Aritmetica e Algebra I

Mirko Torresani

29 febbraio 2024

Indice

Indice **2**

Introduzione **5**

1 Combinatoria **7**

1.1 Principio di Induzione 7
1.2 Prime Nozioni di Cardinalità 11
1.3 Coefficiente Binomiale 16
1.4 Formula di Inclusione-Esclusione 21
1.5 Stars and Bars & Double Counting 23

2 Teoria dei Numeri **27**

2.1 Relazioni d'Ordine 27
2.2 Divisione Euclidea 28
2.3 Equazioni Diofantee Lineari 33
2.4 Primi e Irriducibili 36
2.5 Classi di Resto 39
2.6 Congruenze Lineari 42
2.7 Sistemi di Congruenze 44
2.8 Congruenze di Grado Superiore 51
2.9 Operazioni su $\mathbb{Z}/n\mathbb{Z}$ 53
2.10 Funzioni Aritmetiche 56
2.11 La φ di Eulero 59
2.12 Congruenze Esponenziali 63

2.13 Idem- e Nilpotenti 66
2.14 Quadrati Modulo p 68
2.15 Miscellanea 70

3 Gruppi **77**
3.1 Prime Definizioni 77
3.2 Gruppi Ciclici 85
3.3 Omomorfismi di Gruppi 89
3.4 Omomorfismi tra Gruppi Ciclici 97
3.5 Prodotto Diretto 102
3.6 Classi Laterali 104
3.7 Gruppi di Ordine Piccolo 107
3.8 Quozienti di Gruppi 116
3.9 Gruppi Abeliani Finiti 129
3.10 Il Gruppo $\mathbb{Z}/n\mathbb{Z}^*$ 133
3.11 Presentazione di Gruppi 139
3.12 Il Gruppo D_n 150
3.13 Automorfismi di un Gruppo 155
3.14 Azioni di Gruppo e Formula delle Classi 161
3.15 Gruppi di ordine p^n 171
3.16 Il Gruppo S_n 175
3.17 Sottogruppo Derivato 181
3.18 Prodotti Semidiretti 182
3.19 Gruppi Abeliani Finiti 187
3.20 Teoremi di Sylow 196
3.21 Il Gruppo Q_8 205
3.22 Gruppi Semplici 210

4 Anelli **219**
4.1 Prime Definizioni 219
4.2 L'anello dei Polinomi 221
4.3 Polinomi su un Campo 223
4.4 Polinomi su $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{Q}$ 226
4.5 Quozienti di $K[x]$ 229
4.6 Ideali 231
4.7 Anelli Quoziente 235

4.8 Localizzazioni 240
4.9 Domini Euclidei e a Ideali Principali 245
4.10 Domini a Fattorizzazione Unica 250
4.11 Gli interi di Gauss $\mathbb{Z}[i]$ 258

5 Campi **259**

6 Estensioni di Campi **261**

7 Costruzioni con Riga e Compasso **263**

8 Risolubilità per Radicali **265**

A Dimostrazioni Postposte **267**
A.1 Il Teorema di Cantor-Bernstein-Schröder 267
A.2 Automorfismi di S_n 268
A.3 Teorema di Wedderburn 271
A.4 Dominio a Ideali Principali non Euclideo 273

Bibliografia **279**

Introduzione

Queste pagine raccolgono la teoria presentata dai professori Ilaria del Corso e Davide Lombardo nei corsi di Aritmetica e Algebra I.

La teoria di queste pagine non viene presentata in ordine di corso, ma in ordine di argomento. I primo capitolo riguarda le prime nozioni di Combinatoria relative al corso di Aritmetica. Successivamente si analizzano i primi teoremi di Teoria dei Numeri, in particolare le classi di resto e il teorema cinese del resto. Questo funge da introduzione per la teoria dei gruppi, degli anelli e dei campi relativa ai corsi di Aritmetica e Algebra I. Infine si parlerà di estensioni di campi ed estensioni di Galois, nozioni affrontate specialmente nel corso di Teoria di Campi e di Galois.

Successivamente troviamo le costruzioni con riga e compasso e la risolubilità per radicali, che mostrano la potenza delle teorie sviluppate da Galois.

Infine queste pagine si chiudono con un appendice, che contiene fatti e teoremi complementari, non rientrano nel programma ufficiale dei corsi, ma presentate per ragioni di completezza. Contengono sia complementi presentati dai professori sia dimostrazioni di teoremi da me ricercate.

Buona lettura e buona scoperta del magico mondo dell'Algebra!

Capitolo 1

Combinatoria

1.1 Principio di Induzione

Il primo oggetto del nostro studio è l'insieme $\mathbb{N}$ dei numeri naturali. Li consideriamo già definiti e in particolare possedenti tutte le proprietà date dagli assiomi di Peano. Una loro proprietà, per noi fondamentale, è il *principio del buon ordinamento.*

Fatto 1.1.1 (Principio del Buon Ordinamento)**.** *Ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ammette minimo.*

Di fondamentale importanza è anche il *principio di induzione*, che enunciamo in due forme.

Fatto 1.1.2 (Principio di Induzione - I forma o Debole)**.** *Sia* P *una proprietà definita per i naturali maggiori o uguali di* n_0*. Supponiamo che valgono le seguenti:*

1. $P(n_0)$ *è vera,*
2. *Per ogni naturale maggiore o uguale a* n_0*, se* $P(k)$ *è vera anche* $P(k+1)$ *lo è.*

Allora $P(n)$ *è vera per ogni naturale maggiore o uguale a* n_0*.*

Fatto 1.1.3 (Principio di Induzione - II forma o Forte)**.** *Sia* P *una proprietà definita per i naturali maggiori o uguali di* n_0*. Supponiamo che valgono le seguenti:*

1. *$P(n_0)$ è vera.*

2. *Per ogni naturale k maggiore o uguale a n_0, se $P(n)$ è vera per ogni naturale $n_0 \leq n \leq k$ allora anche $P(k+1)$ è vera.*

Allora $P(n)$ è vera per ogni naturale maggiore o uguale a n_0.

In entrambi i casi chiameremo la prima ipotesi *passo base*, mentre la seconda *passo induttivo*. Inoltre la supposizione su k presente nel passo induttivo verrà chiamata *ipotesi induttiva*. Se non diversamente specificato, per semplificare la notazione, indicheremo con principio di induzione quello debole.

Benché i tre principi sembrino differenti vale la proposizione seguente.

Proposizione 1.1.4. *I tre principi sono equivalenti.*

Dimostrazione. (1.) $\Rightarrow$ (2.) Dimostriamo che il primo implica il secondo. Sia P una proprietà definita per i naturali maggiori o uguali a n_0, tale che valgano le ipotesi per il principio di induzione (I forma). Sia allora

$$S = \{\, n \in \mathbb{N} \mid n \geq n_0, P(n) \text{ è falsa} \,\}$$

e supponiamo per assurdo che $S \neq \emptyset$. Per il principi del minimo, esiste m_0 minimo di S. Essendo che $P(n_0)$ è vera, allora $m_0 > n_0$. Quindi $n_0 \leq m_0 - 1$ ed essendo m_0 minimo per S, $m_0 - 1$ non appartiene a S. Quindi $P(m_0 - 1)$ è vera, e per ipotesi induttiva lo è anche $P(m_0 - 1 + 1) = P(m_0)$. Quindi $m_0 \notin S$. Assurdo.

(2.) $\Rightarrow$ (3.) Dimostriamo che il secondo principio implica il terzo.

Sia P una proprietà definita per i naturali maggiori o uguali a n_0, tale che valgano le ipotesi per il principio di induzione (II forma). Allora consideriamo la proprietà

$$Q(m)\colon P(n) \text{ è vera per ogni naturale } n_0 \leq n \leq m$$

definita sui naturali $m \geq n_0$.

Verifichiamo che Q verifichi le ipotesi per il principio di induzione (I forma).

Dato che $P(n_0)$ è vera, anche $Q(n_0)$ lo è.

Sia $k \geq n_0$ naturale tale che $Q(k)$ è vera. Allora P è vera per ogni naturale $n_0 \leq n \leq k$. Allora $P(k+1)$ è vera. Quindi P è vera per ogni naturale $n_0 \leq n \leq k+1$ e $Q(k+1)$ è vera.

Per il principio di induzione (I forma), $Q(m)$ è vera per ogni naturale $m \geq n_0$. Quindi $P(n)$ è vera per ogni naturale $n \geq n_0$.

(3.) $\Rightarrow$ (1.) Dimostriamo che il terzo principio implica il primo. Sia S sottoinsieme di $\mathbb{N}$ senza minimo. Allora sia la proprietà $P(n)\colon n \notin S$ definita su tutto $\mathbb{N}$.

Sappiamo che $0 \notin S$, altrimenti S avrebbe come minimo 0. Quindi $P(0)$ è vera.

Sia invece k naturale, tale che $P(n)$ è vera per ogni naturale $n_0 \leq n \leq k$. Allora per ogni n nel suddetto intervallo, $n \notin S$. Quindi se per assurdo $k+1$ appartenesse a S, esso sarebbe minimo per S. Ma questo nega l'ipotesi su S. Quindi $k+1 \notin S$ e $P(k+1)$ è vera.

Quindi le ipotesi per il principio di induzione (II forma) sono verificate e $P(n)$ è vera per ogni $n \in \mathbb{N}$. Cioè $n \notin S$ per ogni $n \in \mathbb{N}$ e $S = \emptyset$. □

Con il principio di induzione possiamo già dimostrare la classica formula provata da Gauss sulla somma dei naturali

Proposizione 1.1.5. *Sia $n \geq 0$ numero naturale. Allora*

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

Dimostrazione. Procediamo come annunciato per induzione.

Per $n = 0, 1$ è evidente.

Supponendolo vero per n, dimostriamolo per $n+1$.

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$$

Quindi per il principio di induzione la formula è vera per ogni naturale n. □

Proponiamo anche un esercizio riguardo alla successione di Fibonacci.

Esercizio. Consideriamo la successione di Fibonacci F_n, definita per ricorsione come:

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_{n+2} = F_{n+1} + F_n \end{cases}$$

Per studiare questa successione è importante introdurre la seguente costante, per ragioni storiche/artistiche detta costante aurea o costante di Fidia:

$$\varphi = \frac{1+\sqrt{5}}{2}$$

Notiamo innanzitutto che la costante aurea rappresenta una soluzione dell'equazione $x^2 - x - 1 = 0$, mentre l'altra è costituita da $-\varphi^{-1} = 1 - \varphi$. Questo implica le relazioni ricorsive

$$\varphi^{n+2} = \varphi^{n+1} + \varphi^n$$
$$(1-\varphi)^{n+2} = (1-\varphi)^{n+1} + (1-\varphi)^n$$

Quello che vogliamo dimostrare, per induzione forte, è che

$$F_n = \frac{1}{\sqrt{5}}(\varphi^n - (1-\varphi)^n)$$

Per $n = 0, 1$ ambo i membri dell'uguaglianza valgono 0 e 1 rispettivamente.

Supposta vera per ogni $0 \leq n \leq k$, allora dobbiamo provare che

$$\begin{aligned}\frac{1}{\sqrt{5}}(\varphi^{k+1} - (1-\varphi)^{k+1}) &= F_{k+1} \\ &= F_k + F_{k-1} \\ &= \frac{1}{\sqrt{5}}(\varphi^k - (1-\varphi)^k + \varphi^{k-1} - (1-\varphi)^{k-1}) \\ &= \frac{1}{\sqrt{5}}(\varphi^k + \varphi^{k-1} - (1-\varphi)^k - (1-\varphi)^{k-1})\end{aligned}$$

Questo è sicuramente implicato dal sistema

$$\begin{cases}\varphi^{k+1} = \varphi^k + \varphi^{k-1} \\ (1-\varphi)^{k+1} = (1-\varphi)^k + (1-\varphi)^{k-1}\end{cases}$$

Che è verificato per quello detto precedentemente.

In verità la formula dimostrata si poteva ricavare per altre vie. Noi sappiamo che la successione di Fibonacci verifica la relazione ricorsiva

$$a_{n+2} = a_{n+1} + a_n \tag{1.1}$$

Supponendo di voler cercare una successione della forma $\{\lambda^n\}$ che risolve (1.1), otteniamo l'equazione

$$\lambda^{n+2} = \lambda^{n+1} + \lambda^n \Rightarrow \lambda^2 = \lambda + 1$$

che dà come soluzione $\lambda = \varphi, 1 - \varphi$.

Ma a questo punto notiamo che una ricorsione del tipo (1.1) è determinata da a_0 e a_1. Inoltre ogni ricorsione del tipo

$$a_n = a\varphi^n + b(1-\varphi)^n$$

è soluzione di (1.1). Quindi dobbiamo solo sperare di poter trovare a, b tale che $a_0 = 0$ e $a_1 = 1$. Possiamo quindi imporre il sistema

$$\begin{cases} a + b = 0 \\ a\varphi + b(1-\varphi) = 0 \end{cases}$$

che ha come soluzione

$$\begin{cases} a = -b \\ a = 1/(\varphi - 1 + \varphi) = \frac{1}{\sqrt{5}} \end{cases}$$

1.2 Prime Nozioni di Cardinalità

Ora che abbiamo enunciamo i principi di induzione incominciamo col calcolo combinatorio. Per il suo sviluppo è centrale il concetto di equicardinalità, che procediamo a definire.

Definizione 1.2.1. Siano X e Y due insiemi. Diciamo che X e Y sono equicardinali, e scriviamo che $|X| = |Y|$, se esiste una bigezione tra di essi.

La nozione di equicardinalità gode delle proprietà simmetrica, riflessiva e transitiva possedute dalle delle relazioni di equivalenza.

Inoltre le cardinalità sono in un certo senso "ordinate", nel senso che possiamo andare a definire la seguente relazione

Definizione 1.2.2. Siano X e Y due insiemi. Diciamo che la cardinalità di X è minore o uguale a quella di Y, e scriviamo che $|X| \leq |Y|$, se esiste una mappa iniettiva da X a Y.

Questa relazione gode delle proprietà di transitività e riflessività delle relazioni d'ordine. La proprietà di antisimmetria, invece, è data dal seguente teorema (la cui dimostrazione si può trovare nell'appendice).

Teorema 1.2.3 (Teorema di Cantor-Bernstein-Schröder)**.** *Siano X e Y due insiemi. Se $|X| \leq |Y| \leq |X|$, allora $|X| = |Y|$.*

Una classe speciale di insiemi consiste nei cosiddetti insiemi finiti, di cui diamo la definizione.

Definizione 1.2.4. Sia X un insieme. Diciamo X è finito se esiste un $k \in \mathbb{N}$ tale che X e $\mathbb{N}_k = \{1, \ldots, k\}$ sono equicardinali. (Dove abbiamo posto $\mathbb{N}_0 = \emptyset$).

Sorge spontaneo porre come notazione $|X| = k$. Tuttavia per poter definire in questo modo la cardinalità di un insieme finito occorre il seguente teorema:

Teorema 1.2.5 (Principio dei Cassetti)**.** *Presi due naturali $1 \leq k < n$ allora $|\mathbb{N}_k| < |\mathbb{N}_n|$.*

Dimostrazione. Certamente esiste una mappa iniettiva, data dall'identità, da $\mathbb{N}_k$ a $\mathbb{N}_n$. Volgiamo dimostrare che non può esistere una bigezione $f\colon \mathbb{N}_n \to \mathbb{N}_k$. Procediamo sempre per induzione.

Se $n = 2$ allora ogni mappa $f\colon \{1, 2\} \to \{1\}$ non è banalmente iniettiva.

Posto vero per $n \geq 2$, supponiamo che esista $f\colon \mathbb{N}_{n+1} \to \mathbb{N}_k$ iniettiva. Consideriamo quindi la restrizione

$$F|_{\{1,\ldots,n\}}\colon \{1, \ldots, n\} \to \{1, \ldots, k\} \setminus \{f(n+1)\}$$

Sia allora la bigezione $g\colon \{1, \ldots, k\} \setminus \{f(n+1)\} \to \mathbb{N}_{k-1}$. Allora $g \circ f\colon \mathbb{N}_n \to \mathbb{N}_{k-1}$ è una mappa iniettiva. Assurdo.

Quindi l'affermazione è vera per ogni $n \in \mathbb{N}$. □

Corollario 1.2.6. *Sia X un insieme finito. Allora esso non può avere la stessa cardinalità di un suo sottoinsieme proprio.*

Dimostrazione. Sia X un insieme in bigezione con $\mathbb{N}_k$ tramite $f\colon X \to \mathbb{N}_k$.

Preso $Y \subseteq X$, esso è in bigezione con $f(Y)$ sottoinsieme proprio di $\mathbb{N}_k$. Tramite induzione su $|\mathbb{N}_k \setminus f(Y)|$ si può immediatamente verificare che se $|\mathbb{N}_k \setminus f(Y)| = h$, allora $|f(Y)| = |\mathbb{N}_{k-h}|$. Cioè $\mathbb{N}_k$ e $\mathbb{N}_{k-h}$ sono in bigezione. Impossibile per la proposizione precedente. □

Per gli insiemi finiti valgono interessanti proprietà, tra le quali la seguente utile proposizione

Proposizione 1.2.7. *Siano X e Y due insiemi finiti della stessa cardinalità. Allora una mappa $f\colon X \to Y$ è iniettiva se e solo se è suggettiva (se e solo se è bigettiva) .*

Dimostrazione. (in.) $\Rightarrow$ (sug.) Se f è iniettiva, allora X è in bigezione con $f(X)$ sottoinsieme di Y. Inoltre $|Y| = |X| = |f(X)|$. Per la proposizione precedente $f(X) = Y$ e f è suggettiva.

(sug.) $\Rightarrow$ (in.) Se f è suggettiva, allora consideriamo la mappa

$$\begin{aligned} g\colon Y &\to X \\ y &\mapsto min\{\, x \in X \mid f(x) = y \,\} \end{aligned}$$

Essa è iniettiva, in quanto se $g(x_1) = g(x_2)$, allora $x_1 = f(g(x_1)) = f(g(x_2)) = x_2$. Quindi $|X| = |Y| = |g(Y)|$ e per la proposizione precedente $g(Y) = X$. Ma per ogni $y \in Y$, $g(y) \in f^{-1}\{y\}$. Quindi affinché valga la precedente uguaglianza deve essere che per ogni $y \in Y$, $|f^{-1}\{y\}| = 1$. Cioè deve valere l'iniettività di f. □

A questo punto andiamo a considerare il calcolo di alcune cardinalità fondamentali.

Dati due insiemi X e Y, è interessante considerare la cardinalità dell'insieme di funzioni da X a Y. La prossima proposizione ne dimostra la cardinalità.

Proposizione 1.2.8. *Siano X e Y due insiemi finiti. Allora l'insieme*

$$Y^X = \{f\colon X \to Y\}$$

ha cardinalità $|Y|^{|X|}$.

Dimostrazione. Procediamo per induzione sulla cardinalità di X.

Se $|X| = 0$, allora $X = \emptyset$. Ed esiste ovviamente un unica funzione $f\colon \emptyset \to Y$ (corrispondente a $\emptyset \subseteq X \times Y$).

Posto vero per $n \geq 0$, sia X di cardinalità $n + 1$. Per ogni funzione

$$f\colon X = \{x_1, \ldots, x_{n+1}\} \to Y$$

posso considerare $f|_{\{x_1,\ldots,x_n\}} \in Y^{\{x_1,\ldots,x_n\}}$.

Per ipotesi induttiva $Y^{\{x_1,\ldots,x_n\}}$ ha cardinalità $|Y|^n$. Inoltre ho $|Y|$ scelte per x_{n+1}. Ergo Y^X ha cardinalità $|Y|^n|Y| = |Y|^{n+1} = |Y|^{|X|}$.

Quindi, per il principio di induzione, l'affermazione è valida qualunque sia la cardinalità di X. □

Se invece vogliamo calcolare la cardinalità dell'insieme delle $f \in Y^X$ iniettive, viene in soccorso il seguente.

Proposizione 1.2.9. *Siano X e Y due insiemi finiti di cardinalità n e m rispettivamente. Posto $I(X,Y)$ l'insieme delle funzioni da X a Y iniettive, allora*

$$|I(X,Y)| = \begin{cases} 0 & \text{se } |Y| < |X| \\ \frac{m!}{(m-n)!} & \text{se } |Y| \geq |X| \end{cases}$$

dove con $n!$ intendiamo il fattoriale

$$n! = n(n-1)\dots 1$$

posto per convenzione $0! = 1$.

Dimostrazione. Se $|Y| < n$, allora una eventuale mappa iniettiva $f\colon X \to Y$ darebbe luogo a una bigezione tra X e un sottoinsieme Z di Y. Tuttavia $|Z| \leq |Y| < |X|$.

Se $|Y| \geq n$, notiamo innanzitutto che vale la bigezione

$$\Phi\colon Y^X \to Y^n = Y \times \cdots \times Y$$
$$f \to (f(x_1), \dots, f(x_n))$$

Allora dobbiamo calcolare la cardinalità delle n-uple $(y_1, \dots, y_n)$ tale che $y_i \neq y_j$ per ogni $i \neq j$. Esse sono

$$m(m-1)\dots(m-n+1) = \frac{m!}{(m-n)!}$$

Infatti ho m scelte per y_1, $m-1$ scelte per y_2, $m-2$ scelte per y_3 etc. □

Un tipo particolare di funzioni iniettive sono le cosiddette permutazioni

Definizione 1.2.10. Dato un insieme X, definiamo le permutazioni di X, indicato con $S(X)$ o $Big(X)$, come l'insieme delle funzioni iniettive da X in X.

Proposizione 1.2.11. *Preso un insieme X, allora $S(X)$ ha cardinalità $n!$.*

Dimostrazione. Immediato dalla proposizione precedente. □

Sarebbe naturale introdurre il conteggi delle funzioni suggettive. Tuttavia è utile passare attraverso lo studio dell'insieme delle parti, la cui esistenza è un vero e proprio assioma della moderna teoria degli insiemi:

Fatto 1.2.12 (Assioma delle Parti)**.** *Dato un insieme X, esiste l'insieme delle parti, o insieme potenza, di X, costituito da tutti e soli i sottoinsiemi di X.*

Vorremmo calcolarne la cardinalità. Introduciamo con l'occasione la seguente definizione:

Definizione 1.2.13. Sia X un insieme. Una sua partizione è una collezione di suoi sottoinsiemi $\{X_i\}_{i\in I}$ tale che

1. Ogni X_i è non vuoto.
2. La loro unione è tutto X.
3. Sono a due a due disgiunti, cioè $X_i \neq X_j$ per ogni $i \neq j \in I$.

Andiamo quindi a trattare la cardinalità dell'insieme delle parti, enunciata nella prossima proposizione.

Proposizione 1.2.14. *Sia X un insieme finito. Allora il suo insieme delle parti ha cardinalità $2^{|X|}$.*

Dimostrazione. Procediamo per induzione su $n = |X|$.

Se $n = 0$, allora $X = \emptyset$ e $|P(X)| = |\{\emptyset\}| = 1$.

Posto vero per $n \geq 0$, sia X di cardinalità $n + 1$. Allora $X \neq \emptyset$ ed esiste $x \in X$.

Possiamo quindi considerare la seguente partizione di $P(X)$:

$$P(X) = \{\, A \subseteq X \mid x \in A \,\} \sqcup \{\, A \subseteq X \mid x \notin A \,\} = P_1 \sqcup P_2$$

dove con $\sqcup$ abbiamo indicato, e indicheremo d'ora in poi, il fatto che i due insiemi sono disgiunti.

Sia ora $T = X \setminus \{x\}$. Se $A \in P(T)$, allora $A \subseteq T \subseteq X$ e $x \notin A$. Quindi $A \in P_2$. D'altra parte se $A \in P_2$, allora $x \notin A$ e $A \subseteq X$. Quindi $A \in P(T)$.

Ergo $P(T) = P_2$ e $|T| = n$. Quindi, per ipotesi induttiva, $|P_2| = 2^n$.

D'altra parte sia

$$\begin{aligned} g\colon P_1 &\to P(T) \\ A &\mapsto A \setminus \{x\} \end{aligned}$$

Verifichiamo l'iniettività e la suggettività di questa funzione.

(iniettività) Se $A_1 \neq A_2$ possiamo supporre, senza perdita di generalità, che esista un $a \in A_1 \setminus A_2$. Essendo che $A_2 \in P_1$, allora $x \in A_2$. Quindi x e a sono differenti.

Allora a appartiene a $A_1 \setminus \{x\} = g(A_1)$, ma non appartiene a $A_2 \setminus \{x\} = g(A_2)$. Quindi $g(A_1)$ e $g(A_2)$ sono diversi e g è iniettiva.

(suggettività) Sia $B \in P(T)$. Allora $B \cup \{x\}$ appartiene a P_1. Inoltre, essendo che x non appartiene a B, B è immagine di $B \cup \{x\}$ tramite g.

Quindi g è una bigezione e $|P_1| = |P(T)| = |P_2|$. Quindi $|P(X)| = |P_1| + |P_2| = 2^n + 2^n = 2^{n+1} = 2^{|X|}$. □

1.3 Coefficiente Binomiale

Preso un insieme X, spesso non si è interessati al suo intero insieme delle parti, ma ai seguenti sottoinsiemi

$$P_r(X) = \{\ A \in P(X) \mid |A| = r\ \}$$

Essi sono infatti collegati, per definizione, al coefficiente binomiale:

Definizione 1.3.1. Siano n, r naturali. Definiamo il coefficiente binomiale di n su r come

$$\binom{n}{r} = |P_r(\mathbb{N}_n)|$$

Inoltre si pone che sia nullo se n è un intero negativo.

Grazie alle nostre conoscenze sulle cardinalità possiamo già affermare le seguenti uguaglianze

- $\binom{n}{r} = 0$ per ogni $r > n$
- $\binom{n}{n} = \binom{n}{0} = 1$
- $\binom{n}{1} = n$

In generale vale però una formula esatta sul valore del coefficiente binomiale, data dal seguente teorema

Teorema 1.3.2. *Siano n, k naturali, con $k \leq n$. Allora*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

.

Dimostrazione. Notiamo che per ogni $A \in P_k(\mathbb{N}_n)$, esso è immagine di una mappa $g\colon \mathbb{N}_k \to \mathbb{N}_n$ iniettiva. D'altra parte ogni funzione g di questo tipo è identificata da una k-upla di elementi di $\mathbb{N}_n$. Inoltre $h\colon \mathbb{N}_k \to \mathbb{N}_n$ ha la stessa immagine di g se e solo se la relativa k-upla è ottenuta da quella di g tramite una sua permutazione. Ma $S(\mathbb{N}_k) = k!$.

Quindi ogni $A \in P_k(\mathbb{N}_n)$ è immagine di esattamente $k!$ funzioni iniettive da $\mathbb{N}_k$ a $\mathbb{N}_n$. Ergo

$$|P_k(\mathbb{N}_n)| = \binom{n}{k} = \frac{|I(\mathbb{N}_k, \mathbb{N}_n)|}{k!} = \frac{n!}{k!(n-k)!}$$

□

Osserviamo che la dimostrazione procede anche se $\mathbb{N}_n = X$ qualunque. Quindi $|P_k(X)|$ non dipende dall'insieme X scelto di cardinalità n.

Inoltre data la definizione del coefficiente binomiale è immediata la prossima proposizione.

Proposizione 1.3.3. *Sia $n \geq 0$ naturale. Allora*

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n$$

Dimostrazione. L'insieme $\{P_r(\mathbb{N}_n)\}_{0 \leq r \leq n}$ formano una partizione di $P(\mathbb{N}_n)$. Ergo

$$2^n = |P(\mathbb{N}_n)| = \sum_{r=0}^{n} |P_r(\mathbb{N}_n)| = \sum_{r=0}^{n} \binom{n}{r}$$

□

Benché l'ultima dimostrazione sfrutti la definizione combinatoria del coefficiente binomiale, spesso è utile poterlo trattare in un modo più algebrico. Le *formule di riflessione e di Stiffel* hanno esattamente questo scopo.

Proposizione 1.3.4 (Formula di Riflessione Binomiale)**.** *Siano $0 \leq r \leq n$ naturali. Allora*

$$\binom{n}{r} = \binom{n}{n-r}$$

Dimostrazione. Consideriamo la mappa

$$\begin{aligned} \Phi\colon P_r(\mathbb{N}_n) &\to P_{n-r}(\mathbb{N}_n) \\ A &\mapsto X \setminus A \end{aligned}$$

Essa è banalmente ben definita, iniettiva e suggettiva. Ergo $|P_r(\mathbb{N}_n)| = |P_{n-r}(\mathbb{N}_n)|$ e abbiamo l'uguaglianza cercata. □

Proposizione 1.3.5 (Formula di Stiffel)**.** *Siano $0 < r \leq n$ naturali. Allora*

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

Dimostrazione. Sia $x \in \mathbb{N}_n$. Allora possiamo considerare gli insiemi

$$\begin{aligned} L &= \{\, A \in P_r(\mathbb{N}_n) \mid x \notin A \,\} \\ M &= \{\, A \in P_r(\mathbb{N}_n) \mid x \in A \,\} \\ T &= \mathbb{N}_n \setminus \{x\} \end{aligned}$$

e la mappa

$$\begin{aligned} \Phi\colon L &\to P_r(T) \\ A &\mapsto A \end{aligned}$$

Come nella proposizione precedente è banalmente ben definita, iniettiva e suggettiva. Quindi $|L| = |P_r(T)| = \binom{n-1}{r}$.

D'altra parte sia

$$\begin{aligned} \psi\colon M &\to P_{r-1}(T) \\ A &\mapsto A \setminus \{x\} \end{aligned}$$

Anche questa mappa è ben definita e biunivoca. Quindi M e $P_{r-1}(T)$ hanno la stessa cardinalità, pari a $\binom{n-1}{r-1}$.

Quindi

$$\binom{n}{r} = |P_r(\mathbb{N}_n)| = |L| + |M| = \binom{n-1}{r} + \binom{n-1}{r-1}$$

□

Una applicazione delle suddette formule è la dimostrazione del Binomio di Newton:

Teorema 1.3.6 (Binomio di Newton)**.** *Siano a, b due numeri reali e n naturale. Allora*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j$$

Dimostrazione. Procediamo per induzione su n.

Se $n = 0$ allora

$$(a+b)^0 = 1 = \sum_{j=0}^{0} \binom{0}{j} a^{0-j} b^j$$

Posto vero per $n \geq 0$, scriviamo

$$\begin{aligned}(a+b)^{n+1} &= (a+b)\left(\sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j\right) \\ &= \sum_{j=0}^{n} \binom{n}{j} a^{n+1-j} b^j + \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^{j+1}\end{aligned}$$

Per quanto riguarda il primo addendo, vale

$$\begin{aligned}\sum_{j=0}^{n} \binom{n}{j} a^{n+1-j} b^j &= \binom{n}{0} a^{n+1} + \sum_{j=1}^{n} \binom{n}{j} a^{n+1-j} b^j \\ &= \binom{n}{0} a^{n+1} + \sum_{j=0}^{n-1} \binom{n}{j+1} a^{n-j} b^{j+1}\end{aligned}$$

Mentre per il secondo

$$\sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^{j+1} = \sum_{j=0}^{n-1} \binom{n}{j} a^{n-j} b^{j+1} + \binom{n}{n} b^{n+1}$$

Ma a questo punto basta usare la formula di Stiffel per ottenere

$$\begin{aligned}(a+b)^{n+1} &= \binom{n}{0} a^{n+1} + \sum_{j=0}^{n-1} \left[\binom{n}{j+1} + \binom{n}{j}\right] a^{n-j} b^{j+1} + \binom{n}{n} b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} + \sum_{j=0}^{n-1} \binom{n+1}{j+1} a^{n-j} b^{j+1} + \binom{n+1}{n+1} b^{n+1} \\ &= \binom{n+1}{0} a^{n+1} + \sum_{j=1}^{n} \binom{n+1}{j} a^{n+1-j} b^j + \binom{n+1}{n+1} b^{n+1} \\ &= \sum_{j=0}^{n+1} \binom{n+1}{j} a^{n+1-j} b^j\end{aligned}$$

Per il principio di induzione il teorema vale per ogni n naturale. □

Una immediata applicazione del binomio di Newton è questa interessante proprietà:

Proposizione 1.3.7. *Sia X un insieme non vuoto, allora possiede in egual numero sottoinsiemi di cardinalità pari e dispari.*

Dimostrazione. Grazie al teorema binomiale sappiamo che, posto $n = |X|$,

$$0 = (1-1)^n = \sum_{j=0}^{n} (-1)^j \binom{n}{j}$$

Ergo

$$\sum_{j \text{ dispari}} \binom{n}{j} = \sum_{j \text{ pari}} \binom{n}{j}$$

Cioè

$$\left| \bigcup_{j \text{ dispari}} P_j(X) \right| = \left| \bigcup_{j \text{ pari}} P_j(X) \right|$$

□

Concludiamo questa sezione con una utile generalizzazione del coefficiente binomiale: il cosiddetto *coefficiente multinomiale*. Come quello binomiale diamo prima una definizione insiemistica e poi una formula operativa.

Definizione 1.3.8 (Coefficiente Multinomiale)**.** Siano $n, n_1, \ldots, n_k$ naturali tale che $n_1 + \cdots + n_k = n$. Allora indichiamo con

$$\binom{n}{n_1, \ldots, n_k}$$

il numero di k-uple della forma $(X_1, \ldots, X_k)$ tale che

1. $\{X_i\}_{i=1,\ldots,k}$ partiziona $\mathbb{N}_n$
2. Per ogni $i = 1, \ldots, k$, $|X_i| = n_i$

Proposizione 1.3.9. *Nelle ipotesi precedenti vale l'uguaglianza*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! \ldots n_k!}$$

Dimostrazione. Sia $P_{n_1,\dots,n_k}(\mathbb{N}_n)$ l'insieme di cui vogliamo calcolare la cardinalità. Allora

$$\begin{aligned}|P_{n_1,\dots,n_k}(\mathbb{N}_n)| &= \sum_{\substack{I_1\subseteq\mathbb{N}_n\\|I_1|=n_1}} \sum_{\substack{I_2\subseteq\mathbb{N}_n\setminus I_1\\|I_2|=n_2}} \cdots \sum_{\substack{I_k\subseteq\mathbb{N}_n\setminus(I_1\cup\cdots\cup I_{k-1})\\|I_k|=n_k}} |P_{n_k}(\mathbb{N}_n)| \\ &= \binom{n}{n_1}\binom{n-n_1}{n_2}\dots\binom{n-(n_1+\cdots+n_{k-1})}{n_k} \\ &= \frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdots\frac{(n-n_1-\cdots-n_{k-1})!}{n_k!(n-n_1-\cdots-n_k)!} \\ &= \frac{n!}{n_1!\dots n_k!}\end{aligned}$$

□

1.4 Formula di Inclusione-Esclusione

Consideriamo ora la seguente situazione: presi $A_1,\dots,A_n$ insiemi finiti, quale è la cardinalità della loro unione in funzione delle cardinalità dei A_i e delle loro intersezioni? Per $n=2$ è noto essere $|A_1|+|A_2|-|A_1\cap A_2|$, ma il prossimo teorema ne fornisce una generalizzazione.

Teorema 1.4.1 (Formula di Inclusione-Esclusione)**.** *Siano $A_1,\dots,A_n$ insiemi finiti. Allora anche l'unione lo è e ha cardinalità*

$$\left|\bigcup_{i=1}^{n} A_n\right| = \sum_{\substack{I\subseteq\mathbb{N}_n\\I\neq\emptyset}} (-1)^{|I|+1}\left|\bigcap_{k\in I} A_k\right| \tag{1.2}$$

Dimostrazione. Sia un qualunque x appartenente all'unione degli A_i. Supponiamo che appartenga a $A_{i_1},\dots,A_{i_r}$. Nella formula (1.2) esso viene conteggiato un numero di volte pari a

$$\sum_{j=1}^{r}(-1)^{j+1}\binom{r}{j}$$

In quanto $\binom{r}{j}$ è il numero di sottoinsiemi di $\{i_1,\dots,i_r\}$ di cardinalità j. Tuttavia, grazie alla proposizione (1.3.7), e a meno di cambiare tutti i segni, sappiamo che

$$0 = \sum_{j=0}^{r}(-1)^{j+1}\binom{r}{j}$$

Ergo

$$\sum_{j=1}^{r}(-1)^{j+1}\binom{r}{j} = -(-1)\binom{r}{0} = 1$$

Quindi ogni elemento dell'unione viene conteggiato una e una sola volta. □

Grazie a questo teorema è possibile, per esempio, calcolare la cardinalità delle funzioni suggettive

Proposizione 1.4.2. *Siano X e Y due insiemi finiti. Posto $S(X,Y)$ l'insieme delle funzioni suggettive da X a Y, allora*

$$|S(X,Y)| = \sum_{j=0}^{n}(-1)^{j}\binom{n}{j}(n-j)^{m}$$

con m e n le cardinalità di X e Y rispettivamente.

Dimostrazione. Sia $Y = \{y_1, \dots, y_n\}$ e siano gli insiemi

$$A_i = \left\{\, g \in Y^X \;\middle|\; y_i \notin Im(g) \,\right\} \quad i = 1, \dots, n$$

Innanzitutto è evidente che $S(X,Y) = Y^X \setminus \bigcup A_i$. Inoltre per la formula di esclusione-inclusione abbiamo

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{I\subseteq\mathbb{N}_n \\ I\neq\emptyset}} (-1)^{|I|+1}\left|\bigcap_{k\in I} A_k\right|$$

Notiamo ora che per ogni $I \subseteq \mathbb{N}_n$ non vuoto,

$$\left|\bigcap_{k\in I} A_k\right| = |\{\, f\colon X \to Y \setminus \{y_k\}_{k\in I} \,\}| = (n - |I|)^m$$

Da cui

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{I\subseteq\mathbb{N}_n \\ I\neq\emptyset}} (-1)^{|I|+1}(n - |I|)^m$$

Ma a questo punto possiamo riscrivere la sommatoria indicizzata sulla cardinalità di $j = |I|$. Per ogni $j = 1, \dots, n$ abbiamo $\binom{n}{j}$ sottoinsiemi I di cardinalità j. Quindi

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{j=1}^{n}(-1)^{j+1}\binom{n}{j}(n-j)^{m}$$

Infine

$$\begin{aligned}|S(X,Y)| &= \left|Y^X\right| - \left|\bigcup_{i=1}^{n} A_i\right| \\ &= n^m - \sum_{j=1}^{n}(-1)^{j+1}\binom{n}{j}(n-j)^m \\ &= \sum_{j=0}^{n}(-1)^{j}\binom{n}{j}(n-j)^m\end{aligned}$$

□

1.5 Stars and Bars & Double Counting

Iniziando trattando due problemi a prima vista innocenti, che però si rivelano utili in svariate applicazioni.

Sia n naturale. Quante sono le k-uple naturali che risolvono $x_1 + \cdots + x_k = n$? Le prossime due proposizioni rispondono a questa domanda.

Proposizione 1.5.1. *Sia n naturale positivo. Allora l'equazione*

$$x_1 + \cdots + x_k = n$$

ammette $\binom{n-1}{k-1}$ soluzioni naturali positive.

Dimostrazione. Sia A l'insieme delle soluzioni e sia $\mathbb{N}_+$ l'insieme dei naturali positivi. Notiamo che sussiste la seguente mappa:

$$\begin{aligned}\Phi\colon A &\to \left\{ (y_1,\ldots,y_k) \in \mathbb{N}_+^n \;\middle|\; y_1 < \cdots < y_k = n \right\} \\ y_1 &= x_1 \\ y_2 &= x_1 + x_2 \\ &\cdots \\ y_k &= x_1 + \ldots x_k = n\end{aligned}$$

Essa è una bigezione, ammettendo come inversa

$$\begin{aligned}\Psi\colon \left\{ (y_1,\ldots,y_k) \in \mathbb{N}_+^n \;\middle|\; y_1 < \cdots < y_k = n \right\} &\to A \\ x_1 &= y_1 \\ x_2 &= y_2 - y_1 \\ &\cdots \\ x_k &= y_k - y_{k-1}\end{aligned}$$

Inoltre il dominio di Ψ è in bigezione con $P_{k-1}(\mathbb{N}_{n-1})$. Infatti ad ogni suo elemento $(y_1, \dots, y_k)$ si può associare il sottoinsieme $\{y_1, \dots, y_{k-1}\}$. Viceversa dato un sottoinsieme $\{a_1, \dots, a_{k-1}\}$, esso ammette una unica riordinazione crescente $(a_{i_1}, \dots, a_{i_{k-1}})$, a cui associamo la k-upla $(a_{i_1}, \dots, a_{i_{k-1}}, n)$.

Quindi $|A| = |P_{k-1}(\mathbb{N}_{n-1})| = \binom{n-1}{k-1}$. □

Proposizione 1.5.2. *Sia n naturale positivo. Allora l'equazione*

$$x_1 + \cdots + x_k = n$$

ammette $\binom{n+k-1}{k-1}$ soluzioni naturali.

Dimostrazione. Sia A l'insieme delle soluzioni. è in bigezione, ponendo $x_i + 1 = y_i$, con l'insieme delle soluzioni in $\mathbb{N}_+^n$ dell'equazione

$$y_1 + \cdots + y_k = n + k$$

Per la proposizione precedente sono $\binom{n+k-1}{k-1}$. □

Infine proponiamo niente di meno di una proposizione, che tuttavia mostra l'utile tecnica del double-counting.

Proposizione 1.5.3. *Sia n naturale. Allora*

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$$

Dimostrazione. Consideriamo il seguente insieme

$$X = \{\text{squadre composte da } 1 \leq k \leq n \text{ persone e con un capitano scelto}\}$$

che se vogliamo può essere formalizzato come

$$X = \mathbb{N}_n \cup \{\, (x, A) \mid x \in \mathbb{N}_k, A \subseteq \mathbb{N}_k \setminus \{x\}, 2 \leq k \leq n \,\}$$

Possiamo calcolare la cardinalità di X in due modi.

Da una parte possiamo prima scegliere il sottoinsieme di B di $\mathbb{N}_n$ e poi scegliere un suo elemento x. Avendo $\binom{n}{k}$ sottoinsiemi di cardinalità k e potendo scegliere per ognuno k capitani, abbiamo la cardinalità

$$|X| = \sum_{k=0}^{n} k\binom{n}{k}$$

D'altra parte possiamo prima scegliere $x \in \mathbb{N}_n$, e poi un sottoinsieme B, eventualmente vuoto, di $\mathbb{N}_n \setminus \{x\}$. Ergo X ha anche cardinalità

$$|X| = n2^{n-1}$$

Uguagliando le due espressioni per la cardinalità di X otteniamo il risultato.

□

Capitolo 2

Teoria dei Numeri

2.1 Relazioni d'Ordine

Iniziamo ricordando il concetto di relazione:

Definizione 2.1.1. Sia $X \neq \emptyset$ un insieme. Una relazione su X è un sottoinsieme R di $X \times X$. Diciamo che $x \sim_R y$, cioè x è in relazione con y, se $(x, y) \in R$.

Definizione 2.1.2. Sia X un insieme e R una relazione su X. Diciamo che R è

1. Riflessiva se per ogni $x \in X$ esso è in relazione con se stesso.
2. Simmetrica se per ogni $x, y \in X$, se x è in relazione con y anche y lo è con x.
3. Antisimmetrica se per ogni $x, y \in X$, se x è in relazione con y e y lo è con x allora $x = y$.
4. Transitiva se per ogni $x, y, z \in X$, se x è in relazione con y e y lo è con z, allora anche x lo è con z.
5. Totale se per ogni $x, y \in X$, x è in relazione con y o y lo è con x.

Definizione 2.1.3. Sia X un insieme e R una relazione su X. Diciamo che R è una relazione di

1. Equivalenza se è riflessiva, simmetrica e transitiva

2. Ordine se è riflessiva, antisimmetrica e transitiva

Data infine una relazione d'ordine, è possibile introdurre i seguenti concetti

Definizione 2.1.4. Sia X un insieme e $\leq$ una relazione d'ordine su di esso.

1. Un elemento $y \in X$ è un maggiorante (risp. minorante) per $A \subseteq X$ se ogni $x \in A$ è minore (risp. maggiore) di y.

2. Un sottoinsieme $A \subseteq X$ è superiormente (risp. inferiormente) limitato se ammette maggiorante (risp. minorante).

3. Un elemento $y \in A \subseteq X$ è un elemento massimale (risp. minimale) per A se, posto $x \in A$ e $y \leq x$ (risp. $y \geq x$), allora $x = y$.

4. Un elemento $y \in X$ è l'estremo superiore (risp. inferiore) per $A \subseteq X$ se è il minimo per l'insieme dei maggioranti (risp. minoranti) di A.

5. Un elemento $y \in A \subseteq X$ è il massimo (risp. minimo) per A se è il suo estremo superiore (risp. inferiore).

Osserviamo che gli estremi superiori/inferiori non necessitano di esistere. Per esempio l'insieme dei razionali minori di π non ammette estremo superiore razionale.

2.2 Divisione Euclidea

Passiamo a questo punto lo strumento centrale della teoria dei numeri: la divisione euclidea.

Teorema 2.2.1 (Teorema del Resto)**.** *Per ogni $a, b \in \mathbb{Z}$ con $b \neq 0$, esistono unici $q, r \in \mathbb{Z}$, con $0 < r < |b|$, tali che $a = bq + r$.*

Dimostrazione. (Esistenza) $\mathbf{b > 0}$ Sia

$$X = \{\, r \in \mathbb{Z} \mid r = a - kb, k \in \mathbb{Z} \,\} \cap \mathbb{N}$$

Essendo che $b > 0$, allora $a + |a|b \in X$. Quindi X non è vuoto e ammette minimo r_0.

Essendo che r_0 appartiene a X, esso è della forma $a = q_0 b + r_0$. Inoltre se per assurdo r_0 fosse maggiore o uguale a $|b| = b$, allora $r_0 - b = a - (q_0 + 1)b$

sarebbe maggiore o uguale a zero. Da cui $r_0 - b$ apparterrebbe a X. Assurdo per minimalità di $r_0 - b$.

b < 0 In questo caso, per il punto precedente, esistono $q_0, r_0 < -b = |b|$ tale che $a = q_0(-b) + r_0 = (-q_0)b + r_0$.

(Unicità) Supponiamo che esistano q_1, r_1 e q_2, r_2 tale che $a = q_1b + r_1 = q_2b + r_2$. Supponiamo senza perdita di generalità che r_1 sia maggiore o uguale a r_2. Allora $|r_1 - r_2| = r_1 - r_2$ e

$$|b| > r_1 \geq r_1 - r_2 = (q_2 - q_1)b$$

Se $q_2 \neq q_1$, allora dalla precedente disuguaglianza otterremmo che

$$|b| > r_1 - r_2 = |r_1 - r_2| = |q_1 - q_2||b| \geq |b|$$

Quindi $q_1 = q_2$ e $r_1 = r_2$. □

Grazie all'unicità della divisione euclidea, ha senso la definizione:

Definizione 2.2.2. Siano a, b interi con $b \neq 0$. Diciamo che b divide a, e scriviamo che $b \mid a$, se esiste un intero q tale che $a = qb$. Viceversa a è un multiplo di b.

Proposizione 2.2.3. *La divisibilità è una relazione d'ordine su* $\mathbb{N}_+$.

Dimostrazione. Notiamo innanzitutto che se prendiamo $x, y \in \mathbb{N}_+$ tale che $y = qx$ con q intero, allora $q \in \mathbb{N}_+$. Infatti se fosse negativo anche y lo dovrebbe essere.

La relazione è banalmente riflessiva. Infatti per ogni $x \in \mathbb{N}_+$, $x = 1x$. Quindi $x \mid x$.

Presi $x, y \in \mathbb{N}_+$ tale che $x \mid y$ e $y \mid x$, scriviamo $y = qx = qhy$ con $q, h \in \mathbb{N}_+$. Ergo $1 = qh$ e $q = h = 1$.

Presi $x, y, z \in \mathbb{N}_+$ tale che $y = qx$, $z = hy$, allora $z = hqx$ e $x \mid z$. - □

Con queste definizioni possiamo dare una definizione assiomatica del massimo comune divisore e minimo comune multiplo:

Definizione 2.2.4 (Massimo Comune Divisore)**.** Siano m, n interi non entrambi nulli. Un intero d non nullo è un massimo comune divisore se

1. d divide sia a che b

2. Per ogni c che divide sia a che b, allora c divide d.

Definizione 2.2.5 (Minimo Comune Multiplo)**.** Siano m, n interi non nulli. Un intero d non nullo è un minimo comune multiplo se

1. d è un multiplo sia di a che di b

2. Per ogni c multiplo sia di a che b, allora c è un multiplo di d.

Osserviamo che se $a, b \in \mathbb{N}_+$, le definizioni si possono porre nel seguente modo: un loro massimo comune divisore è un estremo inferiore di $\{a, b\}$, mentre il minimo comune multiplo ne è un estremo superiore.

A questo punto andiamo a dimostrare l'effettiva esistenza e unicità del massimo comune divisore.

Teorema 2.2.6. *Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Allora ammettono un massimo comune divisore. Inoltre è unico a meno del segno.*

Dimostrazione. (Unicità) Siano d_1, d_2 due massimi comuni divisori. Allora

$$d_2 \mid a, d_2 \mid b \Rightarrow d_1 \mid d_2$$
$$d_1 \mid a, d_1 \mid b \Rightarrow d_2 \mid d_1$$

Quindi $d_1 = qhd_2$ con $q, h \in \mathbb{Z}$ e $qh = 1$. Ciò implica che $q = h = 1$ o $q = h = -1$. Cioè $d_1 = \pm d_2$.

(Esistenza) Sia $X = \{\, ax + by \mid x, y \in \mathbb{Z} \,\} \cap \mathbb{N}_+$. Allora supponiamo, senza perdita di generalità, che $a \neq 0$.

Per $(x, y) = (a, 0)$, $ax + by$ appartiene a X che quindi non è vuoto. Ergo ammette minimo d, che vogliamo dimostrare essere un massimo comune divisore.

Sia $a = qd + r$ tramite divisione euclidea. Allora, ponendo $d = ax_0 + by_0$, otteniamo

$$0 \leq r = a - qd = a(1 - qx_0) + b(-qy_0)$$

Quindi $r < d$ appartiene a X. Ergo, per minimalità, $r = 0$ e $q \mid a$. Analogamente $q \mid b$.

Sia $c \in \mathbb{Z}$ che divide sia a che b. Allora, ponendo $a = ca_1$ e $b = cb_1$, vale la scrittura $d = ax_0 + by_0 = c(a_1x_0 + b_1y_0)$. Ergo c divide d. □

Osserviamo che abbiamo dimostrato, in verità, anche una famosa uguaglianza:

Teorema 2.2.7 (Uguaglianza di Bezout)**.** *Siano a, b non entrambi nulli e sia d un loro massimo comune divisore. Allora esistono x_0, y_0 interi tale che $d = x_0a + y_0b$.*

Dimostrazione. Essendo che i massimi comuni divisori coincidono al meno del segno, $d = \pm d'$, con d' il massimo comune divisore identificato nel teorema precedente. Allora, prendendo x_0, y_0 del teorema precedente, $d = \pm d' = \pm x_0a + \pm y_0b$. □

Quindi abbiamo dimostrato l'esistenza del massimo comune divisore e l'identità di Bezout. Tuttavia per ora non abbiamo un metodo costruttivo o algoritmico per la sua costruzione. Si potrebbe dimostrare che il massimo comune divisore, e il minimo comune multiplo, coincidono che quelli calcolabili tramite la scomposizione in primi. Tuttavia, oltre a essere un operazione onerosa, è spesso eccessiva. Per esempio se a divide b, allora il loro massimo comune divisore è b, indipendentemente dalla loro scomposizione in fattori primi. Questo fa pensare che ci possa essere un metodo che non si appoggia ad essa.

La soluzione arriva da un algoritmo che prende il nome da Euclide. L'intero algoritmo si bassa su questa osservazione:

Lemma 2.2.8. *Siano a, b interi non entrambi nulli. Allora preso $k \in \mathbb{Z}$, vale l'uguaglianza*

$$(a, b) = (a, b + ka)$$

dove abbiamo indicato, e indicheremo, con (a, b) il loro massimo comune divisore.

Dimostrazione. Sia $d = (a, b)$.

Certamente $d \mid b + ka$.

Inoltre se c divide sia a che $b+ka$, allora deve dividere anche $(b+ka)-ka = b$. Quindi c divide d.

Ergo d è il massimo comune divisore di $(a, b + ka)$. □

Siamo pronti per enunciare il nostro algoritmo.

Teorema 2.2.9 (Algoritmo di Euclide)**.** *Siano a, b due naturali con $b \neq 0$. Sia inoltre la successione (r_n, q_n) definita come*

$$\begin{cases} r_{-1} = a \\ r_0 = b \\ r_n = q_{n+2} r_{n+1} + r_{n+2} \end{cases}$$

Allora l'algoritmo termina, cioè esiste un $N \leq 1$ tale che $r_N = 0$. Inoltre r_{N-1} è il massimo comune divisore tra a e b e ricostruendo le divisioni euclidee sono trovabili i coefficienti di Bezout.

Dimostrazione. (Termina) La successione $\{r_n\}$ è una successione di numeri naturali strettamente decrescente. Se per assurdo ogni r_n fosse positivo, potremmo ripetere l'algoritmo indefinitivamente. In particolare, posto r_k il minimo tra gli r_n, allora r_{k+1} sarebbe strettamente minore r_k. Assurdo per minimalità.

Per i punti successivi procediamo per induzione su N.

Se $N = 1$, allora $r_0 = b$ dovrebbe essere il massimo comune divisore tra a e b. Infatti $a = q_1 b + 0$ è diviso da b.

Inoltre abbiamo i coefficienti di Bezout: $b = 0a + 1b$.

Se $N > 1$, allora algoritmo per (b, r_1) termina in $N - 1$ passi. Quindi per ipotesi induttiva $r_{N-1} = (b, r_1) = (b, a - q_1 b) = (b, a)$. Inoltre supponendo $r_N = x_0(a - q_1 b) + y_0 b$, allora $r_N = x_0 a + (y_0 - q_1 x_0) b$. □

Esempio. Calcoliamo il massimo comune divisore tra 64 e 14 tramite l'algoritmo di Euclide. Iniziamo eseguendo le divisioni successive

$$\begin{aligned} 64 &= 4 * 14 + 8 \\ 14 &= 1 * 8 + 6 \\ 8 &= 1 * 6 + 2 \\ 6 &= 1 * 2 + 0 \end{aligned}$$

Ergo $(64, 14) = 2$. Inoltre per calcolare i coefficienti di Bezout sostituiamo all'indietro i resti delle divisioni:

$$\begin{aligned} 2 &= 8 - 1 * 6 \\ &= 8 - 1 * (14 - 1 * 8) = -1 * 14 + 2 * 8 \\ &= -1 * 14 + 2 * (64 - 4 * 14) = 2 * 64 + (-9) * 14 \end{aligned}$$

2.3 Equazioni Diofantee Lineari

Dati a, b interi non entrambi nulli e d un loro massimo comune divisore, sappiamo che l'equazione $ax + by = d$ ammette soluzioni intere. Questo è un classico esempio di equazione diofantea

Definizione 2.3.1. Una equazione diofantea è una equazione a coefficienti interi, di cui si cercano soluzioni intere.

In generale le equazioni diofantee sono equazioni estremamente difficili da risolvere. Basti pensare che il problema di Fermat, dimostrato solo nel 1994, ne è un esempio. Di fatto le uniche equazioni di cui si ha un semplice metodo risolutivo sono le equazioni lineare che andremo a trattare.

Definizione 2.3.2. Una equazione diofantea lineare è della forma $ax+by = c$, con a, b, c interi e a, b non entrambi nulli.

Iniziamo trattando l'esistenza delle soluzioni con il seguente teorema:

Teorema 2.3.3. *Sia un'equazione diofantea lineare $ax + by = c$. Allora ammette soluzione se e solo se $d = (a, b)$ divide c.*

Dimostrazione. ($\Rightarrow$) Se l'equazione ammette una soluzione (x_0, y_0), poniamo $a = a_1 d$ e $b = db_1$. Quindi $c = ax_0 + by_0 = d(a_1x_0 + b_1y_0)$. Quindi d divide c.

($\Leftarrow$) Se d divide c, allora per l'identità di Bezout esistono x_0, y_0 tali che $ax_0 + by_0 = d$. Ponendo $c = md$, allora $a(mx_0) + b(my_0) = c$ e l'equazione ammette soluzione. □

Corollario 2.3.4. *Dati due interi a, b non entrambi nulli, essi sono coprimi, cioè $(a, b) = 1$, se e solo se l'equazione diofantea $ax+by = 1$ ammette soluzione.*

Dimostrazione. Immediata conseguenza del teorema precedente. □

Corollario 2.3.5. *Dati a, b due interi non entrambi nulli, poniamo d un loro massimo comune divisore. Posto $a_1d = a$ e $b_1d = b$, allora a_1, b_1 sono coprimi.*

Dimostrazione. Sappiamo che per qualche x_0, y_0 vale l'uguaglianza di Bezout $d = ax_0 + by_0$. Dividendo per d otteniamo $1 = a_1x_0 + b_1y_0$. Cioè a_1, b_1 sono coprimi. □

A questo punto dobbiamo costruire le nostre soluzioni. Il prossimo teorema permette di semplificare il problema:

Teorema 2.3.6. *Sia un'equazione diofantea lineare*

$$ax + by = c \tag{2.1}$$

E sia l'omogenea associata

$$ax + by = 0$$

Allora tutte e sole le soluzioni di (2.1) *si ottengono traslando le soluzioni dell'omogenea di una soluzione particolare.*

Dimostrazione. Sia (x_0, y_0) una soluzione particolare di (2.1). Allora presa (x', y') una soluzione dell'omogenea, $(x_0 + x', y_0 + y')$ è ancora una soluzione di (2.1). Infatti

$$a(x_0 + x') + b(y_0 + y') = ax_0 + by_0 + ax' + by' = c$$

Viceversa sia (x', y') soluzione di (2.1). Allora $(x' - x_0, y' - y_0)$ è una soluzione dell'omogenea. Infatti

$$a(x' - x_0) + b(y' - y_0) = c - c = 0$$

□

Ci siamo quindi ricondotti al caso $c = 0$. Per risolverlo consideriamo il seguente lemma:

Lemma 2.3.7. *Siano a, b interi non entrambi nulli. Se un intero m divide ab ed è coprimo con a, esso divide b.*

Dimostrazione. Se $(a, m) = 1$, allora esistono x, y tale che $mx + ay = 1$. Ergo esistono x, y tale che $bmx + bay = b$. Ma $ab = km$. Ergo $amx + kmy = b$ e m divide b. □

Corollario 2.3.8. *Siano a, b, m interi non nulli tale a, b sono coprimi e dividono m. Allora anche ab divide m.*

Dimostrazione. Poniamo $m = ax$. Essendo che b divide m ed è coprimo con a, allora b divide x per il lemma precedente. Quindi $x = by$ e $m = aby$. Quindi ab divide m. □

Con questo lemma anche le equazioni diofantee lineare omogenee sono risolte

Teorema 2.3.9. *Sia una equazione diofantea omogenea $ax+by=0$. Poniamo $d=(a,b)$ e $a=a_1d$ e $b=b_1b$. Allora le soluzioni dell'equazioni sono tutte e sole le coppie della forma*

$$S = \{\, (x,y) = (-b_1k, a_1k) \mid k \in \mathbb{Z} \,\}$$

Dimostrazione. Certamente presa una coppia $(x,y) \in S$, essa é soluzione. Infatti

$$ax + by = ab_1k - ba_1k = a_1db_1k - b_1da_1k = 0$$

D'altra parte sia (x,y) soluzione dell'omogenea. Allora $ax = -by$ e $a_1x = -b_1y$. Cioè a_1 divide $-b_1y$ tramite x.

Quindi, per il lemma precedente, essendo a_1 e b_1 coprimi, a_1 deve dividere y. Quindi $y = a_1k$ con k intero. Allora $a_1x = -b_1a_1k$ e $x = -b_1k$. □

A questo punto possiamo rispondere al teorema iniziale:

Teorema 2.3.10. *Sia un'equazione diofantea lineare $ax + by = c$. Posto $d = (a,b)$, l'equazione ammette soluzione se e solo se d divide c. In tal caso siano $a = a_1d$, $b = b_1d$. Allora le soluzioni sono tutte e sole le coppie della forma*

$$\begin{cases} x = x_0 + b_1k \\ y = y_0 - a_1k \end{cases}$$

con $k \in \mathbb{Z}$ e (x_0, y_0) una soluzione particolare (data per esempio dall'identità di Bezout riscalando i coefficienti).

Dimostrazione. Dalle proposizioni 2.3.6 e 2.3.9 otteniamo la tesi (dove abbiamo potuto cambiare i segni di k essendo intero). □

Esempio. Sia l'equazione

$$64x + 14y = 8$$

Come visto nell'esercizio precedente, $(64, 14) = 2$ che divide $c = 8$. Quindi l'equazione ammette soluzione.

Inoltre $a_1 = 32$, $b_1 = 7$ e abbiamo già trovato i coefficienti di Bezout $(2, -9)$. Essendo che $c/2 = 4$, sappiamo che possiamo prendere $(x_0, y_0) = (4 * 2, 4 * (-9))$. Quindi le soluzioni sono

$$\begin{cases} x = 8 + 7k \\ y = -36 - 32k \end{cases}$$

con k intero.

2.4 Primi e Irriducibili

Andiamo ora a definire i concetti di primo e irriducibile. Concetti per ora riguardanti solo i numeri interi, ma che verranno ripresi quando tratteremo gli anelli.

Definizione 2.4.1 (Intero Irriducibile)**.** Sia $p \neq -1, 1, 0$ intero. Dico che p è irriducibile se, posto $p = xy$, allora $x = \pm 1$ o $y = \pm 1$.

Definizione 2.4.2 (Intero Primo)**.** Sia $p \neq -1, 1, 0$ intero. Dico che p è primo se per ogni $a, b \in \mathbb{Z}$ tale che p divide ab, allora p divide a o divide b.

Andiamo a capire la loro relazione. Un interessante fatto è il seguente, che vale anche in anelli che non siano $\mathbb{Z}$.

Teorema 2.4.3. *Sia $p \in \mathbb{Z}$ primo. Allora è irriducibile.*

Dimostrazione. Supponiamo che p si scomponga come $p = xy$. Allora p divide se stesso, cioè divide xy. Quindi, essendo primo, deve dividere x o y. Senza perdita di generalità supponiamo che p divida x. Ergo $x = kx$ con k intero. Quindi otteniamo $p = kpy$ e $1 = ky$. Ma gli unici elementi invertibili in $\mathbb{Z}$ sono ± 1. Quindi $x = \pm 1$. □

L'implicazione opposta vale invece in anelli particolari, tra cui quello degli interi, detti cosiddetti anelli a fattorizzazione unica.

Teorema 2.4.4. *Sia $p \in \mathbb{Z}$ irriducibile. Allora è primo.*

Dimostrazione. Supponiamo che p divida ab. Se p divide a, allora ci siamo.

Supponiamo invece che p non divida a. Allora prendiamo $(p, a) = d > 0$. Essendo p irriducibile, allora $d = 1$ o $d = p$. Non potendo p dividere a, allora $d = 1$. Possiamo usare il lemma 2.3.7 per affermare che p divide b. □

Come dice il seguente teorema, i numeri primi formano gli "atomi" che costituiscono tutti i numeri interi.

Teorema 2.4.5 (Teorema Fondamentale dell'Aritmetica)**.** *Ogni numero naturale maggiore o uguale a 2 o è primo o si scompone come prodotto di primi. Inoltre la scrittura è unica a meno del segno dei fattori (e a meno dell'ordine).*

Dimostrazione. (Esistenza) Procediamo per induzione forte.

Se $n = 2$, allora esso è primo.

Posto $n \geq 2$ tale che valga l'ipotesi induttiva, allora o esso è primo, o esso si scrive come prodotto $n = lm$ con l, m maggiori di 1 e minori di n. Per ipotesi induttiva essi si scrivono come prodotto di primi

$$l = \prod_{i=1}^{n} p_i \quad m = \prod_{j=1}^{m} q_i$$

da cui

$$n = lm = \prod_{i=1}^{n} p_i \prod_{j=1}^{m} q_j$$

Quindi n si scrive come prodotto di primi.

Quindi per il principio di induzione forte ogni naturale maggiore di 1 verifica l'affermazione.

(Unicità) Procediamo per induzione debole sul minimo delle lunghezze fattorizzazione esistenti.

Se $n = 1$, sia x che ammette una fattorizzazione di lunghezza 1. Allora $x = p_1$. Inoltre sia un'altra fattorizzazione $q_1 \dots q_r = p_1$.

Ogni q_i divide p_1. Essendo p_1, q_i primi/irriducibili, allora $q_i = \mu p_1$ con $\mu = \pm 1$. Ergo $1 = \mu q_2 \dots q_r$.

Ma q_i sono primi, quindi diversi da ± 1. Allora $r = 1$ e le due fattorizzazioni sono uguali al meno del segno.

Posto vero per $n \geq 1$, sia x che ammette una fattorizzazione di lunghezza $n + 1$. Poniamo $x = p_1 \dots p_{n+1}$ e sia $q_1 \dots q_r$ un'altra fattorizzazione di x. Allora p_1 divide $q_1 \dots q_r$; essendo p_1 primo esso divide un certo q_i. Quindi $q_i = \mu p_1$ con $\mu = \pm 1$.

Senza perdita di generalità possiamo supporre che $i = 1$. Allora

$$p_2 \dots p_{n+1} = \mu q_2 \dots q_r$$

La prima è una fattorizzazione lunga n primi, quindi per ipotesi induttiva $r = n + 1$ e i fattori coincidono a meno del segno.

Quindi anche $p_1 \dots p_{n+1}$,$q_1 \dots q_r$ hanno fattori coincidenti a meno del segno. □

Grazie all'unicità del teorema fondamentale dell'aritmetica è possibile dimostrare il seguente fatto, provato per la primo volta da Eulero:

Teorema 2.4.6. *Esistono infiniti numeri primi.*

Dimostrazione. Innanzitutto 2 è un numero primo.

Siano poi $p_1, \dots, p_k$ numeri primi naturali e sia $N = p_1 \dots p_k + 1 > 1$. Per il teorema fondamentale ammette un divisore primo p. Tuttavia se per assurdo $p = p_i$, allora p divide $N - p_1 \dots p_k = 1$. Assurdo. □

In verità questo algoritmo produce raramente numeri primi. Anzi più i numeri crescono più questo fenomeno è raro. Inoltre posto $P = \{p_1, \dots, p_k\}$, allora

$$\lim_{n \to +\infty} \frac{\#\{\, k \in \mathbb{N}_+ \mid k \leq n, k \text{ ha solo fattori primi in } P \,\}}{n} = 0$$

Dei primi particolari sono i cosiddetti primi di Mersenne e primi di Fermat. Incominciamo dai primi:

Teorema 2.4.7 (Primi di Mersenne)**.** *Sia un intero positivo della forma $p = a^n - 1$ con $n > 1$. Se esso è primo dispari, allora $a = 2$ e n è primo, e p viene detto Primo di Mersenne.*

Dimostrazione. Essendo p dispari, allora a deve essere pari. Inoltre se n si scomponesse come $n = bc$ con $b, c > 1$, allora p non sarebbe primo. Infatti

$$p = a^n - 1 = a^{bc} - 1 = (a^b - 1)(1 + a^b + a^{2b} + \dots a^{(c-1)b})$$

Inoltre vale la scomposizione

$$a^n - 1 = (a - 1)(a + \dots + a^{n-1})$$

che è banale, essendo $a > 1$, se e solo se $a = 2$. □

L'importanza dei primi di Mersenne risiede nel fatto che verificare la primalità di un numero di Mersenne è più facile rispetto che ad un numero generico. Non a caso i numeri primi più grandi finora conosciuti sono primi di Mersenne. Va detto che non tutti i numeri di Mersenne sono primi. Per esempio $M_{11} = 2^{11} - 1 = 2047 = 23 * 89$.

Invece numeri che sono, quasi ingiustamente, chiamati primi sono i cosiddetti Primi di Fermat:

Teorema 2.4.8 (Primi di Fermat)**.** *Sia $p = 2^n + 1$ un numero primo, con $n \geq 1$. Allora n è una potenza di due e p è un Primo di Fermat.*

Dimostrazione. Se n è dispari maggiore di 1, allora vale la scomposizione

$$2^n + 1 = (2 + 1)(2^{n-1} - \cdots + 1) = 3(2^{n-1} - \cdots + 1)$$

Se in generale esistesse un dispari d maggiore di 1 che divide n, comunque vale la scomposizione

$$2^n + 1 = ((2^{n/d})^d + 1) = (2^{n/d} + 1)((2^{n/d})^{d-1} - \cdots + 1)$$

Quindi n è una potenza di 2. □

In generale, posto $F_n = 2^{2^n} + 1$, solo $F_1, \ldots, F_4$ si sono rivelati essere primi. Fermat calcolò solo questi e congetturò che anche gli altri lo fossero. In verità oggi si crede che anche se $F_1, \ldots, F_4$ non fossero gli unici primi di Fermat, comunque i primi di Fermat sarebbero in un numero finito. Infine, a differenza dei primi di Mersenne, oggi conosciamo la fattorizzazione di pochi primi di Fermat, solo fino a F_{11}, vista la loro crescita esponenziale. In ogni caso, grazie a varie tecniche, si può comunque affermare che per esempio $F_{3329780}$ ha un divisore primo pari a $193 * 2^{3329781} - 1$.

2.5 Classi di Resto

Se la divisione euclidea è lo strumento fondamentale per la teoria dei numeri, le classi di resto ne sono l'oggetto principale. Iniziamo con la definizione di congruenza in modulo:

Definizione 2.5.1. Siano a, b, n due interi con $n \geq 2$. Diciamo che a è congruo a b modulo n, e scriviamo $a \equiv b \pmod{n}$, se n divide $b - a$.

Proposizione 2.5.2. *La congruenza in modulo n è una relazione di equivalenza.*

Dimostrazione. Certamente $a \equiv a \pmod{n}$, in quanto n divide $0 = a - a$.

Se $a \equiv b \pmod{n}$, allora $b - a = kn$. Quindi $a - b = (-k)n$ e $b \equiv a \pmod{n}$.

Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, allora $b - a = kn$ e $c - b = hn$. Quindi $c - a = c - b + b - a = (h + k)n$ e $a \equiv c \pmod{n}$. □

Diamo ora delle caratterizzazioni equivalenti di congruenza, che ci saranno utili in seguito:

Proposizione 2.5.3. *Siano a, b, n interi con $n \geq 2$. Sono fatti equivalenti:*

1. *n divide $b - a$,*

2. *esiste un k intero tale che $b - a = kn$,*

3. *$\{nk + a\}_{k\in\mathbb{Z}} = \{nh + b\}_{h\in\mathbb{Z}}$,*

4. *a e b hanno lo stesso resto della divisione per n.*

Dimostrazione. (1.) $\Rightarrow$ (2.) Ovvio.

(2.) $\Rightarrow$ (3.) Sia $z \in \{nk + a\}_{k\in\mathbb{Z}}$. Allora

$$z = nk_0 + a = nk_0 + b + kn = n(k_0 + k) + b \in \{nh + b\}_{h\in\mathbb{Z}}$$

Quindi $\{nk + a\}_{k\in\mathbb{Z}} \subseteq \{nh + b\}_{h\in\mathbb{Z}}$ e per simmetria vale l'uguaglianza.

(3.) $\Rightarrow$ (4.) Posto r_b il resto della divisione di b per n, sappiamo che $r_b \in \{nh + b\}_{h\in\mathbb{Z}} = \{nk + a\}_{k\in\mathbb{Z}}$.

Quindi $r_b = a + nk_0$ e $a = -k_0 n + r_b$. Per unicità della divisione euclidea, r_a è il resto della divisione di a per n.

(4.) $\Rightarrow$ (1.) Se $a = k_a n + r$ e $b = k_b n + r$. Allora $b - a = (k_b - k_a)n$ e n divide $b - a$. □

Come ogni relazione di equivalenza è possibile parlare di classi di equivalenza, che però, grazie al teorema precedente, assumono una precisa forma.

Definizione 2.5.4. Sia $n \geq 2$ intero e sia a intero. La sua classi di resto, o di congruenza, modulo n è la sua classe di equivalenza per la congruenza modulo n. Per la proposizione precedente equivale a

$$\bar{a} = [a] = \{\, a + kn \mid k \in \mathbb{Z} \,\}$$

Inoltre indichiamo con $\mathbb{Z}/n\mathbb{Z}$ l'insieme di tutte le classi di equivalenza.

Proposizione 2.5.5. *Sia $n \geq 2$ intero. Allora $\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$ e ha cardinalità n.*

Dimostrazione. Sia a intero e poniamo r come il resto della divisione di a per n. Allora $r = a - kn$ è congruo ad a modulo n ed è compreso tra 0 e $n-1$.

D'altra parte presi $1 \leq a, b \leq n-1$, allora essi coincidono con i resti delle rispettive divisioni per n. Quindi se sono congruenti per la proposizione precedente sono uguali. □

Notiamo ora le operazioni di somma e prodotto su $\mathbb{Z}$ tendono a "comportarsi bene" con la congruenza modulo n. Vale infatti il seguente:

Proposizione 2.5.6. *Siano a, b, c, d, m, n interi con $m, n \geq 2$. Allora valgono le seguenti affermazioni*

1. *Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ allora $a + c \equiv b + d \pmod{n}$.*
2. *Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ allora $ac \equiv bd \pmod{n}$.*
3. *Se $a \equiv b \pmod{n}$ e $a \equiv b \pmod{m}$ allora $a \equiv b \pmod{[m,n]}$.*
4. *Se $a \equiv b \pmod{n}$ allora $(a, n) = (b, n)$.*
5. *Se $a \equiv b \pmod{n}$ e m divide n allora $a \equiv b \pmod{m}$.*
6. *Se $a \equiv b \pmod{n}$ allora $ka \equiv kb \pmod{kn}$ per ogni intero k.*
7. *Se $ra \equiv rb \pmod{n}$ con r intero, allora $a \equiv b \pmod{n/(n,r)}$*
8. *$ra \equiv rb \pmod{n}$ se e solo se $a \equiv b \pmod{n/(n,r)}$.*

In particolare la proprietà di cancellazione vale per r, n coprimi.

Dimostrazione. (1.) Se $a = b + kn$ e $c = d + hn$ allora $a + c = b + d + (k + h)n$.

(2.) Se $a = b + kn$ e $c = d + hn$ allora $ac = bd + (bh + ck + khn)n$.

(3.) Se m e n dividono $b - a$, allora $[m, n]$ divide $b - a$.

(4.) Poste le divisioni euclidee $a = k_a n + r$ e $b = k_b n + r$, allora possiamo applicare il lemma 2.2.8 per affermare

$$(a, n) = (a - q_a n, n) = (r, n) = (b - q_b n, n) = (b, n)$$

(5.) Ovvio.

(6.) Se $a = kn + b$, allora $ha = k(hn) + hb$.

(7.) Se $ra \equiv rb \pmod{n}$, allora n divide $rb - ra = r(b - a)$. Quindi $n/(n, r)$ divide $(r/(n, r))(b - a)$.

Essendo $n/(n, r)$ e $r/(n, r)$ coprimi, allora $n/(n, r)$ divide $(b - a)$. Quindi $a \equiv b \pmod{n/(n, r)}$.

(8.) Una freccia è il punto precedente. D'altra parte se a e b sono congrui modulo $n/(n, r)$, allora per il punto 6 $ra \equiv rb \pmod{rn/(n, r)}$. Ma $rn/(n, r)$ è un multiplo di n, quindi per il punto 5 $ra \equiv rb \pmod{n}$. □

2.6 Congruenze Lineari

Passiamo ora alla risoluzioni di congruenze. Partendo dal caso più semplice, una congruenza lineare è una equazione della forma

$$ax \equiv b \pmod{n}$$

con a, b, n interi e $n \geq 2$.

Come è tipico nel caso di problemi lineari, essa ammette un algoritmo risolutivo.

Teorema 2.6.1. *Siano a, b, n interi con $n \geq 2$. Allora la congruenza lineare $ax \equiv b \pmod{n}$ ammette soluzione se e solo se $d = (a, n)$ divide b. In tal caso le soluzioni sono tutti e soli gli interi x tali che*

$$x \equiv x_0 + \frac{n}{d}s \pmod{n} \qquad 0 \leq s \leq d - 1$$

con x_0 una soluzione particolare.

Dimostrazione. Un intero x soddisfa l'equazione se e solo se esiste un intero k_x tale che $ax - k_x n = b$. Quindi le soluzioni della congruenza sono tutti

e soli gli interi x, tale che (x, k_x) è soluzione dell'equazione diofantea lineare $ax - k_x n = b$.

Quindi la congruenza ha soluzioni se e solo se (a, n) divide b. In tal caso gli x soluzione sono, in base al teorema 2.3.10,

$$x = x_0 + \frac{n}{d}t \qquad k \in \mathbb{Z}$$

Sia adesso $t = hd + r$ con $0 \leq r < d$. Allora se x è come sopra

$$x = x_0 + \frac{n}{d}(hd + r) = x_0 + hn + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r \pmod{n}$$

Quindi possiamo riscrivere nel seguente modo le soluzioni:

$$x \equiv x_0 + \frac{n}{d}s \pmod{n} \qquad 0 \leq s \leq d - 1$$

□

Notiamo che il teorema aveva lo scopo di scrivere le soluzioni con lo stesso moduli della congruenza originaria. Nel caso questo non fosse richiesto, è possibile risolvere le congruenze lineari in modo più agile, come vediamo nel seguente esempio.

Esempio. Sia la congruenza $8x \equiv 6 \pmod{18}$. Allora $(8, 42) = 2$, quindi la congruenza ammette forma equivalente $4x \equiv 3 \pmod{9}$. A questo punto notiamo che $4 * 7 = 28 \equiv 1 \pmod{9}$. Inoltre 7 è coprimo con 9. Quindi la congruenza è equivalente a $7 * 4x \equiv 7 * 3 \pmod{9}$, cioè $x \equiv 21 \equiv 3 \pmod{9}$.

Nell'esempio abbiamo trovato l'inverso moltiplicativo di 4 modulo 9. Ne approfittiamo per definire questa quantità:

Definizione 2.6.2. Siano a, n interi con $n \geq 2$, allora a ammette un inverso moltiplicativo modulo n se esiste un intero b tale che $ab \equiv 1 \pmod{n}$.

Dal teorema precedente risulta evidente il seguente importante risultato

Proposizione 2.6.3. *Siano a, n interi con $n \geq 2$. Allora a ammette un inverso moltiplicativo modulo n se e solo se $(a, n) = 1$.*

Dimostrazione. Cercare l'inverso moltiplicativo di a equivale a risolvere la congruenza $ax \equiv 1 \pmod{n}$, che sappiamo ammettere soluzioni se e solo se (a, n) divide 1, cioè se e solo se $(a, n) = 1$. □

Con questa nozione possiamo generalizzare il procedimento dell'esempio precedente.

Sia una congruenza lineare $ax \equiv b \pmod{n}$. Se (a, n) non divide b, allora la congruenza non ammette soluzione.

Altrimenti possiamo passare alla congruenza equivalente

$$ax/(a,n) \equiv b/(a,n) \pmod{n/(a,n)}$$

A questo questo punto sappiamo che $a/(a,n)$ e $n/(a,n)$ sono coprimi. Ergo $a/(a,n)$ ammette un'inverso moltiplicativo d, anch'esso coprimo con $n/(a,n)$. Ergo possiamo passare alla congruenza equivalente

$$(da/(a,n))x \equiv db \pmod{n/(a,n)} \Leftrightarrow x \equiv db \pmod{n/(a,n)}$$

2.7 Sistemi di Congruenze

Ora che abbiamo capito come risolvere le congruenze lineari, passiamo a risolvere i sistemi della forma

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \end{cases}$$

Per quanto osservato prima se esiste un i tale che (a_i, m_i) non divide b_i, allora la relativa congruenza e l'intero sistema non ammettono soluzione.

Altrimenti possiamo risolvere le singole congruenze e supporre, senza perdita di generalità, che il sistema sia della forma

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

La prossima proposizione ne dà la soluzione

Teorema 2.7.1. *Sia il sistema lineare precedente. Allora esso ammette soluzione se e solo se (m, n) divide $b - a$. In tal caso le soluzioni sono tutti e soli gli interi della forma*

$$x \equiv a + k_0 n \pmod{[m, n]}$$

con (k_0, h_0) una soluzione particolare di $b - a = mk - nh$.

Dimostrazione. Risolvere il sistema è equivalente a cercare le terne (x, k, h) soluzioni di

$$\begin{cases} x = a + kn \\ x = b + hm \end{cases}$$

Che è equivalente, posto $x = a+kn$, a cercare le soluzioni (k, h) di $a+kn = b + hm$, cioè di $nk - mh = b - a$.

Come sappiamo questa è una equazione diofantea lineare, che ammette soluzione se e solo se $(-m, n) = (m, n)$ divide $b - a$. E in tal caso le soluzioni sono

$$\begin{cases} k = k_0 + \frac{m}{(m,n)}t \\ h = h_0 + \frac{n}{(m,n)}t \end{cases}$$

Ergo gli interi x che risolvono il sistema sono tutti e i soli della forma

$$x = a + \left(k_0 + \frac{m}{(m, n)t}\right) n = a + k_0 n + [m, n]t$$

cioè

$$x \equiv a + k_0 n \pmod{[m, n]}$$

□

Questo metodo, oltre a essere estremamente macchinoso, non è facilmente estendibile al caso di un sistema con più equazioni lineari. Cioè non è estendibile a sistemi della forma

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

In questo caso viene d'aiuto il *Teorema Cinese del Resto*, che però ha bisogno di questi lemmi che dimostriamo una volta per tutte:

Lemma 2.7.2. *Siano a, m, n interi non nulli. Allora valgono i seguenti:*

1. *$(a, mn) = 1$ se e solo se $(a, m) = 1$ e $(a, n) = 1$.*
2. *Se m e n sono coprimi, allora $(a, mn) = (a, m)(a, n)$.*

Dimostrazione. (1., $\Rightarrow$) Gli interi (a, n) e (a, m) dividono sia a che mn, quindi devono dividere $(a, mn) = 1$. Quindi $(a, m) = (a, n) = 1$.

(1., $\Leftarrow$) Sia $d = (a, mn)$ e supponiamo, per assurdo, che possegga un fattore primo p. Dividendo mn, p deve dividere m o n. Quindi dovrebbe dividere $(a, m) = 1$ o $(a, n) = 1$ rispettivamente. Assurdo. Quindi $d = 1$.

(2.) Innanzitutto vogliamo affermare che preso c divisore di mn, allora $c = (c, m)(c, n)$. Infatti (c, m) e (c, n) dividono entrambi c. Inoltre, essendo m, n coprimi, devono esserlo anche (a, m) e (a, n) per il punto precedente. Quindi per il lemma 2.3.8 c è diviso dal loro prodotto. Poniamo quindi $c = k(c, n)(c, m)$.

L'intero k divide mn e supponiamo che possegga un fattore primo p. Allora p divide mn. Supponiamo, senza perdita di generalità, che divida m. Allo stesso modo anche (c, m) divide m. Quindi entrambi, per il punto precedente, sono come m coprimi con n.

Allora lo è anche il loro prodotto $p(c, m)$. Inoltre esso divide mn. Quindi $p(c, m)$ divide m. Tuttavia $p(c, m)$ non divide (c, m). Assurdo per definizione di massimo comune divisore.

Dimostrato questo fatto preliminare, dimostriamo che $(a, m)(a, n)$ è un massimo comune divisore di mn e a.

Come abbiamo notato in precedenza, (a, m) e (a, n) sono coprimi dividenti a. Quindi il loro prodotto divide a. Inoltre divide banalmente mn.

Sia c che divide a e mn. Per il fatto preliminare possiamo porre $c = (c, m)(c, n)$.

Consideriamo l'intero (c, m). Esso divide sia m sia c, che a sua volta divide a. Quindi (c, m) divide (a, m). Allo stesso modo (c, n) divide (a, n). Quindi c divide $(a, m)(a, n)$. □

A questo punto possiamo enunciare il nostro teorema:

Teorema 2.7.3 (Teorema Cinese del Resto - I Forma)**.** *Sia un sistema di congruenze lineare della forma*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

con a_i interi due a due coprimi e m_i interi maggiori di 1. Allora il sistema ammette un'unica soluzione modulo $m_1 \dots m_n$.

Dimostrazione. Procediamo per induzione su n.

Se $n = 1$, allora il sistema è una congruenza lineare $x \equiv a_1 \pmod{m_1}$. Essendo che $(1, m_1) = 1$ divide a_1, allora il sistema ammette un unica soluzione modulo $m_1/(1, m_1) = m_1$.

Posta l'ipotesi induttiva per $n - 1 \geq 1$, sia il sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Consideriamo allora il sottosistema Γ

$$\Gamma\colon \begin{cases} x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

I fattori sono due a due coprimi, quindi Γ ammette, per ipotesi induttiva, un'unica soluzione $x \equiv x_0 \pmod{m_2 \dots m_n}$. Quindi il sistema originario è equivalente a

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv x_0 \pmod{m_2 \dots m_n} \end{cases}$$

Essendo che m_1 è coprimo con m_i per ogni $2 \leq i \leq n$, per il lemma precedente è anche coprimo con il loro prodotto. Inoltre questo è un sistema a due equazioni, che ha soluzione unica modulo $[m_1, m_2 \dots m_n] = m_1 m_2 \dots m_n$. □

Il teorema cinese del resto non fornisce una formula esplicita per la soluzione. Tuttavia è utile per affermare l'unicità della soluzione trovata, per contemplazione, per $n \geq 3$.

Esempio. Sia il sistema

$$\begin{cases} 4x \equiv 6 \pmod{18} \\ 3x \equiv 4 \pmod{5} \end{cases}$$

Procediamo innanzitutto a normalizzare il sistema. Essendo che $(3,5)=1$, 3 ammette un inverso modulo 5. Infatti $2*3=6\equiv 1 \pmod 5$. Quindi abbiamo il sistema equivalente

$$\begin{cases} 4x \equiv 6 \pmod{18} \\ x \equiv 8 \equiv 3 \pmod 5 \end{cases}$$

Per quanto riguarda la prima congruenza dividiamo innanzitutto per il massimo comune divisore $(4,18)=2$,

$$\begin{cases} 2x \equiv 3 \pmod 9 \\ x \equiv 3 \pmod 5 \end{cases}$$

per poi andare a invertire 2 tramite 5, i suo inverso modulo 9.

$$\begin{cases} x \equiv 15 \equiv 6 \pmod 9 \\ x \equiv 3 \pmod 5 \end{cases}$$

A questo punto, grazie al teorema cinese del resto, sappiamo che ammette un'unica soluzione modulo $9*5=45$. O per contemplazione notiamo che 33 funziona, oppure tramite il metodo descritto ad inizio sezione. Nel secondo caso andiamo a scrivere l'equazione diofantea associata:

$$6+9k=3+5h \;\Rightarrow\; 9k-5h=-3$$

Troviamo una soluzione quindi tramite l'algoritmo di Euclide:

$$\begin{aligned} 9 &= 1*(-5)+4 \\ -5 &= (-2)*4+3 \\ 4 &= 1*3+1 \\ 3 &= 3*1+0 \end{aligned}$$

Il risultato è concorde con la primalità di 5 e 9. Inoltre

$$\begin{aligned} 1 &= 4-1*3 \\ &= 4-1*(-5+2*4) = -1*(-5)-1*4 \\ &= -1*(-5)-1*(9-1*(-5)) = -1*9-2*(-5) \end{aligned}$$

Quindi $(k_0,h_0)=(3,6)$ e la soluzione del sistema, scritta in modulo 45, è

$$x \equiv 6+3*9 \equiv 33 \pmod{45}$$

L'ipotesi di coprimalità dei modulo è essenziale per l'applicazione del teorema cinese del resto. Presentiamo ora un esempio in cui la sua applicazione non è possibile

Esempio. Sia il sistema di congruenze lineari

$$\begin{cases} x \equiv 141 \pmod{7^3} \\ x \equiv 20 \pmod{10} \\ x \equiv 20 \pmod{7} \end{cases}$$

La prima e la terza equazione implicano rispettivamente

$$\begin{cases} x \equiv 141 \equiv 1 \pmod{7} \\ x \equiv 20 \equiv -1 \pmod{7} \end{cases}$$

che è ovviamente un sistema impossibile.

Diamo adesso un interessante metodo per la risoluzione di sistemi di due congruenze lineari, che non necessita del passaggio all'equazione di Bezout associata.

Proposizione 2.7.4. *Siano x_1 e x_2 soluzioni, modulo m_1m_2, dei sistemi di congruenze*

$$\begin{cases} x_1 \equiv 1 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_1} \end{cases} \qquad \begin{cases} x_2 \equiv 0 \pmod{m_1} \\ x_2 \equiv 1 \pmod{m_2} \end{cases}$$

Allora per ogni coppia di interi (a, b), l'intero ax_1+bx_2 è soluzione, modulo m_1m_2, del sistema

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

Dimostrazione. Essendo che x_1 e x_2 risolvono le relative congruenze, allora

$$\begin{cases} ax_1 + bx_2 \equiv a * 1 + b * 0 \equiv a \pmod{m_1} \\ ax_1 + bx_2 \equiv a * 0 + b * 1 \equiv b \pmod{m_2} \end{cases}$$

□

Questo metodo semplifica il lavoro, in quanto è relativamente facile trovare una soluzione intuitiva dei sistemi relativi a x_1 e x_2.

Esempio. Sia il sistema

$$\begin{cases} x \equiv 7 \pmod{13} \\ x \equiv 11 \pmod{27} \end{cases}$$

Allora consideriamo i sistemi associati

$$\Gamma\colon \begin{cases} x_1 \equiv 1 \pmod{13} \\ x_1 \equiv 0 \pmod{27} \end{cases} \qquad \Omega\colon \begin{cases} x_2 \equiv 0 \pmod{13} \\ x_2 \equiv 1 \pmod{27} \end{cases}$$

Il sistema Γ ammette soluzione $x_1 \equiv 27 \pmod{13 * 27}$, mentre Ω ammette soluzione $x \equiv -26 \pmod{13 * 27}$. Quindi il sistema originario ammette soluzione, unica per TCR, pari a

$$x \equiv 7 * 27 - 11 * 26 \equiv -97 \equiv 254 \pmod{351}$$

Chiudiamo questa sezione con una simpatica applicazione del teorema cinese del resto:

Proposizione 2.7.5. *Sia $n \geq 1$ intero. Allora valgono i seguenti:*

1. *esistono n interi consecutivi non primi,*
2. *esistono n interi consecutivi non primi e arbitrariamente grandi*
3. *esistono n interi consecutivi non potenze perfette, cioè non della forma a^b con b maggiore di 1, arbitrariamente grandi.*

Dimostrazione. (1.) I seguenti numeri:

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$$

sono rispettivamente divisibili da e maggiori di $2, 3, \ldots, n+1$. Quindi non sono primi.

(2.) Sia $M \geq 1$. Per infinità dei numeri primi esistono $p_1, \ldots, p_n$ primi. Sia quindi il sistema

$$\begin{cases} x \equiv 0 & \pmod{p_1} \\ x + 1 \equiv 0 & \pmod{p_2} \\ \ldots & \ldots \\ x + (n-1) \equiv 0 & \pmod{p_n} \end{cases}$$

Per il TCR esiste una soluzione (unica) modulo $p_1 \dots p_n$. A questo punto basta prendere x soluzione maggiore di M e $p_1 \dots p_n$. In questo modo i singoli $x + i$ sono maggiori di M e p_i. Quindi sono non primi maggiori di M.

(3.) Per questo punto osserviamo un fatto generale: se k è un intero congruo a p modulo p^2 con p primo, allora non può essere potenza perfetta.

Infatti se $k \equiv p \pmod{p^2}$, allora $x \equiv p \equiv 0 \pmod{p}$. Se per assurdo $k = a^b$, allora p divide a^b, quindi divide a per primalità. Essendo b maggiore di 1, questo implica che p^2 divide k e $p \equiv k \equiv 0 \pmod{p^2}$. Assurdo in quanto $p < p^2$.

Detto questo è immediato che, posto

$$\begin{cases} x \equiv p_1 & (\text{mod } p_1^2) \\ x + 1 \equiv p_2 & (\text{mod } p_2^2) \\ \dots & \dots \\ x + (n-1) \equiv p_n & (\text{mod } p_n^2) \end{cases}$$

allora la soluzione modulo $p_1 \dots p_n$, data da TCR, fornisce la soluzione al problema. Inoltre come prima può essere resa arbitrariamente grande. □

2.8 Congruenze di Grado Superiore

Analizziamo ora congruenze oltre quelle lineari. Per esse non c'è un metodo generale, per lo più la risoluzione si basa sul raccoglimento e le proprietà dei primi.

Fondamentale è questa osservazione:

Proposizione 2.8.1. *Siano due interi a, b e sia p primo. Se $ab \equiv 0 \pmod{p}$, allora $a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p}$.*

Dimostrazione. Se $ab \equiv 0 \pmod{p}$, allora p divide ab. Per primalità p divide a o b. Da cui la tesi. □

Possiamo quindi già affermare un importante risultato:

Teorema 2.8.2. *Sia una congruenza di secondo grado $ax^2+bx+c \equiv 0 \pmod{p}$ con $a \neq 0$ e p primo. Allora o essa non ammette alcuna soluzione modulo p,*

oppure ne ammette al massimo 2 legate da

$$\begin{cases} x_1 \equiv -x_0 - a^{-1}b & (\text{mod } p) \\ x_1 \equiv x_0 & (\text{mod } p) \end{cases}$$

Dimostrazione. Siano x_0, x_1 due soluzioni della nostra equazione. Allora

$$\begin{aligned} a(x_0^2 - x_1^2) + b(x_0 - x_1) &\equiv 0 \pmod{p} \\ a(x_0 + x_1)(x_0 - x_1) + b(x_0 - x_1) &\equiv 0 \pmod{p} \\ (x_0 - x_1)\left[a(x_0 + x_1) + b\right] &\equiv 0 \pmod{p} \end{aligned}$$

Quindi o $x_1 \equiv x_0 \pmod{p}$ oppure $a(x_0+x_1)+b \equiv 0 \pmod{p}$. Nel secondo caso

$$x_1 \equiv -x_0 - a^{-1}b \pmod{p}$$

□

Se p non è primo questo non è vero, per esempio $x^2 \equiv 1 \pmod 8$ ha soluzioni $x \equiv 1, 3, 5, 7 \pmod 8$.

Partendo dall'esempio, risolviamo l'equazione $x^2 \equiv 1 \pmod 1$ in generale:

Teorema 2.8.3. *Sia $n \geq 2$ intero. Allora, posto $n = 2^\alpha p_1^{e_1} \dots p_k^{e_k}$, l'equazione $x^2 \equiv 1 \pmod n$ ha $y(\alpha)2^k$ soluzioni, con*

$$y(\alpha) = \begin{cases} 1 & \alpha = 0, 1 \\ 2 & \alpha = 2 \\ 4 & \alpha \geq 3 \end{cases}$$

Dimostrazione. Risolviamo innanzitutto $x^2 \equiv 1 \pmod{p^k}$ con p primo.

$(p = 2, k = 1)$. In questo caso abbiamo unica soluzione $x \equiv 1 \pmod 2$.

$(p = 2, k \geq 2)$ Notiamo innanzitutto che se $(x + 1)(x - 1) \equiv 0 \pmod{2^k}$, allora 2^{k-1} deve dividere uno dei due membri. Infatti $(x+1, x-1) = (x+1, 2)$. Quindi $x + 1$ e $x - 1$ possono al più avere un fattore 2 in comune. Ma allora se 2^k divide il loro prodotto, può solo essere che 2^{k-1} divida uno dei due (a questo punto la parità dell'altro è automatica).

Quindi le soluzioni sono $x \equiv \pm 1 \pmod{2^{k-1}}$, cioè

$$x \equiv 1, 2^{k-1} - 1, 2^{k-1} + 1, -1 \pmod{2^k}$$

che sono 2 soluzioni distinte se $k = 2$ e 4 soluzioni distinte per $k \geq 3$.

($p > 2$) Essendo che $(x+1, x-1) = (x+1, 2)$, allora i fattori $x+1$ e $x-1$ non possono avere fattori p in comune. Quindi se p^k divide $(x+1)(x-1)$, esso deve dividere $x+1$ o $x-1$.

Quindi $x \equiv \pm 1 \pmod{p^k}$

A questo punto presa la congruenza $x^2 \equiv 1 \pmod{n}$, essa è equivalente al sistema

$$\begin{cases} x^2 \equiv 1 \pmod{2^\alpha} \\ x^2 \equiv 1 \pmod{p_1^{e_1}} \\ \dots \\ x^2 \equiv 1 \pmod{p_k^{e_k}} \end{cases}$$

che dà il risultato. □

2.9 Operazioni su $\mathbb{Z}/n\mathbb{Z}$

L'insieme $\mathbb{Z}/n\mathbb{Z}$ non è un semplice insieme di classi, ma ha qualcosa in più. Infatti ci darà il primo esempio di anello, di gruppo e, qualche volta, di campo.

Iniziamo subito con questa osservazione: su $\mathbb{Z}$ sono definite due operazioni, somma e prodotto, che si possono portare al quoziente:

Teorema 2.9.1. *Siano due classi $[a]$, $[b]$ in $\mathbb{Z}/n\mathbb{Z}$. Definiamo la loro somma e prodotto come*

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

Queste operazioni sono ben definite.

Dimostrazione. Dobbiamo verificare che il risultato non dipende dal rappresentante scelto. Presi $[a] = [a + kn]$, $[b] = [b + hn]$, allora

$$[a + kn] + [b + hn] = [a + kn + b + hn] = [a + b + (k + h)n] = [a + b]$$
$$[a + kn][b + hn] = [(a + kn)(b + hn)] = [ab + (bk + ah + khn)n] = [ab]$$

□

Queste operazioni godono di importanti proprietà, portate dalle proprietà delle operazioni su $\mathbb{Z}$.

Per la somma:

1. è associativa,
2. ammette elemento neutro $[0]_n$,
3. ogni elemento $[a]$ ammette un inverso $[-a]$,
4. è commutativa

Mentre per il prodotto:

1. è associativo,
2. ammette elemento inverso $[1]_n$,
3. è commutativo
4. distribuisce rispetto alla somma

Cioè $\mathbb{Z}/n\mathbb{Z}$ munito della somma è un *gruppo abeliano*, mentre munito di somma e prodotto è un *anello commutativo con identità*.

Per quanto riguarda il prodotto, non è detto che ogni elemento di $\mathbb{Z}/n\mathbb{Z}$ abbia un inverso moltiplicativo. Tuttavia sappiamo che $[a] \in \mathbb{Z}/n\mathbb{Z}$ ammette un inverso moltiplicativo se e solo se $(a, n) = 1$. Questa relazione non dipende dal rappresentante scelto, in quanto $(a, n) = (a + kn, n)$.

Inoltre se $[a]$,$[b]$ ammettono inverso, allora a,b, e quindi ab, sono coprimi con n. Quindi ab ammette inverso. Quindi se definiamo

$$\mathbb{Z}/n\mathbb{Z}^* = \{\, [a] \in \mathbb{Z}/n\mathbb{Z} \mid [a] \text{ invertibile} \,\},$$

allora abbiamo una mappa ben definita

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^* &\to \mathbb{Z}/n\mathbb{Z}^* \\ ([a], [b]) &\mapsto [a][b] \end{aligned}$$

Quindi possiamo tranquillamente dire il seguente:

Proposizione 2.9.2. *Sia $n \geq 2$ intero. Allora $\mathbb{Z}/n\mathbb{Z}^*$, munito con il prodotto, è un gruppo abeliano. Inoltre se $n = p$ è primo, allora $\mathbb{Z}/p\mathbb{Z}$ è un campo.*

Dimostrazione. (1.) Le proprietà del prodotto le conosciamo. L'unico controllo, fatto precedentemente, è che il prodotto di due elementi di $\mathbb{Z}/n\mathbb{Z}^*$ stia in $\mathbb{Z}/n\mathbb{Z}^*$.

(2.) Per ogni $[a] \in \mathbb{Z}/p\mathbb{Z}$ non nullo, $(a, p) = 1$. Quindi ogni elemento non nullo è invertibile, cioè $\mathbb{Z}/p\mathbb{Z}$ oltre ad essere anello commutativo con identità è un campo. □

Diamo ora unna nuova versione del teorema cinese del resto:

Teorema 2.9.3 (Teorema Cinese del Resto - II Forma)**.** *Siano $m, n \geq 2$ interi. Allora la mappa*

$$\Phi \colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

è ben definita, ed è bigettiva se e solo se m e n sono coprimi.

Dimostrazione. Innanzitutto se a e b sono equivalenti modulo mn, allora lo sono anche modulo m e n. Quindi Φ è ben definita.

($\Leftarrow$) Preso $([x]_m, [y]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, allora trovare una sua preimmagine significa risolvere il seguente sistema modulo mn:

$$\begin{cases} a \equiv x \pmod{m} \\ a \equiv y \pmod{n} \end{cases}$$

I numeri m e n sono coprimi, quindi il sistema ammette soluzione grazie alla prima forma del TCR.

Quindi Φ è suggettiva, ed è anche iniettiva grazie alle equicardinalità finita di $\mathbb{Z}/mn\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/nZ$.

($\Rightarrow$) Se $(m, n) = d > 1$, allora il seguente sistema:

$$\begin{cases} x \equiv 0 \pmod{m} \\ x \equiv 1 \pmod{n} \end{cases}$$

non ha soluzione, in quanto $(m, n) = d$ non divide $1 - 0 = 1$. Quindi Φ non è suggettiva. □

Corollario 2.9.4. *Se $(m, n) = 1$ allora la seguente mappa*

$$\Phi^* \colon \mathbb{Z}/mn\mathbb{Z}^* \to \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

è ben definita e bigettiva.

Dimostrazione. Grazie al teorema precedente è sufficiente vedere la buona definizione di Φ^* e della sua inversa. Tuttavia questo è immediato, in quanto $[a]_{mn}$ è invertibile se e solo se a e mn sono coprimi. Questo è equivalente a chiedere che a sia coprimo con m e n, cioè che $[a]_m$ e $[a]_n$ siano invertibili. □

2.10 Funzioni Aritmetiche

Legate ai scomposizioni in fattori primi esistono tutta una serie di funzioni con dominio nei naturali, dette funzioni aritmetiche, legate alle proprietà aritmetiche dell'argomento. Fondamentali sono queste definizioni:

Definizione 2.10.1. Sia $f\colon \mathbb{N}_+ \to \mathbb{C}$ funzione aritmetica. Essa si dice

1. Additiva, se per ogni m,n coprimi $f(mn) = f(m) + f(n)$.
2. Completamente Additiva, se per ogni m, n $f(mn) = f(m) + f(n)$.
3. Moltiplicativa, se per ogni m,n coprimi $f(mn) = f(m)f(n)$.
4. Completamente Additiva, se per ogni m, n $f(mn) = f(m)f(n)$.

Un primo esempio è il seguente:

Definizione 2.10.2. Sia $n \in \mathbb{N}_+$. Definiamo $\tau(n)$ come il numero di divisori in $\mathbb{N}_+$ di n.

Teorema 2.10.3. *Sia $n \in \mathbb{N}_+$. Allora, posto $n = p_1^{e_1} \dots p_k^{e_k}$ con p_i distinti,*

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1)$$

Dimostrazione. Se $n = 1$, allora ha senso porre $e_i = 0$ per ogni i. Quindi $\tau(1) = 1$ è in accordo con la formula.

Supponiamo $n > 1$. Vogliamo dimostrare che i divisori di n sono tutti e soli i numeri interi della forma

$$d = p_1^{f_1} \dots p_f^{f_k} \qquad 0 \leq f_i \leq e_i$$

che dà il risultato.

Da una parte, data la scelta degli f_i, questi sono certamente divisori di n.

D'altra parte sia d divisore di n in $\mathbb{N}_+$. Scomponiamo d in divisori primi ponendo $d = q_1^{f_1} \dots q_r^{f_r}$ con q_i distinti. Essendo d divisori vale

$$p_1^{e_1} \dots p_k^{e_k} = n = dm = q_1^{f_1} \dots q_r^{f_r} m$$

Per il teorema fondamentale dell'algebra la fattorizzazione è unica, quindi $\{q_1, \dots q_r\} \subseteq \{p_1, \dots, p_k\}$. Se poi ammettiamo che f_i possano essere nulli vale l'uguaglianza. Quindi $r = k$ e, a meno dell'ordine, $p_i = q_i$. Ma per poter valere l'uguaglianza deve essere $0 \leq f_i \leq e_i$. □

Per quanto la moltiplicatività/additività di $\tau(n)$ vale

Teorema 2.10.4. *La funzione $\tau(n)$ è moltiplicativa, ma non completamente moltiplicativa.*

Dimostrazione. Siano m, n numeri interi positivi coprimi. Allora possiamo porre

$$m = p_1^{e_1} \dots p_k^{e_k}$$
$$n = q_1^{f_1} \dots q_h^{f_h}$$

con $\{q_i, p_i\}$ tutti distinti. Quindi mn ammette fattorizzazione con fattori primi distinti: $mn = p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_h^{f_h}$.

Ergo

$$\tau(mn) = \prod_{i=1}^{k}(e_i + 1) \prod_{j=1}^{h}(f_i + 1) = \tau(m)\tau(n)$$

D'altra parte τ non è completamente moltiplicativa. Infatti sia $m, n = 2$. Allora $\tau(2 * 2) = \tau(4) = 3 \neq 4 = \tau(2)\tau(2)$. □

Un'altra funzione aritmetica importante è la cosiddetta funzione p-adica.

Definizione 2.10.5. Sia $n \in \mathbb{N}_+$ e sia p primo. Definisco la valutazione p-adica di n, indicata con $v_p(n)$, come la massima potenza di p che divide n. Cioè, sfruttando il teorema fondamentale dell'aritmetica, se n si scompone in primi come $n = p^\alpha q$, con $(p, q) = 1$, allora $v_p(n) = \alpha$.

Teorema 2.10.6. *La valutazione p-adica è completamente additiva.*

Dimostrazione. Siano m, n naturali positivi. Se $v_p(m) = \alpha$, $v_p(m) = \beta$, allora

$$\begin{aligned} m &= p^\alpha k \qquad (k,p) = 1 \\ n &= p^\beta h \qquad (h,p) = 1 \end{aligned}$$

Quindi $mn = p^{\alpha+\beta}kh$ e $(p, kh) = 1$. Quindi $v_p(mn) = \alpha + \beta = v_p(m) + v_p(n)$. □

Interessante è il calcolo di $v_p(n!)$. Infatti vale la seguente proposizione:

Proposizione 2.10.7 (Identità di Legendre - de Polignac)**.** *Sia $n \in \mathbb{N}_+$, Allora*

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

dove con $\lfloor x \rfloor$ denotiamo la parte intera inferiore di x, cioè il più grande intero minore o uguale a x.

Dimostrazione. Sia un certo numero k compreso tra n e 1. Allora $v_p(k) = h$ se e solo se 2^h, e non 2^{h+1}, divide k. Quindi se consideriamo la fattorizzazione di $n!$, essa presenta un fattore p per ogni multiplo di p in $\{1, \ldots, n\}$, un ulteriore fattore p per ogni multiplo di p^2 etc. Quindi

$$v_p(n!) = \sum_{k=1}^{n} v_p(k) = \sum_{k=1}^{n} \# \left\{ \, 1 \le d \le n \;\middle|\; p^k \mid d \, \right\} = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

- □

La terza funzione di cui parliamo è la seguente:

Definizione 2.10.8. Sia $n \in \mathbb{N}_+$. Definiamo $\sigma_k(n)$ come la somma delle potenze k-esime dei divisori positivi di n incluso 1 e n.

Diamo la formula esplicita con questo teorema:

Teorema 2.10.9. *La funzione σ_k è moltiplicativa. Inoltre se $n = 1$, $\sigma_k(n) = 1$. Altrimenti se $n = p_1^{e_1} \ldots p_k^{e_k}$*

$$\sigma_k(n) = \prod_{i=1}^{k} \frac{p_i^{(e_i+1)k} - 1}{p_i^k - 1}$$

Dimostrazione. Siano $(a, b) = 1$. Come abbiamo già visto nel lemma 2.7.2, per ogni d divisore di ab, d si scompone come $d = (d, a)(d, b)$.

Abbiamo quindi una bigezione

$$\begin{aligned} \{\text{divisori di } ab\} &\to \{\text{divisori di } a\} \times \{\text{divisori di } b\} \\ d &\mapsto ((a, d), (b, d)) \end{aligned}$$

con inversa

$$\begin{aligned} \{\text{divisori di } a\} \times \{\text{divisori di } b\} &\to \{\text{divisori di } ab\} \\ (d_1, d_2) &\mapsto d_1 d_2 \end{aligned}$$

□

Quindi possiamo scrivere

$$\begin{aligned} \sigma_k(ab) &= \sum_{d|ab} d^k = \sum_{d_1|a} \sum_{d_2|b} (d_1 d_2)^k \\ &= \sum_{d_1|a} d_1^k \sum_{d_2|b} d_2^k = \sigma_k(a)\sigma_k(b) \end{aligned}$$

A questo punto possiamo considerare $n = p_1^{e_1} \dots p_k^{e_k}$

$$\begin{aligned} \sigma_k(n) &= \sigma_k(p_1^{e_1} \dots p_k^{e_k}) = \sigma_k(p_1^{e_1}) \dots \sigma(p_k^{e_k}) \\ &= \prod_{i=1}^{k} \sum_{j=0}^{e_i} p_i^{jk} = \prod_{i=0}^{k} \frac{p_i^{(e_i+1)k} - 1}{p_i^k - 1} \end{aligned}$$

Nella prossima sezione vederemo una tra le funzioni aritmetiche più importanti: la φ di Eulero.

2.11 La φ di Eulero

Definizione 2.11.1. Sia $n \geq 1$ intero. Indichiamo con $\varphi(n)$ il numero di interi $1 \leq k \leq n$ coprimi con n. Equivalentemente, per $n > 1$, è la cardinalità di $\mathbb{Z}/n\mathbb{Z}^*$.

Come le altre funzioni aritmetiche è importante avere una formula quasi esplicita. Il prossimo teorema la dà:

Teorema 2.11.2. *La φ di Eulero è moltiplicativa. Inoltre se $n = 1$, allora $\varphi(n) = 1$, altrimenti se $n = p_1^{e_k} \dots p_k^{e_k}$, allora*

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}$$

Dimostrazione. Ovviamente $\varphi(1) = 1$.

Siano m,n interi coprimi. Se uno di due è 1, allora banalmente $\varphi(mn) = \varphi(m)\varphi(n)$. Altrimenti, grazie al corollario 2.9.4 sappiamo che $\mathbb{Z}/mn\mathbb{Z}^*$ e $\mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$ hanno la stessa cardinalità. Quindi $\varphi(mn) = \varphi(m)\varphi(n)$.

Avendo dimostrato che φ è moltiplicativa, basta calcolarla per una potenza di un primo $n = p^e$.

In questo caso sia $1 \leq m \leq n$ non coprimo con n. Allora n deve contenere p, l'unico fattore di n. Quindi m è della forma $m = pd$, con $1 \leq d \leq p^{e-1}$.

Cioè abbiamo p^{e-1} interi tra 1 e n non coprimi con n. Quindi otteniamo $\varphi(n) = p^e - p^{e-1} = (p-1)p^{e-1}$ □

Questa funzione gioca un ruolo fondamentale per i prossimi teoremi che andremo a dimostrare: il *Piccolo Teorema di Fermat* e il *Teorema di Eulero.* Per dimostrarli dobbiamo passare però per questo risultato:

Teorema 2.11.3 (Teorema del Binomio Ingenuo)**.** *Sia p primo. Allora per ogni coppia di interi x, y vale*

$$(x + y)^p \equiv x^p + y^p \pmod{p}$$

Dimostrazione. Notiamo innanzitutto che per ogni intero $1 \leq i \leq p - 1$, p divide $\binom{p}{i}$. Infatti

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

e p divide il numeratore ma non il denominatore. Essendo p primo, esso deve dividere il rapporto.

Quindi

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

□

Enunciamo quindi il primo importante teorema:

Teorema 2.11.4 (Piccolo Teorema di Fermat)**.** *Sia p primo e x intero. Allora*

$$x^p \equiv x \pmod{p}$$

.

Dimostrazione. ($x \geq 0$) Dimostriamolo per induzione su x.

Per $x = 0$, allora $0^p = 0$, quindi sono in particolar modo congruenti.

Sia ora $x \geq 0$ per cui vale l'ipotesi induttiva. Allora

$$(x+1)^p \equiv x^p + 1^p \equiv x + 1 \pmod{p}$$

($x < 0$) In questo caso $-x > 0$. Quindi $(-x)^p \equiv -x \pmod{p}$.

Se $p > 2$, allora $(-x)^p = -x^p$, da cui la tesi.

Se $p = 2$, allora $x^2 \equiv (-x)^2 \equiv -x \equiv x \pmod{p}$ □

Corollario 2.11.5. *Sia p primo e x intero coprimo con p. Allora*

$$x^{p-1} \equiv 1 \pmod{p}$$

.

Dimostrazione. Essendo x coprimo con p, allora $\bar{x}$ ammette un inverso in $\mathbb{Z}/p\mathbb{Z}^*$. Quindi

$$\bar{x}^{p-1} = \bar{x}^p \bar{x}^{-1} = \bar{x}\bar{x}^{-1} = \bar{1}$$

□

Corollario 2.11.6. *Sia p primo e x intero coprimo con p. Allora $\bar{x}$ ammette $\bar{x}^{p-2}$ come inverso in $\mathbb{Z}/p\mathbb{Z}^*$.*

Dimostrazione. Per verifica diretta

$$\bar{x}^{p-2}\bar{x} = \bar{x}^{p-1} = \bar{1}$$

□

E se p non fosse primo? La risposta viene dalla generalizzazione del piccolo teorema di Fermat, il teorema di Eulero:

Teorema 2.11.7 (Teorema di Eulero)**.** *Siano x, m interi con $m \geq 2$. Se sono coprimi, allora*

$$x^{\varphi(m)} \equiv 1 \pmod{m}$$

Dimostrazione. Sia la mappa

$$\Phi\colon \mathbb{Z}/m\mathbb{Z}^* \to \mathbb{Z}/m\mathbb{Z}^*$$
$$\bar{a} \mapsto \bar{a}\bar{x}$$

Questa mappa è iniettiva. Infatti se $\bar{a_1}\bar{x} = \bar{a_2}\bar{x}$, allora

$$\bar{a}_1 = \bar{a}_1\bar{x}\bar{x}^{-1} = \bar{a}_2\bar{x}\bar{x}^{-1} = \bar{a}_2$$

Quindi Φ è una mappa iniettiva tra insiemi finiti equicardinali. Allora è suggettiva e possiamo scrivere

$$\mathbb{Z}/m\mathbb{Z}^* = \{\bar{x}\bar{a}_1, \ldots, \bar{x}\bar{a}_{\varphi(m)}\}$$

da cui

$$\bar{c} = \prod_{i=1}^{\varphi(m)} \bar{a}_i = \prod_{i=1}^{\varphi(m)} \bar{x}\bar{a}_i = \bar{x}^{\varphi(m)}\bar{c}$$

Infine $\bar{c}$ è un elemento di $\mathbb{Z}/m\mathbb{Z}^*$, quindi

$$\bar{x}^{\varphi(m)} = \bar{x}^{\varphi(m)}\,\bar{c}\,\bar{c}^{-1} = \bar{c}\bar{c}^{-1} = \bar{1}$$

□

Riguardo alla φ di Eulero proponiamo due esercizi interessanti:

Esercizio. Troviamo tutti gli interi $n \geq 1$ tali che $\varphi(n) = 2/5n$. Sicuramente 1 non é soluzione. Quindi scomponendo n come $p_1^{e_1} \ldots p_k^{e_k}$ possiamo porre

$$\frac{2}{5} = \frac{\varphi(n)}{n} = \frac{(p_1 - 1)\ldots(p_k - 1)}{p_1 \ldots p_k} = \left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

Cioè abbiamo l'uguaglianza

$$2p_1 \ldots p_k = 5(p_1 - 1)\ldots(p_k - 1)$$

Senza perdita di generalità possiamo supporre che $p_1 < \cdots < p_k$. Quindi dalla precedente uguaglianza otteniamo che $p_k = 5$.

Quindi sostituendo 5 otteniamo

$$2p_1 \ldots p_k = 5(p_1 - 1)\ldots(p_{k-1} - 1)4$$
$$p_1 \ldots p_k = 5(p_1 - 1)\ldots(p_{k-1} - 1)2$$

Quindi il membro sinistro é pari, da cui $p_1 = 2$. Ergo

$$p_2 \dots p_k = 5(p_1 - 1) \dots (p_{k-1} - 1)$$

Questa espressione é chiaramente impossibile, a meno che n non abbia come soli divisori primi 2 e 5. Quindi $n = 2^a 5^b$, con $a, b \geq 1$.

Esercizio. Consideriamo le funzioni aritmetiche $\varphi(n)$ e $\tau(n)$. Preso un naturale n positivo, allora i seguenti insiemi

$$D = \{ k \in \mathbb{N}_n \mid k \mid n \}$$
$$P = \{ k \in \mathbb{N}_n \mid (k, n) = 1 \}$$

hanno $\{1\}$ come unica intersezione. Ergo $|D| \cup |P|$ vale al più $n + 1$, cioè $\varphi(n) + \tau(n) \leq n + 1$.

D'altra parte ci si potrebbe chiedere quando vale l'uguaglianza. Per un primo p, vale $\varphi(p) = p - 1$ e $\tau(p) = 2$. Quindi $\varphi(p) + \tau(p) = p + 1$. Vogliamo dimostrare che non ci sono altre soluzioni a parte $n = 1, 4$.

Sia n una soluzione diversa da 1 e consideriamo p_1 il suo più piccolo divisore primo. Allora

$$(n, n - p_1) = (n, p_1) = p_1$$

Quindi $n - p_1$ non è coprimo con n. Deve essere quindi un suo divisore.

Allora $n - p_1$ è al più $n/2$, cioè p_1 è almeno $n/2$. Da cui

$$n = p_1^{e_1} \dots p_r^{e_r} \leq 2p_1$$

E quindi

$$p_1^{e_1 - 1} \dots p_r^{e_r} \leq 2$$

Questa cosa è possibile solo se $e_1 - 1 \leq 1$, $r = 1$. Quindi o $n = p_1$ primo, o $n = 2^2 = 4$.

2.12 Congruenze Esponenziali

Andiamo ora a risolvere congruenze esponenziali, cioè della forma

$$a^x \equiv b \pmod{m}$$

Per procedere dobbiamo prima introdurre un concetto, che riprenderemo appena inizieremo con i gruppi:

Definizione 2.12.1. Siano m, a interi coprimi, con $m \geq 2$. Definiamo l'ordine moltiplicativo di $\bar{a}$ in $\mathbb{Z}/m\mathbb{Z}^*$ come

$$o(a) = min \left\{ k > 0 \;\middle|\; a^k \equiv 1 \pmod{m} \right\}$$

dove l'insieme non è vuoto in quanto vi appartiene $\varphi(m)$.

L'ordine moltiplicativo è essenziale per risolvere le congruenze esponenziali, come le seguenti:

Teorema 2.12.2. *Siano m, a interi coprimi, con $m \geq 2$. Allora la soluzione di*

$$a^x \equiv 1 \pmod{m}$$

è

$$x \equiv 0 \pmod{o(a)}$$

Dimostrazione. Certamente se x è diviso da $o(a)$, allora $x = o(a)k$ e

$$a^x \equiv (a^{o(a)})^k \equiv 1^k \equiv 1 \pmod{m}$$

D'altra parte sia x un intero tale che $a^x \equiv 1 \pmod{m}$. Allora se lo dividiamo per $o(a)$, ponendo $x = ko(a) + r$, abbiamo

$$1 \equiv a^x \equiv a^{ko(a)+r} \equiv (a^{o(a)})^k a^r \equiv a^r \pmod{m}$$

Quindi o $0 < r < o(a)$, ma in tal caso violerebbe la minimalità di $o(a)$, oppure $r = 0$, cioè $o(a)$ divide x. □

Notiamo che questo teorema, a differenza dei precedenti, non dà una formula risolutiva. Sappiamo sì che l'ordine di a è minore o uguale a $\varphi(m)$, però c'è modo di sapere quale sia. Quella che stiamo facendo è sostanzialmente il calcolo di un logaritmo modulo m, un operazione che per m elevati diventa computazionalmente impossibile.

Tuttavia sappiamo almeno che la congruenza ammette soluzione. Per congruenze più generali ciò è falso:

Teorema 2.12.3. *Siano a, b, m interi con $m \geq 2$ e $(a, m) = 1$ e sia la seguente congruenza esponenziale:*

$$a^x \equiv b \pmod{m}$$

Se essa ammette soluzione x_0, l'insieme di tutte le soluzioni è dato da

$$x \equiv x_0 \pmod{o(a)}$$

Dimostrazione. Essendo che $a \in \mathbb{Z}/m\mathbb{Z}^*$, anche b vi appartiene essendo un suo prodotto. Quindi indicando con a^{-x_0} l'inverso di a^{x_0}, abbiamo

$$a^x \equiv a^{x_0} \pmod{m} \Leftrightarrow a^{x-x_0} \equiv 1 \pmod{m} \Leftrightarrow x - x_0 \equiv 0 \pmod{o(a)}$$

□

Diamo ora qualche esempio di congruenza esponenziale:

Esempio. Risolviamo il sistema

$$\begin{cases} 2^x \equiv 1 \pmod{3} \\ 2^x \equiv 1 \pmod{5} \\ 2^x \equiv 1 \pmod{7} \end{cases}$$

Andiamo a calcolare gli ordini di 2 modulo 3,

$$2^1 \equiv 2 \pmod{3}$$
$$2^2 \equiv 4 \equiv 1 \pmod{3}$$

modulo 5,

$$2^1 \equiv 2 \pmod{5}$$
$$2^2 \equiv 4 \pmod{5}$$
$$2^3 \equiv 8 \equiv 3 \pmod{5}$$
$$2^4 \equiv 6 \equiv 1 \pmod{5}$$

e modulo 7

$$2^1 \equiv 2 \pmod{7}$$
$$2^2 \equiv 4 \pmod{7}$$
$$2^3 \equiv 8 \equiv 1 \pmod{7}$$

Quindi abbiamo il sistema equivalente

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 0 \pmod{4} \\ x \equiv 0 \pmod{3} \end{cases}$$

La prima equazione è superflua essendoci la seconda. Quindi otteniamo

$$\begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 0 \pmod{3} \end{cases}$$

Che ammette soluzione, unica per TCR, $x \equiv 0 \pmod{12}$.

Esempio. Risolviamo ora $2^x \equiv 23 \pmod{105}$. Scomponendo 105 in fattori primi otteniamo, per TCR, il sistema equivalente

$$\begin{cases} 2^x \equiv 23 \equiv 2 \pmod 3 \\ 2^x \equiv 23 \equiv 3 \pmod 5 \\ 2^x \equiv 23 \equiv 2 \pmod 7 \end{cases}$$

Riguardando i conti precedenti osserviamo che $2 \equiv 2^1 \pmod 3$, $3 \equiv 2^3 \pmod 5$, $2 \equiv 2^1 \pmod 7$. Ergo

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 3 \end{cases}$$

Essendo che $(4, 2) = 2$ divide $3 - 1 = 2$, il sottosistema costituito dalle prime due equazioni ammette soluzione unica modulo $[4, 2] = 4$. Ergo abbiamo il sistema equivalente

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 3 \end{cases}$$

Quindi abbiamo soluzione, unica per TCR, pari a $x \equiv 7 \pmod{12}$.

2.13 Idem- e Nilpotenti

Ora che i fatti fondamentali sono stati spiegati, le prossime sezioni riguarderanno argomenti marginali o comunque secondari. Ho fatto del mio meglio per raggrupparli in base alle lezioni effettuate. La sezione finale "Miscellanea" ha esattamente lo scopo di raggruppare esercizi o risultati a se stanti.

Iniziamo col primo argomento di questa sezione: i nilpotenti.

Definizione 2.13.1. Sia $m \geq 2$ intero. Allora un elemento $\bar{x}$ di $\mathbb{Z}/m\mathbb{Z}$ si dice idempotente se $x^2 \equiv x \pmod m$.

Teorema 2.13.2. *Se $m = p_1^{e_1} \dots p_k^{e_k}$, allora gli elementi $\bar{x}$ idempotenti sono 2^k, tutti e sole le soluzioni di:*

$$\begin{cases} x \equiv 1, 0 \pmod{p_1^{e_1}} \\ \dots \\ x \equiv 1, 0 \pmod{p_k^{e_k}} \end{cases}$$

Dimostrazione. L'equazione

$$x^2 \equiv x \pmod{m}$$

si può disaccoppiare, per TCR, nel sistema

$$\begin{cases} x^2 \equiv x \pmod{p_1^{e_1}} \\ \dots \\ x^2 \equiv x \pmod{p_k^{e_k}} \end{cases}$$

A questo punto consideriamo una singola congruenza $x^2 \equiv x \pmod{p_i^{e_i}}$, riscrivibile come

$$x(x-1) \equiv 0 \pmod{p_i^{e_i}} \tag{2.2}$$

Notiamo che x e $x-1$ non possono avere contemporaneamente un fattore primo in comune, in quanto $(x, x-1) = (1, x-1) = 1$. Quindi se $p_i^{e_i}$ divide $x(x-1)$, allora deve dividere x o $x-1$.

Quindi la congruenza (2.2) ammette uniche soluzione $x \equiv 0, 1 \pmod{p_i^{e_i}}$.

Cioè abbiamo il sistema

$$\begin{cases} x \equiv 1, 0 \pmod{p_1^{e_1}} \\ \dots \\ x \equiv 1, 0 \pmod{p_k^{e_k}} \end{cases}$$

Ognuna delle 2^k scelte dà un'unica soluzione modulo m. Infine le soluzioni sono distinte, in quanto se x_1 e x_2 sono congruenti modulo m, allora lo sono modulo $p_i^{e_i}$ per ogni i. □

Affrontati gli idempotenti passiamo ai nilpotenti:

Definizione 2.13.3. Sia $m \geq 2$ intero. Allora un elemento $\bar{x}$ di $\mathbb{Z}/m\mathbb{Z}$ si dice idempotente se esiste un intero positivo k tale che $x^k \equiv 0 \pmod{m}$.

Teorema 2.13.4. *Se $m = p_1^{e_1} \dots p_k^{e_k}$, allora gli elementi nilpotenti di $\mathbb{Z}/m\mathbb{Z}$ sono tutti e soli gli $\bar{x}$ tale che $x \equiv 0 \pmod{p_1 \dots p_k}$.*

Dimostrazione. ($\Rightarrow$) Se $\bar{x}$ è nilpotente, allora esiste un k intero positivo tale che $x^k \equiv 0 \pmod{m}$. In particolare x^k è nullo modulo p_i per ogni i. Quindi p_i divide x^k. Cioè p_i divide x per ogni i. Allora per TCR x è nullo modulo $p_1 \dots p_k$.

($\Leftarrow$) Se x è nullo modulo $p_1 \dots p_k$, sia $k = max\{e_1, \dots, e_k\}$. Allora

$$x^k \equiv (p_1 \dots p_k h)^k \equiv mr \equiv 0 \pmod{m}$$

□

2.14 Quadrati Modulo p

Iniziamo introducendo definitivamente le notazioni che useremo per quanto riguarda inversi e potenze modulo m. Innanzitutto preso un intero a, indicheremo con $1/\bar{a}$ o più semplicemente $1/a$, l'inverso di $[a]$ modulo m.

Inoltre se a, k sono interi, con k positivo, abbiamo definito $[a]^k$ come $[a^k]$. Abbiamo anche definito $[a]^{-k}$ come l'inverso di $[a]^k$.

Allora, posta a una classe modulo m e k un intero, valgono proprietà familiari:

1. $1/a \cdot 1/b = 1/ab$
2. $a^{-k} = (a^{-1})^k$ e $(1/a)^k = 1/a^k$
3. $a/b + c/d = (ad + bc)/bd$

A questo punto possiamo iniziare, col concetto di quadrati modulo m:

Definizione 2.14.1. Sia $m \geq 2$ intero. Un intero a è un quadrato modulo m se esiste un $\bar{x}$ in $\mathbb{Z}/m\mathbb{Z}$ tale che $\bar{x}^2 = \bar{a}$.

Fondamentale per la teoria dei quadrati è il simbolo di Legendre

Definizione 2.14.2 (Simbolo di Legendre)**.** Sia p primo dispari e sia a un intero. Definiamo i simbolo di Legendre come

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \text{ divide } a \\ 1 & a \text{ è un quadrato modulo } p \\ -1 & a \text{ non è un quadrato modulo } p \end{cases}$$

Il calcolo dei simboli di Legendre non è operazione semplice. In generale aiutano il criterio di Eulero

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

e la legge di reciprocità quadratica:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad p, q \text{ primi dispari}$$

che per ora non dimostreremo.

Tuttavia possiamo già affermare questa implicazione (l'altra ce l'avremo col criterio sopramenzionato)

Teorema 2.14.3. *Sia p primo dispari. Se p è congruo a 3 modulo 4 allora*

$$\left(\frac{-1}{p}\right) = -1$$

Dimostrazione. Supponiamo per assurdo che esiste un intero z tale che

$$z^2 \equiv -1 \pmod{p}$$

L'intero -1 è coprimo con p, quindi anche z. Ergo è definibile l'ordine moltiplicativo di z modulo p.

Non può essere né 1 né 2, in quanto avremmo $z^2 \equiv 1 \not\equiv -1 \pmod{p}$. Tuttavia $z^4 \equiv 1 \pmod{p}$. Quindi, grazie a quello che abbiamo notato sulle congruenze esponenziali, deve essere che $o(z)$ divide 4. Quindi $o(z) = 4$.

Tuttavia $z^{\varphi(p)} \equiv 1 \pmod{p}$. Quindi 4 divide $\varphi(p) = p - 1$ e p è congruo a 1 modulo 4. Assurdo. □

L'esistenze di quadrati è fondamentale per la risoluzione delle congruenze di secondo grado:

Teorema 2.14.4. *Sia p primo dispari e sia la congruenza di secondo grado*

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

Allora la congruenza ammette soluzione se e solo se $\Delta = b^2 - 4ac$ è un quadrato modulo p. E in tal caso le soluzioni sono

$$x_{1,2} \equiv \frac{-b \pm \sqrt{\Delta}}{2a} \pmod{p}$$

Dimostrazione. Notiamo innanzitutto che p è dispari e a è non nullo modulo p. Quindi a e 2 sono invertibili in $\mathbb{Z}/p\mathbb{Z}$. Allora

$$\begin{aligned} ax^2 + bx + c &\equiv 0 \pmod{p} \Leftrightarrow \\ \left(x + \frac{b}{2a}\right)^2 &\equiv \frac{b^2}{4a^2} - \frac{c}{a} \pmod{p} \Leftrightarrow \\ \left(x + \frac{b}{2a}\right)^2 &\equiv \frac{b^2 - 4ac}{4a^2} \pmod{p} \end{aligned}$$

Notiamo che $4a^2$ è ovviamente un quadrato. Quindi il membro destro è un quadrato modulo p se e solo se lo è $b^2 - 4ac = \Delta$. Quindi la congruenza ammette soluzione se e solo se Δ è un quadrato modulo p.

In tal caso sia $\sqrt{\Delta}$ una sua radice. Avendo ogni equazione quadratica modulo p al più due soluzioni, Δ ammette al più due radici pari a $\pm\sqrt{\Delta}$. Quindi

$$\begin{aligned} x_{1,2} + \frac{b}{2a} &\equiv \frac{\pm\sqrt{\Delta}}{2a} \pmod{p} \Leftrightarrow \\ x_{1,2} &\equiv \frac{-b \pm \sqrt{\Delta}}{2a} \pmod{p} \end{aligned}$$

□

2.15 Miscellanea

In questa ultima sezione raccolgo un insieme di fatti non rientranti in sezioni particolari, esercizi per cui non era possibile dedicare un'apposita sezione etc.

Esercizio. Consideriamo l'insieme delle cosiddette frazioni di Farey, indicizzato sui naturali positivi e definito come

$$\mathcal{F}_n = \{\, q \in \mathbb{Q} \mid 0 \leq q \leq 1, q = a/b, |b| \leq n \,\}$$

Per esempio $\mathcal{F}_5$, se ordiniamo le frazioni, è dato da

$$\mathcal{F}_5 = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}$$

le frazioni di Farey hanno interessanti proprietà. Quella che vedremo in questo esercizio è la seguente: date due frazioni consecutive e ridotte ai minimi termini $a/b < c/d$, allora $bc - ad = 1$.

Per dimostrarlo sia l'equazione diofantea $bx - ay = 1$. Vogliamo dimostrare che (c, d) è soluzione.

Innanzitutto l'equazione ammette soluzione, in quanto $(a, b) = 1$. Sia quindi (x, y) una sua soluzione. Allora

$$\frac{x}{y} = \frac{1 + ay}{yb} = \frac{a}{b} + \frac{1}{by}$$

Inoltre, a meno di traslare la soluzione, possiamo supporre che $n - b < y \leq n$.

Se per assurdo (c, d) non è (x, y), allora, essendo entrambe coppie di interi coprimi, vale

$$\frac{x}{y} > \frac{c}{d} > \frac{a}{b}$$

in quanto $a/b < c/d$.

Quindi $dx - cy > 0$, cioè è almeno 1. Da cui

$$\frac{1}{by} = \frac{x}{y} - \frac{a}{b} = \left(\frac{x}{y} - \frac{c}{d}\right) - \left(\frac{a}{b} - \frac{c}{d}\right) = \frac{dx - cy}{dy} + \frac{bc - ad}{db} \geq \frac{1}{dy} + \frac{1}{db}$$

Ergo $d \geq b + y > n$. Assurdo per come abbiamo definito $\mathcal{F}_n$.

Notiamo che abbiamo dimostrato qualcosa di più del voluto: (c, d) è l'unica soluzione (x, y) della nostra diofantea con $n - b < y \leq n$.

La prossima proposizione ci dice invece come calcolare il minimo comune multiplo dal massimo comune divisore

Proposizione 2.15.1. *Siano a, b interi non nulli. Allora il loro minimo comune multiplo è unico a meno del segno ed è*

$$[a, b] = \pm\frac{|a||b|}{(a, b)}$$

Dimostrazione. (Esistenza) Sia $M = |a||b|/(a, b)$, con $(a, b) = d$ un loro massimo comune divisore. Allora verifichiamo che M sia un minimo comune multiplo.

Posto come sempre $a = a_1 d$, $b = b_1 d$, allora $M = |a|b_1 = a_1|b|$ è un multiplo sia di a che di b.

Posto ora c multiplo sia di a che di b, allora $a_1 dx = c = b_1 dy$. Ergo $a_1 x = b_1 y$. Essendo (a_1, b_1) coprimi, a_1 divide y. Quindi $c = db_1 y = db_1 a_1 z = Mz$. Ergo M divide c.

(Unicità) Sia M un minimo comune multiplo di a e b. Voglio dimostrare che $D = ab/M$ è un massimo comune divisore. Infatti ab è un multiplo sia si a che di b. Quindi è un multiplo di M e D è un intero.

Inoltre $M = bz$ e $a = DM/b = Dz$. Quindi D divide a. Equivalentemente D divide b.

Sia ora c che divide sia a che b. Allora ab/c è un multiplo sia di a che di b. Quindi esiste un z intero tale che $Mz = ab/c$. Quindi $cz = ab/M = D$. Quindi c divide D.

Ergo ab/M è un massimo comune divisore di a e b. Essendo D unico a meno del segno, anche M lo deve essere. □

Guardiamo adesso un interessante teorema sull'elevamento a potenza:

Teorema 2.15.2. *Sia p primo, tale che $p-1$ è coprimo con $k>0$. Allora la mappa*

$$\Phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$
$$x \mapsto x^k$$

è una bigezione.

Dimostrazione. Dimostriamo l'iniettività, come sappiamo questo ci darà anche la suggettività.

Siano quindi $x_1^k \equiv x_2^k \pmod p$. Innanzitutto notiamo che se $x_{1,2}^k \equiv 0 \pmod p$, allora $x_{1,2}$ sono nilpotenti modulo p, ergo $x_{1,2} \equiv 0 \pmod p$.

Possiamo quindi supporre che x_1, x_2 siano invertibili modulo p. In tal caso, possiamo scrivere

$$\left(\frac{x_1}{x_2}\right)^k \equiv \frac{x_1^k}{x_2^k} \equiv 1 \pmod p$$

Quindi x_1/x_2 ha ordine moltiplicativo che divide k. Deve anche dividere $\varphi(p) = p-1$. Ergo deve dividere $(k, p-1) = 1$. Cioè x_1/x_2 ha ordine uno ed è l'unità in $\mathbb{Z}/p\mathbb{Z}$. Quindi $x_1 \equiv x_2 \pmod p$. □

Corollario 2.15.3. *Sia p primo congruo a 2 modulo 3. Allora la mappa*

$$\Phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$
$$x \mapsto x^3$$

è una bigezione.

Dimostrazione. Immediata conseguenza del teorema precedente. □

Esercizio. Affrontiamo ora questo problema: calcolare le ultime due cifre di $n = 13^{39^5} \neq 13^{39*5}$. Benché n non è calcolabile nella sua interezza, le congruenze permettono facilmente di risolvere il problema.

Poniamo $n = 100k + 10a_1 + a_0$ con a_1, a_0 da determinare. Innanzitutto andiamo a calcolare $\varphi(100)$, pari a

$$\varphi(100) = \varphi(2^2 * 5^2) = 2 * 4 * 5 = 40$$

Infine va osservato che $39^5 \equiv (-1)^5 \equiv -1 \pmod{40}$. Ergo

$$n = 13^{39^5} \equiv 13^{\varphi(100)h-1} \equiv 13^{-1} \pmod{100}$$

Quindi ci siamo ricondotti a invertire 13. Passando al sistema equivalente

$$\begin{cases} n \equiv 13^{-1} \pmod 4 \\ n \equiv 13^{-1} \pmod{25} \end{cases}$$

arriviamo a

$$\begin{cases} n \equiv 1 \pmod 4 \\ n \equiv 2 \pmod{25} \end{cases}$$

che ammette come unica soluzione $n \equiv 77 \pmod{100}$.

Quindi $10a_1 + a_0 = 77$, cioè $a_1 = 7$ e $a_0 = 7$.

Notiamo che in questo esercizio si è vista la potenza delle congruenze e della teoria che abbiamo costruito. Di per sé il concetto di congruenza è una riscrittura del concetto di divisibilità. Tuttavia risolvere questo esercizio senza la teoria delle congruenze, e senza il teorema cinese del resto, sarebbe stata tutta un'altra storia.

Il prossimo esercizio riguarderà una classe importante di sistemi di congruenze, quelle modulo p^k. La loro risoluzione si basa sulla risoluzione di congruenze di grado sempre più alto, da p a p^k.

Esercizio. Risolviamo la congruenza

$$x^6 + x^2 + 12 \equiv 0 \pmod{16}$$

Questa congruenza implica, non è certamente equivalente, alla congruenza modulo 2

$$x^6 + x^2 \equiv 0 \pmod 2$$

Questa ha soluzione $x \equiv 1, 0 \pmod 2$. Andiamo quindi per casi:

(1.) Se $x = 2k$, allora la congruenza è equivalente a

$$2^6k^6 + 2^2k^2 + 12 \equiv 0 \pmod{16}$$

equivalente a sua volta a

$$k^2 + 3 \equiv 0 \pmod 4$$

Andando a ridurre modulo 2, scopriamo che k è dispari. Ma a questo punto se poniamo $k = 2h + 1$, allora la congruenza

$$\begin{aligned} 4h^2 + 1 + 4h + 3 &\equiv 0 \pmod 4 \\ 0 &\equiv 0 \pmod 4 \end{aligned}$$

non dà altre condizioni su h.

Quindi supponendo x pari, tutte e sole le soluzioni sono

$$x = 2(2h+1) \equiv 2 \pmod 4$$

(2.) Se supponiamo $x = 2k+1$, allora come prima

$$(2k+1)^6 + (2k+1)^2 + 12 \equiv 0 \pmod{16}$$

Svolgendo accuratamente i calcoli si ottiene l'assurdo $14 \equiv 0 \pmod{16}$.

Un altro modo poteva essere il notare che $x^6 + x^2 + 12$ è pari.

Quindi abbiamo la congruenza equivalente

$$\frac{(2k+1)^6 + (2k+1)^2 + 12}{2} \equiv 0 \pmod 8$$

Questa implica una congruenza modulo 2, che è equivalente a quella modulo 4

$$(2k+1)^6 + (2k+1)^2 + 12 \equiv 0 \pmod 4$$

Però se osserviamo i coefficienti di Tartaglia, notiamo che possiamo sviluppare le potenze come

$$1 + 12k + 4(\dots) + 1 + 4(\dots) + 12 \equiv 0 \pmod 4$$

cioè $2 \equiv 4 \pmod 4$ Assurdo.

Il prossimo esercizio invece è un sistema di congruenze con parametro.

Esercizio. Sia la congruenza

$$\begin{cases} 3^x \equiv 7^a & \pmod{11} \\ (a+3)x \equiv 2 & \pmod 5 \end{cases}$$

Vogliamo capire per quali interi a il sistema è risolubile.

Procediamo risolvendo la prima equazione. Innanzitutto notiamo che 3 si può scrivere come $7^4 \pmod{11}$. Quindi riscriviamo il sistema come

$$\begin{cases} 7^{4x} \equiv 7^a & \pmod{11} \\ (a+3)x \equiv 2 & \pmod 5 \end{cases}$$

L'ordine moltiplicativo di 7 modulo 11 é 10, quindi ci siamo ricondotti al sistema

$$\begin{cases} 4x \equiv a & (\text{mod } 10) \\ (a+3) \equiv 2 & (\text{mod } 5) \end{cases}$$

$$\begin{cases} 0 \equiv a & (\text{mod } 2) \\ 4x \equiv a & (\text{mod } 5) \\ (a+3) \equiv 2 & (\text{mod } 5) \end{cases}$$

$$\begin{cases} 0 \equiv a & (\text{mod } 2) \\ x \equiv -a & (\text{mod } 5) \\ (a+3) \equiv 2 & (\text{mod } 5) \end{cases}$$

Abbiamo già delle condizioni su a. Infatti se a é congruo a 2 modulo 5 non ci sono soluzioni, altrimenti possiamo invertire $a+3$ e scrivere

$$\begin{cases} a \equiv 0 & (\text{mod } 2) \\ x \equiv -a & (\text{mod } 5) \\ x \equiv \frac{2}{a+3} & (\text{mod } 5) \end{cases}$$

Quindi il sistema ha soluzione se e solo se valgono le condizioni

$$\begin{cases} a+3 \not\equiv 0 & (\text{mod } 5) \\ a \equiv 0 & (\text{mod } 2) \\ -a \equiv \frac{2}{a+3} & (\text{mod } 5) \end{cases}$$

cioè

$$\begin{cases} a+3 \not\equiv 0 & (\text{mod } 5) \\ a \equiv 0 & (\text{mod } 2) \\ (a+2)(a+1) \equiv 0 & (\text{mod } 5) \end{cases}$$

che dà il sistema finale

$$\begin{cases} a \equiv 0 & (\text{mod } 2) \\ a \equiv 3, 4 & (\text{mod } 5) \end{cases}$$

Concludendo, il sistema originale ha soluzione se e solo se a é equivalente a 8 o 4 modulo 10, e in tal caso la soluzione é

$$x \equiv \frac{2}{a+3} \pmod 5$$

Capitolo 3

Gruppi

3.1 Prime Definizioni

Le classi di resto $\mathbb{Z}/n\mathbb{Z}$, i teoremi di Eulero e di Fermat, nascondono una struttura molto importante, centrale nella matematica moderna: quella di gruppo. Procediamo dandone subito la definizione:

Definizione 3.1.1. Sia G un insieme e $\cdot$ una operazione su di esso

$$G \times G \to G$$
$$(x, y) \mapsto x \cdot y$$

La coppia $(G, \cdot)$ viene detta gruppo se $\cdot$ soddisfa le seguenti proprietà:

1. è associativa, cioè per ogni x, y, z in G allora $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
2. ammette l'elemento neutro. Cioè esiste un elemento e tale che $x \cdot e = e \cdot x = x$ per ogni $x \in G$;
3. ogni elemento $x \in G$ ammette inverso, cioè ammette un elemento $y \in G$ tale che $x \cdot y = y \cdot x = 1$.

Inoltre se l'operazione è commutativa, cioè $x \cdot y = y \cdot x$ per ogni $x, y \in G$, allora il gruppo viene detto abeliano.

Nel caso l'operazione si indichi con $\cdot$, cioè si usi la notazione moltiplicativa, allora porremo x^{-1} come l'inverso di x e 1 l'elemento neutro. Viceversa nel caso usassimo la notazione additiva indicando l'operazione con $+$, allora $-x$ sarà l'inverso e 0 l'elemento neutro.

Inoltre porremo spesso $xy = x \cdot y$, per alleggerire al notazione, quando non c'è pericolo di confondersi.

Inoltre indicheremo spesso, per non dire sempre, il gruppo $(G, \cdot)$ semplicemente con G quando l'operazione è chiara dal contesto o non ci sono possibilità di confondersi.

In verità sarebbe più corretto parlare di *un* elemento neutro e inverso, in quanto per ora non abbiamo ancora dimostrato la loro unicità. Lo dimostreremo adesso, in contemporanea ad alcuni fatti:

Proposizione 3.1.2. *Sia $(G, \cdot)$ un gruppo. Allora*

1. *L'elemento neutro è unico.*
2. *Ogni elemento ammette un unico inverso indicato con g^{-1}.*
3. *Se h è un inverso sinistro o destro di g, allora è il suo inverso.*
4. *Per ogni g in G, l'inverso di g^{-1} è g stesso.*
5. *Per ogni g, h in G, l'inverso di gh è $h^{-1}g^{-1}$.*
6. *Valgono le leggi di cancellazione:*

$$ax = bx \Rightarrow a = b$$
$$xa = xb \Rightarrow a = b$$

Dimostrazione. (1.) Siano e, e' due elementi neutri. Allora per definizione di elemento neutro,

$$e = ee' = e'$$

(2.) Siano g_1 e g_2 due elementi inversi di g. Allora

$$g_1 = g_1 e = g_1(gg_2) = (g_1 g)g_2 = eg_2 = g_2$$

(3.) Supponiamo, per esempio, che h sia un inverso sinistro di g. Allora è anche un suo inverso destro, quindi è il suo inverso. Infatti

$$hg = e \Rightarrow e = h^{-1}eh = h^{-1}hgh = gh$$

(4.) Sappiamo che $gg^{-1} = g^{-1}g = e$, quindi g è l'inverso di g^{-1}.

(5.) Per il punto 3 basta verificare che $h^{-1}g^{-1}$ sia l'inverso sinistro di gh:

$$h^{-1}g^{-1}gh = h^{-1}eh = h^{-1}h = e$$

(6.) Verifichiamo la prima uguaglianza, l'altra è uguale.

$$ax = bx \Rightarrow axx^{-1} = bxx^{-1} \Rightarrow a = b$$

□

Facciamo ora qualche esempio:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono gruppi abeliani con la somma.

2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ non sono invece gruppi col prodotto, in quanto 0 non ha inverso.

3. $(\mathbb{N}, +)$ non è un gruppo, in quanto ogni elemento non nullo non ammette inverso.

4. Abbiamo già visto che $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo abeliano.

5. Posto C_n l'insieme delle radici complesse n-esime dell'unità, allora $(C_n, \cdot)$ è un gruppo abeliano.

6. Invece l'insieme delle radici radici complesse n-esime di 2 non è un gruppo. Infatti il prodotto di $\sqrt{2}$ e $-\sqrt{2}$ non è una radice di 2.

7. Preso un campo $\mathbb{K}$ e indicando con $\mathbb{K}^*$ tutto il campo tolto dello 0, allora sia $(\mathbb{K}, +)$ che $(\mathbb{K}^*, \cdot)$ sono gruppi abeliani.

8. Sia $(\mathbb{Z}^*, \cdot) = (\pm 1, \cdot)$ che $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ sono gruppi abeliani. In generale preso un qualunque anello (commutativo) con identità A, allora $(A^*, \cdot)$ è un gruppo (abeliano).

In generale non tutti i gruppi sono abeliani. La prossima proposizione ne costruisce i primi esempi:

Proposizione 3.1.3. *Sia un insieme X. Allora $(S(X), \circ)$ è un gruppo.*

Dimostrazione. Innanzitutto la composizione di funzioni bigettive è una funzione bigettiva. Quindi l'operazione $\circ\colon S(X) \times S(X) \to S(X)$ è ben definita.

La composizione di funzioni è associativa.

La funzione id_X è l'elemento neutro.

Ogni funzione f in $S(X)$ ammette elemento inverso f^{-1}, che è ancora una bigezione. □

Di grande importanza sono i gruppi simmetrici. Li affronteremo esaustivamente in seguito, mentre per ora ci limiteremo a darne la definizione e a provare la loro non abelianità.

Definizione 3.1.4. Sia n naturale positivo. Definiamo l'ennesimo gruppo simmetrico, indicato con S_n, come l'insieme delle permutazioni di $\mathbb{N}_n$.

Proposizione 3.1.5. *Il gruppo simmetrico S_n non è abeliano se e solo se $n \geq 3$.*

Dimostrazione. ($\Leftarrow$) Siano le seguenti permutazioni

$$\begin{aligned}
\sigma\colon 1 &\mapsto 2 \\
2 &\mapsto 3 \\
3 &\mapsto 1 \\
i &\mapsto i \quad \forall i > 3 \\
\tau\colon 1 &\mapsto 2 \\
2 &\mapsto 1 \\
3 &\mapsto 3 \\
i &\mapsto i \quad \forall i > 3
\end{aligned}$$

Allora esse non commutano. Infatti $(\sigma \circ \tau)(1) = 3$, mentre $(\tau \circ \sigma)(1) = 1$. Quindi $\sigma \circ \tau$ e $\tau \circ \sigma$ sono differenti.

($\Rightarrow$) Se $\mathbb{N} = \{1\}$, allora S_n è costituito dalla sola identità, che ovviamente commuta con se stessa.

Se $\mathbb{N}_n = \{1, 2\}$, allora S_n è costituito solo da id e la permutazione τ che scambia 1 e 2. Sicuramente esse commutano con loro stesse. D'altra parte commutano banalmente tra di loro □

Come gli spazi vettoriali ammettono sottospazi, così i gruppi ammettono i sottogruppi:

Definizione 3.1.6. Sia $(G, \cdot)$ un gruppo. Un suo sottogruppo è un gruppo $(H, \cdot|_{H\times H})$, formato da un sottoinsieme H di G e dalla restrizione di $\cdot$ a H.

Indicheremo con $H \leq G$ il fatto che H è un sottogruppo di G. Inoltre vale una caratterizzazione operativa dei sottogruppi:

Proposizione 3.1.7. *Sia $(G, \cdot)$ un gruppo e H un sottoinsieme non vuoto di G. Allora $(H, \cdot|_{H\times H})$ è un suo sottogruppo se e solo se*

1. *Per ogni h in H, il suo inverso rispetto a $\cdot$ appartiene a H.*

2. *Per ogni g, h in H, il loro prodotto appartiene ad H.*

Dimostrazione. La seconda richiesta è equivalente a richiedere che la restrizione di $\cdot$ ad H sia un'operazione su H.

L'associatività è garantita dall'associatività di $\cdot$.

Per quanto riguarda l'esistenza dell'elemento neutro, prendiamo un h in H. Allora il suo inverso in G appartiene a H. Quindi anche $e = hh^{-1}$ appartiene ad H. Essendo elemento neutro per $\cdot$, sicuramente lo è per $\cdot|_{H\times H}$.

Infine ogni elemento di H ammette un inverso in G, che appartiene ad H ed è banalmente un inverso per $\cdot|_{H\times H}$. □

Per applicare questa proposizione è essenziale dire che H non è vuoto. Normalmente lo si verifica facendo direttamente vedere che l'elemento neutro vi appartiene.

Un importante sottogruppo è il cosiddetto centro del gruppo:

Definizione 3.1.8. Sia G un gruppo. Il suo centro, indicato con $Z(G)$, è l'insieme

$$\{\, x \in X \mid \forall a \in G \; ax = xa \,\}$$

Proposizione 3.1.9. *Sia G un gruppo. Allora il suo centro è un sottogruppo di G. Inoltre G è abeliano se e solo se coincide col suo centro.*

Dimostrazione. Certamente l'identità commuta con tutti gli elementi di G.

Inoltre se h appartiene al centro, allora anche il suo inverso vi appartiene. Infatti per ogni a in G, il suo inverso commuta con h. Ergo

$$h^{-1}a = (a^{-1}h)^{-1} = (ha^{-1})^{-1} = ah^{-1}$$

Infine se g e h appartengono a $Z(G)$, allora verifichiamo che anche il loro prodotto vi appartiene. Infatti per ogni a in G

$$a(gh) = agh = gah = gha = (gh)a$$

Infine è banale verificare che $Z(G) = G$ se e solo se G è abeliano. □

La prossima proposizione trova alcuni sottogruppi di $\mathbb{Z}$. (Vedremo poi che sono tutti)

Proposizione 3.1.10. *Preso k intero, allora l'insieme*

$$k\mathbb{Z} = \{\, kz \mid z \in \mathbb{Z} \,\}$$

è un sottogruppo di $\mathbb{Z}$. Inoltre $m\mathbb{Z}$ è contenuto in $n\mathbb{Z}$ se e solo se n divide m, e sono uguali se e solo se $m = \pm n$.

Dimostrazione. L'identità vi appartiene, in quanto $0 = k0$.

Se kz è un elemento di $k\mathbb{Z}$, allora il suo inverso $-kz = k(-z)$ è ancora un elemento di $k\mathbb{Z}$.

Se kz_1 e kz_2 sono elementi di $k\mathbb{Z}$, allora la loro somma è $k(z_1 + z_2)$, che è ancora un elemento di $k\mathbb{Z}$.

Verifichiamo ora la proprietà dell'inclusione.

Se n divide m, allora $m = kn$. Quindi ogni elemento mz in $m\mathbb{Z}$ si scrive come nkz, e appartiene anche a $n\mathbb{Z}$.

Viceversa se $m\mathbb{Z}$ è contenuto in $n\mathbb{Z}$, allora m in particolare si scrive come $m = nz$, quindi è diviso da n.

Infine $m\mathbb{Z}$ e $n\mathbb{Z}$ sono uguali se e solo se m e n si dividono a vicenda. Ma questo succede se e solo se $m = \pm n$. □

Infine come con i spazi vettoriali, si può vedere cosa succede quando si intersecano e si uniscono sottogruppi. Il risultato non sorprenderà:

Proposizione 3.1.11. *Sia G un gruppo e H,K due suoi sottogruppi. Allora*

1. *La loro intersezione è un sottogruppo.*

2. *La loro unione è un sottogruppo se e solo H è contenuto in K o viceversa.*

Dimostrazione. (1.) L'intersezione contiene l'identità, in quanto essa appartiene sia ad H che a K.

Se h è un elemento di $H \cap K$, allora è un elemento sia di H che di K. Quindi il suo inverso appartiene sia ad H che a K, cioè appartiene alla loro intersezione.

Se g, h sono elementi di $H \cap K$, allora hg è un elemento di H e di K, quindi dell'intersezione.

(2.) Supponiamo che esista $x \in H \setminus K$ e $y \in K \setminus H$. Allora x e y sono elementi di $H \cup K$. Se per assurdo fosse un sottogruppo, allora $z = xy$ è anche esso un elemento dell'unione.

Tuttavia se z appartenesse a H, allora $y = x^{-1}z$ dovrebbe appartenere a H. Se invece z appartenesse a K, allora $x = zy^{-1}$ dovrebbe appartenere a K. In entrambi i casi otteniamo l'assurdo. □

Dopo aver definito cosa è un gruppo, dopo aver parlato di sottogruppi, l'ultimo argomento preparatorio è quello di *ordine*. Iniziamo con la definizione di operazione ripetuta:

Definizione 3.1.12. Sia G un gruppo e x un suo elemento. Preso $k \in \mathbb{Z}$ definiamo x^k come

$$x^k = \begin{cases} e & x = 0 \\ x^{k-1} \cdot x & x > 0 \\ (x^{-k})^{-1} & k < 0 \end{cases}$$

Proposizione 3.1.13. *Presi k, h interi, allora*

$$x^{k+h} = x^k \cdot x^h$$
$$(x^k)^h = x^{kh}$$

Inoltre se G è abeliano, allora

$$(x \cdot y)^k = x^k \cdot y^k$$

Dimostrazione. Semplici conti. □

Possiamo ora introdurre il concetto di sottogruppo generato:

Definizione 3.1.14. Sia G un gruppo e x un suo elemento. Definiamo il sottogruppo generato da x, indicato con $\langle x \rangle$, come l'insieme delle sue potenze:

$$\langle x \rangle = \left\{ x^k \;\middle|\; k \in \mathbb{Z} \right\}$$

Proposizione 3.1.15. *Il sottogruppo generato è effettivamente un sottogruppo. Inoltre è abeliano.*

Dimostrazione. L'identità coincide con x^0, quindi appartiene a $\langle x \rangle$.

Se $g = x^k$ e $h = x^{k'}$ appartengono a $\langle x \rangle$, allora il loro prodotto, pari a $x^{k+k'}$, appartiene a $\langle x \rangle$.

Infine se $g = x^k$ appartiene a $\langle x \rangle$, allora il suo inverso, pari a x^{-k}, appartiene a $\langle x \rangle$.

Infine verifichiamo che $\langle x \rangle$ sia abeliano. Presi $g = x^k$ e $h = x^{k'}$ in $\langle x \rangle$, allora

$$gh = g^{k+k'} = g^{k'+k} = hg$$

□

Legato al sottogruppo generato c'è il concetto di ordine di un elemento:

Definizione 3.1.16. Sia G un gruppo e x un suo elemento. Definisco l'ordine di x come

$$\operatorname{ord}(x) = \min \left\{ k \in \mathbb{N}_+ \;\middle|\; x^k = e \right\}$$

dove abbiamo posto $\operatorname{ord}(x) = +\infty$ se il minimo non esiste.

Teorema 3.1.17. *Sia G un gruppo e x un suo elemento di ordine finito d. Allora $\langle x \rangle$ coincide con*

$$\{x^0, \dots, x^{d-1}\}$$

e ha cardinalità d. Infine $x^h = e$ se e solo se d divide h.

Dimostrazione. Sia h intero e effettuiamo la divisione euclidea $h = qd + r$ con $0 \leq r \leq d - 1$. Allora

$$x^h = x^{qd+r} = (x^d)^q \cdot x^r = e^q \cdot x^r = x^r$$

Abbiamo quindi verificato che ogni x^h in $\langle x \rangle$ si può scrivere come potenza di x compresa tra 0 e $d - 1$.

D'altra parte supponiamo che $x^h = x^k$ con $h \geq k$ e compresi tra 0 e $d - 1$. Allora

$$x^{h-k} = x^h \cdot (x^k)^{-1} = e$$

Essendo che $d > h - k \geq 0$, allora per minimalità di d la differenza $h - k$ deve essere nulla, cioè $h = k$.

Infine se $x^h = e$, allora eseguendo la divisione con resto $h = qd + r$, scopriamo che anche $x^r = 0$. Quindi $r = 0$ per minimalità di d. Quindi d divide h. □

Teorema 3.1.18. *Sia G un gruppo e x un suo elemento di ordine infinito. Allora il sottogruppo generato ha cardinalità infinita. In partcolare ogni potenza di x produce un elemento differente di G.*

Dimostrazione. Supponiamo per assurdo che esistono due interi $k > h$ tale che $x^k = x^h$. Allora la differenza tra k e h è positiva, e $x^{k-h} = e$. Questo implica che x ha ordine finito. Assurdo. □

Abbiamo dimostrato che $\text{ord}(x) = |\langle x \rangle| \leq |G|$. Quindi se il gruppo è finito, allora lo è l'ordine di ogni suo elemento. Il viceversa, vedremo successivamente, è falso.

Infine, per analogia con gli elementi, si indica con ordine di un gruppo la sua cardinalità.

Chiudiamo questa sezione preliminare con il seguente risultato sui sottogruppi:

Proposizione 3.1.19. *Sia G un gruppo finito. Se un suo sottoinsieme è chiuso per prodotti ed contiene l'elemento neutro, allora è un sottogruppo.*

Dimostrazione. Dobbiamo verificare che H sia chiuso per inversi.

Sia quindi h in H. Allora essendo G finito, h deve avere ordine finito. In particolare $h^k = e$ per qualche k positivo. Allora sia che $k - 1$ sia nullo, o che sia un numero positivo, sappiamo che h^{k-1} appartiene a H. Infatti esso è chiuso per prodotto e contiene l'elemento neutro.

Quindi $h^{k-1}h = e$ e h^{k-1} è l'inverso di h, che appartiene a H. □

Procediamo quindi col prossimo argomento: i gruppi ciclici.

3.2 Gruppi Ciclici

La teoria dei gruppi è un classico esempio di teoria che si basa sui definizioni semplici, come è quella di gruppo, ma che riesce facilmente a generare oggetti giganteschi (come il noto "Gruppo Mostro"). Lo studio di un gruppo è in generale cosa difficile. È quindi opportuno iniziare con gruppi facili: i cosiddetti gruppi ciclici.

Definizione 3.2.1 (Gruppo Ciclico)**.** Un gruppo G viene detto ciclico se coincide con il sottogruppo generato da un suo elemento.

Proposizione 3.2.2. *Se G è ciclico, allora è abeliano.*

Dimostrazione. Sappiamo che il sottogruppo generato da un elemento è abeliano. Quindi se G coincide con un tale sottogruppo, allora è abeliano. □

I gruppi ciclici possono essere finiti, come $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$, o infiniti, come $\mathbb{Z} = \langle 1 \rangle$. Come vedremo più avanti questi sono di fatto gli unici esempi.

Per ora enunciamo un importante risultato sui sottogruppi di gruppi ciclici:

Teorema 3.2.3. *Sia G un gruppo ciclico. Allora ogni suo sottogruppo è ciclico.*

Dimostrazione. Supponiamo che G sia generato da g e sia H un suo sottogruppo.

Se H è *banale*, cioè consiste del solo elemento neutro, allora è banalmente generato da esso.

Altrimenti esiste un certo $h = g^k$ che appartiene a H, con k non nullo.

Inoltre anche l'inverso di h, pari a g^{-k}, appartiene a G. Possiamo conseguentemente supporre che k sia positivo.

Sia quindi l'insieme

$$S = \left\{ h > 0 \;\middle|\; g^h \in H \right\}$$

e sia h_0 il suo minimo. Dico che g^{h_0} genera H.

Essendo H chiuso per inversi e prodotti, ogni potenza, anche negativa, di g^{h_0} appartiene ad H. Quindi $\left\langle g^{h_0} \right\rangle$ è incluso in H.

D'altra parte sia g^h in H e eseguiamo la divisione euclidea $h = qh_0 + r$. Allora

$$g^r = (g^{h_0})^{-q} g^h$$

appartiene ad H, in quanto sia g^{h_0} che g^h vi appartengono.

Quindi, per minimalità di h_0, r deve essere nullo. Ergo $h = qh_0$ e $g^h = (g^{h_0})^q$ appartiene ad $\left\langle g^{h_0} \right\rangle$. □

Corollario 3.2.4. *I sottogruppi di $\mathbb{Z}$ sono tutti e soli della forma $H_n = n\mathbb{Z}$ con n naturale. Inoltre gli H_n sono distinti.*

Dimostrazione. Sappiamo che gli H_n sono sottogruppi. Inoltre avendo limitato n fra i naturali, essi sono anche distinti.

D'altra parte preso H sottogruppo di $(\mathbb{Z}, +)$, esso è ciclico, generato da n intero. Essendo la moltiplicazione esattamente la somma ripetuta, possiamo scrivere

$$H = \langle n \rangle = \{ kn \mid k \in \mathbb{Z} \} = n\mathbb{Z} = |n|\mathbb{Z} = H_{|n|}$$

□

A questo punto passiamo a discutere del gruppo ciclico per antonomasia: il gruppo $(\mathbb{Z}/n\mathbb{Z}, +)$. Innanzitutto l'ordine dei suoi elementi è dato da una formula esplicita, dimostrata dalla prossima proposizione.

Proposizione 3.2.5. *Sia $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$. Allora*

$$\text{ord}(\bar{a}) = \frac{n}{(a, n)}$$

Dimostrazione. Per definizione l'ordine di $\bar{a}$ è il più piccolo intero positivo k tale che $k\bar{a} = \bar{0}$ (l'operazione è la somma, e la somma ripetuta è l'usuale moltiplicazione). Stiamo quindi risolvendo la congruenza

$$ka \equiv 0 \pmod{n}$$

Essa ammette soluzione

$$k \equiv 0 \pmod{n/(a, n)}$$

Cioè

$$k = \frac{n}{(a, n)} t \quad t \in \mathbb{Z}$$

L'ordine di $\bar{a}$ è quindi il più piccolo k positivo tra quelli trovati. Cioè è

$$\text{ord}(\bar{a}) = \frac{n}{(a, n)}$$

□

Questa proposizione ha già delle importanti conseguenze, alcune che nascondono teoremi più generali, altre invece peculiari dei gruppi ciclici (sorpresa quali sono).

Proposizione 3.2.6. *Sia il gruppo $\mathbb{Z}/n\mathbb{Z}$. Allora valgono le seguenti proprietà.*

1. *Per ogni $\bar{a}$, il suo ordine divide n.*

2. *Il gruppo ammette $\varphi(n)$ generatori.*

3. *Per ogni d che divide n, ci sono esattamente $\varphi(d)$ elementi di ordine d.*

Dimostrazione. (1.) Ovvio dalla proposizione precedente.

(2.) I generatori sono tutti e soli gli elementi $\bar{a}$ di ordine n. Dalla formula precedente otteniamo che sono tutti e soli quelli tali che a è coprimo con n. Questi sono esattamente $\varphi(n)$.

(3.) Sia $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$. Il suo ordine è d se e solo se vale l'uguaglianza

$$(n, a) = \frac{n}{d}$$

Poniamo ora $a = nb/d$. Allora sostituendo nell'uguaglianza precedente otteniamo

$$\frac{n}{d} = \left(n, \frac{n}{d}b\right) = \left(\frac{n}{d}d, \frac{n}{d}b\right) = \frac{n}{d}(b, d)$$

Quindi gli a cercati sono tutti e soli quelli della forma nb/d con $1 \leq b < d$ e coprimo con d. Quindi sono esattamente $\varphi(d)$. □

Corollario 3.2.7. *Sia n naturale positivo. Allora*

$$n = \sum_{d|n} \varphi(d)$$

Dimostrazione. Per ogni d divisore di n, sia X_d l'insieme degli elementi di $G = \mathbb{Z}/n\mathbb{Z}$ di ordine d. Dalla proposizione precedente è immediato che $\{X_d\}_{d|n}$ é una partizione di G. Ergo

$$n = |G| = \sum_{d|n} |X_d| = \sum_{d|n} \varphi(d)$$

□

Notiamo che il risultato appena ottenuto non è per nulla scontato. È sicuramente possibile dimostrarlo per vie traverse, tramite la scomposizione in primi. Tuttavia la teoria dei gruppi ci ha permesso di ottenere questo risultato come mero corollario.

Chiudiamo questa sezione con il prossimo teorema, che ci dice come sono fatti i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.

Teorema 3.2.8. *Sia il gruppo $G = \mathbb{Z}/n\mathbb{Z}$. Allora valgono le seguenti affermazioni:*

1. *per ogni sottogruppo H di G, il suo ordine divide quello di G;*
2. *viceversa per ogni divisore d di n esiste un unico sottogruppo di ordine d.*

Dimostrazione. (1.) Essendo G ciclico anche H lo è. Quindi $H = \langle h \rangle$ e l'ordine di H è l'ordine di h, che divide l'ordine di G per quanto visto.

(2.) Sia $x = [n/d]$. Esso ha ordine d. Infatti n/d divide n, quindi

$$(n, n/d) = n/d \;\Rightarrow\; \mathrm{ord}(x) = \frac{n}{(n, n/d)} = d$$

Ergo poniamo $H_d = \langle x \rangle$. Esso è un sottogruppo di ordine cercato.

Verifichiamo che sia l'unico.

Sia quindi H un sottogruppo di ordine d. Esso è ciclico e poniamo $\langle \bar{y} \rangle$ un suo generatore.

Avendo $\bar{y}$ ordine d sappiamo, per quello detto prima, che si scrive come $[nb/d]$ con $1 \leq b < d$ coprimo con d. Ma allora $\bar{y}$ appartiene al generato da x, e quindi tutto H è incluso in H_d. Avendo la stessa cardinalità sono uguali. □

Vorremmo adesso parlare dire che tutti i gruppi ciclici sono "sostanzialmente" $\mathbb{Z}$ o $\mathbb{Z}/n\mathbb{Z}$. Per farlo però dobbiamo riuscire a mandare gruppi in gruppi, rispettandone le operazioni. Dobbiamo cioè introdurre il concetto di omomorfismo di gruppi.

3.3 Omomorfismi di Gruppi

Iniziamo subito con la definizione

Definizione 3.3.1. Siano $(G, \cdot)$ e $(G', *)$ due gruppi. Una funzione $f \colon G \to G'$ è un omomorfismo di gruppi se per ogni $g, h \in G$

$$f(g \cdot h) = f(g) * f(h)$$

Enunciamo qualche importante proprietà

Proposizione 3.3.2. *Siano G, G' due gruppi e f un omomorfismo da G a G'. Allora valgono le seguenti proprietà.*

1. *L'identità di G viene mandata nell'identità di G'.*
2. *Per ogni x in G, l'inverso di x viene mandato nell'inverso di $f(x)$.*
3. *Se H è un sottogruppo di G, allora $f(H)$ è un sottogruppo di G'.*
4. *Viceversa se K è un sottogruppo di G', allora $f^{-1}(K)$ è un sottogruppo di G.*
5. *L'immagine di f e nucleo di f, definito come $\mathrm{Ker}(f) = f^{-1}(e')$, sono sottogruppi di G' e di G rispettivamente.*
6. *La funzione è iniettiva se e solo se ha nucleo banale.*
7. *Se G è abeliano, anche $f(G)$ lo è.*
8. *Se G è ciclico, anche $f(G)$ lo è.*

Dimostrazione. D'ora in poi, per alleggerire la notazione, sottintenderemo le operazioni di G e di G' se non c'è pericolo di ambiguità.

(1.) Per semplice verifica diretta

$$f(e) = f(ee) = f(e)f(e) \;\Rightarrow\; e' = f(e)$$

(2.) Sia x' l'inverso di x in G. Essendo G' un gruppo, basta vedere che $f(x')$ sia un inverso sinistro di $f(x)$. Sempre per verifica diretta:

$$f(x')f(x) = f(x'x) = f(e) = e'$$

(3.) L'identità di G, essendo immagine di quella di G, appartiene a $f(H)$.

Presi $f(h_1)$, $f(h_2)$ in $f(H)$, allora il loro prodotto è $f(h_1h_2)$ che appartiene a $f(H)$.

Preso $f(h)$ in $f(H)$, il suo inverso è $f(h^{-1})$ che appartiene ad $f(H)$.

(4.) L'identità di G', appartenendo alla preimmagine di quella di G', appartiene a $f^{-1}(K)$.

Presi g_1, g_2 in $f^{-1}(K)$, allora $f(g_1)$ e $f(g_2)$ appartengono a K. Quindi anche il prodotto di quest'ultimi, uguale a $f(g_1g_2)$, appartiene a K. Quindi g_1g_2 appartiene a $f^{-1}(K)$.

Preso g in $f^{-1}(K)$, allora $f(g)$ appartiene a K. Quindi l'inverso di quest'ultimo, uguale a $f(g^{-1})$, appartiene ad K. Quindi g^{-1} appartiene a $f^{-1}(K)$.

(5.) Essendo G sottogruppo di se stesso $f(G)$ è un sottogruppo di G'. D'altra parte essendo $\{e'\}$ sottogruppo di G', allora $\mathrm{Ker}(f)$ è un sottogruppo di G.

(6.) Certamente se è iniettiva, posto $f(g) = e' = f(e)$, allora $g = e$.

D'altra parte sia $f(x) = f(y)$. Allora $e' = f(x)f(y)^{-1} = f(xy^{-1})$. Avendo f nucleo banale, xy^{-1} è l'identità e $x = y$.

(7.) Siano $g = f(x)$ e $h = f(y)$ nell'immagine di G. Allora

$$gh = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = hg$$

(8.) Supponiamo che G sia generato da g. Allora per ogni y nell'immagine di G, y si scrive come $f(x)$. Inoltre x è della forma g^k. Quindi

$$f(g)^k = \underbrace{f(g) * \cdots * f(g)}_{k \text{ volte}} = f(\underbrace{g \cdot \cdots \cdot g}_{k \text{ volte}}) = f(g^k) = y$$

Quindi $f(G)$ è generato da $f(g)$ ed è ciclico. □

Come si comporta invece un omomorfismo con gli ordini? La prossima proposizione ne discute.

Proposizione 3.3.3. *Siano G, G' due gruppi e f un omomorfismo da G a G'. Allora valgono le seguenti affermazioni.*

1. *Per ogni $x \in G$, l'ordine di $f(x)$ divide quello di x.*

2. *La funzione è iniettiva se e solo se preserva tutti gli ordini.*

dove abbiamo posto, per convenzione, che $+\infty$ è diviso da se stesso e da tutti i naturali positivi.

Dimostrazione. (1.) Sia n l'ordine di x.

Se esso è finito possiamo scrivere

$$f(x)^n = f(x^n) = f(e) = e'$$

Quindi l'ordine di $f(x)$ divide n.

Se invece $n = +\infty$, allora per convenzione l'ordine di $f(x)$ lo divide.

(2., $\Leftarrow$) Sia $x \in \mathrm{Ker}(f)$. Allora l'ordine di $f(x) = e'$, che è 1, coincide con l'ordine di x. Ergo x ha ordine 1, cioè è l'identità.

Quindi f ha nucleo banale ed è iniettiva.

(2. $\Rightarrow$) Sia $x \in G$.

Se l'ordine di $f(x)$ è $+\infty$, allora anche l'ordine di x è $+\infty$, valendo la contronominale del punto precedente.

D'altra parte se $f(x)$ ha ordine finito n, allora dobbiamo solo dimostrare che l'ordine di x divide quello di $f(x)$. Questo si verifica tramite il seguente conto

$$f(x^n) = f(x)^n = e' \;\Rightarrow\; x^n = e$$

Quindi l'ordine di x divide n. □

Notiamo che l'ultima proposizione è necessaria, in quanto non tutti gli omomorfismi sono iniettivi. Infatti la seguente mappa

$$f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$x \mapsto \bar{x}$$

è, per come abbiamo definito le operazioni su $\mathbb{Z}/n\mathbb{Z}$, un omomorfismo. Tuttavia non è iniettivo.

Quindi è necessario introdurre un concetto più forte, quello di isomorfismo:

Definizione 3.3.4. Siano G e G' due gruppi. Un isomorfismo da G a G' è una omomorfismo $f\colon G \to G'$ bigettivo, tale che la sua inversa sia un omomorfismo.

Mentre l'inversa di una funzione continua non è detto che sia continua, questo è invece il caso per gli omomorfismi di gruppi.

Proposizione 3.3.5. *Un omomorfismo bigettivo $f\colon G \to G'$ è un isomorfismo.*

Dimostrazione. Siano x, y in G'. Allora

$$f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) = xy$$

Quindi

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$$

e f^{-1} è un omomorfismo. Quindi f è un isomorfismo. □

Due gruppi isomorfi sono "sostanzialmente la stessa cosa". Gli isomorfismi preservano ordini, cardinalità, normalità (vedremo successivamente cosa è). In soldoni gruppi isomorfi differiscono solamente nel avere i loro elementi chiamati

in modo differente. Per esempio un isomorfismo $f\colon G \to G'$ dà luogo a una bigezione fra i sottogruppi:

$$\begin{aligned} \varphi\colon \{H \leq G\} &\to \{K \leq G'\} \\ H &\mapsto f(K) \end{aligned} \tag{3.1}$$

Col nuovo strumento degli isomorfismi possiamo dimostrare che per ogni ordine esiste sostanzialmente un unico gruppo ciclico di quell'ordine:

Teorema 3.3.6. *Sia G un gruppo ciclico. Se ha cardinalità finita n, esso è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Altrimenti è isomorfo a $\mathbb{Z}$.*

Dimostrazione. Se $G = \langle g \rangle$ ha ordine infinito, la mappa

$$\begin{aligned} \Phi\colon \mathbb{Z} &\to G \\ n &\mapsto g^n \end{aligned}$$

è un omomorfismo, in quanto

$$\Phi(k+h) = g^{k+h} = g^k g^h = \Phi(k)\Phi(h)$$

Inoltre è suggettiva, in quanto G è generato da g, e iniettiva. Infatti se $g^k = e$, allora $k = 0$, avendo g ordine infinito. Quindi il nucleo di Φ è banale ed essa è iniettiva.

Quindi Φ è un omomorfismo bigettivo, ergo è un isomorfismo.

D'altra parte se $G = \langle g \rangle$ ha ordine finito n, sia la mappa

$$\begin{aligned} \Psi\colon \mathbb{Z}/n\mathbb{Z} &\to G \\ \bar{x} &\mapsto g^x \end{aligned}$$

Essa è ben definita. Infatti se $\bar{x} = \bar{y}$, allora $x = kn + y$. Da cui

$$g^x = g^{kn+y} = (g^n)^k g^y = g^y$$

Come prima Ψ è suggettiva. Infatti se g^k appartiene a G', allora $\Psi(\bar{k}) = g^k$.

Inoltre è iniettiva. Infatti se $\Psi(\bar{x}) = g^x = e$, allora x deve essere un multiplo di n. Cioè $\bar{x} = \bar{0}$.

Quindi Ψ è un omomorfismo bigettivo, cioè è un isomorfismo. □

Corollario 3.3.7. *Sia G ciclico. Allora ha cardinalità finita o numerabile.*

Dimostrazione. Immediata conseguenza del risultato precedente. □

Grazie a questo risultato possiamo riprendere i risultati che avevamo ottenuto per i gruppi $\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$.

Teorema 3.3.8. *Sia $G = \langle g \rangle$ un gruppo ciclico infinito.*

1. *Tutti i suoi elementi, esclusa l'identità, hanno ordine infinito.*
2. *Esso ammette esattamente 2 generatori (uno inverso dell'altro).*
3. *I suoi sottogruppi sono tutti e soli i sottoinsiemi della forma*

$$H = \langle g^n \rangle \quad n \in \mathbb{Z}$$

Inoltre ponendo $n \in \mathbb{N}_+$ vengono contanti tutti e una sola volta.

Dimostrazione. Gli isomorfismi mantengono gli ordini. Essendo che in $\mathbb{Z}$ tutti gli elementi escluso lo 0 hanno ordine infinito, così deve essere anche in G.

Gli unici generatori di $\mathbb{Z}$ sono ± 1, quindi G ammette come unici generatori $g^{\pm 1}$

Infine tutti i sottogruppi di $\mathbb{Z}$ hanno la forma $n\mathbb{Z}$ con $n \in \mathbb{N}_+$, e così vengono contati una sola volta. Quindi, grazie alla mappa (3.1), sappiamo che i sottogruppi di G, contati una sola volta, hanno la forma:

$$H_n = f(n\mathbb{Z}) = f(\langle n \rangle) = \langle f(n) \rangle = \langle g^n \rangle$$

con f isomorfismo da $\mathbb{Z}$ a G. □

Teorema 3.3.9. *Sia $G = \langle g \rangle$ un gruppo ciclico finito di ordine n.*

1. *Per ogni elemento g di G, l'ordine di g divide n.*
2. *Per ogni divisore d di n, esistono $\varphi(d)$ elementi di ordine d.*
3. *Il gruppo ammette $\varphi(n)$ generatori.*
4. *Ogni sottogruppo di G ha ordine che divide n.*
5. *Per ogni divisore di n esiste un unico sottogruppo di ordine d.*

Dimostrazione. Sono risultati immediati grazie al fatto che un isomorfismo $f\colon G \to \mathbb{Z}/n\mathbb{Z}$, e il suo inverso, preservano i sottogruppi e l'ordine degli ielementi.

Inoltre se consideriamo un elemento g^k di G, grazie all'isomorfismo f esso avrà ordine

$$\text{ord}(x) = \frac{n}{(k,n)}$$

E per quanto riguarda i sottogruppi, il sottogruppo di ordine $d \mid n$ è il generato da $g^{n/d}$. □

Corollario 3.3.10. *Sia G un gruppo. O non è ciclico, o ammette esattamente 2 generatori nel caso sia infinito, o $\varphi(n)$ generatori nel caso abbia ordine n.*

Dimostrazione. Se G ammette un generatore allora é ciclico. E in tal caso valgono le proposizioni precedenti. □

Questo corollario si può applicare, per esempio, al gruppo $\mathbb{Z}/n\mathbb{Z}^*$. Avendo ordine $\varphi(n)$, o non è ciclico, o ha $\varphi(\varphi(n))$ generatori. Vedremo più avanti quando questo succede.

Con questi teoremi sui gruppi ciclici possiamo già affermare questo interessante fatto preannunciato alla sezione scorsa.

Proposizione 3.3.11. *Esiste un gruppo di ordine infinito con tutti gli elementi di ordine finito.*

Dimostrazione. Sia C_n il sottogruppo di $\mathbb{C}^*$ costituito dalle radici ennesime dell'unità. Consideriamo quindi il sottoinsieme di $\mathbb{C}^*$

$$G = \bigcup_{n=1}^{\infty} C_n$$

Vogliamo dimostrare che è un sottogruppo di $\mathbb{C}^*$.

L'identità appartiene ad ognuno dei C_n, quindi appartiene a G.

Se un elemento h appartiene a G, allora appartiene ad un C_n. Quindi il suo inverso appartiene ad C_n e quindi a G.

Presi due elementi g,h di G, supponiamo che g appartiene ad C_m e h appartiene a C_n. Verifichiamo che il prodotto gh appartenga a C_{mn}:

$$(gh)^{mn} = (g^m)^n (h^n)^m = 1$$

Quindi G è un (sotto)gruppo. Ogni suo elemento ha ordine finito, in quanto se x appartiene a C_n, allora $x^n = 1$ ed esso ha ordine al più n.

D'altra parte G è infinito. Per dimostrarlo notiamo che C_m è incluso in C_n se e solo se m divide n.

Infatti se $n = hm$, allora per ogni x in C_m

$$x^n = (x^m)^h = 1$$

D'altra parte gli elementi di C_k hanno la forma

$$\cos\left(\frac{2\pi d}{k}\right) + i\sin\left(\frac{2\pi d}{k}\right) \quad d = 0, \ldots, k-1$$

che sono potenze di

$$\zeta_k = \cos\left(\frac{2\pi}{k}\right) + i\sin\left(\frac{2\pi}{k}\right)$$

Quindi per ogni k il sottogruppo C_k è ciclico.

Quindi se C_m è incluso in C_n, allora ne è un sottogruppo. Quindi la cardinalità di C_m, pari a m, divide quella di C_n pari a n.

A questo punto è facile dimostrare che G è infinito. Supponiamo per assurdo che esso sia finito. Allora esisterà un N sufficientemente grande tale che

$$G = \bigcup_{n=1}^{N} C_n$$

Sia quindi ζ_{N+1} generatore di $N+1$. Egli dovrebbe appartenere a un certo C_i. Essendo ζ_{N+1} generatore di C_{N+1}, tutto C_{N+1} è un sottogruppo di C_i. Quindi $N+1 > i$ divide i. Assurdo. □

Chiudiamo con la seguente proposizione, che mette in relazione sottogruppi ciclici e ordine degli elementi.

Proposizione 3.3.12. *Sia G un gruppo. Allora il numero degli elementi di ordine d è $\varphi(d)$ volte il numero dei sottogruppi ciclici di ordine d.*

Dimostrazione. Siano gli insiemi

$$X_d = \{\, g \in G \mid \mathrm{ord}(g) = d \,\}$$
$$R_d = \{\, K \leq G \mid \text{ciclico e di ordine } d \,\}$$

e la mappa

$$\Phi \colon X_d \to R_d$$
$$g \mapsto \langle g \rangle$$

Vogliamo dimostrare che Φ è suggettiva, e che ogni elemento dell'immagine ha esattamente $\varphi(d)$ controimmagini.

Innanzitutto Φ è suggettiva, in quanto ogni elemento di R_d è un sottogruppo ciclico di ordine d, e quindi ammette un generatore di ordine d.

Inoltre ogni elemento di R_d ammette, per quanto visto, esattamente $\varphi(d)$ generatori.

Quindi, essendo che le preimmagine partizionano X_d, possiamo scrivere

$$|X_d| = \sum_{K \in R_d} |\Phi^{-1}(K)| = \sum_{K \in R_d} \varphi(d) = \varphi(d)\,|R_d|$$

Cioè il numero degli elementi di ordine d è $\varphi(d)$ volte il numero dei sottogruppi ciclici di ordine d. □

3.4 Omomorfismi tra Gruppi Ciclici

Il calcolo di omomorfismi è in generale un'operazione estremamente complicata, per non dire delle volte impossibile. Il caso più semplice è quando in arrivo abbiamo a che fare con gruppi ciclici.

Come successiva notazione, indicheremo con $\mathrm{Hom}(G, G')$ l'insieme degli omomorfismi da G a G'. In generale questo NON è un gruppo. Tuttavia la prossima proposizione dà una condizione sufficiente affinché gli si possa dare la struttura voluta.

Proposizione 3.4.1. *Siano $(G, \cdot)$, $(G', +)$ due gruppi, con l'ultimo abeliano. Allora $(\mathrm{Hom}(G, G'), *)$ è un gruppo, dove $f * h$ è la funzione*

$$(f * h)(g) = f(g) + h(g)$$

Dimostrazione. La parte delicata è l'affermazione che $f*h$ sia un omomorfismo da G a G'. Per verificarlo siano g, g' in G. Allora

$$\begin{aligned}(f * h)(g \cdot g') &= f(g \cdot g') + h(g \cdot g') \\ &= f(g) + f(g') + h(g) + h(g') \\ &= f(g) + h(g) + f(g') + h(g') \\ &= (f * h)(g) + (f * h)(g')\end{aligned}$$

Ma a questo punto l'associatività di $*$ deriva da quella di $+$.

Inoltre la mappa nulla $g \mapsto e'$ è l'elemento neutro.

Infine ogni elemento f di $\mathrm{Hom}(G, G')$ ha inverso $g \mapsto -f(g)$. □

Allora iniziamo col calcolo degli omomorfismi da $\mathbb{Z}$ ad un altro gruppo G.

Teorema 3.4.2. *Sia $(G, \cdot)$ un gruppo. Allora l'insieme $\mathrm{Hom}(\mathbb{Z}, G)$ è in bigezione con G. Inoltre se G è abeliano i due gruppi sono isomorfi.*

Dimostrazione. Sia $g \in G$. Se supponiamo che f sia un omomorfismo da $\mathbb{Z}$ in G, tale che $f(1) = g$, allora esso è determinato. Infatti per ogni $k \in \mathbb{Z}$ vale

$$f(k) = f(\underbrace{1 + \cdots + 1}_{k \text{ volte}}) = \underbrace{f(1) \cdot \cdots \cdot f(1)}_{k \text{ volte}} = g^k$$

D'altra parte sia g in G. Allora possiamo considerare la mappa

$$\begin{aligned} f \colon \mathbb{Z} &\to G \\ n &\mapsto g^n \end{aligned}$$

Questa è un omomorfismo, in quanto

$$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$$

Quindi abbiamo la bigezione

$$\begin{aligned} \Phi \colon G &\to \mathrm{Hom}(\mathbb{Z}, G) \\ g &\mapsto f_g \colon f(1) = g \end{aligned}$$

Osserviamo che se G è abeliano Φ è un omomorfismo, e quindi isomorfismo, tra i due gruppi. Infatti siano g, h in G. Allora

$$(f_g * f_h)(1) = f_g(1) + f_h(1) = g + h$$

Quindi $\Phi(g) * \Phi(h) = f_g * f_h$ coincide con $f_{g+h} = \Phi(g+h)$. Ergo Φ è un omomorfismo. □

Se invece vogliamo calcolare gli omomorfismi da $\mathbb{Z}/n\mathbb{Z}$, allora la situazione si fa più complicata. Infatti, almeno per ora, possiamo solamente discutere il caso in cui in arrivo ci sia un gruppo ciclico.

Consideriamo quindi i gruppi $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ e $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. Vogliamo capire se sono isomorfi a qualche gruppo noto. Procediamo con primo.

Teorema 3.4.3. *Per ogni $n \geq 1$ il gruppo $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ è banale.*

Dimostrazione. Dimostriamo che se f appartiene a $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$, allora è la mappa nulla.

Ma questo è immediato. L'ordine di $f(\bar{1})$ deve dividere l'ordine di $\bar{1}$ che è n. Tuttavia in $\mathbb{Z}$ tutti gli elementi, tranne 0, hanno ordine infinito.

Quindi $f(\bar{1}) = 0$, ed essendo che $\bar{1}$ genera $\mathbb{Z}/n\mathbb{Z}$, l'intera mappa f è nulla.

D'altra parte la mappa nulla è un banale omomorfismo.

Quindi $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ è il gruppo banale. □

Per il secondo la situazione si fa invece più intrigante.

Teorema 3.4.4. *Il gruppo* $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ *è isomorfo a* $\mathbb{Z}/(m,n)\mathbb{Z}$.

Dimostrazione. Come notato precedentemente, un omomorfismo f da $\mathbb{Z}/m\mathbb{Z}$ a $\mathbb{Z}/n\mathbb{Z}$ è determinato dal valore di $\bar{1}$. Infatti $\bar{1}$ genera $\mathbb{Z}/m\mathbb{Z}$.

Vogliamo comprendere quante scelte sono possibili per $f(\bar{1})$.

Se $f(\bar{1}) = \bar{a}$, allora l'ordine di $\bar{a}$ deve dividere l'ordine di $\bar{1}$, pari a m. Cioè

$$m \equiv 0 \pmod{n/(a,n)}$$

Questa congruenza è equivalente a

$$am \equiv 0 \pmod{n}$$

cioè a

$$a \equiv 0 \pmod{n/(m,n)}$$

Quindi $n/(m,n)$ deve dividere a, compreso tra 0 e $n-1$. Questo mi dà $n/(n/(m,n)) = (m,n)$ possibilità per a. Voglio verificare che una tale scelta è sempre valida.

Sia quindi un tale a, e sia f definita come

$$f_a \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$\bar{x} \mapsto x\bar{a}$$

Verifichiamo che f sia ben definita. Infatti presi $x = y + km$, allora

$$x\bar{a} = (y + km)\bar{a} = y\bar{a} + km\bar{a} = y\bar{a}$$

in quanto l'ordine di $\bar{a}$ divide m. Ma a questo punto l'essere un omomorfismo è una banale verifica:

$$f(\bar{x} + \bar{y}) = f(\overline{x+y}) = (x+y)\bar{a} = x\bar{a} + y\bar{a} = f(\bar{x}) + f(\bar{y})$$

Quindi abbiamo una bigezione

$$\Phi\colon X_{m,n} \to G$$
$$\bar{a} \mapsto f_a$$

con

$$X_{m,n} = \{\, \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid 0 \leq a \leq n-1,\ n/(m,n) \text{ divide } a \,\}$$

che ha cardinalità (m, n).

Come abbiamo detto, però, l'insieme $(G, *)$ è un gruppo. Basta solo vedere che è ciclico. A questo punto, avendo cardinalità (m, n), deve essere isomorfo a $\mathbb{Z}/(m, n)\mathbb{Z}$.

Semplicemente notiamo che la funzione f_1 genera G. Infatti presa f_a in G, allora

$$f_1^a(\bar{1}) = \underbrace{(f_1 * \cdots * f_1)}_{a \text{ volte}}(\bar{1}) = \underbrace{f_1(\bar{1}) + \cdots + f_1(\bar{1})}_{a \text{ volte}} = a\bar{1} = \bar{a}$$

Ergo f_1^a coincide con f_a e G è generato da f_1. □

Concludiamo con l'analisi degli automorfismi. Andiamo prima a definirli.

Definizione 3.4.5. Sia G un gruppo. L'insieme degli automorfismi di G, indicato con $\mathrm{Aut}(G)$, è l'insieme degli isomorfismi da G in sé.

Proposizione 3.4.6. *Dato un gruppo G, l'insieme* $\mathrm{Aut}(G)$*, se dotato della composizione di funzioni, è un gruppo.*

Dimostrazione. Analogo al fatto che $S(G)$ è un gruppo se dotato della composizione. □

Anche in questo caso il calcolo degli automorfismi di un gruppo è operazione non facile. Trattiamo il caso in cui il gruppo sia ciclico.

Teorema 3.4.7. *Il gruppo degli automorfismi di $\mathbb{Z}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$.*

Dimostrazione. Sia f in $\mathrm{Aut}(\mathbb{Z})$. Posto $k = f(1)$, l'immagine di f è $k\mathbb{Z}$ con k intero. Essendo f suggettiva, $k\mathbb{Z} = \mathbb{Z}$. Ma questo è possibile se e solo se $k = \pm 1$.

Quindi $f(1) = \pm 1$ e $f = \pm id$. D'altra parte questi sono banali automorfismi di $\mathbb{Z}$.

Abbiamo quindi dimostrato che $\mathrm{Aut}(\mathbb{Z}) = \{\pm id\}$. Questo gruppo è banalmente generato da $-id$, e quindi è isomorfo a $\mathbb{Z}/2\mathbb{Z}$. □

Per quanto riguarda il caso finito vale il prossimo teorema.

Teorema 3.4.8. *Il gruppo degli automorfismi di $\mathbb{Z}/n\mathbb{Z}$ è isomorfo a $\mathbb{Z}/n\mathbb{Z}^*$.*

Dimostrazione. Sia f un automorfismo. Esso è in particolar modo iniettivo. Quindi $\bar{k} = f(\bar{1})$ ha ordine n. Ergo k è un elemento coprimo con n, e $\bar{k}$ appartiene a $\mathbb{Z}/n\mathbb{Z}^*$.

Dimostriamo che effettivamente un $\bar{k}$ invertibile dà un automorfismo f_k.

Certamente k è diviso $n/(n,n) = 1$, quindi f_k è un omomorfismo da $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ per quanto già visto.

Inoltre f_k è suggettiva. Infatti ogni elemento di $\bar{a}$ di $\mathbb{Z}/n\mathbb{Z}$ è immagine di $\bar{a}\bar{h}$, con $\bar{h}$ inverso di $\bar{k}$.

$$f_k(\bar{a}\bar{h}) = ah\bar{k} = \bar{a}\bar{h}\bar{k} = \bar{a}$$

Quindi f_k è un omomorfismo suggettivo tra insiemi finiti della stessa cardinalità. Ergo è un isomorfismo.

In conclusione abbiamo una bigezione

$$\begin{aligned} \Phi\colon \mathbb{Z}/n\mathbb{Z}^* &\to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ \bar{k} &\mapsto f_k \end{aligned}$$

Verifichiamo che sia un omomorfismo. Presi $\bar{h}$, $\bar{k}$ in $\mathbb{Z}/n\mathbb{Z}^*$, allora

$$(f_h \circ f_k)(\bar{1}) = f_h(\bar{k}) = k\bar{h} = \overline{kh} = f_{kh}(\bar{1})$$

Quindi $f_h \circ f_k$ coincide con f_{kh} e Φ è un omomorfismo bigettivo, quindi è un isomorfismo. □

Chiudiamo questa sezione con i risultati ottenuti fino ad ora:

1. $\mathrm{Hom}(\mathbb{Z}, G)$ è in bigezione con G, e se G è abeliano è isomorfo ad esso.
2. $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$ è banale.
3. $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ è isomorfo a $\mathbb{Z}/(m,n)\mathbb{Z}$.
4. $\mathrm{Aut}(\mathbb{Z})$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$.
5. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ è isomorfo a $\mathbb{Z}/n\mathbb{Z}^*$.

3.5 Prodotto Diretto

Andiamo a considerare ora il prodotto diretto fra gruppi:

Proposizione 3.5.1. *Siano $(G, *_1)$, $(G', *_2)$ due gruppi. Allora $(G \times G', *)$, con*

$$(g_1, h_1) * (g_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$$

è un gruppo, con elemento neutro (e, e') e inverso di (g, h) pari a (g^{-1}, h^{-1}).

Dimostrazione. Semplice verifica. □

Il prodotto diretto è il modo più semplice per combinare gruppi. In particolare valgono le proprietà che uno ci si aspetta, come la seguente:

Proposizione 3.5.2. *Sia $G = G_1 \times G_2$ prodotto diretto di due gruppi. Allora il centro di G è il prodotto dei centri di G_1 e G_2.*

Dimostrazione. Dobbiamo dimostrare l'uguaglianza

$$Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$$

($\subseteq$) Sia (x, y) nel centro di G. Allora preso un qualunque z in G_1 vale la seguente uguaglianza:

$$(zx, y) = (z, e_2)(x, y) = (x, y)(z, e_2) = (xz, e_2)$$

Ergo $zx = xz$ per ogni z in G_1. Quindi x appartiene al centro di G_1. Analogamente si osserva che y appartiene al centro di G_2. Ergo (x, y) appartiene al prodotto dei due centri.

($\supseteq$) Sia (x, y) nel prodotto dei centri. Allora per ogni (v, w) in G vale l'uguaglianza

$$(v, w)(x, y) = (vx, wy) = (xv, yw) = (x, y)(v, w)$$

Ergo (x, y) appartiene al centro di G. □

Corollario 3.5.3. *Dati due gruppi G_1, G_2, essi sono abeliani se e solo se il loro prodotto diretto G lo è.*

Dimostrazione. Notiamo la seguente catena di coimplicazioni:

$$\begin{aligned} Z(G) = G &\Leftrightarrow Z(G_1) \times Z(G_2) = G_1 \times G_2 \\ &\Leftrightarrow Z(G_1) = G_1 \wedge Z(G_2) = G_2 \end{aligned}$$

Otteniamo quindi che G_1 e G_2 sono abeliani se e solo se lo è il loro prodotto. □

Affrontiamo ora questa domanda: quando è che il prodotto diretto di gruppi ciclici è ciclico? Cioè quando è che $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è isomorfo a $\mathbb{Z}/mn\mathbb{Z}$? Il prossimo teorema ci aiuta, andando a esaminare gli ordini degli elementi di un prodotto diretto.

Teorema 3.5.4. *Siano G_1, G_2 due gruppi e G il loro prodotto diretto. Allora per ogni (x, y) in G, esso ha ordine pari al minimo comune multiplo degli ordini di x e y.*

Dimostrazione. Sia (x, y) in $G = G_1 \times G_2$ e sia d il suo ordine. Allora, posto m ordine di x e n ordine di y, $[m, n]$ è multiplo sia di m che di n. Quindi

$$(x, y)^{[m,n]} = (x^{[m,n]}, y^{[m,n]}) = (e_1, e_2)$$

Ergo d divide $[m, n]$.

D'altra parte $(e_1, e_2) = (x, y)^d = (x^d, y^d)$. Quindi d è multiplo sia di m che di n. Ergo è multiplo di $[m, n]$.

Quindi $[m, n]$ e d si dividono a vicenda. Essendo positivi devono coincidere.

□

A questo punto andiamo ad attaccare il nostro problema. La sua risoluzione è la terza forma del TCR

Teorema 3.5.5 (Teorema Cinese del Resto - III Forma)**.** *Il prodotto diretto $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è ciclico se e solo se m e n sono coprimi.*

Dimostrazione. ($\Rightarrow$) Se $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è ciclico, allora esiste un g in G di ordine mn. Posto $g = (\bar{x}, \bar{y})$, allora

$$mn = \text{ord}(g) = [\text{ord}(\bar{x}), \text{ord}(\bar{y})] = \left[\frac{m}{(x, m)}, \frac{n}{(y, n)}\right] \leq [m, n] = \frac{mn}{(m, n)}$$

Quindi m e n sono coprimi.

($\Leftarrow$) Viceversa siano m e n coprimi. Allora $(\bar{1}, \bar{1})$ ha ordine $[m, n] = mn$ e quindi G è ciclico. □

In particolare se m e n sono coprimi, allora la seconda forma del TCR ci dice che

$$\Phi\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

è una bigezione. In verità è un omomorfismo, e quindi è l'isomorfismo cercato:

$$\begin{aligned}\Phi([a]_{mn} + [b]_{mn}) &= \Phi([a+b]_{mn}) \\ &= ([a+b]_m, [a+b]_n) \\ &= ([a]_m + [b]_m, [a]_n + [b]_n) \\ &= ([a]_m, [a]_n) + ([a]_n, [b]_n) \\ &= \Phi([a]_{mn}) + \Phi([b]_{mn})\end{aligned}$$

Il teorema precedente ci dà questo importante corollario:

Teorema 3.5.6. *Siano m, n interi coprimi. Allora $\mathbb{Z}/mn\mathbb{Z}^*$ è isomorfo al prodotto diretto di $\mathbb{Z}/m\mathbb{Z}^*$ e $\mathbb{Z}/n\mathbb{Z}^*$.*

Dimostrazione. Sappiamo che esiste una bigezione

$$\Psi\colon \mathbb{Z}/mn\mathbb{Z}^* \to \mathbb{Z}/m\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}^*$$

data dalla restrizione della Φ precedente. Allora si osserva, come fatto per Φ, che Ψ è un omomorfismo, cioè che per ogni $[a]_{mn}, [b]_{mn}$ nel dominio

$$\Psi([a]_{mn}[b]_{mn}) = \Psi([a]_{mn})\Psi([b]_{mn})$$

□

3.6 Classi Laterali

Abbiamo visto che, nel caso di gruppi ciclici, gli ordini degli elementi e dei sottogruppi dividono l'ordine del gruppo. Questa affermazione non è specifica dei gruppi ciclici, ma è molto più generale. Per arrivarci però dobbiamo introdurre le classi laterali destre e sinistre:

Definizione 3.6.1. Sia G un gruppo e H un sottogruppo. Diciamo che due elementi di G sono sinistra-equivalenti modulo H, e scriviamo $x \sim_H y$, se $y^{-1}x$ appartiene ad H. Detto in altri termini se esiste un h in H tale che $x = yh$.

Analogamente si dicono destra-equivalenti se xy^{-1} appartiene ad H, cioè se $x = hy$ per qualche h in H.

Proposizione 3.6.2. *La destra- e sinistra-equivalenza sono relazioni di equivalenza, e la classe di sinistra-equivalenza di x (analogo per quella destra) è*

$$xH = \{\, xh \mid x \in H \,\}$$

Dimostrazione. Verifichiamolo per la sinistra-equivalenza, l'altra è analoga.

Certamente per ogni x in G, $x = xe$, quindi x è equivalente a se stesso.

D'altra parte se x è equivalente a y, cioè $x = yh$, allora $y = xh^{-1}$. Quindi y è equivalente a x.

Infine se $x = yh$ e $y = zh'$, allora $x = zh'h$ ed è equivalente a z.

Verifichiamo ora che xH è la classe di equivalenza di x.

Se x è equivalente a y, allora $x^{-1}y = h$ appartiene a H. Quindi y coincide con xh e appartiene a xH.

D'altra parte se y appartiene a xH, allora $x^{-1}y$ appartiene a H e x è equivalente a y. □

Da quello detto sopra sappiamo che x e y sono sinistra-equivalente se e solo se le loro classi di equivalenza modulo H coincidono, cioè se e solo se $xH = yH$. Esse vengono dette classi laterali sinistre modulo H. Equivalente per le classi laterali destre.

Possiamo quindi enunciare il nostro teorema sulla divisibilità, il teorema di Lagrange.

Teorema 3.6.3 (Teorema di Lagrange)**.** *Sia G un gruppo e H un sottogruppo. Allora l'ordine di H divide quello di G.*

Dimostrazione. Se G è infinito, allora l'ordine di H, qualunque sia, divide l'ordine di G.

Se invece G ha ordine finito, sia R un insieme di rappresentanti per le classi laterali sinistre modulo H. Allora abbiamo la partizione

$$G = \bigsqcup_{x \in R} xH$$

da cui

$$|G| = \sum_{x \in R} |xH|$$

A questo punto ci basta notare che xH hanno tutte cardinalità pari all'ordine di H.

Infatti la mappa

$$\begin{aligned} \Phi\colon H &\to xH \\ h &\mapsto xh \end{aligned}$$

è una bigezione, ammettendo inversa

$$\begin{aligned} \Psi\colon xH &\to H \\ y &\mapsto x^{-1}y \end{aligned}$$

Quindi otteniamo l'uguaglianza

$$|G| = \sum_{x\in R} |xH| = |\{x \in R\}||H| = |H||R|$$

Ergo l'ordine di H divide quello di G. □

Corollario 3.6.4. *Sia x in G. Allora*

1. *Il suo ordine divide l'ordine di G.*
2. *Se G è finito, $x^{|G|} = e$.*

Dimostrazione. L'ordine di x è l'ordine del sottogruppo generato, che divide l'ordine di G.

Inoltre se G è finito, allora per il primo punto $x^{|G|} = e$. □

Notiamo che stiamo riscrivendo il teorema di Eulero tramite la teoria dei gruppi. Infatti presi a, n interi coprimi, allora $\bar{a}$ appartiene a $\mathbb{Z}/n\mathbb{Z}^*$, che ha ordine $\varphi(n)$. Ergo per quello appena dimostrato

$$\bar{a}^{\varphi(n)} = \bar{1} \;\Rightarrow\; a^{\varphi(n)} \equiv 1 \pmod{n}$$

che è esattamente il risultato fornito dal teorema di Eulero.

Come conseguenza immediata abbiamo questo risultato sui gruppi di ordine un primo:

Teorema 3.6.5. *Se G è un gruppo di ordine primo p, allora è isomorfo a $\mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione. Essendo G di ordine primo p, ammette almeno due elementi. Sia quindi $x \in G$ diverso dall'identità. Allora l'ordine di x è maggiore di 1 e divide p. Ergo x ha ordine p e genera G. □

Abbiamo quindi provato un primo *teorema di classificazione*. I teoremi di classificazione hanno lo scopo di classificare i gruppi a meno di isomorfismo. Abbiamo visto che per ogni primo p il gruppo $\mathbb{Z}/p\mathbb{Z}$ è l'unico gruppo di ordine p a meno di isomorfismo.

Ne vedremo altri di teoremi di questo genere. In particolare classificheremo i gruppi abeliani finiti (mentre per quelli finitamente generati bisogna aspettare Algebra II), e quelli di ordine sufficientemente piccolo. La prossima sezione ha esattamente lo scopo di analizzare quelli fino all'ordine 6.

3.7 Gruppi di Ordine Piccolo

Un modo per classificare i gruppi finiti è quello di usare le *Tavole di Cayley* o tavole di composizione. Esse sono tabelle a doppia entrata raffiguranti i risultati dell'operazione in G. In particolare se $G = \{g_1, \ldots, g_k\}$, allora alla riga i e colonna j troviamo il prodotto $g_i g_j$.

Le tavole di Cayley hanno lo scopo di raffigurare le operazioni in un gruppo G, indipendentemente da come vengono chiamati gli elementi di G. Quindi sono utili per classificare i gruppi a meno di isomorfismo.

Per comprendere come sono fatte, sia un generico gruppo $G = \{e, g, h\}$. Allora ammette tavola di Cayley

	e	g	h
e	e	g	h
g	g	gg	gh
h	h	hg	hh

È evidente che una tavola di Cayley è simmetrica se e solo se il gruppo è abeliano.

Una proprietà delle tavole di Cayley è la seguente, che useremo estensivamente:

Proposizione 3.7.1. *Sia una tavola di Caylery di un gruppo finito* $G =$

$\{a_1, \ldots, a_k\}$, *con* $a_0 = e$*:*

	e	$\ldots$	a_k
e	e	$\ldots$	a_k
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_k	a_k	$\ldots$	a_k^2

Allora essa è un quadrato latino. Cioè presa una qualsiasi riga, essa non può avere due entrate uguali. Analogamente per una qualsiasi colonna.

Dimostrazione. Supponiamo che esista una riga, relativa all'elemento a_i, con due entrate uguali. Cioè esistono a_j, a_k diversi tale che $a_i a_j = a_i a_k$. Questo implica che $a_j = a_k$. Assurdo.

Analogo per una qualsiasi colonna. □

Per entrare invece più nel "concreto", $\mathbb{Z}/2\mathbb{Z}$ ammette tavola di Cayley

	0	1
0	0	1
1	1	0

Essendo $\mathbb{Z}/2\mathbb{Z}$ abeliano, la tavola è simmetrica.

Procederemo adesso a riempire le tavole di Cayley di ordine $1, \ldots, 6$. Vedremo che che per n primo avremo di fatto un unica tavola. Infatti esiste un unico gruppo a meno di isomorfismo di ordine primo.

Per farlo però serve usare il teorema di Cauchy, che per ora dimostreremo solo per il primo che ci serve:

Teorema 3.7.2. *Sia un gruppo finito G di ordine pari. Esso ammette un elemento di ordine 2.*

Dimostrazione. Definiamo la seguente relazione di equivalenza su G:

$$x \sim y \;\Rightarrow\; x = y \vee x = y^{-1}$$

Si osserva immediatamente che questa è una relazione di equivalenza.

Inoltre presa una classe di equivalenza $[x]$, allora essa ammette al più due elementi: x e il suo inverso. In particolare ne ammette solo uno se e solo se x coincide col suo inverso, cioè se e solo se x ha ordine 2 oppure se è l'identità.

Ergo se partizioniamo G, otteniamo

$$\begin{aligned}|G| &= |\{\text{classi di eq. con 1 elemento}\}| + 2 \cdot |\text{classi di eq. con 2 elementi}\}| \\ &= |\{\, g \in G \mid g = e, \text{ord}(g) = 2 \,\}| + 2 \cdot |\{\text{classi di eq. con 2 elementi}\}|\end{aligned}$$

E quindi se passiamo ai moduli

$$\begin{aligned}0 &\equiv |G| \equiv |\{\, g \in G \mid g = e, \text{ord}(g) = 2 \,\}| \pmod 2 \\ 0 &\equiv |G| \equiv |\{\, g \in G \mid \text{ord}(g) = 2 \,\}| + 1 \pmod 2\end{aligned}$$

Quindi l'insieme degli elementi di ordine 2 ha cardinalità dispari, cioè non può essere vuoto. □

Incominciamo quindi ad analizzare tavole.

Se $n = 1$ abbiamo $G = \{e\}$, che dà come unica tavola

	e
e	e

Se $n = 2$, allora l'elemento diverso dall'identità ha ordine 2. Quindi posto a tale elemento, abbiamo la tavola

	e	a
e	e	a
a	a	e

che corrisponde al gruppo $\mathbb{Z}/2\mathbb{Z}$.

Se $n = 3$, siano a, b diversi dall'identità. Entrambi hanno ordine 3. Inoltre abbiamo queste due implicazioni, tutte due che portano all'assurdo

$$\begin{aligned}a^2 = e &\Rightarrow \text{ord}(a) = 2 \\ a^2 = a &\Rightarrow a = e\end{aligned}$$

Quindi $a^2 = b$. Analogamente $b^2 = a$. Possiamo quindi compilare parzialmente la tavola:

	e	a	b
e	e	a	b
a	a	b	
b	b		a

Infine per la proposizione 3.7.1 abbiamo l'entrata forzata $ab = e$ e $ba = e$.

Quindi abbiamo la tavola

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

che corrisponde al gruppo $\mathbb{Z}/3\mathbb{Z}$ (per esempio identificando a con $\bar{1}$ e b con $\bar{2}$).

Per $n = 4$ la cosa si fa più interessante. Consideriamo un suo elemento a di ordine 2, che esiste per Cayley, e poniamo $b \in G \setminus \{e, a\}$. L'ordine di b deve dividere 4, e quindi può essere o 2 o 4. Vedremo che ad un certo punto bisognerà fare una scelta, che porterà a due gruppi distinti.

Per ora consideriamo l'elemento $c = ab$. Non può essere né e, né a, né b. Infatti a, b non sono l'identità, e a ha come inverso se stesso, non b.

Allo stesso modo ba deve differire da e, a, b. Quindi deve coincidere con ab.

Inoltre $b = aab = aba$.

Quindi per ora abbiamo la tavola

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab		
ab	ab	b		

A questo punto abbiamo terminato le scelte obbligate. Infatti imporre che b abbia ordine 2 o 4 non sembra portare ad alcun assurdo.

Proviamo quindi a compilare la tavola per $b^2 = e$. Sfruttando il fatto che la tavola è un quadrato latino, e incrociando i dati sulle righe e colonne, otteniamo in ordine: $(ab)b = a$, $b(ab) = a$, $(ab)(ab) = e$.

Abbiamo quindi la prima tavola:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Torniamo ora indietro a

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab		
ab	ab	b		

e imponiamo $b^4 = e$. Allora deve essere b^2 diverso da e. Quindi grazie alla proposizione 3.7.1 sappiamo che $b^2 = a$ e $(ab)b = e$. Sempre per lo stesso risultato $b(ab) = e$ e $(ab)(ab) = a$

Ergo abbiamo la tavola:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	a	e
ab	ab	b	e	a

In conclusione abbiamo ottenuto le seguenti due tavole di Cayley:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	a	e
ab	ab	b	e	a

Quindi esistono al più due gruppi, a meno di isomorfismo, di ordine 4. O vediamo che le operazioni definite dalle due tavole formano un gruppo, oppure

esibiamo due gruppi di ordine 4. Ed infatti esistono $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $\mathbb{Z}/4\mathbb{Z}$. Non possono essere isomorfi in quanto il secondo non è ciclico.

Il secondo è isomorfo alla seconda tavola, ammettendo $\bar{1}$ come elemento di ordine 4, mentre il primo alla prima ed ammette solo elementi di ordine 2.

Notiamo inoltre che le due tavole hanno un blocco 2x2 in alto a sinistra che corrisponde alla tavola di $\mathbb{Z}/2\mathbb{Z}$. Ed infatti quel blocco è la tavola del sottogruppo generato da a.

Per quanto riguarda $n = 5$ consideriamo a in G di ordine 5. Allora posto $G = \{e, a, b, c, d\} = \{e, a, a^2, a^3, a^4\}$, si osserva, come nel caso $n = 3$, che la tavola di G ha la forma

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Chiudiamo con $n = 6$. Vogliamo dimostrare che esiste un elemento di ordine 3. Se per assurdo non fosse vero, consideriamo comunque a in G di ordine 2. Consideriamo quindi $b \in G \setminus \{e, a\}$ di ordine 2.

Come già fatto per $n = 4$, ab è diverso da a e b. A questo punto semplicemente poniamo $G = \{e, a, b, ab, c, d\}$.

Inoltre sia $b^{-1}a^{-1} = ba$ che ab sono inversi di ab. Ergo $ab = ba$ e riusciamo a compilare parzialmente la tavola:

	e	a	b	ab	c	d
e	e	a	b	ab	c	d
a	a	e	ab	b	d	c
b	b	ab	e	a		
ab	ab	b	a	e		
c						
d						

A questo punto però si vedono già i problemi. Il blocco 4x4 in alto a sinistra corrisponderebbe ad un sottogruppo $H = \{e, a, b, ab\}$ di ordine 4 in un gruppo di ordine 6. Per Lagrange questo è totalmente impossibile.

Un altro modo per individuare l'assurdo è osservare che bc non potrebbe essere nessuno tra e, a, b, ab, in quanto ciò causerebbe, da parte della terza riga, della violazione della proposizione 3.7.1. Tuttavia bc non potrebbe neanche essere uguale a d o c, in quanto questo causerebbe problemi da parte della 5 colonna.

Quindi bc non assume mai un valore accettabile, e abbiamo ottenuto l'assurdo. Quindi G deve contenere un elemento di ordine 3.

Riproviamo ponendo a come prima e b di ordine 3 (come si vede questo approccio per la classificazione dei gruppi diventa sempre più impossibile mano a mano che gli ordini salgono).

In questo caso b^2 non può essere pari a a, altrimenti $b^4 = e$ e b avrebbe ordine che divide 4, cosa non vera.

Seguendo analoghe implicazioni si scopre che gli altri elementi di G sono b^2 e ab^2. Quindi si compila la tavola fino al seguente punto:

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b		b^2	e		
b^2	b^2		e	b		
ab	ab		ab^2	a		
ab^2	ab^2		a	ab		

A questo punto si è totalmente bloccati. Quello che si può cercare di capire è cosa vale ba. Si vede immediatamente che o esso coincide con ab o con ab^2.

Seguendo la prima strada, stiamo di fatto imponendo che il gruppo sia abeliano. Infatti la tavola si completa (si consiglia di sfruttare la proposizio-

ne 3.7.1) a:

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab	b^2	e	ab^2	a
b^2	b^2	ab^2	e	b	a	ab
ab	ab	b	ab^2	a	b^2	e
ab^2	ab^2	b^2	a	ab	e	b

Invece seguendo la seconda strada, abbiamo la tavola completata a

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

Quindi abbiamo al più due gruppi di ordine 6 a meno di isomorfismo. In effetti ne abbiamo esattamente due.

Da una parte abbiamo $\mathbb{Z}/6\mathbb{Z}$, corrispondente alla prima tavola grazie all'identificazione di $\bar{3}$ con a e $\bar{2}$ con b.

D'altra parte abbiamo il gruppo simmetrico S_3 che ha $3! = 6$ elementi. Esso non è abeliano e corrisponde alla seconda tavola tramite l'identificazione

$$\begin{aligned} b = \sigma \colon 1 &\mapsto 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \\ i &\mapsto i \quad \forall i > 3 \\ a = \tau \colon 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 3 \\ i &\mapsto i \quad \forall i > 3 \end{aligned}$$

Chiudiamo questa sezione con una curiosità: Abbiamo detto che le tavole di Cayley sono quadrati latini. Vale il viceversa? Cioè ogni quadrato latino è tavola di composizione di un gruppo?

La risposta è negativa. Per esempio la seguente tavola latina:

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

non può essere la tavola di composizione di un gruppo, in quanto nè a nè b nè c si comportano come un elemento neutro.

Tuttavia le tavole latine hanno associate una struttura algebrica, forse tra le più semplici che si possono costruire: quella di *quasigruppo*.

Definizione 3.7.3. Un quasigruppo è una coppia $(G, *)$, con G un insieme e $*\colon G \times G \to G$ un'operazione, tale che si possano fare le divisioni a destra e a sinistra. Cioè tale che per ogni a, b in G esistono unici g, h in G tali che $a * g = b$ e $h * a = b$.

L'esistenza e l'unicità di g, h danno esattamente la condizione per cui la tavola di composizione sia un quadrato latino: in ogni riga, e in ogni colonna, compaiono tutti gli elementi una sola volta.

Inoltre, dato un quadrato latino è semplice capire se il relativo quasigruppo ammette un elemento neutro. Infatti se $G = \{a_1, \ldots, a_k\}$, allora (l'unico) elemento neutro a_j deve soddisfare la seguente condizione: nella riga e colonna j-esime compaiano, in ordine corretto, gli elementi di G.

Quindi possiamo dire che con le tavole di Cayley possiamo maneggiare oggetti leggermente più complessi dei quasigruppi: i *loop*.

Definizione 3.7.4. Un loop è un quasigruppo $(G, *)$ che ammette un elemento e, detto elemento neutro, tale che $e * x = x = x * e$ per ogni x in G.

I loop associativi sono esattamente i gruppi. Tuttavia qui la faccenda si fa più complicata. Infatti l'associatività è una proprietà su tre elementi, che quindi non si presta ad essere facilmente controllata su una tavola di composizione, che è una tabella a doppia entrata.

3.8 Quozienti di Gruppi

Come con gli spazi vettoriali, lo scopo di questa sezione è la costruzione di quozienti di gruppi. Tuttavia, mentre nel caso di spazi vettoriali potevamo sempre ottenere un nuovo spazio vettoriale quozientando per un sottospazio, nel caso dei gruppi questa affermazione è molto falsa. Il nocciolo delle questione è questo: preso un sottogruppo H di un gruppo G, non è assolutamente detto che le classi laterali sinistre e destre coincidano. Nel senso che può esistere un x in G tale che xH e Hx sono diversi.

Forniamo subito un esempio tramite $G = S_3$. Sappiamo dalla sezione precedente che

$$G = \{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$$

A questo punto prendiamo $H = \langle\tau\rangle = \{e, \tau\}$ e $x = \sigma$. Calcolando le classi laterali si scopre che

$$\sigma H = \{\sigma, \sigma\tau\} = \{\sigma, \tau\sigma^2\}$$
$$\sigma H = \{\sigma, \tau\sigma\}$$

Quindi le classi laterali sono differenti.

Quindi conviene restringersi ad una classe particolare di sottogruppi: quelli *normali*.

Definizione 3.8.1. Sia G un gruppo. Un sottogruppo H è normale in G, e si indica con $H \trianglelefteq G$, se per ogni x in G le sue classi laterali sinistre e destre modulo H coincidono. Equivalentemente se per ogni x in G il sottogruppo H coincide con xHx^{-1}.

Proposizione 3.8.2. *Sia G gruppo e H sottogruppo.*

1. *Se G è abeliano, H è normale in G.*
2. *Se per ogni x in G, xHx^{-1} è incluso in H, allora H è normale in G.*
3. *Se H coincide con $\{e\}$, G o $Z(G)$, allora esso è normale in G.*

Dimostrazione. (1.) Se G è abeliano, allora per ogni h in H, $xhx^{-1} = h$. Quindi $xHx^{-1} = H$.

(2.) Sia z in G. Sappiamo che zHz^{-1} è incluso in H. D'altra parte per ipotesi sappiamo anche che $z^{-1}H(z^{-1})^{-1} = z^{-1}Hz$ è incluso in H. Ergo

$$H = z(z^{-1}Hz)z^{-1} \subseteq zHz^{-1}$$

Quindi per ogni z in G, $zHz^{-1} = H$ e H è normale in G.

(3.) Per $H = \{e\}$ o $H = G$, allora è banalmente normale.

Inoltre per ogni x in G e per ogni h in $Z(G)$, $xhx^{-1} = hxx^{-1} = h$. Ergo $xZ(G)z^{-1} = Z(G)$ e $Z(G)$ è normale in G. □

Sarà utile, per quello che diremo in seguito, notare che i sottogruppi normali si comportano bene per l'intersezione e con gli omomorfismi.

Proposizione 3.8.3. *Sia G un gruppo e H,K sottogruppi, con H normale in G. Allora l'intersezione $H \cap K$ è normale in K, e lo è in G se anche H è normale in G.*

Dimostrazione. Iniziamo con la prima verifica.

Per ogni k in K, allora valgono le seguenti inclusioni:

$$\begin{aligned} k(H \cap K)k^{-1} &\subseteq kKk^{-1} \subseteq K \\ k(H \cap K)k^{-1} &\subseteq kHk^{-1} \underset{H \trianglelefteq G}{\subseteq} H \end{aligned}$$

Allora $k(H \cap K)k^{-1}$ è incluso in $H \cap K$, che quindi è normale in K.

Se anche K è normale in G, sia x in G. Allora

$$\begin{aligned} x(H \cap K)x^{-1} &\subseteq xHx^{-1} \subseteq H \\ x(H \cap K)x^{-1} &\subseteq xKx^{-1} \subseteq K \end{aligned}$$

Allora $x(H \cap K)x^{-1}$ è contenuto in $H \cap K$, che quindi è normale in G. □

Proposizione 3.8.4. *Sia $f\colon G \to G'$ un omomorfismo. Se H' è un sottogruppo normale di G', allora $f^{-1}(H')$ è un sottogruppo normale di G. D'altra parte se H è un sottogruppo normale di H, allora $f(H)$ è un sottogruppo normale di $f(G)$.*

Dimostrazione. Sia H' sottogruppo normale di G'.

Preso x in G sia y la sua immagine in G'. Allora si osserva che vale la seguente uguaglianza:

$$\begin{aligned} x\, f^{-1}(H')\, x^{-1} &\subseteq f^{-1}(y)\, f^{-1}(H')\, f^{-1}(y^{-1}) \\ &= f^{-1}(y\, H'\, y^{-1}) \\ &= f^{-1}(H') \end{aligned}$$

Quindi $f^{-1}(H')$ è normale in G.

D'altra parte sia H sottogruppo di G.

Preso $f(x)$ nell'immagine di f, allora si osserva che vale l'uguaglianza:

$$f(x)\, f(H)\, f(x)^{-1} = f(x)\, f(H)\, f(x^{-1}) = f(xHx^{-1}) = f(H)$$

Quindi $f(H)$ è normale nell'immagine di G. □

Introduciamo ora il concetto di indice di un sottogruppo, passando per questa proposizione.

Proposizione 3.8.5. *Sia G gruppo e H sottogruppo. Allora il numero di classi laterali sinistre e destre modulo H coincidono, e viene detto l'indice di H in G, e indicato con $[G : H]$.*

Dimostrazione. La seguente mappa

$$\begin{aligned} \Phi\colon \{\, xH \mid x \in G \,\} &\to \{\, Hx \mid x \in G \,\} \\ xH &\mapsto Hx \end{aligned}$$

è una banale bigezione ben definita. □

Un interessante proposizione è che tutti i sottogruppi di indice due sono normali.

Proposizione 3.8.6. *Sia G gruppo e H sottogruppo di indice due. Allora H è normale in G.*

Dimostrazione. Sappiamo che le classi laterali sinistre e destre partizionano G. Quindi presa una classe laterale xH, abbiamo due possibilità. O essa è la classe banale $eH = He$, che quindi coincide con la destra associata, oppure è l'altra classe laterale sinistra. Nel secondo caso, avendo H indice due otteniamo

$$Hx = G \setminus He = G \setminus eH = xH$$

Quindi H è normale in G. □

I gruppi normali sono essenziali per creare i quozienti di gruppi. Prima di definirli sfruttiamo le classi laterali per presentare la seguente proposizione.

Proposizione 3.8.7. *Sia un omomorfismo $f\colon G \to G'$. Allora valgono le seguenti affermazioni:*

1. *Il nucleo di f è normale in G.*
2. *Per ogni x, y in G, essi hanno la stessa immagine se e solo le le loro classi laterali modulo $\mathrm{Ker}(f)$ coincidono.*
3. *Se z appartiene all'immagine di f e x è un elemento della preimmagine di z, allora $f^{-1}(z) = x\,\mathrm{Ker}(f)$ e ha cardinalità pari a quella del nucleo.*

Dimostrazione. (1.) Sia g in G e z nel nucleo di f. Allora

$$f(gzg^{-1}) = f(g)f(z)g(g)^{-1} = f(g)e'f(g)^{-1} = e'$$

Quindi gzg^{-1} appartiene al nucleo di f e $\mathrm{Ker}(f)$ è normale in G.

(2.) Semplicemente osservando questa catena di implicazioni:

$$f(x) = f(y) \;\Leftrightarrow\; f(xy^{-1}) = e' \;\Leftrightarrow\; xy^{-1} = \mathrm{Ker}(f) \;\Leftrightarrow\; x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f)$$

(3.) La preimmagine di z sono tutti gli y in G tale che $f(y) = f(x)$. Per il punto precedente sono tutti e soli y in G tale che $x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f)$. Questi y sono esattamente la classe laterale $x\,\mathrm{Ker}(f)$. □

Possiamo definitivamente introdurre il concetto di gruppo quoziente:

Teorema 3.8.8. *Sia G un gruppo e H sottogruppo normale. Indicando con G/H l'insieme delle classi laterali modulo H e con $*$ l'operazione*

$$*\colon G/H \times G/H \to G/H$$
$$(xH, yH) \mapsto (xy)H$$

allora la coppia $(G/H, *)$ è un gruppo.

Dimostrazione. Una volta che dimostriamo la buona definizione di $*$, allora l'associatività è data dall'associatività dell'operazione su G. Inoltre $[e]$ risulta essere l'elemento neutro e $[x^{-1}]$ l'inverso di $[x]$.

Siano quindi x' equivalente a x e y' equivalente a y. Allora $x' = xn$ e $y' = yn'$ con n, n' in H. Inoltre essendo H normale in G, esiste un n'' in H tale che $ny = yn''$. Ergo

$$x'y' = xnyn' = xyn''n' \in (xy)H$$

Quindi il prodotto xy e il prodotto $x'y'$ sono equivalenti modulo H. Quindi la nostra operazione $*$ è ben definita. □

L'omomorfismo canonico che viene col concetto di quoziente è il passaggio al quoziente:

Proposizione 3.8.9. *La mappa*

$$\pi \colon G \to G/H$$
$$x \mapsto xH$$

è un omomorfismo di gruppi con nucleo pari a H

Dimostrazione. Da una parte presi x, y in G, allora

$$\pi(xy) = (xy)H = xH * yH = \pi(x) * \pi(y)$$

Dall'altra il nucleo di π è

$$\mathrm{Ker}(\pi) = \{\, x \in G \mid \pi(x) = \pi(e) \,\} = \{\, x \in G \mid xH = H \,\} = H \qquad \square$$

Corollario 3.8.10. *Dato un gruppo G, i suoi sottogruppi normali sono tutti e soli i nuclei di omomorfismi con dominio G.*

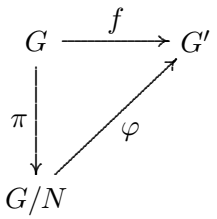
Dimostrazione. Se H è un sottogruppo di G, nucleo di un omomorfismo $\varphi \colon G \to G'$, allora sappiamo che è normale.

Viceversa se H è un sottogruppo normale di G, allora è nucleo del passaggio al quoziente da G a G/H. □

Notiamo che quello che stiamo facendo è esattamente quello che facemmo con l'insieme $\mathbb{Z}/n\mathbb{Z}$, quando abbiamo imposto operazioni sulle classi. E infatti, letto con la teoria dei gruppi, abbiamo quozientato il gruppo $\mathbb{Z}$ per il sottogruppo $n\mathbb{Z}$, che è normale essendo $\mathbb{Z}$ abeliano.

Di fondamentale importanza per i quozienti sono i quattro teoremi di omomorfismi che enuncieremo. Iniziamo con il primo:

Teorema 3.8.11 (I Teorema di Omomorfismo)**.** *Sia $f\colon G \to G'$ omomorfismo e sia N sottogruppo normale di G, contenuto nel nucleo di f. Allora esiste un'unica mappa $\varphi\colon G/N \to G'$ che fa commutare il diagramma*



Inoltre φ e f hanno la stessa immagine, e il nucleo di φ è $\mathrm{Ker}(f)/N = \pi(\mathrm{Ker}(f))$.

Dimostrazione. Innanzitutto φ è obbligata. Infatti sia $\varphi\colon G/N \to G'$ tale che $\varphi \circ \pi = f$. Allora ogni xN in G/N viene mandato in

$$\varphi(xN) = (\varphi \circ \pi)(x) = f(x)$$

D'altra parte sia φ definita come sopra. Dobbiamo verificare innanzitutto che φ sia ben definita.

Presi x, y nella stessa classe laterale, allora $x = yh$ con h in $N \subseteq \mathrm{Ker}(f)$. Allora h appartiene anche a $\mathrm{Ker}(f)$, quindi

$$f(y) = f(xh) = f(x)f(h) = f(x)$$

Quindi $\varphi(xH)$ non dipende dal rappresentante scelto.

Verifichiamo ora che φ, così definita, sia un omomorfismo. Siano quindi xN, yN in G/N. Allora

$$\varphi(xN)\,\varphi(yN) = xy = \varphi((xy)N) = \varphi(xN * yN)$$

Infine $\varphi \circ \pi = f$ per costruzione.

Per quanto riguarda il calcolo dell'immagine abbiamo la catena di uguaglianze

$$\begin{aligned}\mathrm{Im}(\varphi) &= \{\, \varphi(xN) \mid x \in G \,\} \\ &= \{\, f(x) \mid x \in G \,\} \\ &= \mathrm{Im}(f)\end{aligned}$$

Infine

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \left\{ xN \;\middle|\; \varphi(xH) = e' \right\} \\ &= \left\{ xN \;\middle|\; f(x) = e' \right\} \\ &= \{ xN \mid x \in \mathrm{Ker}(f) \} \\ &= \mathrm{Ker}(f)/N\end{aligned}$$

□

Corollario 3.8.12. *Sia $f\colon G \to G'$ omomorfismo. Allora f si scompone come $f = g \circ h$, con H gruppo, $h\colon G \to H$ suriettiva e $g\colon H \to G$ iniettiva.*

Dimostrazione. Prendendo $N = \mathrm{Ker}(f)$ e φ come sopra, allora f si scompone come $\varphi \circ \pi$. Inoltre π è suggettiva essendo il passaggio ad un quoziente e φ ha nucleo

$$\mathrm{Ker}(\varphi) = \mathrm{Ker}(f)/\mathrm{Ker}(f) = \{N\}$$

Cioè φ è iniettiva. □

Corollario 3.8.13. *Sia $f\colon G \to G'$ omomorfismo suggettivo. Allora, posto $N = \mathrm{Ker}(f)$, la φ definita precedentemente è un isomorfismo.*

Dimostrazione. È suggettiva in quanto f lo è. Inoltre è iniettiva per lo stesso ragionamento del corollario precedente. □

Enunciato il primo teorema di omomorfismo, procediamo col secondo.

Teorema 3.8.14 (II Teorema di Omomorfismo)**.** *Sia G un gruppo e H, K sottogruppi normali di G con H incluso di K. Allora H è normale in K, K/H è normale in G/H e G/K è isomorfo a $(G/H)/(K/H)$.*

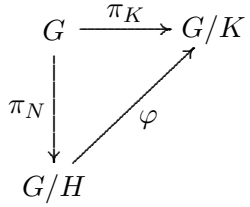
Dimostrazione. Iniziamo verificando la normalità di H in K.

Sappiamo però che $xHx^{-1} = H$ per ogni x in G, quindi vale in particolare per ogni x in K. Quindi H è normale in K.

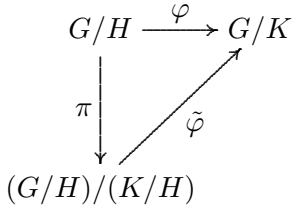
Verifichiamo ora che K/H è normale in G/H. Tuttavia possiamo vedere K/H come l'immagine di K tramite la proiezione π_H su G/H. Essendo K normale in G ed essendo π_H suggettiva, allora K/H è normale in G/H per la proposizione 3.8.4.

Procediamo ora a dimostrare l'isomorfismo.

Applichiamo innanzitutto il primo teorema di omomorfismo a π_K. Essendo che H è incluso in $K = \mathrm{Ker}(\pi_K)$, esiste un'unica φ che fa commutare il diagramma.



Inoltre $\mathrm{Ker}(\varphi) = \mathrm{Ker}(\pi_K)/H = K/H$ ed essendo π_K suggettiva, anche φ lo è. Quindi possiamo applicare nuovamente il teorema di omomorfismo per ottenere $\tilde{\varphi}$, l'isomorfismo cercato.



□

Per il prossimo teorema dobbiamo introdurre il seguente risultato:

Proposizione 3.8.15. *Sia G un gruppo e H, K sottogruppi. Definiamo i seguenti sottoinsiemi:*

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

Se $HK = KH$ allora HK è un sottogruppo (e per simmetria anche KH). Viceversa se HK è un sottogruppo finito, allora $HK = KH$.

Dimostrazione. (1.) Certamente $e = ee$ appartiene a HK.

Inoltre se hk appartiene a HK, allora l'inverso $k^{-1}h^{-1}$ appartiene a KH quindi a HK.

Presi ora h_1k_1 e h_2k_2 in HK, allora k_1h_2 appartiene a KH, quindi a HK. Quindi possiamo porre $k_1h_2 = h_3k_3$, da cui

$$h_1k_1h_2k_2 = h_1h_3k_3k_2 = (h_1h_3)(k_3k_2) \in HK$$

Quindi HK è un sottogruppo.

(2.) Notiamo innanzitutto che KH è incluso in HK.

Sia kh in KH. Esso è l'inverso di $h^{-1}k^{-1}$ che appartiene a HK. Essendo quest'ultimo un sottogruppo, allora anche kh appartiene a HK. Quindi KH è incluso in HK.

Dimostriamo ora che HK e KH hanno la stessa cardinalità. A questo punto, grazie alla finitezza di HK, avremo l'uguaglianza cercata.

La seguente mappa è una banale bigezione:

$$\begin{aligned}\Phi\colon HK &\to KH\\ hk &\mapsto (hk)^{-1} = k^{-1}h^{-1}\end{aligned}$$

□

Corollario 3.8.16. *Sia G un gruppo e H, K sottogruppi. Se H è normale in G, allora HK è un sottogruppo.*

Dimostrazione. Verifichiamo che $HK = KH$.

Essendo H normale in G, per ogni k in K vale che $kH = Hk$. Quindi $KH = HK$ e HK è un sottogruppo. □

Notiamo ora un paio di cose.

Innanzitutto se G è un gruppo infinito, e sia HK che KH sono sottogruppi, allora $HK = KH$. Infatti seguendo la dimostrazione del teorema precedente entrambe le inclusioni.

Inoltre nel teorema precedente abbiamo notato che $HK = KH$ indipendentemente dal fatto che HK sia o meno un sottogruppo. Ci si può chiedere se vale una stima sulla loro cardinalità nel caso siano finiti. In effetti la prossima proposizione afferma proprio quello.

Proposizione 3.8.17. *Sia G un gruppo, H, K sottogruppi. Se HK è un sottoinsieme finito, allora ha cardinalità*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Dimostrazione. Consideriamo la seguente mappa suggettiva

$$\begin{aligned}\Phi\colon H &\to HK\\ (h,k) &\mapsto hk\end{aligned}$$

Affermo che, preso hk nell'immagine, la sua preimmagine è data da

$$\Phi^{-1}(hk) = (ht^{-1}, tk) \quad t \in H \cap K$$

Certamente preso (ht^{-1}, tk) come sopra, allora ha immagine

$$\Phi(ht^{-1}, tk) = ht^{-1}tk = hk$$

D'altra parte preso (h', k') tale che $h'k' = hk$, allora

$$k'k^{-1} = (h')^{-1}h = t \in H \cap K$$

Ergo come volevamo dimostrare

$$h' = ht^{-1} \quad k' = tk \qquad t \in H \cap K$$

Quindi per ogni hk in HK, la sua preimmagine ha cardinalità

$$|\Phi^{-1}(hk)| = |\{\ (ht^{-1}, tk) \ \big|\ t \in H \cap K\ \}| = |H \cap K|$$

E procedendo come nella dimostrazione del teorema di Lagrange

$$|H||K| = |H \times K| = \sum_{y \in HK} |\Phi^{-1}(y)| = |H \cap K||HK|$$

Abbiamo quindi ottenuto l'uguaglianza voluta. □

Affrontato questo argomento, possiamo procedere con terzo teorema di omomorfismo.

Teorema 3.8.18 (III Teorema di Omomorfismo)**.** *Sia G un gruppo e H, K sottogruppi normali in G. Allora K è normale in HK, $H \cap K$ lo è in H e $H/(H \cap K)$ è isomorfo a HK/K.*

Dimostrazione. Innanzitutto essendo H normale in G, il sottoinsieme HK è un sottogruppo di G.

Inoltre K è normale in G, quindi a maggior ragione lo è in HK.

Infine grazie alla proposizione 3.8.3 sappiamo che $H \cap K$ è normale in H.

Per dimostrare l'isomorfismo sia la mappa

$$\varphi \colon H \to HK/K$$
$$x \mapsto xK$$

Essa è un omomorfismo ben definito in quanto restrizione di $\pi\colon HK \to HK/K$.

Verifichiamo che φ sia suggettiva.

Presa una classe in HK/K, essa si scrive come xK con x in HK. Allora $x = hk$ con h in H e k in K. Notiamo quindi che

$$\varphi(h) = hK = (hk)K = xK$$

Quindi xK appartiene all'immagine di φ e φ è suggettiva.

Per quanto riguarda il nucleo di φ, esso è

$$\mathrm{Ker}(\varphi) = \{\, x \in H \mid xK = K \,\} = \{\, x \in H \mid x \in K \,\} = H \cap K$$

Quindi, per il primo teorema di omomorfismo, otteniamo

$$\frac{HK}{K} = \mathrm{Im}(\varphi) \simeq \frac{H}{\mathrm{Ker}(\varphi)} = \frac{H}{H \cap K}$$

□

Concludiamo ora con il teorema di corrispondenza fra sottogruppi, detto anche quarto teorema di omomorfismo.

Teorema 3.8.19 (Teorema di Corrispondenza fra Sottogruppi)**.** *Sia G un gruppo N un suo sottogruppo normale. Allora esiste una corrispondenza biunivoca fra i sottogruppi di G/N e i sottogruppi di G che contengono N:*

$$\begin{aligned} \alpha\colon \{\, H \leq G \mid N \leq H \,\} &\to \{\, \mathcal{H} \leq H/N \,\} \\ H &\mapsto H/N = \pi(H) \end{aligned}$$

Inoltre questa corrispondenza preserva normalità e indici dei sottogruppi.

Dimostrazione. Siano le mappe

$$\begin{aligned} \alpha\colon \{\, H \leq G \mid N \leq H \,\} &\to \{\, \mathcal{H} \leq H/N \,\} \\ H &\mapsto H/N = \pi(H) \end{aligned}$$

$$\begin{aligned} \beta\colon \{\, \mathcal{H} \leq H/N \,\} &\to \{\, H \leq G \mid N \leq H \,\} \\ \mathcal{H} &\mapsto \pi^{-1}(\mathcal{H}) \end{aligned}$$

Verifichiamo innanzitutto che siano ben definite.

Innanzitutto essendo π un omomorfismo, allora immagini e preimmagini di sottogruppi sono sottogruppi.

Dobbiamo quindi verificare che se $\mathcal{H}$ è un sottogruppo di G/N, allora la sua preimmagine contiene N.

Ma questo è immediato. Infatti $\mathcal{H}$ contiene l'elemento neutro di G/N, che è immagine di ogni elemento di N. Quindi la preimmagine di $\mathcal{H}$ contiene N.

Verifichiamo ora che α e β sono una l'inversa dell'altra.

Sia quindi H sottogruppo di G che contiene N. Notiamo innanzitutto che se gN è un elemento di G/N uguale ad un elemento hN di H/N, allora g deve coincidere con hn per qualche n in N. Ma essendo che N è incluso in H, anche g appartiene a H. Ergo

$$\beta(\alpha(H)) = \beta(H/N) = \pi^{-1}(H/N) = H$$

D'altra parte sia $\mathcal{H}$ un sottogruppo di G/N. Allora essendo π suggettiva:

$$\alpha(\beta(\mathcal{H})) = \pi(\pi^{-1}(\mathcal{H})) = \mathcal{H}$$

Quindi α e β sono una l'inversa dell'altra e abbiamo la corrispondenza fra i sottogruppi.

Per quanto riguarda la normalità sappiamo che se H è normale in G, allora H/N è normale in G/N per il secondo teorema di omomorfismo.

D'altra parte se $\mathcal{H}$ è normale in G/N, allora H, essendo la preimmagine di $\mathcal{H}$ secondo π, è normale in G per la proposizione 3.8.4.

Infine per quanto riguarda gli indici, sappiamo grazie al secondo teorema di omomorfismo che

$$\frac{G}{H} \simeq \frac{G/N}{H/N}$$

ergo

$$[G : H] = \left|\frac{G}{H}\right| = \left|\frac{G/N}{H/N}\right| = [G/N : H/N]$$

□

Notiamo che questo teorema dà una rilettura del fatto che $\mathbb{Z}/n\mathbb{Z}$ abbia un unico sottogruppo per ogni divisore di d. Infatti i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono in corrispondenza con i sottogruppi di $\mathbb{Z}$ che contengono $n\mathbb{Z}$. E questi sono esattamente uno, pari a $d\mathbb{Z}$, per ogni d che divide n.

Chiudiamo la sezione sui quozienti con due teoremi, iniziando col teorema di Cauchy per gruppi abeliani.

Teorema 3.8.20 (Teorema di Cauchy Abeliano)**.** *Sia G un gruppo abeliano finito, il cui ordine è diviso da un primo p. Allora esiste un elemento in G di ordine p.*

Dimostrazione. Procediamo per induzione forte su $k = |G|/p$.

Se $k = 1$, allora G ha ordine p. Quindi è ciclico e ammette $p - 1$ elementi di ordine p.

Se $k > 1$, sia g un elemento di G diverso dall'identità.

Se g ha ordine multiplo di p, allora nel sottogruppo ciclico $\langle g \rangle$ troviamo $p - 1 = \varphi(p)$ elementi di ordine p.

Se g non ha ordine multiplo di p, allora il sottogruppo generato è normale in G, essendo quest'ultimo abeliano. Possiamo quindi considerare $H = G/\langle g \rangle$.

L'ordine di H è $|G|/|\langle g \rangle|$, che è minore dell'ordine di G. Inoltre p non divide l'ordine di g, ma divide l'ordine di G. Quindi p divide l'ordine di H.

Quindi per ipotesi induttiva esiste in H un elemento di ordine p. Poniamo $x\langle p \rangle$ tale elemento.

Allora $x\langle p \rangle$ è immagine di x tramite il passaggio al quoziente. Quindi x ha ordine multiplo di p. A questo punto si procede come sopra, trovando in $\langle x \rangle$ un elemento di ordine p. □

Il secondo teorema che chiude questa sezione è un risultato a prima vista innocente, che però si rivelerà estremamente utile in seguito.

Teorema 3.8.21. *Sia G un gruppo. Se $G/Z(G)$ è ciclico, allora G è abeliano.*

Dimostrazione. Sappiamo che $G/Z(G)$ è generato da una certa classe $aZ(G)$. Allora per ogni g in G, la classe $gZ(G)$ coincide con $a^k Z(G)$ per qualche intero k. Cioè esiste un z in $Z(G)$ tale che $g = a^k z$

A questo punto siano g, h due elementi di G. Allora esistono z, z' in $Z(G)$ e due interi k, k', tale che $g = a^k z$ e $h = a^{k'} z'$. Da cui

$$gh = a^k z a^{k'} z' = a^k a^{k'} z z' = a^{k+k'} z' z = a^{k'} a^k z' z = a^{k'} z' a^k z = hg \qquad \square$$

Corollario 3.8.22. *Sia G un gruppo non abeliano. Allora il suo centro non può avere indice primo o 1.*

Dimostrazione. Essendo G non abeliano, allora $Z(G)$ non è tutto G. Inoltre se $Z(G)$ avesse indice primo, allora $G/Z(G)$ sarebbe un gruppo di ordine primo. Quindi sarebbe ciclico e G sarebbe abeliano. Assurdo. □

3.9 Gruppi Abeliani Finiti

In questa sezione vogliamo presentare alcuni risultati riguardo ai gruppi abeliani finiti, ad eccezione della classificazione dei gruppi abeliani finiti, che affronteremo in seguito.

Iniziamo subito con questo risultato

Proposizione 3.9.1. *Sia G abeliano, e siano g, h due elementi di ordine m, n finiti e coprimi. Allora il prodotto gh ha ordine il prodotto degli ordini.*

Dimostrazione. Sia k l'ordine di gh.

Innanzitutto vale l'uguaglianza

$$(gh)^{mn} = g^{mn}h^{nm} = e$$

Quindi k è finito e divide mn.

D'altra parte sappiamo che $(gh)^k$ è l'identità. Quindi anche $(gh)^{mk}$ coincide con l'identità. Inoltre

$$e = (gh)^{mk} = g^{mk}h^{mk} = h^{mk}$$

Quindi n deve dividere mk. Essendo m e n coprimi, n divide k. Analogamente m divide k. Quindi $[m, n] = mn$ divide k.

Ergo k e mn si dividono a vicenda, ed essendo positivi devono essere uguali. □

Le ipotesi di questo risultato sono fondamentali. Infatti presi $\bar{2}$ e $\bar{4}$ in $\mathbb{Z}/6\mathbb{Z}$, allora la loro somma è l'identità, che non ha ordine $3 * 3 = 9$.

D'altra parte se consideriamo il gruppo non abeliano S_3, e i due elementi τ e σ, allora benché abbiamo ordini coprimi il prodotto non ha ordine 6.

Inoltre la proposizione appena dimostrare permette di rispondere a un interessante quesito: Se H è un sottogruppo normale ciclico di un gruppo G, e G/H è ciclico, allora G è ciclico? La risposta è negativa, e il controesempio si individua ponendo $G = S_3$ e $H = \langle\sigma\rangle$.

Il sottogruppo H è ciclico avendo ordine 3, ed è normale avendo indice 2. Inoltre il quoziente ha ordine 2 quindi è ciclico. Tuttavia G non lo è.

La giusta combinazione di ipotesi ce la dà la prossima proposizione.

Proposizione 3.9.2. *Sia G un gruppo abeliano finito e sia H un suo sottogruppo. Se G e G/H hanno ordine coprimo e H e G/H sono ciclici, allora anche G lo è.*

Dimostrazione. Poniamo $H = \langle h \rangle$ e $G/H = \langle gH \rangle$. Sia inoltre m l'ordine di h e n l'ordine di gH.

L'ordine di g è diviso da n, quindi in $\langle g \rangle$ esiste un elemento g' di ordine n. Essendo che g' e h hanno ordini n e m coprimi, allora per la proposizione precedente $g'h$ ha ordine mn. Infine questo è anche l'ordine di G. Infatti $|G| = |H||G/H|$. □

La prima proposizione ci suggerisce che nei gruppi abeliani finiti gli ordini si comportano in maniera abbastanza regolare. In effetti la prossima proposizione ci dice il funzionamento nel loro complesso.

Proposizione 3.9.3. *Sia G un gruppo abeliano finito e sia l'insieme finito*

$$\mathcal{O} = \{ \operatorname{ord}(x) \mid x \in G \}$$

Allora valgono le seguenti affermazioni.

1. *Se n appartiene a $\mathcal{O}$, allora vi appartiene ogni suo divisore;*
2. *Se m, n appartengono a $\mathcal{O}$, allora vi appartiene anche il loro minimo comune multiplo;*
3. *Posto M il massimo di $\mathcal{O}$, allora M è anche il minimo comune multiplo degli elementi di $\mathcal{O}$.*

Dimostrazione. (1.) Sia h in G di ordine n. Poniamo inoltre $H = \langle h \rangle$. Essendo H ciclico di ordine n, in esso troviamo un elemento di ordine d per ogni divisore d di n.

(2.) Se m o n sono uguali a 1, allora l'affermazione è banale. Se in generale sono coprimi, allora la soluzione ce la dà la proposizione ad inizio sezione.

Altrimenti siano

$$m = p_1^{e_1} \dots p_k^{e_k}$$
$$n = p_1^{f_1} \dots p_k^{f_k}$$

con $e_i, f_i \geq 0$. Poniamo adesso a_i, b_i definiti come

$$a_i = \begin{cases} e_i & \text{se } e_i \geq f_i \\ 0 & \text{altrimenti} \end{cases}$$

$$b_i = \begin{cases} f_i & \text{se } f_i > e_i \\ 0 & \text{altrimenti} \end{cases}$$

Siano quindi

$$a = p_1^{a_1} \dots p_k^{a_k}$$
$$b = p_1^{b_1} \dots p_k^{b_k}$$

Per costruzione a e b dividono m e n rispettivamente. Quindi appartengono entrambi a $\mathcal{O}$. Infine essi sono coprimi, quindi il loro prodotto appartiene a $\mathcal{O}$. Infine ab coincide proprio con $[m, n]$, che quindi appartiene a $\mathcal{O}$.

(3.) Sia M il massimo di $\mathcal{O}$. Esso appartiene a $\mathcal{O}$, quindi è minore o uguale del minimo comune multiplo degli elementi di $\mathcal{O}$.

D'altra parte sia m in $\mathcal{O}$. Allora $[m, M]$, per il punto 2, appartiene a $\mathcal{O}$. Quindi per massimalità di M

$$m \leq [m, M] \leq M \leq [m, M] \;\Rightarrow\; [m, M] = M \;\Rightarrow\; m \mid M$$

Valendo questo per ogni m in $\mathcal{O}$, otteniamo che M è diviso dal minimo comune multiplo degli elementi di M. Quindi è maggiore o uguale a esso.

In conclusione M coincide col minimo comune multiplo degli elementi di $\mathcal{O}$. □

Chiudiamo questa sezione con questo teorema:

Teorema 3.9.4. *Sia $G = (\mathbb{Z}/p\mathbb{Z})^k$ con p primo e k intero positivo. Allora il numero di sottogruppi di G di ordine p^h è pari a*

$$\prod_{i=0}^{h-1} \frac{p^k - p^i}{p^h - p^i}$$

Dimostrazione. Indichiamo con $\mathbb{F}_p$ l'insieme $\mathbb{Z}/p\mathbb{Z}$, dotato però delle operazioni di campo invece che semplicemente quella di gruppo. Allora l'insieme G, visto come $\mathbb{F}_p^k$, possiede anche la struttura di spazio vettoriale su $\mathbb{F}_p$. Esso ha dimensione k.

L'osservazione fondamentale è la seguente: i sottospazi di $\mathbb{F}_p^k$ coincidono con i sottogruppi di $(\mathbb{Z}/p\mathbb{Z})^k$.

Infatti l'operazione di somma vettoriale su $\mathbb{F}_p^k$ è definita componente per componente, esattamente come quella di $\mathbb{Z}/p\mathbb{Z}$. Quindi un sottoinsieme di G è chiuso per somma vettoriale se e solo se è chiuso per somma di gruppo. Inoltre essendo G finito, la chiusura per somma di gruppo implica la chiusura per inversi.

Tuttavia essere un sottospazio vettoriale richiede anche la chiusura per prodotto scalare. Tuttavia in $\mathbb{Z}/p\mathbb{Z}$ la moltiplicazione non è altro che una somma ripetuta. Quindi preso un sottogruppo H di $(\mathbb{Z}/p\mathbb{Z})^k$, un vettore v in H e uno scalare $\bar{a}$ in $\mathbb{F}_p$, allora

$$\bar{a} \cdot v = \bar{a} \cdot (\bar{v}_1, \ldots, \bar{v}_k) = \underbrace{(\bar{v}_1, \ldots, \bar{v}_k) + \cdots + (\bar{v}_1, \ldots, \bar{v}_k)}_{a \text{ volte}} \in H$$

Quindi un sottospazio vettoriale di $\mathbb{F}_p^k$ è un sottogruppo di $(\mathbb{Z}/p\mathbb{Z})^k$ e viceversa. Possiamo quindi contare i sottospazi vettorali di $\mathbb{F}_p^k$ di cardinalità p^h.

Dato ora un sottospazio di cardinalità p^h, supponiamo che esso abbia dimensione t. Allora la cardinalità di H è $|\mathbb{F}_p|^{\dim(H)} = p^t$. Quindi H fa dimensione h.

Ci siamo quindi ricondotti a contare i sottospazi di $\mathbb{F}_p^k$ di dimensione h. Per farlo consideriamo la seguente mappa suggettiva

$$\begin{aligned} \Phi\colon \{\, (v_1, \ldots, v_h) \mid \text{ lin. indip. } \} &\to \left\{ H \text{ sottosp. di } \mathbb{F}_p^k \right\} \\ (v_1, \ldots, v_h) &\mapsto \operatorname{Span}(v_1, \ldots, v_h) \end{aligned}$$

Contiamo innanzitutto la cardinalità del dominio.

Sia $B = (v_1, \ldots, v_h)$ una h-upla di vettori linearmente indipendenti. Abbiamo $p^k - 1$ scelte per il primo vettore, cioè tutti i vettori tranne quello nullo. Abbiamo $p^k - p$ scelte per v_2, cioè tutti i vettori tolti quelli nella retta generata da v_2, e $p^k - p^2$ scelte per v_3, cioè tutti tranne quelli nel piano generato da (v_1, v_2) etc.

In conclusione abbiamo un numero di h-uple di vettori indipendenti pari a

$$\prod_{i=0}^{h-1} p^k - p^i$$

Sia adesso un sottospazio H di dimensione h e troviamo il numero delle sue basi. Dobbiamo contare il numero di h-uple di vettori linearmente indipendenti, costituite ora da vettori di H. Seguendo il ragionamento precedente otteniamo

$$\prod_{i=0}^{h-1} p^h - p^i$$

Quindi per ogni H nel codominio, esso ha preimmagine di cardinalità pari al numero trovato sopra.

In conclusione il codominio ha cardinalità pari a

$$\prod_{i=0}^{h-1} \frac{p^k - p^i}{p^h - p^i}$$

□

Osserviamo che abbiamo trovato la cardinalità del seguente gruppo

$$|GL(n, \mathbb{F}_p)| = \prod_{i=0}^{n-1} p^n - p^i$$

3.10 Il Gruppo $\mathbb{Z}/n\mathbb{Z}^*$

Questa sezione è dedicata seguente domanda: quando è che $\mathbb{Z}/n\mathbb{Z}^*$ ciclico? Ci arriveremo per passi. Iniziamo dalla seguente:

Teorema 3.10.1. *Preso un primo p, allora $\mathbb{Z}/p\mathbb{Z}^*$ è ciclico.*

Dimostrazione. Sia $G = (\mathbb{Z}/p\mathbb{Z})^*$ e sia M li massimo degli elementi di G. Allora M è anche il minimo comune multiplo degli elementi di G. Quindi per ogni g in G, il suo ordine divide M.

Ergo $x^M - 1$ ha $p - 1$ radici in $\mathbb{F}_p$. Essendo di grado M, ed essendo $\mathbb{F}_p$ un campo, allora $M \geq p - 1$.

D'altra parte esiste un elemento g in G tale che $\text{ord}(g) = M$. Essendo che l'ordine di g divide $p - 1$, allora $M \leq p - 1$.

Ergo $M = p-1$ ed esiste un elemento di ordine $p-1$. Quindi G è ciclico. □

Corollario 3.10.2 (Criterio di Eulero)**.** *Sia p primo dispari e a intero coprimo con p. Allora*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Dimostrazione. Supponiamo che a abbia simbolo di Legendre pari a 1. Allora esso è un quadrato modulo p. Cioè esiste un intero k tale che k^2 è congruo a a modulo p.

Quindi otteniamo, grazie al piccolo teorema di Fermat,

$$a^{\frac{p-1}{2}} \equiv k^{p-1} \equiv 1 \pmod{p}$$

Se invece $a^{\frac{p-1}{2}}$ è congruo a 1 modulo p, sia $\bar{g}$ un generatore di $(\mathbb{Z}/p\mathbb{Z})^*$.

Poniamo inoltre $\bar{a} = \bar{g}^i$. Allora $\bar{g}^{\frac{i(p-1)}{2}} = \bar{1}$ e l'ordine di $\bar{g}$, pari a $p-1$, divide $i(p-1)/2$.

Ergo i deve esser pari e possiamo porre $\bar{k} = \bar{g}^{i/2}$. Per costruzione è una radice di $\bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$. □

Corollario 3.10.3. *Sia p primo dispari. Allora*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Dimostrazione. Grazie al criterio di Eulerio sappiamo che

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

Tuttavia entrambi i membri della congruenza valgono ± 1. Essendo p diverso da 2, questo implica che la congruenza può essere sostituita con un'uguaglianza. □

Procediamo ora col prossimo step: il gruppo $\mathbb{Z}/p^k\mathbb{Z}^*$ con p dispari e k intero. Prima però dobbiamo procedere con questo lemma:

Lemma 3.10.4. *Sia p primo dispari e k intero maggiore di 1. Allora*

$$(1+p)^{p^{k-2}} \not\equiv 1 \pmod{p^k}$$

Dimostrazione. Dimostriamo per induzione su k il seguente enunciato, più forte:

$$(1+p)^{p^{k-2}} = 1 + hp^{k-1} \quad (h,p) = 1$$

Questo implica il nostro risultato. Infatti posto x della forma sopra, se per assurdo fosse congruo a 1 modulo p^k, allora p^k dovrebbe dividere $x-1 = hp^{k-1}$.

Essendo h coprimo con p, lo è anche con p^k. Quindi quest'ultimo dovrebbe dividere p^{k-1}. Assurdo.

Se $k = 2$, allora $1 + p$ è banalmente della forma richiesta.

Supposto vero per $k \geq 2$, dimostriamolo per $k+1$. Allora tramite il binomio di Newton otteniamo

$$\begin{aligned}(1+p)^{p^{k-1}} &= \left((1+p)^{p^{k-2}}\right)^p \\ &= (1+hp^{k-1})^p \\ &= 1 + \binom{p}{1} hp^{k-1} + \sum_{i=2}^{p-1} \binom{p}{i} h^i p^{i(k-1)} + \binom{p}{p} h^p p^{p(k-1)} \\ &= 1 + h\,p^k + pD\,p^k + h^p p^{p(k-1)} \qquad D \in \mathbb{Z}\end{aligned}$$

Notiamo infine che $p(k-1)$ è maggiore o uguale a $k+1$ se e solo se

$$p \geq \frac{k+1}{k-1} = f(k)$$

La funzione $f(k)$ è decrescente con valore massimo $f(2) = 3$. Quindi la condizione è verificata essendo p dispari (è proprio qui che $p = 2$ non funziona).

Possiamo quindi porre

$$\begin{aligned}(1+p)^{p^{k-1}} &= 1 + h\,p^k + pD\,p^k + pT\,p^k \qquad D, T \in \mathbb{Z} \\ &= 1 + h\,p^k + pR\,p^k \qquad R \in \mathbb{Z} \\ &= 1 + (h + pR)\,p^k \qquad R \in \mathbb{Z}\end{aligned}$$

Questa è nella forma richiesta, in quanto $(h + pR, p) = (h, p) = 1$. □

Grazie a questo lemma possiamo dimostrare il caso $n = p^k$.

Teorema 3.10.5. *Sia $G = \mathbb{Z}/p^k\mathbb{Z}^*$ con p primo dispari e k intero positivo. Allora esso è ciclico.*

Dimostrazione. Sia la mappa

$$\begin{aligned}\pi \colon \mathbb{Z}/p^k\mathbb{Z}^* &\to \mathbb{Z}/p\mathbb{Z}^* \\ [a]_{p^k} &\mapsto [a]_p\end{aligned}$$

È ben definita. Infatti se x è coprimo con p^k, a maggior ragione lo deve essere con p. Inoltre se x, y sono congrui modulo p^k, allora lo sono modulo p.

È un banale omomorfismo.

È suggettiva, in quanto $[i]_p$ è immagine di $[i]_{p^k}$.

Quindi per il teorema di omomorfismo l'immagine, pari a $\mathbb{Z}/p\mathbb{Z}^*$, è isomorfa a G/H con H il nucleo di π.

Quello che dobbiamo verificare è che H sia ciclico. Innanzitutto ha cardinalità pari a $|G|/|\mathrm{Im}(\pi)| = p^{k-1}$. Inoltre sia $h = \overline{p+1}$ in G. Affermo che esso genera H.

Da una parte $[1+p]_p = [1]_p$, quindi h appartiene al nucleo di π.

Verifichiamo ora che il suo ordine sia p^{k-1}. Certamente, essendo elemento di H, ha ordine che divide p^{k-1}.

D'altra parte sappiamo, per il lemma precedente, che $(1+p)^{p^{k-2}}$ non è congruo a 1 modulo p^k. Quindi l'ordine di h non deve dividere p^{k-2}.

Mettendo insieme le condizioni otteniamo che l'ordine di h è esattamente p^{k-1}.

Riassumendo abbiamo H ciclico e G/H isomorfo a $\mathbb{Z}/p\mathbb{Z}^*$, che è ciclico per il teorema precedente. Inoltre G/H ha ordine $\varphi(p^k)/p^{k-1} = p-1$, coprimo con l'ordine di H.

Quindi, per la proposizione 3.9.2, G è ciclico. □

Chiudiamo ora analizzando l'ultimo caso che ci interessa: $\mathbb{Z}/2^h\mathbb{Z}$.

Teorema 3.10.6. *Il gruppo $G = \mathbb{Z}/2^h\mathbb{Z}^*$ è ciclico se e solo se h è uguale a 1 o 2 .*

Dimostrazione. Se h è uguale a 1 o 2, allora G è il gruppo banale, quindi è ciclico.

Se h è maggiore o uguale a 3, allora sappiamo che la congruenza

$$x^2 \equiv 1 \pmod{2^h}$$

ammette quattro soluzioni distinte modulo p^h. Ergo G ammette 3 elementi distinti di ordine 2. Quindi non può essere ciclico. □

Ora abbiamo tutti gli strumenti per affrontare la ciclicità di $\mathbb{Z}/n\mathbb{Z}^*$.

Teorema 3.10.7. *Il gruppo $\mathbb{Z}/n\mathbb{Z}^*$ è ciclico se e solo se $n = 2$, 4, p^k, $2p^k$ con p primo dispari e k intero positivo.*

Dimostrazione. Sia $G = \mathbb{Z}/n\mathbb{Z}^*$.

Se $n = 1, 2$, il gruppo è banale quindi ciclico.

Se $n = 4$, G ha ordine 2 quindi è ciclico.

Se $n = p^k$ come da ipotesi, allora abbiamo dimostrato che G è ciclico.

Se $n = 2p^k$ come da ipotesi, allora possiamo scomporre il gruppo come

$$G \simeq \mathbb{Z}/2\mathbb{Z}^* \times \mathbb{Z}/p^k\mathbb{Z}^* \simeq \mathbb{Z}/p^k\mathbb{Z}^*$$

Quindi G è ciclico.

Per quanto riguarda il viceversa, dimostreremo per passi che se G è ciclico, allora n deve essere come sopra.

Se n non è 1, scomponiamolo in fattori primi

$$n = 2^h p_1^{e_1} \dots p_k^{e_k} \qquad p_i \text{ dispari}, \ e_i \geq 0$$

Allora G si scompone come

$$\begin{aligned} G = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* &\simeq \left(\frac{\mathbb{Z}}{2^h\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right)^* \times \dots \times \left(\frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}\right)^* \\ &= \left(\frac{\mathbb{Z}}{2^h\mathbb{Z}}\right)^* \times \frac{\mathbb{Z}}{p_1^{e_1-1}(p_1-1)\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_k^{e_k-1}(p_k-1)\mathbb{Z}} \end{aligned}$$

Notiamo subito che se h è maggiore di 2, allora G non è ciclico. Infatti in questo caso G conterrebbe un sottogruppo isomorfo a $(\mathbb{Z}/2^h\mathbb{Z})^*$, che sappiamo non essere ciclico.

Quindi G ammetterebbe un sottogruppo non ciclico, ergo neanche lui potrebbe esserlo.

Inoltre k non può essere maggiore di 1. Infatti se lo fosse, allora G conterrebbe un sottogruppo isomorfo al prodotto diretto di $\mathbb{Z}/\varphi(p_1^{e_1})\mathbb{Z}$ e $\mathbb{Z}/\varphi(p_2^{e_2})\mathbb{Z}$.

Questo prodotto però non dà luogo ad un gruppo ciclico, in quanto $\varphi(p_1^{e_1})$ e $\varphi(p_2^{e_2})$ hanno in comune in fattore due. Come prima questo implicherebbe la non ciclicità di G.

Ricapitolando abbiamo dimostrato che n è della forma $2^h p^e$ con h minore di 3 e p primo dispari. Per concludere dobbiamo dimostrare se $e \geq 1$, allora $h \leq 1$.

Supponiamo che questo non sia il caso. Sapendo che $\mathbb{Z}/4\mathbb{Z}^*$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, otteniamo la scomposizione

$$G \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{e-1}(p-1)\mathbb{Z}}$$

Però questa scomposizione non ci dà un gruppo ciclico, in quanto l'ordine dei due fattori ha un fattore 2 in comune.

Quindi se G è ciclico n è della forma $2^h p^e$, con $h = 0, 1, 2$ e $e = 0$, o $h = 0, 1$ e e qualunque. Cioè n è della forma voluta. □

In verità non abbiamo finito di descrivere $\mathbb{Z}/n\mathbb{Z}^*$. Infatti dimostreremo (quando avremo i teoremi più adatti), che benché $(\mathbb{Z}/2^h)^*$ non sia ciclico, si può scrivere comunque come prodotto dei seguenti gruppi ciclici:

$$\mathbb{Z}/2^h\mathbb{Z}^* \simeq \begin{cases} \{e\} & h = 0, 1 \\ \mathbb{Z}/2\mathbb{Z} & h = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{h-2}\mathbb{Z} & h \geq 3 \end{cases}$$

Quindi per ogni naturale n, il gruppo $\mathbb{Z}/n\mathbb{Z}^*$ si scrive come prodotto di gruppi ciclici. In verità questo è un fatto estremamente più generale. Valido, come dimostreremo, per i gruppi abeliani finiti, e che si applica in verità anche a quelli finitamente generati.

3.11 Presentazione di Gruppi

In questa sezione introduciamo un argomento fondamentale nella teoria dei gruppi: quella di presentazione. Se un gruppo è descritto tramite presentazione, non è facilissimo studiarne le caratteristiche. Però per tanti gruppi non esiste metodo migliore.

Iniziamo con la definizione di sottogruppo generato, anche da un insieme arbitrario di elementi.

Proposizione 3.11.1. *Sia un gruppo G e sia S un sottoinsieme. Allora il seguente sottoinsieme*

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H$$

è effettivamente un sottogruppo, detto sottogruppo generato da S.

Dimostrazione. Certamente l'identità appartiene ad ogni sottogruppo di G, quindi appartiene a $\langle S \rangle$.

Siano h e g in $\langle S \rangle$. Allora h e g appartengono ad ogni sottogruppo di G che contiene S. Quindi gh appartengono ad ognuno di questi H, quindi appartengono a $\langle S \rangle$.

Infine preso h in $\langle S \rangle$, allora h appartiene ad ogni sottogruppo di G che contiene S. Quindi h^{-1} appartiene ad ognuno di questi H, quindi appartiene a $\langle S \rangle$. □

Corollario 3.11.2. *Dato un sottogruppo S di G, allora $\langle S \rangle$ è il più piccolo sottogruppo di G che contiene S.*

Dimostrazione. Abbiamo dimostrato che $\langle S \rangle$ è un sottogruppo di G.

Inoltre, preso H sottogruppo di G che contiene S, allora $\langle S \rangle$ è contenuto in H per definizione. □

La definizione di sottogruppo generato è molto astratta. Una definizione leggermente più costruttiva là da il prossimo teorema.

Teorema 3.11.3. *Sia G gruppo e S sottogruppo. Allora*

$$\langle S \rangle = \{e\} \cup \left\{ g_1^{k_1} \dots g_d^{k_d} \;\middle|\; d \in \mathbb{N}_+ \; g_i \in S \; k_i \in \mathbb{Z} \right\}$$

(dove l'unione forzata di e è stata fatta per includere il caso limite in cui S sia vuoto).

Dimostrazione. Sia Z il sottoinisieme di G a destra dell'uguaglianza. Dimostriamo che è un sottogruppo, contenuto in ogni sottogruppo di G che contiene S. Per quello detto prima, questo implica che $Z = \langle S \rangle$

Per costruzione e è incluso in Z.

Inoltre se g e h sono contenuti in Z, allora possiamo porre

$$g = g_1^{k_1} \dots g_d^{k_d}$$
$$h = h_1^{k'_1} \dots h_d^{k'_d}$$

Quindi

$$gh = g_1^{k_1} \dots g_d^{k_d} h_1^{k'_1} \dots h_d^{k'_d}$$

appartiene a Z.

Infine se g è della forma

$$g = g_1^{k_1} \dots g_d^{k_d}$$

allora l'inverso appartiene a Z. avendo forma

$$g^{-1} = g_d^{-k_d} \dots g_1^{-k_1}$$

Concludiamo dicendo che se H è un sottogruppo di G che contiene S, allora egli contiene anche Z. Infatti gli elementi Z sono costruiti tramite inversi e prodotti degli elementi di S, e quindi appartengono a H. □

Notiamo che la definizione di sottogruppo generato necessita che i generatori vivano in un gruppo ambiente G. È possibile creare un gruppo usando però un insieme di simboli, per cui quindi non sono definite delle operazioni?

La presentazione di gruppi vuole rispondere a questa domanda. Però prima bisogna introdurre il concetto fondamentale: quello di gruppo libero.

Definizione 3.11.4. Sia $X = \{ x_i \mid i \in I \}$ un insieme. Poniamo l'insieme formale di simboli $X^{-1} = \left\{ x_i^{-1} \;\middle|\; i \in I \right\}$. Allora "l'alfabeto" corrispondente ad X è l'insieme $A = X \cup X^{-1}$, ed una "parola" è un elemento di

$$L = \bigcup_{n \geq 0} A^n$$

Una parola si dice ridotta se non presenta x_i,x_i^{-1} consecutivi.

Notiamo che se G è un gruppo e X è un suo sottoinsieme, allora abbiamo una identificazione, non necessariamente iniettiva, di L in G:

$$\Phi \colon L \to G$$
$$\emptyset \mapsto e$$
$$(x_1, \ldots, x_k) \mapsto x_1 \cdot \cdots \cdot x_k$$

Definizione 3.11.5 (Grupppo Libero)**.** Sia $X = \{ x_i \mid i \in I \}$ un insieme. Un gruppo G è libero su X se

1. G contiene X, o almeno una sua copia, ed è generato da essa
2. Date due parole ridotte in L, esse vengono mandate, tramite Φ, in elementi diversi di G.

Per esempio $\mathbb{Z}$ è un gruppo libero su $\{1\}$, in quanto una stringa ridotta è della forma

$$\underbrace{(1, \ldots, 1)}_{k \text{ volte}} \underset{\Phi}{\mapsto} k$$

Quindi Φ è iniettiva.

D'altra parte $\mathbb{Z}/2\mathbb{Z}$ non è un gruppo libero su $\bar{1}$, in quanto le stringhe

$$(\bar{1}, \bar{1})$$

e

$$(\bar{1}, \bar{1}, \bar{1}, \bar{1})$$

sono entrambe ridotte, ma corrispondono entrambe all'identità.

Per ora abbiamo solo definito il gruppo libero, niente ci dice che esista o che sia unico (a meno di isomorfismo ovviamente). Per trattare queste due questioni introduciamo il concetto di relazioni di equivalenza generata.

Definizione 3.11.6. Sia S un insieme e sia un sottoinsieme R di $S \times S$. Definiamo la relazione di equivalenza generata da R come la più piccola relazione di equivalenza su S che contiene R. Come al solito, essa è pari a

$$\bigcap_{\substack{T \subseteq S \times S \\ R \subseteq T \\ T \text{ Rel. Eq.}}} T$$

Proposizione 3.11.7. *Sia S un insieme e sia un sottoinsieme R di $S \times S$, contenente la diagonale Δ_S e simmetrico rispetto ad essa. Presi x, y in R, diciamo che $x \sim_R y$ se $(x, y) \in R$. Allora posta $\sim$ la relazione di equivalenza generata da R, vale che due elementi v, w in S sono equivalenti secondo $\sim$ se e solo se esiste una successione finita in S*

$$v = s_0, \ldots, s_k = w$$

tale che

$$v \sim_R s_1 \sim_R \cdots \sim_R s_{k-1} \sim_R w \tag{3.2}$$

Dimostrazione. Sia la relazione $\Gamma \subseteq S \times S$ definita nel seguente modo: $v \sim w$ se e solo se esiste una successione finita in S tale che valga (3.2). Vogliamo dimostrare che Γ è la più piccola relazione di equivalenza che contiene R.

Certamente per ogni (x, y) tale che $x \sim_R y$, allora la successione $s_0 = x, s_1 = y$ verifica (3.2). Quindi $x \sim y$.

Quindi Γ contiene tutto R.

Inoltre verifichiamo che Γ sia una relazione di equivalenza.

Preso x in S, allora $x \sim_R x$, quindi $x \sim x$.

Presi $x \sim y$, allora esiste una successione $s_0, \ldots, s_k$ tale che

$$x = s_0 \sim_R \cdots \sim_R s_k = y$$

Essendo R simmetrico rispetto ad Δ_S, se $s_i \sim_R s_{i+1}$ anche $s_{i+1} \sim_R s_i$. Quindi

$$y = s_k \sim_R \cdots \sim_R s_0 = x,$$

da cui $y \sim x$.

Infine se $x \sim y$ e $y \sim z$, allora possiamo scrivere

$$x = s_0 \sim_R \cdots \sim_R s_k = y$$
$$y = r_0 \sim_R \cdots \sim_R r_{k'} = z$$

Quindi $s_0, \ldots, s_k, r_0 \ldots r_{k'}$ è una successione che "connette" x e z. Ergo $x \sim z$.

Quindi Γ è una relazione di equivalenza contiene R. Verifichiamo che sia la più piccola.

Sia T una relazione di equivalenza su S che contiene R. Verifichiamo che contenga Γ.

Presi $u \sim v$, allora esiste una successione in S che soddisfa (3.2). Per ogni i, s_i e s_{i+1} sono in relazione secondo R, quindi lo sono anche secondo T, in quanto il primo è contenuto nel secondo. Quindi per transitività di T, $u \sim_T v$. □

A questo punto possiamo dimostrare l'esistenza (daremo la traccia della dimostrazione) e l'unicità dei gruppi liberi.

Teorema 3.11.8. *Sia X un insieme. Esiste un gruppo libero su X.*

Dimostrazione. Sia il linguaggio L costruito su X definito precedentemente. Allora sia la relazione $\sim$ su L definita come:

$$\begin{aligned} s \sim s \quad & \forall s \in L \\ s \sim r \ \Rightarrow \ r \sim s \quad & \forall r, s \in L \\ (x, x^{-1}) &\sim \emptyset \\ (x_1, \dots x_k, x_k^{-1}, \dots x_h) &\sim (x_1, \dots, x_{k-1}, x_{k+1} \dots x_h) \end{aligned}$$

grazie alla preposizione precedente sappiamo che $\sim$ genera una relazione di equivalenza su L.

La relazione di equivalenza non fa altro di ridurre le stringhe. Ora dobbiamo imporre l'operazione. Per ora definiamola su L:

$$\begin{aligned} \emptyset * s = s = s * \emptyset \quad & \forall s \in L \\ (x_1, \dots, x_k) * (y_1, \dots, y_{k'}) &= (x_1, \dots, x_k, y_1, \dots, y_{k'}) \end{aligned}$$

Si osserva che $*$ passa al quoziente $P = L/\sim$, e che la coppia $G = (P, *)$ è un gruppo. L'elemento inverso è $[\emptyset]$, mentre l'inverso di $[(x_1, \dots, x_k])$ è

$$[(x_1, \dots, x_k)]^{-1} = [(x_k^{-1}, \dots, x_1^{-1})]$$

Infine G è un gruppo libero su X. Infatti X si immerge in P tramite

$$\begin{aligned} \Phi \colon X \to L \to P \\ x \mapsto (x) \mapsto [(x)] \end{aligned}$$

Inoltre preso un elemento g in G, esso si scrive come

$$[(x_1, \dots, x_k)] = [(x_1)] * \dots * [(x_k)] \quad x_i \in X \cup X^{-1}$$

Quindi G è generato da $\Phi(X)$.

Infine siano due stringhe u, v di $\Phi(L)$ ridotte:

$$u = ([(x_1)], \dots, [(x_k)])$$
$$v = ([(y_1)], \dots, [(y_{k'})])$$

che si immergono in P come

$$u' = [(x_1)] * \cdots * [(x_k)] = [(x_1, \dots, x_k)] \quad x_i \in X \cup X^{-1}$$
$$v' = [(y_1)] * \cdots * [(y_{k'})] = [(y_1, \dots, x_{k'})] \quad y_i \in X \cup X^{-1}$$

Supponiamo ora che u', v' siano uguali, vogliamo dimostrare che questo implica l'uguaglianza fra le stringhe u e v.

Se $u' = v'$, allora $(x_1, \dots, x_k)$ è equivalente a $(y_1, \dots, y_{k'})$. Quest'ultime però sono parole ridotte in L, in quanto u, v sono parole ridotte in $\Phi(L)$. Quindi devono essere uguali, da cui lo sono anche u e v. □

Dato un insieme X, abbiamo costruito il gruppo libero su X. Distogliendo momentaneamente l'attenzione sull'intero impianto teorico della dimostrazione, quello che abbiamo fatto è stato considerare G come tutti i possibili prodotti di elementi di $X \cup X^{-1}$, e abbiamo imposto come unica "regola" di composizione quella più banale: che xx^{-1} sia l'identità. Come vedremo i gruppi presentati sono gruppi costruiti con lo stesso ragionamento, imponendo però regole aggiuntive sulla composizione dei generatori.

Notiamo ora una cosa. Quando abbiamo calcolato gi omomorfismi da $\mathbb{Z}$ in un gruppo G, abbiamo detto che una volta fissato dove va il generatore 1, allora abbiamo identificato un intero omomorfismo da $\mathbb{Z}$. Questo non era vero per esempio con gli omomorfismi da $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$. Infatti l'immagine del generatore $\bar{1}$ doveva rispettare delle condizioni sull'ordine.

La differenza risiede nel fatto che $\mathbb{Z}$ è un gruppo libero su $\{1\}$, mentre $\mathbb{Z}/n\mathbb{Z}$ non è un gruppo libero su $\{\bar{1}\}$. Il prossimo teorema dice per l'appunto che se siamo in presenza di gruppi liberi, allora gli omomorfismi da quel gruppo sono facilmente descritti.

Teorema 3.11.9. *Sia G un gruppo libero su X. Allora preso un gruppo H, gli omomorfismi da G in H sono in bigezione con le mappe da X in H.*

Dimostrazione. Sia la seguente mappa

$$H^X \to H^L$$
$$\varphi \mapsto \tilde{\varphi}$$

dove abbiamo indicato con $\tilde{\varphi}$ l'estensione di φ tale che

$$\tilde{\varphi}(\emptyset) = e_H$$
$$\tilde{\varphi}((x_1^{\pm 1}, \dots, x_k^{\pm 1})) = \varphi(x_1)^{\pm 1} \dots \varphi(x_k)^{\pm 1} \quad x_i \in X$$

Vogliamo adesso dire che è possibile definire la funzione $\tilde{\varphi}$ non sull'alfabeto L, ma su G.

Innanzitutto verifichiamo che se prendiamo una stringa s, allora possiamo innanzitutto ridurla, e poi che questa operazione non modifica la sua immagine tramite $\tilde{\varphi}$.

Sia quindi una stringa $(x_1, \dots, x_k)$ in L e procediamo per induzione su k.

Per $k = 1$, allora la stringa è banalmente ridotta.

Posto vero per k, sia $s = (x_1, \dots, x_k, x_{k+1})$. Allora per induzione possiamo affermare che la sottostringa $s' = (x_1, \dots, x_k)$ ammette una stringa equivalente $r' = (y_1, \dots, y_h)$ ridotta.

Inoltre (s', x_{k+1}) è equivalente a $(r', x_{k+1}) = (y_1, \dots, y_h, x_{k+1})$.

Se x_{k+1} non è y_h^{-1}, allora anche la stringa (s', x_{k+1}) è ridotta. Altrimenti consideriamo $\emptyset$ se $k = 1$, oppure $(y_1, \dots, y_{h-1})$ altrimenti.

Entrambe sono stirnghe equivalenti e ridotte.

Infine supponiamo che due stringhe $s = (x_1, \dots, x_k)$ e $r = (y_1, \dots, y_k)$ siano equivalenti. Allora esiste una successione finita di stringhe $z_0, \dots, z_m$ tale che

$$s = z_0 \sim' \cdots \sim' z_m = r$$

dove z_{i+1} è ottenuta da z_i elidendo una porzione della forma (x, x^{-1}).

Possiamo quindi considerare il caso in cui s e r siano equivalenti secondo $\sim'$. Quindi possiamo porre che $r = (r', r'')$ e $s = (r', x_i, x_i^{-1}, r'')$, con r', r'' due stringhe, eventualmente vuote. Allora (è evidente, per come abbiamo definito $\tilde{\varphi}$, che essa rispetta la concatenazione)

$$\tilde{\varphi}(s) = \tilde{\varphi}(r')\varphi(x_i)\varphi(x_i)^{-1}\tilde{\varphi}(r'') = \tilde{\varphi}(r')\tilde{\varphi}(r'') = \tilde{\varphi}(r)$$

Abbiamo verificato che una qualsiasi stringa è possibile ridurla senza alterare l'immagine secondo $\tilde{\varphi}$. Usiamo questo fatto per definire un omomorfismo da G in H.

Definiamo quindi l'estensione $\tilde{\varphi}_G$, definita su G, nel modo naturale (ricordiamo che G è generato da X).

$$\tilde{\varphi}_G(x_1^{\pm 1} * \cdots * x_k^{\pm 1}) = \tilde{\varphi}((x_1^{\pm 1}, \dots, x_k^{\pm 1})) = \varphi(x_1)^{\pm 1} \dots \varphi(x_k)^{\pm 1} \quad x_i \in X$$

Una volta dimostrata la buona definizione di $\tilde{\varphi}_G$, allora è evidente che esso è un omomorfismo da G.

Per farlo è fondamentale che G sia libero su X. Infatti preso g in G, allora supponiamo che g si scriva come

$$g = x_1^{\pm 1} * \cdots * x_k^{\pm 1} = y_1^{\pm 1} * \cdots * y_{k'}^{\pm 1} \quad x_i, y_i \in X$$

Innanzitutto a meno di sfruttare l'osservazione precedente, possiamo supporre che le stringhe (x_i) e (y_i) siano ridotte. Ma essendo che G è libero su X, questo implica che le due stringhe sono uguali. Quindi la loro immagine tramite $\tilde{\varphi}$ coincide e $\tilde{\varphi}_G$ è ben definita.

In conclusione abbiamo la nostra mappa ben definita

$$\begin{aligned} H^X &\to \mathrm{Hom}(G, H) \\ \varphi &\mapsto \tilde{\varphi}_G \end{aligned}$$

che è una bigezione, avendo come inversa

$$\begin{aligned} \mathrm{Hom}(G, H) &\to H^X \\ \psi &\mapsto \psi|_X \end{aligned}$$

□

Grazie alla proposizione precedente possiamo dimostrare che esiste, a meno di isomorfismo, un unico gruppo libero su X.

Teorema 3.11.10. *Sia X un insieme e siano G_1, G_2 due gruppi liberi su X. Allora sono isomorfi.*

Dimostrazione. Siano i_1 e i_2 le immersioni di X in G_1 e G_2. Allora possiamo considerare la mappa

$$\begin{aligned} j_1 \colon i_1(X) &\to G_2 \\ i_1(x) &\mapsto i_2(x) \end{aligned}$$

Analogamente possiamo considerare j_2 da $i_2(X)$ a G_1. Essendo G_1 e G_2 liberi su X, essi si estendono ad omomorfismi ψ_1 e ψ_2 tra G_1 e G_2.

Infine notiamo che per ogni $x \in X$

$$(\psi_1 \circ \psi_2)(i_2(x)) = \psi_1(i_1(x)) = i_2(x)$$

Quindi $\psi_1 \circ \psi_2$ è l'estensione dell'identità su $i_2(X)$, quindi è l'identità su G_2. Allo stesso modo $\psi_2 \circ \psi_1$ è l'identità su G_1.

Quindi ψ_1 e ψ_2 sono una inversa dell'altra, e G_1 e G_2 sono isomorfi. □

Possiamo quindi parlare del gruppo di X, indicato con $F(X)$. In particolare indicheremo con F_n il gruppo libero su n elementi.

Affrontiamo ora il concetto di gruppo presentato. Il gruppo $\mathbb{Z}/n\mathbb{Z}$ può essere visto come il gruppo generato da un solo elemento, però con una regola di composizione aggiuntiva: $X^n = e$. Saremmo quindi tentati di scrivere qualcosa del tipo

$$\mathbb{Z}/n\mathbb{Z} \simeq \langle x \,|\, x^n = e \rangle$$

La teoria dei gruppi presentati vuole appunto formalizzare questa idea. Per procedere però dobbiamo introdurre il semplice concetto di sottogruppo normalgenerato.

Definizione 3.11.11. Sia un gruppo G e sia un sottoinsieme S. Indichiamo con $\langle S \rangle_N$ il più piccolo sottogruppo normale che contiene S. Come al solito esso coincide con

$$\langle S \rangle_N = \bigcap_{\substack{T \lhd G \\ S \subseteq T}} T$$

Definizione 3.11.12. Sia X un insieme e sia una collezione $W = \{w_i\}_{i \in I}$ di elementi di $F(X)$, dette relazioni. Allora con l'espressione

$$G = \langle X \,|\, W \rangle$$

indichiamo, a meno di isomorfismo, il gruppo

$$G \simeq F(X) / \langle W \rangle_N$$

Il gruppo G è un gruppo presentato, e la coppia $\langle X \,|\, W \rangle$ è una sua presentazione.

La definizione appena data non rende bene l'idea di cosa voglia dire definire un gruppo tramite presentazioni. Il prossimo risultato ne chiarisce meglio il significato.

Teorema 3.11.13. *Sia un gruppo G generato da X. Allora esso è isomorfo ad un gruppo presentato $\langle X \,|\, W \rangle$.*

Dimostrazione. Consideriamo il gruppo libero $F(X)$. Per quello che si è dimostrato la mappa d'immersione $i \colon X \hookrightarrow G$ si estende ad un omomorfismo $\varphi \colon F(X) \to G$. Per il teorema d'omomorfismo esiste un isomorfismo

$$F(X) / \operatorname{Ker}(\varphi) \simeq \operatorname{Im}(\varphi)$$

Tuttavia la mappa $\mathrm{Im}(\varphi)$ è suggettiva, in quanto sia $F(X)$ che G sono generati X. Quindi

$$F(X)/\operatorname{Ker}(\varphi) \simeq G$$

Da cui, prendendo $W = \operatorname{Ker}(\varphi)$, si ottiene che G è isomorfo a $\langle X \,|\, W \rangle$. □

Il gruppo $\langle X \,|\, W \rangle$ è il gruppo ottenuto considerando tutti i possibili prodotti di elementi di $X \cup X^{-1}$, imponendo però delle regole aggiuntive sulla composizione degli elementi, al di fuori di quella banale $xx^{-1} = e$.

Ricordiamo ora che di solito le relazioni vengono scritte in maniera particolare. Per esempio il gruppo

$$\left\langle x, y \,\middle|\, x^2 = e,\ xy = yx \right\rangle$$

è un gruppo generato da due elementi, il primo di ordine 2, e che tra loro commutano. Volendo scrivere il gruppo seguendo la definizione, avremmo dovuto scrivere

$$\left\langle x, y \,\middle|\, x^2,\ x^{-1}y^{-1}xy \right\rangle$$

Per ragioni di chiarezza spesso però si opta a scrivere le relazioni nella prima maniera, più leggibili.

Con questo nuovo strumento possiamo effettivamente dire che il gruppo $\mathbb{Z}/n\mathbb{Z}$ è isomorfo al gruppo presentato $\langle x \,|\, x^n = e \rangle$. Infatti per definizione $\mathbb{Z}/n\mathbb{Z}$ è il quoziente del gruppo libero $Z = F_1$ sul sottogruppo $n\mathbb{Z}$. Il sottogruppo $n\mathbb{Z}$ infine è il sottogruppo normale generato da $\{n\}$, che corrisponde esattamente all'ennesima potenza del generatore.

Un altro esempio è dato dal gruppo $G = \mathbb{Z} \times \mathbb{Z}$. Intuitivamente che G è generato da due elementi, di ordine infinito, che però commutano. Non soprenderà quindi che

$$\mathbb{Z} \times \mathbb{Z} \simeq \langle x, y \,|\, xy = yx \rangle$$

In effetti, ponendo

$$G = F_2/\left\langle y^{-1}x^{-1}yx \right\rangle_N$$

allora le mappe che realizzano l'isomorfismo sono

$$\begin{aligned} \Phi \colon \mathbb{Z} \times \mathbb{Z} &\to G \\ (a, b) &\mapsto [x]^a [y]^b \end{aligned}$$

$$\Psi\colon G \to \mathbb{Z}\times\mathbb{Z}$$
$$[x] \mapsto (1,0)$$
$$[y] \mapsto (0,1)$$

Chiudiamo questa sezione con un criterio, applicabile ad un gruppo presentato, per la determinazione di omomorfismi.

Proposizione 3.11.14. *Sia un gruppo presentato $G \simeq \langle X \,|\, W\rangle$ e sia un secondo gruppo H. Allora l'insieme* $\mathrm{Hom}(G,H)$ *è in bigezione gli omomorfismi da $F(X)$ in H rispettanti le presentazioni, cioè che mandano W nell'identità.*

Dimostrazione. Sia un omomorfismo φ da G in H. Allora sussiste il seguente diagramma commutativo

$$\begin{array}{ccc} F(X) & \xrightarrow{\ f\ } & H \\ {\scriptstyle\pi}\downarrow & \nearrow_{\varphi} & \\ G \simeq F(X)/\langle W\rangle_N & & \end{array}$$

Ed in tal caso f è un omomorfismo da $F(W)$ a H, tale per cui per ogni w in W

$$f(w) = (\varphi\circ\pi)(w) = \varphi([w]) = \varphi(e_G) = e_H$$

Viceversa se f è un omomorfismo da $F(X)$ a H che rispetta le presentazioni, allora W è contenuto nel suo nucleo, così come tutto il suo generato. Inoltre anche il normal-generato ci è contenuto, in quanto il nucleo è un sottogruppo normale.

Quindi $\langle W\rangle_N$ è contenuto nel nucleo di f, che quindi passa al quoziente definendo un omomorfismo da G a H. □

La proposizione appena presentata è la generalizzazione di quello che è stato già fatto, quando abbiamo calcolato gli omomorfismi da $\mathbb{Z}/m\mathbb{Z}$ a $\mathbb{Z}/n\mathbb{Z}$. Infatti $\mathbb{Z}/m\mathbb{Z}$ ha presentazione

$$\mathbb{Z}/m\mathbb{Z} = \langle x \,|\, x^m = e\rangle$$

Quindi per individuare gli omomorfismi in $\mathbb{Z}/n\mathbb{Z}$ devo trovare gli omomorfismi da F_1 in $\mathbb{Z}/n\mathbb{Z}$ che rispettano le presentazioni. Essendo F_1 un gruppo libero, gli omomorfismi da esso in $\mathbb{Z}/n\mathbb{Z}$ sono in bigezioni con le mappe da $\{x\}$ in $\mathbb{Z}/n\mathbb{Z}$. Infine un tale omomorfismo f deve rispettare l'unica presentazione.

Cioè $f(x^m)$ deve essere l'identità di $\mathbb{Z}/n\mathbb{Z}$, cioè $f(x)^m$ lo deve essere. Cioè l'immagine di x deve avere ordine che divide m.

Quindi dalla proposizione precedente possiamo concludere che gli omomorfismi da $\mathbb{Z}/m\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ sono in bigezione con le scelte dell'immagine di x tra gli elementi di ordine divisore di m. Questa era esattamente la conclusione che avevamo ottenuto.

3.12 Il Gruppo D_n

Per ora i gruppi classici di cui conosciamo la struttura sono abbastanza pochi: gruppi ciclici e relatici prodotti diretti. La scorsa sezione abbiamo introdotto i gruppi presentati, di cui però non conosciamo esempi "concreti" diversi da quelli che già conosciamo.

Questa sezione ha lo scopo di introdurne uno nuovo: il diedrale D_n. Andiamo subito a definirlo.

Definizione 3.12.1. Sia $n \geq 3$ naturale. Definiamo il gruppo diedrale D_n come il gruppo delle isometrie del piano che portano l'ennagono regolare il sé, cioè il gruppo delle isometrie mandanti lati in lati e vertici in vertici.

Il gruppo D_n è banalmente in gruppo (in particolare è un sottogruppo delle isometrie del piano). Infatti l'identità appartiene banalmente a D_n. Inoltre se g e h mandano l'ennagono in sé, allora la loro composizione manda l'ennagono in sé. Infine se g preserva l'ennagono, allora anche la sua inversa lo farà.

Andiamo ora a dimostrare la cardinalità di D_n.

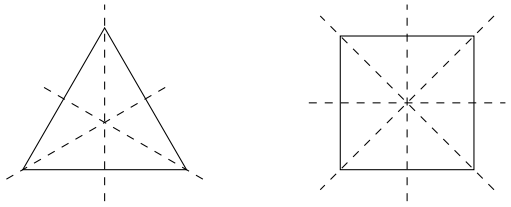
Teorema 3.12.2. *Il gruppo D_n ha cardinalità $2n$.*

Dimostrazione. Certamente conosciamo almeno $2n$ elementi di D_n.

Da una parte abbiamo n rotazioni del piano, che sono le rotazioni di angoli $2\pi/k$ con $k = 0, \ldots, n-1$.

Dall'altra un ennagono regolare possiede n assi di simmetria. Se n è pari, questi sono le rette passanti per le coppie di elementi opposti vertice - vertice e vertice - lato. Se n è dispari, queste sono le rette passanti per le coppie di elementi opposti vertice - lato. Questi assi di simmetria danno luogo a n simmetrie distinte.

Infine le simmetrie non sono rotazioni, in quanto le prime invertono le orientazioni dei vertici, mentre le seconde le preservano. Essendo che $n \geq 2$, allora queste due operazioni non sono compatibili.



Dobbiamo solo verificare che D_n ha al più $2n$ elementi.

Sia quindi Σ il nostro ennagono regolare, con vertici $z_1, \ldots, z_n$, e sia φ un elemento di D_n. Allora z_1 può essere mandato in ognuno dei vertici z_i. Quindi abbiamo n scelte possibili. Inoltre il lato $z_1\bar{}z_2$ deve essere mandato in un lato di Σ.

Quindi una volta fissata la scelta per $\varphi(z_1)$, allora $\varphi(z_2)$ può solo andare in $z_{i\pm1}$.

Infine una volta fissati $\varphi(z_1)$ e $\varphi(z_2)$, allora gli altri vertici devono seguire la stessa orientazione, in quanto φ manda lati in lati e vetici in vetici in vertici. Cioè $\varphi(z_{1+k}) = z_{i\pm k}$.

In conclusione φ è determinata da n scelte per $\varphi(z_1)$ e 2 scelte conseguenti per $\varphi(z_2)$. Quindi D_n ha al più $2n$ elementi. □

Andiamo ora a descrivere meglio gli elementi di D_n tramite la prossima proposizione.

Teorema 3.12.3. *Il gruppo D_n è isomorfo al gruppo presentato*

$$D_n \simeq \left\langle x, y \,\middle|\, x^n = e,\ y^2 = e,\ yxy = x^{-1} \right\rangle$$

Inoltre posta r la rotazione di angolo $2\pi/n$ e s una qualunque simmetria, allora gli elementi di D_n sono

$$D_n = \left\{ id, r, \ldots r^{n-1}, s, sr, \ldots sr^{n-1} \right\}$$

Dimostrazione. Dimostriamo innanzitutto la seconda uguaglianza. Certamente gli elementi descritti sono elementi di D_n, in quanto composizione di elementi di D_n. Dobbiamo solo dimostrare che sono differenti. A questo punti, essendo $2n$, abbiamo l'uguaglianza.

Certamente un elemento r^i non può coincidere con uno della forma sr^j. Infatti la prima è una rotazione (di angolo $2i\pi/n$), mentre la seconda è la composizione di una simmetria ed una rotazione, quindi è una simmetria.

Inoltre la rotazione r ha banalmente ordine n, quindi gli elementi r^i sono distinti. Infine se sr^i coincide con sr^j, allora per cancellazione r^i deve coincidere r^j. Quindi $i = j$.

Dimostriamo infine l'isomorfismo tra D_n è la presentazione data. Innanzitutto è da dimostrare che il gruppo presentato G abbia esattamente $2n$ elementi.

Ogni elemento di G è scrivibile come una stringa di x e y e loro inversi. Sfruttando il fatto che è sempre possibile cambiare yx con $x^{-1}y$, otteniamo che ogni elemento di G è della forma $y^i x^j$. Inoltre sappiamo che y ha ordine 2 e x ordine n; quindi ogni elemento di G è della forma

$$y^i x^j \quad i = 0, 1,\ j = 0, \ldots, n-1$$

Dobbiamo solo mostrare che queste espressioni danno sempre elementi diversi.

Grazie al fatto che x ha ordine n, allora le espressioni con $i = 0$ danno luogo ad elementi diversi. Anche le espressioni yx^j danno luogo ad elementi diversi. Dobbiamo solo verificare che x^j sia distinto da $yx^{j'}$. Equivalentemente dobbiamo verificare che yx^j non sia l'identità, cioè che y non possa essere una potenza di x.

Se per assurdo ciò accadesse, allora il gruppo G sarebbe generato dall'elemento x. Questo implicherebbe la sua abelianità. Ciò però non è possibile, in quanto x ed y non commutano (essendo che x non ha ordine 2, esso non coincide col suo inverso).

Quindi G ha ordine $2n$. Sia ora la mappa

$$\begin{aligned} \Phi \colon D_n &\to G \\ r^j &\mapsto x^j \\ sr^j &\mapsto yx^j \end{aligned}$$

Questa mappa è suriettiva, e quindi è iniettiva andando tra due insiemi della stessa cardinalità. Dimostriamo che è un omomorfismo, cosa evidente in quanto le relazioni tra x e y, r e s sono analoghe.

$$\Phi(s^i r^j \circ s^{i'} r^{j'}) = \Phi(s^{i+i'} r^{j'-j}) = y^{i+i'} x^{j'-j} = y^i x^j y^{i'} x^{j'} = \Phi(s^i r^j)\Phi(s^{i'} r^{j'})$$

Quindi Φ è l'isomorfismo cercato. □

A questo punto concludiamo questa sezione andando a parlare dei sottogruppi di D_n. Ne approfittiamo per enunciare questo risultato.

Proposizione 3.12.4. *Sia G un gruppo, e sia H un suo sottogruppo avente la seguente proprietà: è l'unico sottogruppo ciclico del suo ordine. Allora è normale.*

Dimostrazione. Sia g in G e sia h il generatore di H. Allora il coniugato gHg^{-1} è un sottogruppo di G, della stessa cardinalità di H, e generato da ghg^{-1}. Per ipotesi quindi deve coincidere con H.

Quindi H è normale in G. □

Con questa proposizione possiamo dimostrare la normalità di quasi tutti i sottogruppi del sottogruppo delle rotazioni.

Teorema 3.12.5. *Sia un gruppo diedrale D_n. Allora per ogni d diverso da 2 che divide n, il sottogruppo generato da $r^{n/d}$ è normale .*

Dimostrazione. Dimostriamo che il sottogruppo $R_d = \langle r^{n/d} \rangle$ è l'unico sottogruppo ciclico di ordine d in D_n. Con questa informazione, e la proposizione precedente, abbiamo il risultato.

Sia quindi un sottogruppo H generato da un certo h di ordine d. Allora h è una rotazione, in quanto le simmetrie hanno ordine 2. Quindi H è un sottogruppo di ordine d del gruppo ciclico R. Quindi coincide con R_d. □

Abbiamo lasciato da parte il caso $d = 2$. Non perché non sia normale, ma perché su di esso vale un risultato più forte.

Teorema 3.12.6. *Il centro di D_n è dato dalla seguente formula*

$$Z(D_n) = \begin{cases} \{e\} & n \text{ dispari} \\ \langle r^{n/2} \rangle & n \text{ pari} \end{cases}$$

Dimostrazione. Dimostriamo che se x è un elemento che commuta con tutto D_n, allora n deve essere pari e x deve coincidere con e o $r^{n/2}$.

Preso quindi un tale x della forma $s^\varepsilon r^j$ con j minore di n, esso commuta con tutto D_n. Quindi commuta in particolar modo con r, s. Allora

$$s^{\varepsilon+1} r^{-j} = s^\varepsilon s r^{-j} = s^\varepsilon r^j s = s s^\varepsilon r^j = s^{\varepsilon+1} r^j$$

Questo implica che

$$-j \equiv j \pmod{n} \Rightarrow 2j \equiv 0 \pmod{n}$$

Se n è dispari, questo è equivalente a

$$j \equiv 0 \pmod{n}$$

che implica che x è una potenza di s. O è l'identità, che sappiamo commutare con tutto il gruppo, o è la simmetria s, che però sappiamo non commutare con r. Quindi se n è dispari D_n ha centro banale.

Se n è pari, troviamo invece la congruenza equivalente

$$j \equiv 0 \pmod{n/2}$$

Se j coincide con n, questo porta a dire che x è l'identità.

Supponiamo invece che $j = n/2$. Dobbiamo dimostrare che ε non può essere 1. Ma infatti $sr^{n/2}$ non commuta con r

$$sr^{n/2}r \neq sr^{n/2}r^{-1} = rsr^{n/2}$$

Quindi x è $r^{n/2}$. Dimostriamo in effetti che tale elemento è nel centro di D_n. Per farlo basta osservare che commuta con ogni generatore di D_n. Sicuramente commuta con r; inoltre commuta anche con s.

$$sr^{n/2} = r^{-n/2}s = rn - n/2s = n^{n/2}s$$

Quindi il centro di D_n è il generato da $r^{n/2}$. □

Abbiamo parlato dei sottogruppi generati da una rotazione. Per quanto riguarda i sottogruppi generati da una simmetria che si può dire? La prossima proposizione nega la loro normalità

Proposizione 3.12.7. *I sottogruppi di D_n generati da una simmetria non sono normali.*

Dimostrazione. Sia un sottogruppo $H = \langle r^i s \rangle$ generato da una simmetria. Allora se lo coniughiamo per r otteniamo

$$rHr^{-1} = \langle rr^i sr^{-1} \rangle = \langle r^{i+2}s \rangle$$

che differisce da H. Infatti essendo entrambi generati da un elemento di ordine due, allora possono coincidere se e solo se $r^{i+2}s$ coincide $r^i s$. Questo però non può avvenire, in quanto 2 non è congruo a 0 modulo n. □

Concludiamo con questa semplice osservazione

Proposizione 3.12.8. *Il gruppo D_n si immerge in S_n.*

Dimostrazione. Consideriamo l'ennagono regolare con vertici $z_1, \ldots, z_n$. Allora possiamo considerare il gruppo delle loro permutazioni, isomorfo a S_n. Esiste quindi una mappa da D_n in S_n

$$\begin{aligned} \Phi \colon D_n &\to S_n \\ \sigma &\mapsto \sigma|_{\{z_1,\ldots,z_n\}} \end{aligned}$$

Va solo visto che questa mappa sia una immersione.

Certamente è iniettiva. Infatti sappiamo che una isometria in D_n è determinata dall'immagine di z_1 e z_2.

Inoltre è un banale omomorfismo, essendo una restrizione di un omomorfismo. □

3.13 Automorfismi di un Gruppo

Vogliamo adesso parlare degli automorfismi di un gruppo, in quanto saranno alla base del prodotto semidiretto tra gruppi, una costruzione che affronteremo in seguito.

Come sappiamo gli automorfismi di un gruppo G sono il gruppo degli isomorfismo del gruppo in sè. Di particolare rilevanza sono i cosiddetti automorfismi interni, descritti dalla prossima proposizione.

Proposizione 3.13.1. *Sia G un gruppo. Allora preso g in G, indichiamo con φ_g la mappa di coniugio*

$$\begin{aligned} \varphi_g \colon G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

Valgono le seguenti affermazioni:

1. *Per ogni g in G, la mappa φ_g è un automorfismo.*
2. *L'insieme di tali automorfismi, detti automorfismi interi, è un sottogruppo normale in* $\mathrm{Aut}(G)$.

Dimostrazione. (1.) È immediato verificare che φ_g sia un omomorfismo:

$$\varphi_g(xy) = gxyg^{-1} = gxyg^{-1}gxyg^{-1} = \varphi_g(x)\varphi_g(y)$$

Inoltre è suggettiva, in quanto l'elemento x di G è immagine di $g^{-1}xg$.

Infine è iniettiva, in quanto se x appartiene al nucleo, allora $g^{-1}xg = e$ implica che x sia l'identità.

Quindi φ_g è un automorfismo.

(2.) Dimostriamo che l'insieme degli automorfismi interi, indicato con $\mathrm{Inn}(G)$, sia un sottogruppo normale di $\mathrm{Aut}(G)$.

L'identità vi appartiene, in quanto φ_e è la mappa banale.

Se φ_{g_1} e φ_{g_2} sono automorfismi interi, allora la loro composizione coincide con $\varphi_{g_1g_2}$

$$(\varphi_{g_1} \circ \varphi_{g_2})(x) = \varphi_{g_1}(g_2xg_2^{-1}) = g_1g_2xg_2^{-1}g_1^{-1} = \varphi_{g_1g_2}(x)$$

Infine l'inverso di φ_g è ancora un automorfismo interno, pari a $\varphi_{g^{-1}}$.

Sia ora un automorfismo interno φ_g e un automorfismo f. Allora per ogni x in G vale l'uguaglianza

$$\begin{aligned}(f \circ \varphi_g \circ f^{-1})(x) &= (f \circ \varphi_g)(f^{-1}(x)) \\ &= f(gf^{-1}(x)g^{-1}) \\ &= f(g)xf(g)^{-1} \\ &= \varphi_{f(g)}(x)\end{aligned}$$

Quindi $f \circ \varphi_g \circ f^{-1}$ coincide con $\varphi_{f(g)}$, che è un automorfismo interno. Quindi $\mathrm{Inn}(G)$ è normale in $\mathrm{Aut}(G)$. □

Mentre il gruppo degli automorfismi può essere estremamente difficoltoso da calcolare, per gli automorfismi interi l'operazione è più agevole. Vale infatti

Proposizione 3.13.2. *Sia G un gruppo. Allora*

$$\mathrm{Inn}(G) \simeq G/Z(G)$$

Dimostrazione. Consideriamo la mappa

$$\begin{aligned}\Phi\colon G &\to \mathrm{Inn}(G) \\ g &\mapsto \varphi_g\end{aligned}$$

Innanzitutto verifichiamo che sia un omomorfismo. Presi g_1 e g_2 in G, allora abbiamo già osservato che $\varphi_{g_1} \circ \varphi_{g_2}$ coincide con $\varphi_{g_1 g_1}$. Cioè $\Phi(g_1) \circ \Phi(g_2)$ coincide con $\Phi(g_1 g_2)$ e Φ è un omomorfismo.

Per costruzione Φ è suggettiva.

Dobbiamo solo calcolarne il nucleo. Preso g in G, esso è nel nucleo se per ogni x in G, $\varphi_g(x)$ coincide con x. Cioè per ogni x in G

$$x = \varphi_g(x) = gxg^{-1}$$

Cioè g deve commutare con ogni elemento di G. Quindi il nucleo di Φ è il centro di G.

Possiamo quindi concludere usando il primo teorema di omomorfismo

$$\mathrm{Inn}(G) = \mathrm{Im}(\Phi) \simeq G/\operatorname{Ker}(\Phi) = G/Z(G) \qquad \square$$

Corollario 3.13.3. *Sia G un gruppo. Se il gruppo degli automorfismi interni è ciclico, allora è banale.*

Dimostrazione. Dalla proposizione precedente, se $\mathrm{Inn}(G)$ è ciclico, anche $G/Z(G)$ lo è. Quindi G è abeliano e $G/Z(G)$ è banale. Quindi lo è anche $\mathrm{Inn}(G)$. $\square$

Osserviamo che se H è un sottogruppo normale in G se e solo se esso è invariante per ogni automorfismo interno (cioè $f(H) = H$ per ogni $f \in \mathrm{Inn}(G)$). Se andiamo a fare una richiesta analoga, ma usando l'intero gruppo degli automorfismi, otteniamo la definizione di sottogruppo caratteristico.

Definizione 3.13.4. Sia G un gruppo. Un sottogruppo H si dice caratteristico se è invariante per gli automorfismi di G. Cioé se $f(H) = H$ per ogni f in $\mathrm{Aut}(G)$.

Ovviamente un sottogruppo normale è caratteristico, anche se il viceversa è falso. Per esempio consideriamo i sottogruppi di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ pari a

$$H_1 = \langle(\bar{1}, \bar{0})\rangle \qquad H_2 = \langle(\bar{0}, \bar{1})\rangle \qquad H_3 = \langle(\bar{1}, \bar{1})\rangle$$

Questi sono normali in quanto il gruppo è abeliano. Tuttavia non sono caratteristici. Infatti la mappa

$$\begin{aligned} &\Phi\colon G \to G \\ &(\bar{1}, \bar{0}) \mapsto (\bar{1}, \bar{1}) \\ &(\bar{0}, \bar{1}) \mapsto (\bar{0}, \bar{1}) \end{aligned}$$

è una mappa definita sui generatori di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si può provare che quest'ultimo ha presentazione:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \langle x, y \,|\, x^2 = e,\ y^2 = e,\ xy = yx \rangle$$

Essendo che le immagini di dei generatori rispettano le presentazioni, allora abbiamo un omomorfismo da G in G della forma

$$\begin{aligned} \Phi(\bar{a}, \bar{b}) &= a\,\Phi(\bar{1}, \bar{0}) + b\,\Phi(\bar{0}, \bar{1}) \\ &= (\bar{a}, \bar{a}) + (\bar{0}, \bar{b}) \\ &= (\bar{a}, \bar{a} + \bar{b}) \end{aligned}$$

La mappa Φ è un isomorfismo, in quanto è un omomorfismo suriettivo da G, gruppo finito, in sé: ogni elemento $(\bar{x}, \bar{y})$ in G ha preimmagine $(\bar{x}, \bar{y} - \bar{x})$.

Quindi Φ è un automorfismo di G che manda H_1 in H_3. Quindi nessuno dei due possono essere caratteristici. Allo stesso modo H_2 non lo è

L'essere normale e l'essere caratteristico si collegano tramite la seguente proposizione:

Proposizione 3.13.5. *Sia G un gruppo. Se H è un sottogruppo normale di G caratteristico, e K è un sottogruppo in H e caratteristico in esso, allora K è normale in G.*

Dimostrazione. Consideriamo la mappa seguente

$$\begin{aligned} \Phi\colon \mathrm{Inn}(G) &\to \mathrm{Aut}(H) \\ \varphi_g &\mapsto \varphi_g|_H \end{aligned}$$

Essa è ben definita. Infatti H è invariante per automorfismi interni. Quindi per ogni φ_g automorfismo intero, $\varphi_g|_H$ è una mappa da H in sé suggettiva. Inoltre è iniettiva in quanto φ lo era in partenza. Quindi $\varphi_g|_H$ è un automorfismo di H (in generale non è un automorfismo interno di H, in quanto g non appartiene ad H).

Sia quindi g in G. Allora essendo K caratteristico in H, esso è invariante per $\varphi_g|_H$. Quindi

$$\varphi_g(K) = \varphi_g|_H(K) = K$$

Quindi K è normale in G. □

La richiesta che K sia caratteristico in H non si può sostituire con l'ipotesi di normalità. Come controesempio consideriamo $G = D_4$, $K = \langle s \rangle$, $H = \langle s, r^2 \rangle$. Il gruppo H è generato da due elementi di ordine 2, che commutano tra loro, in quanto r^2 genera il centro di D_4. Quindi H è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e ha ordine 4.

Quindi K ha indice 2 in H, che ha indice 2 in G. Quindi K è normale in H, che e normale in G. Tuttavia abbiamo già osservato che K non è normale in G.

Andiamo ora ad analizzare come si comporta il gruppo degli automorfismi col prodotto di gruppi. La punto chiave è la seguente proposizione.

Proposizione 3.13.6. *Siano H e K due gruppi finiti di ordine coprimi. Posto G il loro prodotto diretto, allora $\{e\} \times K$ e $H \times \{e\}$ sono sottogruppi caratteristici di G.*

Dimostrazione. Dimostriamo che (h, k) appartiene a $\{e\} \times K$ se e solo se il suo ordine divide la cardinalità di K.

($\Rightarrow$) Se (h, k) appartiene a $\{e\} \times K$, allora $h = e_H$. Quindi posta m la cardinalità di K, vale che

$$(e_h, k)^m = (e_h, k^m) = (e_h, e_k)$$

Quindi l'ordine di (h, k) divide quello di K.

($\Leftarrow$) Se l'ordine di (h, k) divide quello di K, allora $(h, k)^m = (e_H, e_K)$. Ergo

$$\begin{cases} h^m = e_H \\ k^m = e_K \end{cases}$$

Quindi l'ordine di h divide l'ordine K, oltre che ovviamente l'ordine di H. Quindi divide il loro massimo comune divisore, che è 1. Quindi h è l'identità e (h, k) appartiene a $\{e\} \times K$.

Allo stesso modo (h, k) appartiene a $H \times \{e\}$ se e solo se l'ordine di (h, k) divide l'ordine di H.

Adesso possiamo facilmente concludere. Gli automorfismi di G preservano l'ordine degli elementi, quindi i sottogruppi $\{e\} \times K$ e $H \times \{e\}$ sono caratteristici. □

Poniamo adesso la domanda ovvia riguardo agli automorfismi di un prodotto diretto: quando è che $\mathrm{Aut}(H \times K)$ è isomorfo a $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$? Il prossimo risultato fornisce la risposta.

Teorema 3.13.7. *Sia G un gruppo, prodotto diretto di H e K. Se $\{e\} \times K$ e $H \times \{e\}$ sono caratteristici, allora $\mathrm{Aut}(G)$ è isomorfo a $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Viceversa se G è finito, e $\mathrm{Aut}(G)$ è isomorfo a $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$, allora $\{e\} \times K$ e $H \times \{e\}$ sono caratteristici.*

Dimostrazione. Sia l'immersione

$$\begin{aligned} \Phi\colon \mathrm{Aut}(H) \times \mathrm{Aut}(K) &\hookrightarrow \mathrm{Aut}(G) \\ (\varphi_1, \varphi_2) &\mapsto (\varphi_1\varphi_2) \end{aligned}$$

dove con $\varphi_1\varphi_2$ è definita come

$$(\varphi_1\varphi_2)(x, y) = (\varphi_1(x), \varphi_2(y))$$

Allora possiamo dimostrare i due risultati.

(1.) Se $\{e\}\times K$ e $H\times\{e\}$ sono caratteristici, allora la mappa Φ è suggettiva. Infatti per ogni φ automorfismo di G, allora $\varphi|_{H\times\{e\}}$ e $\varphi|_{\{e\}\times K}$ sono automorfismi di $H\times\{e\}$ e $\{e\}\times K$ rispettivamente. Inoltre $\Phi(\varphi|_{H\times\{e\}}, \varphi|_{\{e\}\times K})$ coincide con φ.

Quindi Φ è suggettiva ed è l'isomorfismo cercato.

(2.) Se $\mathrm{Aut}(G)$ e $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ sono isomorfi, allora hanno la stessa cardinalità. Essendo finita, allora la mappa Φ, oltre ad essere iniettiva, deve essere anche suggettiva. Quindi per ogni φ in G, esso è immagine di (φ_1, φ_2). Ergo per ogni (h, e) in $H \times \{e\}$

$$\varphi(H \times \{e\}) = \varphi_1(H) \times \varphi_2(\{e\}) = H \times \{e\}$$

Quindi $H \times \{e\}$ è caratteristico. Allo stesso modo lo è $\{e\} \times K$. □

Concludiamo la sezione col gruppo di automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$:

Teorema 3.13.8. *Sia il gruppo $(\mathbb{Z}/p\mathbb{Z})^n$ e indichiamo con $\mathbb{F}_p$ l'insieme $\mathbb{Z}/p\mathbb{Z}$ con la struttura di campo. Allora il gruppo di automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$ è isomorfo a $GL_n(\mathbb{F}_p)$, cioè alle matrici $n \times n$ invertibili a coefficienti in $\mathbb{F}_p$. Inoltre ha cardinalità*

$$|GL_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1} (p^n - p^i)$$

Dimostrazione. Abbiamo già osservato che i sottogruppi di $\mathbb{Z}/p\mathbb{Z}$ coincidono con i sottospazi vettoriali di $\mathbb{F}_p^n$. Analogamente è immediato che gli automorfismi di gruppo di $(\mathbb{Z}/p\mathbb{Z})^n$ coincidono con gli automorfismi di $\mathbb{F}_p^n$ come $\mathbb{F}_p$-spazio vettoriale. Infatti preso omomorfismo φ da $(\mathbb{Z}/p\mathbb{Z})^n$ in sè, allora esso rispetta anche la moltiplicazione per scalare:

$$\varphi([n]v) = \varphi(\underbrace{v + \cdots + v}_{n}) = \underbrace{\varphi(v) + \cdots + \varphi(v)}_{n} = [n]\varphi(v)$$

Quindi gli automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$ coincidono con gli automorfismi di $\mathbb{F}_p^n$. Come sappiamo dall'algebra lineare, questi sono $GL_n(\mathbb{F}_p)$. Infine per quanto riguarda la cardinalità, sappiamo che una matrice $n \times n$ appartiene al gruppo lineare se e solo se le colonne costituiscono una base di $\mathbb{F}_p^n$. Come già osservato quando contavamo i sottospazi, queste sono pari a

$$\prod_{i=0}^{n-1}(p^n - p^i) \qquad \square$$

Corollario 3.13.9. *Il gruppo degli automorfismi di $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ è isomorfo a S_3.*

Dimostrazione. Ogni automorfismo scambia i tre elementi di ordine 2 di G. Quindi ne abbiamo al più 6, pari alla cardinalità di S_3. D'altra parte sappiamo che la cardinalità di $GL_2(\mathbb{F}_2)$ è esattamente 6. Quindi gli automorfismi di $(\mathbb{Z}/2\mathbb{Z})^2$ corrispondono esattamente alle permutazioni dei tre elementi di ordine 2. Quindi $\mathrm{Aut}(G)$ è isomorfo a S_3.

Inoltre andando a calcolare esplicitamente le basi di $\mathbb{F}_2^2$, possibile data la bassa cardinalità, otteniamo che le 6 matrici sono

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix} \qquad \square$$

3.14 Azioni di Gruppo e Formula delle Classi

In questa sezione tratteremo un fondamentale concetto della teoria dei gruppi: quella di azione di gruppo.

Definizione 3.14.1. Sia X un insieme e G un gruppo. Un'azione di G su X è un omomorfismo da G alle permutazioni di X.

Posta un'azione

$$\Phi \colon G \to S(X)$$
$$g \mapsto \varphi_g$$

allora dal fatto che Φ sia un omomorfismo seguono le seguenti proprietà:

1. $\varphi_e = id_X$
2. $\varphi_g \circ \varphi_{g'} = \varphi_{gg'}$
3. $\varphi_g^{-1} = \varphi_{g^{-1}}$

Prima di considerare degli esempi concreti, andiamo a introdurre gli importanti concetti di orbita e stabilizzatore. Iniziamo col primo concetto.

Proposizione 3.14.2. *Sia un gruppo G che agisce su un insieme X. Allora posta la relazione*

$$x \sim y \;\Leftrightarrow\; \exists g \in G \text{ t.c. } \varphi_g(x) = y$$

essa è una relazione di equivalenza. Inoltre la classe di equivalenza di x viene detta orbita di x.

Dimostrazione. Ogni elemento x di X è in relazione con se stesso, in quanto $\varphi_e(x) = x$.

Se x è in relazione con y tramite g in G, allora y è in relazione con x tramite g^{-1}.

Se x è in relazione con y tramite g, e y lo è con z tramite g', allora x lo è con z tramite gg'. □

Definizione 3.14.3. Sia G gruppo agente su X. Allora definiamo lo stabilizzatore di x come

$$\mathrm{Stab}(x) = \{\, g \in G \mid \varphi_g(x) = x \,\}$$

Proposizione 3.14.4. *Sia G gruppo agente su X. Allora per ogni x in X, il suo stabilizzatore è un sottogruppo di G.*

Dimostrazione. Certamente e appartiene a $\mathrm{Stab}\, x$, in quanto $\varphi_e(x) = x$.

Inoltre se g, g' appartengono a $\mathrm{Stab}\, x$, allora anche il loro prodotto vi appartiene. Infatti

$$\varphi_{gg'}(x) = \varphi_g(\varphi_{g'}(x)) = \varphi_g(x) = x$$

Infine se g appartiene a $\operatorname{Stab} x$, allora anche g^{-1} fissa x

$$\varphi_{g^{-1}}(x) = \varphi_g^{-1}(x) = x$$

□

Le orbite e gli stablizzatori sono fortemente collegati, col teorema orbita-stabilizzatore

Teorema 3.14.5 (Teorema Orbita-Stabilizzatore)**.** *Sia un gruppo G finito agente su X. Allora per ogni x in X vale la relazione*

$$|G| = |\operatorname{orb}(x)||\operatorname{Stab}(x)|$$

Dimostrazione. Il punto della dimostrazione è verificare che la mappa

$$\begin{aligned} \Phi\colon \operatorname{orb}(x) &\to G/\operatorname{Stab}(x) \\ \varphi_g(x) &\mapsto g\operatorname{Stab}(x) \end{aligned}$$

sia una bigezione ben definita (dove abbiamo indicato con $G/\operatorname{Stab}(x)$ l'insieme delle classi laterali, che in generali non è un gruppo).

Verifichiamo contemporaneamente la buona definizione e l'iniettività

$$\begin{aligned} \varphi_g(x) = \varphi_h(x) &\Leftrightarrow \varphi_{h^{-1}}(\varphi_g(x)) = x \\ &\Leftrightarrow \varphi_{h^{-1}g}(x) = x \\ &\Leftrightarrow h^{-1}g \in \operatorname{Stab}(x) \\ &\Leftrightarrow h\operatorname{Stab}(x) = g\operatorname{Stab}(x) \end{aligned}$$

Infine Φ è banalmente suriettiva.

Quindi possiamo concludere la dimostrazione

$$|G| = |G/\operatorname{Stab}(x)||\operatorname{Stab}(x)| = |\operatorname{orb}(x)||\operatorname{Stab}(x)|$$

□

Diamo adesso due importanti esempi di azioni di gruppo. Il primo esempio è quello che conosciamo già: quella di coniugio

$$\begin{aligned} \varphi\colon G &\to S(G) \\ \varphi &\mapsto (\varphi_g(h) = ghg^{-1}) \end{aligned}$$

Avevamo di fatto già dimostrato che questa è un'azione, quando avevamo affermato che il gruppo degli automorfismi interni è isomorfo a $G/Z(G)$.

Gli stabilizzatori per l'azione di coniugio prendono un nome particolare: quello di centralizzatore:

Definizione 3.14.6. Sia G un gruppo e sia g un suo elemento. Definiamo il centralizzatore di g, indicato con $Z_G(g)$, come lo stabilizzatore di g per l'azione di coniugo.

Rispondiamo brevemente a questa domanda: come interviene il centro di un gruppo in questo contesto? La risposta viene dalla prossima proposizione.

Proposizione 3.14.7. *Sia G un gruppo e φ una azione su un certo insieme X. Allora il nucleo di φ è l'intersezione degli stabilizzatori.*

Dimostrazione. Vogliamo dimostrare che

$$\mathrm{Ker}(\varphi) = \bigcap_{x \in X} \mathrm{Stab}(x)$$

L'identità di $S(G)$ è pari a id_X. Ergo g è nel nucleo di G se e solo se $\varphi_g = id_X$. Questo equivale a dire che per ogni x in X, $\varphi_g(x) = x$. Cioè è equivalente ad affermare che g appartiene a tutti gli stabilizzatori. □

Corollario 3.14.8. *Sia G un gruppo. Allora*

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

Dimostrazione. Banale corollario della proposizione precedente. □

Un'altra azione importante è quella di coniugio sui sottogruppi.

Proposizione 3.14.9. *Sia G un gruppo e sia X l'insieme di tutti i sottogruppi di G. Allora la mappa*

$$\begin{aligned} \varphi \colon G &\to S(X) \\ g &\mapsto (\varphi_g(H) = gHg^{-1}) \end{aligned}$$

è una azione di gruppo.

Dimostrazione. Verifichiamo che sia ben definita.

Sia quindi g in G. Allora φ_g manda innanzitutto sottogruppi in sottogruppi. Inoltre è iniettiva. Infatti se gHg^{-1} coincide con gKg^{-1}, allora

$$H = g^{-1}(gHg^{-1})g = g^{-1}(gKg^{-1})g = K$$

Inoltre preso un sottogruppo H, allora $g^{-1}Hg$ è evidentemente la sua preimmagine.

Infine φ è un omomorfismo. Infatti presi g, g' in G e un sottogruppo H

$$\varphi_{gg'}(H) = gg'G(gg')^{-1} = gg'Hg'^{-1}g^{-1} = (\varphi_g \circ \varphi_{g'})(H)$$

quindi $\varphi_{gg'}$ coincide con $\varphi_g \circ \varphi_{g'}$ e φ è un omomorfismo. □

Analogalmente al centralizzatore di un elemento, si definisce il normalizzatore di un sottogruppo nel seguente modo:

Definizione 3.14.10. Sia G un gruppo e H un sottogruppo. Definiamo il normalizzatore di H, indicato con $N_G(H)$, come lo stabilizzatore di H rispetto all'azione di G sull'insieme dei suoi sottogruppi.

Il normalizzatore di un sottogruppo ammette la seguente utile caratterizzazione:

Proposizione 3.14.11. *Sia G un gruppo e H un sottogruppo. Allora $N_G(H)$ è il più grande sottogruppo per cui H è normale in esso.*

Dimostrazione. Sia l'insieme

$$\mathcal{F} = \{\, K \leq G \mid H \trianglelefteq K \,\}$$

Vogliamo affermare che

$$N_G(H) = \bigcup_{K \in \mathcal{F}} K$$

($\subseteq$) Il sottogruppo H è banalmente normale nel suo normalizzatore. Infatti preso g in $N_G(H)$, allora g appartiene allo stabilizzatore di H secondo l'azione di coniugio. Quindi $gHg^{-1} = H$.

Quindi $N_G(H)$ appartiene a $\mathcal{F}$, ed è incluso in nell'unione.

($\supseteq$) Preso un qualunque K in $\mathcal{F}$, allora per ogni g in esso, $gHg^{-1} = H$. Ergo K è incluso nel normalizzatore per ogni K in $\mathcal{F}$. Quindi anche l'unione è inclusa. □

Presentiamo adesso con due importanti risultati: la formula delle classi e il teorema di Cauchy.

Teorema 3.14.12 (Formula delle Classi)**.** *Sia G un gruppo e poniamo R un insieme di rappresentanti per le orbite di coniugio. Allora*

$$|G| = |Z(G)| \quad + \sum_{R \setminus Z(G)} \frac{|G|}{|Z_G(g)|}$$

catena

Dimostrazione. Notiamo innanzitutto un fatto, caratteristico dell'azione di coniugio.

Se g e h sono due elementi di G, tale che g appartiene al centralizzatore di h, allora h appartiene al centralizzatore di g.

$$\varphi_g(h) = h \Rightarrow ghg^{-1} = h \Rightarrow hgh^{-1} = g$$

Quindi h appartiene al centralizzatore di g.

A questo punto se prendiamo g in $Z(G) \cap R$, allora la sua orbita è banale. Infatti preso x in essa, allora esiste un certo h in G tale che $\varphi_h(g) = x$. Tuttavia g è nel centro, quindi appartiene ad ogni centralizzatore. In particolare appartiene al centralizzatore di x, che quindi appartiene al centralizzatore di g. Ergo

$$x = \varphi_h(g) = g$$

Quindi per ogni g in $Z(G) \cap R$, la sua orbita è banale. A questo punto sfruttiamo il fatto che le orbite partizionano G. Grazie a questo sappiamo che R deve contenere tutto il centro, in quanto ogni g in esso ha solo se stesso come rappresentante della sua orbita. Quindi

$$\begin{aligned}
|G| = \sum_R |\mathrm{orb}(g)| &= \sum_{R \cap Z(G)} |\mathrm{orb}(g)| \quad + \sum_{R \setminus Z(G)} |\mathrm{orb}(g)| \\
&= \sum_{Z(G)} |\mathrm{orb}(g)| \quad + \sum_{R \setminus Z(G)} |\mathrm{orb}(g)| \\
&= |Z(G)| \quad + \sum_{R \setminus Z(G)} |\mathrm{orb}(g)| \\
&= |Z(G)| \quad + \sum_{R \setminus Z(G)} \frac{|G|}{|Z_G(g)|}
\end{aligned}$$

□

Chiudiamo questa questa sezione con una serie di teoremi che sfruttano la teoria delle azioni. Iniziamo col teorema di Cauchy nel caso generale (ricordiamo che parleremo spesso di coniugati di $x \in X$ anche quando un azione non sia di coniugio).

Teorema 3.14.13 (Teorema di Cauchy)**.** *Sia G un gruppo di ordine finito, e sia p primo che divide il suo ordine. Allora G ammette un elemento di ordine p.*

Dimostrazione. Consideriamo l'insieme delle p-uple di G indicizzate con $\mathbb{Z}/p\mathbb{Z}$.

$$G^p = \{\, \varphi\colon \mathbb{Z}/p\mathbb{Z} \to G \,\} = \{\, (g_{\bar{1}}, \dots, g_{\bar{p}}) \mid g_{\bar{\imath}} \in G \,\}$$

Sia inoltre il seguente suo sottoinsieme

$$X = \{\, (g_{\bar{1}}, \dots, g_{\bar{p}}) \in G^p \mid g_{\bar{1}} \cdot \dots \cdot g_{\bar{p}} = e \,\}$$

Allora $\mathbb{Z}/p\mathbb{Z}$ agisce su X tramite *shift*

$$\begin{aligned} \varphi\colon \mathbb{Z}/p\mathbb{Z} &\to S(X) \\ \bar{a} &\mapsto (\varphi_{\bar{a}}\colon (g_{\bar{1}}, \dots, g_{\bar{p}}) \mapsto (g_{\bar{1}+\bar{a}}, \dots, g_{\bar{p}+\bar{a}})) \end{aligned}$$

L'unica verifica delicata è che $\varphi_{\bar{a}}$ sia una permutazione da X in sé. Infatti se $(x_{\bar{1}}, \dots, x_{\bar{p}})$ è un elemento di X, allora $x_{\bar{p}}$ è l'inverso di

$$g_{\bar{1}} \cdot \dots \cdot g_{\bar{p-1}}$$

Quindi deve essere in particolar modo un inverso sinistro, da cui

$$g_{\bar{p}} \cdot g_{\bar{1}} \cdot \dots \cdot g_{\bar{p-1}} = e$$

A questo punto sia x in X. Allora la sua orbita ha cardinalità che divide l'ordine di G. Quindi può solo essere p o 1. Tuttavia è facile individuare le condizioni per cui la cardinalità sia 1.

Se $x = (g, \dots, g)$, allora l'insieme di coniugati è costituito solo da se stesso.

Viceversa, se esistono due $\bar{\imath} \neq \bar{\jmath}$ tale che $g_{\bar{\imath}} \neq g_{\bar{\jmath}}$, allora $\bar{\jmath} - \bar{\imath}$ manda x in un certo y, e

$$y_{\bar{\imath}} = x_{\bar{\imath}+\bar{\jmath}-\bar{\imath}} = x_{\bar{\jmath}} \neq x_{\imath}$$

Quindi y è un coniugato di x diverso da x stesso. Quindi l'orbita di x ha almeno due elementi.

Quindi grazie al vincolo sulle cardinalità sulle orbite, possiamo affermare che tutti e soli gli elementi in X la cui ha orbita ha cardinalità 1, sono quelli della forma $(g, \dots, g)$. Inoltre per come abbiamo definito X, $g^p = e$. Quindi

$$\{ x \in X \mid |\mathrm{orb}(x)| = 1 \} = \{ (g, \dots, g) \mid \mathrm{ord}(g) = p \} \cup \{(e, \dots, e)\}$$

A questo punto dobbiamo trovare la cardinalità di X. Esso ha cardinalità $|G|^{p-1}$, in quanto la seguente mappa

$$\begin{aligned} \Phi \colon G^{p-1} &\to X \\ (a_1, \dots, a_{p-1}) &\mapsto (a_1, \dots, a_{p-1}, (a_1 \dots a_{p-1})^{-1}) \end{aligned}$$

è una banale bigezione.

Inoltre

$$|X| = \sum_{x \in R} |\mathrm{orb}\, x| = p\,|\{\text{orbite lunghezza } p\}| + |\{\text{orbite lunghezza } 1\}|$$

Quindi possiamo passare ai moduli:

$$0 \equiv |X| \equiv |\{\text{orbite lunghezza } 1\}| = |\{ g \in G \mid \mathrm{ord}(g) = p \vee g = e \}| \pmod p$$

Quindi l'ultimo insieme ha cardinalità maggiore di 1, e quindi deve esistere un elemento di ordine p. □

Grazie al teorema di Cauchy abbiamo ottenuto un grosso strumento. Per esempio possiamo dimostrare il prossimo teorema di classificazione:

Teorema 3.14.14. *Sia p primo. Allora D_p e $\mathbb{Z}/2p\mathbb{Z}$ sono gli unici gruppi di ordine $2p$ a meno di isomorfismo.*

Dimostrazione. Per il teorema di Cauchy esistono due elementi h, k in G, uno di ordine 2 e uno di ordine p. Allora $\langle h, k \rangle$ contiene i sottogruppi $\langle h \rangle, \langle k \rangle$ che sono di ordine 2 e p rispettivamente. Quindi $\langle h, k \rangle$ ha ordine diviso da $[2, p] = 2p$. Cioè $\langle 2, p \rangle$ ha ordine $2p$ e coincide con G.

Se h e k commutano, allora $\mathrm{ord}(hk) = [2, p] = 2p$. Quindi hk genera G che è isomorfo a $\mathbb{Z}/2p\mathbb{Z}$.

Altrimenti cosa può succedere? Essendo $K = \langle k \rangle$ di indice 2, esso è normale ed è possibile considerare la mappa

$$\mathbb{Z}/2\mathbb{Z} \simeq \langle h \rangle \hookrightarrow G \to \mathrm{Inn}(G) \to \mathrm{Aut}(K) \simeq \mathbb{Z}/p\mathbb{Z}^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

che associa ad ogni x in $\langle h \rangle$ la restrizione di φ_x ad K.

Im particolare l'ordine di φ_h deve dividere l'ordine di h. Quindi può solo essere 1 o 2.

Se l'ordine di φ_h è 1, allora la catena precedente associa a h la classe $y = 1$, e quindi

$$hkh^{-1} = \varphi_h(k) = id(k) = k$$

E come già detto G è isomorfo a $\mathbb{Z}/2p\mathbb{Z}$.

Se invece φ_h ha ordine 2, allora la mappa precedente associa a h la classe $y = -1$, l'unica di ordine 2. Quindi

$$hkh^{-1} = \varphi_h(k) = k^{-1}$$

In questo caso

$$\begin{aligned} \Phi \colon D_p &\to G \\ r &\mapsto k \\ s &\mapsto h \end{aligned}$$

è l'isomorfismo cercato. Infatti h e k rispettano le relazioni di s e r. Quindi Φ è un omomorfismo. Inoltre è suggettiva, in quanto G è generato da g e h. Infine per cardinalità la mappa è anche iniettiva e quindi è un isomorfismo. □

Il prossimo teorema che dimostriamo è l'utile teorema di Poincaré

Teorema 3.14.15 (Teorema di Poincaré)**.** *Sia G un gruppo, con H un suo sottogruppo di indice finito n. Allora esiste N, sottogruppo normale in G contenuto in H, tale che*

$$n \mid [G : N] \mid n!$$

Dimostrazione. Consideriamo l'insieme delle classi G/H, non necessariamente un gruppo, e consideriamo l'azione di G su di esso

$$\begin{aligned} \varphi \colon G &\to S(G/H) \\ g &\mapsto (\varphi_g(xH) = gxH) \end{aligned}$$

Scegliamo $N = \mathrm{Ker}(\varphi)$, e verifichiamo che abbia le caratteristiche volute.

Sicuramente è normale. Inoltre se x appartiene a N, allora $\varphi_x(H) = xH$ coincide con H. Quindi x appartiene a H.

Infine sappiamo che l'immagine di φ ha ordine che divide $n!$, quindi da una parte

$$[G : N] = |\mathrm{Im}(\varphi)| \mid n!$$

e dall'altra parte

$$\frac{[G : N]}{n} = \frac{[G : N]}{[G : H]} = \frac{|G|/|N|}{|G|/|H|} = \frac{|H|}{|N|} \in \mathbb{Z}$$

□

Corollario 3.14.16. *Un gruppo di ordine 44 contiene un sottogruppo di ordine 11 normale.*

Dimostrazione. Per il teorema di Cauchy esiste un g in G di ordine 11. Poniamo $H = \langle g \rangle$.

Per il teorema di Poincaré esiste un sottogruppo N, contenuto in H, di indice che divide $4! = 24$ e diviso da 4. Ma l'indice di N divide anche l'ordine di G. Ergo

$$4 \mid [G : N] \mid (44, 11) = 4$$

Quindi N ha indice parti a 4, e quindi coincide con N che è normale. □

Osserviamo che il teorema di Poincaré non ci dice che ogni gruppo ammette necessariamente sottogruppi normali "interessanti". Infatti N potrebbe essere o il gruppo banale o tutto G.

Procediamo a dimostrare il seguente fatto sulla normalità dei sottogruppi

Teorema 3.14.17. *Sia G gruppo finito, e sia H un sottogruppo di G di cardinalità il più piccolo primo p che divide l'ordine di G. Allora H è normale in G.*

Dimostrazione. Come nel teorema precedente consideriamo l'insieme delle classi laterali G/H e l'azione

$$\begin{aligned} \varphi \colon G &\to S(G/H) \simeq S_p \\ g &\mapsto (\varphi_g(xH) = gxH) \end{aligned}$$

Allora l'immagine di φ ha come ordine l'indice di $\mathrm{Ker}(\varphi)$, che quindi divide contemporaneamente l'ordine di G e di S_p. Ergo

$$|\mathrm{Im}(\varphi)| \mid (p!, |G|)$$

Ma p è il più piccolo primo che divide l'ordine di G. Quindi $p!$ e $|G|$ possono solo avere p come fattore comune. Quindi $\mathrm{Im}(\varphi)$ ha cardinalità che può solo essere p o 1.

Se per assurdo la cardinalità fosse 1, allora il nucleo coinciderebbe con tutto G (in questo caso l'azione si dice *fedele*). Tuttavia se ciò accadesse, potremmo considerare un g in $G \setminus H$. Allora $gH = \varphi_g(H) = H$. Assurdo.

Quindi l'immagine di φ ha ordine p e il nucleo ha ordine $|G|/p$.

Infine, come già osservato nel teorema precedentemente, il nucleo di φ è incluso in H. Infine per cardinalità devono coincidere. □

Concludiamo la sezione col teorema di Cayley. Esso venne dimostrato da Cayley, uno dei padri della teoria dei gruppi, quando non era ancora chiaro se ogni gruppo potesse essere pensato come azione su un insieme. In particolare Cayley si chiedeva se tutti i gruppi potessero essere visti come sottogruppi di gruppi di permutazioni. Il teorema che prende il suo nome lo conferma.

Teorema 3.14.18 (Teorema di Cayley)**.** *Sia G un gruppo. Allora esso si immerge in $S(G)$.*

Dimostrazione. Consideriamo la seguente mappa

$$\begin{aligned} \Phi \colon G &\to S(G) \\ g &\mapsto (\varphi_g \colon h \mapsto gh) \end{aligned}$$

Esso è un banale omomorfismo. Inoltre se φ_g è banale, allora $e = \varphi_g(e) = g$. Quindi Φ ha nucleo banale ed è una immersione. □

3.15 Gruppi di ordine p^n

Consideriamo adesso il prossimo mattone per la teoria dei gruppi: i gruppi di ordine p^n con p primo e $n > 0$, che per brevità chiameremmo p-gruppi. Essi posseggono diverse proprietà interessanti, ad iniziare dalla seguente:

Teorema 3.15.1. *Sia G un p-gruppo. Allora il suo centro non può essere banale.*

Dimostrazione. Consideriamo la formula delle classi

$$|G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

Per ogni x in $R \setminus Z(G)$, allora il suo centralizzatore non può essere tutto G, altrimenti x apparterrebbe al centro di G. Quindi $|G| = p^n$ e $|Z_g(x)| = p^h$ con $h < n$. In particolare il loro rapporto è diviso da p.

Infine p divide l'ordine di G, e usando la formula delle classi si può concludere che p divide l'ordine del centro, che quindi è non banale. □

Da questo teorema discende per esempio un altro facile teorema di classificazione.

Teorema 3.15.2. *Sia G un gruppo di ordine p^2. Allora è abeliano, ed è isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ o a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione. Innanzitutto è immediato vedere che G deve essere abeliano. Infatti il centro di G può avere cardinalità o 1 o p o p^2.

Il primo caso è negato dal risultato precedente.

Il secondo è negato dal fatto che il centro avrebbe indice un primo, cosa impossibile.

Quindi $Z(G)$ ha ordine p^2 e coincide con G, che quindi è abeliano.

Sia a questo punto un g in G diverso dall'identità.

Se h ha ordine p^2 allora G è ciclico.

Altrimenti deve avere ordine p, e possiamo considerare un k in $G \setminus \langle h \rangle$ diverso dall'identità.

Se k ha ordine p^2 abbiamo di nuovo concluso.

Altrimenti siano $H = \langle h \rangle$ e $K = \langle k \rangle$. La loro intersezione è banale. Infatti l'intersezione è un sottogruppo di ordine 1 o p. L'ultima è negata in quanto k non appartiene al generato da h. Quindi

$$|HK| = \frac{|H||K|}{|H \cap K|} = p^2$$

e HK coincide con G. Inoltre HK è certamente contenuto in $\langle h, k \rangle$, che quindi deve anch'esso coincidere con G.

Allora se ricordiamo l'isomorfismo

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \left\langle x, y \,\middle|\, [x, y] = xyx^{-1}y^{-1} = 1 \right\rangle$$

possiamo considerare

$$\begin{aligned} \varphi \colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} &\to G \\ x &\mapsto h \\ y &\mapsto k \end{aligned}$$

Essendo che h e k commutano e generano, allora la mappa è un omomorfismo suggettivo. Infine per cardinalità è un isomorfismo. □

Andiamo ad enunciare il prossimo interessante fatto sui p-gruppi. Sappiamo che un gruppo ciclico ammette sottogruppi di ogni ordine "ammissibile". Osserviamo che questo è vero anche per i p-gruppi, e anzi vale un risultato più forte.

Teorema 3.15.3. *Sia G un p-gruppo di cardinalità p^n. Allora esiste una catena di sottogruppi*

$$\{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{i-1} \trianglelefteq H_n = G$$

tale che H_i ha cardinalità p^i ed è normale in G.

Dimostrazione. Procediamo per induzione forte su n.

Se $n = 1$, allora $\{e\} \trianglelefteq H_1 = G$ è la nostra catena.

Preso $n \geq 2$, allora dividiamo la trattazione in due casi.

Se G è abeliano, allora preso x in G di ordine p, il sottogruppo $\langle x \rangle$ è normale e $G/\langle x \rangle$ è un gruppo di ordine p^{n-1} abeliano. Per ipotesi induttiva esiste una catena

$$\{\bar{e}\} \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_{n-1} = G/\langle x \rangle$$

con $|K_i| = p^i$ e normali in $G/\langle x \rangle$.

Grazie al teorema di corrispondenza fra sottogruppi si può scrivere come

$$\{\bar{e}\} \trianglelefteq H_2/\langle x \rangle \trianglelefteq \cdots \trianglelefteq H_n/\langle x \rangle = G/\langle x \rangle$$

Sempre grazie al teorema di corrispondenza, possiamo affermare di aver trovato $H_1, \dots H_{n-1}$ normali in G tali che

$$\{e\} \trianglelefteq \langle x \rangle = H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

Se invece G non è abeliano, possiamo comunque considerare il centro $Z(G)$, diverso da G e non banale essendo G un p-gruppo. Quindi $G/Z(G)$ è un gruppo di ordine p^l con l compreso tra 1 e $n-1$. Per ipotesi induttiva possiamo quindi trovare una catena della forma

$$\{\bar{e}\} \trianglelefteq H_{1+l}/Z(G) \trianglelefteq \cdots \trianglelefteq H_n/Z(G) = G/Z(G)$$

con $|H_i| = p^i$, che corrisponde alla catena

$$Z(G) = H_l \trianglelefteq H_{l+1} \trianglelefteq \cdots \trianglelefteq H_n = G$$

con H_i normali in G.

Infine essendo $Z(G)$ abeliano, esiste una catena associata

$$\{e\} \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{l-1} \trianglelefteq H_l = Z(G)$$

con H_i normali in $Z(G)$.

Infine se i è compreso fra 1 e l, allora H_i è normale in $Z(G)$, che è caratteristico in G. Quindi gli H_i sono normali anche in G. □

Chiudiamo ora con un fatto estremamente importante, che ci sarà utile per la classificazione dei gruppi abeliani finiti. Preannunciamo però questo lemma di carattere generale:

Lemma 3.15.4. *Sia G un gruppo e H un suo sottogruppo normale. Allora per ogni K compreso tra H e K vale che*

$$N_{G/H}(K/H) = \pi(N_G(K))$$

Dimostrazione. ($\supseteq$) Certamente se $gKg^{-1} = K$, allora

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

($\subseteq$) D'altra parte preso $\pi(g)$ tale che per ogni k in K, $\pi(g)\pi(k)\pi^{-1}$ appartiene a K, allora abbiamo le seguenti implicazioni (ricordiamo che H è incluso in K)

$$\begin{aligned}
&\forall k \in K\ \exists k' \in K \text{ t.c. } \pi(gkg^{-1}) = \pi(k') \\
\Rightarrow &\forall k \in K\ \exists k' \in K, h \in H \text{ t.c. } gkg^{-1} = k'h \\
\Rightarrow &\forall k \in K\ \exists k'' \in K \text{ t.c. } gkg^{-1} = k'' \\
\Rightarrow &gKg^{-1} = K
\end{aligned}$$

□

Teorema 3.15.5. *Sia G un p-gruppo re H un sottogruppo proprio. Allora il normalizzatore $N_G(H)$ non può coincidere con H.*

Dimostrazione. Andiamo per induzione su n tale che $p^n = |G|$.

Per $n = 1$, allora il gruppo è isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Esso ammette $\{e\}$ come unico sottogruppo non banale, il cui normalizzatore è l'intero gruppo.

Se $n > 1$, allora consideriamo il centralizzatore $Z = Z(G)$. Se non è contenuto il H, allora abbiamo trovato un elemento del normalizzatore che non sta in H, in quanto $Z(G)$ è contenuto nel normalizzatore di ogni sottogruppo.

Se invece il centro è contenuto in H, allora possiamo quozientare per Z che è proprio. Allora $G/Z(G)$ ha cardinalità minore di p^n. Inoltre per il teorema di corrispondenza fra sottogruppi $\pi(H)$ è un sottogruppo proprio del quoziente. Quindi non può coincidere col normalizzatore.

Infine per il lemma precedente $\pi(N_G(H)) = N_{G/Z}(H/Z)$. Quindi sempre per il teorema di corrispondenza $N_G(H)$ non coincide con H.

□

3.16 Il Gruppo S_n

Procediamo a trattare un insieme di gruppi molto importante: i gruppi simmetrici S_n. Ricordiamo la definizione:

Definizione 3.16.1. Indichiamo con S_n il gruppo delle permutazioni di n elementi.

A questo punto è fondamentale introdurre il concetto di ciclo e permutazioni cicliche.

Notiamo quindi che il gruppo S_n agisce sull'insieme $\{ 1, \dots, n \}$. In particolare preso un elemento x di $\mathbb{N}_n$, allora

$$\mathrm{orb}(x) = \left\{ x, \sigma(x), \dots, \sigma^{k-1}(x) \right\}$$

con k pari a

$$k = \min \left\{ h \geq 1 \;\middle|\; \sigma^h(x) = x \right\}$$

Chiamiamo *ciclo* l'orbita di x ordinata, cioè la k-upla $(x, \sigma(x), \dots, \sigma^{k-1}(x))$. Ogni ciclo ammette k scritture differenti, date dalla scelta arbitraria del primo elemento.

Inoltre ogni permutazione σ è determinata dai suoi cicli, e quindi si può usare la notazione

$$\sigma = (x_1, \dots, \sigma^{k_1-1}(x_1)) \dots (x_h, \dots, \sigma^{k_h-1}(x_h))$$

Per esempio

$$\sigma = (1\,2\,3)(4\,5)(6\,7)(8)(9)$$

è la permutazione di S_9

$$1 \mapsto 2$$
$$2 \mapsto 3$$
$$3 \mapsto 1$$
$$4 \mapsto 5$$
$$5 \mapsto 4$$
$$6 \mapsto 7$$
$$7 \mapsto 6$$
$$8 \mapsto 8$$
$$9 \mapsto 9$$

Normalmente i cicli banali non vengono scritti, quindi σ è semplicemente

$$\sigma = (1\,2\,3)(4\,5)(6\,7)$$

Infine indichiamo con permutazioni cicliche le permutazioni composte da un unico ciclo. Notiamo che possiamo comporre i cicli come fossero permutazioni, nel senso che nella σ precedente, la giustapposizione di cicli si può intendere come vera e propria composizione

$$\sigma_1 = (1\,2\,3)$$
$$\sigma_2 = (4\,5)$$
$$\sigma_3 = (6\,7)$$
$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$$

Infine notiamo che cicli disgiunti banalmente commutano. Quindi una qualsiasi permutazione si scrive in modo "unico" come prodotto di cicli, cioè a meno di scambio di essi o riscritture in forma equivalente.

Quindi S_n è generato dalle permutazioni cicliche, ed è utile la seguente formula:

$$|\{\, \sigma \in S_n \mid \sigma \text{ } k\text{-ciclo} \,\}| = \binom{n}{k}\frac{k!}{k} = \binom{n}{k}(k-1)!$$

Data dal fatto che un k-ciclo è determinato una volta scelti i suoi k elementi, averne scelto l'ordine, e aver contato il fatto che un k-ciclo ammette k scritture equivalenti.

Essendo che ogni ciclo si scompone come prodotto di cicli $\sigma_1 \circ \cdots \circ \sigma_n$, è utile a seguente proposizione

Teorema 3.16.2. *Sia σ permutazione scomposto in cicli disgiunti*

$$\sigma = (i_{1,1} \ \dots \ i_{1,k_1}) \dots (i_{n,1} \ \dots \ i_{n,k_n})$$

Allora l'ordine di σ è $mcm(k_1, \dots, k_n)$.

Dimostrazione. Sia d il minimo comune multiplo. Allora essendo i cicli disgiunti

$$\sigma^d = (\sigma_1 \circ \cdots \circ \sigma_n)^d = \sigma_1^d \circ \cdots \circ \sigma_n^d = id$$

Quindi l'ordine di σ divide d.

D'altra parte dal fatto che $\sigma^d = id$ e sapendo che i cicli sono disgiunti, deve essere che $\sigma_i^d = id$ per ogni i. Quindi d è multiplo dei vari k_i e quindi anche del loro minimo comune multiplo. □

Il gruppo S_n da cosa è generato? La prossima proposizione lo afferma

Proposizione 3.16.3. *Il gruppo S_n è generato dai seguenti insiemi*

$$H_1 = \{ (i, j) \mid 1 \leq i, j \leq n \}$$
$$H_2 = \{ (1, i) \mid 1 \leq i \leq n \}$$
$$H_3 = \{ (i, i+1) \mid 1 \leq i \leq n-1 \}$$
$$H_4 = \{ (1, 2), (1, \dots, n) \}$$

Dimostrazione. Sappiamo già che S_n è generato dai cicli. Dobbiamo dimostrare che ogni ciclo si genera dai 2-cicli, dette anche trasposizioni. Infatti si osserva che

$$(1, \dots, k) = (1, k) \dots (1, 2)$$

Quindi H_1 e H_2 generano. Dimostriamo che ogni elemento di H_2 si può costruire tramite H_3. Infatti $(1, 2)$ appartiene a H_3 per costruzione. Inoltre

$$(1, i+1) = (i, i+1)(1, i)(i, i+1)$$

Infine H_4 genera gli elementi di H_3. Infatti

$$(1, \dots, n)^i (1, 2) (1, \dots, n)^{-i}$$ □

Andiamo ora a definire un importante caratteristiche delle permutazioni: il segno.

Definizione 3.16.4. Sia una permutazione di $S_n = S(\{1, \dots, n\})$. Definiamo il suo segno come il numero reale

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Proposizione 3.16.5. *Il segno è un omomorfismo suggettivo tra S_n e $\{\pm 1\} \simeq \mathbb{Z}/3\mathbb{Z}^*$.*

Dimostrazione. Verifichiamo che sia un omomorfismo da S_n a $\mathbb{R}^*$. Prese σ e τ permutazioni allora

$$\begin{aligned}
\operatorname{sgn}(\sigma \circ \tau) &= \prod_{1 \le i < j \le n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} \\
&= \prod_{1 \le i < j \le n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \frac{\tau(i) - \tau(j)}{i - j} \\
&= \prod_{1 \le i' < j' \le n} \frac{\sigma(i') - \sigma(j')}{i' - j'} \prod_{1 \le i < j \le n} \frac{\tau(i) - \tau(j)}{i - j} \\
&= \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau)
\end{aligned}$$

Quindi dobbiamo verificare semplicemente che $\operatorname{sgn}(\tau)$ appartenga a $\{\pm 1\}$ per ogni trasposizione τ. A questo punto usando il fatto che le trasposizioni generano S_n e che sgn è un omomorfismo concludiamo.

Sia quindi una trasposizione $\tau = (h, k)$ con $h < k$. Allora notiamo subito che la funzione segno eseguiamo un prodotto sulle coppie (i, j) con $i < j$. Questo è equivalente ad eseguire il prodotto sulle paia $\{i, j\}$ con $i \neq j$. Infatti

$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{\tau(j) - \tau(i)}{j - i}$$

Consideriamo quindi l'insieme delle paia $\{(i, j)\}_{i \neq j}$, e partizionamolo nel seguente modo:

1. Abbiamo il caso in cui $\{i, j\}$ e $\{h, k\}$ sono disgiunti. Allora

$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{i - j}{i - j} = 1$$

2. Se accoppiamo gli elementi del tipo $\{i,h\}$ e $\{i,k\}$ con $i \neq h,k$, otteniamo

$$\frac{\tau(i)-\tau(h)}{i-h}\frac{\tau(i)-\tau(k)}{i-k} = \frac{i-k}{i-h}\frac{i-h}{i-k} = 1$$

3. Infine se consideriamo $\{i,j\} = \{h,k\}$ allora

$$\frac{\tau(h)-\tau(k)}{h-k} = \frac{k-h}{h-k} = -1$$

Quindi mettendo tutto insieme otteniamo

$$\operatorname{sgn}(\tau) = \prod_{i,j\, i\neq j} \frac{\tau(i)-\tau(j)}{i-j} = -1$$

□

Corollario 3.16.6. *Sia σ in S_n. Se $\sigma = \tau_1 \circ \cdots \circ \tau_k$, allora* $\operatorname{sgn}(\sigma) = (-1)^k$.

Il segno è un omomorfismo. Quindi possiamo tranquillamente considerare il suo nucleo. Questo porta alla definizione di *gruppo alterno o alternante.*

Definizione 3.16.7. Definiamo l'ennesimo gruppo alterno A_n come il nucleo dell'omomorfismo segno su S_n.

Proposizione 3.16.8. *Il gruppo alterno A_n ha ordine* 1 *se $n = 1$; altrimenti ha ordine $n!/2$.*

Dimostrazione. L'applicazione segno, che ha codominio pari a $\{\pm 1\}$, può avere immagine di ordine uno o due. Se n è almeno 2, allora la trasposizione (1, 2) ha segno -1. Quindi l'immagine ha ordine 2, e A_n ha cardinalità

$$|A_n| = |\operatorname{Ker}(\operatorname{sgn})| = \frac{|S_n|}{2} = \frac{n!}{2}$$

□

Concludiamo questa trattazione con le classi di coniugio in S_n, un argomento molto potente.

In generale dato un elemento di un gruppo G, non è facile determinare i suoi coniugati. Nel caso di S_n la faccenda si fa estremamente più facile

Teorema 3.16.9. *Sia σ in S_n, e supponiamo che si scomponga in cicli $\sigma_1, \ldots, \sigma_t$ di lunghezza $k_1, \ldots, k_t$. Definiamo il tipo di σ come la stringa*

$$\text{type}(\sigma) = (k_1, \ldots, k_t)$$

Allora i coniugati di σ sono tutti e sole le permutazioni dello stesso tipo.

Dimostrazione. Consideriamo un coniugato $\lambda = \tau\sigma\tau^{-1}$, con

$$\sigma = (i_{1,1} \ \ldots \ i_{1,k_1}) \ldots (i_{t,1} \ \ldots \ i_{t,k_n})$$

Allora è immediato che

$$\lambda = (\tau(i_{1,1}) \ \ldots \ \tau(i_{1,k_1})) \ldots (\tau(i_{t,1}) \ \ldots \ \tau(i_{t,k_t}))$$

e quindi λ e σ hanno lo stesso tipo.

Viceversa supponiamo che λ abbia lo stesso tipo di σ. Cioè supponiamo che λ si scriva come

$$\lambda = (j_{1,1} \ \ldots \ j_{1,k_1}) \ldots (j_{t,1} \ \ldots \ j_{t,k_t})$$

Allora posta τ che manda $i_{h,k}$ in $j_{h,k}$, è evidente, per l'osservazione precedente, che $\tau\sigma\tau^{-1} = \lambda$. □

Corollario 3.16.10. *Il numero di classi di coniugio di S_n è pari a*

$$|\{ \mathcal{C}_\sigma \mid \sigma \in S_n \}| = p(n)$$

dove $p(n)$ sono le partizioni di n, cioè il numero di modi di scrivere n come somma di naturali decrescenti.

Chiudiamo questa sezione con un teorema che ci permette di avere qualche strumento in più per la classificazione dei gruppi.

Teorema 3.16.11. *Sia un gruppo di ordine $2d$ con d dispari. Allora ammette un sottogruppo di indice 2 (e quindi normale).*

Dimostrazione. Il segreto consiste nell'analizzare meglio il teorema di Cayley.

Preso un g in G, allora la sua permutazione associata $\varphi_g \in S(G)$ ammette una scrittura in cicli. Per identificarla notiamo che preso un qualsiasi h in G, allora

$$\varphi_g^k(h) = g^k h$$

e coincide con h se e solo se $g^k = e$.

Quindi è evidente come la scomposizione in cicli di φ_g è costituita da cicli di lunghezza pari a l'ordine di g. Essi inoltre sono $|G|/\operatorname{ord}(g)$.

A questo punto basta considerare l'immersione Φ di G in $S(G)$, e dimostrare che $\Phi(G)$ ammette un sottogruppo di ordine d.

Il sottogruppo A_{2d} è il nucleo dell'applicazione segno su S_{2d}. Quindi $A_{2d} \cap \Phi(G)$ è il nucleo dell'applicazione segno ristretta a $\Phi(G)$. A questo punto dobbiamo solamente dimostrare che $\operatorname{sgn}|_{\Phi(G)}$ ha immagine $\{\pm 1\}$.

Notiamo però che G ammette un elemento g di ordine 2 per il teorema di Cauchy. Quindi φ_g si scompone come $|G|/2 = d$ trasposizioni. Ergo ha segno $(-1)^d = -1$ e l'applicazione $\operatorname{sgn}|_{\Phi(G)}$ ha immagine $\{\pm 1\}$.

Quindi $\Phi(G) \cap A_{2d}$ è il sottogruppo di $\Phi(G)$ cercato:

$$|\Phi(G) \cap A_{2d}| = |\operatorname{Ker}(\operatorname{sgn}|_{\Phi(G)})| = \frac{|\Phi(G)|}{2} \qquad \square$$

Sullo stesso spirito della conclusione della scorsa dimostrazione, proviamo una proposizione che ci sarà di grande aiuto.

Proposizione 3.16.12. *Sia un naturale $n \geq 2$, e consideriamo un sottogruppo $H \leq S_n$. Allora o H è contenuto in A_n, o $|H \cap A_n|$ è pari a $|H|/2$.*

Dimostrazione. Per definizione di A_n sappiamo che

$$|H \cap A_n| = |\operatorname{Ker}(\operatorname{sgn}|_H)| = \frac{|H|}{|\operatorname{Im}(\operatorname{sgn}|_H)|}.$$

Siccome sgn è a immagine in $\{\pm 1\}$, allora $|H \cap A_n|$ può solamente essere o $|H|$ o $|H|/2$. $\square$

3.17 Sottogruppo Derivato

Questa breve sezione ha lo scopo di introdurre il sottogruppo derivato, un concetto che sembra secondario, ma che riveste una grande importanza nella teoria dei gruppi risolubili. Iniziamo con la definizione di commutatore.

Definizione 3.17.1. Sian G un gruppo e siano x, y in G. Definisco il commutatore di x e y come

$$[x, y] = xyx^{-1}y^{-1}$$

Definizione 3.17.2. Sia G un gruppo. Definiamo il derivato di G come

$$D(G) = [G, G] = \langle [x, y] \,|\, x, y \in G \rangle$$

Inoltre definiamo la catena di derivati come

$$\begin{cases} D^0(G) = G \\ D^{i+1}(G) = D(D^i(G)) \end{cases}$$

Il derivato di un gruppo è importante per il seguente risultato:

Teorema 3.17.3. *Sia G un gruppo. Allora valgono le seguenti affermazioni*

1. *Il derivato di G è caratteristico in G.*
2. *Dato un sottogruppo normale di G, G/H è abeliano se e solo se H contiene $D(G)$.*

Dimostrazione. (1.) Sia un automorfismo f di G. Allora notiamo innanzitutto che per ogni commutatore $[x, y]$ vale

$$f([x, y]) = [f(x), f(y)^{-1}]$$

Ergo f manda l'insieme dei commutatori in se stesso suggettivamente. Ergo $f(D(G))$ coincide con $D(G)$.

(2.) Per ogni xH, yH in G/H valgono le seguenti catene di coimplicazioni

$$\begin{aligned} xHyH = yHxH &\Leftrightarrow (xy)H = (yx)H \\ &\Leftrightarrow (xyx^{-1}y^{-1})H = H \\ &\Leftrightarrow xyx^{-1}y^{-1} \in H \\ &\Leftrightarrow [x, y] \in H \end{aligned}$$

Quindi G/H è abeliano se e solo se il sottogruppo derivato è incluso in H. □

3.18 Prodotti Semidiretti

In questa sezione affronteremo un metodo essenziale per costruire gruppi a partire da gruppi di partenza: quello del prodotto semidiretto. Per arrivarci però è utile dire ancora alcune cose sui prodotti diretti. Iniziamo col seguente lemma

Lemma 3.18.1. *Sia G un gruppo e H, K due sottogruppi normali ad intersezione banale. Allora i rispettivi gruppi commutano, cioè $hk = kh$ per ogni h in H e k in K.*

Dimostrazione. Per ogni h in H e k in K consideriamo il prodotto $[h, k] = hkh^{-1}k^{-1}$. Allora notiamo che questo commutatore appartiene sia a H, in quanto khk^{-1} vi appartiene, e anche a K, in quanto vi appartiene hkh^{-1}. Avendo H e K intersezione banale, allora $[h, k]$ è banale e h, k commutano. □

Teorema 3.18.2. *Sia G un gruppo, e siano H e K due sottogruppi tali che*

1. $H, K \trianglelefteq G$
2. $HK = G$
3. $H \cap K = \{e\}$

Allora G è isomorfo al prodotto diretto $H \times K$.

Dimostrazione. Sia la mappa

$$\begin{aligned} \Phi \colon H \times K &\to G \\ (h, k) &\mapsto hk \end{aligned}$$

Essa è un omomorfismo (è essenziale il lemma precedente):

$$\Phi((h, k)(h', k')) = hh'kk' = hkh'k' = \Phi((h, k))\Phi((h', k'))$$

Inoltre è suggettiva, in quanto $HK = G$, ed è iniettiva. Infatti se $\Phi((h, k))$ è banale, allora hk è l'identità. cioè h e k sono uno l'inverso dell'altro e appartengono all'intersezione di H e K. Essendo essa banale, allora lo è anche (h, k). □

Osserviamo che questa costruzione riflette la seguente osservazione: se G è un prodotto diretto di gruppi $G_1 \times G_2$, allora $G_1 \times \{e\}$ e $\{e\} \times G_2$ soddisfano le condizione del teorema precedente.

Adesso vogliamo rispondere alla seguente domanda: e se solo uno dei due sottogruppi è normale, ma valgono comunque le altre condizioni? Allora la struttura associata diventa quella di prodotto semidiretto, che andiamo a definire.

Definizione 3.18.3. Siano H e K due gruppi, e sia φ un omomorfismo da K in $\mathrm{Aut}(H)$. Allora definiamo il prodotto semidiretto $H \rtimes_\varphi K$ come il gruppo avente come supporto $H \times K$, e come operazione la seguente:

$$(h,k)\cdot(h',k') = (h\cdot\varphi_k(h'), k\cdot k')$$

con $\varphi_k = \varphi(k)$.

Osserviamo che il prodotto semidiretto è diretto se e solo se $\varphi\colon K \to \mathrm{Aut}(H)$ è banale. Inoltre $H\times\{e\}$ è un sottogruppo normale, in quanto nucleo dell'omomorfismo

$$\begin{aligned}\pi\colon H\rtimes_\varphi K &\to K\\ (h,k) &\mapsto h\end{aligned}$$

Osserviamo che in generale $\{e\}\times K$ non è normale. Infatti se anche K fosse normale, allora $\{e\}\times K$ e $H\times\{e\}$ soddisfarebbero le condizioni del teorema precedente, e G si potrebbe scomporre in prodotto diretto. Tuttavia ovviamente esistono prodotti diretti non banali. Il primo esempio è un qualunque $\mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$; esistendo due soli gruppi di ordine 6, allora tutti i prodotti semidiretti non banali sono isomorfi a $D_3 = S_3$.

Infine se la mappa φ è chiara dal contesto, o se a meno di isomorfismo esiste un unico prodotto semidiretto non banale, allora indicheremo spesso $H\rtimes K$ sottointendendo la φ.

Procediamo col teorema di scomposizione di prodotto semidiretti:

Teorema 3.18.4. *Sia G un gruppo, e siano H e K due sottogruppi tali che*

1. $H \trianglelefteq G$
2. $HK = G$
3. $H\cap K = \{e\}$

Allora G è isomorfo al prodotto semidiretto $H\rtimes_\varphi K$, dove φ è l'azione di coniugio di K su H.

Dimostrazione. Come prima basta la seguente mappa:

$$\begin{aligned}\Phi\colon H\rtimes_\varphi K &\to G\\ (h,k) &\mapsto hk\end{aligned}$$

che è un omomorfismo:

$$\Phi((h,k)(h',k')) = \Phi((h\varphi_k(h'), kk')) = hkh'k^{-1}kk' = hkh'k' = \Phi((h,k))\Phi((h',k'))$$

Inoltre è suggettiva ed iniettiva per le stesse ragioni del teorema precedente. □

Osserviamo che se abbiamo un prodotto semidiretto $H \rtimes_\varphi H'$, e H, H' sono isomorfi a K, K', allora il prodotto semidiretto è isomorfo a $K \rtimes_\tau K'$, con τ una opportuna mappa. In generale se K, K' ammettono un "unico" prodotto semidiretto allora la si può sottintendere, altrimenti può non essere chiaro quale sia "concretamente" la τ giusta.

Proponiamo adesso alcuni esempi:

Proposizione 3.18.5. *Il gruppo simmetrico S_n è isomorfo a $A_n \rtimes \langle (1,\,2)\rangle$.*

Dimostrazione. Consideriamo i sottogruppi di A_n e $\langle (1,\,2)\rangle$ di S_n. Allora A_n è normale ed ha intersezione banale con $\langle (1,\,2)\rangle$. Infine il loro prodotto dà S_n. Infatti

$$|A_n \langle (1,\,2)\rangle| = \frac{|A_n|\,|\langle (1,\,2)\rangle|}{|A_n \cap \langle (1,\,2)\rangle|} = n!$$

Quindi valgono tutte le ipotesi necessarie e S_n è isomorfo a $A_n \rtimes \langle (1,\,2)\rangle$. □

Corollario 3.18.6. *Il gruppo S_n è isomorfo ad un $A_n \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.*

Proposizione 3.18.7. *Il gruppo diedrale D_n è isomorfo a $R_n \rtimes \langle s\rangle$.*

Dimostrazione. Analogo alla dimostrazione precedente. □

Corollario 3.18.8. *Il gruppo diedrale D_n è isomorfo ad un $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, e se $\mathbb{Z}/n\mathbb{Z}^*$ è ciclico allora è isomorfo all'unico prodotto semidiretto non banale.*

Dimostrazione. Sappiamo che D_n è isomorfo a un $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, con

$$\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}^*$$

Quindi se $\mathbb{Z}/n\mathbb{Z}^*$ è ciclico, allora ammette un unico elemento di ordine 2, e $\bar{1}$ può essere mandato nell'identità o in quell'elemento. Non essendo D_n abeliano, abbiamo solo la seconda opzione, che ci dà l'unico prodotto semidiretto. □

Abbiamo classificato i gruppi di ordine $2p$. In verità quello era un caso particolare dei gruppi di ordine pq, che adesso procederemo a classificare. Per farlo però è utile introdurre un criterio di isomorfismo per prodotti semidiretti.

Proposizione 3.18.9. *Siano N, H, A, B 4 gruppi e sia un prodotto semidiretto $N \rtimes_\varphi H$. Presi due isomorfismi $\sigma\colon H \to B$ e $\tau\colon N \to A$, allora $N \rtimes_\varphi H$ è isomorfo a $A \rtimes_\psi B$ con*

$$\begin{aligned} \psi\colon B &\to \mathrm{Aut}(A) \\ b &\mapsto \tau \circ (\varphi \circ \sigma^{-1})(b) \circ \tau^{-1} \end{aligned}$$

Dimostrazione. Consideriamo la mappa

$$\begin{aligned} \Phi\colon N \rtimes_\varphi H &\to A \rtimes_\psi B \\ (n,h) &\mapsto (\tau(n), \sigma(h)) \end{aligned}$$

Esso è in effetti un omomorfismo:

$$\begin{aligned} \Phi((n_1,h_1) *_1 (n_2,h_2)) &= \Phi((n_1\varphi_{h_1}(n_2), h_1h_2)) \\ &= (\tau(n_1)(\tau \circ \varphi_{h_1})(n_2), \sigma(h_1h_2)) \\ &= (\tau(n_1),\sigma(h_1)) *_2 (\tau(n_2),\sigma(h_2)) \\ &= \Phi((n_1,h_1)) *_2 \Phi((n_2,h_2)) \end{aligned}$$

Inoltre è banalmente suriettivo e iniettivo. □

Possiamo procedere a classificare i gruppi di ordine pq.

Teorema 3.18.10. *Siano p, q primi distinti con p minore di q.*

1. *Se p non divide $q-1$, allora $\mathbb{Z}/p\mathbb{Z}$ e $\mathbb{Z}/q\mathbb{Z}$ non ammettono prodotti semidiretti non banali. Altrimenti ne esiste almeno uno e sono tutti tra di loro isomorfi.*

2. *Ogni gruppo di ordine pq è isomorfo ad un prodotto semidiretto di $\mathbb{Z}/q\mathbb{Z}$ e $\mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione. Sia un prodotto semidiretto $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ con

$$\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/q\mathbb{Z}^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$$

Il generatore 1_p di $\mathbb{Z}/p\mathbb{Z}$ deve andare in un elemento di ordine 1 o p. Nel primo caso la mappa φ è banale e otteniamo il prodotto diretto $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ isomorfo a $\mathbb{Z}/pq\mathbb{Z}$.

Il secondo caso può succedere se p divide l'ordine dell'immagine, pari a $q-1$. In questo nell'immagine abbiamo $\varphi(p)$ elementi di ordine p. Dobbiamo dimostrare che tutti i prodotti semidiretti che si ottengono sono isomorfi.

Siano quindi α e β in $\mathbb{Z}/q\mathbb{Z}^*$ di ordine p e siano φ_α e φ_β le mappe che mandano 1_p in α e β rispettivamente.

Essendo che α e β sono dello stesso ordine, e usando il fatto che $\mathbb{Z}/q\mathbb{Z}$ è ciclico, otteniamo che esiste un k coprimo con p tale che $\beta = k\alpha$.

Dimostriamo che, posto l'automorfismo

$$\sigma \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$
$$[m] \mapsto k[m]$$

allora $\varphi_\beta = \varphi_\alpha \circ \sigma$. Per ogni $[m]$ in $\mathbb{Z}/p\mathbb{Z}$

$$\varphi_\beta([m]) = \beta[m] = k\alpha[m] = k\varphi_\alpha([m]) = \varphi_\alpha(k[m]) = (\varphi_\alpha \circ \sigma)([m])$$

Quindi φ_β coincide con $\varphi_\alpha \circ \sigma$, e i prodotti semidiretti dati da φ_α e φ_β sono isomorfi per il lemma precedente.

Il prossimo passo è dimostrare che ogni gruppo di ordine pq è isomorfo ad un prodotto semidiretto $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ (eventualmente banale).

Sia quindi un tale gruppo G. Allora ammette due elementi, h e k, di ordine p e q rispettivamente. Essi danno origine a due sottogruppi, H e K, di ordine p e q. Il sottogruppo K ha indice p, il più piccolo dei due primi. Quindi è normale.

Inoltre H e K hanno ordine coprimi, quindi hanno intersezione banale. Inoltre per cardinalità $HK = G$.

Quindi per il teorema di scomposizione G è isomorfo al prodotto semidiretto, tramite coniugio, tra K e H. Infine H e K sono isomorfi a $\mathbb{Z}/p\mathbb{Z}$ e $Z/q\mathbb{Z}$ rispettivamente. Quindi G è isomorfo ad un certo prodotto semidiretto $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$. - □

3.19 Gruppi Abeliani Finiti

Questa sezione ha il compito di dimostrare uno dei maggiori teoremi di classificazione possibili con la teoria di Algebra I: la classificazione dei gruppi abeliani finiti.

Teorema 3.19.1. *7 Un gruppo abeliano finito G si può decomporre come prodotto diretto di gruppi ciclici*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_{t-1}\mathbb{Z} \times \mathbb{Z}/n_t\mathbb{Z}$$

Inoltre la decomposizione è unica se si impone che n_{i+1} divide n_i per ogni i.

Per semplicità suddividiamo la dimostrazione in due teoremi, che hanno bisogno innanzitutto di questa definizione:

Definizione 3.19.2. Dato un gruppo G e un primo p, allora definiamo sottoinsieme di p-torsione, indicato con $G(p)$, come il sottoinsieme

$$G(p) = \left\{ g \in G \;\middle|\; \mathrm{ord}(g) = p^k, k \in \mathbb{N} \right\}$$

Esso in generale è un sottoinsieme, però nella nostra situazione vale il seguente lemma

Lemma 3.19.3. *Se G è un gruppo abeliano, allora $G(p)$ è un sottogruppo per ogni p primo; inoltre se G è finito esso è un p-sottogruppo.*

Dimostrazione. Preso un primo p, allora $\mathrm{ord}(e) = 1 = p^0$, e quindi $e \in G(p)$. Inoltre presi due elementi $x, y \in G(p)$ di ordine p^k, p^h, allora

$$(xy)^{p^{k+h}} = x^{p^{k+h}} y^{p^{h+k}} = e.$$

Quindi $\mathrm{ord}(xy) \,|\, p^{k+h}$, che implica che $xy \in G(p)$. Infine $G(p)$ è ovviamente chiuso per inverso.

Quindi abbiamo dimostrato che $G(p)$ è un sottogruppo di G.

Se oltre a essere abeliano, G è anche finito, otteniamo che $G(p)$ è finito di cardinalità $p_1^{e_1} \dots p_k^{e_k}$. Se per assurdo esistesse un $p_i \neq p$, allora per il teorema di Cauchy $G(p)$ ammetterebbe un elemento di ordine p_i, ma $G(p)$ contiene solo elementi di ordine potenze di p.

Quindi $G(p)$ è un p-sottogruppo, eventualmente banale.

□

Con questa definizione, possiamo enunciare i teoremi in cui separeremo la dimostrazione del teorema di struttura

Teorema 3.19.4. *Ogni gruppo abeliano finito G di cardinalità $|G| = p_1^{e_1} \dots p_s^{e_s}$ si scompone come prodotto dei suoi sottogruppi di p-torsione*

$$G \simeq G(p_1) \times G(p_2) \times \cdots \times G(p_{s-1}) \times G(p_s)$$

Inoltre a meno dell'ordine questa è l'unica scomposizione di G in p-sottogruppi di ordine coprimi.

Teorema 3.19.5. *Ogni p-gruppo abeliano finito G si scompone come prodotto diretto di gruppi ciclici*

$$G \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_{t-1}}\mathbb{Z} \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

La decomposizione è unica imponendo che $r_1 \geq r_2 \geq \cdots \geq r_{t-1} \geq r_t$.

Passiamo quindi a dimostrare questi teoremi

Dimostrazione 1. Sia G gruppo abeliano finito di ordine $|G| = n = p_1^{e_1} \dots p_s^{e_s}$. Dimostriamo prima l'esistenza della scomposizione poi l'unicità.
Esistenza Per l'esistenza procediamo per induzione su s.
($s = 1$) In questo caso G è un p-gruppo, e corrisponde al suo sottogruppo di p-torsione, cioè

$$G = G(p)$$

($s \geq 2$) In questo caso possiamo porre $n = mm'$, con m e m' coprimi e strettamente compresi tra 1 e n. Nello specifico poniamo

$$\begin{aligned} m &= p_1^{e_1} \dots p_i^{e_i} \\ m' &= p_{i+1}^{e_{i+1}} \dots p_s^{e_s} \qquad 1 < i < s \end{aligned}$$

Vogliamo ora dimostrare che $G \simeq mG \times m'G$. Per farlo notiamo che

1. Essendo G abeliano, allora $mG, m'G \trianglelefteq G$.

2. $mG + m'G = G$. Infatti essendo m e m' coprimi esistono $\alpha, \beta \in \mathbb{Z}$ tale che $\alpha m + \beta m' = 1$. Ma allora ogni $g \in G$ posso scriverlo come

   $$g = (\alpha m + \beta m')g = \alpha mg + \beta m'g = m\alpha g + m'\beta g = mg_\alpha + m'g_\beta \in mG + m'G$$

3. $mG \cap m'G = \{0\}$. Infatti sia $x \in mG \cap m'G$; allora $x = mg = m'g'$ con $g, g' \in G$.

   Ergo $m'x = m'mg = 0$ essendo che G ha ordine n. Equivalentemente $mx = 0$. Ma allora l'ordine di x divide m' e m, cioè l'ordine di x divide $(m, m') = 1$. Quindi abbiamo concluso che $x = 0$.

Quindi si ottiene che $G \simeq mG \times m'G$.

Detto questo poniamo

$$\begin{aligned} G_m &= \{\, g \in G \mid mg = 0 \,\} \\ G_{m'} &= \left\{\, g \in G \;\middle|\; m'g = 0 \,\right\} \end{aligned}$$

Vogliamo dimostrare che $mG = G_{m'}$ e $m'G = G_m$. Dimostriamo solo la prima uguaglianza, l'altra è analoga.

Innanzitutto $mG \subseteq G_{m'}$, infatti per ogni $x \in mG$ vale che $m'x = m'mg = ng = 0$.

D'altra parte $G_{m'} \subseteq mG$. Infatti sia $x \in G_{m'}$; per Bezout esistono $h, h' \in \mathbb{Z}$ tale che $mh + m'h' = 1$. Ma allora come prima

$$x = mhx + m'h'x = mhx + h'm'x = mhx \in mG$$

Quindi abbiamo ottenuto che

$$G \simeq mG \times m'G = G_{m'} \times G_m \simeq G_m \times G_{m'} \tag{3.3}$$

Da (3.3) si osserva che G_m e $G_{m'}$ hanno cardinalità rispettivamente m e m'. Infatti il teorema di Cauchy impone che la fattorizzazione della cardinalità di G_m contenga tutti e soli i primi che dividono m. Equivalentemente la fattorizzazione della cardinalità di $G_{m'}$ contiene tutti e soli i primi che dividono m'. Inoltre dall'isomorfismo (3.3) si ottiene che $|G| = |G_m||G_{m'}|$, e quindi che $|G_m| = m$ e $G_{m'} = m'$.

Con l'ultimo isomorfismo possiamo usare l'ipotesi induttiva. Infatti $1 < m, m' < n$, da cui:

$$G \simeq G_m(p_1) \times \cdots \times G_m(p_i) \times G_{m'}(p_{i+1}) \times \cdots \times G_{m'}(p_s)$$

Infine è da verificare che $G_m(p_j) = G(p_j)$ e $G_{m'} = G(p_j)$ per i relativi j. Ma questo è banalmente vero, infatti prendendo per semplicità la prima uguaglianza, sicuramente $G_m(p_j) \subseteq G(p_j)$. D'altra parte se $x \in G(p_j)$ allora $p_j^{e_j} x = 0$. Tuttavia $p_j^{e_j}$ divide m e quindi $mx = 0$, cioè $x \in G_m$.

Abbiamo quindi ottenuto l'isomorfismo cercato

$$G \simeq G(p_1) \times G(p_2) \times \cdots \times G(p_{s-1}) \times G(p_s)$$

Questo isomorfismo ci dice inoltre che $|G(p_i)| = p_i^{e_i}$.

Unicità Per dimostrare l'unicità, supponiamo che G si scomponga in un ulteriore modo oltre quello esposto prima:

$$\begin{aligned} G &\simeq G(p_1) \times \cdots \times G(p_s) \\ &\simeq H_1 \times \cdots \times H_f \qquad |H_i| = q_i^{\alpha_i} \ (q_i, q_j) = 1 \ \forall i \neq j \end{aligned}$$

Ma allora notiamo subito che possiamo scrivere $n = p_1^{e_1} \dots p_s^{e_s} = q_1^{\alpha_1} \dots q_f^{\alpha_f}$. Quindi per l'unicità della fattorizzazione si ottiene che $f = s$, e che $|H_i| = p_i^{e_i}$.

Ci siamo quindi ricondotti alla seguente situazione:

$$\begin{aligned} G &\simeq G(p_1) \times \cdots \times G(p_s) \\ &\simeq H_1 \times \cdots \times H_s \qquad |H_i| = p_i^{e_1} \end{aligned}$$

Per costruzione H_i è un p_i-sottogruppo, e quindi $H_i \leq G(p_i)$. Ma per cardinalità si ottiene che

$$H_i = G(p_i) \ \forall i = 1, \dots, s$$

che conclude anche la dimostrazione dell'unicità. □

Per la seconda dimostrazione serve il seguente lemma:

Lemma 3.19.6. *Sia G un p-gruppo abeliano e sia*

$$\mathcal{O}_G = \{\mathrm{ord}(g) \,|\, g \in G\}$$

Allora preso un qualsiasi $x_1 \in G$ tale che $\mathrm{ord}(x_1) = \max \mathcal{O}_G$, la seguente affermazione è vera:

$$\forall\, \bar{x} \in G/\langle x_1 \rangle \ \ \exists y \in \pi^{-1}(\bar{x}) \ t.c. \ \mathrm{ord}(y) = \mathrm{ord}(\bar{x})$$

Dimostrazione. Prima di incominciare la dimostrazione ricordiamo che essendo G un gruppo abeliano finito, allora $\max \mathcal{O}_G = \mathrm{mcm}\, \mathcal{O}_G$.

Sia quindi un p-gruppo abeliano G e sia x_1 come nelle ipotesi. Poniamo per comodità $H = G/\langle x_1 \rangle$.

Sia un qualunque $\bar{x} \in H$, e sia y un qualunque elemento di $\pi^{-1}(\bar{x})$. Esso si scrive come $y = x + ax_1$. Essendo G un p-gruppo, anche il quoziente è un p-gruppo, quindi possiamo porre $\mathrm{ord}(\bar{x}) = p^r, \mathrm{ord}(x_1) = p^{r_1}$.

Avendo $\bar{x}$ ordine p^r, allora $p^r x$ appartiene a $\langle x_1 \rangle$, cioè $p^r x = bx_1$ per qualche $b \in \mathbb{Z}$. Vogliamo dimostrare che p^r divide b.

Sappiamo che x_1 ha ordine massimo in G, quindi l'ordine di x divide p^{r_1}. Questo implica che

$$0 = p^{r_1} x = p^{r_1 - r} p^r x = p^{r_1 - r} b x_1$$

che a sua volta implica che

$$\begin{aligned} & p^{r_1} \mid p^{r_1 - r} b \\ \Rightarrow\ & p^r \mid b \\ \Rightarrow\ & b = p^r b_1 \end{aligned}$$

Detto questo, supponiamo che esista un y nella controimmagine di $\bar{x}$ di ordine p^r. Tentiamo di capire la forma di y.

Sappiamo innanzitutto che

$$\begin{aligned} 0 = p^r y = p^r x + p^r a x_1 \\ \Rightarrow p^r x = -p^r a x_1 \\ \Rightarrow b x_1 = -p^r a x_1 \end{aligned}$$

Questo è sicuramente verificato se $b = -p^r a$, cioè se $p^r b_1 = -p^r a$. Con questa condizione otteniamo che y è della forma $y = x - b_1 x_1$.

D'altra parte questa y funziona sempre, infatti:

$$p^r y = p^r x - p^r b_1 x_1 = b x_1 - b x_1 = 0$$

Quindi $y = x - b_1 x_1$ ha ordine che divide p^r. D'altra parte $\bar{x}$, immagine di y tramite π, ha ordine p^r. Quindi p^r divide l'ordine di y. □

Dimostrazione 2. Anche qua dimostriamo prima l'esistenza poi l'unicità.

Esistenza Sia $|G| = p^n$. Per questa dimostrazione useremo l'induzione su n. In particolare dimostriamo che esistono $y_1, \dots, y_t$ che generano G e tali che

$$\begin{aligned} \langle y_1 \rangle \times \cdots \times \langle y_t \rangle \to G \\ (a_1 y_1, \dots, a_t y_t) \mapsto a_1 y_1 + \cdots + a_t y_t \end{aligned}$$

sia un isomorfismo.

($n = 1$) In questo caso $|G| = p$ e $G \simeq \mathbb{Z}/p\mathbb{Z}$

($n \geq 2$) Sia p^{r_1} il massimo di $\mathcal{O}_G$ e sia x_1 un elemento di tale ordine.

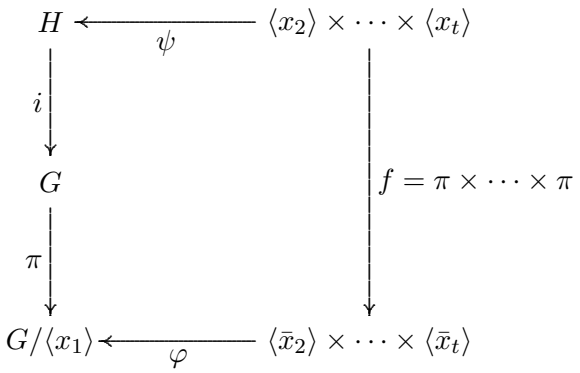
Se $r_1 = n$, allora G è ciclico e $|G| = \mathbb{Z}/p^n\mathbb{Z}$.

Se invece $0 < r_1 < n$, allora consideriamo $G/\langle x_1 \rangle$ di ordine p^{n-r_1}. Per ipotesi induttiva

$$G/\langle x_1 \rangle \overset{\varphi}{\simeq} \langle \bar{x}_2 \rangle \times \langle \bar{x}_3 \rangle \times \cdots \times \langle \bar{x}_t \rangle \quad \operatorname{ord}(\bar{x}_i) = p^{r_i} \quad r_2 \geq \cdots \geq r_t \tag{3.4}$$

Per il Lemma 3.19.6 posso supporre, senza perdita di generalità, che x_i abbia ordine p^{r_i} per ogni i.

Poniamo $H = \langle x_2, \dots, x_t \rangle$ e consideriamo il diagramma commutativo



con ψ la mappa

$$\begin{aligned}\langle x_2\rangle \times \langle x_3\rangle \times \cdots \times \langle x_t\rangle &\to H\\ (a_2x_2, \ldots, a_tx_t) &\mapsto a_2x_2 + \cdots + a_tx_t\end{aligned}$$

La mappa f è un isomorfismo. Infatti è suggettiva e dominio e immagine hanno la stessa cardinalità grazie alla scelta degli x_i.

La mappa φ è un isomorfismo per costruzione.

Quindi $\varphi \circ f$ è un isomorfismo, ed è in particolar modo iniettiva. Quindi lo deve essere anche ψ, ed essendo banalmente suggettiva è un isomorfismo.

Infine concludiamo che anche l'ultima mappa $\pi \circ i$ deve essere un isomorfismo.

Ora dobbiamo ancora costruire G. Per farlo affermiamo che G è isomorfo al prodotto diretto di $\langle x_1\rangle$ e H. Infatti:

1. I sottoinsiemi $\langle x_1\rangle, H$ sono sottogruppi.

2. I sottogruppi $\langle x_1\rangle, H$ sono normali essendo G abeliano.

3. Sia $g \in \langle x_1\rangle \cap H$. Allora g si scrive come

$$g = a_1x_1 = a_2x_2 + \cdots + a_tx_t$$

e passando al quoziente si ottiene

$$\bar{g} = \bar{0} = a_2\bar{x}_2 + \cdots + a_t\bar{x}_t$$

Essendo $\pi|_H$ un isomorfismo si ottiene che $g = 0$.

4. $\langle x_1 \rangle + H = G$. Infatti per ogni $g \in G$ posso scrivere $\bar{g}$ come

$$\begin{aligned}
\bar{g} &= a_2\bar{x}_2 + \cdots + a_t\bar{x}_t \\
\bar{g} - a_2\bar{x}_2 + \cdots + a_t\bar{x}_t &= \bar{0} \\
g - a_2x_2 + \cdots + a_tx_t &\in \langle x_1 \rangle \\
g = a_1x_1 + a_2x_2 + \cdots + a_tx_t &\in \langle x_1 \rangle + H
\end{aligned}$$

Quindi per il teorema di scomposizione abbiamo un isomorfismo

$$G \simeq \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_t \rangle \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

che manda $a_1x_1 + \cdots + a_tx_t$ in $(a_1x_1, \ldots, a_tx_t)$.

Essendo che $r_1 \geq r_2 \geq \cdots \geq r_t$, abbiamo ottenuto il risultato.

Unicità Sia $|G| = p^n$ e procediamo anche qui per induzione.

($n = 1$) In questo caso $G \simeq \mathbb{Z}/p\mathbb{Z}$ e non può esserci un'altra decomposizione.

($n \geq 2$) Sia $|G| = p^n$ e supponiamo di poterlo decomporre in

$$\begin{aligned}
G &\simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_t}\mathbb{Z} \qquad r_1 \geq \cdots \geq r_t \\
&\simeq \mathbb{Z}/p^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{k_h}\mathbb{Z} \qquad k_1 \geq \cdots \geq k_k
\end{aligned}$$

Innanzitutto notiamo che preso

$$G_p = \{\, g \in G \mid \operatorname{ord}(g) \mid p \,\}$$

allora

$$(\mathbb{Z}/p\mathbb{Z})^t \simeq G_p \simeq (\mathbb{Z}/p\mathbb{Z})^h$$

Quindi $t = h$.

D'altra parte possiamo considerare il sottogruppo pG. Dal primo teorema di omomorfismo otteniamo che

$$|pG| = \frac{|G|}{|G_p|} = p^{n-t} < p^n$$

E quindi osservando che

$$\begin{aligned}
pG &\simeq p\frac{\mathbb{Z}}{p^{r_1}\mathbb{Z}} \times \cdots \times p\frac{\mathbb{Z}}{p^{r_t}\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p^{r_1-1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p^{r_t-1}\mathbb{Z}} \\
&\simeq p\frac{\mathbb{Z}}{p^{k_1}\mathbb{Z}} \times \cdots \times p\frac{\mathbb{Z}}{p^{k_t}\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p^{k_1-1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p^{k_t-1}\mathbb{Z}}
\end{aligned}$$

otteniamo per induzione che $r_i = k_i \ \forall i = 1, \ldots, t$, cioè che la decomposizione è unica. □

Dimostrato anche il secondo teorema, possiamo andare a dimostrare il teorema di struttura.

Dimostrazione del Teorema di Struttura. Dividiamo come prima in esistenza ed unicità

Esistenza Sia G un gruppo finito di cardinalità $|G| = p_1^{e_1} \dots p_s^{e_s}$. Allora per il Teorema 3.19.4 possiamo decomporre G come

$$G \simeq G(p_1) \times \cdots \times G(p_s)$$

e grazie al Teorema 3.19.5 possiamo decomporlo ulteriormente come

$$G \simeq \prod_{j=1}^{t_1} \mathbb{Z}/p_1^{r_{1,j}}\mathbb{Z} \times \cdots \times \prod_{j=1}^{t_s} \mathbb{Z}/p_s^{r_{1,j}}\mathbb{Z}$$

con

$$r_{i,1} \geq r_{i,2} \geq \cdots \geq r_{i,t_i} \ \forall i = 1, \dots, s$$

Eventualmente, ponendo dei gruppi banali, posso considerare $t = \max\{t_1, \dots, t_n\}$ e porre $t_1 = \cdots = t_s = t$. Ma allora unendo i gruppi ciclici nel modo appropriato si ottiene

$$\begin{aligned} G &\simeq \mathbb{Z}/(p_1^{r_{1,1}} \dots \ p_s^{r_{s,1}})\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_1^{r_{1,t}} \dots \ p_s^{r_{s,t}})\mathbb{Z} \\ &= \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z} \end{aligned}$$

con $n_{i+1} \mid n_i \ \forall i = 1, \dots, t$. Abbiamo quindi dimostrato l'esistenza della decomposizione. Guardiamo ora l'unicità

Unicità Se per assurdo G si decomponesse in modi differenti, allora possiamo usare l'unicità nel Teorema 3.19.3 per trovare scomposizioni differenti dei gruppi di p-torsione. Ma il grazie al Teorema 3.19.6 otteniamo l'assurdo. □

Sappiamo che un gruppo ciclico ammette elementi e sottogruppi di ogni ordine che divide l'ordine del gruppo. Sappiamo che preso un gruppo non ciclico allora non esistono elementi di ordine l'ordine del gruppo. Tuttavia non è ancora chiaro quando esistono sottogruppi di un determinato ordine. Grazie al teorema di struttura sappiamo che per trovare controesempi bisogna guardare oltre i gruppi abeliani, ed in generale bisogna uscire dalla seguente classe di gruppi:

Teorema 3.19.7. *Siano $\{G_i\}_{i=1}^s$ p_i-gruppi e sia G il loro prodotto diretto. Allora per ogni divisore dell'ordine di G, esiste un sottogruppi di tale ordine.*

Dimostrazione. Sia la cardinalità di G

$$|G| = n = p_1^{e_1} \dots p_s^{e_s}$$

e sia un suo divisore

$$d = p_1^{f_1} \dots p_s^{f_s} \quad f_i \leq e_i$$

Allora per ogni G_i, esiste un suo sottogruppo H_i di ordine $p_i^{f_i}$. Ergo $H = H_1 \times \cdots \times H_s$ è il sottogruppo di G di ordine cercato. □

Corollario 3.19.8. *Preso un gruppo abeliano finito G, allora per ogni divisore d del suo ordine esiste un sottogruppo di ordine d.*

Dimostrazione. Essendo che G è isomorfo al prodotto diretto dei suoi sottogruppi di torsione, che sono p-gruppi, possiamo applicare il teorema precedente. □

3.20 Teoremi di Sylow

Riprendiamo la domanda della sezione precedente: cosa possiamo dire sull'ordine dei sottogruppi di un gruppo G? Per ora sappiamo solo che certi gruppi ammettono sottogruppi di ogni ordine "ammissibile". Questo non è sempre vero. Dimostriamo infatti che A_4 non ammette sottogruppi di ordine 6. Per farlo però dobbiamo enunciare un importante risultato sulle classi di coniugio in A_n.

Teorema 3.20.1. *Sia σ in A_n. Allora possono verificarsi due casi*

1. *Se il centralizzatore di σ in S_n è costituito solo da permutazioni pari, allora i coniugati di σ, come elemento di A_n, sono la metà dei coniugati di σ come elemento di S_n.*

2. *Se il centralizzatore di σ in S_n ammette una permutazione dispari, allora i coniugati di σ in A_n sono tutti e soli quelli in S_n.*

Dimostrazione. Poniamo le due classi di coniugio di σ

$$\mathcal{C}_\sigma^{(S_n)} = \left\{ \tau \in S_n \;\middle|\; \exists \rho \in S_n \text{ t.c. } \rho\sigma\rho^{-1} = \tau \right\}$$
$$\mathcal{C}_\sigma^{(A_n)} = \left\{ \tau \in A_n \;\middle|\; \exists \rho \in A_n \text{ t.c. } \rho\sigma\rho^{-1} = \tau \right\}$$

Notando allora che

$$Z_{A_n}(\sigma) = Z_{S_n}(\sigma) \cap A_n$$

otteniamo nel primo caso

$$|\mathcal{C}_\sigma^{(A_n)}| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|S_n|}{2|Z_{S_n}(\sigma)|} = \frac{1}{2}\,|\mathcal{C}_\sigma^{(S_n)}|$$

mentre nel secondo

$$|\mathcal{C}_\sigma^{(A_n)}| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{2|S_n|}{2|Z_{S_n}(\sigma)|} = |\mathcal{C}_\sigma^{(S_n)}|$$

Essendo che $\mathcal{C}_\sigma^{(A_n)}$ è sempre incluso in $\mathcal{C}_\sigma^{(S_n)}$ abbiamo concluso. □

Teorema 3.20.2. *Il gruppo A_4 non ammette sottogruppi di ordine 6.*

Dimostrazione. Supponiamo che esista un sottogruppo H di ordine 6. Allora per il teorema di Cauchy ammetterebbe un elemento di ordine 2. Essendo che gli unici elementi pari di ordine 2 in S_4 sono le doppie trasposizioni, allora H ammette una doppia trasposizione σ.

Il sottogruppo H è normale in A_4, avendo indice 2. Quindi contiene tutti i coniugati di σ in A_4. Se σ è $(a,\, b)(c,\, d)$, allora la trasposizione $(a\, b)$ appartiene al centralizzatore, che quindi ammette una trasposizione dispari. Ergo i coniugati di σ in A_n sono tutti e soli quelli in S_n, cioè sono tutte e sole le doppie trasposizioni. Ergo H contiene il sottoinsieme

$$K = \{e, (1,\, 2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

che tuttavia è un sottogruppo importante, il sottogruppo di A_4 detto sottogruppo di Klein. Quindi H conterrebbe un sottogruppo di ordine 4. Assurdo. □

Quindi esistono gruppi che non ammettono sottogruppi di un determinato ordine. I teoremi di Sylow hanno esattamente lo scopo di provare l'esistenza di certi determinate classi di sottogruppi: i sottogruppi di Sylow.

Definizione 3.20.3. Sia G un gruppo finito e p un primo tale che $p \,|\, |G|$. Posto $|G| = p^n m$ con $(p, m) = 1$, un p-sottogruppo di Sylow, o semplicemente p-Sylow, è un sottogruppo di ordine p^n.

Notiamo che il teorema di struttura per i gruppi abeliani ha come conseguenza che se G è un gruppo abeliano finito, allora gli unici p-Sylow sono i sottogruppi di p-torsione. In generale invece questo affermazione non è vera, e anzi per ogni p primo possono esistere diversi p-Sylow. I teoremi di Sylow permettono di fare luce sui gruppi non abeliani finiti.

Andiamo quindi a dimostrare i teoremi di Sylow.

Teorema 3.20.4 (Teoremi di Sylow)**.** *Sia G un gruppo finito e sia p un primo tale che $p \,|\, |G|$. Inoltre sia $|G| = p^n m$ con $(p, m) = 1$. Allora valgono le seguenti affermazioni*

1. *Esistenza: Per ogni $1 \leq \alpha \leq n$ esiste un sottogruppo H tale che $|H| = p^\alpha$.*
2. *Prima Inclusione: Ogni p-sottogruppo è contenuto in un p-Sylow.*
3. *Coniugio: Due qualunque p-Sylow sono couniugati.*
4. *Seconda Inclusione: Per ogni $1 \leq \alpha \leq n-1$, ogni sottogruppo di ordine p^α è contenuto in un sottogruppo di ordine $p^{\alpha+1}$.*
5. *Numero: Sia n_p il numero di p-Sylow di G. Allora*
   - $n_p \,|\, |G|$
   - $n_p \equiv 1 \pmod{p}$

Dimostrazione. (Esistenza) Iniziamo con dimostrare l'esistenza dei p-sottogruppi per ogni ordine. Definiamo innanzitutto per ogni $1 \leq \alpha \leq n$

$$M_\alpha = \{\, X \in P(G) \mid |X| = p^\alpha \,\}$$

Chiaramente

$$|M_\alpha| = \binom{p^n m}{p^\alpha} = \prod_{i=0}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$$

Ora vogliamo dimostrare che p non divide

$$\prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$$

Per fare ciò consideriamo la valutazione p-adica v_p. Allora per ogni i compreso fra 1 re $p^\alpha - 1$ vale che

$$v_p(p^n m - i) = v_p(p^\alpha - i) = v_p(i)$$

e quindi

$$v_p\left[\prod_{i=1}^{p^\alpha-1}\frac{p^n m-i}{p^\alpha-i}\right]=\sum_{i=1}^{p^\alpha-1}v_p\left[\frac{p^n m-i}{p^\alpha-i}\right]=\sum_{i=1}^{p^\alpha-1}v_p(p^n m-i)-v_p(p^\alpha-i)=0$$

che equivale proprio a quello che volevamo dimostrare. Quindi abbiamo ottenuto che

$$v_p(|M_\alpha|)=n-\alpha$$

A questo punto consideriamo la seguente azione $\varphi\in\mathcal{A}(G,M_\alpha)$

$$\begin{aligned}\varphi\colon G&\to S(M_\alpha)\\ g&\mapsto \varphi_g\colon H\mapsto gH\end{aligned}$$

Per la formula orbita-stabilizzatore otteniamo

$$|M_\alpha|=\left|\bigcup_{i=1}^{s}\mathrm{orb}(H_i)\right|=\sum_{i=1}^{s}\frac{|G|}{|\mathrm{Stab}(H_i)|}=\sum_{i=1}^{s}\frac{p^n m}{|\mathrm{Stab}(H_i)|}$$

Sapendo che $v_p(M_\alpha)=n-\alpha$, concludiamo che deve esistere un certo $i_0\in\{1,\dots,s\}$ tale che

$$p^{n-\alpha+1}\nmid|\mathrm{orb}(H_{i_0})|=\frac{p^n m}{|\mathrm{Stab}(H_{i_0})|}$$

e quindi deve esistere un $i_0\in\{1,\dots,s\}$ tale che $p^\alpha\,|\,|\mathrm{Stab}(H_{i_0})|$.

Cioè abbiamo trovato un sottogruppo, $\mathrm{Stab}(H_{i_0})$, di ordine maggiore o uguale a p^α. Per concludere dobbiamo dimostrare la disuguaglianza opposta. Sia quindi un $x\in H_{i_0}$ e sia la seguente funzione

$$\begin{aligned}\psi\colon \mathrm{Stab}(H_{i_0})&\to H_{i_0}\\ y&\mapsto yx\end{aligned}$$

essa è iniettiva, quindi $|\mathrm{Stab}(H_{i_0})|\le|H_{i_0}|=p^\alpha$.

Quindi $\mathrm{Stab}(H_{i_0})$ è il nostro sottogruppo cercato.

(Prima Inclusione) Per dimostrare questa inclusione sia S un p-Sylow di G, che esiste per la parte precedente. Allora preso un sottogruppo H di ordine p^α, con $1\le\alpha\le n$, sia

$$X=\{\,gS\mid g\in G\,\}$$

Poniamo $|X|=\gamma$ e consideriamo l'azione $\varphi\in\mathcal{A}(H,X)$

$$\begin{aligned}\varphi\colon H&\to S(X)\\ h&\mapsto \varphi_h\colon gS\mapsto hgS\end{aligned}$$

Allora sempre per il teorema orbita-stabilizzatore

$$\gamma = |X| = \sum_{i=1}^{r} |\mathrm{orb}(g_i S)| = \sum_{i=1}^{r} \frac{|H|}{|\mathrm{Stab}(g_i S)|} = \sum_{i=1}^{r} p^{\alpha_i} \quad 0 \leq \alpha_i \leq \alpha$$

Ora ricordiamo che S è un p-Sylow. Questo implica, per il teorema di Lagrange, che $p \nmid \gamma$. Ma allora esiste un $i \in \{1, \ldots, r\}$ tale che $\mathrm{orb}(g_i S)$ è banale, cioè tale che $\mathrm{Stab}(g_i S) = H$.

Ma allora per ogni $h \in H$, $hg_i S = g_i S$, cioè $g_i^{-1} h g_i \in S$. Quindi $H \subseteq g_i S g_i^{-1}$, che è il p-Sylow cercato.

(Coniugio) Siano S_1, S_2 due p-Sylow. Allora se ripetiamo il procedimento di sopra con $S = S_2$ scopriamo che $S_1 \subseteq g S_2 g^{-1}$. Ma per cardinalità otteniamo che $S_1 = g S_2 g^{-1}$. Cioè S_1 e S_2 sono coniugati.

(Seconda Inclusione) Sia H un p-sottogruppo di ordine p^α, con α compresto tra 1 e $n-1$. Per la prima inclusione dimostrata esiste un p-Sylow S tale che $H \subsetneq S$. Inoltre sappiamo, per un risultato sui p-gruppi, che H non coincide con $N_S(H)$.

D'altra parte H è normale in $N_S(H)$. Quindi possiamo considerare il quoziente non banale $N_S(H)/H$. Essendo un p-gruppo esiste un $\overline{x}$ in $N_S(H)/H$ tale che $\mathrm{ord}(\overline{x}) = p$. Ma allora per il teorema di corrispondenza fra sottogruppi, se consideriamo $T = \pi^{-1}(\langle \overline{x} \rangle)$, otteniamo che $H \subseteq T$ e $|T| = p^{\alpha+1}$. Come volevasi dimostrare.

(Numero) Vogliamo dimostrare innanzitutto che n_p coincide con $[G : N_G(S)]$, con S un qualunque p-Sylow. Questo però è immediato, se consideriamo che tutti i p-Sylow sono coniugati per il punto precedente. Quindi sempre per il teorema orbita-stabilizzatore se prendiamo un p-Sylow S, allora

$$n_p = |\mathcal{C}_S| = \frac{|G|}{|N_G(S)|} = [G : N_G(S)]$$

Otteniamo quindi che n_p divide $|G|$, che era il primo fatto da dimostrare.

Dimostrato questo, consideriamo il seguente insieme X_p

$$X_p = \{\, S_i \leq G \mid S_i \text{ } p\text{-Sylow} \,\}$$

e la seguente azione $\varphi \in \mathcal{A}(S, X_p)$

$$\begin{aligned} \varphi \colon S &\to S(X_p) \\ s &\mapsto \varphi_s \colon S_i \mapsto s S_i s^{-1} \end{aligned}$$

Vogliamo dimostrare che φ ha una e unica orbita banale. Sicuramente $\text{orb}(S) = \{S\}$. D'altra parte supponiamo che esista un altro p-Sylow H tale che $\text{orb}(H) = \{H\}$. Certamente H e S sono contenuti in $N_G(H)$. Essendo H normale nel normalizzatore, allora SH è un sottogruppo di G di cardinalità

$$|SH| = \frac{|S||H|}{|S \cap H|} = \frac{p^n p^n}{p^k} = p^{2n-k}$$

con $k < n$. Essendo che $|SH|$ non divide l'ordine di G otteniamo l'assurdo.

Quindi c'è un unico p-Sylow di orbita banale. Gli altri p-Sylow hanno orbita di cardinalità divisore di S non banale. Quindi otteniamo che

$$n_p = |X_p| = \sum_{i=1}^{r} \text{orb}(S_i) + |\text{orb}(S)| = \sum_{i=1}^{r} p^{\beta_i} + 1 \equiv 1 \pmod{p} \quad 1 \leq \beta_i \leq n$$

che era quello che volevamo dimostrare. □

Grazie al fatto che tutti i p-Sylow sono coniugati otteniamo che è un p-Sylow è normale se e solo se è l'unico p-Sylow.

I teoremi di Sylow sono strumwnti importanti nella classificazione dei gruppi. Per dare un esempio consideriamo il prossimo teorema di classificazione: quelli dei gruppi di ordine 12. Per rendere più chiara la dimostrazione premettiamo i seguenti lemmi:

Lemma 3.20.5. *Il gruppo S_4 ammette A_4 come unico sottogruppo di ordine 12.*

Dimostrazione. Sia un sottogruppo H di S_4 di ordine 12. Se esso è incluso in A_4, allora per cardinalità coincidono. Altrimenti $H \cap A_4$ ha cardinalità pari a $12/2 = 6$. Tuttavia sappiamo che A_4 non ammette sottogruppi di ordine 6. □

Lemma 3.20.6. *Sia n dispari. Allora $D_n \times \mathbb{Z}/2\mathbb{Z}$ è isomorfo a D_{2n}.*

Dimostrazione. Sia G il nostro prodotto diretto. Allora possiamo considerare

$$\begin{aligned} \psi \colon D_{2n} &\to G \\ r_{2n} &\mapsto (r_n, 1) \\ s_{2n} &\mapsto (s_n, 0) \end{aligned}$$

La mappa è un omomorfismo ben definito, in quanto

$$(s_n, 0)(r_n, 1)(s_n, 0)^{-1} = (r_n, 1)^{-1}$$

Inoltre ψ è suggettiva. Infatti $(r_n, 1)$ ha ordine il minimo comune multiplo tra n e 2, che è $2n$. Quindi $\langle (r_n, 1) \rangle$ genera un sottogruppo H di ordine $2n$. Inoltre $K = \langle (s_n, 0) \rangle$ ha ordine 2. Essendo che H e K hanno intersezione banale, allora HK coincide con G per cardinalità. Quindi $(r_n, 1)$ e $(s_n, 0)$ generano G.

Infine per cardinalità è un isomorfismo. □

Lemma 3.20.7. *Siano A, B, C tre gruppi con $\mathrm{Aut}(C)$ abeliano. Allora posti due omomorfismi*

$$\varphi \colon A \to \mathrm{Aut}(C)$$
$$\psi \colon B \to \mathrm{Aut}(C)$$

con ψ nullo, vale l'isomorfismo

$$C \rtimes_{(\varphi,\psi)} (A \times B) \simeq (C \rtimes_{\varphi} A) \times B$$

con

$$(\varphi, \psi)_{(a,b)} = \tau_{(a,b)} = \varphi_a \circ \psi_b$$

Dimostrazione. Dal punto strettamente insiemistico sussiste una banale bigezione

$$\Phi \colon C \rtimes_{(\varphi,\psi)} (A \times B) \to (C \rtimes_{\varphi} A) \times B$$
$$(c, a, b) \mapsto (c, a, b)$$

Dobbiamo verificare che sia un omomorfismo.

$$\begin{aligned}
\Phi((c_1, a_1, b_1) *_1 (c_2, a_2, b_2)) &= \Phi((c_1 \tau_{(a_1,b_1)}(c_2), a_1 a_2, b_1 b_2)) \\
&= (c_1 \tau_{(a_1,b_1)}(c_2), a_1 a_2, b_1 b_2) \\
&= (c_1 (\varphi_{a_1} \circ \psi_{b_1})(c_2), a_1 a_2, b_1 b_2) \\
&= (c_1 \varphi_{a_1}(c_2), a_1 a_2, b_1 b_2) \\
&= (c_1, a_1, b_1) *_2 (c_2, a_2, b_2) \\
&= \Phi((c_1, a_1, b_1)) *_2 \Phi((c_2, a_2, b_2))
\end{aligned}$$ □

Lemma 3.20.8. *Sia un gruppo di ordine 12. Allora ammette o un 3-Sylow normale o un 2-Sylow normale.*

Dimostrazione. Siano P_3 e P_2 un 3-Sylow e 2-Sylow.

Se P_3 non è normale, allora ne esistono almeno 2. In particolare essendo che n_3 deve dividere 12 ed essere congruo a 1 modulo 3, otteniamo che ce ne devono essere 4. Essendo che un 3-Sylow ha cardinalità prima 3, allora può solo avere intersezione banale con un altro 3-Sylow.

Ergo l'unione dei 4 3-Sylow contiene 8 elementi di ordine 3 e l'identità. Quindi il gruppo G contiene altri 3 elementi a, b, c.

Presi ora due 2-Sylow P_2^1 e P_2^2, i loro elementi hanno ordine 1 o 2 o 4. Quindi l'unione $P_2^1 \cup P_2^2$ è contenuta in $\{a, b, c\}$. Se P_2^1 e P_2^2 fossero distinti, allora la loro intersezione avrebbe al più due elementi. Ergo la loro unione avrebbe almeno 6 elementi. Assurdo. Quindi esiste un unico 2-Sylow che è normale. □

Teorema 3.20.9. *A meno di isomorfismo esistono cinque gruppi di ordine 12:*

$$\mathbb{Z}/12\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \quad A_4 \quad D_6 \quad \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$$

Dimostrazione. Siano P_3 e P_2 un 3-Sylow e 2-Sylow. Per il lemma precedente possiamo supporre che uno dei due sia normale. In tutti due i casi G coincide, per cardinalità, con P_2P_3 in quanto P_2 e P_3 hanno intersezione banale.

($P_2 \trianglelefteq G$) In questo caso G è isomorfo a $P_2 \rtimes P_3$. Dividiamo la discussione in base alla classe di isomorfismo di P_2 (che ha ordine 4).

Se P_2 è isomorfo a $\mathbb{Z}/4\mathbb{Z}$, allora G è isomorfo ad un prodotto semidiretto $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$, con

$$\varphi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$$

Essendo che $\bar{1}$ in $\mathbb{Z}/3\mathbb{Z}$ ha ordine 3, allora può andare solo nell'identità. Ergo G è isomorfo a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$.

Se P_2 è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, allora come prima G è isomorfo ad un prodotto semidiretto $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$, con

$$\varphi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq S_3$$

L'elemento $\bar{1}$ in $\mathbb{Z}/3\mathbb{Z}$ può andare nell'identità, che dà il prodotto diretto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, o in uno dei due elementi di ordine 3 in S_3.

Posto φ_1 l'omomorfismo che manda $\bar{1}$ in (1, 2, 3), allora possiamo coniugare $\varphi_1(\bar{1})$ per la permutazione (2, 3), ottenendo la mappa φ_2, che manda $\bar{1}$ in

(1, 3, 2). Per il criterio sui prodotto semidiretti, otteniamo che i prodotti semidiretti dati da φ_1 e φ_2 sono isomorfi.

Vogliamo capire meglio la classe di isomorfismo di questi prodotti semidiretti. In particolare vogliamo dimostrare che sono isomorfi ad A_4.

Notiamo che P_3 non può essere normale, in quanto se lo fosse G sarebbe isomorfo al gruppo abeliano $P_2 \times P_3$. Quindi esistono 4 3-Sylow, ed abbiamo una azione per coniugio di G su questi sottogruppi. ne Dimostriamo che questa azione

$$\psi \colon G \to S(\{P_{3,1}, P_{3,2}, P_{3,3}, P_{3,4}\}) \simeq S_4$$

è un omomorfismo iniettivo.

Infatti per ogni $P_{3,i}$, il suo normalizzatore ha cardinalità

$$|N_G(P_{3,i})| = \frac{|G|}{n_3} = 3$$

Essendo che $P_{3,i}$ è contenuto nel suo normalizzatore, otteniamo che in verità $P_{3,i}$ e $N_G(P_{3,i})$ coincidono. Quindi possiamo affermare che ψ ha nucleo

$$\mathrm{Ker}(\psi) = \bigcap_{i=1}^{4} N_G(P_{3,i}) = \bigcap_{i=1}^{4} P_{3,i} = \{e\}$$

Quindi G si immerge in S_4 come sottogruppo di ordine 12. Per uno dei lemmi precedenti $\psi(G)$ deve essere A_4.

($P_3 \trianglelefteq G$) Se P_2 è isomorfo a $\mathbb{Z}/4\mathbb{Z}$, allora G è isomorfo ad un prodotto semidiretto $\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$, con

$$\varphi \colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}^*$$

L'elemento $\bar{1}$ di $\mathbb{Z}/4\mathbb{Z}$ può andare in ognuno dei due elementi di $\mathbb{Z}/3\mathbb{Z}^*$. In un caso otteniamo $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ isomorfo a $\mathbb{Z}/12\mathbb{Z}$, nell'altro otteniamo l'unico prodotto semidiretto $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

Se P_2 è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, allora G è isomorfo a $\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ con

$$\varphi \colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}^*$$

Tentiamo di capire quanti gruppi, a meno di isomorfismo, possiamo ottenere. Certamente abbiamo un prodotto diretto

$$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

D'altra parte gli altri omomorfismi da $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a $\mathbb{Z}/3\mathbb{Z}^*$ sono $\varphi_{1,-1}$, $\varphi_{-1,1}$, $\varphi_{-1,-1}$, con

$$\varphi_{i,j}((1,0)) = i$$
$$\varphi_{i,j}((0,1)) = j$$

Vogliamo dimostrare che tutti questi prodotti semidiretti sono isomorfi. Infatti è possibile, tramite un automorfismo di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, permutare i tre elementi di ordine 2. In particolare, fissato un $\varphi_{i,j}$, allora esistono due elementi di ordine due che vengono mandati in -1. Quindi è possibile individuare un automorfismo σ per cui

$$\varphi_{i,j}(\sigma(1,0)) = -1 = \varphi_{-1,-1}((1,0))$$
$$\varphi_{i,j}(\sigma(0,1)) = -1 = \varphi_{-1,-1}((0,1))$$

Quindi tutti i prodotti semidiretti non banali sono isomorfi. Consideriamo quello dato da $\varphi_{-1,1}$. Essendo che la seconda componente agisce banalmente otteniamo

$$\begin{aligned} G &\simeq \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \\ &\simeq (\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} \\ &\simeq D_3 \times \mathbb{Z}/2\mathbb{Z} \\ &\simeq D_6 \end{aligned}$$

□

3.21 Il Gruppo Q_8

Se uno riflette possiamo classificare, a meno di isomorfismo, tutti i gruppi con ordine compreso fra 1 e 15, *ad eccezione di 8*. Lo scopo di questa sezione è appunto introdurre l'ultimo tassello: il gruppo dei quaternioni Q_8

Definizione 3.21.1. Definiamo il gruppo dei quaternioni come il gruppo dato dalla presentazione seguente:

$$Q_8 = \langle i, j \mid i^4 = e, i^2 = j^2, ji = i^{-1}j \rangle$$

Proposizione 3.21.2. *Il gruppo dei quaternioni ha otto elementi, che nello specifico sono*

$$Q_8 = \{ e, i, i^2, i^3, j, j^3, ij, i^3 j \}$$

Dimostrazione. Osserviamo innanzitutto che grazie al poter scambiare ji con i^3j, è immediato come Q_8 sia dato dal prodotto $\langle i\rangle\,\langle j\rangle$. Inoltre i due generatori hanno, grazie alla presentazione, ordire al più 4. Quindi Q_8 ha cardinalità

$$|Q_8| = \frac{|\langle i\rangle||\langle j\rangle|}{|\langle i\rangle \cap \langle j\rangle|} \leq \frac{4\cdot 4}{2} = 8$$

Per concludere la dimostrazione dobbiamo solamente provare che in effetti i e j hanno ordine 4. Tuttavia non è facile dimostrare proprietà a partire dalla sola presentazione. (Dovremmo dimostrare che i^2 non appartiene al generato normale di $\{i^4, i^2j^{-2}, jij^{-1}i^{-3}\}$).

Un'altra via consiste nell'esibire un gruppo con tale presentazione. Sia il gruppo G dato dalla seguente tavola di Cayley

	e	$\bar{e}$	i	$\bar{\imath}$	j	$\bar{\jmath}$	k	$\bar{k}$
e	e	$\bar{e}$	i	$\bar{\imath}$	j	$\bar{\jmath}$	k	$\bar{k}$
$\bar{e}$	$\bar{e}$	e	$\bar{\imath}$	i	$\bar{\jmath}$	j	$\bar{k}$	k
i	i	$\bar{\imath}$	$\bar{e}$	e	k	$\bar{k}$	$\bar{\jmath}$	j
$\bar{\imath}$	$\bar{\imath}$	i	e	$\bar{e}$	$\bar{k}$	k	j	$\bar{\jmath}$
j	j	$\bar{\jmath}$	$\bar{k}$	k	$\bar{e}$	e	i	$\bar{\imath}$
$\bar{\jmath}$	$\bar{\jmath}$	j	k	$\bar{k}$	e	$\bar{e}$	$\bar{\imath}$	i
k	k	$\bar{k}$	j	$\bar{\jmath}$	$\bar{\imath}$	i	$\bar{e}$	e
$\bar{k}$	$\bar{k}$	k	$\bar{\jmath}$	j	i	$\bar{\imath}$	e	$\bar{e}$

Allora l'omomorfismo

$$\begin{aligned} \Phi\colon Q_8 &\to G \\ i &\mapsto i \\ j &\mapsto j \end{aligned}$$

è ben definito, in quanto la presentazione è rispettata. Inoltre Φ è suggettiva. Ergo Q_8 ha cardinalità almeno 8. Ma per quello già detto otteniamo che Q_8 ha cardinalità esattamente 8 e Φ è un isomorfismo.

Infine gli elementi di Q_8 corrispondono agli 8 elementi di G, che sono quelli scritti in precedenza, una volte notate le seguenti uguaglianze

$$\bar{e} = i^2$$
$$\bar{\imath} = i^3$$
$$\bar{\jmath} = j^3$$
$$k = ij$$
$$\bar{k} = i^3 j$$

□

Osserviamo inoltre che Q_8 si immerge nel gruppo speciale lineare $SL_2(\mathbb{C})$, una volta identificati i e j con le seguenti matrici

$$i \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$
$$j \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Il gruppo Q_8 possiede delle proprietà interessanti, dati dai seguenti teoremi:

Teorema 3.21.3. *Il centro di Q_8 è $\langle i^2 \rangle$.*

Dimostrazione. Essendo che Q_8 non è abeliano, il suo centro non può essere tutto Q_8, nè avere indice 2. Quindi ha cardinalità 2 o è banale. Tuttavia essendo Q_8 un p-gruppo, il centro non può essere banale. Ed in effetti i^2 appartiene al centro. □

Teorema 3.21.4. *Q_8 ammette solo sottogruppi normali benché non sia abeliano.*

Dimostrazione. Sia H sottogruppo di Q_8

1. Se H è banale o è tutto Q_8 è normale
2. Se H ha ordine 2 allora è generato da i^2, unico elemento di ordine 2, e quindi è il centro.
3. Se H ha ordine 4 è normale avendo indice 2

□

Teorema 3.21.5. *Q_8 non si può scomporre come prodotto semidiretto in maniera non banale. Cioè non esistono due sottogruppi propri per cui Q_8 sia isomorfo al loro prodotto semidiretto tramite coniugio.*

Dimostrazione. Semplicemente presi due sottogruppi non banali, allora condividono, per il teorema di Cauchy, l'unico elemento di ordine 2. □

Il gruppo dei quaternioni permette di chiudere la classificazione dei gruppi di ordine 8. Per la relativa dimostrazione serve premettere questo lemma:

Lemma 3.21.6. *Se G è un gruppo con elementi di ordine 1 o 2, allora è abeliano.*

Dimostrazione. Siano a e b in G. Allora

$$aba^{-1}b^{-1} = abab = (ab)^2 = e$$

Ergo a e b commutano. □

Teorema 3.21.7. *A meno di isomorfismo esistono 5 gruppi di ordine 8:*

$$\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad D_4 \quad Q_8$$

Dimostrazione. Sia G un gruppo di ordine 8. Se esso è abeliano, allora possiamo già concludere col teorema di classificazione dei gruppi abeliani finiti. Supponiamo quindi che G non sia abeliano.

Allora, per il Lemma precedente, ammette un elemento a di ordine 4 o 8. Essendo che siamo nel caso non abeliano, a ha ordine 4.

Il sottogruppo $\langle a \rangle$ è normale in G avendo indice 2. Quindi possiamo considerare $G/\langle a \rangle$ che consiste negli elementi $\langle a \rangle$ e $b\langle a \rangle$. Il secondo ha ordine 2, che implica che b^2 appartiene a $\langle a \rangle$.

Osserviamo innanzitutto che il coniugio per b, ristretto a $\langle a \rangle$, è un automorfismo di $\langle a \rangle$ essendo quest'ultimo normale. Quindi bab può solamente essere, per ordine, pari a a o a^{-1}. Se fosse pari al primo, allora a e b commuterebbero, e G, generato da quest'ultimi, sarebbe abeliano.

Inoltre se b^2 coincidesse con a o a^3, allora b avrebbe ordine 8. Tuttavia ciò non è possibile vista la non abelianità di G. Inoltre vista la descrizione di $G/\langle a \rangle$ è immediato che a e b generino G.

Se $b^2 = 1$ il gruppo G è isomorfo a D_4. Infatti sia la mappa

$$\begin{aligned}\Phi\colon \left\langle r, s \,\middle|\, r^4 = 1, s^4 = 1, srs = r^{-1}\right\rangle &\to G\\ r &\mapsto a\\ s &\mapsto b\end{aligned}$$

Essa è suggettiva, in quanto a e b generano G, ed è un omomorfismo in quanto a e b rispettano le presentazioni.

Quindi Φ è un omomorfismo suggettivo. Per ordini è un isomorfismo.

Se $b^2 = a^2$, dimostriamo che G è isomorfo a Q_8. Infatti anche in questo caso abbiamo la mappa

$$\begin{aligned}\Psi\colon \left\langle i, j \,\middle|\, i^4 = 1, i^2 = j^2, ji = i^{-1}j\right\rangle &\to G\\ i &\mapsto a\\ j &\mapsto b\end{aligned}$$

che per le stesse ragioni di prima è un omomorfismo suggettivo. □

Chiudiamo questa sezione con l'ultimo teorema di classificazione:

Teorema 3.21.8. *A meno di isomorfismo esistono 3 gruppi di ordine 30:*

$$\mathbb{Z}/30\mathbb{Z} \quad D_{15} \quad D_3 \times \mathbb{Z}/5\mathbb{Z} \quad D_5 \times \mathbb{Z}/3\mathbb{Z}$$

Dimostrazione. Sappiamo che esiste un sottogruppo H di ordine 15. Sappiamo inoltre che 15 è della forma pq con p che non divide $q - 1$. Quindi H è ciclico.

Inoltre esiste un elemento k di ordine 2, che genera un sottogruppo K di ordine 2. Quindi per il teorema di scomposizione, essendo che 2 e 15 sono coprimi, otteniamo che G è isomorfo a $\mathbb{Z}/15\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, con

$$\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}^* \times \mathbb{Z}/5\mathbb{Z}^*$$

Nel codominio esistono tre elementi di ordine 2 e l'identità. Quindi i 4 gruppi propositi devono essere tutti. □

Concludiamo con una tabella che elenca i gruppi (ad eccezione degli abeliani finiti) che abbiamo classificato (indichiamo con C_n l'ennesimo gruppo

ciclico)

1	$\{e\}$
8	$C_8 \quad C_4 \times C_2 \quad C_2 \times C_2 \times C_2 \quad D_4 \quad Q_8$
12	$C_{12} \quad C_2 \times C_6 \quad C_3 \rtimes C_4 \quad A_4 \quad D_6$
30	$C_{30} \quad D_3 \times C_5 \quad D_5 \times C_3 \quad D_{15}$
p	C_p
p^2	$C_{p^2} \quad C_p \times C_p$
$pq, p \nmid q-1$	C_{pq}
$pq, p \mid q-1$	$C_{pq} \quad C_q \rtimes C_p$

3.22 Gruppi Semplici

Con questa sezione affrontiamo un argomento fondamentale: i gruppi semplici.

Definizione 3.22.1. Sia G un gruppo. Esso si dice semplice se non ammette sottogruppi normali fuori da G e il sottogruppo banale.

Vogliamo dimostrare che tra gli ordini compresi fra 1 e 100 i gruppi $\mathbb{Z}/p\mathbb{Z}$ e A_5 sono gli unici gruppi semplici. Incominciamo con i primi risultati.

Teorema 3.22.2. *I gruppi $\mathbb{Z}/p\mathbb{Z}$ sono semplici.*

Dimostrazione. Il gruppo $\mathbb{Z}/p\mathbb{Z}$ ammette come unici sottogruppi, per ragioni di divisibilità, $\{e\}$ e $\mathbb{Z}/p\mathbb{Z}$. □

Dimostriamo che A_n è semplice per $n \geq 5$. Per poterlo fare però servono un paio di lemmi tecnici.

Lemma 3.22.3. *Il gruppo A_n è generato dai 3-cicli.*

Dimostrazione. Sappiamo che A_n è generato dalle permutazioni $(a, b)(c, d)$. Basta quindi dimostrare che tramite i 3-cicli possiamo generare tutte queste.

Infatti presa σ pari a $(a, b)(c, d)$, allora vale

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

Lemma 3.22.4. *Sia σ una permutazione in S_n costituita da cicli di lunghezza diversa. Se*

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_l$$

allora il centralizzatore di σ è

$$Z_{S_n}(\sigma) = \left\{ \sigma_1^{k_1} \circ \cdots \circ \sigma_l^{k_l} \right\}$$

Dimostrazione. Sappiamo che in S_n σ ha coniugati pari alle permutazioni dello stesso tipo. Se

$$\text{type}(\sigma) = (s_1, \ldots, s_l) \qquad s_1 + \cdots + s_l = n$$

esse sono, usando la notazione multinomiale

$$\begin{aligned} |\mathcal{C}_\sigma| &= \prod_{i=1}^{l} \binom{n - s_1 - \cdots - s_{i-1}}{s_i} (s_i - 1)! \\ &= \binom{n}{s_1 \ldots s_l} \prod_{i=1}^{l} (s_i - 1)! \\ &= \frac{n!}{s_1 \ldots s_l} \end{aligned}$$

e quindi il centralizzatore di σ ha cardinalità pari a

$$|Z_{S_n}(\sigma)| = \frac{|S_n|}{|C_\sigma|} = s_1 \ldots s_l$$

D'altra parte l'insieme proposto ha questa cardinalità, ed è immediato verificare che sia nel centralizzatore. Quindi coincidono. □

Lemma 3.22.5. *In A_5 le classi di coniugio hanno le seguenti cardinalità:*

σ	$\lvert\mathcal{C}_\sigma^{(S_n)}\rvert$	$\lvert\mathcal{C}_\sigma^{(A_n)}\rvert$
$(a,\, b)(c,\, d)$	15	15
$(a,\, b,\, c)$	20	20
$(a,\, b,\, c,\, d,\, e)$	24	12

Dimostrazione. È sufficiente calcolare le classi di coniugio in S_n, e osservare che $(a,\, b)(c,\, d)$ viene centralizzato da $(a,\, b)$ che è dispari, $(a,\, b,\, c)$ da $(d,\, e)$ che è sempre dispari, e $(a,\, b,\, c,\, d,\, e)$ solo dalle sue potenze che sono tutte pari. □

Procediamo quindi al primo vero risultato di questa sezione:

Teorema 3.22.6. *Il gruppo A_5 è semplice.*

Dimostrazione. Sia H sottogruppo in A_5 non banale. Dimostriamo che contiene almeno un 3-ciclo, considerando innanzitutto un σ in H arbitrario.

1. Se σ è già un 3-ciclo abbiamo concluso.

2. Se σ è un 5-ciclo, allora contiene tutti i coniugati di σ in A_5. Cioè H ha almeno 12 elementi. Inoltre dovendo avere l'identità ne ha almeno 13. Inoltre la cardinalità di H divide quella di A_5, cioè 60. Quindi H può avere solamente 15, 20, 30 o 60 elementi. In tutti questi casi contiene per Cauchy un elemento di ordine 3, quindi un 3-ciclo, o un elemento di ordine 2, quindi una doppia trasposizione.

3. Se σ è una doppia trasposizione $(a, b)(c, d)$, allora sappiamo che H contiene il suo coniugato $(c, d)(b, e)$. Quindi H contiene il loro prodotto $(a, b)(b, e)$, pari a (a, b, e).

Quindi H contiene un 3-ciclo. Ergo contiene tutti i 3-cicli essendo normale. Infine per generazione coincide con A_5. □

Potevamo dimostrare questo risultato anche per altre vie, dimostrando che

$$1 + a_1 20 + a_2 15 + a_3 12 + a_4 12 \mid 60 \quad \{a_i\} \subseteq \{0, 1\}$$

ha soluzioni solamente per $\{a_i\}$ pari tutti a 0 o a 1. Questo implica che un sottogruppo normale H di A_5, quindi unione disgiunta di classi di coniugio, può solamente avere ordine 60 o 1.

Per dimostrare la semplicità di A_n serve il prossimo lemma

Lemma 3.22.7. *Sia un elemento σ di $A_n \setminus \{e\}$, con n maggiore o uguale a 5. Allora esiste un coniugato τ, diverso da σ, tale che $\tau(x)$ e $\sigma(x)$ coincidano per qualche x tra 1 e n.*

Dimostrazione. Supponiamo che σ si scomponga in cicli di lunghezza massima l. Allora, a meno di coniugio, possiamo supporre che σ abbia nella decomposizione esattamente il ciclo $\rho = (1, \ldots, l)$.

1. Se l è almeno 3, allora possiamo considerare $\tau = (3, 4, 5)$. Allora

$$\tau\sigma\tau^{-1}(1) = 2 = \sigma(1)$$

e

$$\tau\sigma\tau^{-1}(2) = 4 \neq 3 = \sigma(2)$$

2. Se l è 2, allora σ, per parità, si scompone in almeno 2 traposizioni. In particolare, a meno di coniugio, σ ammette la doppia trasposizione $(1, 2)(3, 4)$. Allora posto $\tau = (1, 2, 3)$ vale

$$\tau\sigma\tau^{-1}(5) = \sigma(5)$$

e

$$\tau\sigma\tau^{-1}(2) = 3 \neq 1 = \sigma(2)$$

□

Teorema 3.22.8. *Il gruppo A_n è semplice per $n \geq 5$.*

Dimostrazione. La dimostrazione procede sostanzialmente per induzione, con $n = 5$ il caso base già dimostrato.

Sia ora A_n con $n > 5$, e consideriamo

$$R_i = \{\, \sigma \in A_n \mid \sigma(i) = i \,\} \quad 1 \leq i \leq n$$

Dobbiamo dimostrare che A_i sono tutti isomorfi a A_{n-1}.

Certamente R_n è isomorfo a A_{n-1} tramite l'isomorfismo

$$\begin{aligned} A_{n-1} &\to R_n \\ \sigma &\mapsto \sigma \circ (n) \end{aligned}$$

Inoltre l'azione di A_n su $\{1, \ldots, n\}$ è transitiva, in quanto $(a, b)(c, d)$ manda a in b per ogni a, b. Ergo gli stabilizzatori $R_i = \mathrm{Stab}(i)$ sono isomorfi tramite coniugio.

Sia ora H sottogruppo normale di A_n. Allora notiamo innanzitutto che se $\sigma R_i \sigma^{-1} = R_j$, allora

$$\sigma(H \cap R_i)\sigma^{-1} = H \cap R_j$$

Ergo le intersezioni $H \cap R_i$ sono tutte isomorfe tra di loro. Inoltre $H \cap R_i$ è un sottogruppo normale di R_i per ogni i. Siccome R_i sono isomorfi a A_{n-1}, allora le intersezioni sono tutte banali, o sono tutte pari a R_i.

1. Se $H \cap R_i = R_i$ per ogni i, allora R_i è incluso in H per ogni i. Ergo H contiene tutte le permutazioni che fissano un punto. Quindi contiene le permutazioni della forma $(a, b)(c, d)$. Infine sappiamo che queste generano A_n.

2. Se $H \cap R_i$ è sempre banale, allora per ogni σ in H non pari all'identità, σ non ha punti fissi.

   Sia ora σ in H. Se per assurdo non fosse l'identità, allora ammetterebbe un coniugato $\tau\sigma\tau^{-1} = \rho$ diverso da se stesso, tale che $\rho(x) = \sigma(x)$ per qualche x. In tal caso avremmo

   $$(\rho^{-1} \circ \sigma)(x) = x \qquad \rho^{-1} \circ \sigma \neq e$$

   con $\rho^{-1} \circ \sigma$ appartenente a H per normalità. Assurdo.

Quindi o H è banale, o coincide con tutto A_n. □

Corollario 3.22.9. *Sia un sottogruppo normale di S_n, per $n \neq 4$. Allora coincide con $\{e\}$, A_n o S_n.*

Dimostrazione. I casi $n = 2, 3$ sono banali.

Se $n \geq 5$, consideriamo un sottogruppo H di S_5 normale. Allora $H \cap A_5$ è è un sottogruppo normale di A_n di cardinalità pari a $|H|$ o $|H|/2$.

Nel primo caso, vista la semplicità di A_n, otteniamo che H coincide o con $\{e\}$ o con A_n.

Nel secondo caso, otteniamo che $H = S_n$ o ha due elementi. Tuttavia se $|H| = 2$, allora potremmo considerare l'azione di coniugio di S_n su H. Questo ci dà una mappa

$$\Phi \colon S_n \to \mathrm{Aut}(H) \simeq \{e\}$$

Siccome $\mathrm{Ker}(\Phi) = S_n$, allora otteniamo che H appartiene al centro di S_n. Assurdo, in quanto S_n ha centro banale. □

Corollario 3.22.10. *Sia un sottogruppo di S_n di indice 2. Allora coincide con A_n.*

Dimostrazione. Se $n \neq 4$ possiamo concludere con il corollario precedente.

Per quanto riguarda il caso $n = 4$, consideriamo un sottogruppo $H \trianglelefteq S_4$ e il passaggio al quoziente

$$\pi \colon S_4 \to S_4/H \simeq \mathbb{Z}/2\mathbb{Z}$$

Siccome tutti gli elementi di ordine dispari devono appartenere a $\mathrm{Ker}(\pi) = H$, allora quest'ultimo contiene tutti i 3-cicli. Siccome i 3-cicli generano A_4, allora $A_4 \subseteq H$, che quindi coincidono per cardinalità. □

Corollario 3.22.11. *Sia un sottogruppo di S_n di indice n. Allora è isomorfo a S_{n-1}.*

Dimostrazione. Sia H un sottogruppo come da ipotesi, e consideriamo l'azione Φ di S_n su $X := S_n/H$ data da $\sigma \cdot \tau H = (\sigma\tau)H$.

Siccome tale azione è transitiva, il nucleo di tale applicazione è banale. Analizziamo quindi $\Phi(H) \leq S(X) \simeq S_n$. Per definizione di Φ esso è contenuto in

$$\{ \sigma \in S(X) \mid \sigma \cdot H = H \}$$

Inoltre per cardinalità questo insieme coincide con $\Phi(H)$. Quindi

$$H \simeq \Phi(H) = \{ \sigma \in S(X) \mid \sigma \cdot H = H \} \simeq S_{n-1}$$ □

Quindi $\mathbb{Z}/p\mathbb{Z}$ e A_n, per $n > 5$, sono semplici. Ce ne sono altri, almeno di ordine compreso tra 1 e 100? I prossimi teoremi negano questo fatto.

Teorema 3.22.12. *Sia G un gruppo di ordine compreso tra 2 e 100, non primo e diverso da 60. Allora non è semplice.*

Dimostrazione. Una dimostrazione esaustiva sarebbe improponibile. Presentiamo solamente lo *sketch* della dimostrazione, lasciando al lettore la verifica che in effetti un qualsiasi numero compreso tra 1 e 100 rientra nei casi sottodescritti. (Prima o poi metterò la tabella a riguardo).

1. In alcuni casi i teoremi di Sylow danno immediatamente la risposta. Per esempio preso $n = 20 = 2^2 * 5$, allora n_5 deve necessariamente essere pari a 1. Quindi esiste un unico 5-Sylow normale.

2. In altri casi il teorema di Poincaré arriva in soccorso. Per esempio preso $n = 96 = 2^5 * 3$, allora consideriamo un 2-Sylow P_2. Per il teorema di Poincaré esiste un sottogruppo H, normale in G, tale che

   $$3 \mid [G : N] \mid 6$$

   Quindi H è un sottogruppo proprio e non banale.

3. Incredibilmente questi due casi esauriscono quasi tutte le cardinalità non prime e diverse da 60. La prima che rimane fuori è $56 = 2^3 * 7$.

   Se $n_7 = 7$, allora l'unione dei 7-Sylow ha 49 elementi, in quanto ogni coppia di 7-Sylow ha intersezione banale. A questo punto un 2-Sylow, a meno dell'identità, è incluso nel complementare di questa unione, costituito da 7 elementi. Quindi è immediato che n_2 deve essere pari a 1.

   La seconda cardinalità non trattata, che si risolve con questo metodo, è 80.

4. La terza cardinalità non ancora considerata è $72 = 2^3 * 3^2$. In questo caso sappiamo che il gruppo G agisce per coniugio sui 3-Sylow con un'azione transitiva. Se per assurdo G fosse semplice, allora n_3 deve essere pari a 4. Abbiamo quindi un omomorfismo

   $$\Phi \colon G \to S(P_{3,1}, P_{3,2}, P_{3,3}, P_{3,4}) \simeq S_4$$

   Siccome G è semplice, il nucleo di Φ è banale o non è proprio.

   Nel primo caso otteniamo l'assurdo, in quanto G di ordine 72 si immergerebbe in S_4 di ordine 24.

   Nel secondo caso otteniamo comunque l'assurdo, in quanto l'azione, per poter essere transitiva, non può avere nucleo pari a tutto G.

□

Chiudiamo la trattazione sui gruppi semplici con il caso $|G| = 60$.

Lemma 3.22.13. *Il gruppo A_5 ha 5 2-Sylow.*

Dimostrazione. Consideriamo gli insiemi R_i definiti precedentemente.

Allora se consideriamo per esempio R_1, esso è dato da

$$\{e, (1,\,2)(3,\,4), (1,\,3)(2,\,4), (1,\,4)(2,\,3)\}$$

che tuttavia è esattamente un 2-Sylow, isomorfo al sottogruppo di Klein di A_4.

Analogamente tutti gli altri R_i sono 2-Sylow.

D'altra parte ogni 2-Sylow arbitrario è coniugato ad R_1, e quindi anche esso fissa un elemento. Nello specifico se $P = \tau R_1 \tau^{-1}$, allora P fissa $\tau(1)$.

Quindi i 2-Sylow di A_5 sono 5, dati da R_i con $i \in \{1, \ldots, 5\}$. □

Teorema 3.22.14. *Sia G un gruppo semplice di ordine 60. Esso è isomorfo a A_5.*

Dimostrazione. Tramite i teoremi di Sylow, sappiamo che n_2 appartiene a $\{1, 3, 5, 15\}$. Escludiamo innanzitutto che n_2 non possa essere 5.

$n_2 = 1$ Siccome G è semplice, questo caso si esclude immediatamente.

$n_2 = 3$ In questo caso consideriamo l'azione di G sui 2-Sylow, ottenendo una immersione di G in S_3. Per cardinalità questo è ovviamente assurdo.

$n_2 = 5$ Siccome $n_5 \in \{1, 6\}$, allora può essere solamente pari a 5 per la semplicità di A_5. Se i 2-Sylow si intersecassero tutti banalmente, allora in A_5 ci sarebbero

$$1 + n_5 * 4 + n_2 * 3 = 70$$

elementi. Quindi esistono due 2-Sylow P_2, P_2', che hanno due elementi in comune.

Consideriamo quindi P_2, P_2' tali che $H = P_2 \cap P_2'$ non si banale. Consideriamo inoltre $K = N_G(H)$. Siccome $[P_2 : H] = [P_2' : H] = 2$, allora P_2 e P_2' sono contenuti in K. Quindi

$$|H| \mid |K| \mid |G|$$

cioè

$$4 \mid |K| \mid 60$$

Inoltre $|K|$ è almeno 8, in quanto P_2P_2', contenuto in K, ha cardinalità pari a 8.

Se $|K| = 12$, possiamo considerare l'azione di G su G/K, che ha cardinalità pari a 5. Siccome G è semplice, allora otteniamo una immersione di G in S_5. Siccome l'unico sottogruppo di A_5 di ordine 60 è A_5, allora otteniamo che G è isomorfo a quest'ultimo. Quindi $n_2(G) = 5$. Assurdo.

Se $|K| = 20$, per il teorema di Poincaré esiste un sottogruppo normale H di G di indice $[G : H]$, tale che

$$3 \mid [G : H] \mid 3! = 6$$

Quindi $1 < |H| < 60$. Assurdo per la semplicità di G.

Se $|K| = 60$, allora H è normale di G. Assurdo sempre per se semplicità di G.

Quindi $n_2 = 5$, e abbiamo una immersione di G in S_5. Siccome $|G| = 60$, allora G otteniamo un isomorfismo tra G e A_5. □

Capitolo 4

Anelli

4.1 Prime Definizioni

Definizione 4.1.1. Sia A un insieme e $+, \cdot$ due operazioni su di esso. La tripla $(A, +, \cdot)$ viene detto anello con identità se $\cdot, +$ soddisfano le seguenti proprietà:

1. $(A, +)$ è un gruppo abeliano;
2. $\cdot$ è associativa (cioè $(A, \cdot)$ è un semigruppo);
3. per ogni $x, y, z3A$ valgono le leggi distributive

$$(x + y)z = xz + yz \qquad x(y + z) = xy + xz.$$

Se $\cdot$ è commutativa, allora A si dice anello commutativo. Inoltre se ammette un identità, cioè un elemento $1 \in A$ tale che

$$1x = x1 = x \quad \forall x \in A,$$

allora A viene detto anello con identità.

Definizione 4.1.2. Sia A un anello con identità. Un elemento $x \in A$ viene detto invertibile se esiste un $y \in A$ tale che $xy = yx = 1$. L'insieme degli elementi invertibili di A viene indicato con A^*.

Proposizione 4.1.3. *Se A è un anello con identità, la coppia $(A^*, \cdot)$ è un gruppo.*

Dimostrazione. Per definizione ogni $x \in A$ ammette un inverso.

Inoltre xy ammette inverso pari a $y^{-1}x^{-1}$.

L'elemento $1 \in A$ è banalmente invertibile, quindi appartiene a A^*.

Infine $\cdot$ è associativa. □

Se x ammette un inverso, allora è unico. Inoltre non tutti gli elementi necessitano di avere un inverso. Per esempio $\mathbb{Z}^* = \{\pm 1\}$.

Diamo le definizioni di corpo e campo.

Definizione 4.1.4. Un corpo è un anello con identità, tale che ogni elemento sia invertibile.

Definizione 4.1.5. Un campo è un corpo commutativo diverso da (0).

Benché l'anello (0) potrebbe soddisfare tutti gli assiomi di un campo, per ragioni categoriali non viene considerato un campo. Difatti si osserva che tutti i teoremi che valgono per i campi, falliscono per il "campo con un solo elemento" (0). Una interessante teoria è nata con lo scopo di cercare un oggetto che si possa comportare veramente come un campo con un solo elemento.

I corpi sono una struttura intermedia tra gli anelli e i campi. Sorprendentemente sussiste il teorema di Wedderburn, la cui dimostrazione si trova nell'appendice.

Teorema 4.1.6 (di Wedderburn)**.** *Un corpo finito è necessariamente un campo.*

Gli insiemi $\mathbb{Z}/n\mathbb{Z}$ hanno la struttura di anello. La cosa particolare, a differenza di $\mathbb{Z}$, è che ammettono divisori di zero.

Definizione 4.1.7. Sia A un anello commutativo con identità. Un elemento $x \in A$ è un divisore di zero se esiste un y non nullo tale che $xy = 0$. Se $A \setminus \{0\}$ non contiene divisori di zero, A viene detto dominio di integrità.

Proposizione 4.1.8. *Sia A un dominio di integrità. Allora vale la proprietà di cancellazione: se $ab = ac$, con $a \neq 0$, allora $b = c$.*

Dimostrazione. Se $ab = ac$, allora $a(b - c) = 0$. Siccome $a \neq 0$, combinato cl fatto che A è un dominio di integrità, allora $b - c = 0$. □

Teorema 4.1.9. *Sia A un anello commutativo con identità finito. Allora ogni elemento o è un divisore di zero o è invertibile.*

Dimostrazione. Consideriamo un elemento $x \in A$. Allora sia la mappa

$$\Phi\colon A \to A$$
$$y \mapsto yx$$

Questa mappa è suggettiva se e solo se x è invertibile, ed è iniettiva se e solo se x è un divisore di zero. Siccome A è finito, questo implica che x è invertibile se e solo se non è un divisore di 0. □

Corollario 4.1.10. *Ogni dominio di integrità finito è un campo.*

Diamo infine la nozione di elemento nilpotente.

Definizione 4.1.11. Un elemento $x \in A$ è un elemento nilpotente se esiste un naturale n tale che $x^n = 0$.

D'ora in poi con "anello" indicheremo gli anelli commutativi con identità.

Concludiamo questa sezione con la definizione di omomorfismo di anelli.

Definizione 4.1.12. contenuto...

4.2 L'anello dei Polinomi

Un anello intensamente studiato, per esempio anche nel corso di Algebra II, è l'anello dei polinomi $R[X]$.

Definizione 4.2.1. Sia R un anello, e $X = \{x_\lambda\}_{\lambda\in\Lambda}$ un insieme di indeterminate. Definiamo l'anello $R[X]$ come l'insieme dei polinomi in tali variabili a coefficienti in R, cioè come le somme finite di monomi della forma

$$a\prod_{i=1}^{r} x_{\lambda_i}^{n_i} \quad a \in R, \lambda_i \in \Lambda$$

La somma ed il prodotto su $R[X]$ sono definiti nel modo usuale.

Noi guarderemo sostanzialmente il caso $K[x]$ con K un campo, lasciando il caso $R[x_1, \ldots, x_n]$ ad Algebra II ed Istituzioni di Algebra.

Come sappiamo, per i polinomi è definito un grado.

Definizione 4.2.2. Sia A un anello, e $f(x)$ un polinomio in $A[x]$ non nullo. Posto $f = \sum a_n x^n$, definiamo il grado di f come

$$\deg(f) = \max\{\, n \in \mathbb{N} \mid a_n \neq 0 \,\}.$$

Proposizione 4.2.3. *Sia A un dominio di integrità e consideriamo f, g in $A[x]$. Allora*

$$\deg(fg) = \deg(f) + \deg(g)$$
$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$

Dimostrazione. Se $m = \deg(f)$ e $n = \deg(g)$, allora possiamo scrivere

$$f = \sum_{i=1}^{m} a_i x^i$$
$$g = \sum_{i=1}^{n} b_i x^i$$

Da cui

$$fg = a_m b_n x^{m+n} + h(x)$$

con $h(x)$ avente grado minore di $m+n$.

Siccome A è un dominio di integrità, allora $a_m b_n$ non può annullarsi, e quindi $\deg(fg) = m+n$.

D'altra parte supponiamo senza perdita di generalità che $m \leq n$. Allora se $m < n$, sappiamo che

$$f + g = b_n x^n + h(x)$$

con $h(x)$ avente grado minore di n. Quindi $\deg(f+g) = \deg(g)$, che coincide con $\max\{\deg(f), \deg(g)\}$.

Se invece $m = n$, allora

$$f + g = (a_m + b_m)x^m + h(x)$$

con $h(x)$ analogo a sopra. In generale $a_m + b_m$ potrebbe annullarsi, e quindi possiamo dire al più che $\deg(f+g) \leq m = \max\{\deg(f), \deg(g)\}$. □

Corollario 4.2.4. *Se A è un dominio di integrità, $A[x]$ è un dominio di integrità.*

Dimostrazione. Se f, g sono polinomi non nulli, allora fg non è nullo per la discussione precedente. □

Vogliamo dire quali sono gli elementi invertibili di $A[x]$, con A anello generico. Il teorema generale necessiterà del linguaggio degli ideali. Per ora diamo questo risultato parziale.

Proposizione 4.2.5. *Sia A un dominio di integrità. Allora $(A[x])^* = A^*$.*

Dimostrazione. Sicuramente se a appartiene ad A^*, allora appartiene ad $(A[x])^*$.

D'altra parte se consideriamo un elemento $f(x) \in (A[x])^*$, allora esiste un $g(x)$ per cui $fg = 1$. Questo implica in particolare che

$$0 = \deg(1) = \deg(f) + \deg(g)$$

cioè che $\deg(f) = \deg(g) = 0$. Quindi f e g appartengono ad A, e quindi appartengono ad A^*. □

4.3 Polinomi su un Campo

Specializziamo a questo punto il discorso, ad anelli polinomiali della forma $K[x]$, con K un campo. Per questi campi sussiste una divisione con resto, analoga a quella presente in $\mathbb{Z}$.

Teorema 4.3.1. *Sia K un campo. Allora per ogni coppia di polinomi $f(x), g(x) \in K[x]$, con g non nullo, esistono unici $q(x), r(x)$ tali che*

$$\begin{cases} f(x) = q(x)g(x) + r(x) \\ \deg(r) < \deg(g) \vee r = 0 \end{cases}$$

Dimostrazione. Se $f = 0$, allora basta porre $q = r = 0$.

Altrimenti procediamo per induzione su $\deg(f)$.

Se $\deg(f) = 0$ e $\deg(g) > 0$, allora basta considerare $q = 0$ e $r = f$.

Se $\deg(f) = \deg(g) = 0$, allora consideriamo $q = f/g$ e $r = 0$.

Se $\deg(f) > 0$, e $\deg(f) < \deg(g)$, allora è sufficiente porre $q = 0$ e $r = f$.

Se $\deg(f) > 0$ e $\deg(f) \geq \deg(g)$, poniamo $f = \sum a_i x^i$, $g = \sum b_j x^j$, e $m = \deg(f)$, $n = \deg(g)$. Definiamo quindi $f_1 = f - a_m/b_n x^{m-n} g$. Siccome $\deg(f_1) < \deg(f)$, per ipotesi induttiva esistono q_1, r_1 tali che $f_1 = q_1 g + r_1$. Inoltre $\deg(r_1) < \deg(g)$. Quindi

$$f_1 = q_1 g + r_1$$

da cui

$$f = f_1 + a_m/b_n x^{m-n} g = (q_1 + a_m/b_n x^{m-n})g + r_1$$

Per quanto riguarda l'unicità supponiamo che $q_1 g + r_1 = q_2 g + r_2$. Allora $(q_2 - q_1)g = r_2 - r_1$.

Se $r_2 - r_1 = 0$, allora anche $q_2 - q_1 = 0$ e abbiamo l'unicità.

Se $r_2 - r_1 \neq 0$, allora $q_2 - q_1 \neq 0$, e troviamo un assurdo (supponiamo $r_1 = 0$ o $\deg(r_2) \geq \deg(r_1)$):

$$\deg(g) > \deg(r_2) \geq \deg(r_2 - r_1) = \deg((q_2 - q_1)g) \geq \deg(g) \qquad \square$$

Osserviamo l'analogia con la divisione euclidea tra interi. Quando tratteremo i domini euclidei riparleremo di questo fatto.

Corollario 4.3.2 (Teorema di Ruffini)**.** *Sia K un campo e $f \in K[x]$, $a \in K$. Allora $f(a) = 0$ se e solo se $x - a \mid f$.*

Dimostrazione. Certamente se $x - a$ divide f, allora $f(a) = 0$.

Se invece $f(a) = 0$, allora usiamo la divisione euclidea in $K[x]$: esistono $q, r \in K[x]$ tale che $f = q(x - a) + r$. Inoltre $r = 0$ o $\deg(r) < \deg(x - a) =$; quindi r è una costante. In definitiva

$$0 = f(a) = r(a) = r$$

e $x - a$ divide f. $\square$

Come nel caso di $\mathbb{Z}$, si può definire il massimo comune divisore in $K[x]$.

Definizione 4.3.3. Siano $f(x), g(x)$ non entrambi nulli. Un polinomio $d(x) \in K[x]$ è un massimo comune divisore tra f e g se

1. $d \mid f$ e $d \mid g$;

2. per ogni polinomio $h \in K[x]$ che divide sia f che g, esso divide anche d.

Proposizione 4.3.4. *Il massimo comune divisore è unico a meno di elementi di K^*.*

Dimostrazione. Come nel caso intero, se d_1 e d_2 sono due massimi comun divisori, allora esistono due polinomi $h, k \neq 0$ per cui

$$\begin{cases} d_1 = hd_2 \\ d_2 = kd_1 \\ d_1 = hkd_1 \end{cases}$$

Siccome $K[x]$ è un dominio di integrità, otteniamo $1 = hk$. Quindi d_1 e d_2 differiscono per invertibili di $K[x]$, cioè per elementi di K^*. □

Proposizione 4.3.5. *Il massimo comun divisore esiste, ed esistono due polinomi $a(x)$ e $b(x)$ per cui $d = af + bg$.*

Dimostrazione. È sufficiente considerare l'algoritmo di euclide intero, e sostituire il valore assoluto $|\cdot|$ con il grado deg. □

Un'altra analogia con gli interi consiste nella trattazione degli irriducibili e primi.

Definizione 4.3.6. Sia f un polinomio di $K[x]$ non nullo e neanche invertibile.

1. f è primo se per ogni prodotto di polinomi gh, tale che $f \mid gh$, allora $f \mid g$ o $f \mid h$;
2. f è irriducibile se posto $f = gh$, allora g o h è invertibile.

Proposizione 4.3.7. *Un polinomio $f \in K[x]$ non nullo e non invertibile è primo se e solo se è irriducibile.*

Dimostrazione. Analogo al caso intero. □

Proposizione 4.3.8. *Un polinomio $f \in K[x]$ non nullo e non invertibile si scrive come prodotto di elementi primi, in modo unico a meno dell'ordine dei fattore e a meno di prodotto per invertibili.*

Dimostrazione. Anche qua analogo al caso intero. □

Proposizione 4.3.9. *I polinomi di primo grado sono irriducibili.*

Dimostrazione. Supponiamo che f si scomponga come $f = gh$. Allora

$$1 = \deg(f) = \deg(g) + \deg(h).$$

Questo implica che $\deg(g) = 0$ o $\deg(h) = 0$, cioè che $g \in K^*$ o $h \in K^*$. □

Corollario 4.3.10. *Un polinomio $f \in K[x]$ ha un numero di radici, contate con molteplicità, pari al più all suo grado.*

Dimostrazione. Siano $\alpha_1, \ldots, \alpha_r$ radici con molteplicità $e_1, \ldots, e_r$. Allora siccome $(x - \alpha_i)$ sono sia primi che irriducibili, f si scompone come

$$f(x) = (x - \alpha_1)^{e_1} \ldots (x - \alpha_r)^{e_r} g(x)$$

Allora $\deg(f) = e_1 + \cdots + e_r + \deg(g)$, e quindi $e_1 + \cdots + e_r$ è al più $\deg(f)$. □

4.4 Polinomi su $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{Q}$

Specializziamo ulteriormente il discorso ai campi $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{Q}$, e all'anello $\mathbb{Z}$. Nel primo caso vale il famoso teorema, la cui dimostrazione si può trovare a pagina **??**.

Teorema 4.4.1 (Fondamentale dell'Algebra)**.** *Ogni polinomio in $\mathbb{C}[x]$ non costante ammette una radice complessa.*

Corollario 4.4.2. *Un polinomio in $\mathbb{C}[x]$ è irriducibile se e solo se ha grado 1.*

Dimostrazione. Se $p(x)$ è un polinomio in $\mathbb{C}[x]$ di grado 1, allora sappiamo già che è irriducibile.

Se $p(x)$ non ha grado maggiore di 1, consideriamo una sua radice $\alpha \in \mathbb{C}$.. Allora $p(x) = (x - \alpha)g(x)$, con $\deg(g) \geq 1$. Siccome nessuno dei due fattori è invertibile, allora $p(x)$ non è irriducibile. □

Corollario 4.4.3. *Ogni polinomio in $\mathbb{C}[x]$ non costante si fattorizza in polinomi di primo grado.*

Dimostrazione. Immediata conseguenza del corollario precedente e del fatto che in $\mathbb{C}[x]$ ogni polinomio non costante si scompone in elementi irriducibili. □

Consideriamo ora l'anello $\mathbb{R}[x]$. Tale anello può essere immerso in $\mathbb{C}[x]$ ottenendo un interessante risultato.

Teorema 4.4.4. *Sia $p(x) \in \mathbb{R}[x]$ e consideriamolo come polinomio a coefficienti complessi. Allora se $\alpha \in \mathbb{C}$ è una radice di $p(x)$, anche $\bar{\alpha}$ è una radice di tale polinomio. Inoltre $(x - \alpha)(x - \bar{\alpha})$ è un polinomio reale, e α, $\bar{\alpha}$ sono radici di $p(x)$ con la stessa molteplicità.*

Dimostrazione. Innanzitutto siccome $p(x)$ è a coefficienti complessi, allora vale la catena di uguaglianze:

$$p(\bar{\alpha}) = \bar{p}(\bar{\alpha}) = \overline{p(\alpha)} = \bar{0} = 0 \tag{4.1}$$

Per la seconda affermazione della nostra tesi è immediato che

$$(x-\alpha)(x-\bar{\alpha}) = x^2 - 2\,\mathrm{Re}(\alpha)x + |\alpha|^2 \in \mathbb{R}[x]$$

Supponiamo quindi che α sia uno zero di $p(x)$ di molteplicità e. Allora se per assurdo $\bar{\alpha}$ avesse molteplicità $f > e$, potremmo scomporre (in $\mathbb{C}[x]$) il polinomio $p(x)$ come

$$p(x) = (x-\alpha)^e (x-\bar{\alpha})^e g(x)$$

con $g(x) \in \mathbb{R}[x]$. Siccome $f > e$, allora $\bar{\alpha}$ è una radice di $g(x)$, che tuttavia non ha α come radice. Questo è assurdo, in quanto α è il coniugato di $\bar{\alpha}$.

Analogamente se $e > f$ ripetiamo il ragionamento, ma considerando $z = \bar{\alpha}$ e $\bar{z} = \alpha$. □

Corollario 4.4.5. *Un polinomio $p(x) \in \mathbb{R}[x]$ è irriducibile se e solo se è di primo grado, o è di secondo grado con discriminante negativo.*

Dimostrazione. Se $p(x)$ ha grado pari a 1, allora è irriducibile.

Se $p(x)$ ha secondo grado con discriminante negativo, allora non ha soluzione reali. Siccome $p(x)$ è di secondo grado, allora è irriducibile.

D'altra parte supponiamo che $p(x)$ sia monico. Sappiamo che le radici di $p(x)$ in $\mathbb{C}[x]$ si partizionano come $\{u_i\}_{i=1}^r \subseteq \mathbb{R}$ e $\{w_j, \bar{w}_j\}_{j=1}^s \subseteq \mathbb{C} \setminus \mathbb{R}$. Allora $p(x)$ si scompone in $\mathbb{C}[x]$ come

$$\begin{aligned} p(x) &= \prod_{i=1}^{r}(x-u_i) \prod_{j=1}^{s}(x-w_j)(x-\bar{w}_j) \\ &= \prod_{i=1}^{r}(x-u_i) \prod_{j=1}^{s}(x^2 - 2\,\mathrm{Re}(w_j)x + |w_j|^2) \end{aligned}$$

che tuttavia è una scomposizione in $\mathbb{R}[x]$ come prodotto di polinomi di primo e secondo grado. □

Parliamo infine dei polinomi in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$. In generale la scomposizione in tali anelli può essere estremamente difficoltosa, come sottolineato dal Corollario 4.4.10.

Innanzitutto osserviamo come la scomposizione in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$ siano estremamente legate.

Proposizione 4.4.6. *Sia un polinomio $p(x) \in \mathbb{Z}[x]$ primitivo, cioè tale che il massimo comune divisore dei coefficienti sia pari a 1. Allora $p(x)$ è irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$.*

La dimostrazione di questo fatto, in ambienti più generali, si troverà a pagina 254.

Diamo ora risultati sui polinomi a coefficienti in $\mathbb{Z}[x]$.

Proposizione 4.4.7. *Sia $p(x)$ un polinomio in $\mathbb{Z}[x]$, e consideriamo una radice $\alpha/\beta \in \mathbb{Q}$ tale che α e β siano coprimi. Se $p = \sum_i a_i x^i$, allora α divide a_0 e β divide a_n.*

Dimostrazione. Siccome α/β è una radice di $p(x)$, allora

$$0 = a_n \frac{\alpha^n}{\beta^n} + \cdots + a_1 \frac{\alpha}{\beta} + a_0$$

Moltiplicando per β^n otteniamo

$$\alpha(a_n \alpha^{n-1} + \cdots + a_1 \alpha \beta^{n-1}) = -a_0 \beta^n$$

Quindi α divide $-a_0\beta^n$, e siccome α e β sono coprimi abbiamo che α divide a_0.

Analogamente β divide a_n, in quanto vale l'uguaglianza

$$-a_n \alpha^n = \beta(a_{n-1}\alpha^{n-1} + \cdots + a_0 \beta^{n-1}) \qquad \square$$

Proposizione 4.4.8. *Sia $f(x) \in \mathbb{Z}[x]$, e consideriamo un primo p. Se $p \nmid a_n$ e la riduzione $\bar{p}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$, allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.*

Dimostrazione. Supponiamo che $p(x)$ si riduca come $g(x)h(x)$. Allora $\bar{f}(x)$ si scompone come $\bar{g}(x)\bar{h}(x)$. I gradi di $\bar{g}(x)$ e $\bar{h}(x)$ on possono calare, in quanto $p \nmid a_n$ e quindi

$$\deg(\bar{f}) = \deg(\bar{g}) + \deg(\bar{h}) \leq \deg(g) + \deg(h) = \deg(f) = \deg(\bar{f})$$

Siccome i gradi di $\bar{g}$ e $\bar{h}$ non sono calati di grado, essi non sono invertibili. Quindi $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ è una riduzione di $\bar{f}(x)$. $\square$

Proposizione 4.4.9 (Criterio di Eisenstein)**.** *Sia $f(x) \in \mathbb{Z}[x]$ e consideriamo un primo p. Se*

1. *$p \nmid a_n$;*
2. *$p \mid a_i$ per ogni $i < n$;*
3. *$p^2 \nmid a_0$,*

allora $f(x)$ è irriducibile.

Dimostrazione. Supponiamo per assurdo che $f(x)$ si riduca come $g(x)h(x)$. Allora se effettuiamo una riduzione modulo p, sfruttando la prima e seconda ipotesi otteniamo

$$a_n x^n = \bar{g}(x)\bar{h}(x)$$

Siccome $\mathbb{Z}/p\mathbb{Z}$ è un campo, allora in $\mathbb{Z}/p\mathbb{Z}[x]$ vale la Proposizione 4.3.8. Quindi $\bar{g}(x) = \bar{b}_m x^m$ e $h = \bar{c}_{n-m}x^{n-m}$. Quindi in particolare $b_0 \equiv c_0 \equiv 0 \pmod{p}$.

In conclusione $a_0 = b_0 c_0 \equiv 0 \pmod{p^2}$, che è assurdo per la terza ipotesi dell'enunciato. □

Corollario 4.4.10. *Per ogni naturale $n > 0$, esistono infiniti polinomi in $\mathbb{Q}[x]$ irriducibili di grado n.*

Dimostrazione. Per il criterio di Eisenstein i polinomi $x^n + p$ sono irriducibili in $\mathbb{Z}[x]$ per ogni primo p, e quindi in $\mathbb{Q}[x]$ in quanto sono polinomi primitivi. □

4.5 Quozienti di $K[x]$

Definizione 4.5.1. Consideriamo un anello dei polinomi $K[x]$, ed un polinomio $f(x)$. Definiamo l'ideale generato $(f(x))$ come l'insieme

$$(f(x)) = \{q(x)f(x) \mid q(x) \in K[x]\}$$

e definiamo il quoziente $K[x]/(f(x))$ come l'insieme delle classi dato dalla relazione di equivalenza

$$g(x) \sim h(x) \Leftrightarrow f(x) \mid g(x) - h(x)$$

Ricordiamo che una K-algebra è un anello A, che contiene un campo K su cui A sia un K-spazio vettoriale. La dimensione di una K-algebra è posta come la dimensione di A come K-spazio vettoriale.

Proposizione 4.5.2. *L'insieme $K[x]/f(x)$ è una K-algebra di dimensione finita, con la struttura di anello data dalle operazioni*

$$[g(x)] + [h(x)] = [g(x) + h(x)]$$
$$[g(x)][h(x)] = [g(x)h(x)]$$

ed una K-base data da $\{[1], \dots, [x^{n-1}]\}$ con $n = \deg(f)$.

Dimostrazione. Siccome $(K[x], +)$ è commutativo, sappiamo che il sottogruppo $((f(x)), +)$ è normale. Quindi l'operazione di somma è ben definita. Infine osserviamo che prese due classi

$$[g(x)] = [g'(x)]$$
$$[h(x)] = [h'(x)]$$

allora

$$g'(x) = g(x) + m(x)f(x)$$
$$h'(x) = h(x) + n(x)f(x)$$

e quindi

$$[g'(x)h'(x)] = [g(x)h(x)+g(x)n(x)f(x)+h(x)m(x)f(x)+m(x)n(x)f(x)^2] = [g(x)h(x)]$$

Quindi le operazioni su $K[x]/(f(x))$ sono ben definite, ed è immediato che formino un anello.

Infine dimostriamo che $\{[1], \dots, [x^{n-1}]\}$ sia una K-base. Poniamo $\bar{g} = [g]$.

Preso un elemento $\bar{g} \in K[x]/(f(x))$, allora possiamo porre $g(x) = r(x) + m(x)f(x)$, con $r(x) = 0$ o $\deg(r) < n$.

Quindi $\bar{g} = \bar{r}$ è rappresentato da un polinomio nullo, o di grado al più $n-1$. Quindi è combinazione lineare di $\{\bar{1}, \dots, \bar{x}^{n-1}\}$.

D'altra parte supponiamo che esista una K-combinazione lineare

$$\bar{g} = a_{n-1}\bar{x}^{n-1} + \cdots + a_1\bar{x} + a_0\bar{1}$$

a coefficienti non tutti nulli che coincida con $\bar{0}$.

Questo implica che esiste un polinomio non nullo $\sum a_i x^i$ diviso da f. Siccome f ha polinomio che dia la classe $\bar{0}$. Questo implicherebbe che f divida un polinomio di grado $n-1$. Assurdo. □

Chiudiamo questa breve sezione con due risultati riguardanti elementi invertibili e divisori di 0 di $K[x]/((f(x))$.

Proposizione 4.5.3. *Sia $\bar{g}$ in $K[x]/((f(x))$. Allora*

1. *$\bar{g}$ è invertibile se e solo se $(g, f) = 1$;*

2. *$\bar{g}$ è divisore di 0 se e solo se $(g, f) \neq 1$.*

Dimostrazione. 1. Affermare che $\bar{g} \in K[x]/(f(x))$ è invertibile è equivalente a dire che esiste un polinomio $\bar{h}$ per cui $\bar{g}\bar{h} = \bar{1}$. Cioè stiamo dicendo che esiste un polinomio $\bar{r}$ per cui $1 = g(x)h(x) - r(x)f(x)$. Grazie ai coefficienti di Bezout questo è equivalente ad affermare che $(f, g) = 1$.

2. D'altra parte $\bar{g}\bar{h} = \bar{0}$ per qualche elemento non nullo $\bar{h}$ se e solo se $f(x)$ divide $g(x)h(x)$.

   Siccome in $K[x]$ vale il teorema di fattorizzazione unica in elementi irriducibili, allora i fattori primi di $f(x)$ non possono tutti dividere $h(x)$, in quanto $\bar{h} \neq \bar{0}$. Quindi $g(x)$ ammette un fattore primo in comune con $f(x)$, e $(g, f) \neq 1$.

   D'altra parte se $(f, g) \neq 1$, cioè g ammette un fattore primo in comune con f, è sufficiente considerare il polinomio h dato dal prodotto dei fattori primi di f rimanenti. Per unicità della fattorizzazione f non può dividere h, mentre divide gh.

□

Corollario 4.5.4. *Sono fatti equivalenti che $K[x]/(f(x))$ sia un campo, che sia un dominio e che f sia irriducibile.*

Dimostrazione. Immediata conseguenza dal risultato precedente. □

4.6 Ideali

In questa sezione andremo a trattare in maniera sistematica alcune nozioni fondamentali sugli ideali. Procediamo iniziando a definire il concetto stesso di ideale.

Definizione 4.6.1. Preso un anello A, un ideale I di A è un sottogruppo di $(A, +)$ che assorba rispetto alla moltiplicazione, cioè tale che

$$xa \in I \ \forall x \in I, a \in A$$

Sugli ideali è possibile definire una serie di operazioni, che potremmo dimostrare restituiscono degli ideali.

Proposizione 4.6.2. *Sia una famiglia $\{I_j\}_{j\in J}$ di ideali di A. Allora la loro intersezione è ancora un ideale.*

Dimostrazione. Immediata verifica. □

Definiamo adesso l'ideale generato.

Definizione 4.6.3. Sia A un anello, e consideriamo un sottoinsieme $S \subseteq A$. Definiamo l'ideale generato (S) come

$$(S) := \{\, a_1 s_1 + \cdots + a_n s_n \mid a_i \in A, s_i \in S \,\}$$

Se S è dato da un solo elemento, l'ideale $I = (s)$ viene detto *principale*, e ha la forma $\{as \mid a \in A\}$.

Come nel caso di sottospazi vettoriali generati vale il seguente risultato.

Proposizione 4.6.4. *L'ideale generato (S) coincide con l'intersezione degli ideali che contengono I, e quindi in particolare è un ideale.*

Come già annunciato possediamo delle operazioni classiche sugli ideali.

$$\begin{aligned} I + J &:= (I \cup J) = \{i + j \mid i \in I, j \in J\} \\ IJ &:= (\{ij \mid i \in I, j \in J\}) \\ (I : J) &:= \{x \in A \mid xJ \subseteq I\} \\ \sqrt{I} &:= \{x \in I \mid \exists n \in \mathbb{N}\, x^n \in I\} \end{aligned}$$

In particolare definiamo il nilradicale $\mathcal{N}(A) = \sqrt{(0)}$.

Proposizione 4.6.5. *Un ideale I è diverso da A (cioè è proprio) se e solo se non contiene alcun elemento invertibile.*

Dimostrazione. Se I contiene un invertibile x, allora contiene anche l'unità, in quanto $1 = x^{-1}x \in I$ per assorbimento. A questo punto I contiene tutto l'anello, sempre per assorbimento.

Viceversa se I coincide con A, allora contiene 1. □

Corollario 4.6.6. *Un anello A è un campo se e se (0) è l'unico ideale proprio.*

Dimostrazione. Supponiamo che A sia un campo. Allora un ideale I proprio non può contenere elementi non nulli, perché sono tutti invertibili. Quindi deve coincidere con (0).

D'altra parte preso un anello A come da ipotesi, ed un elemento $x \in A \setminus (0)$, allora (x) deve coincidere con tutto A. Quindi contiene 1 ed x è invertibile. □

Ideali estremamente importanti sono gli ideali primi e massimali, che recupereremo tra quale sezione.

Definizione 4.6.7. Un ideale I proprio di A si dice primo se posto $xy \in I$, allora uno tra x e y appartiene a I.

Definizione 4.6.8. Un ideale I proprio di A si dice massimale se posto $I \subseteq J$, allora $J = I$ o $J = A$.

Vogliamo dire che esiste sempre un ideale massimale. Per farlo è necessario introdurre il famoso Lemma di Zorn.

Definizione 4.6.9. Sia $(X, \leq)$ un insieme parzialmente ordinato. Una catena C è un sottoinsieme di X tale che $(X, \leq)$ sia totalmente ordinato

Fatto 4.6.10 (Lemma di Zorn)**.** *Sia $(X, \leq)$ un insieme parzialmente ordinato, tale che ogni sua catena C non vuota ammetta un maggiorante $x \in X$. Allora X ammette un elemento massimale.*

Teorema 4.6.11. *Ogni ideale proprio I in un anello non nullo A è contenuto in un ideale massimale.*

Dimostrazione. Consideriamo l'insieme X degli ideali $J \supseteq I$, e ordiniamolo parzialmente attraverso l'inclusione. Verifichiamo che verifichi le ipotesi del Lemma di Zorn.

Consideriamo quindi una catena $C = \{C_n\}_{n \in N}$, e consideriamo l'insieme $J = \bigcup_{n \in N} C_n$. Affermiamo che è elemento in X massimale per C.

Certamente J contiene I, in quanto quest'ultimo è contenuto in un qualsiasi C_n.

Preso un elemento a nell'anello A e un j in J, allora esiste certamente C_n che contiene j. Quindi aj appartiene a C_n, e in definitiva a J.

Presi infine a e b in J, allora $a \in C_n$ e $b \in C_m$ per qualche m e n. Inoltre possiamo supporre che $C_m \subseteq C_n$, in quanto C è totalmente ordinato. Quindi b appartiene anche a C_n, e $a + b$ sta in $C_n \subseteq J$. □

Corollario 4.6.12. *Un anello A è un campo se e solo se $\{0\}$ è un ideale massimale.*

Dimostrazione. Se A è un campo, allora ogni ideale non banale contiene un elemento invertibile; quindi coincide con tutto l'anello A. Quindi $\{0\}$ è massimale.

D'altra parte se $\{0\}$ è massimale, allora ogni elemento $a \in A$ non nullo genera un ideale (a) che coincide con A. Ergo a è invertibile. □

Passiamo ora a parlare brevemente di ideali primi. Essi entrano in gioco tramite il prossimo teorema:

Teorema 4.6.13. *Dato un anello A ed un ideale I vale la scrittura seguente:*

$$\sqrt{I} = \bigcap_{\substack{P \text{ primo} \\ I \subseteq P}} P \tag{4.2}$$

Dimostrazione. Dimostriamo le due inclusioni separatamente.

($\subseteq$) Consideriamo un $x \in A$ tale che x^n appartenga a I. Allora per un qualsiasi primo P sopra I, x^n appartiene anche a P. Quindi $x \in P$ per la primalità di P.

($\supseteq$) Consideriamo un elemento $a \in A$ che non appartenga a $\sqrt{I}$, e definiamo

$$S = \{a^n \mid n \in \mathbb{N}\}$$

Sia inoltre X l'insieme degli ideali di A che non intersecano S. L'insieme X non è vuoto, in quanto vi appartiene I. Inoltre se consideriamo una catena $\{C_\lambda\}_{\lambda \in \Lambda}$ di $(X, \subseteq)$, allora $J = \bigcup_{\lambda \in \Lambda} C_\lambda$ è un elemento massimale. Infatti se per assurdo a^{n_0} appartenesse a J, allora apparterrebbe ad un certo C_λ. Inoltre J è un ideale per gli stesso argomenti del teorema precedente.

Quindi per il Lemma di Zorn esiste un certo elemento massimale Q. Supponiamo per assurdo che Q non sia un ideale primo. Ciò implica che esistono due elementi x, y in $A \setminus Q$, tali che $xy \in Q$. Siccome x non appartiene a Q, allora (Q, x) contiene strettamente Q. Quindi siccome Q è massimale in X, allora esiste un naturale n per cui $a^n \in (Q, x)$. Cioè a^n si scrive come $q_1 + b_1 x$

per $q_1 \in Q$ e $b_1 \in A$. Allo stesso modo $a^m = q_2 + b_2 y$ per qualche $m \in \mathbb{N}$. Quindi

$$a^{n+m} = q_1 q_2 + q_1 b_2 y + q_2 b_1 x + b_1 b_2 xy$$

che appartiene a Q. Assurdo in quanto Q appartiene a X e non interseca S.

Quindi Q è primo e non contiene $a = a^1$. Quindi a non appartiene alla intersezione di (4.2). □

Corollario 4.6.14.

$$\mathcal{N}(A) = \bigcap_{P \text{ primo}} P$$

4.7 Anelli Quoziente

Procediamo ora ai quozienti di ideali. Procediamo subito con la definizione

Definizione 4.7.1. Sia A un anello, e consideriamo un ideale I. Definiamo l'anello quoziente A/I come l'anello ottenuto dal gruppo $(A/I, +)$ aggiungendo l'operazione

$$[x] \cdot [y] = [xy]$$

Proposizione 4.7.2. *L'anello A/I è un ben definito anello commutativo con identità.*

Dimostrazione. Siccome $(A, +)$ è abeliano, allora $(I, +)$ è normale in $(A, +)$. Quindi A/I ha una ben definita struttura additiva. D'altra parte la struttura moltiplicativa è anche ben definita; infatti per ogni $x, y \in A$ e $i, j \in I$

$$(x + i)(y + j) = xy + xj + yi + ij \in xy + I$$ □

Per ogni quoziente A/I, esiste una naturale proiezione $A \to A/I$, che mappa x in $[x]$.

Vogliamo ora dimostrare un teorema di corrispondenza per anelli, analogo a quello per i gruppi.

Lemma 4.7.3. *Sia $f\colon A \to B$ un omomorfismo di anelli. Allora*

1. *se J è un ideale di B, allora $f^{-1}(J)$ è un ideale di A;*
2. *se I è un ideale di A, allora $f(I)$ è un ideale di* $\mathrm{Im}(f)$.

Dimostrazione. Dalla teoria dei gruppi sappiamo che $f^{-1}(J)$ e $f(I)$ sono entrambi sottogruppi additivi di $(A, +)$.

Per quanto riguarda la struttura moltiplicativa osserviamo che per ogni $f(a) \in \mathrm{Im}(A)$ e $f(i) \in f(I)$ allora

$$f(a)f(i) = f(\underbrace{ai}_{\in I}) \in f(I).$$

Inoltre, per ogni $x \in f^{-1}(J)$ e per ogni $a \in A$ possiamo osservare che

$$f(ax) = f(a)\underbrace{f(x)}_{\in J} \in J \;\Rightarrow\; ax \in f^{-1}(J). \qquad \square$$

Teorema 4.7.4 (di Corrispondenza)**.** *Per ogni anello A e per ogni ideale I sussiste una corrispondenza*

$$\{J \trianglelefteq A \mid I \subseteq J\} \leftrightarrow \{J \trianglelefteq A/I\}.$$

Dimostrazione. Grazie al lemma precedente la bigezione ha la forma

$$I \mapsto \pi(I)$$
$$J \mapsto \pi^{-1}(J)$$

dove π è la proiezione $A \to A/I$. $\square$

Un importante proprietà degli anelli quoziente è il loro legame con gli ideali primi e massimali, legame chiarito col prossimo risultato:

Proposizione 4.7.5. *L'anello A/I è un dominio se e solo se I è primo, ed è un campo se e solo se I è massimale.*

Dimostrazione.

1. L'anello A/I è un dominio se e solo se per ogni $\bar{x}$, $\bar{y}$ in A/I, l'uguaglianza $\bar{x}\bar{y} = \bar{0}$ implica che uno tra $\bar{x}$ o $\bar{y}$ sia $\bar{0}$. Questo è equivalente all'implicazione

   $$xy \in I \Rightarrow x \in I \vee y \in I$$

   che rappresenta esattamente la definizione di ideale primo.

2. L'anello A/I è un campo se e solo se $\bar{0}$ è l'unico ideale massimale. Per il Teorema di Corrispondenza questa affermazione equivale a richiedere che non esista ideale proprio in A contenente I. Otteniamo quindi esattamente che I sia massimale.

$\square$

Corollario 4.7.6. *Se I è massimale, allora è primo.*

Dimostrazione. Immediata conseguenza della proposizione precedente. □

Come per i gruppi, sussistono i Teoremi di Omomorfismo. Le dimostrazioni sono completamente analoghe.

Teorema 4.7.7. *Per ogni morfismo di anelli $\varphi\colon A \to B$ e per ogni ideale $\mathrm{Ker}(\varphi) \subseteq I$ esiste un morfismo di anelli $\tilde{\varphi}\colon A/I \to B$ tale che $\tilde{\varphi} \circ \pi = \varphi$. Inoltre $\mathrm{Ker}(\tilde{\varphi}) = \mathrm{Ker}(\varphi)/I$.*

Corollario 4.7.8. *Nella situazione precedente, se $I = \mathrm{Ker}(f)$ allora $\tilde{\varphi}$ è iniettiva.*

Teorema 4.7.9. *Dato un anello A, e due ideali $I \subseteq J$, allora $(A/I)/(J/I)$ è naturalmente isomorfo a A/J.*

Corollario 4.7.10. *Dato un anello A ed un ideale I, allora la Corrispondenza fra Ideali mantiene la primalità e la massimalità degli ideali.*

Dimostrazione. Preso un certo ideale J contenente I, allora è sufficiente considerare la seguente catena di implicazioni:

$$\begin{aligned} J \text{ è primo/massimale} &\Leftrightarrow A/J \text{ è dominio/campo} \quad \text{per 4.7.5} \\ &\Leftrightarrow (A/I)/(J/I) \text{ è dominio/campo} \quad \text{per 4.7.9} \\ &\Leftrightarrow J/I \text{ è primo/massimale} \end{aligned}$$

□

Teorema 4.7.11. *Dati due anelli I e J, allora sussiste un naturale isomorfismo*

$$\frac{I+J}{I} \simeq \frac{I}{I \cap J}.$$

Chiudiamo col Teorema Cinese per Anelli. Per dare senso all'enunciato ricordiamo la seguente proposizione.

Proposizione 4.7.12. *Dati due ideali I e J, allora IJ è contenuto in $I \cap J$, e coincidono se I, J sono comassimali, i.e. se $I + J = A$.*

Dimostrazione. Per ogni $i \in I$ e $j \in J$, l'elemento ij è contenuto sia in I che in J per la proprietà d'assorbimento degli ideali.

D'altra parte se $I+J=A$, allora l'identità 1 coincide con $i+j$ per qualche $i \in I$ e $j \in J$. Per ogni $x \in I \cap J$ vale l'identità

$$x = xi + xj$$

dove entrambi gli addendi appartengono a IJ. □

Teorema 4.7.13. *Sia A un anello, e siano I, J due ideali, allora la mappa naturale*

$$f\colon A \to A/I \times A/J$$

è un morfismo di anelli, con nucleo pari a $I \cap J$. Inoltre f è suriettiva se e solo se $I + J = A$. In tal caso quindi sussiste l'isomorfismo

$$\frac{A}{IJ} \simeq \frac{A}{I} \times \frac{A}{J}.$$

Dimostrazione. Siccome le proiezioni su A/I e A/J sono morfismi, anche f risulta essere un morfismo per verifica immediata.

Il nucleo è dato da

$$\begin{aligned}\mathrm{Ker}(f) &= \{a \in A \mid [a]_I = [0]_I \wedge [a]_J = [0]_J\} \\ &= \{a \in A \mid a \in I \wedge a \in J\} \\ &= I \cap J.\end{aligned}$$

Guardiamo ora la questione della suriettività.

Se f è suriettiva, allora esiste un certo $a \in A$ tale che

$$f(a) = (I, 1 + J).$$

cioè tale che

$$(a + I, a + J) = (I, a + J).$$

Ciò implica le seguenti:

$$\begin{cases} a + I = I \\ a + J = 1 + J \end{cases} \Rightarrow \begin{cases} a \in I \\ a - 1 \in J \end{cases}$$

Ergo

$$1 = (1 - a) + a \in I + J.$$

D'altra parte supponiamo che $I + J = A$. Allora esistono $i \in I$ e $j \in J$ tali che $i + j = 1$.

Consideriamo ora una certa coppia $(a+I, b+J)$ nel codominio. Definiamo inoltre $x := ai + bj$, e applichiamoci f. Allora otteniamo

$$\begin{aligned} f(x) &= (ai + bj + I, ai + bj + J) \\ &= (bj + I, ai + J) \qquad ai \in I, bj \in J \\ &= (b - bi + I, a - aj + J) \qquad i + j = 1 \\ &= (a + I, b + J). \end{aligned}$$

Quindi f è suriettiva.

Infine, se siamo in questa situazione, allora f è suriettiva e $IJ = I \cap J$, grazie alla proposizione precedente. Quindi per il teorema di omomorfismo

$$A/IJ = A/\operatorname{Ker}(f) \simeq \operatorname{Im}(f) = A/I \times A/J \qquad \square$$

Concludiamo questa sezione con un enunciato, che ci eravamo lasciato indietro, riguardanti gli anelli polinomiali.

Lemma 4.7.14. *Sia A un anello. Allora per ogni ideale primo P, il quoziente $A[x]/P[x]$ è canonicamente identificabile con $A/P[x]$*

Dimostrazione. Consideriamo la mappa da $A[x]$ a $A/P[x]$, che manda un polinomio $f(x)$ nella riduzione $\bar{f}(x)$. La mappa è suriettiva e il suo nucleo è evidentemente l'insieme dei polinomi in $P[x]$. Quindi, per il teoremi di isomorfismo, $A[x]/P[x]$ è isomorfo a $A/P[x]$. $\square$

Proposizione 4.7.15. *Sia A un anello. Allora un polinomio $\sum a_i x^i$ è invertibile in $A[x]$ se e solo se $a_0 \in A^*$ e ogni a_i, con i positivo, è nilpotente.*

Dimostrazione. ($\Leftarrow$) Consideriamo $p(x)$ come da ipotesi. Siccome a_0 è invertibile, possiamo supporre che $a_0 = 1$, e poniamo $p(x) = 1 + q(x)$. I coefficienti di $q(x)$ sono nilpotenti. Quindi, siccome $\mathcal{N}(A[x])$ è un ideale, otteniamo che tutto $q(x)$ è nilpotente. Quindi esiste un naturale $N \geq 1$ tale che $q(x)^N = 0$. A questo punto concludiamo:

$$(1 - q(x))(1 + q(x) + \cdots + q(x)^{N-1}) = 1 - q(x)^N = 1$$

($\Rightarrow$) Supponiamo che esista un polinomio $r(x)$ tale che $p(x) * r(x) = 1$. Allora, valutando in 0, otteniamo $a_0 \cdot r_0 = 1$. Quindi a_0 è invertibile.

Proviamo ora che per ogni $i > 1$, a_i appartiene a $\mathcal{N}(A[x]) = \bigcap P$.
Consideriamo un ideale primo P di $A[x]$. Allora riducendo in $A/P[x]$ otteniamo $\bar{p}(x) \cdot \bar{r}(x) = \bar{1}$. Siccome A/P è un dominio, allora otteniamo $\deg(\bar{p}) + \deg(\bar{r}) = 0$. Ergo $\deg(\bar{p}) = 0$ e $\bar{p}$ appartiene a A/P. Ergo per ogni coefficiente a_i con $i > 1$ si ha che $a_i \in P$. □

4.8 Localizzazioni

Lo scopo di questa sezione è definire un importante strumento dell'algebra commutativa: le localizzazioni. Definiamo la localizzazione nel caso un po' più generale, anche se saremo per lo più interessati ai domini di integrità.

Definizione 4.8.1. Sia A un anello. Un sistema moltiplicativo S è un sottoinsieme di A, che non contiene lo 0, contiene l'unità, ed è chiuso per moltiplicazione.

Definizione 4.8.2. Sia A un anello, e S un suo sistema moltiplicativo. Definiamo la localizzazione $S^{-1}A$ come l'insieme quoziente $A \times S/\sim$, dove

$$\frac{a}{b} \sim \frac{c}{d} \leftrightarrow \exists t \in S \text{ s.t. } t(ad - bc) = 0$$

La relazione definita sopra è in effetti una relazione di equivalenza. Perché ciò sia vero, tuttavia è necessario definirla in tal modo. Infatti supponiamo che $a \in A$ è un divisore di 0, tale che per qualche $s \in S$, $as = 0$. Allora

$$\frac{a}{1} = \frac{as}{s} = \frac{0}{s} = \frac{0}{1}.$$

Quindi se $\sim$ è transitivo, deve essere che

$$\exists t \in S \text{ t.c. } ta = 0$$

E difatti basta porre $t := s$.

Nel caso di A un dominio di integrità la relazione di equivalenza si semplifica, ed è analoga a quella presente su $\mathbb{Q}$.

$$\frac{a}{b} \sim \frac{c}{d} \leftrightarrow ad - bc = 0$$

Teorema 4.8.3. *L'insieme $S^{-1}A$ è un anello, e la mappa $A \xrightarrow{i} S^{-1}A$, che manda a in $a/1$, manda S in invertibili.*

Dimostrazione. Non verranno fatte tutte le verifiche (che sono abbastanza tediose). Definiamo somma e prodotto come nel caso delle frazioni:

$$a/b + c/d := (ad + bc)/(bd)$$
$$a/b \cdot c/d := (ac)/(bd)$$

Su può verificare che in effetti i risultati non dipendono dai rappresentati scelti per le frazioni.

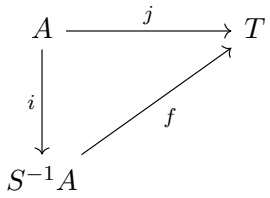
Infine per ogni $s \in S$ l'elemento $s/1 \in S^{-1}A$ è invertibile. Infatti ha come inverso $1/s$. □

Teorema 4.8.4 (Proprietà Universale delle Localizzazioni)**.** *La coppia* $(A, S^{-1}A, i)$ *soddisfa la seguente proprietà universale: per ogni altra terna* (A, T, j)*, dove*

1. T *è un anello;*

2. j *manda* S *in invertibili,*

esiste un unica mappa $f\colon S^{-1}A \to T$ *tale che*



commuti.

Dimostrazione. Consideriamo un elemento $a \in A$, ed notiamo innanzitutto che $f(a/1)$ deve necessariamente essere $j(a)$.

D'altra parte, un elemento $s \in S$ soddisfa

$$1 = f(s/1) \cdot f(1/s)$$

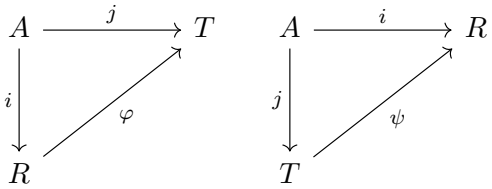
Quindi, siccome $f(s/1) = j(s)$ è invertibile, allora $f(1/s)$ è precisamente $j(s)^{-1}$. Abbiamo quindi ottenuto che per ogni $a \in A$ e $s \in S$ deve necessariamente essere che

$$f(a/s) = j(a) \cdot j(s)^{-1}$$

D'altra parte è immediato verificare che una tale f non dipende dal rappresentante scelto per la frazione, e anche che f sia un morfismo. □

Teorema 4.8.5. *Date due coppie (A, R, i) e (A, T, j) che soddisfano la proprietà universale, allora sono canonicamente isomorfe: esiste un unico isomorfismo $\varphi\colon R \to T$ tale che $\varphi \circ i = j$.*

Dimostrazione. Siccome i e j mandano S in invertibili, per la proprietà universale esistono uniche $\varphi\colon R \to S$ e $\psi\colon T \to R$ tali che i digrammi seguenti commutino:



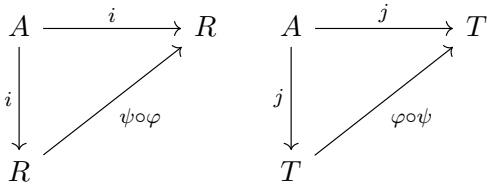
Inoltre, osserviamo che

$$\psi \circ \varphi \circ i = \psi \circ j = i$$

e analogamente

$$\psi \circ \varphi \circ j = \psi \circ \ j = j$$

Questo implica che $\psi \circ \varphi$ e $\varphi \circ \psi$ si innestano in diagrammi



Per unicità data dalla proprietà universale, allora $\psi \circ \varphi = id_T$ e $\varphi \circ \psi = id_R$. □

Data una localizzazione $S^{-1}A$ sussiste un teorema corrispondenza, che mostra un comportamento rovesciato rispetto a quello dei quozienti.

Teorema 4.8.6. *Sia A un anello.*

1. *Dato un ideale I di A, allora l'insieme $S^{-1}I := \{a/s \mid a \in A\, s \in S\}$ è un ideale, e coincide con il generato da $i(I)$.*

2. *$S^{-1}A$ è proprio se e solo se I non interseca S.*

3. *Dato un ideale J di $S^{-1}A$, allora $S^{-1}i^{-1}(J) = J$.*

4. Sussiste la seguente corrispondenza tra ideali primi:

$$\{P \trianglelefteq A \mid P \text{ primo t.c. } P \cap S = \emptyset\} \leftrightarrow \{Q \trianglelefteq S^{-1}A \mid Q \text{ primo}\}$$
$$P \mapsto S^{-1}P$$
$$i^{-1}(Q) \mapsfrom Q$$

Dimostrazione. 1. Se a/s è un elemento di $S^{-1}A$, e i/t è un elemento di $S^{-1}I$, allora

$$a/s \cdot i/t = (ai)/(st) \in S^{-1}I$$

Inoltre, se i/s e j/t appartengono a $S^{-1}I$, allora

$$i/s + j/t = (it + sj)/st$$

appartiene ancora a $S^{-1}I$.

Quindi $S^{-1}I$ è un ideale. Dobbiamo verificare che coincide con l'estensione di $i(I)$.
Certamente $(i(I))$ contiene $S^{-1}I$. D'altra parte se consideriamo un elemento i/s in $S^{-1}I$, allora esso coincide con $i/1 \cdot 1/s$, e quindi appartiene all'ideale $(i(I))$.

2. Se $I \cap S$ contiene un certo elemento s, allora $1 = s/s$ appartiene a $S^{-1}I$, che quindi non è proprio.
D'altra parte se $S^{-1}I = S^{-1}A$, allora esiste $1 = i/s$ per $i \in I$ e $s \in S$. Detto altrimenti, esiste $t \in S$ tale che

$$t(s - i) = 0 \;\Rightarrow\; I \ni ti = ts \in S$$

3. L'insieme $i(i^{-1}(J))$ è contenuto in J. Quindi anche il generato deve essere contenuto.

Viceversa, preso a/s in J, allora $a/1 = s \cdot a/s$ deve ancora appartenere a J. Quindi $i^{-1}(J)$ contiene a, e a/s appartiene a $S^{-1}i^{-1}(J)$.

4. Innanzitutto osserviamo che se Q è un ideale primo di $S^{-1}A$, allora $i^{-1}(Q)$ è un ideale primo, per teoremi generali, e non interseca S in quanto Q è proprio.
D'altra parte, se P è un ideale primo di A tale che $P \cap S = \emptyset$, allora $S^{-1}P$ è proprio. Dobbiamo verificare che sia primo.

Consideriamo quindi a/s e b/t tali che $(ab)/(st)$ appartenga a $S^{-1}P$. Questo implica che esistano $u, v \in S$, $p \in P$ tali che

$$v(abu - stp) = 0 \;\Rightarrow\; abvu = pvst$$

Il termine di destra appartiene a P, quindi anche quello di sinistra. Tuttavia, vu appartiene a S, che non interseca P. Ergo $ab \in P$, e quindi $a \in P$ o $b \in P$. Otteniamo quindi che a/s appartiene a $S^{-1}P$ o b/t appartiene a $S^{-1}P$.

Dimostriamo che $i^{-1}(S^{-1}P)$ coincide con P. Infatti, se $a/1$ è equivalente a p/s per $a \in A$, $s \in S$ e $p \in P$, allora esiste $t \in S$ tale che

$$tsa = pt \in P$$

Ergo, siccome come prima ts non può appartenere a P, otteniamo che a appartiene a P.

Viceversa, dal punto precedente sappiamo che $S^{-1}i^{-1}(Q) = Q$.

□

In generale, abbiamo provato che esiste una surgezione

$$\{I \trianglelefteq A \mid I \cap S = \emptyset\} \twoheadrightarrow \{J \trianglelefteq S^{-1}A\}$$
$$I \mapsto S^{-1}I$$

Al contrario, invece, è generalmente falso che otteniamo tutti gli ideali di A applicando i^{-1} a ideali di $S^{-1}A$.

Un tipo di localizzazioni sono le cosiddette "localizzazioni su un ideale primo". Il senso di questa definizione viene dal prossimo risultato.

Proposizione 4.8.7. *Sia A un anello, e P un suo ideale primo. Allora $A \setminus P$ è un sistema moltiplicativo.*

Dimostrazione. Ovviamente $0 \notin A \setminus P$. Inoltre, siccome P è proprio, allora $1 \in A \setminus P$.

Infine se r, s non appartengono a P, allora neanche il prodotto ci appartiene per primalità. □

Definizione 4.8.8. Definiamo la localizzazione a P come la localizzazione $A_P := (A \setminus P)^{-1}A$.

Chiudiamo la sezione col trattare il caso dei domini di integrità.

Proposizione 4.8.9. *Se A è un dominio, anche $S^{-1}A$ è un dominio, e $A \to S^{-1}A$ è un'immersione.*

Dimostrazione. Se imponiamo che $a/1 = 0$, allora otteniamo $a - 0 = 0$. □

Nel caso dei domini sussiste il più "grande campo che contiene A", cioè il **campo delle frazioni**.

Definizione 4.8.10. Dato un dominio A, definiamo il campo delle frazioni come $Q(A) := A_{(0)}$.

Teorema 4.8.11. *La tripla $(A, Q(A), i)$ soddisfa la seguente proprietà universale: per ogni altra tripla (A, K, j) tale che*

1. *K è un campo;*
2. *$j \colon A \to K$ è iniettiva,*

esiste un'unica immersione $f \colon Q(A) \to K$ tale che $f \circ i = j$.

Inoltre, per ogni altra tripla (A, K, i) che soddisfa la stessa proprietà universale esiste un unico isomorfismo $f \colon Q(A) \to K$ tale che $f \circ i = j$.

Dimostrazione. Semplice specializzazione del teorema già visto. □

Osserviamo che possiamo dare un controesempio all'osservazione precedente. Preso infatti un dominio A, allora il campo delle frazioni contiene solamente $\{0\}$ come ideale proprio. Quindi certamente non possiamo ottenere tutti gli ideali di A via i^{-1}.

4.9 Domini Euclidei e a Ideali Principali

Questa sezione si concentrerà sul concetto di *divisibilità*. Iniziamo con la definizione.

Definizione 4.9.1. Dato un anello A, diciamo che a divide b se esiste un elemento $c \in A$ tale che $b = ca$. Equivalentemente, se $(b) \subseteq (a)$.

Definizione 4.9.2. Dato un anello A, due elementi a e a' si dicono associati se generano lo stesso ideale.

Proposizione 4.9.3. *Se A è un dominio, allora le seguenti sono equivalenti:*

1. *a e a' sono associati;*

2. *esiste un invertibile $u \in A^*$ tale che $a = ua'$.*

In generale invece, la seconda condizione è più forte.

Dimostrazione. (1. $\Rightarrow$ 2.) Se $a = xa'$ e $a' = ya$, allora otteniamo $a = yxa$. Questo implica, considerando che A è un dominio, che $xy = 1$. Ergo x e y sono invertibili.

(2. $\Rightarrow$ 1.) Se $a = ua'$ con $u \in A^*$, allora possiamo dire che $ya = a'$, con y l'inverso di u. □

Definizione 4.9.4. Sia A un arbitrario anello, e x, y due suoi elementi. Diciamo che d è un loro massimo comune divisore, se

1. d divide sia x che y;

2. per ogni c che divide x e y, allora c divide anche d.

Come nel casi già visti, due massimi comuni divisori sono coniugati.

Illustriamo brevemente come si possa ricondurre la questione di mcd a questioni di ideali.

Proposizione 4.9.5. *Dati x, y, allora un loro mcd è un generatore di un elemento* minimo *di*

$$\{(z) \trianglelefteq A \mid (x, y) \subseteq (z)\}$$

Dimostrazione. Siccome d divide x e y, allora (x, y) è incluso in (z).

Inoltre, se (x, y) è incluso in qualche (c), allora c divide x e y. Quindi c divide d e (d) è incluso in (c). □

Proposizione 4.9.6. *Se (x, y) ammettono coefficienti di Bezout a e b tali che $ax + by = d$, allora $(x, y) = (d)$.*

Dimostrazione. I coefficienti di Bezout forniscono esattamente l'inclusione $(d) \subseteq (x, y)$. □

Proposizione 4.9.7. *Se ogni ideale della forma (x, y) è principale, allora ogni ideale finitamente generato è principale.*

Dimostrazione. Sia $I = (a_1, \ldots, a_n)$, e procediamo per induzione su n.

Per $n = 1$, I è già principale.

Per $n = 2$, allora I ricade nella casistica dell'ipotesi.

Per $n > 2$, innanzitutto sappiamo che $(a_1, \ldots, a_{n-1}) = (z)$. Quindi $I = (z, a_n)$, che quindi è principale. □

Procediamo con la definizione di primi e irriducibili, nella più vasta generalità.

Definizione 4.9.8. Un elemento p non nullo e non invertibile è primo se $p \mid xy$ implica $p \mid x$ o $p \mid y$.

Definizione 4.9.9. Un elemento p non nullo e non invertibile è irriducibile se l'uguaglianza $p = xy$ implica x invertibile o y invertibile.

Queste definizioni possono essere rilette nel contesto degli ideali.

Proposizione 4.9.10. *Sia A un anello. Allora p, non nullo e non invertibile, è primo se e solo se (p) è un ideale primo.*

Dimostrazione. Imponiamo $xy \in (p)$. Allora p divide xy, quindi, per primalità, p divide x o y. Ergo $x \in (p)$ o $y \in (p)$. □

Proposizione 4.9.11. *Sia A un anello. Allora p, non nullo e non invertibile, è irriducibile se e solo se (p) è un ideale massimale* tra gli ideali principali propri.

Dimostrazione. Supponiamo $(p) \subseteq (z)$, con (z) proprio. Allora $p = qz$. Per irriducibilità, sappiamo che o z è invertibile, impossibile in quanto (z) è proprio, o q è invertibile. Otteniamo quindi che $(p) = (z)$. □

Proposizione 4.9.12. *Se A è un dominio, allora ogni primo è irriducibile.*

Dimostrazione. Supponiamo che p sia un primo, e scomponiamolo come $p = xy$. Siccome p divide il prodotto, deve dividere uno dei due fattori. Supponiamo che p divida x.

Quindi $p = xy = puy$ per un certo $u \in A$. Questo implica, siccome A è un dominio, che $uy = 1$. Ergo y è invertibile. □

A questo punto andiamo a considerare delle prime tipologie di domini di integrità, in cui la divisione si discosta sempre di più dalla divisione euclidea.

Domini Euclidei

Definizione 4.9.13. Un dominio A si dice un Dominio Euclideo, se ammette una funzione $d\colon A \setminus \{0\} \to \mathbb{N}$, detta grado, tale che

1. $d(x) \leq d(xy)$ per ogni $x, y \in A \setminus \{0\}$;
2. per ogni $x \in A$, e per ogni $y \in A \setminus \{0\}$, esistono $q, r \in A$ tali che $x = qy + r$ e $r = 0$ o $d(r) < d(y)$.

Esempi di domini euclidei sono $\mathbb{Z}$, dove possiamo prendere $d = |\cdot|$, e $K[x]$ con K campo, in cui possiamo prendere $d = \deg$.

Enunciamo ora delle proposizioni, che ci mostrano come i Domini Euclidei siano estremamente "semplici".

Proposizione 4.9.14. *Sia A un Dominio Euclideo. Allora posso trovare il massimo comun divisore di ogni coppia (x, y) tramite l'Algoritmo di Euclide. Inoltre, lo stesso algoritmo permetto di ricavare i coefficienti di Bezout.*

Dimostrazione. Analogo agli interi. □

Quindi sappiamo che ideale finitamente generato è principale. In verità sappiamo di più, come mostrano le prossime proposizioni.

Proposizione 4.9.15. *Sia A un Dominio Euclideo. Allora ogni ideale è principale, ed è generato da un arbitrario elemento di grado minimo (o I è nullo).*

Dimostrazione. Sia I un ideale non nullo. Allora possiamo considerare l'insieme $\{d(a) \mid a \in I\} \subseteq \mathbb{N}$. Esso ha un elemento minimo $d(x)$.

Certamente (x) è incluso in I.

D'altra parte, preso $y \in I$, possiamo eseguire la divisione euclidea, e porre $y = qx + r$. Siccome $d(x)$ è un minimo, allora $r = 0$
Quindi $r = 0$, x divide y e y appartiene a (x). □

Proposizione 4.9.16. *Sia A un Dominio Euclideo. Allora gli elementi di grado minimo sono esattamente gli elementi invertibili.*

Dimostrazione. Per la proposizione precedente, se prendiamo un elemento x di grado minimo in A, allora $(x) = A$. Cioè x è invertibile.

Viceversa, supponiamo $(x) = A$. Allora per ogni $y \in A$ sappiamo che esiste q tale che $y = qx$. Ergo $d(y)$ coincide con $d(qx) \geq d(x)$. Quindi $d(x)$ è un minimo. □

Domini a Ideali Principali

Definizione 4.9.17. Un dominio si dice un Dominio a Ideali Principali se ogni ideale è principale.

Proposizione 4.9.18. *Dato un Dominio a Ideali Principali, allora ogni coppia di numeri ammette un massimo comun divisore e coefficienti di Bezout.*

Dimostrazione. Semplice conseguenza del fatto che (x, y) è principale. □

Va osservato, tuttavia, che non esiste un algoritmo che trovi il massimo comun divisore.

Questa categoria di anelli ammette "pochi" ideali primi. In termini tecnici, il prossimo risultato di dice infatti che ogni dominio a ideali principali ha dimensione di Krull 1 (o è nullo).

Proposizione 4.9.19. *Dato un Dominio a Ideali Principali, allora ogni ideale primo non nullo è massimale.*

Dimostrazione. Sia $P = (p)$ un ideale primo non nullo. Allora p è primo. Quindi è irriducibile. Quindi (p) è massimale tra gli ideali principali propri. Siccome tutti gli ideali sono principali, allora otteniamo che (p) è massimale. □

A questo punto ci si può chiedere se esistano Domini a Ideali Principali che non sono Euclidei. In effetti ciò è vero, ma la situazione è molto sottile.

Proposizione 4.9.20. *L'anello* $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ *non è un Dominio Euclideo, ma è a Ideali Principali.*

La dimostrazione si può trovare nell'appendice.

4.10 Domini a Fattorizzazione Unica

Concludiamo con l'ultima categoria di domini che riusciamo a trattare decentemente. Innanzitutto dobbiamo definire cosa vuol dire per due fattorizzazioni essere "uguali".

Definizione 4.10.1. Due fattorizzazioni $p_1 \dots p_h = q_1 \dots q_k$ sono considerate uguali se $h = k$, e se esiste una permutazione σ di $\{1, \dots, k\}$ tale che p_i è coniugato a $p_{\sigma(i)}$.

In generale fattorizzazioni in primi/irriducibili potrebbero non esistere. Le fattorizzazioni in primi sono tuttavia particolari.

Proposizione 4.10.2. *Sia A un dominio. Se un elemento ammette una fattorizzazione in primi, allora essa è unica.*

Dimostrazione. Supponiamo $p_1 \dots p_h = q_1 \dots q_k$. e procediamo per induzione sul minimo tra h e k.

Se siamo nella situazione $p = q_1 \dots q_n$, allora dobbiamo provare che $n = 1$. Se per assurdo $n \geq 2$, allora dall'irriducibilità di p otteniamo che uno dei q_i è invertibile. Ciò non può essere in quanto q_i è primo.

Supponiamo ora $1 < h \leq k$. Allora p_1 divide il prodotto $q_1 \dots q_k$. Siccome è primo, deve dividere uno dei fattori. Sempre perché A è un dominio, otteniamo $p_2 \dots p_h = uq_2 \dots q_k$, dove $q_1 = up_1$. Siccome q_1 è irriducibile, e p_1 è primo, allora u deve essere invertibile. A questo punto si procede per induzione. □

Le fattorizzazioni interessanti tuttavia sono quelle in irriducibili.

Definizione 4.10.3. Dato un dominio A, esso è un Dominio a Fattorizzazione Unica se ogni elemento non nullo e non invertibile si fattorizza in maniera unica come prodotto di irriducibili.

Proposizione 4.10.4. *Dato un Dominio a Fattorizzazione Unica A, allora ogni coppia di elementi ammette un massimo comune divisore (ma può non ammettere coefficienti di Bezout)*

Dimostrazione. È sufficiente osservare che possiamo ricavare un massimo comune divisore tramite la regole imparate alla scuola: *dati $x, y \in A$, e scritta la loro fattorizzazione in irriducibili, allora un mcd è dato dal prodotto dei fattori comuni, ognuno preso col minimo esponente.* □

I domini in questione in verità hanno una caratterizzazione estremamente più utile, che non dimostreremo.

Teorema 4.10.5. *I Domini a Fattorizzazione Unica sono equivalentemente caratterizzati come i domini per cui*

1. *ogni elemento irriducibile è primo;*
2. *ogni catena ascendente di ideali principali si stabilizza; i.e. per ogni sequenza* $(a_0) \subseteq (a_1) \subseteq \dots$, *allora definitivamente gli ideali coincidono.*

Approssimativamente, la seconda condizione si occupa dell'esistenza di una fattorizzazione in irriducibili, mentre la prima condizione si occupa dell'unicità.

Proposizione 4.10.6. *Se A è un Dominio a Ideale Principali, allora A è a Fattorizzazione Unica.*

Dimostrazione. Usiamo le la caratterizzazione del Teorema 4.10.5.

(1.) Supponiamo che p è un elemento irriducibile. Allora sappiamo che (p) è massimale tra gli ideali principali propri. Siccome A è a Ideali Principali, allora (p) è un ideale massimale, quindi primo. Ergo p è primo.

(2.) Consideriamo una catena ascendente $(a_0) \subseteq (a_1) \subseteq \dots$. Possiamo definire $I := \bigcup(a_i)$; esso è necessariamente principale. Poniamo $(z) = I$.

A questo punto, sappiamo che z appartiene ad un certo (a_{n_0}).

Affermiamo che per ogni $i \geq n_0$ vale l'uguaglianza $(a_i) = (a_{n_0})$.

Certamente conosciamo l'inclusione $(a_i) \supseteq (a_{n_0})$.

D'altra parte, abbiamo l'inclusione

$$(a_i) \subseteq I = (z) \subseteq (a_{n_0}) \qquad \square$$

Diamo ora invece tre non-esempi.

Esempio. L'anello $K[x^{1/n}]_{n\geq 1}$ (che si può pensare come ottenuto dall'anello dei polinomi in un numero numerabile di variabili $K[x_n]_{n\geq 1}$ dopo che valutiamo x_n nella nuova variabile $x^{1/n}$). In questo caso abbiamo una catena di ideali che non stabilizza: $(x) \subseteq (x^{1/2}) \subseteq \dots$.

Esempio. Prendiamo l'insieme degli interi algebrici, definito come

$$\mathcal{O} = \{\alpha \in \mathbb{C} \mid \exists f \in \mathbb{Z}[x] \text{ monico t.c. } f(\alpha) = 0\}$$

Questo risulta essere in effetti un anello. Inoltre, è chiuso per estrazione di radice: se $f(\alpha) = 0$ allora $g(\sqrt{\alpha}\,) = 0$ con $g(x) = f(x^2)$. Questo implica che questo anello ha la seguente particolarità: non esistono proprio elementi irriducibili. Infatti per ogni $\alpha \in \mathcal{O}$ allora $\alpha = \sqrt{\alpha} \cdot \sqrt{\alpha}$.

Esempio. Consideriamo $Z[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Allora 2 è irriducibile: se imponiamo $2 = (a+b\sqrt{-5})\cdot(c+d\sqrt{-5})$, allora $4 = (a^2+5b^2)\cdot(c^2+5d^2)$ implica $a = \pm 2, c = \pm 1, d = b = 0$.

Tuttavia 2 non è primo, in quanto 2 divide $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, ma non divide nessuno dei due fattori.

Quindi possiamo aspettarci che esistano fattori in irriducibili non uniche. E difatti 6 ha le scomposizioni $2 \cdot 3$ e $(1+\sqrt{-5}) \cdot (1-\sqrt{-5})$.

L'intera restante parte della sezione sarà devota a dimostrare, tramite il Teorema 4.10.5, la seguente importante risultato.

Teorema 4.10.7. *Se A è un Dominio a Fattorizzazione Unica, allora $A[x]$ è un Dominio a Fattorizzazione Unica.*

In generale non possiamo dire di più.

Proposizione 4.10.8. *L'anello $\mathbb{Z}[x]$ è un Dominio a Fattorizzazione Unica, ma non a Ideali Principali.*

Dimostrazione. Consideriamo $I = (2, x)$. Siccome 2 e x non ammettono divisori comuni, allora è immediato che $mcd(2, x) = (1)$. Se $(2, x)$ fosse principale, allora $(2, x)$ dovrebbe essere generato da 1. Tuttavia, è evidente che l'equazione

$$1 = 2 \cdot a(x) + x \cdot b(x)$$

non è risolubile, in quanto valutata in 0 dà $1 = 2 \cdot a(0)$. □

La dimostrazione del Teorema 4.10.7 procederà per diversi passaggi, dove sostanzialmente verificheremo le ipotesi date dal Teorema 4.10.5.

Per il resto della sezione, A sarà un Dominio a Fattorizzazione Unica.

Iniziamo con le fondamentali definizioni di *contenuto* e *polinomio primitivo.*

Definizione 4.10.9. Dato un polinomio $f \in A[x] \setminus \{0\}$, definiamo un suo contenuto come un massimo comune divisore dei suo coefficienti. f è primitivo se il suo contenuto è invertibile.

Indicheremo con $c(f)$ il contenuto di f. Esso è definito a meno di invertibile, ma questo dettaglio non sarà mai un problema.

Inoltre, preso $f \in A[x]$, possiamo considerare il polinomio primitivo g tale che $f = c(f)g$. Indicheremo g via f'. Osserviamo che nel definire g, e nel dire che esso è primitivo, stiamo pesantemente usando l'esistenza di un massimo comune divisore.

Successivamente proviamo il cosiddetto "Lemma di Gauss" (o almeno una delle sue varianti).

Lemma 4.10.10 (Lemma di Gauss)**.** *Il contenuto è moltiplicativo.*

Dimostrazione. Vogliamo provare che $c(fg) = c(f)c(g)$ (osserviamo che siccome $A[x]$ è un dominio, allora fg non è nullo). Dividiamo la dimostrazione per casi.

1. Se $f = a$ è una constante, allora possiamo concludere, in quanto $c(ag)$ coincide con $ac(g)$, cioè con $c(a)c(g)$.

2. Se f e g sono primitivi, dobbiamo provare che fg è anch'esso primitivo.

   Se così non fosse, allora $c(fg)$ non sarebbe invertibile. Ergo esisterebbe un certo irriducibile (quindi primo) p che divide fg. Quindi, dovrebbe dividere f o g. In ogni caso, p dovrebbe dividere il loro contenuto. Assurdo.

3. Nel caso generale, sappiamo che

   $$c(fg)(fg)' = fg = c(f)c(g)f'g'$$

   Se adesso uguagliamo i contenuti otteniamo

   $$c(fg)c((fg)') = c(f)c(g)c(f'g')$$

   Ma siccome f' e g' sono primitivi, lo è anche il loro prodotto. Ergo $c(f') = c(g') = c((fg)') = 1$ e otteniamo

   $$c(fg) = c(f)c(g)$$ □

A questo punto possiamo iniziare a legare la divisibilità in $A[x]$ con la divisibilità in $Q(A)[x]$, con $Q(A)$ il campo delle frazioni di A. Per il resto della sezione sia $K := Q(A)$.

Proposizione 4.10.11. *Se f e g sono polinomi in $A[x]$ tali che f è primitivo e divide g in $K[x]$, allora lo divide anche in $A[x]$ (con lo stesso quoziente).*

Dimostrazione. Sappiamo che $g = fh$, con h in $K[x]$. Moltiplicando per un denominatore comune dei coefficienti di h, possiamo trovare $d \in A$, tale che $dh =: h_1$ appartenga a $A[x]$. A questo punto otteniamo quindi $df = f\,h_1$.

Quindi $dc(g)$ coincide con $c(f)c(h_1)$, cioè con $c(h_1)$ in quanto f è primitivo. Ergo, d divide $c(h_1)$ (in A). Quindi h, che coincide con h_1/d, cioè con $c(h_1)h_1'/d$, appartiene ad $A[x]$. □

Proposizione 4.10.12. *Se f è un polinomio in $A[x]$, tale che $f = gh$, allora esiste $\delta \in K^*$ tale che δg e $\delta^{-1}h$ appartengono a $A[x]$*

Dimostrazione. Come prima, consideriamo $d \in A$ tale che $g_1 := dg$ appartiene a $A[x]$. In questo caso, f coincide con $c(g_1)g_1'(d^{-1}h)$. Quindi otteniamo che g_1', che è primitivo, divide f in $K[x]$. Per il risultato precedente, sappiamo che il quoziente è in $A[x]$. A questo punto abbiamo concluso, in quanto è sufficiente porre $\delta = d/c(g_1)$, in quanto in questo caso

$$\delta g = dg_1/c(g_1) = dg_1' \in A[x] \qquad \delta^{-1}h = c(g_1)h/d \in A[x]$$ □

Possiamo ora dimostrare il primo risultato vero il Teorema 4.10.7.

Teorema 4.10.13. *I polinomi irriducibili di $A[x]$ sono tutti e soli i polinomi f che soddisfano una tra:*

1. *f appartiene a A, ed è irriducibile in A;*
2. *$\deg(f) \geq 1$, è primitivo, ed è irriducibile in $K[x]$.*

Dimostrazione. Consideriamo $f \in A[x]$, e dividiamo la discussione in base al grado di f.

(1.) Se $\deg(f) = 0$, e f è irriducibile come elemento di $A[x]$, allora lo è come elemento di A. Infatti, supposto $f = gh$, allora uno tra g e h appartiene a $(A[x])^* = A^*$.

D'altra parte supponiamo che f sia irriducibile in A. Allora, se scomponiamo f come gh, per questioni di grado g e h appartengono a A (l'anello è un dominio). Quindi uno dei due appartiene a $A^* = (A[x])^*$.

(2.) Se $\deg(f) \geq 1$, supponiamo che esso sia irriducibile in $A[x]$. Innanzitutto, se scomponiamo f come $c(f)f'$, allora per irriducibilità di f sappiamo che $c(f) \in (A[x])^*$ o $f' \in (A[x])^*$. La seconda condizione non può verificarsi, in quanto $A[x] = A^*$ e f ha grado positivo.
Quindi $c(f)$ è un invertibile in $A[x]$, cioè è un invertibile di A. Abbiamo quindi provato che f è primitivo

Diciamo che f è irriducibile anche in $K[x]$. Scomponiamo f in $K[x]$ come gh. Per la proposizione precedente, sappiamo che possiamo supporre che g e h appartengano a $A[x]$. Inoltre questa supposizione non cambia l'invertibilità (in $K[x]$) di f e g.
Siccome f è irriducibile in $A[x]$, allora uno tra g e h è invertibile in $A[x]$, ergo in $K[x]$.

Viceversa, supponiamo che f è primitivo e irriducibile in $K[x]$. Affermiamo che f è irriducibile in $A[x]$.
Fattorizziamo f come gh via polinomi in $A[x]$. Siccome f è irriducibile in $K[x]$, allora possiamo supporre che g appartenga a $(K[x])^* = K^*$. Quindi g è una costante, ed in particolare è una costante in A. Inoltre, se calcoliamo i contenuti otteniamo

$$1 = c(f) = gc(h)$$

Quindi g appartiene a A^*. □

Teorema 4.10.14. *Ogni irriducibile in $A[x]$ è primo.*

Dimostrazione. Sia $f \in A[x]$, vogliamo dimostrare che è primo. Supponiamo quindi che f divida un prodotto gh. Dividiamo la dimostrazione in base alle casistiche del teorema precedente.

(1.) Se f è un irriducibile in A, allora è anche primo in A. Quindi la divisibilità dei contenuti $c(f) \mid c(g)c(h)$ implica che $f = c(f)$ divide uno tra $c(g)$ e $c(h)$. Quindi divide g o h.

(2.) Se f è un primitivo, irriducibile in $K[x]$, allora sappiamo che f è primo in $K[x]$. Infatti, $K[x]$ è un dominio euclideo, quindi in particolare un Dominio a Fattorizzazione Unica. Come conseguenza, f divide in $K[x]$ uno tra g o h. Tuttavia, siccome f è primitivo, per la Proposizione 4.10.11 la divisibilità avviene in $A[x]$. □

Possiamo procedere con la dimostrazione del secondo criterio del Teorema 4.10.5.

Teorema 4.10.15. *Ogni catena ascendente di ideali principali in $A[x]$ stabilizza.*

Dimostrazione. Consideriamo una catena $(f_0) \subseteq (f_1) \subseteq \dots$.

Da una parte otteniamo una catena di contenuti discendente $\cdots \mid c(f_1) \mid c(f_0)$. Siccome A è a Fattorizzazione Unica, allora $c(f_i)$ è associato a $c(f_{n_0})$ per ogni $i \geq n_0$.

Dall'altra parte, abbiamo anche una catena di divisibilità $\cdots \mid f_1' \mid f_0'$. Infatti da $f = gh$, otteniamo $c(g)c(h)f' = c(f)f' = c(g)c(h)g'h'$.

Da questa catena di divisibilità otteniamo una catena di naturali $\deg(f_0') \geq \deg(f_1') \geq \dots$ discendente. Quindi deve necessariamente stabilizzare, cioè $\deg(f_i') = \deg(f_{m_0}')$ per ogni $i \geq m_0$.

Quindi per ogni $i \geq m_0$, f_i' divide f_{m_0}' e inoltre hanno lo stesso grado. Quindi $f_i' = \lambda f_{m_0}'$ per qualche costante $\lambda \in A$. Tuttavia, siccome sia f_i' che f_{m_0}' sono primitivi, λ deve essere invertibile. Ergo f_i' e f_{m_0} sono in verità coniugati.

Abbiamo quindi dimostrato che definitivamente le catene $\{c(f_i)\}_i$ e $\{f_i'\}_i$ sono composte da elementi coniugati. Quindi ciò deve anche essere vero per $\{f_i = c(f_i)f_i'\}_i$. □

Dimostrazione del Teorema 4.10.7. È sufficiente unire il Teorema 4.10.5 con i Teoremi 4.10.14 e 4.10.15. □

Corollario 4.10.16. *Se A è un Dominio a Fattorizzazione Unica, allora $A[x_1, \dots, x_n]$ lo è.*

Dimostrazione. Semplice induzione. □

Anche se A è un campo, non possiamo dire di più.

Proposizione 4.10.17. *Se K è un campo, $K[x_1, \ldots, x_n]$ non è mai principale se n è almeno 2.*

Dimostrazione. Supponiamo che l'ideale $I := (x_1, \ldots, x_n)$ sia principale. Allora dovrebbe essere generato da un polinomio $a(x_1, \ldots, x_n)$.

Tuttavia, siccome x_1 appartiene a I, allora dovrebbe sussistere un'uguaglianza della forma $x_1 = ga$. Questo implica che $\deg_{x_i}(a) = 0$ per ogni $i \geq 2$. Quindi a è un polinomio nella sola variabile x_1.
Allo stesso modo, siccome x_2 appartiene a I, otteniamo che a è un elemento di $K[x_2]$. Ergo, a è una costante. Tuttavia, è immediato che $I = (x_1, \ldots, x_n)$ non contiene costanti. □

Il prossimo teorema è una generalizzazione dei Criterio di Eisenstein visto per gli interi.

Proposizione 4.10.18. *Sia A un Dominio a Fattorizzazione Unica, e $f = \sum a_n x^n$ un polinomio e P è un ideale primo di A, tali che*

1. *$a_i \notin P$;*
2. *$a_i \in P$ per ogni $i < n$;*
3. *$a_0 \in P \setminus P^2$.*

Allora f è irriducibile in $K[x]$.

Dimostrazione. Supponiamo che f si riduca in $K[x]$ come gh. Grazie alla Proposizione 4.10.12, possiamo supporre che i fattori appartengano a $A[x]$.

A questo punto, possiamo considerare la riduzione in $A/P[x]$, dove otteniamo $\bar{a}_n \bar{x}^n = \bar{g}\bar{h}$. Vogliamo affermare che $g = \bar{b}\bar{x}^m$ e $h = \bar{c}\bar{x}^{n-m}$.

Supponiamo quindi, senza perdita di generalità, che per g ciò non valga. Quindi $\bar{g}$ può essere scritto come $\sum_{k \leq i \leq m} \bar{b}_i \bar{x}^i$, con $k < m$. Analogamente, $\bar{h}$ si scrive come $\sum_{k' \leq i \leq n-m} \bar{c}_i \bar{x}^i$.

Successivamente, è sufficiente notare che l'insieme dei vari prodotti $\{\bar{b}_i \bar{x}^i \bar{c}_j \bar{x}^j\}_{i,j}$ contiene due prodotti che si scrivono in modo unico: $\bar{b}_k \bar{c}_{k'} \bar{x}^{k+k'}$ e $\bar{b}_m \bar{c}_{n-m} \bar{x}^n$ (i.e. i prodotti dei monimi di grado massimo e minimo).
Siccome A/P è un dominio, il primo prodotto non può essere nullo. Inoltre, siccome $\bar{a}_n \neq \bar{0}$, neanche può esserlo il secondo prodotto. Infine, siccome $k < m$, sappiamo che $k + k' < n$. Quindi il prodotto $\bar{g}\bar{h}$ contiene due monomi

non nulli di grado differente. Questo è un assurdo, in quanto $\bar{f}$ concide con $\bar{a}_0\bar{x}^n$.

Abbiamo quindi ottenuto che g e h coincidono con $\bar{b}\bar{x}^m$ e $h = \bar{c}\bar{x}^{n-m}$ rispettivamente. Tuttavia, otteniamo comunque una contraddizione, in quanto queste uguaglianze implicano che b_0 e c_0 appartengono a P. Quindi anche $a_0 = b_0c_0$ dovrebbe appartenere a P^2. Ma le ipotesi lo escludono. □

Corollario 4.10.19. *Se f soddisfa le condizioni del Criterio di Eisenstein ed è primitivo, allora è irriducibile in $A[x]$.*

Dimostrazione. Semplice applicazione della classificazione dei polinomi irriducibili. □

4.11 Gli interi di Gauss $\mathbb{Z}[i]$

Capitolo 5

Campi

Capitolo 6

Estensioni di Campi

Capitolo 7

Costruzioni con Riga e Compasso

Capitolo 8

Risolubilità per Radicali

Appendice A

Dimostrazioni Postposte

A.1 Il Teorema di Cantor-Bernstein-Schröder

In questa sezione proveremo il seguente teorema, fondamentale nella teoria degli insiemi:

Teorema A.1.1 (Teorema di Cantor-Bernstein-Schröder)**.** *Siano X e Y due insiemi. Se $|X| \leq |Y| \leq |X|$, allora $|X| = |Y|$.*

Dimostrazione. Supponiamo che esistano due funzioni iniettive $f\colon X \to Y$ e $g\colon Y \to X$.

Definiamo quindi per induzione i seguenti sottoinsiemi di X:

$$X_n = \begin{cases} X \setminus g(Y) & n = 0 \\ g(f(X_{n-1})) & n > 0 \end{cases}$$

Definiamo inoltre $h\colon X \to Y$ come

$$h(x) = \begin{cases} f(x) & \exists n\colon x \in X_n \\ g^{-1}(x) & \text{altrimenti} \end{cases}$$

Dobbiamo verificare che h sia ben definita, iniettiva e suriettiva.

1. Se x non appartiene a X_n per ogni n, allora in particolare $x \notin X_0 = X \setminus g(Y)$. Quindi x appartiene a $g(Y)$, e possiamo considerare $g^{-1}(x)$.

2. Se $h(x) = h(y)$, ed x e y rientrano nella stessa casistica, allora ovviamente $x = y$.

Se $x \in X_k$ e y non appartiene a nessun X_n, allora potremmo dire che

$$y = g(g^{-1}(y)) = g(h(y)) = g(h(x)) = g(f(x))$$

Di conseguenza $y \in g(f(X_k)) = X_{k+1}$. Otteniamo quindi una contraddizione.

3. Sia $y \in Y$. Se y appartiene a qualche $f(X_n)$, allora $y = f(x)$, con $x \in X_n$. Inoltre, per definizione di h, $f(x) = h(x)$. Quindi y appartiene all'immagine di h.

   Se, invece, non esiste n per cui $y \in f(X_n)$, poniamo $x := g(y)$. Vogliamo dimostrare, per assurdo, che x non appartiene a nessun X_n.

   Se $x \in X_0$, allora avremmo che $x = g(y) \in X \setminus g(Y)$. Otteniamo quindi una contraddizione.

   Se $x \in X_k$ per qualche $k > 0$, poniamo $k = j + 1$. Quindi X_k coincide con $g(f(X_j))$, e x coincide con $g(f(x'))$ per qualche $x' \in X_j$. Quindi, $y = g^{-1}(x)$ coincide con $f(x) \in f(X_j)$. Ma anche qui otteniamo una contraddizione, in quanto y non apparteneva a nessun $f(X_n)$.

   Abbiamo quindi dimostrato che x non appartiene ad alcun X_n. Ergo, $y = g^{-1}(x)$ coincide con $h(x)$.

□

A.2 Automorfismi di S_n

In questa sezione viene provato questo importante teorema:

Teorema A.2.1. *Se $n \geq 3$ e $n \neq 3$, allora gli automorfismi di S_n sono tutti interni, e $\mathrm{Aut}(S_n) \simeq S_n$.*

Certamente, siccome S_n ha centro banale per $n \geq 3$, allora $\mathrm{Inn}(S_n) \simeq S_n/Z(S_n)$ è isomorfo a S_n. Vogliamo capire se esistono automorfismi "esterni". La dimostrazione non è molto suggestiva, come già suggerisce il prossimo lemma.

Lemma A.2.2. *Per ogni intero $m > 4$, $(m-2)(m-3)/m$ è* strettamente *maggiore di 1. Inoltre per $m \geq 8$ allora $(m-2)(m-3)/m \geq 15/4$.*

Dimostrazione. Imponiamo $(m-2)(m-3) > m$. Questa condizione è equivalente a $m^2 - 6m + 6 > 0$. Una semplice verifica indica che questa condizione è verificata per ogni intero $m > 4$.

Ancora, se imponiamo $(m-2)(m-3) \geq 15/4m$, allora si può ottenere $m \geq 8$. □

Lemma A.2.3. *Un automorfismo di S_n è interno se e solo se manda trasposizioni in trasposizioni.*

Dimostrazione. Gli automorfismi interni di S_n preservano il tipo delle permutazioni. Quindi in particolare mandano trasposizioni in trasposizioni.

D'altra parte, supponiamo che la proprietà sia verificata da una generica $\varphi \in \mathrm{Aut}(S_n)$.

A questo punto consideriamo le trasposizioni

$$(1\,2), (1\,2), \ldots, (n-1\,n) \tag{A.1}$$

Esse generano S_n, quindi è sufficiente verificare che φ agisce per coniugio su di esse. Esse hanno la particolarità che ogni trasposizione commuta solo con le trasposizioni vicine. Questa proprietà deve essere preservata da φ.

Quindi $\varphi(1\,2) = (a\,b)$ e $\varphi(2\,3) = (c\,d)$, con $b = c$. Inoltre, $\varphi(3\,4)$ non può commutare con $(b\,c)$ ma con $(a\,b)$. Quindi $\varphi(3\,4) = (c\,e)$, con e una nuova lettera. Andando avanti otteniamo che è possibile definire una permutazione $\sigma \in S_n$ come $\sigma(1) = a$, $\sigma(2) = b$, $\sigma(3) = e$ etc.

Per costruzione, φ concorda con il coniugio per σ sulle trasposizioni (A.1). □

Dimostrazione del Teorema A.2.1. Sia φ un automorfismo di S_n. Esso permuta le classi di coniugio, e preserva anche gli ordini degli elementi. Come conseguenza, sappiamo che l'applicazione di φ a S_n implica una permutazione delle classi di coniugio

$$\{T_k\}_{1 \leq k \leq \lfloor n/2 \rfloor} := \{\mathcal{C}_{\tau_k}\}_{1 \leq k \leq \lfloor n/2 \rfloor}$$

dove τ_k sono gli unici elementi di S_n di ordine 2, cioè scomponibili in cicli come

$$\tau_k = (a_1\,b_1)(a_2\,b_2)\ldots(a_k\,b_k)$$

Se $n = 3$, abbiamo già concluso. Infatti k può solo essere 1. Quindi φ manda necessariamente trasposizioni in trasposizioni.

Supponiamo quindi che $n > 3$. Mostreremo che $|T_1| \neq |T_k|$ per ogni $k \neq 1$, $n > 3$ e $n \neq 6$. Questo implicherà che per tali n, $\varphi(T_1)$ non può coincidere con T_k se non per $k = 1$. Cioè, φ deve mandare trasposizioni in trasposizioni. A questo punto potremmo concludere col lemma precedente.

Analizziamo quindi $|T_k|$ (per $k > 1$). Esso è dato dalla formula seguente:

$$|T_k| = \frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2(k-1)}{2}$$

Essa deriva dal scegliere successivamente gli elementi per le k trasposizioni. Inoltre, possiamo permutare le k trasposizioni ed ottenere la stessa permutazione.

A questo punto, notiamo che la precedente espressione si può riscrivere come

$$\begin{aligned}|T_k| &= \binom{n}{2}\frac{(n-2)(n-3)}{2k}\frac{(n-4)(n-5)}{2k-2}\cdots\frac{(n-2k+2)(n-2k+1)}{4} \\ &= |T_1|\,\frac{(n-2)(n-3)}{2k}\frac{(n-4)(n-5)}{2k-2}\cdots\frac{(n-2k+2)(n-2k+1)}{4}\end{aligned}$$

Una generica frazione nel prodotto precedente è data da

$$\frac{(n-2-h)(n-3-h)}{2k-h} \tag{A.2}$$

con $0 \leq h \leq 2k-4$. Essa si può minorare da

$$\frac{(n-2-h)(n-3-h)}{2k-h} \geq \frac{(n-h-2)(n-h-3)}{n-h}$$

Dalle condizioni su h sappiamo che $n-4 \geq 2k-h \geq 4$. Quindi, dal Lemma A.2.2, sappiamo che la frazione (A.2) è strettamente maggiore di 1 *tranne eventualmente nell'ultima frazione.*

Essa infatti non è maggiore di 1 se $n-2k+4 = 4$, cioè se $n = 2k$. In tal caso (A.2) vale $1/2$.

Se $n = 4$, allora le possibilità sono solamente $k = 2$. In tal caso, $|T_2| = |T_1|/2 < |T_1|$.

Se $n = 2k \geq 8$, sempre per il Lemma A.2.2 sappiamo che la prima frazione vale almeno $15/4$. Quindi otteniamo che $|T_k| \geq 15/8|T_1| > |T_1|$. □

Osserviamo che $|T_1|$ coincide effettivamente con $|T_3|$ per $n = 6$. Quindi S_6 potrebbe avere automorfismi non interi. Ogni tale isomorfismo deve scambiare T_1 con T_3. In particolare, il prodotto di due automorfismi esterno è per

forza interno. Questo ci dice che $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6)$ è al più $\mathbb{Z}/2\mathbb{Z}$. In effetti è un'uguaglianza.

Teorema A.2.4. $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6) \simeq \mathbb{Z}/2\mathbb{Z}$.

A.3 Teorema di Wedderburn

In questa sezione viene dimostrato il teorema di Wedderburn, che riportiamo. La prima metà della dimostrazione ricalca l'idea originale di Wedderburn. La seconda parte, che usa i polinomi ciclotomici, è stata presentata per la prima volta in [1].

Teorema A.3.1 (di Wedderburn)**.** *Un corpo finito è necessariamente un campo.*

Ricordiamo che un corpo è un anello *anche non commutativo*, con identità, in cui ogni elemento non nullo ammette un inverso.

Svolgiamo un po' di lavoro preparativo.

Sia K un corpo finito. Definiamo il centro di K come

$$Z = \{x \in K \mid zx = xz \ \forall z \in K\}$$

Esso coincide con $\{0\} \cup Z_{gr}$, con Z_{gr} il centro del gruppo moltiplicativo $K^* = K \setminus \{0\}$.

Inoltre, per definizione, Z è un campo. Siccome K è finito, lo è anche Z. Quindi Z è isomorfo $\mathbb{F}_q = \mathbb{F}_{p^s}$. Inoltre, K è un Z-spazio vettoriale. Quindi $|K| = q^n$.

A questo punto, per ogni $a \in K$ definiamo il centralizzatore di a come

$$Z(a) = \{x \in K \mid ax = xa\}$$

Come prima, se $a \neq 0$, esso coincide con $\{0\} \cup Z_{gr}(a)$. Inoltre, vale il contenimento $Z \subseteq Z(a)$. Inoltre, anche quest'ultimo è un Z-spazio vettoriale. Poniamo quindi $|Z(a)| = q^{n(a)}$.

Lemma A.3.2. *$n(a)$ divide n.*

Dimostrazione. È sufficiente osservare che $Z_{gr}(a)$ è un sottogruppo di Z_{gr}. Quindi abbiamo una divisibilità delle cardinalità, cioè sappiamo che $|Z_{gr}(a)| = q^{n(a)} - 1$ divide $|Z_{gr}| = q^n - 1$. A questo punto concludiamo tramite la Proposizione **??**. □

A questo punto possiamo applicare la Formula delle Classi a K^*:

$$|K^*| = |Z_{gr}| + \sum_{K^* \setminus Z_{gr}} \frac{|K^*|}{|Z_{gr}(a)|}$$

cioè

$$q^n - 1 = q - 1 + \sum_{K^* \setminus Z_{gr}} \frac{q^n - 1}{q^{n(a)} - 1} \tag{A.3}$$

Ora che abbiamo svolto i lavori preparatori, possiamo procedere. La dimostrazione userà i polinomi ciclotomici. Denoteremo con Φ_d il d-esimo polinomio ciclotomico su $\mathbb{Q}$.

Lemma A.3.3. *Se d è un divisore proprio di n, allora Φ_n divide su $\mathbb{Z}[X]$ il rapporto $(X^n - 1)/(X^d - 1)$.*

Dimostrazione. Innanzitutto sappiamo che

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Ergo,

$$\frac{X^n - 1}{X^d - 1} = \prod_{k|n} \Phi_k(X) \cdot \left[\prod_{h|d} \Phi_h(X) \right]^{-1} = \prod_{\substack{k|n \\ k\nmid d}} \Phi_k(X)$$

L'ultima produttoria appartiene a $\mathbb{Z}[X]$, e contiene Φ_n. □

Dimostrazione del Teorema di Wedderburn. Supponiamo che K non è commutativo, cioè che $Z \neq K$. Questo implica che l'equazione (A.3) si verifica per qualche $n > 1$. Vogliamo ottenere una contraddizione.

Per ogni $a \in K^* \setminus Z_{gr}$, esso è un divisore proprio di $n(a)$. Quindi $\Phi_n(X)$ divide su $\mathbb{Z}[X]$ il rapporto $(X^n - 1)/(X^{n(a)} - 1)$; allora $\Phi_n(q)$ divide su $\mathbb{Z}$ il rapporto $(q^n - 1)/(q^{n(a)} - 1)$. Inoltre, questo implica che divide su $\mathbb{Z}$ anche $q^n - 1$.

D'altra parte, posto $\Phi_n(q) = \prod_{(n,k)=1}(q - \zeta_n^k)$, allora per ogni k nella produttoria possiamo osservare che

$$|q - \zeta_n^k| = \sqrt{\left(q - \cos\left(\frac{2k\pi}{n}\right)\right)^2 + \left(\sin\left(\frac{2k\pi}{n}\right)\right)^2} > \sqrt{(q-1)^2} = q - 1 \geq 1$$

Come conseguenza, otteniamo che se $n \neq 1$ allora $|\Phi_n(q)| = \prod_{(k,n)=1}|q - \zeta_n^k|$ è strettamente maggiore di $q - 1$.

A questo punto possiamo concludere. Infatti, se esistesse un $a \in K^* \setminus Z_{gr}$, allora $n > 1$. Ergo $|\Phi_n(q)| > q - 1$. Quindi non può esserci una divisibilità tra interi $\Phi_n(q) \mid q - 1$.
D'altra parte, $\Phi_n(q)$ divide sia la sommatoria, che il termine a sinistra, nell'equazione (A.3). Otteniamo quindi l'assurdo voluto. □

A.4 Dominio a Ideali Principali non Euclideo

In questa viene riportata la dimostrazione presente in [2].

Sia $\omega := (1 + \sqrt{-19})/2$. Vogliamo provare che $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ è Euclideo, ma non è a Ideali Principali.

Su questo anello è presente una norma, data dal coniugio complesso:

$$|\alpha| := \|\alpha\|_{\mathbb{C}}^2 = a^2 + ab + 19b^2$$

Osserviamo che questa norma *è sempre un numero naturale.*

Lemma A.4.1. *Sia $\alpha \in \mathbb{Z}[\omega]$. Allora le seguenti affermazioni sono equivalenti:*

1. $\alpha = \pm 1$;
2. $|\alpha|$ *è un'unità in* $\mathbb{Z}[\omega]$;
3. $|\alpha| = 1$.

Dimostrazione. (1. ⇒ 2.) Immediato.

(2. ⇒ 3.) Se $\alpha\beta = 1$, allora $1 = |\alpha||\beta|$. Siccome la norma è naturale, otteniamo $|\alpha| = 1$.

(3. ⇒ 1.) Posto $\alpha = a + b\omega$, allora $1 = a^2 + ab + 19b^2$. A questo punto osserviamo che

$$1 = a^2 + ab + 19b^2 = (a + b/2)^2 + 19b^2/4.$$

Siccome $19/4 > 4$ e a, b sono interi, allora $b = 0$ e conseguentemente $a = \pm 1$. □

A questo punto dobbiamo trovare degli speciali irriducibili. Essi sono ± 2 e ± 3.

Lemma A.4.2. ± 2 *e* ± 3 *sono irriducibili.*

Dimostrazione. Siccome ± 1 sono unità, è sufficiente dimostrare l'irriducibilità di 2 e 3.

Se $2 = \alpha\beta$, allora passando alle norme otteniamo $4 = |\alpha||\beta|$. Siccome le norme sono dei numeri naturali, allora sappiamo che le uniche possibilità per $(|\alpha|, |\beta|)$ sono $(2,2)$, $(1,4)$ e $(4,1)$.
Se siamo nel primo o terzo caso, allora per il Lemma A.4.1 α o β sono invertibili. Altrimenti, siamo nella situazione in cui

$$2 = |\alpha| = (a + b/2)^2 + 19b^2/4$$

Come nel caso di ± 1, b è forzato ad essere nullo. Quindi $a^2 = 2$, che dà la contraddizione voluta.

Il caso $3 = \alpha\beta$ è completamente analogo. □

Teorema A.4.3. *L'anello $\mathbb{Z}[\omega]$ non è un Dominio Euclideo.*

Dimostrazione. Supponiamo che $\mathbb{Z}[\omega]$ sia un Dominio Euclideo. Allora dovrebbe esistere una norma D, che soddisfa le proprietà della Definizione 4.9.13.

Consideriamo $m \in \mathbb{Z}[\omega]$ non nullo e non invertibile, tale che $D(m)$ sia minimo (ovviamente $\mathbb{Z}[\omega]$ non è un campo). Vogliamo affermare che m appartiene a $\{\pm 2, \pm 3\}$.

Poniamo $2 = qm + r$. Siccome $r = 0$, o $D(r) < D(m)$, sappiamo che r è nullo o è un unità.

1. Se $r = 0$, allora m divide 2. Siccome quest'ultimo è irriducibile e siccome m non è unità, allora $2/m$ deve essere ± 1 (ricordiamo che quest ultime sono le uniche unità di $\mathbb{Z}[\omega]$). Quindi m è ± 2.

2. Se $r = -1$, allora $qm = 2 - r = 3$. Quindi m divide 3. Come nel punto precedente, in questo caso otteniamo che $m = \pm 3$.

3. Se $r = 1$, allora m divide 1. Cioè m dovrebbe essere un'unità. Ma questo non è possibile.

A questo punto, procediamo con una ulteriore divisione euclidea: $\omega = q'm + r'$. Come per r, r' può solo essere 0 o ± 1.

1. Se $r' = 0$, allora m dovrebbe dividere ω in $\mathbb{Z}[\omega]$. Ma il rapporto (complesso) ω/m appartiene a $\{\pm\omega/2, \pm\omega/3\}$. Ma nessuno di questi elementi appartiene a $\mathbb{Z}[\omega]$.

2. Se $r' = 1$, allora un elemento di $\mathbb{Z}[\omega]$ dovrebbe essere trovato in $\{\pm(-1+\omega)/2, \pm(-1+\omega)/3\}$. Ma neanche questo insieme non interseca $\mathbb{Z}[\omega]$.

3. Infine, se $r' = -1$, allora l'elemento in $\mathbb{Z}[\omega]$ dovrebbe poter essere trovato in $\{\pm(1+\omega)/2, \pm(1+\omega)/3\}$. Anche qua abbiamo un intersezione vuota con $\mathbb{Z}[\omega]$.

□

Teorema A.4.4. *L'anello $\mathbb{Z}[\omega]$ è un Dominio a Ideali Principali.*

Dimostrazione. Consideriamo un ideale I non nullo, e consideriamo β di norma minore tra gli elementi di $I \setminus \{0\}$. Affermiamo che $I = (\beta)$.

Consideriamo un certo $\alpha \in I$, e consideriamo $\alpha/\beta \in \mathbb{C}$.

Sappiamo che la parte immaginaria $\mathrm{Im}(\omega)$ è $\sqrt{19}/2$. Ergo, possiamo considerare un intero m tale che

$$-\tfrac{\sqrt{19}}{4} < \mathrm{Im}(\alpha/\beta + m\omega) \leq \tfrac{\sqrt{19}}{4}$$

Analizziamo adesso differenti casi.

1. Supponiamo che la parte immaginaria di $\alpha/\beta + m\omega$ sia strettamente compresa tra $-\sqrt{3}/2$ e $\sqrt{3}/2$.

   In questo caso, consideriamo un intero n tale che la parte reale di $\alpha/\beta + m\omega + n$ soddisfi

   $$-\tfrac{1}{2} < \mathrm{Re}(\alpha/\beta + m\omega + n) \leq \tfrac{1}{2}$$

   Inoltre, siccome la parte immaginaria è rimasta invariata, vale anche

   $$-\tfrac{\sqrt{3}}{2} < \mathrm{Im}(\alpha/\beta + m\omega + n) < \tfrac{\sqrt{3}}{2}$$

   Quindi, abbiamo ottenuto la seguente disuguaglianza:

   $$|\alpha/\beta + m\omega + n| < (1/2)^2 + (\sqrt{3}/2)^2 = 1$$

   Inoltre,

   $$|\alpha + (m\omega + n)\beta| = |\alpha/\beta + m\omega + n||\beta| < |\beta|$$

   Tuttavia, $\alpha + (m\omega + n)\beta$ è un elemento di I. Quindi, la disuguaglianza precedente implica che sia nullo. Ergo α coincide con $-(m\omega + n)\omega$, che appartiene a (β).

2. Supponiamo invece che

$$-\tfrac{\sqrt{19}}{4} < \mathrm{Im}(\alpha/\beta + m\omega) \leq -\tfrac{\sqrt{3}}{2}$$

oppure

$$\tfrac{\sqrt{3}}{2} \leq \mathrm{Im}(\alpha/\beta + m\omega) \leq \tfrac{\sqrt{19}}{4}$$

Nel primo caso, poniamo $\alpha' := -\alpha - m\omega\beta$.

Nel secondo caso, invece, sia $\alpha' := \alpha + m\omega\beta$.

In entrambi i casi otteniamo un elemento di I.

Osserviamo che comunque α' sia definito, sicuramente

$$\tfrac{\sqrt{3}}{2} \leq \mathrm{Im}(\alpha'/\beta) \leq \tfrac{\sqrt{19}}{4}$$

A questo punto, come già fatto, consideriamo $n \in \mathbb{Z}$ tale che

$$-\tfrac{1}{2} < \mathrm{Re}(\alpha'/\beta + n) \leq \tfrac{1}{2}$$

Definiamo quindi $\alpha'' := \alpha' + n\beta \in I$. Siccome α''/β coincide con $\alpha'/\beta + n$, allora sappiamo che

$$\begin{aligned} -\tfrac{1}{2} &< \mathrm{Re}(\alpha''/\beta) \leq \tfrac{1}{2} \\ \tfrac{\sqrt{3}}{2} &\leq \mathrm{Im}(\alpha''/\beta) \leq \tfrac{\sqrt{19}}{4} \end{aligned}$$

Spostiamo ora l'attenzione su α''. In tal senso, consideriamo $2\alpha''/\beta - \omega \in \mathbb{C}$. Sappiamo che

$$\begin{aligned} -\tfrac{3}{2} < \mathrm{Re}(\tfrac{2\alpha''}{\beta} - \omega) &\leq \tfrac{1}{2} \\ -\tfrac{\sqrt{3}}{2} < \sqrt{3} - \tfrac{\sqrt{19}}{2} \leq \mathrm{Im}(\tfrac{2\alpha''}{\beta} - \omega) &\leq 0 \end{aligned}$$

(per non usare una calcolatrice possiamo usare che $\sqrt{19} < \sqrt{27} = 3\sqrt{3}$).

A questo punto possiamo procedere per due sub-casi. Otterremo una contraddizione in entrambi.

a) Supponiamo che

$$-\tfrac{1}{2} < \mathrm{Re}(\tfrac{2\alpha''}{\beta} - \omega) \leq \tfrac{1}{2}$$

In questo caso, $|2\alpha''/\beta - \omega|$ è strettamente minore di $(1/2)^2 + (-\sqrt{3}/2)^2 = 1$. Quindi,

$$|2\alpha'' - \omega\beta| = |2\alpha''/\beta - \omega||\beta| < |\beta|$$

Quindi, per la scelta fatta a β all'inizio del teorema, sappiamo che $2\alpha'' - \omega\beta$ è nullo. Questo implica che $\omega\beta/2$ coincide con α'', e quindi appartiene a I.

A questo punto, osserviamo che

$$\tfrac{1}{2}\beta = \tfrac{5}{2}\beta - 2\beta = \overline{\omega}\tfrac{\omega\beta}{2} - 2\beta \in I$$

Ma qui troviamo una contraddizione, in quanto $|\beta/2| < |\beta|$.

b) Supponiamo invece che

$$-\tfrac{3}{2} < \mathrm{Re}(\tfrac{2\alpha''}{\beta} - \omega) \leq -\tfrac{1}{2}$$

In questo sub-caso, consideriamo $2\alpha''/\beta - \omega + 1 \in \mathbb{C}$. Chiaramente,

$$-\tfrac{1}{2} < \mathrm{Re}(\tfrac{2\alpha''}{\beta} - \omega + 1) \leq \tfrac{1}{2}$$

e

$$-\tfrac{\sqrt{3}}{2} < \mathrm{Im}(\tfrac{2\alpha''}{\beta} - \omega + 1) \leq 0$$

Quindi, con lo stesso ragionamento del sotto-caso precedente, otteniamo che $2\alpha'' - \omega\beta + \beta$ è nullo. Quindi $(\omega - 1)\beta/2$ coincide con α'', e appartiene a I.

Come prima, dal fatto che $(\overline{\omega - 1})(\omega - 1) = 5$, otteniamo che $\beta/2$ appartiene a I. Da qui otteniamo una contraddizione.

□

Bibliografia

[1] Ernst Witt. «Über die kommutativität edlicher schiefkörper». In: *Abh. Math. Sem. Univ. Hamburg* 8.1 (1931), p. 413.

[2] Conan Wong. «On a Principal Ideal Domain that is not a Euclidean Domain». In: *International Mathematical Forum* 8.29 (2013), pp. 1405–1412. URL: http://dx.doi.org/10.12988/imf.2013.37144.