \ .$$

Dunque

$$\sum_{i=0}^{n} (i+1)^3 - \sum_{i=0}^{n} i^3 = (n+1)^3 = 3\sum_{i=0}^{n} i^2 + 3\sum_{i=0}^{n} i + \sum_{i=0}^{n} 1$$

e, sfruttando la formula dell'esercizio **1**,

$$\sum_{i=0}^{n} i^2 = \frac{(n+1)^3}{3} - \frac{n(n+1)}{6} - \frac{n+1}{3} = \frac{n(n+1)(2n+1)}{6} \ .$$

3. Calcolare le formule per $\sum_{i=0}^{n} i^3$ e $\sum_{i=0}^{n} i^4$ partendo da $(i+1)^4$ e $(i+1)^5$. Dimostrare (tramite induzione) le formule

$$\sum_{i=0}^{n} i^3 = \frac{n^2(n+1)^2}{4} \ ,$$

$$\sum_{i=0}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} \ .$$

4. Dimostrare che, per ogni $n \geq 0$, 5 divide $3^{4n} - 1$.

5. Sia $k \in \mathbb{N}$ fissato. Dimostrare che, per ogni $n \geq k$,

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1} \ .$$

6. *Polinomio di Newton.* Siano $a, b \in \mathbb{C}$, dimostrare che, per ogni $n \geq 0$,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \ .$$

7. Dimostrare che, per ogni n pari $n \geq 0$, 9 divide $5^n - 4^n$.

8. Dimostrare che, per ogni n dispari $n \geq 1$, 9 divide $5^n + 4^n$.

9. **Teorema** Tutte le persone hanno lo stesso stipendio.
Dim. Dimostriamo per induzione l'affermazione $P(n)$ "Preso un qualsiasi insieme di n persone, tutte le persone dell'insieme hanno lo stesso stipendio" che è ovviamente equivalente alla tesi. L'affermazione $P(1)$ è ovviamente vera. Supponiamo che $P(n)$ sia vera e consideriamo un insieme di $n+1$ persone $\{A_1, \ldots, A_{n+1}\}$. Per induzione negli insiemi $\{A_1 \ldots, A_n\}$ e $\{A_2, \ldots, A_{n+1}\}$ (entrambi composti da n persone) tutti hanno lo stesso stipendio, dunque

$$\text{Stipendio } A_{n+1} = \text{Stipendio } A_2 = \text{Stipendio } A_1$$

e tutti in $\{A_1, \ldots, A_{n+1}\}$ hanno lo stesso stipendio. $\square$

10. Se la dimostrazione del punto **9** vi convince, avete ancora molto da imparare (in generale, non solo dalla matematica), se non vi convince, quale è l'errore ?

3.2 Relazioni di equivalenza

Definizione 3.2.1 Sia E un insieme, una *relazione di equivalenza* su E è un sottoinsieme $\mathscr{R}$ di $E \times E$ che verifica le seguenti proprietà:

1. *riflessiva*, $\forall\, a \in E$ si ha che $(a, a) \in \mathscr{R}$;
2. *simmetrica*, $(a, b) \in \mathscr{R} \Longrightarrow (b, a) \in \mathscr{R}$;
3. *transitiva*, $(a, b) \in \mathscr{R}$ e $(b, c) \in \mathscr{R} \Longrightarrow (a, c) \in \mathscr{R}$.

Notazione Invece di $(a, b) \in \mathscr{R}$ scriveremo $a \sim_{\mathscr{R}} b$ o semplicemente $a \sim b$ se è chiara la relazione a cui ci si riferisce.

Esempi - Esercizi Verificare che le seguenti sono relazioni di equivalenza.

1. Su $\mathbb{Z}$ la congruenza modulo n (per ogni $n \geq 1$), cioè definiamo $a \sim b \iff n|a-b$. In questo caso $a \sim b$ si scrive canonicamente $a \equiv b \pmod{n}$.
2. Su $\mathbb{R}^n$ definiamo $P \sim Q \iff d(P, O) = d(Q, O)$ dove O è l'origine e d la distanza.
3. Su $\mathbb{Z}$ definiamo $a \sim b \iff a$ e b hanno gli stessi fattori primi (cioè $p|a \iff p|b$ per ogni primo p).

Definizione 3.2.2 Sia E un insieme con una relazione di equivalenza $\sim$. Sia $a \in E$, la *classe di equivalenza di* a è l'insieme $[a] = \{b \in E \,:\, a \sim b\}$ (l'insieme di tutti gli elementi di E equivalenti ad a).
Un *insieme di rappresentanti* per E (rispetto a $\sim$) è un sottoinsieme di E che contenga uno ed un solo elemento per ognuna delle classi di equivalenza di E. L'insieme delle classi di equivalenza di E si dice *insieme quoziente*.

Proposizione 3.2.3 *Sia E un insieme con una relazione di equivalenza $\sim$.*

1. *Siano $a, b \in E$ allora $[a] = [b]$ o $[a] \bigcap [b] = \emptyset$.*
2. *Se R è un insieme di rappresentanti per E allora*

$$E = \bigcup_{a \in R} [a] \ .$$

Dim. Esercizio. $\square$

Esempi - Esercizi Negli esempi precedenti le classi di equivalenza ed alcuni insiemi di rappresentanti sono:

1. le classi resto modulo n con rappresentanti gli interi $0, 1, \ldots, n-1$;

2. le sfere di centro l'origine con insieme di rappresentanti una qualsiasi semiretta partente dall'origine stessa;

3. un insieme di rappresentanti è dato da tutti gli insiemi finiti di primi distinti e, per ogni elemento $\{p_1, \ldots, p_k\}$ di tale insieme di rappresentanti, la classe di equivalenza è data da tutti gli interi del tipo $\prod_{i=1}^{k} p_i^{a_i}$ con $a_i \geq 1$ per ogni i.

Osservazione 3.2.4 Sia $E = \bigcup_{i \in I} E_i$ una decomposizione di E i sottoinsiemi disgiunti. Definiamo $a \sim b \iff \exists\, i \in I$ tale che $a, b \in E_i$ (verificare che è una relazione di equivalenza su E). Si ha dunque una corrispondenza biunivoca

$$\{\text{Relazioni di equivalenza su } E\} \leftrightarrow \left\{ \begin{array}{c} \text{Decomposizioni di } E \\ \text{in insiemi disgiunti} \end{array} \right\}.$$

Definizione 3.2.5 Sia E un insieme con un operazione $*$ ed una relazione di equivalenza $\sim$. Si dice che la relazione $\sim$ è *compatibile* con l'operazione $*$ se $a \sim b$ e $c \sim d$ implicano $a * c \sim b * d$.

Esempi - Esercizi Negli esempi precedenti si può verificare che:

1. la congruenza modulo n è compatibile con $+$ e $\cdot$ in $\mathbb{Z}$;

2. la relazione non è compatibile con la somma vettoriale su $\mathbb{R}^n$ data da $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$ (per esempio, per $n = 2$, $P_1 = (0, 1) \sim Q_1 = (1, 0)$ e $P_2 = (4, 3) \sim Q_2 = (5, 0)$ ma $P_1 + P_2 = (4, 4) \not\sim Q_1 + Q_2 = (6, 0)$);

3. la relazione data non è compatibile con $+$ (per esempio $2 \sim 4$ e $3 \sim 9$ ma $2 + 3 = 5 \not\sim 4 + 9 = 13$) ma è compatibile con $\cdot$ su $\mathbb{Z}$ (dimostrarlo).

3.3 Costruzione dei quozienti

In questa sezione (anche se non è strettamente necessario per definire gli anelli dei quozienti) supporremo sempre A dominio di integrità per semplificare notazioni e calcoli.

Definizione 3.3.1 Un sottoinsieme S di A si dice *sistema moltiplicativo* se:

1. $0 \notin S$ e $1 \in S$;
2. $\forall\, s_1\,, s_2 \in S$ si ha $s_1 s_2 \in S$.

Esempi - Esercizi

1. In $\mathbb{Z}$ l'insieme $\mathbb{Z} - \{0\}$ è un sistema moltiplicativo. In generale in un dominio A l'insieme $A - \{0\}$ è un sistema moltiplicativo.
2. Sia P un ideale primo di A, allora $S_P = A - P$ è un sistema moltiplicativo. Infatti $0 \in P$ e $1 \notin P \Longrightarrow 0 \notin S_P$ e $1 \in S_P$. Inoltre siano $s_1\,, s_2 \in S_P$ allora, per definizione di ideale primo, $s_1 s_2 \in S_P$.

Lemma 3.3.2 *Sia S un sistema moltiplicativo di un dominio A. Su $A \times S$ la relazione data da $(a, s) \sim (b, t) \iff at = bs$ è una relazione di equivalenza.*

Dim. Le proprietà riflessiva e simmetrica sono ovvie. Per la transitiva supponiamo $(a, s) \sim (b, t)$ e $(b, t) \sim (c, u)$ allora $at = bs$ e $bu = ct$, dunque $atu = bsu = sct \Longrightarrow t(au - cs) = 0$. Dato che $t \in S$ (quindi $t \neq 0$) ed A è un dominio, deve essere $au = cs$ cioè $(a, s) \sim (c, u)$. $\square$

L'insieme delle classi di equivalenza di $A \times S$ rispetto alla relazione definita nel Lemma 3.3.2 si indica con $S^{-1}A$ e, su tale insieme, possiamo definire delle operazioni indotte da quelle di A (per semplicità la classe di equivalenza di (a, s) verrà ancora indicata con (a, s)):
somma: $(a, s) + (b, t) = (at + bs, st)$;
prodotto: $(a, s)(b, t) = (ab, st)$.

Proposizione 3.3.3 *Con le operazioni appena definite $S^{-1}A$ è un anello che si definisce* anello dei quozienti *di A rispetto ad S. Se $S = A - \{0\}$ allora $S^{-1}A$ si indica anche con $Q(A)$, è un campo e si definisce* campo dei quozienti *di A.*

Dim. Si deve verificare che le operazioni sono ben definite e che soddisfano le proprietà di un anello o, nel caso di $Q(A)$, di un campo. Sono semplici applicazioni delle definizioni quindi diamo solo qualche breve accenno senza entrare troppo nei dettagli (è un'altra di quelle cose che il fantomatico "volenteroso lettore" dovrebbe fare "once in a lifetime").
• Somma ben definita: se $(a,s) \sim (b,t)$ e $(c,u) \sim (d,v)$ allora $at = bs$ e $cv = du$. Per definizione $(a,s)+(c,u) = (au+cs, su)$ e $(b,t)+(d,v) = (bv+dt, tv)$, inoltre

$$(au+cs)tv = atuv + cvts = bsuv + dust = (bv+dt)su$$

che implica $(au+cs, su) \sim (bv+dt, tv)$.
• Prodotto ben definito: analogo alla somma.
• Proprietà delle operazioni: seguono direttamente da quelle delle operazioni di A. L'elemento neutro per la somma è $(0,s)$, l'inverso di additivo di (a,s) è $(-a,s)$ e l'unità è $(1,1)$.
• $Q(A)$ è un campo: infatti se $a \neq 0$ allora $a \in S$ e si verifica che l'inverso moltiplicativo di (a,s) è (s,a). $\square$

Esempi

1. Usando (per comodità e consuetudine) la notazione $(a,s) = \frac{a}{s}$ è facile vedere che $Q(\mathbb{Z}) = \mathbb{Q}$.

2. Sia p un numero primo ed $S = \mathbb{Z} - (p)$, allora

$$S^{-1}\mathbb{Z} = \left\{ \frac{m}{n} \in \mathbb{Q} \; t.c. \; (n,p) = 1 \right\} .$$

3. Sia $a \in A - \{0\}$ ed $S = \{a^n : n \in \mathbb{N}\}$, allora

$$S^{-1}A = \left\{ \frac{b}{a^n} \; t.c. \; b \in S \text{ ed } n \in \mathbb{N} \right\} .$$

Definizione 3.3.4 Sia A un dominio di integrità e P un ideale primo. Sia $S_P = A - P$, allora $S_P^{-1}A$ si dice *localizzazione* di A in P e si indica anche con A_P.

Proposizione 3.3.5 *Sia S un sistema moltiplicativo in un dominio A. Sia $S^{-1}A$ l'anello quoziente e sia J un ideale di $S^{-1}A$. Allora $\exists\, I$ ideale di A tale che $J = S^{-1}I = \{(b,s) \in S^{-1}A : b \in I\}$. Inoltre se $I \bigcap S \neq \emptyset$ allora $S^{-1}I = S^{-1}A$.*

Dim. È facile vedere che se I è un ideale di A allora $S^{-1}I$ è un ideale di $S^{-1}A$. Inoltre se $\exists\, s \in I \bigcap S$ allora $(s,s) \sim (1,1) \in S^{-1}I$ e quindi $S^{-1}I = S^{-1}A$. Dato che $1 \in S$, per ogni $a \in A$ abbiamo $(a,1) \in S^{-1}A$. Definiamo allora $I = \{a \in A \ t.c. \ (a,1) \in J\}$. Si può verificare che I è un ideale di A e che $S^{-1}I \subset J$ (dimostrarlo). Per l'altra inclusione sia $(a,s) \in J$, allora $(a,s)(s,1) = (as,s) \sim (a,1) \in J \implies a \in I$ e dunque, per definizione, $J \subset S^{-1}I$. $\square$

Corollario 3.3.6 *Sia S un sistema moltiplicativo in un dominio A. Gli ideali di $S^{-1}A$ sono tutti e soli gli ideali $S^{-1}I$ con I ideale di A. Inoltre $S^{-1}I = S^{-1}A \iff I \bigcap S \neq \emptyset$.*

Esercizio Sia p un numero primo e sia $S_p = \mathbb{Z} - (p)$. Quali sono tutti gli ideali di $S_p^{-1}\mathbb{Z}$?

Bibliografia

[1] I.N. Herstein *Algebra*, Editori Riuniti, V Edizione (2003).

[2] S. Lang *Algebra*, **GTM 211**, Springer-Verlag (2002).